Documentación de Active IQ Unified Manager

Active IQ Unified Manager 9.12

NetApp
October 16, 2025

This PDF was generated from https://docs.netapp.com/es-es/active-iq-unified-manager-912/index.html on October 16, 2025. Always check docs.netapp.com for the latest.

Tabla de contenidos

Documentación de Active IQ Unified Manager . . . 1
Notas de la versión . . . 2
Manos a la obra . . . 3
Instrucciones de inicio rápido para instalaciones de VMware . . . 3
Requisitos del sistema . . . 3
Instalando Active IQ Unified Manager . . . 3
Instrucciones de inicio rápido para instalaciones Linux . . . 4
Requisitos del sistema . . . 4
Instalando Active IQ Unified Manager . . . 4
Instrucciones de inicio rápido para instalaciones de Windows . . . 5
Requisitos del sistema . . . 5
Instalando Active IQ Unified Manager . . . 6
Instale Unified Manager en sistemas VMware vSphere . . . 7
Introducción a Active IQ Unified Manager . . . 7
Lo que hace Unified Manager Server . . . 7
Descripción general de la secuencia de instalación . . . 7
Requisitos para instalar Unified Manager . . . 8
Requisitos del sistema de hardware e infraestructura virtual . . . 8
Requisitos de instalación y software de VMware . . . 10
Exploradores compatibles . . . 10
Requisitos de protocolo y puerto . . . 11
Rellenar la hoja de cálculo . . . 14
Instalación, actualización y eliminación del software Unified Manager . . . 16
Información general del proceso de implementación . . . 16
Ponga en marcha Unified Manager . . . 17
Actualizar Unified Manager . . . 21
Reiniciar la máquina virtual de Unified Manager . . . 24
Se quita Unified Manager . . . 24
Instale Unified Manager en sistemas Linux . . . 26
Introducción a Active IQ Unified Manager . . . 26
Lo que hace Unified Manager Server . . . 26
Descripción general de la secuencia de instalación . . . 26
Requisitos para instalar Unified Manager . . . 27
Requisitos del sistema de hardware e infraestructura virtual . . . 27
Requisitos de instalación y software Linux . . . 29
Exploradores compatibles . . . 31
Requisitos de protocolo y puerto . . . 31
Rellenar la hoja de cálculo . . . 34
Instalación, actualización y eliminación del software Unified Manager . . . 36
Descripción general del proceso de instalación . . . 36
Configurar repositorios de software necesarios . . . 37
Requisitos de SELinux en recursos compartidos NFS y CIFS . . . 39
Instalación de Unified Manager en sistemas Linux . . . 42

Actualización de Unified Manager en Red Hat Enterprise Linux o CentOS . . . 48
Actualización de productos de terceros tras la instalación de Unified Manager . . . 54
Reiniciar Unified Manager . . . 54
Se quita Unified Manager . . . 55
Quitar el usuario personalizado de umadmin y el grupo de mantenimiento . . . 56
Instale Unified Manager en sistemas Windows . . . 57
Introducción a Active IQ Unified Manager . . . 57
Lo que hace Unified Manager Server . . . 57
Descripción general de la secuencia de instalación . . . 57
Requisitos para instalar Unified Manager . . . 58
Requisitos del sistema de hardware e infraestructura virtual . . . 58
Requisitos de instalación y software de Windows . . . 60
Exploradores compatibles . . . 61
Requisitos de protocolo y puerto . . . 62
Rellenar la hoja de cálculo . . . 64
Instalación, actualización y eliminación del software Unified Manager . . . 66
Descripción general del proceso de instalación . . . 66
Instalación de Unified Manager en Windows . . . 67
Cambio de la contraseña de JBoss . . . 70
La ruta de actualización compatible con las versiones de Unified Manager . . . 71
Actualizar Unified Manager . . . 72
Actualizar productos de terceros . . . 73
Reiniciar Unified Manager . . . 74
Desinstale Unified Manager . . . 75
Realizar tareas administrativas y de configuración . . . 77
Configurando Active IQ Unified Manager . . . 77
Descripción general de la secuencia de configuración . . . 77
Acceder a la interfaz de usuario web de Unified Manager . . . 77
Realizando la configuración inicial de la interfaz de usuario web de Unified Manager . . . 78
Añadir clústeres . . . 80
Configuración de Unified Manager para enviar notificaciones de alerta . . . 82
Cambiando la contraseña de usuario local . . . 91
Configurar el tiempo de espera de inactividad de la sesión . . . 92
Cambie el nombre de host de Unified Manager . . . 92
Habilitar y deshabilitar la gestión del almacenamiento basada en políticas . . . 97
Configuración de backup de Unified Manager . . . 98
Gestión de la configuración de funciones . . . 98
Permitir la gestión del almacenamiento basada en políticas . . . 99
Habilitar API Gateway . . . 99
Especificación del tiempo de espera de inactividad . . . 100
Habilitar los eventos del portal de Active IQ . . . 100
Activación y desactivación de la configuración de seguridad para cumplir las normativas . . . 101
Habilitar y deshabilitar la carga de scripts . . . 102
Adición de un banner de inicio de sesión . . . 102
Mediante la consola de mantenimiento . . . 102

Qué funcionalidad proporciona la consola de mantenimiento . . . 103
Lo que hace el usuario de mantenimiento . . . 103
Capacidades de diagnóstico del usuario . . . 103
Acceso a la consola de mantenimiento . . . 103
Acceder a la consola de mantenimiento mediante la consola de la máquina virtual de vSphere . . . 104
Menús de la consola de mantenimiento . . . 105
Cambiar la contraseña del usuario de mantenimiento en Windows . . . 110
Cambiar la contraseña de umadmin en sistemas Linux . . . 110
Cambiar los puertos Unified Manager utiliza para los protocolos HTTP y HTTPS . . . 111
Se añaden interfaces de red . . . 112
Agregar espacio en disco al directorio de la base de datos de Unified Manager . . . 112
Gestión del acceso de usuarios . . . 116
Adición de usuarios . . . 116
Edición de la configuración de usuario . . . 118
Ver usuarios . . . 118
Eliminación de usuarios o grupos . . . 119
Qué es RBAC . . . 119
Qué hace el control de acceso basado en roles . . . 119
Definiciones de tipos de usuario . . . 119
Definiciones de roles de usuario . . . 120
Roles y funcionalidades de usuario de Unified Manager . . . 121
Gestión de la configuración de autenticación SAML . . . 123
Requisitos del proveedor de identidades . . . 124
Habilitación de la autenticación SAML . . . 125
Cambiar el proveedor de identidades utilizado para la autenticación SAML . . . 126
Actualizar la configuración de autenticación SAML después de cambiar el certificado de seguridad de Unified Manager . . . 127
Deshabilitación de la autenticación SAML . . . 128
Deshabilitar la autenticación SAML de la consola de mantenimiento . . . 129
Página autenticación SAML . . . 129
Gestión de la autenticación . . . 130
Editar servidores de autenticación . . . 131
Eliminar servidores de autenticación . . . 131
Autenticación con Active Directory u OpenLDAP . . . 131
Registro de auditoría . . . 132
Autenticación remota . . . 135
Gestión de certificados de seguridad . . . 138
Visualizar el certificado de seguridad HTTPS . . . 138
Descargar una solicitud de firma de certificación HTTPS . . . 138
Instalar una CA firmada y devolvió un certificado HTTPS . . . 139
Instalar un certificado HTTPS generado con herramientas externas . . . 140
Descripciones de página para la gestión de certificados . . . 142
Supervisar y gestionar el almacenamiento . . . 145
Introducción a Active IQ Unified Manager . . . 145
Introducción a la supervisión del estado de Active IQ Unified Manager . . . 145

Introducción a la supervisión del rendimiento de Active IQ Unified Manager . . . 146
Usar API de REST de Unified Manager . . . 147
Lo que hace Unified Manager Server . . . 147
La interfaz de usuario . . . 148
Diseños de ventana típicos . . . 148
Personalización del diseño de ventanas . . . 149
Uso de la ayuda de Unified Manager . . . 150
Guardado de marcadores de sus temas favoritos de la Ayuda . . . 151
Buscar objetos de almacenamiento . . . 151
Exportar datos de almacenamiento como informes . . . 152
Filtrado del contenido de la página de inventario . . . 154
Ver eventos activos desde el timbre de notificación . . . 155
Supervisar y gestionar clústeres desde la consola . . . 155
Consola . . . 156
Gestión de problemas o funciones de ONTAP directamente desde Unified Manager . . . 159
Gestionar clústeres . . . 167
Cómo funciona el proceso de detección del clúster . . . 167
Se muestra la lista de clústeres supervisados . . . 168
Añadir clústeres . . . 168
Editar clústeres . . . 171
Quitar clústeres . . . 171
Volver a detectar clústeres . . . 172
Supervisión de la infraestructura virtual de VMware . . . 172
Qué no se admite . . . 175
Ver y añadir vCenter Server . . . 176
Supervisar máquinas virtuales . . . 178
Visualización de la infraestructura virtual en una configuración de recuperación ante desastres . . . 180
Aprovisionamiento y gestión de cargas de trabajo . . . 182
Información general de cargas de trabajo . . . 183
Niveles de servicio de rendimiento . . . 190
Gestión de políticas de eficiencia del almacenamiento . . . 197
Gestionar y supervisar configuraciones de MetroCluster . . . 199
Comportamiento del volumen durante la conmutación de sitios y la conmutación de estado . . . 200
Definiciones de estado de conectividad de clúster para la configuración de MetroCluster over FC . . . 202
Definiciones de estado de mirroring de datos para MetroCluster over FC . . . 203
Supervisar las configuraciones de MetroCluster . . . 203
Supervisar la replicación de MetroCluster . . . 206
Gestión de cuotas . . . 207
Qué límites de cuota son . . . 207
Visualización de cuotas de usuarios y grupos de usuarios . . . 207
Creación de reglas para generar direcciones de correo electrónico . . . 208
Creación de un formato de notificación por correo electrónico para cuotas de usuarios y grupos de usuarios . . . 209
Edición de direcciones de correo electrónico de cuotas de usuarios y grupos . . . 209
Más información acerca de las cuotas . . . 210

Descripción de los cuadros de diálogo cuotas . . . 211
Resolución de problemas . . . 214
Agregar espacio en disco al directorio de la base de datos de Unified Manager . . . 214
Cambiar el intervalo de recogida de estadísticas de rendimiento . . . 218
Cambiar el periodo de tiempo, Unified Manager conserva los datos de eventos y rendimiento . . . 219
Error de autenticación desconocido . . . 220
Usuario no encontrado . . . 220
Problema al agregar LDAP mediante otros servicios de autenticación . . . 220
Gestionar eventos y alertas . . . 222
Gestión de eventos . . . 222
¿Qué son los eventos de la plataforma Active IQ . . . 222
Qué son los eventos del sistema de gestión de eventos . . . 222
Qué sucede cuando se recibe un evento . . . 228
Ver eventos y detalles de eventos . . . 230
Visualización de eventos sin asignar . . . 231
Reconocer y resolver eventos . . . 231
Asignar eventos a usuarios específicos . . . 232
Deshabilitar eventos no deseados . . . 233
Solución de problemas mediante la solución automática de Unified Manager . . . 234
Habilitar y deshabilitar la generación de informes de eventos de Active IQ . . . 235
Carga de un nuevo archivo de reglas de Active IQ . . . 236
Cómo se generan los eventos de la plataforma Active IQ . . . 237
Resolver eventos de la plataforma Active IQ . . . 237
Configuración de los ajustes de retención de eventos . . . 238
Qué es una ventana de mantenimiento de Unified Manager . . . 238
Gestionar eventos de recursos del sistema host . . . 241
Más información acerca de los eventos . . . 241
Lista de eventos y tipos de gravedad . . . 247
Descripción de ventanas de eventos y cuadros de diálogo . . . 309
Gestión de alertas . . . 322
¿Qué alertas son . . . 322
Qué información se incluye en un correo electrónico de alerta . . . 322
Adición de alertas . . . 323
Adición de alertas para eventos de rendimiento . . . 326
Probar alertas . . . 327
Habilitar y deshabilitar alertas para eventos resueltos y obsoletos . . . 327
No se incluye el hecho de que los volúmenes de destino de recuperación ante desastres generen alertas . . . 328
Visualizar alertas . . . 329
Editar alertas . . . 329
Eliminar alertas . . . 330
Descripción de ventanas de alerta y cuadros de diálogo . . . 330
Administrar scripts . . . 336
Cómo funcionan los scripts con alertas . . . 336
Añadiendo scripts . . . 337

Eliminar scripts . . . 338
Prueba de la ejecución de scripts . . . 339
Comandos de CLI de Unified Manager compatibles . . . 339
Descripción de ventanas de script y cuadros de diálogo . . . 345
Supervise y gestione el rendimiento de los clústeres . . . 347
Introducción a la supervisión del rendimiento de Active IQ Unified Manager . . . 347
Funciones de supervisión del rendimiento de Unified Manager . . . 347
Las interfaces de Unified Manager que se utilizan para gestionar el rendimiento del sistema de almacenamiento . . . 348
Actividad de recogida de datos de rendimiento y configuración del clúster . . . 348
Qué es un ciclo de recopilación de continuidad de datos . . . 350
Lo que significa la Marca de hora en los datos y eventos recopilados . . . 351
Navegar por los flujos de trabajo de rendimiento en la interfaz gráfica de usuario de Unified Manager . . . 351
Iniciar sesión en la interfaz de usuario de . . . 352
Interfaz gráfica y rutas de navegación . . . 352
Buscar objetos de almacenamiento . . . 358
Filtrado del contenido de la página de inventario . . . 359
Supervisar el rendimiento del clúster en la consola de . . . 361
Descripción de los paneles de rendimiento de la consola . . . 361
Mensajes y descripciones de banner de rendimiento . . . 362
Cambiar el intervalo de recogida de estadísticas de rendimiento . . . 362
Solucionar problemas de cargas de trabajo mediante el analizador de cargas de trabajo . . . 363
¿Qué datos muestra el analizador de cargas de trabajo . . . 364
¿Cuándo se debe utilizar el analizador de cargas de trabajo . . . 365
Mediante el analizador de cargas de trabajo . . . 366
Supervisar el rendimiento del clúster en la página Performance Cluster Landing . . . 366
Descripción de la página de destino del clúster de rendimiento . . . 367
Página de destino de Cluster de rendimiento . . . 367
Supervisión del rendimiento mediante las páginas Performance Inventory . . . 372
Ver las páginas de inventario de rendimiento para todos los objetos de almacenamiento . . . 373
Afinar el contenido de la página del inventario de rendimiento . . . 379
Descripción de las recomendaciones de Unified Manager para organizar los datos en niveles en el cloud . . . 381
Supervisión del rendimiento mediante las páginas Performance Explorer . . . 383
Descripción del objeto raíz . . . 383
Aplicar filtrado para reducir la lista de objetos correlacionados de la cuadrícula . . . 383
Especificación de un intervalo de tiempo para objetos correlacionados . . . 383
Definir la lista de objetos correlacionados para la representación gráfica de comparación . . . 385
Gráficos de contadores . . . 386
Tipos de gráficos de contadores de rendimiento . . . 387
Selección de gráficos de rendimiento para mostrar . . . 391
Ampliación del panel Contador de gráficos . . . 391
Cambiar el enfoque de los gráficos de contador a un período de tiempo más corto . . . 391
Visualización de detalles de eventos en la línea de tiempo de eventos . . . 392
Vista de zoom de las cartas de contador . . . 393

Ver la latencia de volumen por componente del clúster . . . 395
Ver tráfico de IOPS de SVM por protocolo . . . 396
Vea los gráficos de latencia de volúmenes y LUN para verificar la garantía de rendimiento . . . 397
Visualización del rendimiento de los clústeres de cabinas All SAN . . . 397
Ver las IOPS de los nodos según las cargas de trabajo que solo residen en el nodo local . . . 398
Componentes de las páginas de destino de objetos . . . 398
Gestione el rendimiento mediante información del grupo de políticas de calidad de servicio . . . 404
Cómo la calidad de servicio de almacenamiento puede controlar el rendimiento de la carga de trabajo 405
Ver todos los grupos de políticas de calidad de servicio disponibles en todos los clústeres . . . 406
Ver volúmenes o LUN que estén en el mismo grupo de políticas de calidad de servicio . . . 406
Ver la configuración del grupo de políticas de calidad de servicio aplicable a volúmenes o LUN específicos . . . 407
Ver los gráficos de rendimiento para comparar volúmenes o LUN que están en el mismo grupo de políticas de calidad de servicio . . . 408
Cómo se muestran los diferentes tipos de políticas de calidad de servicio en los gráficos de rendimiento . . . 408
Ver la configuración mínima y máxima de calidad de servicio de la carga de trabajo en el Explorador de rendimiento . . . 410
Gestión del rendimiento mediante la capacidad de rendimiento y la información de IOPS disponible . . . 411
La capacidad de rendimiento utilizada . . . 412
Qué significa el valor de capacidad de rendimiento utilizada . . . 413
Qué es IOPS disponible . . . 414
Ver los valores de capacidad de rendimiento de los nodos y los agregados . . . 415
Ver los valores de IOPS disponibles de los nodos y los agregados . . . 416
Ver los gráficos de contadores de capacidad de rendimiento para identificar los problemas . . . 416
La capacidad de rendimiento utilizada condiciones de umbral de rendimiento . . . 418
Uso del contador de capacidad de rendimiento utilizada para gestionar el rendimiento . . . 419
Comprender y utilizar la página Node Failover Planning . . . 420
Uso de la página Planificación de conmutación por error de nodos para determinar las acciones correctivas . . . 420
Componentes de la página Node Failover Planning . . . 420
Uso de una directiva de umbral con la página Planificación de conmutación por error de nodos . . . 422
Usar el gráfico de desglose de capacidad de rendimiento utilizada para la planificación de conmutación por error . . . 422
Recogida de datos y supervisión del rendimiento de carga de trabajo . . . 424
Tipos de cargas de trabajo supervisadas por Unified Manager . . . 424
Valores de medición del rendimiento de la carga de trabajo . . . 425
Qué rango esperado de rendimiento es . . . 427
Cómo se utiliza el pronóstico de latencia en el análisis de rendimiento . . . 428
Cómo Unified Manager utiliza la latencia de carga de trabajo para identificar problemas de rendimiento . . . 429
Cómo las operaciones del clúster pueden afectar a la latencia de carga de trabajo . . . 430
Supervisión del rendimiento de las configuraciones de MetroCluster . . . 431
Comprender los eventos y las alertas de rendimiento . . . 432
Fuentes de eventos de rendimiento . . . 432

Tipos de gravedad de eventos de rendimiento . . . 433
Cambios de configuración detectados por Unified Manager . . . 434
Tipos de políticas de umbral de rendimiento definidas por el sistema . . . 434
Análisis y notificación de eventos de rendimiento . . . 437
La forma en que Unified Manager determina el impacto en el rendimiento de un evento . . . 439
Los componentes del clúster y el motivo por los que pueden estar en contención . . . 440
Funciones de las cargas de trabajo involucradas en un evento de rendimiento . . . 442
Gestión de los umbrales de rendimiento . . . 443
Cómo funcionan las políticas de umbral de rendimiento definidas por el usuario . . . 443
Qué sucede cuando se incumple una política de umbral de rendimiento . . . 445
Se puede realizar un seguimiento de los contadores de rendimiento mediante umbrales . . . 446
Qué objetos y contadores pueden utilizarse en políticas de umbral de combinación . . . 448
Creación de políticas de umbral de rendimiento definidas por el usuario . . . 449
Asignación de políticas de umbral de rendimiento a objetos de almacenamiento . . . 450
Ver las políticas de umbral de rendimiento . . . 451
Editar políticas de umbral de rendimiento definidas por el usuario . . . 452
Eliminación de políticas de umbral de rendimiento de objetos de almacenamiento . . . 452
Qué ocurre cuando se cambia una política de umbral de rendimiento . . . 453
Qué sucede con las políticas de umbral de rendimiento cuando se mueve un objeto . . . 453
Análisis de eventos de rendimiento . . . 454
Mostrar información acerca de los eventos de rendimiento . . . 455
Análisis de eventos de umbrales de rendimiento definidos por el usuario . . . 455
Analizar eventos de umbrales de rendimiento definidos por el sistema . . . 456
Analizar eventos de umbrales dinámicos de rendimiento . . . 462
Resolver eventos de rendimiento . . . 470
Confirmación de que la latencia se encuentra dentro del rango esperado . . . 470
Revise el impacto de los cambios de configuración en el rendimiento de la carga de trabajo . . . 471
Opciones para mejorar el rendimiento de las cargas de trabajo desde el cliente . . . 471
Compruebe si existen problemas con los clientes o la red . . . 471
Verifique si otros volúmenes del grupo de políticas de calidad de servicio tienen una actividad inusualmente alta . . . 472
Mover interfaces lógicas (LIF) . . . 472
Ejecute operaciones de eficiencia del almacenamiento en momentos de menor actividad . . . 473
Añada discos y reasigne datos . . . 474
Cómo habilitar Flash Cache en un nodo puede mejorar el rendimiento de la carga de trabajo . . . 474
Cómo habilitar Flash Pool en un agregado de almacenamiento puede mejorar el rendimiento de la carga de trabajo . . . 475
Comprobación del estado de la configuración de MetroCluster . . . 475
Verificación de la configuración de MetroCluster . . . 476
Mover las cargas de trabajo a otro agregado . . . 476
Mover las cargas de trabajo a un nodo diferente . . . 478
Mover las cargas de trabajo a un agregado en un nodo diferente . . . 479
Mover cargas de trabajo a un nodo en un par de alta disponibilidad diferente . . . 481
Mover cargas de trabajo a otro nodo en un par de alta disponibilidad diferente . . . 482
Utilice la configuración de la política de calidad de servicio para priorizar el trabajo de este nodo . . . 484

Quite los volúmenes y las LUN inactivos . . . 485
Añada discos y realice la reconstrucción de distribución de agregados . . . 485
Configuración de una conexión entre un servidor Unified Manager y un proveedor de datos externo . . . 486
Datos de rendimiento que se pueden enviar a un servidor externo . . . 486
Configurar Graphite para obtener datos de rendimiento de Unified Manager . . . 487
Configuración de una conexión desde un servidor de Unified Manager con un proveedor de datos externo . . . 488
Supervise y gestione el estado del clúster . . . 491
Introducción a la supervisión del estado de Active IQ Unified Manager . . . 491
Capacidad física y lógica . . . 491
Unidades de medida de capacidad . . . 491
Funciones de supervisión del estado de Unified Manager . . . 492
Las interfaces de Unified Manager que se utilizan para gestionar el estado del sistema de almacenamiento . . . 493
Gestionar y supervisar clústeres y el estado de objetos del clúster . . . 494
Supervisión del clúster . . . 494
Ver la lista del clúster y sus detalles . . . 496
Comprobar el estado de los clústeres en una configuración de MetroCluster . . . 496
Ver el estado y la capacidad de los clústeres de la cabina All SAN . . . 498
Ver la lista y los detalles del nodo . . . 499
Generar un informe de inventario de hardware para la renovación de contrato . . . 500
Consulte la lista y los detalles de la máquina virtual de almacenamiento . . . 500
Consulte la lista de agregados y los detalles . . . 501
Visualización de información de capacidad de FabricPool . . . 501
Ver los detalles del pool de almacenamiento . . . 503
Ver la lista de volúmenes y los detalles . . . 503
Ver detalles acerca de los recursos compartidos de NFS . . . 504
Ver detalles sobre los recursos compartidos de SMB/CIFS . . . 505
Ver la lista de copias Snapshot . . . 506
Eliminar copias Snapshot . . . 506
Cálculo del espacio de la reclamación para las copias snapshot . . . 507
Descripción de las ventanas y cuadros de diálogo del objeto del clúster . . . 508
Flujos de trabajo y tareas comunes del estado de Unified Manager . . . 508
Supervisión y solución de problemas de disponibilidad de datos . . . 510
Resolver problemas de capacidad . . . 517
Gestión de umbrales de salud . . . 518
Gestión de los objetivos de seguridad del clúster . . . 524
Gestión de operaciones de backup y restauración . . . 536
Administrar scripts . . . 553
Gestión y supervisión de grupos . . . 556
Priorizando eventos de objetos de almacenamiento mediante anotaciones . . . 565
Enviar un paquete de soporte a través de la interfaz de usuario web y la consola de mantenimiento . . . 574
Tareas e información relacionada con varios flujos de trabajo . . . 581
Proteja y restaure sus datos . . . 641
Creación, supervisión y solución de problemas de relaciones de protección . . . 641

Tipos de protección SnapMirror . . . 641
Configuración de las relaciones de protección en Unified Manager . . . 643
Recuperación tras fallos y recuperación de una relación de protección . . . 645
Solucionar un error de un trabajo de protección . . . 649
Resolución de problemas de desfase . . . 653
Gestión y supervisión de relaciones de protección . . . 654
Ver el estado de protección de volumen . . . 654
Visualización de las relaciones de protección de volúmenes . . . 657
Supervisar las LUN en una relación de grupo de consistencia . . . 657
Crear una relación de protección SnapVault desde la vista Estado: Todos los volúmenes . . . 658
Crear una relación de protección SnapVault desde la página de detalles Volume/Health . . . 659
Crear una relación de protección de SnapMirror desde la vista Estado: Todos los volúmenes . . . 660
Crear una relación de protección SnapMirror desde la página de detalles Volume/Health . . . 661
Crear una relación de SnapMirror con una replicación de versión flexible . . . 663
Crear relaciones SnapMirror con una replicación de versión flexible con la opción de backup . . . 664
Configurar los ajustes de eficiencia de destino . . . 665
Crear programaciones de SnapMirror y SnapVault . . . 665
Crear relaciones en cascada o con ventilador para ampliar la protección a partir de una relación de protección existente . . . 666
Editar las relaciones de protección en la página Volume Relationships . . . 667
Editar las relaciones de protección desde la página de detalles volumen / Estado . . . 667
Creación de una política de SnapMirror para maximizar la eficiencia de transferencia . . . 668
Creación de una política de SnapVault para maximizar la eficiencia de transferencia . . . 669
Cancelar una transferencia de protección de datos activa desde la página Relaciones de volumen . . . 669
Cancelación de una transferencia de protección de datos activa desde la página de detalles volumen / Salud . . . 670
Desactivación de una relación de protección en la página Relaciones de volumen . . . 671
Desactivación de una relación de protección desde la página de detalles volumen / Salud . . . 672
Interrumpir una relación de SnapMirror en la página Volume Relationships . . . 672
Quitar una relación de protección en la página Volume Relationships . . . 673
Reanude las transferencias programadas en una relación de modo inactivo en la página Relaciones de volumen . . . 673
Reanude las transferencias programadas en una relación en modo inactivo en la página de detalles Volume/Health . . . 674
Inicializando o actualizando relaciones de protección en la página Volume Relationships . . . 675
Inicializar o actualizar las relaciones de protección en la página de detalles Volume / Health . . . 676
Resincronizando las relaciones de protección desde la página Volume Relationships . . . 677
Inversión de las relaciones de protección en la página Volume Relationships . . . 678
Restaurar datos mediante las páginas de detalles Volume y Volume/Health . . . 679
Qué pools de recursos son . . . 680
Creación de pools de recursos . . . 680
Editar pools de recursos . . . 681
Ver el inventario de pools de recursos . . . 681
Agregar miembros del pool de recursos . . . 681
Eliminación de agregados de pools de recursos . . . 682

Eliminación de pools de recursos . . . 683
Supervisar las relaciones de protección de recuperación ante desastres de las máquinas virtuales de almacenamiento . . . 683
Asociaciones de máquinas virtuales de almacenamiento . . . 685
Requisitos de SVM y pool de recursos para dar soporte a servicios de almacenamiento . . . 688
Qué trabajos son . . . 688
Supervisar trabajos de . . . 689
Ver los detalles del trabajo . . . 689
Anulación de trabajos . . . 689
Volver a intentar un trabajo de protección con errores . . . 690
Descripción de las ventanas y cuadros de diálogo de relaciones de protección . . . 690
Generar informes personalizados . . . 734
Informes de Unified Manager . . . 734
Puntos de acceso para generar informes . . . 734
Informes . . . 736
Comprensión de la relación de vista e informe . . . 737
Tipos de informes . . . 737
Limitaciones en la generación de informes . . . 739
Trabajar con informes . . . 739
Flujo de trabajo de informes . . . 739
Inicio rápido de informes . . . 740
Buscando un informe programado . . . 743
Personalización de informes . . . 743
Descargando informes . . . 747
Programación de informes . . . 747
Programar un informe . . . 748
Gestión de programas de informes . . . 750
Informes personalizados de muestra . . . 752
Personalizar informes de almacenamiento de clúster . . . 753
Personalizar los informes de capacidad de agregados . . . 756
Personalización de los informes de capacidad de volúmenes . . . 758
Personalizar los informes de capacidad de Qtree . . . 761
Personalización de informes de recursos compartidos de NFS . . . 762
Personalizar los informes de VM de almacenamiento . . . 764
Personalización de los informes de relaciones de volumen . . . 765
Personalización de los informes de rendimiento de volúmenes . . . 769
Informes de ejemplo de Microsoft Excel . . . 770
Creación de un informe para mostrar un gráfico y una tabla de capacidad agregada . . . 770
Creación de un informe para mostrar los gráficos de capacidad total agregado frente a los disponibles 773
Creación de un informe para ver los gráficos de capacidad de los volúmenes disponibles . . . 777
Crear un informe para ver los agregados con la tasa de IOPS más disponible . . . 779
Gestión del almacenamiento usando API de REST . . . 782
Primeros pasos con API de REST de Active IQ Unified Manager . . . 782
Destinatarios para este contenido . . . 782
Categorías y acceso API de Active IQ Unified Manager . . . 782

Servicios DE REST ofrecidos en Active IQ Unified Manager . . . 784
Versión de API en Active IQ Unified Manager . . . 785
Recursos de almacenamiento en ONTAP . . . 785
Acceso y autenticación de API DE REST en Active IQ Unified Manager . . . 786
Autenticación . . . 788
códigos de estado HTTP utilizados en Active IQ Unified Manager . . . 789
Recomendaciones para el uso de las API para Active IQ Unified Manager . . . 790
Registros para solución de problemas . . . 790
Procesos asincrónicos de objetos de trabajo . . . 791
Hola servidor API . . . 792
API de REST de Unified Manager . . . 796
Gestionar objetos de almacenamiento en un centro de datos mediante API . . . 797
Acceso a API de ONTAP a través de acceso de proxy . . . 804
Realización de tareas administrativas mediante API . . . 807
Gestionar usuarios mediante API . . . 808
Ver las métricas de rendimiento mediante API . . . 809
Ver trabajos y detalles del sistema . . . 820
Gestionar eventos y alertas mediante API . . . 821
Gestionar cargas de trabajo mediante API . . . 824
Flujos de trabajo API comunes para la gestión del almacenamiento . . . 833
Llamadas API que se usan en los flujos de trabajo . . . 833
Determinar problemas de espacio en agregados mediante las API . . . 834
Determinar problemas en objetos de almacenamiento mediante las API de eventos . . . 836
Solución de problemas de volúmenes de ONTAP mediante API de puerta de enlace . . . 837
Flujos de trabajo API para la gestión de cargas de trabajo . . . 841
Avisos legales . . . 868
Derechos de autor . . . 868
Marcas comerciales . . . 868
Estadounidenses . . . 868
Política de privacidad . . . 868
Código abierto . . . 868

Documentación de Active IQ Unified Manager

Notas de la versión

Proporciona un resumen de las nuevas funciones, las limitaciones y los problemas conocidos de Active IQ Unified Manager 9.12.

Para obtener más información, consulte "Notas de la versión de Active IQ Unified Manager".

Manos a la obra

Instrucciones de inicio rápido para instalaciones de VMware

Puede descargar la `.tar` archivo que contiene un certificado raíz, un `README` archivo, y una `OVA` Archivar y poner en marcha Unified Manager como dispositivo virtual.

Requisitos del sistema

- Sistema operativo: VMware ESXi 6.5, 6.7 y 7.0.x
- RAM: 12 GB
- CPU: 9572 MHz en total
- Espacio libre en disco: 5 GB (thin provisioning), 152 GB (thick provisioning)

Para ver los requisitos detallados del sistema, consulte "Requisitos para instalar Unified Manager" y.. "Matriz de interoperabilidad".

Instalando Active IQ Unified Manager

Descargue el instalador

1. Descargue el `.tar` archivo que contiene un certificado raíz, un `README` archivo, y una `OVA` archivo.
2. Guarde el archivo en un directorio local o en un directorio de red al que pueda acceder vSphere Client.
3. En el directorio en el que ha descargado el `.tar` archivo, introduzca la `tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz` comando. + el requerido `OVA` archivo, un certificado raíz y un `README` el archivo se descomprime en el directorio de destino.

Verifique la integridad

Puede verificar la integridad de `OVA` siga los pasos proporcionados en `README` archivo.

Instale Unified Manager

1. En vSphere Client, haga clic en **Archivo > implementar plantilla OVF**.
2. Busque el archivo OVA y utilice el asistente para implementar el dispositivo virtual en el servidor ESXi.
3. En la página revisar detalles, en la sección Publisher, aparece el mensaje `Entrust Code Signing - OVCS2 (Trusted certificate)` confirma la integridad de la descarga `OVA` archivo. Para el mensaje `Entrust Code Signing - OVCS2 (Invalid certificate)`, Actualice VMware vCenter Server a 7.0U3E o una versión posterior.
4. En la página Personalizar plantilla, en la ficha Propiedades, rellene los campos según sea necesario para el tipo de instalación que esté realizando:
   - Para la configuración estática, introduzca la información requerida en todos los campos. No es necesario agregar información para el campo **DNS secundario**.
   - Para DHCP que utilice IPv4, no añada ninguna información en ningún campo.

    - Para DHCP con IPv6, marque la casilla “Habilitar direccionamiento IPv6 automático”. No añada ninguna información en ningún otro campo.
5. Encienda la máquina virtual.
6. Haga clic en la ficha Consola para ver el proceso de inicio inicial.
7. Configure la zona horaria.
8. Introduzca un nombre de usuario y una contraseña de mantenimiento de Unified Manager.

Al finalizar la instalación, se muestra la información para conectarse a la interfaz de usuario web de Unified Manager.

Instrucciones de inicio rápido para instalaciones Linux

Puede descargar el paquete de instalación e instalar Unified Manager en una plataforma física o virtual Red Hat Enterprise Linux o CentOS.

Requisitos del sistema

- Sistema operativo: Red Hat Enterprise Linux versiones 7.x y de 8,0 a 8,6, o CentOS versión 7.x basada en la arquitectura x86_64, instalado utilizando el entorno base “Servidor con GUI” de la opción **Selección de software** del instalador del sistema operativo
- RAM: 12 GB, CPU: 9572 MHz en total
- Espacio libre en disco: 100 GB de espacio en disco `/opt/netapp/data` directorio, 50 GB en la partición raíz. Para montaje independiente `/opt` y.. `/var/log` directorios, asegúrese de que `/opt` Tiene 15 GB, `/var/log` Tiene 16 GB, y. `/tmp` Tiene 10 GB de espacio libre.

Para obtener información detallada sobre los requisitos del sistema y sobre cómo instalar el producto en un sitio protegido, consulte "Requisitos para instalar Unified Manager" y la "Matriz de interoperabilidad".

Instalando Active IQ Unified Manager

Descargue el instalador

1. Descargue el `ActiveIQUnifiedManager-<version>.zip` paquete de instalación junto con certificado de firma de código (`.pem`) y firma digital (`.sig`) .
2. En el directorio en el que ha descargado el archivo de instalación, ejecute:

```
# unzip ActiveIQUnifiedManager-<version>.zip
```

Verifique la integridad

Ejecute los siguientes comandos para verificar la integridad del paquete del instalador:

- Ejecución `openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem > <public_key_file_name>` para crear un archivo con la clave pública desde el certificado de firma de código.
- Ejecución `openssl dgst -sha256 -verify <public_key_file_name> -signature <signature_file_name> ActiveIQUnifiedManager-<version>.zip` para verificar la firma en el paquete del instalador.

Verificar la configuración de repositorio

Los procedimientos para configurar repositorios de Red Hat Enterprise Linux o CentOS son específicos del sitio. Puede utilizar el `pre_install_check.sh` script incluido en el paquete de instalación para verificar la configuración del sistema operativo. Si el sistema está conectado a Internet, recibirá automáticamente instrucciones para configurar los repositorios de Red Hat Enterprise Linux o CentOS.

```
# sudo ./pre_install_check.sh
```

Instale Unified Manager

Unified Manager utiliza `yum` utilidad para instalar el software y cualquier software dependiente. Debido a que hay varias imágenes de Red Hat Enterprise Linux o CentOS, los paquetes instalados dependen del software presente en las imágenes. La `yum` utilidad determina los paquetes de software dependientes para la instalación. Si necesita más información sobre los paquetes de software dependientes, consulte "Requisitos de instalación y software Linux".

Para instalar Unified Manager, ejecute el siguiente comando, ya sea como usuario raíz o mediante `sudo`, desde el directorio en el que se descomprimió el archivo de instalación:

```
# yum install netapp-um<version>.x86_64.rpm
```

o.

```
% sudo yum install netapp-um<version>.x86_64.rpm
```

Al finalizar la instalación, se muestra la información para conectarse a la interfaz de usuario web de Unified Manager. Si no puede conectarse a la interfaz de usuario web, consulte `README` archivo empaquetado con el software para obtener más información acerca de las restricciones del puerto 443.

Instrucciones de inicio rápido para instalaciones de Windows

Puede descargar el paquete de instalación e instalar Unified Manager para supervisar y solucionar problemas de capacidad de almacenamiento de datos, disponibilidad, rendimiento y protección.

Requisitos del sistema

- Sistemas operativos
  - Microsoft Windows Server 2019 Standard y Datacenter Edition
  - Microsoft Windows Server 2022 Standard y Datacenter Edition

    Unified Manager es compatible con el sistema operativo Windows de 64 bits para los siguientes idiomas:

  - Inglés
  - Japonés
  - Chino simplificado
- RAM: 12 GB

- CPU: 9572 MHz en total
- Espacio libre en disco: 100 GB de espacio en disco para el directorio de instalación, 50 GB de espacio en disco para el directorio de datos de MySQL

Para ver los requisitos detallados del sistema, consulte "Requisitos para instalar Unified Manager" y.. "Matriz de interoperabilidad".

Instalando Active IQ Unified Manager

Descargue el instalador

1. Descargue el `ActiveIQUnifiedManager-<version>.exe` paquete de instalación.
2. Copie el archivo de instalación en un directorio del sistema de destino.

Instale Unified Manager

Para instalar Unified Manager, asegúrese de tener instalado Microsoft .NET 4.5.2 o una versión posterior. Como parte del proceso de instalación, Unified Manager instala otros paquetes de terceros según sea necesario. Para obtener más información acerca de los paquetes de software dependientes, consulte "Requisitos de instalación y software de Windows".

1. Inicie sesión en Windows con la cuenta de administrador local predeterminada.
2. En el directorio en el que ha descargado el archivo de instalación, haga clic con el botón derecho del ratón y ejecute el archivo ejecutable (.exe) de Unified Manager como administrador.
3. Cuando se le solicite, introduzca el nombre de usuario y la contraseña para crear el usuario de mantenimiento de Unified Manager.
4. En el asistente Database Connection, introduzca la contraseña raíz de MySQL.
5. Siga el resto de las indicaciones para completar la instalación.
6. Haga clic en **Finalizar** al final de la instalación y aparecerá la interfaz de usuario web de Unified Manager.

Instale Unified Manager en sistemas VMware vSphere

Introducción a Active IQ Unified Manager

Active IQ Unified Manager (anteriormente Unified Manager de OnCommand) le permite supervisar y gestionar el estado y el rendimiento de sus sistemas de almacenamiento de ONTAP desde una única interfaz. Puede implementar Unified Manager en un servidor Linux, en un servidor de Windows o como dispositivo virtual en un host VMware.

Después de completar la instalación y añadir los clústeres que desea gestionar, Unified Manager proporciona una interfaz gráfica que muestra el estado de la capacidad, la disponibilidad, la protección y el rendimiento de los sistemas de almacenamiento supervisados.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Lo que hace Unified Manager Server

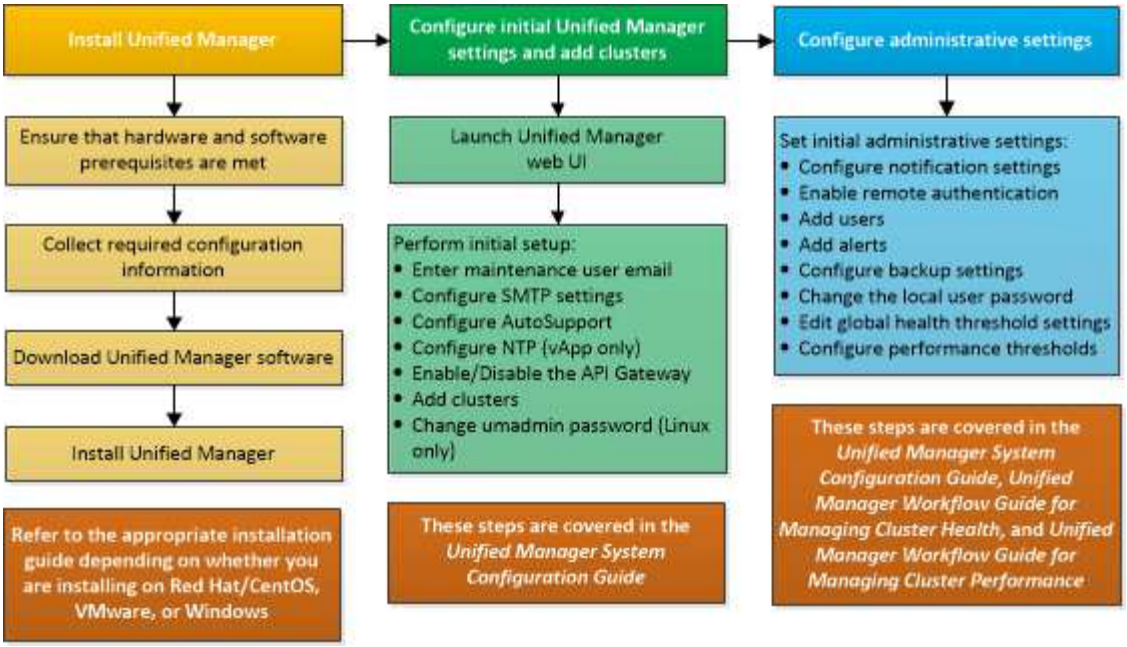
La infraestructura de servidor de Unified Manager consta de una unidad de recogida de datos, una base de datos y un servidor de aplicaciones. Proporciona servicios de infraestructura como detección, supervisión, control de acceso basado en roles (RBAC), auditoría y registro.

Unified Manager recopila información del clúster, almacena los datos en la base de datos y analiza los datos para ver si hay algún problema con el clúster.

Descripción general de la secuencia de instalación

El flujo de trabajo de instalación describe las tareas que deben realizarse para poder usar Unified Manager.

Estas secciones describen cada uno de los elementos mostrados en el flujo de trabajo siguiente.



Requisitos para instalar Unified Manager

Antes de iniciar el proceso de instalación, asegúrese de que el servidor en el que desea instalar Unified Manager cumpla con los requisitos específicos de software, hardware, CPU y memoria.

NetApp no admite ninguna modificación del código de aplicación de Unified Manager. Si necesita aplicar cualquier medida de seguridad al servidor de Unified Manager, debe realizar estos cambios en el sistema operativo en el que está instalado Unified Manager.

Para obtener más información sobre la aplicación de medidas de seguridad en Unified Manager Server, consulte el artículo de la base de conocimientos.

"Compatibilidad con las medidas de seguridad aplicadas a Active IQ Unified Manager para Clustered Data ONTAP"

Información relacionada

Para obtener más información, consulte "Herramienta de matriz de interoperabilidad de NetApp"

Requisitos del sistema de hardware e infraestructura virtual

La instalación de Unified Manager en una infraestructura virtual o un sistema físico debe cumplir con los requisitos mínimos de memoria, CPU y espacio en disco.

La siguiente tabla muestra los valores recomendados para los recursos de memoria, CPU y espacio en disco. Se han cualificado estos valores para que Unified Manager cumpla niveles de rendimiento aceptables.

Configuración de hardware	Configuración recomendada
RAM	12 GB (requisito mínimo de 8 GB)

Configuración de hardware	Configuración recomendada
Procesadores	4 CPU
Capacidad del ciclo de la CPU	9572 MHz en total (requisito mínimo de 9572 MHz)
Libere espacio en disco	• 5 GB (con Thin Provisioning) • 152 GB (Thick-Provisioning)

Unified Manager se puede instalar en sistemas con una pequeña cantidad de memoria, pero los 12 GB de RAM recomendados garantizan que haya suficiente memoria disponible para un rendimiento óptimo, por lo que el sistema puede acomodar clústeres y objetos de almacenamiento adicionales a medida que crezca su configuración. No debe establecer ningún límite de memoria en la máquina virtual donde se haya puesto en marcha Unified Manager y no debe habilitar ninguna función (por ejemplo, una configuración en globo) que impida que el software utilice la memoria asignada en el sistema.

Asimismo, existe un límite en cuanto al número de nodos que puede supervisar una única instancia de Unified Manager antes de instalar una segunda instancia de Unified Manager. Para obtener más información, consulte "Guía de prácticas recomendadas de Unified Manager".

El intercambio de la memoria por página afecta negativamente al rendimiento del sistema y de la aplicación de gestión. Competir por recursos CPU que no están disponibles debido al uso general del host puede degradar el rendimiento.

Requisito para un uso dedicado

El sistema físico o virtual en el que se instala Unified Manager se debe utilizar exclusivamente para Unified Manager y no se debe compartir con otras aplicaciones. Otras aplicaciones pueden consumir recursos del sistema y reducir drásticamente el rendimiento de Unified Manager.

Requisitos de espacio para backups

Si tiene previsto utilizar la función de backup y restauración de Unified Manager, asigne capacidad adicional para que el directorio o disco «data» tenga 150 GB de espacio. Una copia de seguridad se puede escribir en un destino local o en un destino remoto. La práctica recomendada es identificar una ubicación remota externa al sistema host de Unified Manager que tiene un mínimo de 150 GB de espacio.

Requisitos para la conectividad de host

El sistema físico o el sistema virtual en el que instala Unified Manager debe configurarse de modo que pueda hacerlo correctamente `ping` el nombre de host del propio host. En caso de configuración IPv6, debe verificar que sí `ping6` El nombre de host se realiza correctamente para garantizar que la instalación de Unified Manager se realice correctamente.

Es posible usar el nombre de host (o la dirección IP del host) para acceder a la interfaz de usuario web del producto. Si configuró una dirección IP estática para la red durante la implementación, debe designar un nombre para el host de red. Si configuró la red mediante DHCP, debe obtener el nombre de host del DNS.

Si planea permitir a los usuarios acceder a Unified Manager mediante el nombre corto en lugar de usar el nombre de dominio completo (FQDN) o la dirección IP, la configuración de red debe resolver este nombre corto con un FQDN válido.

Requisitos de instalación y software de VMware

El sistema VMware vSphere en el que se instala Unified Manager requiere versiones específicas del sistema operativo y el software compatible.

Software del sistema operativo

Se admiten las siguientes versiones de VMware ESXi:

- ESXi 6.5, 6.7 y 7.0.x.

> El OVA de Unified Manager en sistemas VMware vSphere ejecuta Debian OS 11 (bullseye) internamente. Para obtener información sobre las versiones del hardware de la máquina virtual que pueden admitir las versiones compatibles de los servidores ESXi, consulte la documentación de VMware.

Se admiten las siguientes versiones de vSphere:

- VMware vCenter Server 6.5, 6.7 y 7.0.x.

Consulte la matriz de interoperabilidad para ver la lista completa y más actual de versiones ESXi compatibles.

"mysupport.netapp.com/matrix"

La hora del servidor VMware ESXi debe ser la misma que la del servidor NTP para que el dispositivo virtual funcione correctamente. La sincronización de la hora del servidor VMware ESXi con la hora del servidor NTP evita un fallo del tiempo.

Requisitos de instalación

Se admite la alta disponibilidad de VMware para el dispositivo virtual de Unified Manager.

Si se implementa un almacén de datos NFS en un sistema de almacenamiento que ejecuta el software ONTAP, se debe utilizar el plugin de NFS de NetApp para VMware VAAI para utilizar aprovisionamiento grueso.

Si se produce un error en la implementación con su entorno habilitado para alta disponibilidad debido a recursos insuficientes, es posible que deba modificar las Opciones de máquina virtual de las características de clúster desactivando la prioridad de reinicio de la máquina virtual y dejando encendida la respuesta de aislamiento del host.

> Durante la instalación o actualización de Unified Manager, las revisiones de seguridad y software de terceros necesarias se instalan o actualizan automáticamente en un sistema VMware vSphere. Dado que los procesos de instalación y actualización de Unified Manager controlan estos componentes, no debe intentar una instalación o actualización independientes de ningún componente de terceros.

Exploradores compatibles

Para acceder a la interfaz de usuario web de Unified Manager, utilice un explorador compatible.

La matriz de interoperabilidad tiene la lista de versiones de exploradores compatibles.

"mysupport.netapp.com/matrix"

En todos los navegadores, la desactivación de los bloqueadores de ventanas emergentes garantiza que las funciones de software se muestren correctamente.

Si planea configurar Unified Manager para la autenticación SAML y que un proveedor de identidades (IDP) pueda autenticar usuarios, debe comprobar también la lista de exploradores compatibles con IDP.

Requisitos de protocolo y puerto

Los puertos y protocolos necesarios permiten la comunicación entre el servidor de Unified Manager y los sistemas de almacenamiento gestionados, los servidores y otros componentes.

Conexiones con el servidor de Unified Manager

En instalaciones típicas no es necesario especificar números de puerto al conectarse a la interfaz de usuario web de Unified Manager, ya que siempre se utilizan los puertos predeterminados. Por ejemplo, como Unified Manager siempre intenta ejecutar en su puerto predeterminado, puede introducir `https://<host>` en lugar de `https://<host>:443`.

El servidor de Unified Manager utiliza protocolos específicos para acceder a las siguientes interfaces:

Interfaz	Protocolo	Puerto	Descripción
Interfaz de usuario web de Unified Manager	HTTP	80	Se utiliza para acceder a la IU web de Unified Manager; redirige automáticamente al puerto seguro 443.
API de interfaz de usuario web y programas de Unified Manager	HTTPS	443	Se usa para acceder de manera segura a la interfaz de usuario web de Unified Manager o para realizar llamadas API, ya que las llamadas API solo se pueden realizar mediante HTTPS.
Consola de mantenimiento	SSH/SFTP	22	Se usa para acceder a la consola de mantenimiento y recuperar los paquetes de soporte.
Línea de comandos de Linux	SSH/SFTP	22	Se utiliza para acceder a la línea de comandos Red Hat Enterprise Linux o CentOS y recuperar paquetes de soporte.

Interfaz	Protocolo	Puerto	Descripción
Syslog	UDP	514	Se utiliza para acceder a los mensajes de EMS basados en suscripción desde sistemas ONTAP y para crear eventos basados en los mensajes.
DESCANSO	HTTPS	9443	Se utiliza para acceder a eventos EMS basados en API DE REST en tiempo real desde sistemas ONTAP autenticados.

El puerto predeterminado de MySQL, 3306, está restringido solo a localhost mientras se instala Unified Manager en sistemas VMware vSphere. Esto no afecta a ningún escenario de actualización donde se mantenga la configuración anterior. Esta configuración puede modificarse y la conexión puede ponerse a disposición de otros hosts mediante el `Control access to MySQL port 3306` de la consola de mantenimiento. Para obtener más información, consulte "Opciones de menú adicionales". Los puertos que se utilizan para la comunicación HTTP y HTTPS (puertos 80 y 443) pueden cambiarse con la consola de mantenimiento de Unified Manager. Para obtener más información, consulte "Menús de la consola de mantenimiento".

Conexiones desde el servidor de Unified Manager

Debe configurar el firewall para que abra puertos que permitan la comunicación entre el servidor de Unified Manager y los sistemas de almacenamiento gestionados, los servidores y otros componentes. Si un puerto no está abierto, la comunicación falla.

Según su entorno, puede elegir modificar los puertos y los protocolos que utiliza el servidor de Unified Manager para conectarse a destinos específicos.

El servidor de Unified Manager se conecta utilizando los siguientes protocolos y puertos a los sistemas de almacenamiento gestionados, los servidores y otros componentes:

Destino	Protocolo	Puerto	Descripción
Sistema de almacenamiento	HTTPS	443 TCP	Se utiliza para supervisar y gestionar sistemas de almacenamiento. Si utiliza este puerto o cualquier otro puerto para conectarse a los servidores VMware vCenter Server o ESXi, asegúrese de que el puerto esté disponible y que pueda estar conectado en un sitio seguro.
Sistema de almacenamiento	NDMP	10000 TCP	Se utiliza para ciertas operaciones de restauración de Snapshot.
Servidor AutoSupport	HTTPS	443	Se utiliza para enviar información de AutoSupport. Requiere el acceso a Internet para realizar esta función.
Servidor de autenticación	LDAP	389	Se utiliza para realizar solicitudes de autenticación y solicitudes de búsqueda de usuarios y grupos.
LDAPS	636	Se utiliza para comunicación LDAP segura.	Servidor de correo

Destino	Protocolo	Puerto	Descripción
SMTP	25	Se utiliza para enviar correos electrónicos de notificación de alertas.	Remitente de captura SNMP
SNMPv1 o SNMPv3	162/UDP	Se utiliza para enviar notificaciones de alerta de capturas de SNMP.	Servidor de proveedores de datos externos
TCP	2003	Se utiliza para enviar datos de rendimiento a un proveedor de datos externo, como Graphite.	Servidor NTP

Rellenar la hoja de cálculo

Antes de instalar y configurar Unified Manager, debe tener disponible información específica acerca de su entorno. Puede registrar la información en la hoja de cálculo.

Información de instalación de Unified Manager

Los detalles necesarios para instalar Unified Manager.

Sistema en el que se ha puesto en marcha el software	Su valor
Dirección IP del servidor ESXi	
Nombre de dominio completo del host	
Dirección IP del host	
Máscara de red	
Dirección IP de la pasarela	
Dirección DNS principal	
Dirección DNS secundaria	
Buscar dominios	
Nombre de usuario de mantenimiento	
Contraseña de usuario de mantenimiento	

Información de configuración de Unified Manager

Los detalles para configurar Unified Manager después de la instalación. Algunos valores son opcionales según la configuración.

Ajuste	Su valor
Dirección de correo electrónico del usuario de mantenimiento	
Servidor NTP	
Nombre de host o dirección IP del servidor SMTP	
Nombre de usuario SMTP	
Contraseña SMTP	
Puerto SMTP	25 (valor predeterminado)
Correo electrónico desde el cual se envían notificaciones de alerta	
Nombre de host o dirección IP del servidor de autenticación	
El nombre de administrador de Active Directory o el nombre distintivo de enlace LDAP	
Contraseña de Active Directory o contraseña de enlace LDAP	
Nombre distintivo de la base del servidor de autenticación	
URL del proveedor de identidades (IDP)	
Metadatos del proveedor de identidades (IDP)	
Direcciones IP del host de destino de capturas SNMP	
Puerto SNMP	

Información del clúster

Los detalles sobre los sistemas de almacenamiento que gestiona mediante Unified Manager.

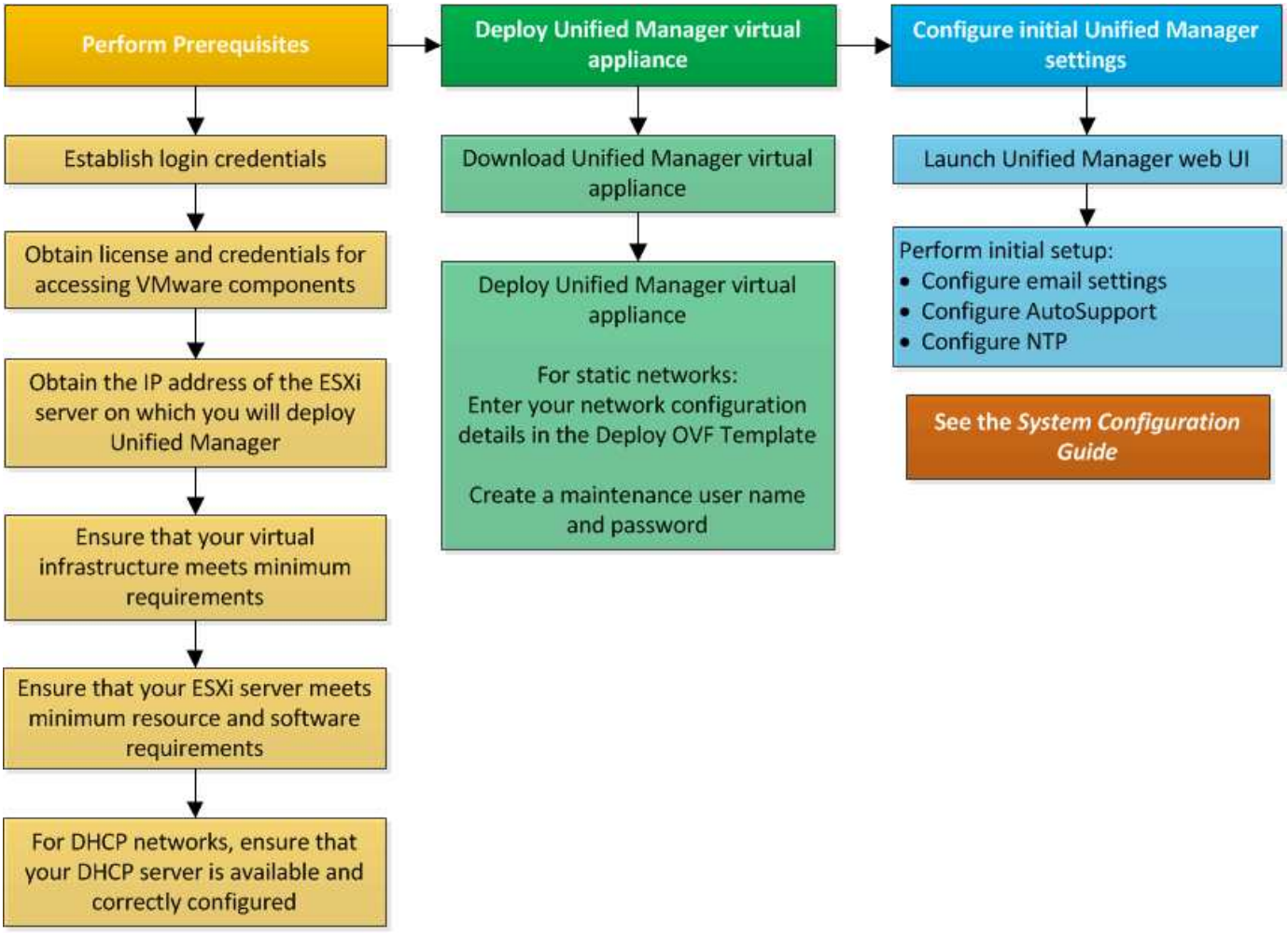
Clúster 1 de N	Su valor
El nombre de host o la dirección IP de administración del clúster	
Nombre de usuario del administrador ONTAP Al administrador se le debe haber asignado la función «admin».	
Contraseña del administrador de ONTAP	
Protocolo	HTTPS

Instalación, actualización y eliminación del software Unified Manager

En sistemas VMware vSphere, puede instalar Unified Manager, actualizar a una versión más reciente del software o quitar el dispositivo virtual de Unified Manager (vApp).

Información general del proceso de implementación

En el flujo de trabajo de implementación, se describen las tareas que deben realizarse para poder usar Unified Manager.



Ponga en marcha Unified Manager

La puesta en marcha de Unified Manager incluye la descarga de software, la puesta en marcha de dispositivos virtuales, la creación de un nombre de usuario y una contraseña de mantenimiento, y la realización de la configuración inicial en la interfaz de usuario web.

Lo que necesitará

- Debe verificar y completar los requisitos del sistema para la puesta en marcha.

  Consulte "Requisitos del sistema".

- Asegúrese de disponer de la siguiente información:
  - Credenciales de inicio de sesión para el sitio de soporte de NetApp
  - Credenciales para acceder a VMware vCenter Server y vSphere Web Client
  - Dirección IP del servidor ESXi en el que va a implementar el dispositivo virtual de Unified Manager
  - Detalles sobre el centro de datos, como el espacio de almacenamiento en el almacén de datos y los requisitos de memoria
  - Se debe habilitar IPv6 en el host si tiene pensado usar direcciones IPv6.

Puede poner en marcha Unified Manager como dispositivo virtual en un servidor VMware ESXi.

Debería acceder a la consola de mantenimiento mediante la consola de VMware, y no mediante SSH.

> A partir de Unified Manager 9.8, VMware Tools se ha sustituido por Open VM Tools `open-vm-tools`). Ya no es necesario instalar VMware Tools como parte de la instalación debido a esto `open-vm-tools` Se incluye en el paquete de instalación de Unified Manager.

Una vez finalizada la puesta en marcha y la configuración inicial, puede añadir clústeres o configurar ajustes de red adicionales en la consola de mantenimiento y, a continuación, acceder a la interfaz de usuario web.

Pasos

1. Siga los pasos de "Descargue Unified Manager".
2. Además, siga los pasos de "Ponga en marcha el dispositivo virtual Unified Manager".

Descargue el archivo de instalación de Unified Manager

Descargue el archivo de instalación de Unified Manager desde el sitio de soporte de NetApp para poner en marcha Unified Manager como dispositivo virtual.

Lo que necesitará

Debe tener las credenciales de inicio de sesión en el sitio de soporte de NetApp.

El archivo de instalación es un `.tar` archivo que contiene un certificado raíz, un `README` archivo, y una `OVA` Archivo que contiene el software Unified Manager configurado para un dispositivo virtual.

Pasos

1. Inicie sesión en el sitio de soporte de NetApp y desplácese hasta la página de descarga de Unified Manager:

   "Sitio de soporte de NetApp"

2. Seleccione la versión requerida de Unified Manager y acepte el contrato de licencia para usuarios finales (CLUF).
3. Descargue y guarde el `.tar` Instalación de archivo para VMware vSphere en un directorio local o directorio de red al que se puede acceder su cliente vSphere.
4. Compruebe la suma de comprobación para asegurarse de que el software se ha descargado correctamente.
5. Desplácese hasta el directorio en el que ha descargado el `.tar` File e introduzca el siguiente comando en la ventana de terminal para ampliar el paquete de Unified Manager:

   ```
   tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz
   ```

   El requerido `OVA` archivo, un certificado raíz y un `README` El archivo para Unified Manager se descomprime en el directorio de destino.

6. Compruebe la integridad del `OVA` siga los pasos proporcionados en `README` archivo.

Puesta en marcha del dispositivo virtual Unified Manager

Después de descargar el archivo de instalación, debe poner en marcha Unified Manager como dispositivo virtual. Utilice vSphere Web Client para implementar el dispositivo virtual en un servidor ESXi. Al implementar el dispositivo virtual, se crea una máquina virtual.

Lo que necesitará

Debe revisar los requisitos del sistema. Realice los cambios necesarios antes de implementar el dispositivo virtual de Unified Manager.

Consulte "Requisitos de infraestructura virtual".

Consulte "Requisitos de instalación y software de VMware".

Si utiliza el protocolo de configuración dinámica de hosts (DHCP), asegúrese de que el servidor DHCP esté disponible y que las configuraciones de adaptador de red de DHCP y máquina virtual (VM) sean correctas. De forma predeterminada, DHCP está configurado.

Si utiliza una configuración de red estática, asegúrese de que la dirección IP no esté duplicada en la misma subred y de que se hayan configurado las entradas del servidor DNS adecuadas.

Obtenga la siguiente información antes de implementar el dispositivo virtual:

- Credenciales para acceder a VMware vCenter Server y vSphere Web Client
- Dirección IP del servidor ESXi en el que va a implementar el dispositivo virtual de Unified Manager
- Detalles sobre el centro de datos, como la disponibilidad de espacio de almacenamiento
- Si no utiliza DHCP, obtenga las direcciones IPv4 o IPv6 de los dispositivos de red a los que planea conectarse:
  - Nombre de dominio completo (FQDN) del host
  - Dirección IP del host
  - Máscara de red
  - Dirección IP de la puerta de enlace predeterminada
  - Direcciones DNS principales y secundarias
  - Buscar dominios

A partir de Unified Manager 9.8, VMware Tools se ha sustituido por Open VM Tools (`open-vm-tools`). No es necesario instalar VMware Tools como parte del proceso de instalación debido a esto `open-vm-tools` Se incluye en el paquete de instalación de Unified Manager.

Cuando se implementa el dispositivo virtual, se genera un certificado autofirmado único para el acceso HTTPS. Al acceder a la interfaz de usuario web de Unified Manager, es posible que aparezca una advertencia del explorador sobre certificados que no son de confianza.

Se admite la alta disponibilidad de VMware para el dispositivo virtual de Unified Manager.

Pasos

1. En vSphere Client, haga clic en **Archivo** > **implementar plantilla OVF**.

2. Complete el asistente Deploy OVF Template para implementar el dispositivo virtual de Unified Manager.

   En la página revisar detalles:

   - Compruebe los detalles de la sección Publisher. El mensaje **firma de código de confianza - OVCS2 (certificado de confianza)** confirma la integridad de la descarga `OVA` archivo. + Si aparece el mensaje **firma de código de Entrust - OVCS2 (certificado no válido)**, actualice VMware vCenter Server a la versión 7.0U3E o superior.

     En la página Personalizar plantilla:

   - Deje todos los campos en blanco cuando utilice direcciones DHCP y IPv4.
   - Active la casilla "'Habilitar direccionamiento IPv6 automático'" y deje todos los demás campos en blanco al utilizar direcciones DHCP e IPv6.
   - Si desea utilizar una configuración de red estática, puede completar los campos de esta página y estas opciones se aplican durante la implementación. Asegúrese de que la dirección IP sea única para el host en el que está implementada, que no está en uso y que tiene una entrada DNS válida.

3. Después de implementar el dispositivo virtual Unified Manager en el servidor ESXi, encienda el equipo virtual haciendo clic con el botón derecho del ratón en el equipo virtual y, a continuación, seleccionando **encendido**.

   Si la operación de encendido falla debido a recursos insuficientes, agregue recursos y vuelva a intentar la instalación.

4. Haga clic en la ficha **Consola**.

   El proceso de arranque inicial tarda unos minutos en completarse.

5. Para configurar su zona horaria, introduzca su área geográfica y su ciudad o región como se le solicite en la ventana de la consola de VM.

   Toda la información de fechas que se muestra utiliza la zona horaria configurada para Unified Manager, independientemente de la configuración de zona horaria en los dispositivos gestionados. Si los sistemas de almacenamiento y el servidor de gestión están configurados con el mismo servidor NTP, hacen referencia al mismo instante en el tiempo, incluso si aparecen de manera diferente. Por ejemplo, si crea una copia de Snapshot con un dispositivo que está configurado con una zona horaria diferente a la del servidor de gestión, la Marca de hora es la hora del servidor de gestión.

6. Si no hay servicios DHCP disponibles o si se produce un error en los detalles de la configuración de red estática, seleccione una de las siguientes opciones:

Si usa…	Realice lo siguiente…
DHCP	Seleccione **Reintentar DHCP**. Si planea utilizar DHCP, debe asegurarse de que esté configurado correctamente. Si utiliza una red habilitada para DHCP, las entradas del servidor DNS y FQDN se darán al dispositivo virtual automáticamente. Si DHCP no está configurado correctamente con DNS, el nombre de host "'UnifiedManager'" se asigna automáticamente y se asocia con el certificado de seguridad. Si no configuró una red habilitada para DHCP, debe introducir manualmente la información de configuración de redes.
Una configuración de red estática	a. Seleccione **Introduzca los detalles de la configuración de red estática**. El proceso de configuración tarda unos minutos en completarse. b. Confirme los valores introducidos y seleccione **y**.

7. En el símbolo del sistema, introduzca un nombre de usuario de mantenimiento y, a continuación, haga clic en **Intro**.

   El nombre de usuario de mantenimiento debe comenzar con una letra de a-z, seguida de cualquier combinación de -, a-z o 0-9.

8. En el indicador, introduzca una contraseña y, a continuación, haga clic en **Intro**.

   La consola de máquinas virtuales muestra la URL para la interfaz de usuario web de Unified Manager.

Puede acceder a la interfaz de usuario web de para realizar la configuración inicial de Unified Manager, como se describe en "Configurando Active IQ Unified Manager".

Actualizar Unified Manager

Puede actualizar Active IQ Unified Manager a la versión 9.12 únicamente de la versión 9.10 o la 9.11.

Durante el proceso de actualización, Unified Manager no está disponible. Debe completar todas las operaciones en ejecución antes de actualizar Unified Manager.

Si Unified Manager se empareja con una instancia de OnCommand Workflow Automation y hay nuevas versiones del software disponibles para ambos productos, debe desconectar los productos y, a continuación, configurar una nueva conexión de Workflow Automation tras las actualizaciones. Si solo actualiza uno de los productos, deberá iniciar sesión en Workflow Automation tras la actualización y comprobar que aún se recopilen datos de Unified Manager.

Pasos

1. Siga los pasos de "Descargue la imagen ISO de Unified Manager".
2. Además, siga los pasos descritos en "Actualice Unified Manager".

La ruta de actualización compatible con las versiones de Unified Manager

Active IQ Unified Manager admite una ruta de actualización específica para cada versión.

No todas las versiones de Unified Manager pueden realizar una actualización sin movimiento a versiones posteriores. Las actualizaciones de Unified Manager se limitan a un modelo N-2, lo que significa que la actualización solo se puede realizar en las próximas dos versiones de todas las plataformas. Por ejemplo, puede realizar una actualización a Unified Manager 9.12 solo desde Unified Manager 9.10 y 9.11.

Si ejecuta una versión anterior a las versiones compatibles, primero deberá actualizar la instancia de Unified Manager con una de las versiones compatibles y, a continuación, actualizarla a la versión actual.

Por ejemplo, si la versión instalada es OnCommand Unified Manager 9.5 y desea actualizar a la versión más reciente de Active IQ Unified Manager 9.12, siga una secuencia de actualizaciones.

Ruta de actualización de ejemplo:

1. Actualice Unified Manager 9.5 de OnCommand → Active IQ Unified Manager 9.7.
2. Actualización 9.7 → 9.9.
3. Actualización 9.9 → 9.11.
4. Actualización 9.11 → 9.12.

Para obtener más información acerca de la matriz de rutas de actualización, consulte este tema "Artículo de la base de conocimientos (KB)".

Descargando el archivo de actualización de Unified Manager

Antes de actualizar Unified Manager, descargue el archivo de actualización de Unified Manager desde el sitio de soporte de NetApp.

Lo que necesitará

Debe tener credenciales de inicio de sesión en el sitio de soporte de NetApp.

Pasos

1. Inicie sesión en el sitio de soporte de NetApp:

   "Sitio de soporte de NetApp"

2. Vaya a la página de descarga para actualizar Unified Manager en VMware vSphere.
3. Descargue el `.iso` Imagen para la actualización y guárdelo en un directorio local o un directorio de red al que se pueda acceder vSphere Client.
4. Compruebe la suma de comprobación para asegurarse de que el software se ha descargado correctamente.

Actualización del dispositivo virtual de Unified Manager

Puede actualizar el dispositivo virtual Active IQ Unified Manager de las versiones 9.10 o

9.11 a 9.12.

Lo que necesitará

Asegúrese de lo siguiente:

- Ha descargado el archivo de actualización, la imagen ISO del sitio de soporte de NetApp.
- El sistema donde se actualiza Unified Manager cumple con los requisitos del sistema y del software.

  Consulte "Requisitos de infraestructura virtual".

  Consulte "Requisitos de instalación y software de VMware".

- Para vSphere 6.5 y usuarios posteriores, ha instalado VMware Remote Console (VMRC).
- Durante la actualización, es posible que se le solicite confirmar si desea mantener la configuración predeterminada anterior para conservar los datos de rendimiento durante 13 meses o cambiarla a 6 meses. Al confirmar, los datos de rendimiento históricos se purgan al cabo de 6 meses.
- Tiene la siguiente información:
  - Credenciales de inicio de sesión para el sitio de soporte de NetApp
  - Credenciales para acceder a VMware vCenter Server y vSphere Web Client
  - Credenciales para el usuario de mantenimiento de Unified Manager

Durante el proceso de actualización, Unified Manager no está disponible. Debe completar todas las operaciones en ejecución antes de actualizar Unified Manager.

Si ha emparejado Workflow Automation y Unified Manager, debería actualizar manualmente el nombre del host en Workflow Automation.

Pasos

1. En vSphere Client, haga clic en **Inicio** > **Inventario** > **VMs and Templates**.
2. Seleccione la máquina virtual (VM) en la que esté instalado el dispositivo virtual de Unified Manager.
3. Si la VM de Unified Manager se está ejecutando, vaya a **Resumen** > **comandos** > **Apagar invitado**.
4. Crear una copia de backup, como una copia Snapshot o un clon, del equipo virtual de Unified Manager para crear un backup coherente con las aplicaciones.
5. En vSphere Client, encienda la máquina virtual de Unified Manager.
6. Inicie VMware Remote Console.
7. Haga clic en el icono **CDROM** y seleccione **conectar al archivo de imagen de disco (.iso)**.
8. Seleccione la `ActiveIQUnifiedManager-<version>-virtual-update.iso` Y haga clic en **Abrir**.
9. Haga clic en la ficha **Consola**.
10. Inicie sesión en la consola de mantenimiento de Unified Manager.
11. En el menú principal, seleccione **Actualizar**.

    Se muestra un mensaje que Unified Manager no está disponible durante el proceso de actualización y se reanuda una vez que se completa.

12. Tipo `y` para continuar.

Aparece una advertencia que le recuerda realizar una copia de seguridad de la máquina virtual en la que reside el dispositivo virtual.

13. Tipo `y` para continuar.

    El proceso de actualización y el reinicio de los servicios de Unified Manager pueden tardar varios minutos en completarse.

14. Pulse cualquier tecla para continuar.

    Se cerrará automáticamente la sesión de la consola de mantenimiento.

15. **Opcional:** Inicie sesión en la consola de mantenimiento y verifique la versión de Unified Manager.

Puede iniciar la interfaz de usuario web en una nueva ventana en un explorador web compatible e iniciar sesión para utilizar la versión actualizada de Unified Manager. Tenga en cuenta que debe esperar a que el proceso de detección finalice antes de realizar cualquier tarea en la interfaz de usuario de.

Reiniciar la máquina virtual de Unified Manager

Puede reiniciar la máquina virtual (VM) de Unified Manager desde la consola de mantenimiento. Debe reiniciar la máquina virtual después de generar un nuevo certificado de seguridad, o si hay un problema con la máquina virtual.

Lo que necesitará

- El dispositivo virtual debe estar encendido.
- Debe iniciar sesión en la consola de mantenimiento de Unified Manager como usuario de mantenimiento.

También puede reiniciar la máquina virtual desde vSphere mediante la opción VMware **Restart Guest**.

Pasos

1. En la consola de mantenimiento, seleccione **Configuración del sistema** > **Reiniciar máquina virtual**.
2. Inicie la interfaz de usuario web de Unified Manager desde el explorador e inicie sesión.

Información relacionada

"Referencia de cmdlets de VMware vSphere PowerCLI: Restart-VMGuest"

Se quita Unified Manager

Puede desinstalar Unified Manager si elimina la máquina virtual (VM) en la que está instalado el software Unified Manager.

Lo que necesitará

- Debe tener credenciales para acceder a VMware vCenter Server y vSphere Web Client.
- Se debe cerrar cualquier conexión activa del servidor de Unified Manager con un servidor de Workflow Automation.
- Todos los clústeres (orígenes de datos) se deben quitar del servidor de Unified Manager antes de quitar la máquina virtual (VM).

Pasos

1. Utilice la consola de mantenimiento de Unified Manager para verificar que el servidor de Unified Manager no tenga una conexión activa con un proveedor de datos externo.
2. En vSphere Client, haga clic en **Inicio** > **Inventario** > **VMs and Templates**.
3. Seleccione la máquina virtual que desea eliminar y haga clic en la ficha **Resumen**.
4. Si la máquina virtual se está ejecutando, haga clic en **Alimentación** > **Apagar invitado**.
5. Haga clic con el botón derecho del ratón en la VM que desea eliminar y haga clic en **Eliminar del disco**.

Instale Unified Manager en sistemas Linux

Introducción a Active IQ Unified Manager

Active IQ Unified Manager (anteriormente Unified Manager de OnCommand) le permite supervisar y gestionar el estado y el rendimiento de sus sistemas de almacenamiento de ONTAP desde una única interfaz. Puede implementar Unified Manager en un servidor Linux, en un servidor de Windows o como dispositivo virtual (vApp) en un host de VMware.

Después de completar la instalación y añadir los clústeres que desea gestionar, Unified Manager proporciona una interfaz gráfica que muestra el estado de la capacidad, la disponibilidad, la protección y el rendimiento de los sistemas de almacenamiento supervisados.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Lo que hace Unified Manager Server

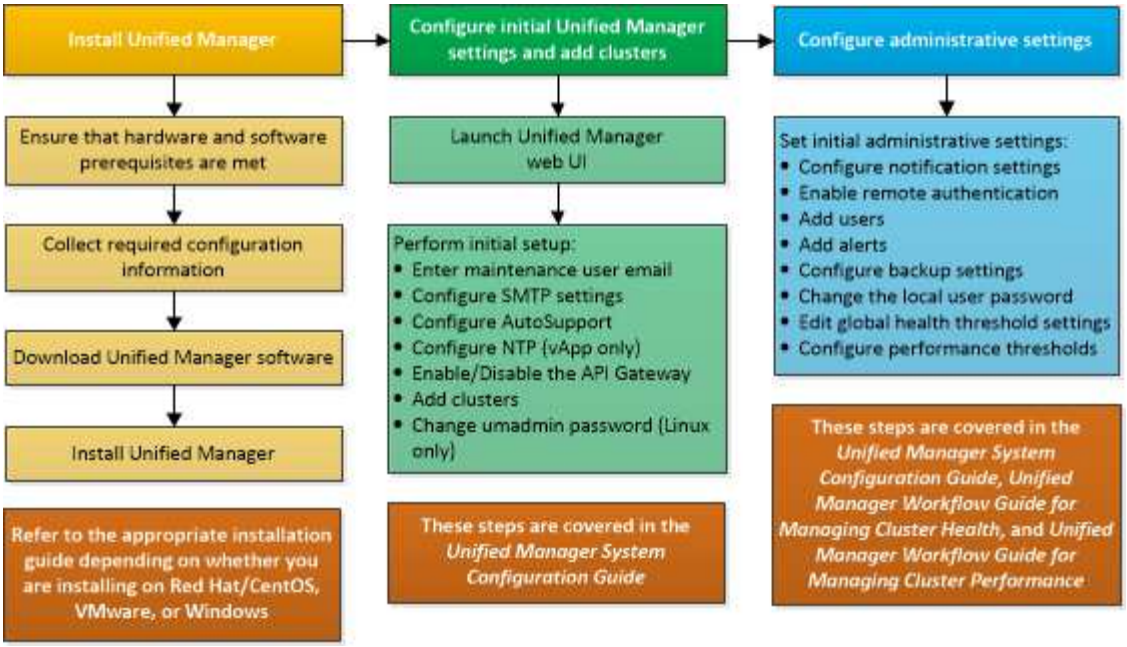
La infraestructura de servidor de Unified Manager consta de una unidad de recogida de datos, una base de datos y un servidor de aplicaciones. Proporciona servicios de infraestructura como detección, supervisión, control de acceso basado en roles (RBAC), auditoría y registro.

Unified Manager recopila información del clúster, almacena los datos en la base de datos y analiza los datos para ver si hay algún problema con el clúster.

Descripción general de la secuencia de instalación

El flujo de trabajo de instalación describe las tareas que deben realizarse para poder usar Unified Manager.

Estas secciones describen cada uno de los elementos mostrados en el flujo de trabajo siguiente.



Requisitos para instalar Unified Manager

Antes de iniciar el proceso de instalación, asegúrese de que el servidor en el que desea instalar Unified Manager cumpla con los requisitos específicos de software, hardware, CPU y memoria.

NetApp no admite ninguna modificación del código de aplicación de Unified Manager. Si necesita aplicar cualquier medida de seguridad al servidor de Unified Manager, debe realizar estos cambios en el sistema operativo en el que está instalado Unified Manager.

Para obtener más información sobre la aplicación de medidas de seguridad en Unified Manager Server, consulte el artículo de la base de conocimientos.

"Compatibilidad con las medidas de seguridad aplicadas a Active IQ Unified Manager para Clustered Data ONTAP"

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Requisitos del sistema de hardware e infraestructura virtual

La instalación de Unified Manager en una infraestructura virtual o un sistema físico debe cumplir con los requisitos mínimos de memoria, CPU y espacio en disco.

La siguiente tabla muestra los valores recomendados para los recursos de memoria, CPU y espacio en disco. Se han cualificado estos valores para que Unified Manager cumpla niveles de rendimiento aceptables.

Configuración de hardware	Configuración recomendada
RAM	12 GB (requisito mínimo de 8 GB)

Configuración de hardware	Configuración recomendada
Procesadores	4 CPU
Capacidad del ciclo de la CPU	9572 MHz en total (requisito mínimo de 9572 MHz)
Libere espacio en disco	150 GB, en los que se asigna la capacidad de la siguiente manera: • 50 GB asignados a la partición raíz • 100 GB de espacio libre en disco asignado al `/opt/netapp/data` directorio, que se monta en una unidad LVM o en un disco local independiente conectado al sistema de destino Para montaje independiente `/opt` y.. `/var/log` directorios, asegúrese de que `/opt` Tiene 15 GB y. `/var/log` Tiene 16 GB de espacio libre. La `/tmp` el directorio debe tener al menos 10 GB de espacio libre.

Unified Manager se puede instalar en sistemas con una pequeña cantidad de memoria, pero los 12 GB de RAM recomendados garantizan que haya suficiente memoria disponible para un rendimiento óptimo, por lo que el sistema puede acomodar clústeres y objetos de almacenamiento adicionales a medida que crezca su configuración. No debe establecer ningún límite de memoria en la máquina virtual donde se haya puesto en marcha Unified Manager y no debe habilitar ninguna función (por ejemplo, una configuración en globo) que impida que el software utilice la memoria asignada en el sistema.

Asimismo, existe un límite en cuanto al número de nodos que puede supervisar una única instancia de Unified Manager antes de instalar una segunda instancia de Unified Manager. Para obtener más información, consulte la *Best Practices Guide*.

"Informe técnico 4621: Guía de prácticas recomendadas de Unified Manager"

El intercambio de la memoria por página afecta negativamente al rendimiento del sistema y de la aplicación de gestión. Competir por recursos CPU que no están disponibles debido al uso general del host puede degradar el rendimiento.

Requisito para un uso dedicado

El sistema físico o virtual en el que se instala Unified Manager se debe utilizar exclusivamente para Unified Manager y no se debe compartir con otras aplicaciones. Otras aplicaciones pueden consumir recursos del sistema y reducir drásticamente el rendimiento de Unified Manager.

Requisitos de espacio para backups

Si tiene previsto utilizar la función de backup y restauración de Unified Manager, asigne capacidad adicional para que el directorio o disco «data» tenga 150 GB de espacio. Una copia de seguridad se puede escribir en un destino local o en un destino remoto. La práctica recomendada es identificar una ubicación remota externa al sistema host de Unified Manager que tiene un mínimo de 150 GB de espacio.

Requisitos para la conectividad de host

El sistema físico o el sistema virtual en el que instala Unified Manager debe configurarse de modo que pueda hacerlo correctamente `ping` el nombre de host del propio host. En caso de configuración IPv6, debe verificar que sí `ping6` El nombre de host se realiza correctamente para garantizar que la instalación de Unified Manager se realice correctamente.

Es posible usar el nombre de host (o la dirección IP del host) para acceder a la interfaz de usuario web del producto. Si configuró una dirección IP estática para la red durante la implementación, debe designar un nombre para el host de red. Si configuró la red mediante DHCP, debe obtener el nombre de host del DNS.

Si planea permitir a los usuarios acceder a Unified Manager mediante el nombre corto en lugar de usar el nombre de dominio completo (FQDN) o la dirección IP, la configuración de red debe resolver este nombre corto con un FQDN válido.

Requisitos de instalación y software Linux

El sistema Linux en el que instala Unified Manager requiere versiones específicas del sistema operativo y del software compatible.

Software del sistema operativo

El sistema Linux debe tener instaladas las siguientes versiones del sistema operativo y el software de soporte:

- Red Hat Enterprise Linux versiones 7.x y de 8,0 a 8,6, basado en la arquitectura x86_64.
- CentOS versión 7.x basado en arquitectura x86_64 CentOS Stream no es compatible.

Consulte la matriz de interoperabilidad para ver la lista completa y más actualizada de las versiones compatibles de Red Hat Enterprise Linux y CentOS.

"mysupport.netapp.com/matrix"

Software de terceros

Unified Manager se ha puesto en marcha en un servidor web de WildFly. WildFly 19.0.0 se incluye y configura con Unified Manager.

Se requieren los siguientes paquetes de terceros, pero no se incluyen con Unified Manager. Estos paquetes son instalados automáticamente por el `yum` instalador durante la instalación, siempre que haya configurado los repositorios como se menciona en las siguientes secciones.

- MySQL Community Edition versión 8.0.30 (del repositorio de MySQL).
- OpenJDK versión 11.0.17 (del repositorio de Red Hat Extra Enterprise Linux Server)
- Python 3.6.x
- P7zip versión 16.02 o posterior (del repositorio de Red Hat Extra Packages para Enterprise Linux)

Debe apagar una instancia en ejecución de Unified Manager antes de actualizar cualquier software de terceros. Tras completar la instalación del software de terceros, puede reiniciar Unified Manager.

Requisitos de autorización de usuarios

La instalación de Unified Manager en un sistema Linux puede realizarlo el usuario raíz o los usuarios no raíz mediante el `sudo` comando.

Requisitos de instalación

A continuación se enumeran las mejores prácticas para instalar Red Hat Enterprise Linux o CentOS y los repositorios asociados en su sistema. Los sistemas instalados o configurados de manera diferente, o puestos en marcha fuera de las instalaciones (en el cloud), pueden requerir pasos adicionales y es posible que Unified Manager no se ejecute correctamente en dichas puestas en marcha.

- Debe instalar Red Hat Enterprise Linux o CentOS de acuerdo con las mejores prácticas de Red Hat y debe seleccionar las siguientes opciones predeterminadas, lo que requiere seleccionar el entorno base "servidor con GUI".
- Durante la instalación de Unified Manager en Red Hat Enterprise Linux o CentOS, el sistema debe tener acceso al repositorio adecuado para que el programa de instalación pueda acceder a todas las dependencias de software necesarias e instalarlas.
- Para la `yum` Instalador para buscar software dependiente en los repositorios de Red Hat Enterprise Linux, debe haber registrado el sistema durante la instalación de Red Hat Enterprise Linux o después mediante una suscripción válida a Red Hat.

  Consulte la documentación de Red Hat para obtener información acerca de Red Hat Subscription Manager.

- Debe habilitar el repositorio de paquetes adicionales para Enterprise Linux (EPEL) para instalar correctamente las utilidades de terceros necesarias en el sistema.

  Si el repositorio de EPEL no está configurado en su sistema, debe descargar y configurar manualmente el repositorio.

  Consulte "Configurar manualmente el repositorio de EPEL".

- Si no está instalada la versión correcta de MySQL, debe habilitar el repositorio de MySQL para que pueda instalar correctamente el software MySQL en el sistema.

  Si el repositorio de MySQL no está configurado en el sistema, debe descargar y configurar manualmente el repositorio.

  Consulte "Configurar manualmente el repositorio de MySQL".

Si su sistema no tiene acceso a Internet y los repositorios no se duplican desde un sistema conectado a Internet al sistema no conectado, siga las instrucciones de instalación para determinar las dependencias de software externo de su sistema. A continuación, puede descargar el software necesario en el sistema conectado a Internet y copiar el `.rpm` Archivos en el sistema en el que tiene pensado instalar Unified Manager. Para descargar los artefactos y paquetes, debe usar `yum install` comando. Debe asegurarse de que los dos sistemas ejecutan la misma versión del sistema operativo y de que la licencia de suscripción es para la versión adecuada de Red Hat Enterprise Linux o CentOS.

No debe instalar el software de terceros necesario desde repositorios distintos a los que se enumeran aquí. El software instalado desde los repositorios de Red Hat se ha diseñado explícitamente para Red Hat Enterprise Linux y cumple con las prácticas recomendadas de Red Hat (diseños de directorios, permisos, etc.). Es posible que el software desde otras ubicaciones no siga estas directrices, lo que puede provocar errores en la instalación de Unified Manager o podría provocar problemas con actualizaciones futuras.

Requisito del puerto 443

Las imágenes genéricas de Red Hat Enterprise Linux y CentOS pueden bloquear el acceso externo al puerto 443. Debido a esta restricción, es posible que no se pueda conectar a la interfaz de usuario web del administrador después de instalar Unified Manager. La ejecución del comando siguiente permite el acceso al puerto 443 para todos los usuarios y aplicaciones externos en un sistema genérico Red Hat Enterprise Linux o CentOS.

```
# firewall-cmd --zone=public --add-port=443/tcp --permanent; firewall-cmd
--reload
```

Debe instalar Red Hat Enterprise Linux y CentOS con el entorno base "servidor con GUI". Proporciona los comandos utilizados por las instrucciones de instalación de Unified Manager. Es posible que otros entornos base requieran instalar comandos adicionales para validar o completar la instalación. Si la `firewall-cmd` no está disponible en el sistema, debe instalarlo ejecutando el siguiente comando:

```
# sudo yum install firewalld
```

Póngase en contacto con EL departamento de TI antes de ejecutar los comandos para ver si sus políticas de seguridad requieren un procedimiento diferente.

THP (páginas grandes transparentes) debe desactivarse en sistemas CentOS y Red Hat. Cuando se habilita esta opción, en algunos casos puede provocar que Unified Manager se apague cuando ciertos procesos consuman demasiado memoria y queden terminados.

Exploradores compatibles

Para acceder a la interfaz de usuario web de Unified Manager, utilice un explorador compatible.

La matriz de interoperabilidad tiene la lista de versiones de exploradores compatibles.

"mysupport.netapp.com/matrix"

En todos los navegadores, la desactivación de los bloqueadores de ventanas emergentes garantiza que las funciones de software se muestren correctamente.

Si planea configurar Unified Manager para la autenticación SAML y que un proveedor de identidades (IDP) pueda autenticar usuarios, debe comprobar también la lista de exploradores compatibles con IDP.

Requisitos de protocolo y puerto

Los puertos y protocolos necesarios permiten la comunicación entre el servidor de Unified Manager y los sistemas de almacenamiento gestionados, los servidores y otros componentes.

Conexiones con el servidor de Unified Manager

En instalaciones típicas no es necesario especificar números de puerto al conectarse a la interfaz de usuario web de Unified Manager, ya que siempre se utilizan los puertos predeterminados. Por ejemplo, como Unified Manager siempre intenta ejecutar en su puerto predeterminado, puede introducir `https://<host>` en lugar de `https://<host>:443`.

El servidor de Unified Manager utiliza protocolos específicos para acceder a las siguientes interfaces:

Interfaz	Protocolo	Puerto	Descripción
Interfaz de usuario web de Unified Manager	HTTP	80	Se utiliza para acceder a la IU web de Unified Manager; redirige automáticamente al puerto seguro 443.
API de interfaz de usuario web y programas de Unified Manager	HTTPS	443	Se usa para acceder de manera segura a la interfaz de usuario web de Unified Manager o para realizar llamadas API, ya que las llamadas API solo se pueden realizar mediante HTTPS.
Consola de mantenimiento	SSH/SFTP	22	Se usa para acceder a la consola de mantenimiento y recuperar los paquetes de soporte.
Línea de comandos de Linux	SSH/SFTP	22	Se utiliza para acceder a la línea de comandos Red Hat Enterprise Linux o CentOS y recuperar paquetes de soporte.
Base de datos MySQL	MySQL	3306	Se utiliza para habilitar el acceso de OnCommand Workflow Automation y OnCommand API Services a Unified Manager.
Syslog	UDP	514	Se utiliza para acceder a los mensajes de EMS basados en suscripción desde sistemas ONTAP y para crear eventos basados en los mensajes.

Interfaz	Protocolo	Puerto	Descripción
DESCANSO	HTTPS	9443	Se utiliza para acceder a eventos EMS basados en API DE REST en tiempo real desde sistemas ONTAP autenticados.

El puerto predeterminado de MySQL, 3306, está restringido solo a localhost mientras se instala Unified Manager en sistemas Linux. Esto no afecta a ningún escenario de actualización donde se mantenga la configuración anterior. Esta configuración puede modificarse y la conexión puede ponerse a disposición de otros hosts mediante el `Control access to MySQL port 3306` de la consola de mantenimiento. Para obtener más información, consulte "Opciones de menú adicionales". Los puertos que se utilizan para la comunicación HTTP y HTTPS (puertos 80 y 443) pueden cambiarse con la consola de mantenimiento de Unified Manager. Para obtener más información, consulte "Menús de la consola de mantenimiento".

Conexiones desde el servidor de Unified Manager

Debe configurar el firewall para que abra puertos que permitan la comunicación entre el servidor de Unified Manager y los sistemas de almacenamiento gestionados, los servidores y otros componentes. Si un puerto no está abierto, la comunicación falla.

Según su entorno, puede elegir modificar los puertos y los protocolos que utiliza el servidor de Unified Manager para conectarse a destinos específicos.

El servidor de Unified Manager se conecta utilizando los siguientes protocolos y puertos a los sistemas de almacenamiento gestionados, los servidores y otros componentes:

Destino	Protocolo	Puerto	Descripción
Sistema de almacenamiento	HTTPS	443 TCP	Se utiliza para supervisar y gestionar sistemas de almacenamiento.
Sistema de almacenamiento	NDMP	10000 TCP	Se utiliza para ciertas operaciones de restauración de Snapshot.
Servidor AutoSupport	HTTPS	443	Se utiliza para enviar información de AutoSupport. Requiere el acceso a Internet para realizar esta función.
Servidor de autenticación	LDAP	389	Se utiliza para realizar solicitudes de autenticación y solicitudes de búsqueda de usuarios y grupos.

Destino	Protocolo	Puerto	Descripción
LDAPS	636	Se utiliza para comunicación LDAP segura.	Servidor de correo
SMTP	25	Se utiliza para enviar correos electrónicos de notificación de alertas.	Remitente de captura SNMP
SNMPv1 o SNMPv3	162/UDP	Se utiliza para enviar notificaciones de alerta de capturas de SNMP.	Servidor de proveedores de datos externos
TCP	2003	Se utiliza para enviar datos de rendimiento a un proveedor de datos externo, como Graphite.	Servidor NTP

Rellenar la hoja de cálculo

Antes de instalar y configurar Unified Manager, debe tener disponible información específica acerca de su entorno. Puede registrar la información en la hoja de cálculo.

Información de instalación de Unified Manager

Los detalles necesarios para instalar Unified Manager.

Sistema en el que se ha puesto en marcha el software	Su valor
Nombre de dominio completo del host	
Dirección IP del host	
Máscara de red	
Dirección IP de la pasarela	
Dirección DNS principal	
Dirección DNS secundaria	
Buscar dominios	
Nombre de usuario de mantenimiento	

Sistema en el que se ha puesto en marcha el software	Su valor
Contraseña de usuario de mantenimiento	

Información de configuración de Unified Manager

Los detalles para configurar Unified Manager después de la instalación. Algunos valores son opcionales según la configuración.

Ajuste	Su valor
Dirección de correo electrónico del usuario de mantenimiento	
Nombre de host o dirección IP del servidor SMTP	
Nombre de usuario SMTP	
Contraseña SMTP	
Puerto SMTP	25 (valor predeterminado)
Correo electrónico desde el cual se envían notificaciones de alerta	
Nombre de host o dirección IP del servidor de autenticación	
El nombre de administrador de Active Directory o el nombre distintivo de enlace LDAP	
Contraseña de Active Directory o contraseña de enlace LDAP	
Nombre distintivo de la base del servidor de autenticación	
URL del proveedor de identidades (IDP)	
Metadatos del proveedor de identidades (IDP)	
Direcciones IP del host de destino de capturas SNMP	
Puerto SNMP	

Información del clúster

Los detalles sobre los sistemas de almacenamiento que gestiona mediante Unified Manager.

Clúster 1 de N	Su valor
El nombre de host o la dirección IP de administración del clúster	
Nombre de usuario del administrador ONTAP Al administrador se le debe haber asignado la función «admin».	
Contraseña del administrador de ONTAP	
Protocolo	HTTPS

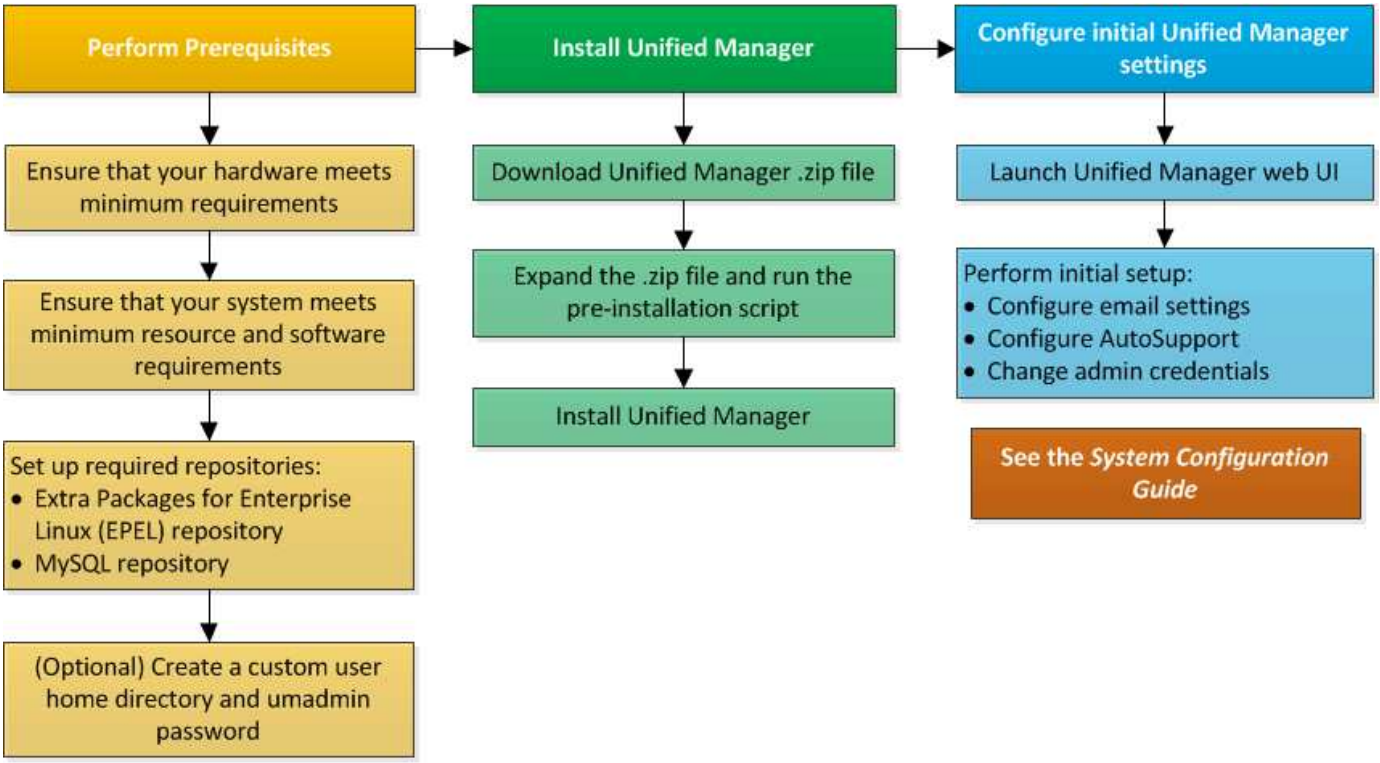
Instalación, actualización y eliminación del software Unified Manager

En los sistemas Linux, puede instalar el software Unified Manager, actualizar a una versión más reciente del software o quitar Unified Manager.

Unified Manager se puede instalar en servidores Red Hat Enterprise Linux o CentOS. El servidor Linux en el que instala Unified Manager puede ejecutarse en un equipo físico o en un equipo virtual que ejecute VMware ESXi, Microsoft Hyper-V o Citrix XenServer.

Descripción general del proceso de instalación

El flujo de trabajo de instalación describe las tareas que deben realizarse para poder usar Unified Manager.



Configurar repositorios de software necesarios

El sistema debe tener acceso a ciertos repositorios para que el programa de instalación pueda acceder e instalar todas las dependencias de software necesarias.

Configurar manualmente el repositorio de EPEL

Si el sistema en el que está instalando Unified Manager no tiene acceso al repositorio de paquetes extra para Enterprise Linux (EPEL), debe descargar y configurar manualmente el repositorio para una instalación correcta.

El repositorio de EPEL proporciona acceso a las utilidades de terceros necesarias que deben instalarse en el sistema. Puede utilizar el repositorio de EPEL tanto si está instalando Unified Manager en un sistema Red Hat Enterprise Linux o CentOS.

Pasos

1. Descargue el repositorio de EPEL para su instalación. Para Red Hat Enterprise Linux 7, descárguelo de:

   ```
   wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
   ```

   Para la versión 8, descárguela de:

   ```
   wget https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

2. Configurar el repositorio de EPEL:

   ```
   yum install epel-release-latest-<version>.noarch.rpm
   ```

Para sistemas Red Hat Enterprise Linux 8, si tiene repositorios internos con paquetes RPM modulares, por

ejemplo, *javapackages-filesystem-<version>.module.rpm*, asegúrese de que los metadatos de los paquetes modulares estén también disponibles en el mismo repositorio.

Configurar manualmente el repositorio de MySQL

Si el sistema en el que está instalando Unified Manager no tiene acceso al repositorio de MySQL Community Edition, debe descargar y configurar manualmente el repositorio para una instalación correcta.

El repositorio de MySQL proporciona acceso al software MySQL necesario que debe instalarse en el sistema.

Esta tarea podría fallar si el sistema no tiene conectividad a Internet. Consulte la documentación de MySQL si el sistema en el que va a instalar Unified Manager no tiene acceso a Internet.

Pasos

1. Descargue el repositorio de MySQL adecuado para su instalación. Para Red Hat Enterprise Linux 7, descárguelo de:

   ```
   wget http://repo.mysql.com/yum/mysql-8.0-community/el/7/x86_64/mysql80-community-release-el7-3.noarch.rpm
   ```

   Para la versión 8, descárguela de:

   ```
   wget http://repo.mysql.com/yum/mysql-8.0-community/el/8/x86_64/mysql80-community-release-el8-1.noarch.rpm
   ```

2. Configure el repositorio de MySQL:

   ```
   yum install mysql80-community-release-<version>.noarch.rpm
   ```

Para el sistema Red Hat Enterprise Linux 8, si tiene repositorios internos con java-11-openjdk, p7zip y otros paquetes de software proporcionados por el repositorio AppStream, debe deshabilitar el repositorio de AppStream e instalar MySQL Community Server. Ejecute el siguiente comando:

```
# sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install  mysql-community-server
```

Si recibe un error cuando falta una clave o falta de coincidencia de claves y la instalación falla, intente realizar los siguientes pasos:

- En un sistema conectado, importe la clave MySQL actualizada ejecutando el siguiente comando:

```
rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-<xxxx>

for example:

rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2022
```

- En un sistema que no tiene conectividad a Internet, actualice el archivo MySQL repo y desactívelo `gpgcheck` marcando `gpgcheck=0`.

Requisitos de SELinux en recursos compartidos NFS y CIFS

Si tiene pensado montar `/opt/netapp` o. `/opt/netapp/data` En un dispositivo NAS o SAN, y ha activado SELinux, debe ser consciente de algunas consideraciones.

Si tiene pensado montar `/opt/netapp` o. `/opt/netapp/data` Desde cualquier otro lugar que no sea el sistema de archivos raíz, y ha habilitado SELinux en su entorno, debe establecer el contexto correcto para los directorios montados. Para el escenario aplicable en su entorno, siga estos pasos para configurar y confirmar el contexto SELinux correcto.

Configuración del contexto SELinux cuando `/opt/netapp/data` está montado

Si ha montado `/opt/netapp/data` En su sistema y SELinux está configurado como `Enforcing`, Asegúrese de que el tipo de contexto SELinux para `/opt/netapp/data` se establece en `mysqld_db_t`, que es el elemento de contexto predeterminado para la ubicación de los archivos de base de datos.

1. Ejecute este comando para comprobar el contexto:

   ```
   ls -dZ /opt/netapp/data
   ```

   Una salida de muestra:

   ```
   drwxr-xr-x. mysql root unconfined_u:object_r:default_t:s0
   /opt/netapp/data
   ```

   > En este resultado, el contexto es `default_t`. Debe cambiar este contexto a. `mysqld_db_t`.

2. Realice estos pasos para establecer el contexto en función de cómo se haya montado `/opt/netapp/data`.

   a. Ejecute los siguientes comandos para establecer el contexto en `mysqld_db_t`:
   `semanage fcontext -a -t mysqld_db_t "/opt/netapp/data"`
   `` `restorecon -R -v /opt/netapp/data ``

   b. Si se configuró `/opt/netapp/data` pulg `/etc/fstab`, debe editar el `/etc/fstab` archivo. Para la `/opt/netapp/data/` mount, añada la etiqueta MySQL como:

   ```
   context=system_u:object_r:mysqld_db_t:s0
   ```

   c. Desmontar y volver a montar `/opt/netapp/data/` para habilitar el contexto.

   d. Si tiene un montaje NFS directo, ejecute el siguiente comando para establecer el contexto en `mysqld_db_t`:

   ```
   mount <nfsshare>:/<mountpoint> /opt/netapp/data -o
   context=system_u:object_r:mysqld_db_t:s0
   ```

3. Compruebe si el contexto está configurado correctamente:

```
ls -dZ /opt/netapp/data/
```

Una salida de muestra:

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/
```

Configuración del contexto SELinux cuando `/opt/netapp` está montado, y. `/opt/netapp/data/` también se monta por separado

En este escenario, al principio, debe establecer el contexto para `/opt/netapp/data/` como se describe en la sección anterior. Después de establecer el contexto correcto para `/opt/netapp/data/`, asegúrese de que el directorio principal `/opt/netapp` No tiene el contexto SELinux establecido en `file_t`.

Pasos

1. Ejecute este comando para comprobar el contexto:

   ```
   ls -dZ /opt/netapp
   ```

   Una salida de muestra:

   ```
   drwxr-xr-x. mysql root unconfined_u:object_r:file_t:s0 /opt/netapp
   ```

   En este resultado, el contexto es `file_t` debe cambiarse. Los siguientes comandos establecen el contexto en `usr_t`. Puede establecer el contexto en cualquier valor distinto de `file_t` según sus requisitos de seguridad.

2. Realice estos pasos para definir el contexto, en función de cómo se haya montado `/opt/netapp`.

   a. Ejecute los siguientes comandos para configurar el contexto:

```
semanage fcontext -a -t usr_t "/opt/netapp"
restorecon -v /opt/netapp
```

1. Si se configuró `/opt/netapp` pulg `/etc/fstab`, debe editar el `/etc/fstab` archivo. Para la `/opt/netapp` mount, añada la etiqueta MySQL como:

   ```
   context=system_u:object_r:usr_t:s0
   ```

2. Desmonte y, a continuación, monte de nuevo `/opt/netapp` para habilitar el contexto.
3. Si tiene un montaje NFS directo, ejecute el siguiente comando para establecer el contexto:

   ```
   mount <nfsshare>:/<mountpoint> /opt/netapp -o
   context=system_u:object_r:usr_t:s0
   ```

a. Compruebe si el contexto está configurado correctamente:

```
ls -dZ /opt/netapp
```

Salida de muestra

```
drwxr-xr-x. mysql root unconfined_u:object_r:usr_t:s0 /opt/netapp
```

Configuración del contexto SELinux cuando `/opt/netapp` está montado, y. `/opt/netapp/data/` no se monta por separado

Si ha montado `/opt/netapp` En su sistema y SELinux está configurado como `Enforcing`, Asegúrese de que el tipo de contexto SELinux para `/opt/netapp` se establece en `mysqld_db_t`, que es el elemento de contexto predeterminado para la ubicación de los archivos de base de datos.

Pasos

1. Ejecute este comando para comprobar el contexto:

   ```
   ls -dZ /opt/netapp
   ```

   Una salida de muestra:

   ```
   drwxr-xr-x. mysql root unconfined_u:object_r:default_t:s0 /opt/netapp
   ```

   En este resultado, el contexto es `default_t`. Debe cambiar este contexto a. `mysqld_db_t`.

2. Realice los pasos siguientes para establecer el contexto en función de cómo se haya montado `/opt/netapp`.

   a. Ejecute los siguientes comandos para establecer el contexto en `mysqld_db_t`:
   `semanage fcontext -a -t mysqld_db_t "/opt/netapp"`
   `` `restorecon -R -v /opt/netapp ``

   b. Si se configuró `/opt/netapp` pulg `/etc/fstab`, edite la `/etc/fstab` archivo. Para la `/opt/netapp/` mount, añada la etiqueta MySQL como:
   `context=system_u:object_r:mysqld_db_t:s0`

   c. Desmonte y, a continuación, monte de nuevo `/opt/netapp/` para habilitar el contexto.

   d. Si tiene un montaje NFS directo, ejecute el siguiente comando para establecer el contexto en `mysqld_db_t`:
   `mount <nfsshare>:/<mountpoint> /opt/netapp -o context=system_u:object_r:mysqld_db_t:s0`

3. Compruebe si el contexto está configurado correctamente:

```
ls -dZ /opt/netapp/
```

Una salida de muestra:

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysqld_db_t:s0 /opt/netapp/
```

Instalación de Unified Manager en sistemas Linux

Es importante comprender que la secuencia de pasos para descargar e instalar Unified Manager varía en función de su situación de instalación.

Creación de un directorio inicial de usuario personalizado y una contraseña umadmin antes de la instalación

Puede crear un directorio inicial personalizado y definir su propia contraseña de usuario umadmin antes de instalar Unified Manager. Esta tarea es opcional, pero es posible que algunos sitios necesiten la flexibilidad para anular la configuración predeterminada de la instalación de Unified Manager.

Lo que necesitará

- El sistema debe cumplir los requisitos descritos en "Requisitos del sistema de hardware".
- Debe poder iniciar sesión como usuario root en el sistema Red Hat Enterprise Linux o CentOS.

La instalación predeterminada de Unified Manager realiza las siguientes tareas:

- Crea el usuario umadmin con `/home/umadmin` como directorio principal.
- Asigna la contraseña predeterminada "'admin'" al usuario umadmin.

Porque algunos entornos de instalación restringen el acceso a. `/home`, la instalación falla. Debe crear el directorio inicial en una ubicación diferente. Además, algunos sitios pueden tener reglas acerca de la complejidad de la contraseña o requerir que los administradores locales establezcan las contraseñas en lugar de ser configuradas por el programa de instalación.

Si su entorno de instalación requiere que usted anule estos valores predeterminados de instalación, siga estos pasos para crear un directorio particular personalizado y para definir la contraseña del usuario umadmin.

Cuando esta información se define antes de la instalación, el script de instalación detecta esta configuración y utiliza los valores definidos en lugar de utilizar la configuración predeterminada de instalación.

Además, la instalación predeterminada de Unified Manager incluye el usuario umadmin en los archivos sudoers (`ocum_sudoers` y.. `ocie_sudoers`) en la `/etc/sudoers.d/` directorio. Si elimina este contenido del entorno debido a políticas de seguridad o a alguna herramienta de supervisión de seguridad, debe volver a añadirlo. Debe conservar la configuración de sudoers porque algunas operaciones de Unified Manager requieren estos privilegios sudo.

Las políticas de seguridad del entorno no deben restringir los privilegios sudo para el usuario de mantenimiento de Unified Manager. Es posible que se produzca un error en algunas operaciones de Unified Manager si se restringen los privilegios. Verifique que pueda ejecutar el siguiente comando sudo cuando inicie sesión como usuario umadmin después de una instalación correcta.

```
sudo systemctl status ocie
```

Este comando debería devolver el estado adecuado del servicio ocie sin ningún error.

Pasos

1. Inicie sesión como usuario root en el servidor.
2. Crear la cuenta de grupo umadmin llamada «mantenimiento»:

   ```
   groupadd maintenance
   ```

3. Cree la cuenta de usuario "'umadmin'" en el grupo de mantenimiento bajo un directorio inicial de su elección:

   ```
   adduser --home <home_directory\> -g maintenance umadmin
   ```

4. Defina la contraseña umadmin:

   ```
   passwd umadmin
   ```

   El sistema le pide que introduzca una nueva cadena de contraseña para el usuario umadmin.

Después de instalar Unified Manager, debe especificar el shell de inicio de sesión de usuario umadmin.

Descargue Unified Manager

Debe descargar Unified Manager `.zip` Archivo del sitio de soporte de NetApp para instalar Unified Manager.

Lo que necesitará

Debe tener credenciales de inicio de sesión en el sitio de soporte de NetApp.

Puede descargar el mismo paquete de instalación de Unified Manager para sistemas Red Hat Enterprise Linux y CentOS.

Pasos

1. Inicie sesión en el sitio de soporte de NetApp y desplácese hasta la página de descarga de Unified Manager:

   "Sitio de soporte de NetApp"

2. Seleccione la versión requerida de Unified Manager y acepte el contrato de licencia para usuarios finales (CLUF).
3. Descargue el archivo del instalador de Unified Manager para Linux y guarde el `.zip` archivo en un directorio del sistema de destino.

   - Asegúrese de descargar la versión correcta del archivo de instalación del sistema Red Hat Enterprise Linux. Según si tiene Red Hat Enterprise Linux 7 o 8 instalado, asegúrese de descargar la versión adecuada de Unified Manager `.zip` archivo.
   - NetApp recomienda descargar el certificado de firma de código (`.pem`) y firma digital (`.sig`) junto con el `.zip` archivo.

4. Compruebe la suma de comprobación para comprobar la integridad del software descargado.

5. Si ha descargado el certificado de firma de código y la firma digital, puede comprobar la integridad del archivo del instalador. Puede utilizar los siguientes comandos para comprobar la integridad del archivo del instalador:
   - Este comando crea un archivo con la clave pública a partir del certificado de firma de código:

     ```
     openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem >
     <public_key_file_name>
     ```

     - Donde **AIUM-RHEL-CLIENT-INTER-ROOT.pem** es el archivo que contiene el certificado de firma de código.
   - Este comando verifica la firma en el archivo del instalador:

     ```
     openssl dgst -sha256 -verify <public_key_file_name> -signature
     <signature_file_name> ActiveIQUnifiedManager-<version>.zip
     ```

     Mensaje similar a. `Verified Ok` confirma que el archivo del instalador es seguro de utilizar.

Instalación de Unified Manager

Puede instalar Unified Manager en una plataforma física o virtual Red Hat Enterprise Linux o CentOS.

Lo que necesitará

- El sistema en el que desea instalar Unified Manager debe cumplir con los requisitos del sistema y del software.

  Consulte "Requisitos del sistema de hardware".

  Consulte "Requisitos de instalación y software Linux".

- Debe haber descargado el Unified Manager `.zip` Archivo del sitio de soporte de NetApp al sistema de destino.
- Debe haber verificado la integridad de la descarga `.zip` archivo.
- Debe tener un navegador web compatible.
- El software de emulación de terminal debe tener activado sscrrollback.

El sistema Red Hat Enterprise Linux o CentOS puede tener instaladas todas las versiones necesarias del software compatible necesario (Java, MySQL, utilidades adicionales), sólo parte del software necesario instalado o puede ser un sistema recién instalado sin el software necesario instalado.

Pasos

1. Inicie sesión en el servidor en el que está instalando Unified Manager.
2. Escriba los comandos apropiados para evaluar qué software puede requerir la instalación o actualización en el sistema de destino para admitir la instalación:

Versión mínima y del software necesarios	Comando para verificar el software y la versión
OpenJDK versión 11.0.17	`java -version`
Edición comunitaria de MySQL 8.0.30	`rpm -qa
grep -i mysql`	p7zip 16.02
`rpm -qa	grep p7zip`

3. Si la versión instalada de MySQL es anterior a MySQL 8.0.30 Community Edition, introduzca el siguiente comando para desinstalarla:

   `rpm -e <mysql_package_name>`

   Si recibe errores de dependencia, debe agregar `--nodeps` opción para desinstalar el componente.

4. Desplácese hasta el directorio en el que ha descargado la instalación `.zip` Archive y expanda el paquete de Unified Manager:

   `unzip ActiveIQUnifiedManager-<version>.zip`

   El requerido `.rpm` Los módulos de Unified Manager se descomprimen en el directorio de destino.

5. Compruebe que el siguiente módulo esté disponible en el directorio:

   `ls *.rpm`

   `netapp-um<version>.x86_64.rpm`

6. Ejecute el script de instalación previa para garantizar que no haya ninguna configuración del sistema o ningún software instalado que pueda entrar en conflicto con la instalación de Unified Manager:

   `sudo ./pre_install_check.sh`

   La secuencia de comandos de preinstalación comprueba que el sistema tiene una suscripción válida a Red Hat Enterprise Linux y que tiene acceso a los repositorios de software necesarios. Si el script identifica cualquier problema, debe corregir los problemas antes de instalar Unified Manager.

   En el caso del sistema Red Hat Enterprise Linux 8, si tiene repositorios internos con JDK 11 - OpenJDK, p7zip y otros paquetes de software proporcionados por el repositorio de AppStream, debe deshabilitar el repositorio de AppStream e instalar MySQL Community Server. Ejecute el siguiente comando:

   ```
   # sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install
   mysql-community-server
   ```

7. **Opcional:** debe realizar el paso 7 sólo si su sistema no está conectado a Internet y tiene que descargar manualmente los paquetes necesarios para su instalación. Si su sistema tiene acceso a Internet y todos los paquetes necesarios están disponibles, vaya al paso 8. Para los sistemas que no están conectados a Internet o que no utilizan los repositorios de Red Hat Enterprise Linux, realice los siguientes pasos para

determinar si falta algún paquete necesario y, a continuación, descargue dichos paquetes:

a. En el sistema en el que está instalando Unified Manager, consulte la lista de paquetes disponibles y no disponibles:
`yum install netapp-um<version>.x86_64.rpm --assumeno`

   Los elementos de la sección «'instalación:'» son los paquetes que están disponibles en el directorio actual, y los elementos de la sección «'instalación de dependencias:'» son los paquetes que faltan en su sistema.

b. En un sistema que tenga acceso a Internet, descargue los paquetes que faltan:

   `yum install <package_name> --downloadonly --downloaddir=.`

   Puesto que el complemento "'yum-plugin-downloadonly'" no siempre está activado en los sistemas Red Hat Enterprise Linux, es posible que tenga que habilitar la funcionalidad para descargar un paquete sin instalarlo:
   `yum install yum-plugin-downloadonly`

a. Copie los paquetes que faltan del sistema conectado a Internet en el sistema de instalación.

8. Como usuario raíz, o usando `sudo`, ejecute el siguiente comando para instalar el software:

   `yum install netapp-um<version>.x86_64.rpm`

   Este comando instala los paquetes .rpm, todo el software de soporte necesario y el software Unified Manager.

   No intente la instalación utilizando comandos alternativos (como `rpm -ivh`). Una instalación correcta de Unified Manager en un sistema Red Hat Enterprise Linux o CentOS requiere que todos los archivos de Unified Manager y los archivos relacionados se instalen en un orden específico en una estructura de directorio específica que el aplique automáticamente `yum install netapp-um<version>.x86_64.rpm` comando.

9. Ignore la notificación de correo electrónico que se muestra inmediatamente después de los mensajes de instalación.

   El correo electrónico notifica al usuario raíz de un error inicial en la tarea de cron, que no tiene ningún efecto adverso en la instalación.

10. Una vez hayan completado los mensajes de instalación, desplácese hacia atrás por los mensajes hasta ver el mensaje en el que el sistema muestra una dirección IP o una URL para la interfaz de usuario web de Unified Manager, el nombre de usuario de mantenimiento (umadmin) y una contraseña predeterminada.

    El mensaje es similar al siguiente:

```
Active IQ Unified Manager installed successfully.
Use a web browser and one of the following URL(s) to configure and
access the Unified Manager GUI.
https://default_ip_address/    (if using IPv4)
https://[default_ip_address]/  (if using IPv6)
https://fully_qualified_domain_name/

Log in to Unified Manager in a web browser by using following details:
  username: umadmin
  password: admin
```

11. Registre la dirección IP o URL, el nombre de usuario asignado (umadmin) y la contraseña actual.
12. Si ha creado una cuenta de usuario umadmin con un directorio inicial personalizado antes de instalar Unified Manager, debe especificar el shell de inicio de sesión de usuario umadmin:

    ```
    usermod -s /bin/maintenance-user-shell.sh umadmin
    ```

Acceda a la interfaz de usuario web para cambiar la contraseña predeterminada del usuario umadmin y ejecute la configuración inicial de Unified Manager, como se describe en "Configurando Active IQ Unified Manager". Es obligatorio cambiar la contraseña predeterminada del usuario umadmin.

Usuarios creados durante la instalación de Unified Manager

Al instalar Unified Manager en Red Hat Enterprise Linux o CentOS, Unified Manager crea los siguientes usuarios y las utilidades de terceros: Umadmin, jboss y mysql.

- **umadmin**

  Se utiliza para iniciar sesión en Unified Manager por primera vez. A este usuario se le asigna una función de usuario «'Administrador de aplicaciones'» y se configura como el tipo «Usuario de mantenimiento». Este usuario lo crea Unified Manager.

- **jboss**

  Se utiliza para ejecutar servicios de Unified Manager relacionados con la utilidad JBoss. Este usuario lo crea Unified Manager.

- **mysql**

  Se utiliza para ejecutar consultas de base de datos de MySQL de Unified Manager. Este usuario es creado por la utilidad de terceros de MySQL.

Además de estos usuarios, Unified Manager también crea los grupos correspondientes: Mantenimiento, jboss y mysql. Unified Manager crea los grupos de mantenimiento y jboss, mientras que el grupo mysql lo crea una utilidad de terceros.

Si creó un directorio inicial personalizado y definió su propia contraseña de usuario umadmin antes de instalar Unified Manager, el programa de instalación no volverá a crear el grupo de mantenimiento ni el usuario umadmin.

Cambio de la contraseña de JBoss

Puede restablecer la contraseña de JBoss específica de la instancia que se haya establecido durante la instalación. Es posible restablecer la contraseña de manera opcional; en caso de que el sitio requiera esta funcionalidad de seguridad para anular la configuración de instalación de Unified Manager. Esta operación también cambia la contraseña que JBoss utiliza para acceder a MySQL.

- Debe tener acceso de usuario raíz al sistema Red Hat Enterprise Linux o CentOS en el que está instalado Unified Manager.
- Debe poder acceder a la información proporcionada por NetApp `password.sh` script en el directorio `/opt/netapp/essentials/bin`.

Pasos

1. Inicie sesión como usuario root en el sistema.
2. Detenga los servicios de Unified Manager introduciendo los siguientes comandos en el orden mostrado:

   ```
   systemctl stop ocieau

   systemctl stop ocie
   ```

   No detenga el software MySQL asociado.

3. Introduzca el siguiente comando para iniciar el proceso de cambio de contraseña:

   ```
   /opt/netapp/essentials/bin/password.sh resetJBossPassword
   ```

4. Cuando se le solicite, introduzca la nueva contraseña de JBoss y, a continuación, introdúzcala una segunda vez para confirmarla.

   Tenga en cuenta que la contraseña debe tener entre 8 y 16 caracteres, y debe contener al menos un dígito, mayúsculas y minúsculas caracteres, y al menos uno de estos caracteres especiales:

   ```
   !@%^*-_=[]:<>.?/~+
   ```

5. Una vez finalizado el script, inicie los servicios de Unified Manager introduciendo los siguientes comandos en el orden que se muestra:

   ```
   systemctl start ocie

   systemctl start ocieau
   ```

6. Después de iniciar todos los servicios, puede iniciar sesión en la interfaz de usuario de Unified Manager.

Actualización de Unified Manager en Red Hat Enterprise Linux o CentOS

Es posible actualizar Unified Manager cuando hay una nueva versión disponible.

Los parches del software Unified Manager, que se proporcionan con NetApp, se instalan siguiendo el mismo procedimiento que las versiones nuevas.

Si Unified Manager se empareja con una instancia de OnCommand Workflow Automation y hay nuevas

versiones del software disponibles para ambos productos, debe desconectar los productos y, a continuación, configurar una nueva conexión de Workflow Automation tras las actualizaciones. Si solo actualiza uno de los productos, deberá iniciar sesión en Workflow Automation tras la actualización y comprobar que aún se recopilen datos de Unified Manager.

La ruta de actualización compatible con las versiones de Unified Manager

Active IQ Unified Manager admite una ruta de actualización específica para cada versión.

No todas las versiones de Unified Manager pueden realizar una actualización sin movimiento a versiones posteriores. Las actualizaciones de Unified Manager se limitan a un modelo N-2, lo que significa que la actualización solo se puede realizar en las próximas dos versiones de todas las plataformas. Por ejemplo, puede realizar una actualización a Unified Manager 9.12 solo desde Unified Manager 9.10 y 9.11.

Si ejecuta una versión anterior a las versiones compatibles, primero deberá actualizar la instancia de Unified Manager con una de las versiones compatibles y, a continuación, actualizarla a la versión actual.

Por ejemplo, si la versión instalada es OnCommand Unified Manager 9.5 y desea actualizar a la versión más reciente de Active IQ Unified Manager 9.12, siga una secuencia de actualizaciones.

Ruta de actualización de ejemplo:

1. Actualice Unified Manager 9.5 de OnCommand → Active IQ Unified Manager 9.7.
2. Actualización 9.7 → 9.9.
3. Actualización 9.9 → 9.11.
4. Actualización 9.11 → 9.12.

Para obtener más información acerca de la matriz de rutas de actualización, consulte este tema "Artículo de la base de conocimientos (KB)".

Actualizar Unified Manager

Puede actualizar desde Unified Manager 9.10 o 9.11 a 9.12 descargando y ejecutando el archivo de instalación en la plataforma Linux.

Lo que necesitará

- El sistema donde se actualiza Unified Manager debe cumplir con los requisitos del sistema y del software.

  Consulte "Requisitos del sistema de hardware".

  Consulte "Requisitos de instalación y software Linux".

- Debe disponer de una suscripción al administrador de suscripciones de Red Hat Enterprise Linux.
- Debe instalar o actualizar a la versión correcta de OpenJDK antes de actualizar Unified Manager.

  Consulte "Actualizar JRE en Linux".

- Para evitar la pérdida de datos, debe haber creado un backup de la base de datos de Unified Manager en caso de que haya un problema durante la actualización. NetApp recomienda mover el archivo de backup desde la `/opt/netapp/data` directorio a una ubicación externa.
- Durante la actualización, es posible que se le solicite que confirme si desea mantener la configuración predeterminada anterior para conservar los datos de rendimiento durante 13 meses o si desea cambiarla a

6 meses. Al confirmar, los datos de rendimiento históricos se purgan al cabo de 6 meses.

- Debe haber completado todas las operaciones en ejecución, ya que Unified Manager no está disponible durante el proceso de actualización.
- MySQL Community Edition se actualiza automáticamente durante la actualización de Unified Manager. Si la versión instalada de MySQL en el sistema es anterior a 8.0.30, el proceso de actualización de Unified Manager actualiza automáticamente MySQL a 8.0.30.

Pasos

1. Inicie sesión en el servidor Red Hat Enterprise Linux o CentOS de destino.
2. Descargue el paquete de Unified Manager en el servidor.

   Consulte "Descarga de Unified Manager para Linux".

3. Desplácese hasta el directorio de destino y expanda el paquete Unified Manager:

   ```
   unzip ActiveIQUnifiedManager-<version>.zip
   ```

   Los módulos RPM necesarios para Unified Manager se descomprimen en el directorio de destino.

4. Compruebe que el siguiente módulo esté disponible en el directorio:

   ```
   ls *.rpm
   ```

   ```
   netapp-um<version>.x86_64.rpm
   ```

5. Ejecute la secuencia de comandos previa a la instalación para asegurarse de que no haya ninguna configuración del sistema ni ningún software instalado que pueda entrar en conflicto con la actualización:

   ```
   sudo ./pre_install_check.sh
   ```

   La secuencia de comandos de preinstalación comprueba que el sistema tiene una suscripción válida a Red Hat Enterprise Linux y que tiene acceso a los repositorios de software necesarios. Si el script identifica algún problema, debe corregir los problemas y continuar con la actualización.

   Si se detecta algún paquete que falta, realice los pasos mencionados en "Pasos adicionales que se deben realizar para los paquetes que faltan". Si no faltan paquetes, continúe con los siguientes pasos.

6. Actualice Unified Manager con el siguiente script:

   ```
   upgrade.sh
   ```

   Esta secuencia de comandos ejecuta automáticamente los módulos RPM, actualizando el software compatible necesario y los módulos Unified Manager que se ejecutan en ellos. Además, el script de actualización comprueba si hay alguna configuración del sistema o cualquier software instalado que pueda entrar en conflicto con la actualización. Si el script identifica algún problema, debe corregir los problemas antes de actualizar Unified Manager. Si ha instalado paquetes previamente, como *net-snmp* antes de actualizar Unified Manager, la dependencia de MySQL podría desinstalar el paquete durante la actualización. Debe volver a instalar el paquete manualmente para continuar con su uso.

7. Una vez completada la actualización, desplácese hacia atrás por los mensajes hasta que vea el mensaje que muestra una dirección IP o una URL para la interfaz de usuario web de Unified Manager, el nombre de usuario de mantenimiento (umadmin) y la contraseña predeterminada.

El mensaje es similar al siguiente:

```
Active IQ Unified Manager upgraded successfully.
Use a web browser and one of the following URLs to access the Unified
Manager GUI:

https://default_ip_address/    (if using IPv4)
https://[default_ip_address]/  (if using IPv6)
https://fully_qualified_domain_name/
```

Introduzca la dirección IP o URL especificada en una nueva ventana de un explorador web compatible para iniciar la interfaz de usuario web de Unified Manager y, a continuación, inicie sesión con el mismo nombre de usuario de mantenimiento (umadmin) y la misma contraseña que estableció anteriormente.

Pasos adicionales que se deben realizar para los paquetes que faltan

Si hay algún paquete que falte en su sitio durante la actualización, o si su sistema no está conectado a Internet, o si no está utilizando los repositorios de Red Hat Enterprise Linux, realice los pasos siguientes para determinar si falta algún paquete necesario y descargue esos paquetes.

> Estos pasos deben realizarse después del paso *5* del procedimiento principal. Este procedimiento actualiza Unified Manager y no es necesario ejecutar ningún paso adicional para actualizar.

1. Consulte la lista de paquetes disponibles y no disponibles:

   ```
   yum install netapp-um<version>.x86_64.rpm --assumeno
   ```

   Los elementos de la sección «'instalación:'» son los paquetes que están disponibles en el directorio actual, y los elementos de la sección «'instalación de dependencias:'» son los paquetes que faltan en su sistema.

2. En otro sistema que tenga acceso a Internet, ejecute el siguiente comando para descargar los paquetes que faltan.

   ```
   yum install package_name --downloadonly --downloaddir=.
   ```

   Los paquetes se descargan en el directorio especificado como `--downloaddir=`.

   Puesto que el complemento "'yum-plugin-downloadonly'" no siempre está activado en los sistemas Red Hat Enterprise Linux, es posible que tenga que habilitar la funcionalidad para descargar un paquete sin instalarlo:

   ```
   yum install yum-plugin-downloadonly
   ```

3. Copie los paquetes descargados en el directorio donde descomprimió el paquete Unified Manager en el sistema de instalación.
4. Cambie los directorios a ese directorio y ejecute el siguiente comando para instalar los paquetes que faltan, junto con sus dependencias.

   ```
   yum install *.rpm
   ```

5. Inicie el servidor de Unified Manager. Ejecute estos comandos:

```
systemctl start ocie

systemctl start ocieau
```

Este proceso completa el proceso de actualización de Unified Manager. Introduzca la dirección IP o URL especificada en una nueva ventana de un explorador web compatible para iniciar la interfaz de usuario web de Unified Manager y, a continuación, inicie sesión con el mismo nombre de usuario de mantenimiento (umadmin) y la misma contraseña que estableció anteriormente.

Actualizar el sistema operativo del host desde Red Hat Enterprise Linux 7.x a 8.x.

Si anteriormente instaló Unified Manager en un sistema Red Hat Enterprise Linux 7.x y debe actualizar a Red Hat Enterprise Linux 8.x, debe seguir uno de los procedimientos enumerados en este tema. En ambos casos, debe crear una copia de seguridad de Unified Manager en el sistema Red Hat Enterprise Linux 7.x y, a continuación, restaurar el backup en un sistema Red Hat Enterprise Linux 8.x. Tenga en cuenta que las versiones compatibles de Red Hat Enterprise Linux van del 8,0 al 8,6.

La diferencia entre las dos opciones que se muestran a continuación es que, en un caso, se está ejecutando la restauración de Unified Manager en un nuevo servidor 8.x y, en el otro caso, se está realizando la operación de restauración en el mismo servidor.

Dado que esta tarea requiere que se cree un backup de Unified Manager en el sistema Red Hat Enterprise Linux 7.x, debe crear el backup solo cuando esté preparado para completar todo el proceso de actualización de modo que Unified Manager no tenga conexión durante el menor período de tiempo posible. Las brechas en los datos recopilados se muestran en la interfaz de usuario de Unified Manager durante el periodo de tiempo durante el cual se apaga el sistema Red Hat Enterprise Linux 7.x y antes de que se inicie la nueva versión de Red Hat Enterprise Linux 8.x.

Consulte "Gestión de operaciones de backup y restauración" si necesita revisar instrucciones detalladas para los procesos de copia de seguridad y restauración.

Actualización del sistema operativo host mediante un nuevo servidor

Siga estos pasos si tiene un sistema de repuesto en el que puede instalar el software Red Hat Enterprise Linux 8.x para poder realizar la restauración de Unified Manager en ese sistema mientras el sistema Red Hat Enterprise Linux 7.x sigue estando disponible.

1. Instale y configure un servidor nuevo con el software Red Hat Enterprise Linux 8.x.

   Consulte "Requisitos de instalación y software Linux".

2. En el sistema Red Hat Enterprise Linux 8.x, instale la misma versión del software Unified Manager que tiene en el sistema Red Hat Enterprise Linux 7.x.

   Consulte "Instalación de Unified Manager en Linux".

   No inicie la interfaz de usuario ni configure ningún clúster, usuario ni configuración de autenticación cuando se complete la instalación. El archivo de backup rellena esta información durante el proceso de restauración.

3. En el sistema Red Hat Enterprise Linux 7.x, desde el menú Administration de la interfaz de usuario web, cree un backup de Unified Manager y, a continuación, copie el archivo de backup (`.7z` archivo) y el contenido del directorio del repositorio de la base de datos (`/database-dumps-repo` subdirectorio) a una ubicación externa.
4. En el sistema Red Hat Enterprise Linux 7.x, apague Unified Manager.
5. En el sistema Red Hat Enterprise Linux 8.x, copie el archivo de copia de seguridad (`.7z` archivo) desde la ubicación externa a. `/opt/netapp/data/ocum-backup/` y los archivos del repositorio de la base de datos en `/database-dumps-repo` subdirectorio bajo el `/ocum-backup` directorio.
6. Introduzca el siguiente comando para restaurar la base de datos de Unified Manager desde el archivo de backup:

   ```
   um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>
   ```

7. Introduzca la dirección IP o la URL en el explorador web para iniciar la interfaz de usuario web de Unified Manager y, a continuación, inicie sesión en el sistema.

Una vez que haya comprobado que el sistema funciona correctamente, puede eliminar Unified Manager del sistema Red Hat Enterprise Linux 7.x.

Actualización del sistema operativo host en el mismo servidor

Siga estos pasos si no dispone de un sistema de repuesto en el que puede instalar el software Red Hat Enterprise Linux 8.x.

1. En el menú Administration de la interfaz de usuario web, cree un backup de Unified Manager y, a continuación, copie el archivo de backup (`.7z` archivo) y el contenido del directorio del repositorio de la base de datos (`/database-dumps-repo` subdirectorio) a una ubicación externa.
2. Retire la imagen de Red Hat Enterprise Linux 7.x del sistema y límpiela por completo.
3. Instale y configure el software Red Hat Enterprise Linux 8.x en el mismo sistema.

   Consulte "Requisitos de instalación y software Linux".

4. En el sistema Red Hat Enterprise Linux 8.x, instale la misma versión del software Unified Manager que tenía en el sistema Red Hat Enterprise Linux 7.x.

   Consulte "Instalación de Unified Manager en Linux".

   No inicie la interfaz de usuario ni configure ningún clúster, usuario ni configuración de autenticación cuando se complete la instalación. El archivo de backup rellena esta información durante el proceso de restauración.

5. Copie el archivo de copia de seguridad (`.7z` archivo) desde la ubicación externa a. `/opt/netapp/data/ocum-backup/` y los archivos del repositorio de la base de datos en `/database-dumps-repo` subdirectorio bajo el `/ocum-backup` directorio.
6. Introduzca el siguiente comando para restaurar la base de datos de Unified Manager desde el archivo de backup:

   ```
   um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>
   ```

7. Introduzca la dirección IP o la URL en el explorador web para iniciar la interfaz de usuario web de Unified Manager y, a continuación, inicie sesión en el sistema.

Actualización de productos de terceros tras la instalación de Unified Manager

Puede actualizar productos de terceros, como JRE, cuando Unified Manager ya está instalado en sistemas Linux.

Las empresas que desarrollan estos productos de terceros notifican periódicamente vulnerabilidades de seguridad. Puede actualizar a versiones más recientes de este software según su propio horario.

Actualización de OpenJDK en Linux

Puede realizar una actualización a una versión más reciente de OpenJDK en el servidor Linux en el que está instalado Unified Manager para obtener correcciones de vulnerabilidades de seguridad.

Lo que necesitará

Debe tener privilegios de usuario raíz para el sistema Linux en el que está instalado Unified Manager.

Puede actualizar versiones de OpenJDK dentro de las familias de versiones. Por ejemplo, puede actualizar de OpenJDK 11.0.14 a OpenJDK 11.0.17, pero no puede actualizar directamente de OpenJDK 11 a OpenJDK 12.

Pasos

1. Inicie sesión como usuario raíz en el equipo host de Unified Manager.
2. Descargue la versión adecuada de OpenJDK (64 bits) en el sistema de destino.
3. Detenga los servicios de Unified Manager:

```
systemctl stop ocieau

systemctl stop ocie
```

4. Instale la versión más reciente de OpenJDK en el sistema.
5. Inicie los servicios de Unified Manager:

```
systemctl start ocie

systemctl start ocieau
```

Reiniciar Unified Manager

Es posible que tenga que reiniciar Unified Manager después de realizar cambios de configuración.

Lo que necesitará

Debe tener acceso de usuario raíz al servidor Red Hat Enterprise Linux o CentOS en el que está instalado Unified Manager.

Pasos

1. Inicie sesión como usuario raíz en el servidor en el que desea reiniciar el servicio Unified Manager.
2. Detenga el servicio Unified Manager y el software MySQL asociado en el orden que se muestra:

```
systemctl stop ocieau

systemctl stop ocie

systemctl stop mysqld
```

3. Inicie Unified Manager en el orden mostrado:

```
systemctl start mysqld

systemctl start ocie

systemctl start ocieau
```

`mysqld` Es un programa daemon requerido para iniciar y detener el servidor MySQL.

Se quita Unified Manager

Puede detener y desinstalar Unified Manager desde el host Red Hat Enterprise Linux o CentOS con un solo comando.

Lo que necesitará

- Debe tener acceso de usuario raíz al servidor desde el que desea quitar Unified Manager.
- Security-Enhanced Linux (SELinux) debe estar desactivado en el sistema Linux. Cambie el modo de tiempo de ejecución de SELinux a "'permisive'" mediante el `setenforce 0` comando.
- Todos los clústeres (orígenes de datos) deben quitarse del servidor de Unified Manager antes de quitar el software.
- Debe eliminar manualmente las reglas de firewall que se crean para permitir o bloquear el puerto MySQL 3306. Las reglas de firewall no se eliminan automáticamente.

Pasos

1. Inicie sesión como usuario raíz en el servidor en el que desea quitar Unified Manager.
2. Detenga y quite Unified Manager del servidor:

```
rpm -e netapp-um
```

Este paso elimina todos los paquetes de RPM de NetApp asociados. No elimina los módulos de software previos, como Java, MySQL y p7zip.

3. **Opcional:** Si procede, retire los módulos de software compatibles, como Java, MySQL y p7zip:

```
rpm -e p7zip mysql-community-client mysql-community-server mysql-community-common mysql-community-libs java-x.y
```

Una vez finalizada esta operación, se elimina el software. Todos los datos del `/opt/netapp/data` el directorio se mueve al `/opt/netapp/data/BACKUP` carpeta tras la desinstalación. Al desinstalar Unified Manager también se quitan los paquetes de Java y MySQL, a menos que los paquetes sean necesarios y los use otra aplicación del sistema. Sin embargo, los datos de MySQL no se eliminan.

Quitar el usuario personalizado de umadmin y el grupo de mantenimiento

Si ha creado un directorio inicial personalizado para definir su propia cuenta de usuario umadmin y de mantenimiento antes de instalar Unified Manager, debe eliminar estos elementos después de haber desinstalado Unified Manager.

La desinstalación estándar de Unified Manager no quita una cuenta de mantenimiento y usuario umadmin definida de forma personalizada. Debe eliminar estos elementos manualmente.

Pasos

1. Inicie sesión como usuario root en el servidor Red Hat Enterprise Linux.
2. Eliminar el usuario umadmin:

   ```
   userdel umadmin
   ```

3. Elimine el grupo de mantenimiento:

   ```
   groupdel maintenance
   ```

Instale Unified Manager en sistemas Windows

Introducción a Active IQ Unified Manager

Active IQ Unified Manager (anteriormente Unified Manager de OnCommand) le permite supervisar y gestionar el estado y el rendimiento de sus sistemas de almacenamiento de ONTAP desde una única interfaz. Puede implementar Unified Manager en un servidor Linux, en un servidor de Windows o como dispositivo virtual en un host VMware.

Después de completar la instalación y añadir los clústeres que desea gestionar, Unified Manager proporciona una interfaz gráfica que muestra el estado de la capacidad, la disponibilidad, la protección y el rendimiento de los sistemas de almacenamiento supervisados.

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Lo que hace Unified Manager Server

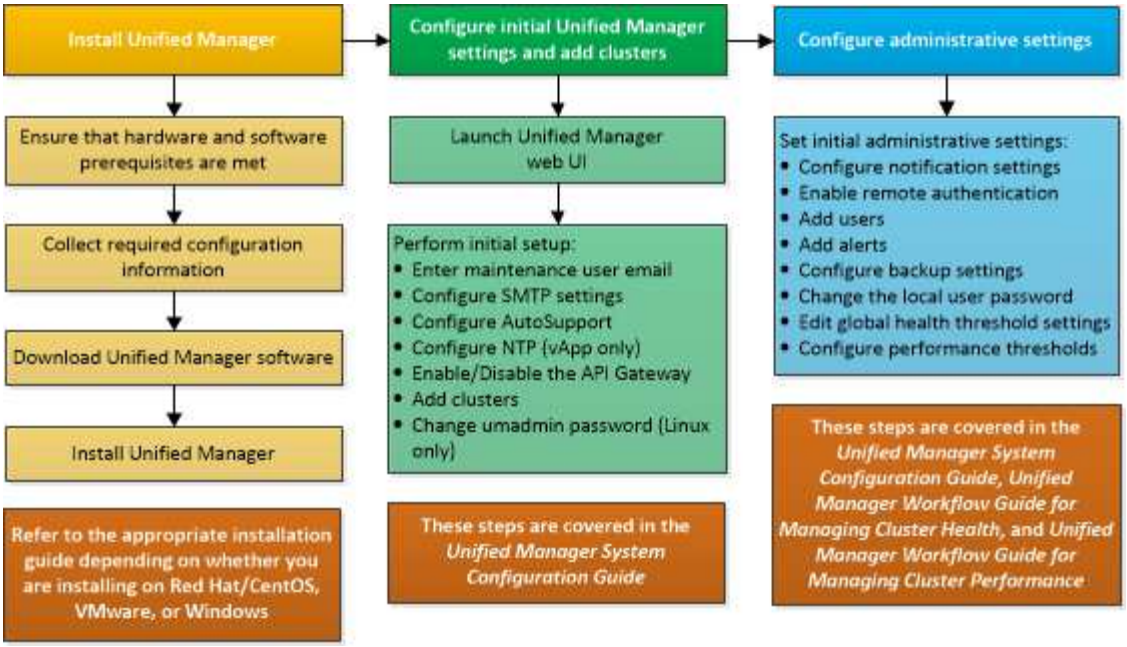
La infraestructura de servidor de Unified Manager consta de una unidad de recogida de datos, una base de datos y un servidor de aplicaciones. Proporciona servicios de infraestructura como detección, supervisión, control de acceso basado en roles (RBAC), auditoría y registro.

Unified Manager recopila información del clúster, almacena los datos en la base de datos y analiza los datos para ver si hay algún problema con el clúster.

Descripción general de la secuencia de instalación

El flujo de trabajo de instalación describe las tareas que deben realizarse para poder usar Unified Manager.

Estas secciones describen cada uno de los elementos mostrados en el flujo de trabajo siguiente.



Requisitos para instalar Unified Manager

Antes de iniciar el proceso de instalación, asegúrese de que el servidor en el que desea instalar Unified Manager cumpla con los requisitos específicos de software, hardware, CPU y memoria.

NetApp no admite ninguna modificación del código de aplicación de Unified Manager. Si necesita aplicar cualquier medida de seguridad al servidor de Unified Manager, debe realizar estos cambios en el sistema operativo en el que está instalado Unified Manager.

Para obtener más información sobre la aplicación de medidas de seguridad en Unified Manager Server, consulte el artículo de la base de conocimientos.

"Compatibilidad con las medidas de seguridad aplicadas a Active IQ Unified Manager para Clustered Data ONTAP"

Información relacionada

"Herramienta de matriz de interoperabilidad de NetApp"

Requisitos del sistema de hardware e infraestructura virtual

La instalación de Unified Manager en una infraestructura virtual o un sistema físico debe cumplir con los requisitos mínimos de memoria, CPU y espacio en disco.

La siguiente tabla muestra los valores recomendados para los recursos de memoria, CPU y espacio en disco. Se han cualificado estos valores para que Unified Manager cumpla niveles de rendimiento aceptables.

Configuración de hardware	Configuración recomendada
RAM	12 GB (requisito mínimo de 8 GB)

Configuración de hardware	Configuración recomendada
Procesadores	4 CPU
Capacidad del ciclo de la CPU	9572 MHz en total (requisito mínimo de 9572 MHz)
Libere espacio en disco	150 GB, en los que se asigna la capacidad de la siguiente manera: • 100 GB de espacio en disco para el directorio de instalación • 50 GB de espacio en disco para el directorio de datos de MySQL

Unified Manager se puede instalar en sistemas con una pequeña cantidad de memoria, pero los 12 GB de RAM recomendados garantizan que haya suficiente memoria disponible para un rendimiento óptimo, por lo que el sistema puede acomodar clústeres y objetos de almacenamiento adicionales a medida que crezca su configuración. No debe establecer ningún límite de memoria en la máquina virtual donde se haya puesto en marcha Unified Manager y no debe habilitar ninguna función (por ejemplo, una configuración en globo) que impida que el software utilice la memoria asignada en el sistema.

Asimismo, existe un límite en cuanto al número de nodos que puede supervisar una única instancia de Unified Manager antes de instalar una segunda instancia de Unified Manager. Para obtener más información, consulte la *Best Practices Guide*.

"Informe técnico 4621: Guía de prácticas recomendadas de Unified Manager"

El intercambio de la memoria por página afecta negativamente al rendimiento del sistema y de la aplicación de gestión. Competir por recursos CPU que no están disponibles debido al uso general del host puede degradar el rendimiento.

Requisito para un uso dedicado

El sistema físico o virtual en el que se instala Unified Manager se debe utilizar exclusivamente para Unified Manager y no se debe compartir con otras aplicaciones. Otras aplicaciones pueden consumir recursos del sistema y reducir drásticamente el rendimiento de Unified Manager.

Requisitos de espacio para backups

Si tiene previsto utilizar la función de backup y restauración de Unified Manager, asigne capacidad adicional para que el directorio o disco «data» tenga 150 GB de espacio. Una copia de seguridad se puede escribir en un destino local o en un destino remoto. La práctica recomendada es identificar una ubicación remota externa al sistema host de Unified Manager que tiene un mínimo de 150 GB de espacio.

Requisitos para la conectividad de host

El sistema físico o el sistema virtual en el que instala Unified Manager debe configurarse de modo que pueda hacerlo correctamente `ping` el nombre de host del propio host. En caso de configuración IPv6, debe verificar que sí `ping6` El nombre de host se realiza correctamente para garantizar que la instalación de Unified Manager se realice correctamente.

Es posible usar el nombre de host (o la dirección IP del host) para acceder a la interfaz de usuario web del

producto. Si configuró una dirección IP estática para la red durante la implementación, debe designar un nombre para el host de red. Si configuró la red mediante DHCP, debe obtener el nombre de host del DNS.

Si planea permitir a los usuarios acceder a Unified Manager mediante el nombre corto en lugar de usar el nombre de dominio completo (FQDN) o la dirección IP, la configuración de red debe resolver este nombre corto con un FQDN válido.

Requisitos de instalación y software de Windows

Para que la instalación correctamente de Unified Manager en Windows, debe asegurarse de que el sistema en el que se está instalando Unified Manager cumpla los requisitos de software.

Software del sistema operativo

Puede instalar Unified Manager en las siguientes ediciones de Windows:

- Microsoft Windows Server 2019 Standard y Datacenter Edition
- Microsoft Windows Server 2022 Standard y Datacenter Edition

Unified Manager es compatible con el sistema operativo Windows de 64 bits para los siguientes idiomas:

- Inglés
- Japonés
- Chino simplificado

Consulte la matriz de interoperabilidad para ver la lista completa y más actual de versiones de Windows compatibles.

"mysupport.netapp.com/matrix"

NetApp no admite la instalación de Unified Manager con herramientas de terceros, como Microsoft System Center Configuration Manager (SCCM).

El servidor debe estar dedicado a ejecutar Unified Manager. No se deben instalar otras aplicaciones en el servidor. Es posible que se instale un software antivirus activo en el sistema Windows debido a las normativas de la empresa. Debe deshabilitar el software antivirus antes de instalar Unified Manager para evitar que se produzca un fallo en la instalación.

Software de terceros

Los siguientes paquetes de terceros se incluyen en Unified Manager. Si estos paquetes de terceros no están instalados en su sistema, Unified Manager los instala como parte de la instalación.

- Microsoft Visual C++ 2015 paquete redistribuible versión 14.26.28720.3
- Microsoft Visual C++ Paquetes redistribuibles para Visual Studio 2013 versión 12.0.40660.0
- MySQL Community Edition versión 8.0.30
- Python 3.11.1
- OpenJDK versión 11.0.16
- p7zip versión 18.05 o posterior

A partir de Unified Manager 9.5, OpenJDK se proporciona en el paquete de instalación de Unified Manager y se instala automáticamente. Oracle Java no es compatible a partir de Unified Manager 9.5.

Si MySQL está preinstalado, debe asegurarse de que:

- Utiliza el puerto predeterminado.
- Las bases de datos de ejemplo no están instaladas.
- El nombre del servicio es «MYSQL8».

Unified Manager se ha puesto en marcha en un servidor web de WildFly. WildFly 19.0.0 se incluye y configura con Unified Manager.

Debe apagar una instancia en ejecución de Unified Manager antes de actualizar cualquier software de terceros. Tras completar la instalación del software de terceros, puede reiniciar Unified Manager.

Requisitos de instalación

- Se debe instalar Microsoft .NET 4.5.2 o superior.
- La `temp` el directorio debe configurarse con 2 GB de espacio en disco para extraer los archivos de instalación. Para comprobar si se ha creado el directorio, ejecute el siguiente comando en la interfaz de línea de comandos: `echo %temp%`
- Se deben reservar 2 GB de espacio en disco en la unidad de Windows para almacenar en caché los archivos MSI de Unified Manager.
- El servidor Microsoft Windows Server en el que desea instalar Unified Manager debe estar configurado con un nombre de dominio completo (FQDN), de modo que `ping` Las respuestas al nombre de host y al FQDN se realizan correctamente.
- Debe deshabilitar el servicio de publicación Web de Microsoft IIS en todo el mundo y asegurarse de que los puertos 80 y 443 son gratuitos.
- Debe asegurarse de que la configuración del host de sesión de Escritorio remoto para "'compatibilidad RDS de Windows Installer'" esté desactivada durante la instalación.
- El puerto UDP 514 debe estar libre y no debe ser utilizado por ningún otro servicio.
- Debe deshabilitar todo el software antivirus en el sistema antes de instalar Unified Manager. Una vez finalizada la instalación, asegúrese de excluir manualmente las siguientes rutas del análisis antivirus:
  - Directorio de datos de Unified Manager, por ejemplo, `C:\ProgramData\NetApp\OnCommandAppData\`
  - Directorio de instalación de Unified Manager, por ejemplo, `\C:\Program Files\NetApp\`
  - Directorio de datos de MySQL, por ejemplo, `C:\ProgramData\MySQL\MySQLServerData`

Exploradores compatibles

Para acceder a la interfaz de usuario web de Unified Manager, utilice un explorador compatible.

La matriz de interoperabilidad tiene la lista de versiones de exploradores compatibles.

"mysupport.netapp.com/matrix"

En todos los navegadores, la desactivación de los bloqueadores de ventanas emergentes garantiza que las funciones de software se muestren correctamente.

Si planea configurar Unified Manager para la autenticación SAML y que un proveedor de identidades (IDP) pueda autenticar usuarios, debe comprobar también la lista de exploradores compatibles con IDP.

Requisitos de protocolo y puerto

Los puertos y protocolos necesarios permiten la comunicación entre el servidor de Unified Manager y los sistemas de almacenamiento gestionados, los servidores y otros componentes.

Conexiones con el servidor de Unified Manager

En instalaciones típicas no es necesario especificar números de puerto al conectarse a la interfaz de usuario web de Unified Manager, ya que siempre se utilizan los puertos predeterminados. Por ejemplo, como Unified Manager siempre intenta ejecutar en su puerto predeterminado, puede introducir `https://<host>` en lugar de `https://<host>:443`.

El servidor de Unified Manager utiliza protocolos específicos para acceder a las siguientes interfaces:

Interfaz	Protocolo	Puerto	Descripción
Interfaz de usuario web de Unified Manager	HTTP	80	Se utiliza para acceder a la IU web de Unified Manager; redirige automáticamente al puerto seguro 443.
API de interfaz de usuario web y programas de Unified Manager	HTTPS	443	Se usa para acceder de manera segura a la interfaz de usuario web de Unified Manager o para realizar llamadas API, ya que las llamadas API solo se pueden realizar mediante HTTPS.
Consola de mantenimiento	SSH/SFTP	22	Se usa para acceder a la consola de mantenimiento y recuperar los paquetes de soporte.
Línea de comandos de Linux	SSH/SFTP	22	Se utiliza para acceder a la línea de comandos Red Hat Enterprise Linux o CentOS y recuperar paquetes de soporte.

Interfaz	Protocolo	Puerto	Descripción
Syslog	UDP	514	Se utiliza para acceder a los mensajes de EMS basados en suscripción desde sistemas ONTAP y para crear eventos basados en los mensajes.
DESCANSO	HTTPS	9443	Se utiliza para acceder a eventos EMS basados en API DE REST en tiempo real desde sistemas ONTAP autenticados.
Base de datos MySQL	MySQL	3306	Se utiliza para habilitar el acceso de OnCommand Workflow Automation y OnCommand API Services a Unified Manager.

El puerto predeterminado de MySQL, 3306, está restringido solo a localhost mientras se instala Unified Manager en sistemas Windows. Esto no afecta a ningún escenario de actualización donde se mantenga la configuración anterior. Esta configuración puede modificarse y la conexión puede ponerse a disposición de otros hosts mediante el `Control access to MySQL port 3306` de la consola de mantenimiento. Para obtener más información, consulte "Opciones de menú adicionales". Los puertos que se utilizan para la comunicación HTTP y HTTPS (puertos 80 y 443) pueden cambiarse con la consola de mantenimiento de Unified Manager. Para obtener más información, consulte "Configurando Active IQ Unified Manager".

Conexiones desde el servidor de Unified Manager

Debe configurar el firewall para que abra puertos que permitan la comunicación entre el servidor de Unified Manager y los sistemas de almacenamiento gestionados, los servidores y otros componentes. Si un puerto no está abierto, la comunicación falla.

Según su entorno, puede elegir modificar los puertos y los protocolos que utiliza el servidor de Unified Manager para conectarse a destinos específicos.

El servidor de Unified Manager se conecta utilizando los siguientes protocolos y puertos a los sistemas de almacenamiento gestionados, los servidores y otros componentes:

Destino	Protocolo	Puerto	Descripción
Sistema de almacenamiento	HTTPS	443 TCP	Se utiliza para supervisar y gestionar sistemas de almacenamiento.

Destino	Protocolo	Puerto	Descripción
Sistema de almacenamiento	NDMP	10000 TCP	Se utiliza para ciertas operaciones de restauración de Snapshot.
Servidor AutoSupport	HTTPS	443	Se utiliza para enviar información de AutoSupport. Requiere el acceso a Internet para realizar esta función.
Servidor de autenticación	LDAP	389	Se utiliza para realizar solicitudes de autenticación y solicitudes de búsqueda de usuarios y grupos.
LDAPS	636	Se utiliza para comunicación LDAP segura.	Servidor de correo
SMTP	25	Se utiliza para enviar correos electrónicos de notificación de alertas.	Remitente de captura SNMP
SNMPv1 o SNMPv3	162/UDP	Se utiliza para enviar notificaciones de alerta de capturas de SNMP.	Servidor de proveedores de datos externos
TCP	2003	Se utiliza para enviar datos de rendimiento a un proveedor de datos externo, como Graphite.	Servidor NTP

Rellenar la hoja de cálculo

Antes de instalar y configurar Unified Manager, debe tener disponible información específica acerca de su entorno. Puede registrar la información en la hoja de cálculo.

Información de instalación de Unified Manager

Los detalles necesarios para instalar Unified Manager.

Sistema en el que se ha puesto en marcha el software	Su valor
Nombre de dominio completo del host	

Sistema en el que se ha puesto en marcha el software	Su valor
Dirección IP del host	
Máscara de red	
Dirección IP de la pasarela	
Dirección DNS principal	
Dirección DNS secundaria	
Buscar dominios	
Nombre de usuario de mantenimiento	
Contraseña de usuario de mantenimiento	

Información de configuración de Unified Manager

Los detalles para configurar Unified Manager después de la instalación. Algunos valores son opcionales según la configuración.

Ajuste	Su valor
Dirección de correo electrónico del usuario de mantenimiento	
Nombre de host o dirección IP del servidor SMTP	
Nombre de usuario SMTP	
Contraseña SMTP	
Puerto SMTP	25 (valor predeterminado)
Correo electrónico desde el cual se envían notificaciones de alerta	
Nombre de host o dirección IP del servidor de autenticación	
El nombre de administrador de Active Directory o el nombre distintivo de enlace LDAP	

Ajuste	Su valor
Contraseña de Active Directory o contraseña de enlace LDAP	
Nombre distintivo de la base del servidor de autenticación	
URL del proveedor de identidades (IDP)	
Metadatos del proveedor de identidades (IDP)	
Direcciones IP del host de destino de capturas SNMP	
Puerto SNMP	

Información del clúster

Los detalles sobre los sistemas de almacenamiento que gestiona mediante Unified Manager.

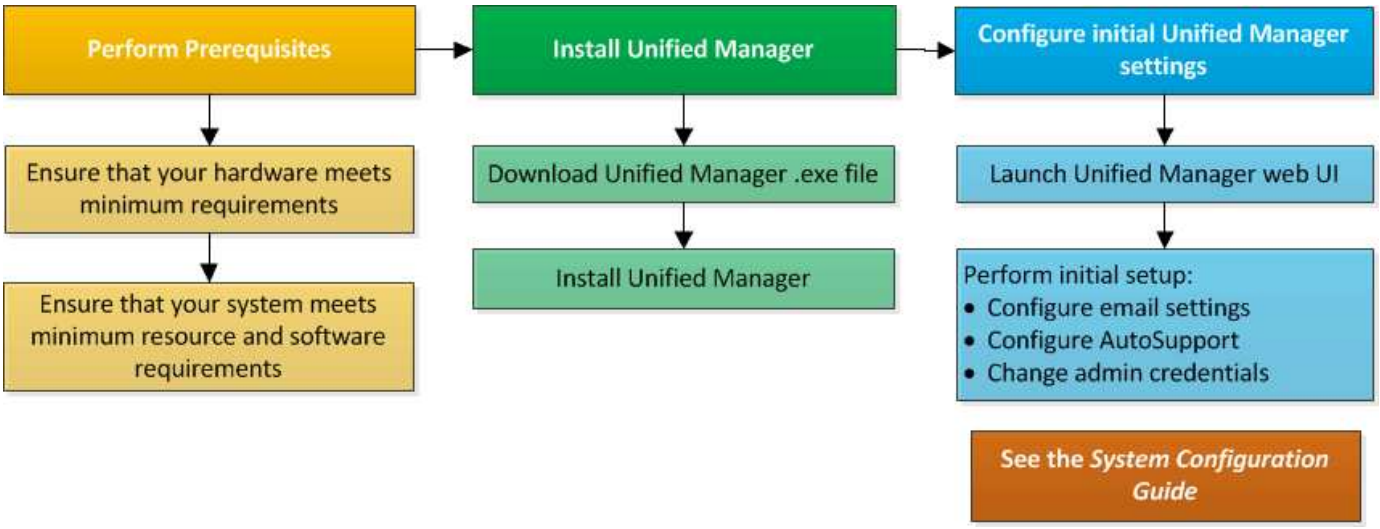
Clúster 1 de N	Su valor
El nombre de host o la dirección IP de administración del clúster	
Nombre de usuario del administrador ONTAP Al administrador se le debe haber asignado la función «admin».	
Contraseña del administrador de ONTAP	
Protocolo	HTTPS

Instalación, actualización y eliminación del software Unified Manager

Puede instalar Unified Manager, actualizar a una versión más reciente o quitar la aplicación Unified Manager.

Descripción general del proceso de instalación

El flujo de trabajo de instalación describe las tareas que deben realizarse para poder usar Unified Manager.



Instalación de Unified Manager en Windows

Es importante comprender la secuencia de pasos para descargar e instalar Unified Manager en Windows.

Instalación de Unified Manager

Puede instalar Unified Manager para supervisar y solucionar problemas de capacidad de almacenamiento de datos, disponibilidad, rendimiento y protección.

Lo que necesitará

- El sistema en el que planea instalar Unified Manager debe cumplir con los requisitos del sistema y del software.

  Consulte "Requisitos del sistema de hardware".

  Consulte "Requisitos de instalación y software de Windows".

  > A partir de Unified Manager 9.5, OpenJDK se proporciona en el paquete de instalación y se instala automáticamente. Oracle Java no es compatible a partir de Unified Manager 9.5.

- Debe tener privilegios de administrador de Windows. Asegúrese de que su nombre de usuario no comience con un signo de exclamación "`"!". Installation of Unified Manager might fail if the user name of user running the installation begins with "!"`.
- Debe tener un navegador web compatible.
- La contraseña de usuario de mantenimiento de Unified Manager debe tener entre 8 y 20 caracteres, debe contener letras mayúsculas o minúsculas, números y caracteres especiales.
- No se permiten los siguientes caracteres especiales en la cadena de contraseña para el usuario de mantenimiento o para el usuario raíz de MySQL: " ' ' % , = & < > | # \ / ( ) [ ] ;:

  Se permiten los siguientes caracteres especiales: ~ ! @ # $ * - ? . + { }

Pasos

1. Inicie sesión en Windows con la cuenta de administrador local predeterminada.
2. Inicie sesión en el sitio de soporte de NetApp y desplácese hasta la página de descarga de Unified Manager:

   "Sitio de soporte de NetApp"

3. Seleccione la versión requerida de Unified Manager y acepte el contrato de licencia para usuarios finales (CLUF).
4. Descargue el archivo de instalación de Unified Manager Windows en un directorio de destino en el sistema Windows.
5. Vaya al directorio donde se encuentra el archivo de instalación.
6. Haga clic con el botón derecho en y ejecute el archivo ejecutable (.exe) del instalador de Unified Manager como administrador.

   Unified Manager detecta los paquetes de terceros que faltan o están instalados previamente y los enumera. Si no se instalan los paquetes de terceros necesarios en el sistema, Unified Manager los instala como parte de la instalación.

7. Haga clic en **Siguiente**.
8. Introduzca el nombre de usuario y la contraseña para crear el usuario de mantenimiento.
9. En el asistente Database Connection, introduzca la contraseña raíz de MySQL.
10. Haga clic en **Cambiar** para especificar una nueva ubicación para el directorio de instalación de Unified Manager y el directorio de datos MySQL.

    Si no cambia el directorio de instalación, se instala Unified Manager en el directorio de instalación predeterminado.

11. Haga clic en **Siguiente**.
12. En el asistente Ready to Install Shield, haga clic en **instalar**.
13. Una vez finalizada la instalación, haga clic en **Finalizar**.
14. Si tiene instalado un software antivirus activo en el sistema Windows, excluya manualmente las siguientes rutas del análisis antivirus una vez completada la instalación:
    - Directorio de datos de Unified Manager
    - Directorio de instalación de Unified Manager
    - Directorio de datos de MySQL

La instalación crea varios directorios:

- Directorio de instalación

  Este es el directorio raíz de Unified Manager, que ha especificado durante la instalación. Ejemplo: `C:\Program Files\NetApp\`

- Directorio de datos de MySQL

  Este es el directorio en el que se almacenan las bases de datos de MySQL, que ha especificado durante la instalación. Ejemplo: `C:\ProgramData\MySQL\MySQLServerData\`

- Directorio Java

Este es el directorio en el que está instalado OpenJDK. Ejemplo: `C:\Program Files\NetApp\JDK\`

- Directorio de datos de aplicaciones de Unified Manager (appDataDir)

  Este es el directorio en el que se almacenan todos los datos generados por la aplicación. Esto incluye registros, paquetes de soporte, backup y todos los demás datos adicionales. Ejemplo: `C:\ProgramData\NetApp\OnCommandAppData\`

Puede acceder a la interfaz de usuario web de para realizar la configuración inicial de Unified Manager, como se describe en "Configurando Active IQ Unified Manager".

Realizar una instalación desatendida de Unified Manager

Puede instalar Unified Manager sin intervención del usuario mediante la interfaz de línea de comandos. Puede completar la instalación desatendida pasando los parámetros en pares clave-valor.

Pasos

1. Inicie sesión en la interfaz de línea de comandos de Windows mediante la cuenta de administrador local predeterminada.
2. Desplácese hasta la ubicación en la que desee instalar Unified Manager y elija una de las siguientes opciones:

Opción	Instrucciones

Si los paquetes de terceros están preinstalados	`ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR=\"Installation directory\" MYSQL_DATA_DIR=\"MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_password MAINTENANCE_USERNAME=maintenance_username /qn /l*v CompletePathForLogFile"`
	
	Ejemplo:
	
	`ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR=\"C:\Program Files\NetApp\" MYSQL_DATA_DIR=\"C:\ProgramData\MYSQL\MySQLServer\" MAINTENANCE_PASSWORD=* MAINTENANCE_USERNAME=admin /qn /l*v C:\install.log"`

Opción	Instrucciones

Si no se instalan paquetes de terceros	`ActiveIQUnifiedManager-x.y.exe /V"MYSQL_PASSWORD=mysql_password INSTALLDIR=\"Installation directory\" MYSQL_DATA_DIR=\"MySQL data directory\" MAINTENANCE_PASSWORD=maintenance_password MAINTENANCE_USERNAME=maintenance_username /qr /l*v CompletePathForLogFile"`
	
	Ejemplo:
	
	`ActiveIQUnifiedManager.exe /s /v"MYSQL_PASSWORD=netapp21! INSTALLDIR=\"C:\Program Files\NetApp\" MYSQL_DATA_DIR=\"C:\ProgramData\MYSQL\MySQLServer\" MAINTENANCE_PASSWORD=* MAINTENANCE_USERNAME=admin /qr /l*v C:\install.log"`

La `/qr` la opción permite el modo silencioso con una interfaz de usuario reducida. Se muestra una interfaz de usuario básica, donde se muestra el progreso de la instalación. No se le solicitan entradas. Si los paquetes de terceros, como JRE, MySQL y 7zip, no están preinstalados, debe usar el `/qr` opción. La instalación da error si el `/qn` la opción se utiliza en un servidor en el que no se instalan paquetes de terceros.

La `/qn` la opción permite el modo silencioso sin interfaz de usuario. Durante la instalación no se muestra ninguna interfaz de usuario ni detalles. No debe utilizar el `/qn` opción cuando no se instalan paquetes de terceros.

3. Inicie sesión en la interfaz de usuario web de Unified Manager mediante la siguiente URL:

   `https://IP address`

Cambio de la contraseña de JBoss

Puede restablecer la contraseña de JBoss específica de la instancia que se haya establecido durante la instalación. Es posible restablecer la contraseña de manera opcional; en caso de que el sitio requiera esta funcionalidad de seguridad para anular la configuración de instalación de Unified Manager. Esta operación también cambia la contraseña que JBoss utiliza para acceder a MySQL.

Lo que necesitará

- Debe tener privilegios de administrador de Windows en el sistema en el que está instalado Unified Manager.
- Debe tener la contraseña del usuario raíz de MySQL.
- Debe poder acceder a todo lo que proporciona NetApp `password.bat` script en el directorio

`C:\Program Files\NetApp\essentials\bin`.

Pasos

1. Inicie sesión como usuario administrador en la máquina host de Unified Manager.
2. Utilice la consola de servicios de Windows para detener los siguientes servicios de Unified Manager:
   - Servicio de adquisición de NetApp Active IQ (OCIE-au)
   - Servicio de servidores de gestión de Active IQ de NetApp (Oncommandsvc)
3. Inicie el `password.bat` secuencia de comandos para iniciar el proceso de cambio de contraseña:

   ```
   C:\Program Files\NetApp\essentials\bin> password.bat resetJBossPassword
   ```

4. Cuando se le solicite, introduzca la contraseña de usuario raíz de MySQL.
5. Cuando se le solicite, introduzca la nueva contraseña de usuario de JBoss y, a continuación, vuelva a introducirla para confirmarla.

   Tenga en cuenta que la contraseña debe tener entre 8 y 16 caracteres, y debe contener al menos un dígito, mayúsculas y minúsculas caracteres, y al menos uno de estos caracteres especiales:

   ```
   !@%^*-_=[]:<>.?/~+
   ```

6. Una vez finalizado el script, inicie los servicios de Unified Manager mediante la consola de Windows Services:
   - Servicio de servidores de gestión de Active IQ de NetApp (Oncommandsvc)
   - Servicio de adquisición de NetApp Active IQ (OCIE-au)
7. Después de iniciar todos los servicios, puede iniciar sesión en la interfaz de usuario de Unified Manager.

La ruta de actualización compatible con las versiones de Unified Manager

Active IQ Unified Manager admite una ruta de actualización específica para cada versión.

No todas las versiones de Unified Manager pueden realizar una actualización sin movimiento a versiones posteriores. Las actualizaciones de Unified Manager se limitan a un modelo N-2, lo que significa que la actualización solo se puede realizar en las próximas dos versiones de todas las plataformas. Por ejemplo, puede realizar una actualización a Unified Manager 9.12 solo desde Unified Manager 9.10 y 9.11.

Si ejecuta una versión anterior a las versiones compatibles, primero deberá actualizar la instancia de Unified Manager con una de las versiones compatibles y, a continuación, actualizarla a la versión actual.

Por ejemplo, si la versión instalada es OnCommand Unified Manager 9.5 y desea actualizar a la versión más reciente de Active IQ Unified Manager 9.12, siga una secuencia de actualizaciones.

Ruta de actualización de ejemplo:

1. Actualice Unified Manager 9.5 de OnCommand → Active IQ Unified Manager 9.7.
2. Actualización 9.7 → 9.9.
3. Actualización 9.9 → 9.11.
4. Actualización 9.11 → 9.12.

Para obtener más información acerca de la matriz de rutas de actualización, consulte este tema "Artículo de la

base de conocimientos (KB)".

Actualizar Unified Manager

Puede actualizar Unified Manager 9.10 o 9.11 a 9.12 descargando y ejecutando el archivo de instalación en la plataforma Windows.

Lo que necesitará

- El sistema donde se actualiza Unified Manager debe cumplir con los requisitos del sistema y del software.

  Consulte "Requisitos del sistema de hardware".

  Consulte "Requisitos de instalación y software de Windows".

  A partir de Unified Manager 9.5, OpenJDK se proporciona en el paquete de instalación y se instala automáticamente. Oracle Java no es compatible a partir de Unified Manager 9.5.

  Asegúrese de que Microsoft .NET 4.5.2 o superior esté instalado en el sistema antes de iniciar la actualización.

- MySQL Community Edition se actualiza automáticamente durante la actualización de Unified Manager. Si la versión instalada de MySQL en el sistema es anterior a 8.0.30, el proceso de actualización de Unified Manager actualiza automáticamente MySQL a 8.0.30. No debe ejecutar una actualización independiente de una versión anterior de MySQL a la versión 8.0.30.
- Debe tener privilegios de administrador de Windows. Asegúrese de que su nombre de usuario no comience con un signo de exclamación "`!`". `Installation of Unified Manager might fail if the user name of user running the installation begins with "!`".
- Debe tener credenciales válidas para iniciar sesión en el sitio de soporte de NetApp.
- Para evitar la pérdida de datos, debe haber creado un backup de la máquina de Unified Manager en caso de que haya un problema durante la actualización.
- Debe tener suficiente espacio en disco disponible para realizar la actualización.

  El espacio disponible en la unidad de instalación debe ser 2.5 GB mayor que el tamaño del directorio de datos. La actualización se detiene y muestra un mensaje de error que indica la cantidad de espacio que debe añadirse si no hay suficiente espacio libre.

- Durante la actualización, es posible que se le solicite que confirme si desea mantener la configuración predeterminada anterior para conservar los datos de rendimiento durante 13 meses o si desea cambiarla a 6 meses. Al confirmar, se depuran los datos de rendimiento históricos después de 6 meses.
- Antes de realizar la actualización, debe cerrar cualquier archivo o carpeta abiertos en *<InstallDir>\JDK* y *MySQL Data Directory*.
- Si tiene un software antivirus activo instalado en el sistema Windows, es posible que se produzca un error en la actualización de Unified Manager. Debe deshabilitar todo el software de análisis de virus en el sistema antes de actualizar Unified Manager.

Durante el proceso de actualización, Unified Manager no está disponible. Debe completar todas las operaciones en ejecución antes de actualizar Unified Manager.

Si Unified Manager se empareja con una instancia de OnCommand Workflow Automation y hay nuevas

versiones del software disponibles para ambos productos, debe desconectar los productos y, a continuación, configurar una nueva conexión de Workflow Automation tras las actualizaciones. Si solo actualiza uno de los productos, deberá iniciar sesión en Workflow Automation tras la actualización y comprobar que aún se recopilen datos de Unified Manager.

Pasos

1. Inicie sesión en el sitio de soporte de NetApp y desplácese hasta la página de descarga de Unified Manager:

   "Sitio de soporte de NetApp".

2. Seleccione la versión requerida de Unified Manager y acepte el contrato de licencia para usuarios finales (CLUF).
3. Descargue el archivo de instalación de Unified Manager Windows en un directorio de destino en el sistema Windows.
4. Haga clic con el botón derecho en y ejecute el archivo ejecutable (.exe) del instalador de Unified Manager como administrador.

   Unified Manager le solicita el siguiente mensaje:

   ```
   This setup will perform an upgrade of Unified Manager. Do you want to
   continue?
   ```

5. Haga clic en **Sí** y, a continuación, haga clic en **Siguiente**.
6. Introduzca la contraseña de root MySQL8 que se estableció durante la instalación y, a continuación, haga clic en **Siguiente**.
7. Inicie la interfaz de usuario web en una nueva ventana en un explorador web compatible e inicie sesión para utilizar la versión actualizada de Unified Manager.
8. Si tiene instalado un software antivirus activo en el sistema Windows, asegúrese de excluir manualmente las siguientes rutas del análisis antivirus una vez completada la actualización:
   - Directorio de datos de Unified Manager
   - Directorio de instalación de Unified Manager
   - Directorio de datos de MySQL

> Para realizar una actualización silenciosa de Unified Manager, ejecute el siguiente comando: `ActiveIQUnifiedManager-<version\>.exe /s /v"MYSQL_PASSWORD=<password> /qn /l*v <system_drive>:\install.log"`

Actualizar productos de terceros

Puede actualizar productos de terceros, como JRE, en Unified Manager cuando está instalado en sistemas de Windows.

Las empresas que desarrollan estos productos de terceros notifican periódicamente vulnerabilidades de seguridad. Puede actualizar a versiones más recientes de este software según su propio horario.

Actualización de OpenJDK

Puede realizar una actualización a una versión más reciente de OpenJDK en el servidor Windows en el que está instalado Unified Manager para obtener correcciones de vulnerabilidades de seguridad.

Lo que necesitará

Debe tener privilegios de administrador de Windows en el sistema en el que está instalado Unified Manager.

Puede actualizar versiones de OpenJDK dentro de las familias de versiones. Por ejemplo, puede actualizar de OpenJDK 11.0.14 a OpenJDK 11.0.16, pero no puede actualizar directamente de OpenJDK 11 a OpenJDK 12.

Pasos

1. Inicie sesión como usuario administrador en la máquina host de Unified Manager.
2. Descargue la versión adecuada de OpenJDK (64 bits) del sitio OpenJDK en el sistema de destino.

   Por ejemplo, descargar `openjdk-11_windows-x64_bin.zip from` http://jdk.java.net/11/.
3. Utilice la consola de servicios de Windows para detener los siguientes servicios de Unified Manager:
   - Servicio de adquisición de NetApp Active IQ (OCIE-au)
   - Servicio de servidores de gestión de Active IQ de NetApp (Oncommandsvc)
4. Expanda el `zip` archivo.
5. Copie los directorios y archivos del resultado `jdk` directorio (por ejemplo, `jdk-11.0.16` A la ubicación donde está instalado Java. Ejemplo: `C:\Program Files\NetApp\JDK\`
6. Inicie los servicios de Unified Manager mediante la consola de servicios de Windows:
   - Servicio de servidores de gestión de Active IQ de NetApp (Oncommandsvc)
   - Servicio de adquisición de NetApp Active IQ (OCIE-au)

Reiniciar Unified Manager

Es posible que tenga que reiniciar Unified Manager después de realizar cambios de configuración.

Lo que necesitará

Debe tener privilegios de administrador de Windows.

Pasos

1. Inicie sesión en Windows con la cuenta de administrador local predeterminada.
2. Detenga los servicios de Unified Manager:

Del…	Detener los servicios en el siguiente orden…
Línea de comandos	a. `sc stop ocie-au` b. `sc stop Oncommandsvc`

Del…	Detener los servicios en el siguiente orden…
Service Manager de Microsoft	a. Servicio de adquisición de NetApp Active IQ (OCIE-au) b. Servicio de servidores de gestión de Active IQ de NetApp (Oncommandsvc)

3. Inicie los servicios de Unified Manager:

Del…	Iniciar los servicios en el siguiente orden…
Línea de comandos	a. `sc start Oncommandsvc` b. `sc start ocie-au`
Service Manager de Microsoft	a. Servicio de servidores de gestión de Active IQ de NetApp (Oncommandsvc) b. Servicio de adquisición de NetApp Active IQ (OCIE-au)

Desinstale Unified Manager

Puede desinstalar Unified Manager mediante el asistente de programas y características o realizando una desinstalación desatendida desde la interfaz de línea de comandos.

Lo que necesitará

- Debe tener privilegios de administrador de Windows.
- Todos los clústeres (orígenes de datos) deben eliminarse del servidor de Unified Manager antes de desinstalar el software.
- Debe eliminar manualmente las reglas de firewall que se crean para permitir o bloquear el puerto MySQL 3306. Las reglas de firewall no se eliminan automáticamente.

Pasos

1. Desinstale Unified Manager seleccionando una de las siguientes opciones:
   - Si desinstala Unified Manager del asistente **programas y características**, siga estos pasos:
     i. Vaya a **Panel de control** > **Programa y funciones**.
     ii. Seleccione Active IQ Unified Manager y haga clic en **Desinstalar**.
   - Si desinstala Unified Manager de la línea de comandos, siga estos pasos:
     i. Inicie sesión en la línea de comandos de Windows con privilegios de administrador.
     ii. Desplácese hasta el directorio Active IQ Unified Manager y ejecute el siguiente comando:

```
msiexec /x {A78760DB-7EC0-4305-97DB-E4A89CDFF4E1} /qn /l*v
%systemdrive%\UmUnInstall.log
```

Si el Control de cuentas de usuario (UAC) está activado en el servidor y ha iniciado sesión como

usuario de dominio, debe utilizar el método de desinstalación de la línea de comandos.

Unified Manager se desinstala del sistema.

2. Desinstale los siguientes paquetes y datos de terceros que no se quitan durante la desinstalación de Unified Manager:
   - Paquetes de terceros: JRE, MySQL, Microsoft Visual C++ 2015 redistribuible, Python, y 7zip
   - Datos de aplicaciones MySQL generados por Unified Manager
   - Registros de aplicaciones y contenido del directorio de datos de aplicaciones

Realizar tareas administrativas y de configuración

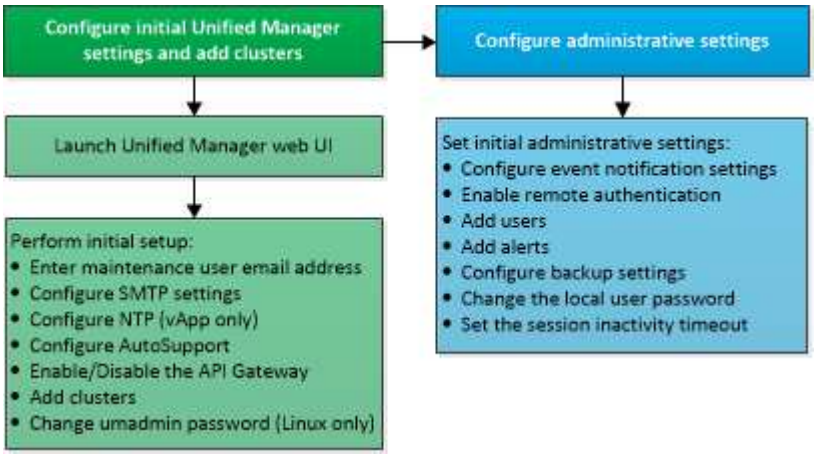
Configurando Active IQ Unified Manager

Después de instalar Active IQ Unified Manager (anteriormente Unified Manager de OnCommand), debe completar la configuración inicial (también llamada el primer asistente de experiencia) para acceder a la interfaz de usuario web de. Después, puede realizar otras tareas de configuración, como añadir clústeres, configurar la autenticación remota, añadir usuarios y añadir alertas.

Algunos de los procedimientos descritos en este manual son necesarios para completar la configuración inicial de su instancia de Unified Manager. Otros procedimientos son los ajustes de configuración recomendados que son útiles para configurar en la nueva instancia, o que son buenos saber acerca de antes de iniciar la supervisión regular de los sistemas ONTAP.

Descripción general de la secuencia de configuración

En el flujo de trabajo de configuración, se describen las tareas que deben realizarse para poder usar Unified Manager.



Acceder a la interfaz de usuario web de Unified Manager

Después de instalar Unified Manager, puede acceder a la interfaz de usuario web de para configurar Unified Manager de modo que pueda comenzar a supervisar los sistemas de ONTAP.

Lo que necesitará

- Si es la primera vez que accede a la interfaz de usuario web, debe iniciar sesión como el usuario de mantenimiento (o usuario umadmin para instalaciones de Linux).
- Si piensa permitir a los usuarios acceder a Unified Manager mediante el nombre corto en lugar de usar el nombre de dominio completo (FQDN) o la dirección IP, la configuración de red debe resolver este nombre corto con un FQDN válido.

- Si el servidor utiliza un certificado digital autofirmado, es posible que el explorador muestre una advertencia que indica que el certificado no es de confianza. Puede reconocer el riesgo de continuar con el acceso o instalar un certificado digital firmado por una entidad de certificación (CA) para la autenticación del servidor.

Pasos

1. Inicie la interfaz de usuario web de Unified Manager desde el explorador mediante la URL que se muestra al final de la instalación. La URL es la dirección IP o el nombre de dominio completo (FQDN) del servidor de Unified Manager.

   El enlace tiene el siguiente formato: `https://URL`.

2. Inicie sesión en la interfaz de usuario web de Unified Manager con sus credenciales de usuario de mantenimiento.

> Si se realizan tres intentos consecutivos para iniciar sesión en la interfaz de usuario web en una hora, se bloqueará fuera del sistema y deberá ponerse en contacto con el administrador del sistema. Esto es aplicable únicamente para usuarios locales.

Realizando la configuración inicial de la interfaz de usuario web de Unified Manager

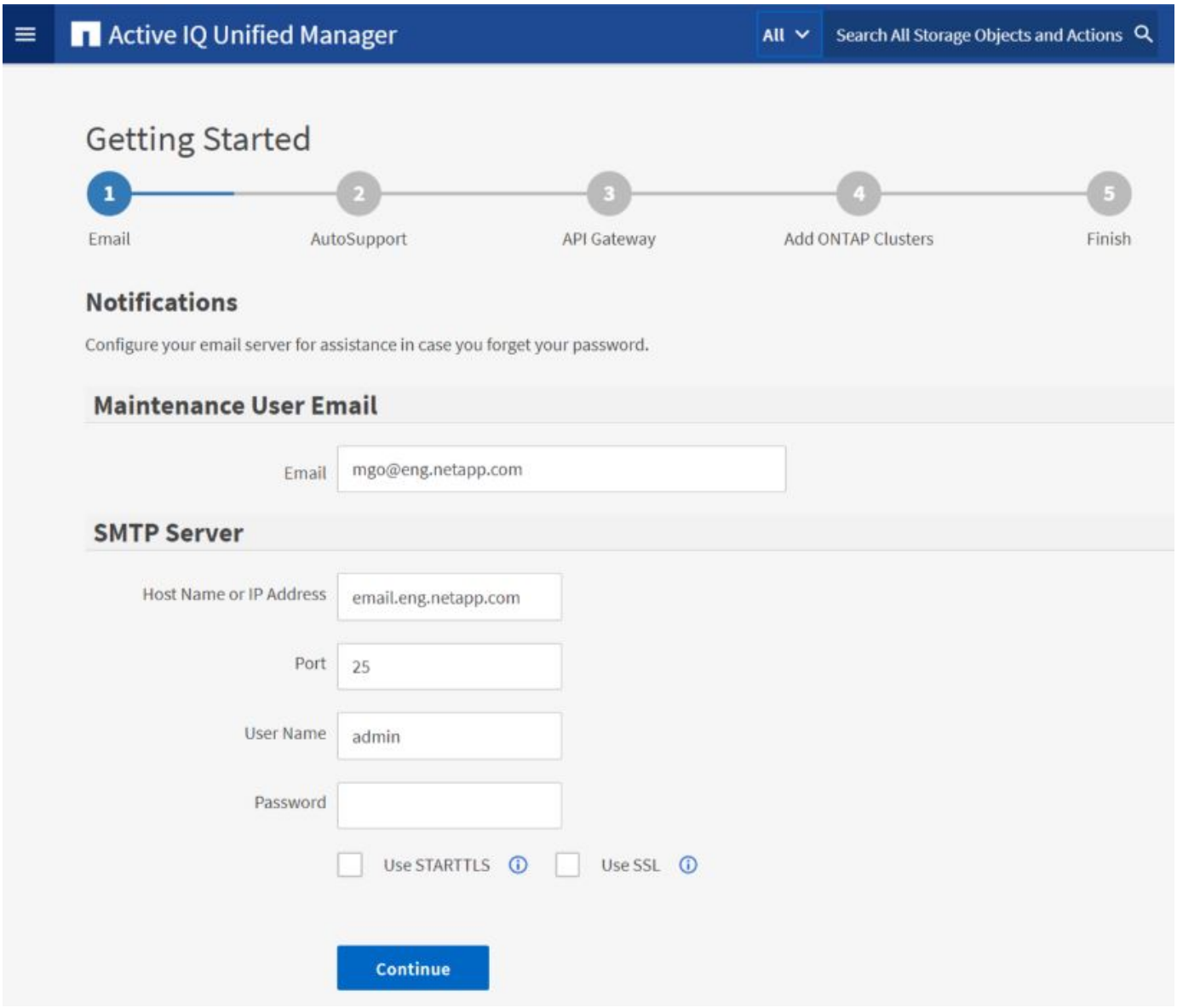
Para utilizar Unified Manager, primero es necesario configurar las opciones de configuración iniciales, incluido el servidor NTP, la dirección de correo electrónico del usuario de mantenimiento, el host del servidor SMTP y añadir clústeres de ONTAP.

Lo que necesitará

Debe haber realizado las siguientes operaciones:

- Inició la interfaz de usuario web de Unified Manager mediante la URL proporcionada después de la instalación
- Inició sesión con el nombre de usuario y la contraseña de mantenimiento (usuario umadmin para instalaciones Linux) creados durante la instalación

La página Active IQ Unified Manager Getting Started aparece solo cuando se accede por primera vez a la interfaz de usuario web. La siguiente página procede de una instalación en VMware.



Si desea cambiar alguna de estas opciones más adelante, puede seleccionar su opción en las opciones General del panel de navegación izquierdo de Unified Manager. Tenga en cuenta que la configuración de NTP es solo para instalaciones de VMware y se puede cambiar más adelante con la consola de mantenimiento de Unified Manager.

Pasos

1. En la página Active IQ Unified Manager Initial Setup, introduzca la dirección de correo electrónico de usuario de mantenimiento, el nombre de host del servidor SMTP y todas las opciones adicionales SMTP, y el servidor NTP (solo instalaciones VMware). A continuación, haga clic en **continuar**.

   Si ha seleccionado la opción **usar STARTTLS** o **usar SSL**, aparecerá una página de certificado después de hacer clic en el botón **continuar**. Compruebe los detalles del certificado y acepte el certificado para continuar con la configuración inicial de la interfaz de usuario web.

2. En la página AutoSupport, haga clic en **Acepto y continúe** para activar el envío de mensajes de AutoSupport desde Unified Manager a Active IQ de NetApp.

   Si necesita designar un proxy para proporcionar acceso a Internet con el fin de enviar contenido

AutoSupport, o si desea desactivar AutoSupport, utilice la opción **General** > **AutoSupport** de la interfaz de usuario web.

3. En los sistemas Red Hat y CentOS, cambie la contraseña de usuario umadmin de la cadena "'admin'" predeterminada a una cadena personalizada.
4. En la página Set up API Gateway, seleccione si desea utilizar la función API Gateway que permite a Unified Manager gestionar los clústeres de ONTAP que planea supervisar mediante API de REST de ONTAP. A continuación, haga clic en **continuar**.

   Puede activar o desactivar esta configuración más adelante en la interfaz de usuario web desde **General** > **Configuración de la función** > **puerta de enlace API**. Para obtener más información sobre las API, consulte "Primeros pasos con API de REST de Active IQ Unified Manager".

5. Añada los clústeres que desea que Unified Manager administre y haga clic en **Siguiente**. Para cada clúster que vaya a administrar, debe tener el nombre de host o la dirección IP de administración del clúster (IPv4 o IPv6) junto con las credenciales de nombre de usuario y contraseña; el usuario debe tener el rol «'admin'».

   Este paso es opcional. Puede agregar clústeres más adelante en la interfaz de usuario web desde **Storage Management** > **Cluster Setup**.

6. En la página Summary (Resumen), compruebe que todos los ajustes son correctos y haga clic en **Finish** (Finalizar).

Se cierra la página Getting Started y se muestra la página Unified Manager Dashboard.

Añadir clústeres

Puede añadir un clúster a la Active IQ Unified Manager para poder supervisar el clúster. Esto incluye la capacidad de obtener información del clúster, como el estado, la capacidad, el rendimiento y la configuración del clúster, para poder encontrar y resolver cualquier problema que pueda ocurrir.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe tener la siguiente información:
  - El nombre de host o la dirección IP de administración del clúster

    El nombre de host es el nombre FQDN o el nombre corto que Unified Manager utiliza para conectarse con el clúster. El nombre de host debe resolver a la dirección IP de administración del clúster.

    La dirección IP de administración del clúster debe ser el LIF de gestión del clúster de la máquina virtual de almacenamiento (SVM) administrativa. Si utiliza un LIF de gestión de nodos, la operación da error.

  - El clúster de debe ejecutar el software ONTAP versión 9.1 o posterior.
  - Nombre de usuario y contraseña del administrador de ONTAP

    Esta cuenta debe tener el rol *admin* con acceso a aplicaciones establecido en *ontapi*, *Console* y *http*.

  - El número de puerto para conectarse al clúster mediante el protocolo HTTPS (por lo general, puerto

443)

- Tiene los certificados necesarios. Unified Manager instala certificados de seguridad al añadir un clúster:

  Certificados de servidor: Este certificado es propiedad de Unified Manager. Se genera un certificado SSL (HTTPS) autofirmado predeterminado con una instalación nueva de Unified Manager. NetApp recomienda actualizarlo a certificado firmado por CA para mejorar la seguridad. Si el certificado de servidor caduca, debe volver a regenerarlo y reiniciar Unified Manager para que los servicios incorporen el nuevo certificado. Para obtener más información acerca de la regeneración del certificado SSL, consulte "Generar un certificado de seguridad HTTPS".

  Certificados para la comunicación mutua con TLS: Se utiliza durante la comunicación mutua con TLS entre Unified Manager y ONTAP. La autenticación basada en certificados está habilitada para un clúster de acuerdo con la versión de ONTAP. Si el clúster que ejecuta la versión de ONTAP es inferior a la versión 9.5, la autenticación basada en certificados no está habilitada.

  La autenticación basada en certificados no se habilita automáticamente para un clúster, si va a actualizar una versión anterior de Unified Manager a Unified Manager 9.12. Sin embargo, puede habilitarla mediante la modificación y el guardado de los detalles del clúster. Si el certificado caduca, debe regenerarlo para incorporar el nuevo certificado. Para obtener más información sobre la visualización y regeneración del certificado, consulte "Editar clústeres".

  - La autenticación basada en certificados se habilita automáticamente si se añade un clúster de la interfaz de usuario web de. Si agrega un clúster desde la consola de mantenimiento, la autenticación basada en certificados no está habilitada.
  - Si la autenticación basada en certificados está habilitada para un clúster, y realiza el backup de Unified Manager desde un servidor y la restauración a otro servidor de Unified Manager donde se cambia el nombre de host o la dirección IP, la supervisión del clúster puede fallar. Para evitar el error, edite y guarde los detalles del clúster. Para obtener más información sobre cómo editar detalles del clúster, consulte "Editar clústeres".

  +
  Certificados de cliente: Se utiliza durante la autenticación de mensajes EMS recibidos de ONTAP. Este certificado es propiedad de ONTAP y es obligatorio cuando se añade un clúster de ONTAP a Unified Manager. No puede agregar un clúster a Unified Manager con un certificado caducado y si el certificado de cliente ya ha caducado, debe volver a regenerarlo antes de agregar el clúster. Sin embargo, si este certificado caduca en un clúster que ya se ha añadido y está siendo utilizado por Unified Manager, la mensajería de EMS sigue funcionando con el certificado caducado. Para obtener información acerca de la generación de certificados, consulte el artículo de la base de conocimientos (KB) "Cómo renovar un certificado autofirmado de ONTAP en la interfaz de usuario de System Manager".

- Debe tener espacio suficiente en el servidor de Unified Manager. Se le impide agregar un clúster al servidor cuando ya se consume más del 90% del espacio en el directorio de la base de datos.

Para una configuración de MetroCluster, debe añadir los clústeres local y remoto, y los clústeres deben configurarse correctamente.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Storage Management** > **Cluster Setup**.
2. En la página Cluster Setup, haga clic en **Add**.
3. En el cuadro de diálogo Add Cluster, especifique los valores requeridos, como el nombre de host o la

dirección IP del clúster, el nombre de usuario, la contraseña y el número de puerto.

Es posible cambiar la dirección IP de gestión del clúster de IPv6 a IPv4 o de IPv4 a IPv6. La nueva dirección IP se refleja en la cuadrícula del clúster y en la página de configuración del clúster una vez completado el siguiente ciclo de supervisión.

4. Haga clic en **Enviar**.
5. En el cuadro de diálogo autorizar host, haga clic en **Ver certificado** para ver la información del certificado sobre el clúster.
6. Haga clic en **Sí**.

   En Unified Manager 9.12, después de guardar los detalles del clúster, puede ver el certificado para comunicación mutua TLS para un clúster.

   Si la autenticación basada en certificados no está habilitada, Unified Manager comprueba el certificado solo cuando se añade el clúster inicialmente. Unified Manager no comprueba el certificado para cada llamada API a ONTAP.

Después de detectar todos los objetos de un clúster nuevo, Unified Manager comienza a recopilar datos históricos de rendimiento de los 15 días anteriores. Estas estadísticas se recopilan mediante la funcionalidad de recogida de continuidad de datos. Esta función le proporciona más de dos semanas de información sobre el rendimiento de un clúster inmediatamente después de añadir. Una vez completado el ciclo de recogida de continuidad de datos, se recogen datos de rendimiento del clúster en tiempo real, de forma predeterminada, cada cinco minutos.

Dado que la recogida de 15 días de datos de rendimiento requiere un uso intensivo de la CPU, se sugiere escalonar la adición de nuevos clústeres de manera que las encuestas de recogida de continuidad de datos no se ejecuten en demasiados clústeres al mismo tiempo. Además, si reinicia Unified Manager durante el período de recogida de continuidad de datos, la recogida se detiene y verá vacíos en los gráficos de rendimiento correspondientes al periodo que falta.

Si recibe un mensaje de error que no puede añadir el clúster, compruebe si los relojes de los dos sistemas no están sincronizados y la fecha de inicio del certificado HTTPS de Unified Manager es posterior a la fecha del clúster. Debe asegurarse de que los relojes se sincronicen con NTP o un servicio similar.

Información relacionada

"Instalar una CA firmada y devolvió un certificado HTTPS"

Configuración de Unified Manager para enviar notificaciones de alerta

Puede configurar Unified Manager para que envíe notificaciones que le alertan de los eventos de su entorno. Antes de que las notificaciones se puedan enviar, debe configurar varias otras opciones de Unified Manager.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Después de implementar Unified Manager y completar la configuración inicial, se debe considerar configurar el entorno para activar alertas y generar correos electrónicos de notificación o capturas SNMP en función de la

recepción de eventos.

Pasos

1. "Configure los ajustes de notificación de eventos".

   Si desea que las notificaciones de alerta se envíen cuando ciertos eventos ocurran en el entorno, debe configurar un servidor SMTP y suministrar una dirección de correo electrónico desde la que se enviará la notificación de alerta. Si desea utilizar capturas SNMP, puede seleccionar esa opción y proporcionar la información necesaria.

2. "Habilite la autenticación remota".

   Si desea que los usuarios remotos de LDAP o Active Directory accedan a la instancia de Unified Manager y reciban notificaciones de alerta, debe habilitar la autenticación remota.

3. "Agregue servidores de autenticación".

   Puede agregar servidores de autenticación para que los usuarios remotos dentro del servidor de autenticación puedan acceder a Unified Manager.

4. "Añadir usuarios".

   Puede añadir varios tipos de usuarios locales o remotos y asignar roles específicos. Cuando crea una alerta, asigna un usuario para que reciba las notificaciones de alerta.

5. "Añadir alertas".

   Después de añadir la dirección de correo electrónico para enviar notificaciones, se añadieron usuarios para recibir las notificaciones, configurar los ajustes de red y configurar las opciones SMTP y SNMP necesarias para el entorno, y después puede asignar alertas.

Configuración de los ajustes de notificación de eventos

Es posible configurar Unified Manager para que envíe notificaciones de alerta cuando se genera un evento o cuando se asigna un evento a un usuario. Puede configurar el servidor SMTP que se usa para enviar la alerta y se pueden configurar varios mecanismos de notificación; por ejemplo, las notificaciones de alerta se pueden enviar como correos electrónicos o capturas SNMP.

Lo que necesitará

Debe tener la siguiente información:

- Dirección de correo electrónico desde la cual se envía la notificación de alertas

  La dirección de correo electrónico aparece en el campo «'de'» en las notificaciones de alerta enviadas. Si el correo electrónico no se puede entregar por cualquier motivo, esta dirección de correo electrónico también se utiliza como destinatario para el correo no entregable.

- El nombre de host del servidor SMTP, así como el nombre de usuario y la contraseña para acceder al servidor
- Nombre de host o dirección IP del host de destino de captura que recibirá la captura SNMP, junto con la versión SNMP, el puerto de capturas saliente, la comunidad y otros valores de configuración SNMP

requeridos

Para especificar varios destinos de capturas, separe cada host con una coma. En este caso, todas las demás configuraciones de SNMP, como la versión y el puerto de captura saliente, deben ser las mismas para todos los hosts de la lista.

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Notificaciones**.
2. En la página Notifications, configure los ajustes adecuados.

   Notas:

   - Si la dirección de origen está precargada con la dirección "ActiveIQUnifiedManager@localhost.com", debe cambiarla a una dirección de correo electrónico real y operativa para asegurarse de que todas las notificaciones de correo electrónico se entregan correctamente.
   - Si no se puede resolver el nombre de host del servidor SMTP, puede especificar la dirección IP (IPv4 o IPv6) del servidor SMTP en lugar del nombre de host.
3. Haga clic en **Guardar**.
4. Si ha seleccionado la opción **usar STARTTLS** o **usar SSL**, aparecerá una página de certificado después de hacer clic en el botón **Guardar**. Compruebe los detalles del certificado y acepte el certificado para guardar la configuración de notificación.

   Puede hacer clic en el botón **Ver detalles del certificado** para ver los detalles del certificado. Si el certificado existente ha caducado, desactive la casilla **usar STARTTLS** o **usar SSL**, guarde la configuración de notificación y vuelva a marcar la casilla **usar STARTTLS** o **usar SSL** para ver un nuevo certificado.

Habilitación de la autenticación remota

Puede habilitar la autenticación remota para que el servidor de Unified Manager pueda comunicarse con los servidores de autenticación. Los usuarios del servidor de autenticación pueden acceder a la interfaz gráfica de Unified Manager para gestionar los objetos de almacenamiento y los datos.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

> El servidor de Unified Manager debe estar conectado directamente con el servidor de autenticación. Debe deshabilitar cualquier cliente LDAP local, como SSSD (demonio de servicios de seguridad del sistema) o NSLCD (demonio de almacenamiento en caché LDAP del servicio de nombres).

Puede habilitar la autenticación remota mediante Open LDAP o Active Directory. Si la autenticación remota está deshabilitada, los usuarios remotos no pueden acceder a Unified Manager.

La autenticación remota es compatible con LDAP y LDAPS (LDAP seguro). Unified Manager utiliza 389 como puerto predeterminado para la comunicación no segura y 636 como puerto predeterminado para la comunicación segura.

El certificado que se utiliza para autenticar usuarios debe cumplir el formato X.509.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. Marque la casilla para **Activar autenticación remota…**.
3. En el campo Servicio de autenticación, seleccione el tipo de servicio y configure el servicio de autenticación.

Para tipo de autenticación…	Introduzca la siguiente información…
Active Directory	• Nombre del administrador del servidor de autenticación en uno de los siguientes formatos: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (Usando la notación LDAP adecuada) • Contraseña de administrador • Nombre completo base (con la notación LDAP adecuada)
Abra LDAP	• Enlazar nombre distintivo (en la notación LDAP correspondiente) • Enlazar contraseña • Nombre distintivo de base

Si la autenticación de un usuario de Active Directory tarda mucho tiempo o agota el tiempo de espera, es probable que el servidor de autenticación tarde mucho tiempo en responder. Al deshabilitar la compatibilidad con los grupos anidados en Unified Manager, es posible que se reduzca el tiempo de autenticación.

Si selecciona la opción Use Secure Connection para el servidor de autenticación, Unified Manager se comunica con el servidor de autenticación mediante el protocolo Secure Sockets Layer (SSL).

4. **Opcional:** Agregue servidores de autenticación y pruebe la autenticación.
5. Haga clic en **Guardar**.

Deshabilitar grupos anidados de la autenticación remota

Si tiene habilitada la autenticación remota, puede deshabilitar la autenticación de grupos anidados para que solo los usuarios individuales y no los miembros de grupos se puedan autenticar de forma remota a Unified Manager. Puede deshabilitar los grupos anidados cuando desee mejorar el tiempo de respuesta de autenticación de Active Directory.

Lo que necesitará

- Debe tener la función Administrador de aplicaciones.

- La desactivación de grupos anidados sólo se aplica cuando se utiliza Active Directory.

Al deshabilitar la compatibilidad con los grupos anidados en Unified Manager, es posible que se reduzca el tiempo de autenticación. Si la compatibilidad de grupos anidados está deshabilitada y, si se añade un grupo remoto a Unified Manager, los usuarios individuales deben ser miembros del grupo remoto para autenticarse en Unified Manager.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. Active la casilla de verificación **Desactivar búsqueda de grupo anidada**.
3. Haga clic en **Guardar**.

Configurar servicios de autenticación

Los servicios de autenticación permiten la autenticación de usuarios remotos o grupos remotos en un servidor de autenticación antes de otorgar acceso a Unified Manager. Puede autenticar usuarios utilizando servicios de autenticación predefinidos (como Active Directory u OpenLDAP) o configurando su propio mecanismo de autenticación.

Lo que necesitará

- Debe haber habilitado la autenticación remota.
- Debe tener la función Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. Seleccione uno de los siguientes servicios de autenticación:

Si selecciona…	Realice lo siguiente…
Active Directory	a. Introduzca el nombre y la contraseña del administrador. b. Especifique el nombre completo base del servidor de autenticación. Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, entonces el nombre completo base es **cn=ou,dc=domain,dc=com**.

Si selecciona…	Realice lo siguiente…
OpenLDAP	a. Introduzca el nombre distintivo del enlace y la contraseña de enlace. b. Especifique el nombre completo base del servidor de autenticación. Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, entonces el nombre completo base es **cn=ou,dc=domain,dc=com**.
Otros	a. Introduzca el nombre distintivo del enlace y la contraseña de enlace. b. Especifique el nombre completo base del servidor de autenticación. Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, entonces el nombre completo base es **cn=ou,dc=domain,dc=com**. c. Especifique la versión de protocolo LDAP que admite el servidor de autenticación. d. Introduzca el nombre de usuario, la pertenencia a grupos, el grupo de usuarios y los atributos miembro.

Si desea modificar el servicio de autenticación, debe eliminar todos los servidores de autenticación existentes y, a continuación, agregar nuevos servidores de autenticación.

3. Haga clic en **Guardar**.

Añadiendo servidores de autenticación

Puede añadir servidores de autenticación y habilitar la autenticación remota en el servidor de gestión para que los usuarios remotos dentro del servidor de autenticación puedan acceder a Unified Manager.

Lo que necesitará

- Debe estar disponible la siguiente información:
  - Nombre de host o dirección IP del servidor de autenticación
  - Número de puerto del servidor de autenticación
- Debe haber habilitado la autenticación remota y configurado el servicio de autenticación para que el servidor de administración pueda autenticar usuarios o grupos remotos en el servidor de autenticación.
- Debe tener la función Administrador de aplicaciones.

Si el servidor de autenticación que va a añadir forma parte de un par de alta disponibilidad (ha) (con la misma base de datos), también puede añadir el servidor de autenticación asociado. Esto permite que el servidor de administración se comunique con el asociado cuando no se puede acceder a uno de los servidores de autenticación.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. Activar o desactivar la opción **utilizar conexión segura**:

Si desea…	Realice lo siguiente…
Habilite	a. Seleccione la opción **utilizar conexión segura**. b. En el área servidores de autenticación, haga clic en **Agregar**. c. En el cuadro de diálogo Add Authentication Server, introduzca el nombre o la dirección IP de autenticación (IPv4 o IPv6) del servidor. d. En el cuadro de diálogo autorizar host, haga clic en Ver certificado. e. En el cuadro de diálogo Ver certificado, compruebe la información del certificado y, a continuación, haga clic en **Cerrar**. f. En el cuadro de diálogo autorizar host, haga clic en **Sí**. Al activar la opción **usar autenticación de conexión segura**, Unified Manager se comunica con el servidor de autenticación y muestra el certificado. Unified Manager utiliza 636 como puerto predeterminado para una comunicación segura y el número de puerto 389 para una comunicación no segura.
Deshabilitarla	a. Desactive la opción **utilizar conexión segura**. b. En el área servidores de autenticación, haga clic en **Agregar**. c. En el cuadro de diálogo Add Authentication Server, especifique el nombre de host o la dirección IP (IPv4 o IPv6) del servidor y los detalles del puerto. d. Haga clic en **Agregar**.

El servidor de autenticación que ha agregado se muestra en el área servidores.

3. Realice una autenticación de prueba para confirmar que puede autenticar usuarios en el servidor de autenticación que ha agregado.

Prueba de la configuración de los servidores de autenticación

Puede validar la configuración de los servidores de autenticación para garantizar que el servidor de gestión pueda comunicarse con ellos. Puede validar la configuración buscando un usuario remoto o un grupo remoto desde los servidores de autenticación y autentificándolos con la configuración configurada.

Lo que necesitará

- Usted debe haber habilitado la autenticación remota y configurado el servicio de autenticación para que el servidor de Unified Manager pueda autenticar el usuario remoto o el grupo remoto.
- Debe haber agregado los servidores de autenticación para que el servidor de administración pueda buscar el usuario remoto o el grupo remoto desde estos servidores y autentificarlos.
- Debe tener la función Administrador de aplicaciones.

Si el servicio de autenticación está establecido en Active Directory y si está validando la autenticación de usuarios remotos que pertenecen al grupo principal del servidor de autenticación, la información sobre el grupo principal no se muestra en los resultados de la autenticación.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. Haga clic en **probar autenticación**.
3. En el cuadro de diálogo probar usuario, especifique el nombre de usuario y la contraseña del usuario remoto o el nombre de usuario del grupo remoto y, a continuación, haga clic en **Prueba**.

   Si va a autenticar un grupo remoto, no debe introducir la contraseña.

Adición de alertas

Puede configurar alertas para que le notifiquen un evento determinado. Es posible configurar alertas para un solo recurso, para un grupo de recursos o para eventos de un tipo de gravedad determinado. Puede especificar la frecuencia con la que desea que se le notifique y asociar un script a la alerta.

Lo que necesitará

- Debe haber configurado los ajustes de notificación, como la dirección de correo electrónico de usuario, el servidor SMTP y el host de captura SNMP, con el fin de permitir que el servidor Active IQ Unified Manager utilice estos ajustes para enviar notificaciones a los usuarios cuando se genera un evento.
- Debe conocer los recursos y los eventos sobre los que desea activar la alerta, así como los nombres de usuario o las direcciones de correo electrónico de los usuarios a los que desea notificar.
- Si desea que un script se ejecute según el evento, debe haber añadido el script a Unified Manager mediante la página Scripts.
- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Puede crear una alerta directamente desde la página de detalles Event después de recibir un evento además

de crear una alerta desde la página Alert Setup, tal y como se describe aquí.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de alertas**.
2. En la página Configuración de alertas, haga clic en **Agregar**.
3. En el cuadro de diálogo Agregar alerta, haga clic en **Nombre** e introduzca un nombre y una descripción para la alerta.
4. Haga clic en **Recursos** y seleccione los recursos que se incluirán o excluirán de la alerta.

   Puede establecer un filtro especificando una cadena de texto en el campo **Nombre contiene** para seleccionar un grupo de recursos. Según la cadena de texto que especifique, la lista de recursos disponibles solo muestra los recursos que coinciden con la regla de filtro. La cadena de texto que especifique distingue mayúsculas y minúsculas.

   Si un recurso cumple las reglas de inclusión y exclusión especificadas, la regla de exclusión tiene prioridad sobre la regla de inclusión y no se genera la alerta para los eventos relacionados con el recurso excluido.

5. Haga clic en **Eventos** y seleccione los eventos según el nombre del evento o el tipo de gravedad del evento para el que desea activar una alerta.

   Para seleccionar más de un evento, pulse la tecla Ctrl mientras realiza las selecciones.

6. Haga clic en **acciones** y seleccione los usuarios a los que desea notificar, elija la frecuencia de notificación, elija si se enviará una captura SNMP al receptor de capturas y asigne una secuencia de comandos para que se ejecute cuando se genere una alerta.

   Si modifica la dirección de correo electrónico especificada para el usuario y vuelve a abrir la alerta para su edición, el campo Nombre aparecerá en blanco porque la dirección de correo electrónico modificada ya no está asignada al usuario que se seleccionó previamente. Además, si modificó la dirección de correo electrónico del usuario seleccionado desde la página usuarios, la dirección de correo electrónico modificada no se actualizará para el usuario seleccionado.

   También puede optar por notificar a los usuarios a través de las capturas SNMP.

7. Haga clic en **Guardar**.

Ejemplo de añadir una alerta

Este ejemplo muestra cómo crear una alerta que cumpla con los siguientes requisitos:

- Nombre de alerta: HealthTest
- Recursos: Incluye todos los volúmenes cuyo nombre contenga «'abc'» y excluye todos los volúmenes cuyo nombre contenga «'xyz'».
- Eventos: Incluye todos los eventos críticos de salud
- Acciones: Incluye «sample@domain.com», una secuencia de comandos «'Prueba» y el usuario deberá recibir una notificación cada 15 minutos

Realice los siguientes pasos en el cuadro de diálogo Agregar alerta:

Pasos

1. Haga clic en **Nombre** e introduzca **HealthTest** en el campo **Nombre de alerta**.
2. Haga clic en **Recursos** y, en la ficha incluir, seleccione **volúmenes** en la lista desplegable.
   a. Introduzca **abc** en el campo **Name contains** para mostrar los volúmenes cuyo nombre contenga "'abc'".
   b. Seleccione **<<All Volumes whose name contains 'abc'>>** en el área Recursos disponibles y muévalos al área Recursos seleccionados.
   c. Haga clic en **excluir** e introduzca **xyz** en el campo **Nombre contiene** y, a continuación, haga clic en **Agregar**.
3. Haga clic en **Eventos** y seleccione **críticos** en el campo gravedad del evento.
4. Seleccione **todos los eventos críticos** en el área Eventos coincidentes y muévalos al área Eventos seleccionados.
5. Haga clic en **acciones** e introduzca **sample@domain.com** en el campo Alerta a estos usuarios.
6. Seleccione **Recordar cada 15 minutos** para notificar al usuario cada 15 minutos.

   Puede configurar una alerta para que envíe repetidamente notificaciones a los destinatarios durante un período de tiempo específico. Debe determinar la hora desde la cual está activa la notificación de eventos para la alerta.

7. En el menú Select Script to Execute, seleccione **Test** script.
8. Haga clic en **Guardar**.

Cambiando la contraseña de usuario local

Es posible cambiar la contraseña de inicio de sesión de usuario local para evitar riesgos potenciales para la seguridad.

Lo que necesitará

Debe iniciar sesión como usuario local.

Las contraseñas del usuario de mantenimiento y de los usuarios remotos no se pueden cambiar mediante estos pasos. Para cambiar una contraseña de usuario remoto, póngase en contacto con el administrador de contraseñas. Para cambiar la contraseña de usuario de mantenimiento, consulte "Mediante la consola de mantenimiento".

Pasos

1. Inicie sesión en Unified Manager.
2. En la barra de menús superior, haga clic en el icono de usuario y, a continuación, haga clic en **Cambiar contraseña**.

   La opción **Cambiar contraseña** no se muestra si es un usuario remoto.

3. En el cuadro de diálogo Change Password, introduzca la contraseña actual y la contraseña nueva.
4. Haga clic en **Guardar**.

Si Unified Manager se configura en una configuración de alta disponibilidad, debe cambiar la contraseña en el segundo nodo de la configuración. Ambas instancias deben tener la misma contraseña.

Configurar el tiempo de espera de inactividad de la sesión

Es posible especificar el valor de tiempo de espera de inactividad para Unified Manager a fin de que la sesión se finalice automáticamente después de un cierto periodo de tiempo. De manera predeterminada, el tiempo de espera está configurado en 4,320 minutos (72 horas).

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Esta configuración afecta a todas las sesiones de usuario que han iniciado sesión.

Esta opción no está disponible si tiene habilitada la autenticación del lenguaje de marcado de aserción de seguridad (SAML).

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Configuración de funciones**.
2. En la página **Configuración de característica**, especifique el tiempo de espera de inactividad seleccionando una de las siguientes opciones:

Si desea…	Realice lo siguiente…
No tener tiempo de espera configurado para que la sesión nunca se cierre automáticamente	En el panel **tiempo de espera de inactividad**, mueva el botón deslizante hacia la izquierda (OFF) y haga clic en **aplicar**.
Establezca un número específico de minutos como valor de tiempo de espera	En el panel **tiempo de espera de inactividad**, mueva el botón deslizante hacia la derecha (Activado), especifique el valor de tiempo de espera de inactividad en minutos y haga clic en **aplicar**.

Cambie el nombre de host de Unified Manager

En algún momento, es posible que desee cambiar el nombre de host del sistema en el que instaló Unified Manager. Por ejemplo, quizás desee cambiar el nombre del host para identificar más fácilmente los servidores de Unified Manager por tipo, grupo de trabajo o grupo de clústeres supervisado.

Los pasos necesarios para cambiar el nombre de host varían en función de si Unified Manager se ejecuta en un servidor VMware ESXi, en un servidor Red Hat o CentOS Linux o en un servidor Microsoft Windows.

Cambiar el nombre de host de la aplicación virtual de Unified Manager

El host de red se asigna un nombre cuando se pone en marcha el dispositivo virtual de Unified Manager por primera vez. Es posible cambiar el nombre de host después de la implementación. Si cambia el nombre de host, también debe volver a generar el certificado HTTPS.

Lo que necesitará

Debe iniciar sesión en Unified Manager como usuario de mantenimiento o tener asignado la función de administrador de aplicaciones para realizar estas tareas.

Puede usar el nombre de host (o la dirección IP del host) para acceder a la interfaz de usuario web de Unified Manager. Si configuró una dirección IP estática para la red durante la implementación, debería haber designado un nombre para el host de red. Si configuró la red mediante DHCP, el nombre de host debe tomarse del DNS. Si DHCP o DNS no están configurados correctamente, el nombre de host "'Unified Manager'" se asigna y se asocia automáticamente con el certificado de seguridad.

Independientemente de cómo se asignó el nombre de host, si cambia el nombre de host y piensa usar el nuevo nombre de host para acceder a la interfaz de usuario web de Unified Manager, debe generar un nuevo certificado de seguridad.

Si accede a la interfaz de usuario web mediante la dirección IP del servidor en lugar del nombre de host, no es necesario generar un nuevo certificado si cambia el nombre de host. Sin embargo, se recomienda actualizar el certificado de forma que el nombre de host del certificado coincida con el nombre de host real.

Si cambia el nombre de host en Unified Manager, debe actualizar manualmente el nombre de host en OnCommand Workflow Automation (WFA). El nombre de host no se actualiza automáticamente en WFA.

El nuevo certificado no se aplicará hasta que se reinicie la máquina virtual de Unified Manager.

Pasos

1. Genere un certificado de seguridad HTTPS

   Si desea usar el nuevo nombre de host para acceder a la interfaz de usuario web de Unified Manager, debe volver a generar el certificado HTTPS para asociarlo con el nuevo nombre de host.

2. Reinicie la máquina virtual de Unified Manager

   Después de volver a generar el certificado HTTPS, debe reiniciar la máquina virtual de Unified Manager.

Generar un certificado de seguridad HTTPS

Cuando se instala Active IQ Unified Manager por primera vez, se instala un certificado HTTPS predeterminado. Es posible generar un nuevo certificado de seguridad HTTPS que reemplace el certificado existente.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Puede haber varios motivos para regenerar el certificado, como si desea tener mejores valores para el nombre distintivo (DN) o si desea un tamaño de clave mayor, o un período de caducidad más largo o si el certificado actual ha caducado.

Si no tiene acceso a la interfaz de usuario web de Unified Manager, puede volver a generar el certificado HTTPS con los mismos valores mediante la consola de mantenimiento. Al regenerar los certificados, puede definir el tamaño de la clave y la duración de validez de la clave. Si utiliza la `Reset Server Certificate` Opción de la consola de mantenimiento, se crea un nuevo certificado HTTPS que es válido durante 397 días. Este certificado tendrá una clave RSA de tamaño 2048 bits.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Certificado HTTPS**.
2. Haga clic en **regenerar certificado HTTPS**.

   Aparece el cuadro de diálogo Regenerate HTTPS Certificate.

3. Seleccione una de las siguientes opciones en función de cómo desee generar el certificado:

Si desea…	Realice lo siguiente…
Regenere el certificado con los valores actuales	Haga clic en la opción **Regenerate usando atributos de certificado actuales**.

Si desea…	Realice lo siguiente…
Genere el certificado con diferentes valores	Haga clic en la opción **Actualizar atributos de certificado actuales**. Los campos Nombre común y nombres alternativos utilizarán los valores del certificado existente si no introduce nuevos valores. El "'Nombre común'" debe ajustarse al FQDN del host. Los demás campos no requieren valores, pero puede introducir valores, por ejemplo, PARA EL CORREO ELECTRÓNICO, LA EMPRESA, EL DEPARTAMENTO, Ciudad, provincia y país si desea que esos valores se rellenen en el certificado. También puede seleccionar EL TAMAÑO de CLAVE disponible (el algoritmo de clave es "'RSA'"). Y PERÍODO DE VALIDEZ. • Los valores permitidos para el tamaño de clave son `2048`, `3072` y.. `4096`. • Los períodos de validez son como mínimo de 1 día a un máximo de 36500 días. Aunque se permita un período de validez de 36500 días, se recomienda que utilice un período de validez de no más de 397 días o 13 meses. Como si selecciona un periodo de validez de más de 397 días y piensa exportar una CSR para este certificado y conseguir que la firme una CA bien conocida, la validez del certificado firmado que la CA le devolvió se reducirá a 397 días. • Puede seleccionar la casilla de verificación “excluir información de identificación local (p. ej., localhost)” si desea quitar la información de identificación local del campo nombres alternativos del certificado. Cuando se selecciona esta casilla de verificación, sólo se utiliza lo que se introduce en el campo nombres alternativos. Cuando se deja en blanco, el certificado resultante no tendrá ningún campo nombres alternativos.

4. Haga clic en **Sí** para regenerar el certificado.
5. Reinicie el servidor de Unified Manager para que el nuevo certificado surta efecto.
6. Compruebe la información del nuevo certificado; para ello, consulte el certificado HTTPS.

Reiniciar la máquina virtual de Unified Manager

Puede reiniciar el equipo virtual desde la consola de mantenimiento de Unified Manager. Debe reiniciar después de generar un nuevo certificado de seguridad o si hay un problema con la máquina virtual.

Lo que necesitará

El dispositivo virtual está encendido.

Ha iniciado sesión en la consola de mantenimiento como usuario de mantenimiento.

También puede reiniciar la máquina virtual desde vSphere mediante la opción **Restart Guest**. Para obtener más información, consulte la documentación de VMware.

Pasos

1. Acceda a la consola de mantenimiento.
2. Seleccione **Configuración del sistema** > **Reiniciar Virtual Machine**.

Cambiar el nombre de host de Unified Manager en sistemas Linux

En algún momento, puede que desee cambiar el nombre de host del equipo Red Hat Enterprise Linux o CentOS en el que ha instalado Unified Manager. Por ejemplo, quizás desee cambiar el nombre del host para identificar más fácilmente los servidores de Unified Manager por tipo, grupo de trabajo o grupo de clústeres supervisado cuando enumere las máquinas Linux.

Lo que necesitará

Debe tener acceso de usuario raíz al sistema Linux en el que está instalado Unified Manager.

Puede usar el nombre de host (o la dirección IP del host) para acceder a la interfaz de usuario web de Unified Manager. Si configuró una dirección IP estática para la red durante la implementación, debería haber designado un nombre para el host de red. Si configuró la red mediante DHCP, el nombre de host debe tomarse del servidor DNS.

Independientemente de cómo se asignó el nombre de host, si cambia el nombre de host y piensa usar el nuevo nombre de host para acceder a la interfaz de usuario web de Unified Manager, debe generar un nuevo certificado de seguridad.

Si accede a la interfaz de usuario web mediante la dirección IP del servidor en lugar del nombre de host, no es necesario generar un nuevo certificado si cambia el nombre de host. Sin embargo, se recomienda actualizar el certificado de forma que el nombre de host del certificado coincida con el nombre de host real. El nuevo certificado no se aplicará hasta que se reinicie el equipo Linux.

Si cambia el nombre de host en Unified Manager, debe actualizar manualmente el nombre de host en OnCommand Workflow Automation (WFA). El nombre de host no se actualiza automáticamente en WFA.

Pasos

1. Inicie sesión como usuario raíz en el sistema Unified Manager que desee modificar.
2. Detenga el software Unified Manager y el software MySQL asociado introduciendo el comando siguiente:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Cambie el nombre de host con Linux `hostnamectl` comando:

   ```
   hostnamectl set-hostname new_FQDN
   ```

   ```
   hostnamectl set-hostname nuhost.corp.widget.com
   ```

4. Regenere el certificado HTTPS para el servidor:

   ```
   /opt/netapp/essentials/bin/cert.sh create
   ```

5. Reinicie el servicio de red:

   ```
   service network restart
   ```

6. Después de reiniciar el servicio, compruebe si el nuevo nombre de host puede hacer ping a sí mismo:

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   Este comando debe devolver la misma dirección IP que se configuró con anterioridad para el nombre de host original.

7. Después de completar y verificar el cambio de nombre de host, reinicie Unified Manager introduciendo el comando siguiente:

   ```
   systemctl start mysqld ocie ocieau
   ```

Habilitar y deshabilitar la gestión del almacenamiento basada en políticas

A partir de Unified Manager 9.7, puede aprovisionar cargas de trabajo de almacenamiento (volúmenes y LUN) en los clústeres de ONTAP y gestionar esas cargas de trabajo en función de los niveles de servicio de rendimiento asignados. Esta funcionalidad es similar a crear cargas de trabajo en ONTAP System Manager y asociar políticas de calidad de servicio, pero cuando se aplica mediante Unified Manager, puede aprovisionar y gestionar cargas de trabajo en todos los clústeres que supervisa la instancia de Unified Manager.

Debe tener la función Administrador de aplicaciones.

Esta opción está habilitada de forma predeterminada, pero puede deshabilitarla si no se desean aprovisionar y gestionar cargas de trabajo mediante Unified Manager.

Cuando está activada, esta opción proporciona muchos elementos nuevos en la interfaz de usuario:

Nuevo contenido	Ubicación
Una página para aprovisionar nuevas cargas de trabajo	Disponible en **tareas comunes** > **aprovisionamiento**
Página para crear políticas de nivel de servicio de rendimiento	Disponible en **Ajustes** > **políticas** > **niveles de servicio de rendimiento**
Página para crear políticas de eficiencia del almacenamiento de rendimiento	Disponible en **Ajustes** > **políticas** > **eficiencia del almacenamiento**
Paneles que describen el rendimiento de su carga de trabajo actual y las IOPS de su carga de trabajo	Disponible en la consola

Consulte la ayuda en línea del producto para obtener más información sobre estas páginas y sobre esta función.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Configuración de funciones**.
2. En la página **Configuración de función**, desactive o habilite la administración del almacenamiento basada en políticas eligiendo una de las siguientes opciones:

Si desea…	Realice lo siguiente…
Desactive la administración del almacenamiento basada en políticas	En el panel **Administración de almacenamiento basada en directivas**, mueva el botón deslizante hacia la izquierda.
Gestión del almacenamiento basada en normativas	En el panel **Administración de almacenamiento basada en directivas**, mueva el botón deslizante hacia la derecha.

Configuración de backup de Unified Manager

Puede configurar la funcionalidad de backup en Unified Manager mediante un conjunto de pasos de configuración que se realizarán en los sistemas host y en la consola de mantenimiento.

Para obtener información acerca de los pasos de configuración, consulte "Gestión de operaciones de backup y restauración".

Gestión de la configuración de funciones

La página Configuración de la función permite habilitar y deshabilitar funciones específicas en Active IQ Unified Manager. Esto incluye la creación y gestión de objetos de almacenamiento basados en políticas, la habilitación de la puerta de enlace de la API y el banner de inicio de sesión, la carga de scripts para gestionar alertas, el

establecimiento de un tiempo de sesión de la interfaz de usuario web basado en el tiempo de inactividad y la deshabilitación de la recepción de eventos de la plataforma de Active IQ.

> La página Configuración de funciones sólo está disponible para usuarios con la función Administrador de aplicaciones.

Para obtener más información acerca de carga de scripts, consulte "Habilitar y deshabilitar la carga de scripts".

Permitir la gestión del almacenamiento basada en políticas

La opción **Gestión de almacenamiento basada en normativas** permite la administración del almacenamiento en función de los objetivos de nivel de servicio (SLO). Esta opción está habilitada de forma predeterminada.

Al activar esta función, puede aprovisionar cargas de trabajo de almacenamiento en los clústeres de ONTAP añadidos a la instancia de Active IQ Unified Manager y gestionar estas cargas de trabajo en función de los niveles de servicio de rendimiento y las políticas de eficiencia del almacenamiento asignados.

Puede activar o desactivar esta función en **General** > **Configuración de funciones** > **Administración de almacenamiento basada en directivas**. Al activar esta función, están disponibles las siguientes páginas para su funcionamiento y supervisión:

- Aprovisionamiento (aprovisionamiento de carga de trabajo de almacenamiento)
- **Políticas** > **niveles de servicio de rendimiento**
- **Políticas** > **eficiencia del almacenamiento**
- Columna Workloads by Performance Service Level en la página Clusters Setup
- Panel de rendimiento de la carga de trabajo en **Dashboard**

Puede utilizar las pantallas para crear niveles de servicio de rendimiento y políticas de eficiencia del almacenamiento, así como para aprovisionar las cargas de trabajo de almacenamiento. También puede supervisar las cargas de trabajo de almacenamiento que cumplen los niveles de servicio de rendimiento asignados, así como las no conformes. El panel IOPS de carga de trabajo y rendimiento de cargas de trabajo también le permite evaluar la capacidad y el rendimiento (IOPS) totales, disponibles y utilizados de los clústeres en todo el centro de datos en función de las cargas de trabajo de almacenamiento que se aprovisionen en ellos.

Después de activar esta función, puede ejecutar las API REST de Unified Manager para realizar algunas de estas funciones desde **barra de menús** > **botón de ayuda** > **Documentación de API** > **proveedor de almacenamiento**. También puede introducir el nombre de host o la dirección IP y la URL para acceder a la página API DE REST en el formato https://<hostname>/docs/api/

Para obtener más información sobre las API, consulte "Primeros pasos con API de REST de Active IQ Unified Manager".

Habilitar API Gateway

La función de puerta de enlace de API permite a Active IQ Unified Manager ser un único plano de control desde el cual puede gestionar varios clústeres de ONTAP sin iniciar

sesión de forma individual.

Puede habilitar esta función en las páginas de configuración que aparecen cuando se inicia sesión por primera vez en Unified Manager. También puede activar o desactivar esta función en **General** > **Configuración de funciones** > **Puerta de enlace API**.

Las API DE REST de Unified Manager son diferentes de las API de REST de ONTAP. No todas las funcionalidades de las API DE REST de ONTAP se pueden obtener usando LAS API DE REST de Unified Manager. Sin embargo, si tiene un requisito empresarial específico de acceso a las API de ONTAP para gestionar funciones específicas que no se exponen a Unified Manager, puede habilitar la función API Gateway y ejecutar las API de ONTAP. La puerta de enlace actúa como proxy para tunear las solicitudes de API manteniendo las solicitudes de encabezado y cuerpo en el mismo formato que en las API de ONTAP. Puede usar sus credenciales de Unified Manager y ejecutar las API específicas para acceder a los clústeres de ONTAP y gestionarlos sin aprobar las credenciales de un clúster individual. Unified Manager se realiza como un único punto de gestión para ejecutar las API en los clústeres de ONTAP gestionados por la instancia de Unified Manager. La respuesta que devuelven las API es la misma que la respuesta que devuelven las respectivas API DE REST de ONTAP ejecutadas directamente desde ONTAP.

Después de activar esta función, puede ejecutar las API REST de Unified Manager desde **barra de menús** > **botón de ayuda** > **Documentación de API** > **categoría de puerta de enlace**. Como alternativa, es posible introducir el nombre de host o la dirección IP y la URL para acceder a la página de API DE REST en formato `https://<hostname>/docs/api/`

Para obtener más información sobre las API, consulte "Primeros pasos con API de REST de Active IQ Unified Manager".

Especificación del tiempo de espera de inactividad

Puede especificar el valor de tiempo de espera de inactividad para Active IQ Unified Manager. Tras una inactividad de la hora especificada, la aplicación se cierra automáticamente. Esta opción está habilitada de forma predeterminada.

Puede desactivar esta función o modificar el tiempo desde **General** > **Configuración de función** > **tiempo de espera de inactividad**. Una vez que active esta función, deberá especificar el límite de tiempo de inactividad (en minutos) en el campo **LOGOUT AFTER**, después de lo cual el sistema cerrará automáticamente la sesión. El valor predeterminado es 4320 minutos (72 horas).

Esta opción no está disponible si tiene habilitada la autenticación del lenguaje de marcado de aserción de seguridad (SAML).

Habilitar los eventos del portal de Active IQ

Puede especificar si desea habilitar o deshabilitar los eventos del portal Active IQ. Este ajuste permite al portal de Active IQ detectar y mostrar eventos adicionales sobre la configuración del sistema, el cableado, etc. Esta opción está habilitada de forma predeterminada.

Al habilitar esta función, Active IQ Unified Manager muestra eventos detectados por el portal Active IQ. Estos eventos se crean ejecutando un conjunto de reglas contra los mensajes de AutoSupport generados desde todos los sistemas de almacenamiento supervisados. Estos eventos son distintos de los demás eventos de Unified Manager e identifican incidentes o riesgos relacionados con la configuración, el cableado, las prácticas recomendadas y los problemas de disponibilidad del sistema.

Puede activar o desactivar esta función en **General** > **Configuración de funciones** > **Eventos del portal Active IQ**. En los sitios sin acceso a la red externa, debe cargar las reglas manualmente desde **Storage Management** > **Event Setup** > **Upload Rules**.

Esta función está habilitada de forma predeterminada. Al deshabilitar esta función, se detienen los eventos de Active IQ no se detectan o se muestran en Unified Manager. Cuando está deshabilitada, al habilitar esta función, Unified Manager puede recibir los eventos de Active IQ en un clúster a una hora predefinida de 00:15 para esa zona horaria del clúster.

Activación y desactivación de la configuración de seguridad para cumplir las normativas

Mediante el botón **Personalizar** del panel **Panel de seguridad** de la página Configuración de características, puede habilitar o deshabilitar los parámetros de seguridad para la supervisión de cumplimiento en Unified Manager.

La configuración que se habilita o se deshabilita en esta página rige el estado de cumplimiento general de los clústeres y las máquinas virtuales de almacenamiento en Unified Manager. Según las selecciones, las columnas correspondientes se pueden ver en la vista **Seguridad: Todos los clústeres** de la página de inventario Clusters y la vista **Seguridad: Todos los equipos virtuales de almacenamiento** de la página de inventario de máquinas virtuales de almacenamiento.

Solo los usuarios con rol de administrador pueden editar esta configuración.

Los criterios de seguridad para los clústeres de ONTAP, las máquinas virtuales de almacenamiento y los volúmenes se evalúan con respecto a las recomendaciones definidas en la "Guía de fortalecimiento de la seguridad para NetApp ONTAP 9". El panel Seguridad de la consola y la página Seguridad muestran el estado de cumplimiento de normativas de seguridad predeterminado de los clústeres, las máquinas virtuales de almacenamiento y los volúmenes. Asimismo, se generan eventos de seguridad y se habilitan las acciones de gestión para los clústeres y las máquinas virtuales de almacenamiento que tienen infracciones de seguridad.

Personalización de los ajustes de seguridad

Para personalizar la configuración para fines de supervisión de cumplimiento según corresponda a su entorno de ONTAP, siga estos pasos:

Pasos

1. Haga clic en **General > Configuración de características > Panel de seguridad > Personalizar**. Aparece la ventana emergente **Personalizar configuración del panel de seguridad**.

   Los parámetros de cumplimiento de normativas de seguridad que se habilitan o deshabilitar pueden afectar directamente a las vistas de seguridad predeterminadas, los informes y los informes programados en las pantallas Clusters and Storage VMs. Si ha cargado un informe de Excel desde estas pantallas antes de modificar los parámetros de seguridad, es posible que los informes de Excel descargados estén defectuosos.

2. Para activar o desactivar la configuración personalizada de los clústeres de ONTAP, seleccione la configuración general necesaria en **clúster**. Para obtener información sobre las opciones para personalizar el cumplimiento de normativas de clústeres, consulte "Categorías de cumplimiento de clusters".
3. Para activar o desactivar la configuración personalizada de los equipos virtuales de almacenamiento, seleccione la configuración general necesaria en **Storage VM**. Para obtener información acerca de las

opciones para personalizar el cumplimiento de normativas de equipos virtuales de almacenamiento, consulte "Categorías de cumplimiento de normativas para máquinas virtuales de almacenamiento".

Personalización de los ajustes de AutoSupport y autenticación

En la sección **Configuración de AutoSupport**, puede especificar si se va a utilizar el transporte HTTPS para enviar mensajes AutoSupport desde ONTAP.

En la sección **Configuración de autenticación**, puede habilitar alertas de Unified Manager que se elevarán para el usuario administrador de ONTAP predeterminado.

Habilitar y deshabilitar la carga de scripts

La capacidad de cargar scripts en Unified Manager y ejecutarlas está habilitada de forma predeterminada. Si la organización no desea permitir esta actividad debido a motivos de seguridad, puede desactivar esta funcionalidad.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Configuración de funciones**.
2. En la página **Configuración de característica**, desactive o habilite la secuencia de comandos eligiendo una de las siguientes opciones:

Si desea…	Realice lo siguiente…
Desactivar scripts	En el panel **carga de secuencia de comandos**, mueva el botón deslizante hacia la izquierda.
Activar scripts	En el panel **carga de secuencia de comandos**, mueva el botón deslizante hacia la derecha.

Adición de un banner de inicio de sesión

Al añadir un banner de inicio de sesión, su organización puede mostrar cualquier información, como, por ejemplo, quién puede acceder al sistema y los términos y condiciones de uso durante el inicio de sesión y el cierre de sesión.

Cualquier usuario, como operadores de almacenamiento o administradores, puede ver la ventana emergente de este banner de inicio de sesión durante el inicio de sesión, el cierre de sesión y el tiempo de espera de la sesión.

Mediante la consola de mantenimiento

Puede utilizar la consola de mantenimiento para configurar los ajustes de red, configurar y gestionar el sistema donde está instalado Unified Manager y realizar otras tareas de

mantenimiento que le ayuden a evitar y solucionar los posibles problemas.

Qué funcionalidad proporciona la consola de mantenimiento

La consola de mantenimiento de Unified Manager permite mantener la configuración en el sistema Unified Manager y realizar los cambios necesarios para evitar que se produzcan problemas.

Según el sistema operativo en el que instaló Unified Manager, la consola de mantenimiento incorpora las siguientes funciones:

- Solucione cualquier problema que pueda haber con su dispositivo virtual, especialmente si la interfaz web de Unified Manager no está disponible
- Actualice a las versiones más recientes de Unified Manager
- Genere paquetes de soporte para su envío al soporte técnico
- Configure los ajustes de red
- Cambie la contraseña del usuario de mantenimiento
- Conéctese a un proveedor de datos externo para enviar estadísticas de rendimiento
- Cambie la recopilación de datos de rendimiento interna
- Restaure las opciones de configuración y base de datos de Unified Manager desde una versión de backup anterior.

Lo que hace el usuario de mantenimiento

El usuario de mantenimiento se crea durante la instalación de Unified Manager en un sistema Red Hat Enterprise Linux o CentOS. El nombre de usuario de mantenimiento es el usuario "'umadmin'". El usuario de mantenimiento tiene la función Administrador de aplicaciones en la interfaz de usuario web, y ese usuario puede crear usuarios posteriores y asignarles roles.

El usuario de mantenimiento, o el usuario umadmin, también puede acceder a la consola de mantenimiento de Unified Manager.

Capacidades de diagnóstico del usuario

El objetivo del acceso de diagnóstico es habilitar el soporte técnico para ayudarle a solucionar problemas, y solo se debe utilizar cuando lo indique el soporte técnico.

El usuario de diagnóstico puede ejecutar comandos de nivel de sistema operativo cuando así lo indique el soporte técnico, con fines de solución de problemas.

Acceso a la consola de mantenimiento

Si la interfaz de usuario de Unified Manager no está en funcionamiento o si necesita ejecutar funciones que no están disponibles en la interfaz de usuario, puede acceder a la consola de mantenimiento para gestionar el sistema de Unified Manager.

Lo que necesitará

Debe haber instalado y configurado Unified Manager.

Tras 15 minutos de inactividad, la consola de mantenimiento cierra la sesión.

Cuando se instala en VMware, si ya ha iniciado sesión como usuario de mantenimiento a través de la consola VMware, no podrá iniciar sesión simultáneamente con Secure Shell.

Paso

1. Siga estos pasos para acceder a la consola de mantenimiento:

En este sistema operativo…	Siga estos pasos…
VMware	a. Mediante Secure Shell, conéctese a la dirección IP o al nombre de dominio completo del dispositivo virtual de Unified Manager. b. Inicie sesión en la consola de mantenimiento con su nombre de usuario y contraseña de mantenimiento.
Linux	a. Mediante Secure Shell, conéctese a la dirección IP o al nombre de dominio completo del sistema Unified Manager. b. Inicie sesión en el sistema con el nombre y la contraseña del usuario de mantenimiento (umadmin). c. Introduzca el comando `maintenance_console` Y pulse Intro.
Windows	a. Inicie sesión en el sistema Unified Manager con credenciales de administrador. b. Inicie PowerShell como administrador de Windows. c. Introduzca el comando `maintenance_console` Y pulse Intro.

Se muestra el menú de la consola de mantenimiento de Unified Manager.

Acceder a la consola de mantenimiento mediante la consola de la máquina virtual de vSphere

Si la interfaz de usuario de Unified Manager no está en funcionamiento o si necesita realizar funciones que no están disponibles en la interfaz de usuario, puede acceder a la consola de mantenimiento para volver a configurar el dispositivo virtual.

Lo que necesitará

- Debe ser el usuario de mantenimiento.
- El dispositivo virtual debe estar encendido para acceder a la consola de mantenimiento.

Pasos

1. En vSphere Client, busque el dispositivo virtual Unified Manager.
2. Haga clic en la ficha **Consola**.
3. Haga clic dentro de la ventana de la consola para iniciar sesión.
4. Inicie sesión en la consola de mantenimiento con su nombre de usuario y contraseña.

   Tras 15 minutos de inactividad, la consola de mantenimiento cierra la sesión.

Menús de la consola de mantenimiento

La consola de mantenimiento consta de distintos menús que permiten mantener y gestionar funciones especiales y ajustes de configuración del servidor de Unified Manager.

Según el sistema operativo en el que instaló Unified Manager, la consola de mantenimiento consta de los siguientes menús:

- Actualización de Unified Manager (solo VMware)
- Configuración de red (solo VMware)
- Configuración del sistema (sólo VMware)
  a. Soporte/Diagnóstico
  b. Restablecer certificado de servidor
  c. Proveedor de datos externos
  d. Restaurar copia de seguridad
  e. Configuración del intervalo de sondeo de rendimiento
  f. Deshabilite la autenticación SAML
  g. Ver/cambiar puertos de aplicación
  h. Depurar configuración de registro
  i. Controlar el acceso al puerto MySQL 3306
  j. Salga

Puede seleccionar el número de la lista para acceder a la opción de menú específica. Por ejemplo, para copia de seguridad y restauración, seleccione *4*.

Menú Configuración de red

El menú Configuración de red le permite administrar los ajustes de red. Debe usar este menú cuando la interfaz de usuario de Unified Manager no esté disponible.

Este menú no está disponible si Unified Manager está instalado en Red Hat Enterprise Linux, CentOS o Microsoft Windows.

Están disponibles las siguientes opciones de menú.

- **Mostrar configuración de dirección IP**

  Muestra la configuración de red actual del dispositivo virtual, incluida la dirección IP, la red, la dirección de retransmisión, la máscara de red, la puerta de enlace, Y servidores DNS.

- **Cambiar la configuración de la dirección IP**

  Permite cambiar cualquier configuración de red del dispositivo virtual, incluidos la dirección IP, la máscara de red, la puerta de enlace o los servidores DNS. Si cambia la configuración de red desde DHCP a la red estática mediante la consola de mantenimiento, no puede editar el nombre de host. Debe seleccionar **commit Changes** para que se realicen los cambios.

- **Mostrar configuración de búsqueda de nombres de dominio**

  Muestra la lista de búsqueda de nombres de dominio utilizada para resolver nombres de host.

- **Cambiar la configuración de búsqueda de nombres de dominio**

  Permite cambiar los nombres de dominio en los que se desea buscar al resolver nombres de host. Debe seleccionar **commit Changes** para que se realicen los cambios.

- **Mostrar rutas estáticas**

  Muestra las rutas de red estáticas actuales.

- **Cambiar rutas estáticas**

  Permite agregar o eliminar rutas de red estáticas. Debe seleccionar **commit Changes** para que se realicen los cambios.

  - **Añadir ruta**

    Permite agregar una ruta estática.

  - **Eliminar ruta**

    Permite eliminar una ruta estática.

  - **Atrás**

    Le lleva de vuelta al **Menú principal**.

  - **Salida**

    Sale de la consola de mantenimiento.

- **Desactivar la interfaz de red**

  Deshabilita las interfaces de red disponibles. Si solo hay disponible una interfaz de red, no puede deshabilitarla. Debe seleccionar **commit Changes** para que se realicen los cambios.

- **Activar interfaz de red**

  Habilita las interfaces de red disponibles. Debe seleccionar **commit Changes** para que se realicen los

cambios.

- **Commit Changes**

  Aplica los cambios realizados en la configuración de red del dispositivo virtual. Debe seleccionar esta opción para promulgar cualquier cambio realizado o no se producirán los cambios.

- **Hacer ping a un Host**

  Hace ping en un host de destino para confirmar cambios en la dirección IP o la configuración DNS.

- **Restaurar valores predeterminados**

  Restablece todos los ajustes a los valores predeterminados de fábrica. Debe seleccionar **commit Changes** para que se realicen los cambios.

- **Atrás**

  Le lleva de vuelta al **Menú principal**.

- **Salida**

  Sale de la consola de mantenimiento.

Menú Configuración del sistema

El menú Configuración del sistema le permite administrar su dispositivo virtual proporcionando diversas opciones, como ver el estado del servidor y reiniciar y apagar la máquina virtual.

Cuando Unified Manager se instala en un sistema Linux o Microsoft Windows, en este menú solo está disponible la opción «'Restaurar desde un backup de Unified Manager'».

Están disponibles las siguientes opciones de menú:

- **Estado del servidor de visualización**

  Muestra el estado actual del servidor. Las opciones de estado incluyen en ejecución o no en ejecución.

  Si el servidor no está en ejecución, es posible que deba ponerse en contacto con el soporte técnico.

- **Reiniciar máquina virtual**

  Reinicia la máquina virtual, deteniendo todos los servicios. Tras reiniciar, la máquina virtual y los servicios se reinician.

- **Apagar máquina virtual**

  Apaga la máquina virtual, deteniendo todos los servicios.

  Solo puede seleccionar esta opción desde la consola de máquinas virtuales.

- **Cambiar contraseña de usuario de <logged in user>**

Cambia la contraseña del usuario que está conectado actualmente, que sólo puede ser el usuario de mantenimiento.

- **Aumentar el tamaño del disco de datos**

  Aumenta el tamaño del disco de datos (disco 3) en la máquina virtual.

- **Aumente el tamaño del disco de intercambio**

  Aumenta el tamaño del disco de intercambio (disco 2) en la máquina virtual.

- **Cambiar zona horaria**

  Cambia la zona horaria a su ubicación.

- **Cambiar servidor NTP**

  Cambia la configuración del servidor NTP, como la dirección IP o el nombre de dominio completo (FQDN).

- **Cambiar el servicio NTP**

  Cambia entre `ntp` y.. `systemd-timesyncd` servicios.

- **Restaurar desde una copia de seguridad de Unified Manager**

  Restaura los ajustes de configuración y base de datos de Unified Manager desde una versión de backup anterior.

- **Restablecer certificado de servidor**

  Restablece el certificado de seguridad del servidor.

- **Cambiar nombre de host**

  Cambia el nombre del host en el que está instalado el dispositivo virtual.

- **Atrás**

  Sale del menú Configuración del sistema y vuelve al menú principal.

- **Salida**

  Sale del menú de la consola de mantenimiento.

Menú de soporte y diagnóstico

El menú Soporte y diagnóstico permite generar un bundle de soporte que puede enviar al soporte técnico para la ayuda de solución de problemas.

Están disponibles las siguientes opciones de menú:

- **Generar paquete de soporte ligero**

  Permite producir un paquete de soporte ligero que contiene sólo 30 días de registros y registros de la base de datos de configuración, lo que excluye datos de rendimiento, archivos de registro de adquisición y

volcado de pila del servidor.

- **Generar paquete de soporte**

  Permite crear un bundle de soporte completo (archivo 7-Zip) que contiene información de diagnóstico en el directorio inicial del usuario de diagnóstico. Si el sistema está conectado a Internet, también puede cargar el paquete de soporte a NetApp.

  El archivo incluye información generada por un mensaje de AutoSupport, el contenido de la base de datos de Unified Manager, los datos detallados sobre las redes internas del servidor de Unified Manager y los registros a nivel detallado que normalmente no se incluyen en los mensajes de AutoSupport o en el paquete de soporte ligero.

Opciones de menú adicionales

Las siguientes opciones de menú le permiten realizar varias tareas administrativas en el servidor de Unified Manager.

Están disponibles las siguientes opciones de menú:

- **Restablecer certificado de servidor**

  Regenera el certificado del servidor HTTPS.

  Puede regenerar el certificado de servidor en la GUI de Unified Manager haciendo clic en **General** > **certificados HTTPS** > **regenerar certificado HTTPS**.

- **Deshabilitar autenticación SAML**

  Deshabilita la autenticación SAML de modo que el proveedor de identidades (IDP) ya no proporcione autenticación de inicio de sesión para los usuarios que acceden a la interfaz gráfica de usuario de Unified Manager. Normalmente, esta opción de consola se usa cuando un problema con la configuración de servidor IDP o SAML impide que los usuarios accedan a la interfaz gráfica de usuario de Unified Manager.

- **Proveedor de datos externos**

  Proporciona opciones para conectar Unified Manager a un proveedor de datos externo. Tras establecer la conexión, los datos de rendimiento se envían a un servidor externo para que los expertos en rendimiento del almacenamiento puedan representar las métricas de rendimiento mediante software de terceros. Se muestran las siguientes opciones:

  - **Configuración del servidor de visualización**--muestra los valores actuales de conexión y configuración para un proveedor de datos externo.
  - **Agregar / Modificar conexión del servidor**--le permite introducir nuevos ajustes de conexión para un proveedor de datos externo, o cambiar la configuración existente.
  - **Modificar la configuración del servidor**--le permite introducir nuevos valores de configuración para un proveedor de datos externo, o cambiar los valores existentes.
  - **Eliminar conexión del servidor**--elimina la conexión a un proveedor de datos externo.

    Una vez eliminada la conexión, Unified Manager pierde su conexión con el servidor externo.

- **Restauración de copia de seguridad**

Para obtener información, consulte los temas en "Gestión de operaciones de backup y restauración".

- **Configuración del intervalo de sondeo de rendimiento**

  Proporciona una opción para configurar la frecuencia con la que Unified Manager recopila datos estadísticos de rendimiento de clústeres. El intervalo de recopilación predeterminado es de 5 minutos.

  Puede cambiar este intervalo a 10 o 15 minutos si descubre que las colecciones de clústeres grandes no se están completando a tiempo.

- **Ver/cambiar puertos de aplicación**

  Proporciona una opción para cambiar los puertos predeterminados que Unified Manager utiliza para los protocolos HTTP y HTTPS, si corresponde a la seguridad. Los puertos predeterminados son 80 para HTTP y 443 para HTTPS.

- **Control del acceso al puerto MySQL 3306**

  Controla el acceso del host al puerto MySQL 3306 predeterminado. Por motivos de seguridad, el acceso a través de este puerto se restringe solo a localhost durante una nueva instalación de Unified Manager en sistemas Linux, Windows y VMware vSphere. Esta opción permite cambiar la visibilidad de este puerto entre los hosts localhost y remotos, es decir, si está habilitado para localhost solo en el entorno, puede hacer que este puerto esté disponible también para hosts remotos. De forma alternativa, cuando se habilita para todos los hosts, puede restringir el acceso de este puerto a localhost únicamente. Si el acceso se habilitó en hosts remotos anteriormente, la configuración se mantiene en un escenario de actualización.

- **Salida**

  Sale del menú de la consola de mantenimiento.

Cambiar la contraseña del usuario de mantenimiento en Windows

Es posible cambiar la contraseña de usuario de mantenimiento de Unified Manager si es necesario.

Pasos

1. En la página de inicio de sesión de la interfaz de usuario web de Unified Manager, haga clic en **Contraseña olvidada**.

   Aparece una página que solicita el nombre del usuario cuya contraseña desea restablecer.

2. Introduzca el nombre de usuario y haga clic en **Enviar**.

   Se envía un correo electrónico con un enlace para restablecer la contraseña a la dirección de correo electrónico definida para ese nombre de usuario.

3. Haga clic en el enlace **restablecer contraseña** del correo electrónico y defina la nueva contraseña.
4. Vuelva a la interfaz de usuario web e inicie sesión en Unified Manager con la nueva contraseña.

Cambiar la contraseña de umadmin en sistemas Linux

Por motivos de seguridad, debe cambiar la contraseña predeterminada del usuario

umadmin de Unified Manager inmediatamente después de completar el proceso de instalación. Si es necesario, puede cambiar la contraseña de nuevo en cualquier momento.

Lo que necesitará

- Unified Manager debe estar instalado en un sistema Red Hat Enterprise Linux o CentOS de Linux.
- Debe tener las credenciales de usuario raíz del sistema Linux en el que está instalado Unified Manager.

Pasos

1. Inicie sesión como usuario raíz en el sistema Linux en el que está ejecutando Unified Manager.
2. Cambiar la contraseña de umadmin:

   ```
   passwd umadmin
   ```

   El sistema le pide que introduzca una nueva contraseña para el usuario umadmin.

Cambiar los puertos Unified Manager utiliza para los protocolos HTTP y HTTPS

Los puertos predeterminados que Unified Manager utiliza para los protocolos HTTP y HTTPS se pueden cambiar después de la instalación si es necesario para la seguridad. Los puertos predeterminados son 80 para HTTP y 443 para HTTPS.

Lo que necesitará

Debe tener un ID de usuario y una contraseña autorizados para iniciar sesión en la consola de mantenimiento del servidor de Unified Manager.

> Hay algunos puertos que se consideran no seguros cuando se utilizan los navegadores Mozilla Firefox o Google Chrome. Consulte con el navegador antes de asignar un nuevo número de puerto para el tráfico HTTP y HTTPS. La selección de un puerto no seguro podría hacer que el sistema no sea accesible, lo que requeriría que se pusiera en contacto con el servicio de atención al cliente para obtener una resolución.

La instancia de Unified Manager se reinicia automáticamente después de cambiar el puerto, por lo que debe asegurarse de que es bueno momento para dejar el sistema inactivo durante un breve período de tiempo.

1. Inicie sesión con SSH como usuario de mantenimiento en el host de Unified Manager.

   Se muestran los mensajes de la consola de mantenimiento de Unified Manager.

2. Escriba el número de la opción de menú con la etiqueta **Ver/Cambiar puertos de aplicación** y, a continuación, pulse Intro.
3. Si se le solicita, vuelva a introducir la contraseña de usuario de mantenimiento.
4. Escriba los números de puerto nuevos para los puertos HTTP y HTTPS y, a continuación, pulse Intro.

   Si deja un número de puerto en blanco, se asigna el puerto predeterminado para el protocolo.

   Se le pregunta si desea cambiar los puertos y reiniciar Unified Manager ahora.

5. Escriba **y** para cambiar los puertos y reinicie Unified Manager.
6. Salga de la consola de mantenimiento.

Después de este cambio, los usuarios deben incluir el nuevo número de puerto en la URL para acceder a la interfaz de usuario web de Unified Manager, por ejemplo: https://host.company.com:1234, https://12.13.14.15:1122 o https://[2001:db8:0:1]:2123.

Se añaden interfaces de red

Puede agregar nuevas interfaces de red si necesita separar el tráfico de red.

Lo que necesitará

Debe haber añadido la interfaz de red al dispositivo virtual mediante vSphere.

El dispositivo virtual debe estar encendido.

> No puede realizar esta operación si Unified Manager está instalado en Red Hat Enterprise Linux o en Microsoft Windows.

Pasos

1. En el menú principal de la consola de vSphere, seleccione **Configuración del sistema** > **Reiniciar el sistema operativo**.

   Después de reiniciarse, la consola de mantenimiento puede detectar la interfaz de red recién añadida.

2. Acceda a la consola de mantenimiento.
3. Seleccione **Configuración de red** > **Activar interfaz de red**.
4. Seleccione la nueva interfaz de red y pulse **Intro**.

   Seleccione **eth1** y pulse **Intro**.

5. Escriba **y** para activar la interfaz de red.
6. Introduzca los ajustes de red.

   Se le pedirá que introduzca la configuración de red si se utiliza una interfaz estática o si no se detecta DHCP.

   Tras introducir los ajustes de red, volverá automáticamente al menú **Configuración de red**.

7. Seleccione **Commit Changes**.

   Debe confirmar los cambios para añadir la interfaz de red.

Agregar espacio en disco al directorio de la base de datos de Unified Manager

El directorio de bases de datos de Unified Manager contiene todos los datos de estado y rendimiento que se recopilan en los sistemas ONTAP. Algunas circunstancias pueden requerir que aumente el tamaño del directorio de la base de datos.

Por ejemplo, el directorio de base de datos se puede llenarse si Unified Manager está recopilando datos de un

gran número de clústeres en los que cada clúster tiene muchos nodos. Recibirá un evento de advertencia cuando el directorio de la base de datos esté lleno al 90% y un evento crítico cuando el directorio esté lleno al 95%.

No se recopilan datos adicionales de los clústeres después de que el directorio se encuentra lleno al 95 %.

Los pasos necesarios para añadir capacidad al directorio de datos son distintos en función de si Unified Manager se ejecuta en un servidor VMware ESXi, en un servidor Red Hat o CentOS Linux o en un servidor Microsoft Windows.

Adición de espacio al directorio de datos del host Linux

Si ha asignado poco espacio en disco a `/opt/netapp/data` directorio para admitir Unified Manager cuando originalmente configuró el host Linux y después instaló Unified Manager, es posible añadir espacio en disco después de la instalación aumentando espacio en disco en la `/opt/netapp/data` directorio.

Lo que necesitará

Debe tener acceso de usuario raíz a la máquina Red Hat Enterprise Linux o CentOS Linux en la que está instalado Unified Manager.

Le recomendamos que realice un backup de la base de datos de Unified Manager antes de aumentar el tamaño del directorio de datos.

Pasos

1. Inicie sesión como usuario root en el equipo Linux en el que desea agregar espacio en disco.
2. Detenga el servicio Unified Manager y el software MySQL asociado en el orden que se muestra:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Crear una carpeta de copia de seguridad temporal (por ejemplo, `/backup-data`) con suficiente espacio en disco para contener los datos de la corriente `/opt/netapp/data` directorio.
4. Copie la configuración de contenido y privilegios de la existente `/opt/netapp/data` directorio en el directorio de datos de copia de seguridad:

   ```
   cp -arp /opt/netapp/data/* /backup-data
   ```

5. Si se Linux está habilitado:

   a. Obtenga el tipo de Linux de se para las carpetas existentes `/opt/netapp/data` carpeta:

      ```
      se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |
      head -1
      ```

      El sistema devuelve una confirmación similar a la siguiente:

```
echo $se_type
mysqld_db_t
```

a. Ejecute el comando chcon para establecer el tipo de Linux se para el directorio de copia de seguridad:

```
chcon -R --type=mysqld_db_t /backup-data
```

6. Elimine el contenido del `/opt/netapp/data` directorio:
   a. `cd /opt/netapp/data`
   b. `rm -rf *`
7. Expanda el tamaño de `/opt/netapp/data` directorio a un mínimo de 150 GB a través de comandos de LVM o mediante la adición de discos adicionales.

> Si ha creado `/opt/netapp/data` desde un disco, no debe intentar montarlo `/opt/netapp/data` Como una unidad NFS o CIFS. Porque, en este caso, si intenta expandir el espacio en disco, algunos comandos de LVM como `resize` y.. `extend` es posible que no funcione como se espera.

8. Confirme que el `/opt/netapp/data` el propietario del directorio (mysql) y el grupo (root) no cambian:

```
ls -ltr /opt/netapp/ | grep data
```

El sistema devuelve una confirmación similar a la siguiente:

```
drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
```

9. Si se activa Linux, confirme que el contexto del `/opt/netapp/data` el directorio todavía está establecido en mysqld_db_t:
   a. `touch /opt/netapp/data/abc`
   b. `ls -Z /opt/netapp/data/abc`

      El sistema devuelve una confirmación similar a la siguiente:

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. Elimine el archivo abc de modo que este archivo no provoque un error en la base de datos en el futuro.
11. Copie el contenido de los datos de backup al expandido `/opt/netapp/data` directorio:

```
cp -arp /backup-data/* /opt/netapp/data/
```

12. Si se Linux está habilitado, ejecute el siguiente comando:

```
chcon -R --type=mysqld_db_t /opt/netapp/data
```

13. Inicie el servicio MySQL:

```
systemctl start mysqld
```

14. Una vez iniciado el servicio MySQL, inicie los servicios ocie y ocieau en el orden que se muestra:

```
systemctl start ocie ocieau
```

15. Después de iniciar todos los servicios, elimine la carpeta de copia de seguridad `/backup-data`:

```
rm -rf /backup-data
```

Adición de espacio al disco de datos de la máquina virtual de VMware

Si necesita aumentar la cantidad de espacio en el disco de datos de la base de datos de Unified Manager, puede añadir capacidad después de la instalación aumentando el espacio en disco mediante la consola de mantenimiento de Unified Manager.

Lo que necesitará

- Debe tener acceso a vSphere Client.
- La máquina virtual no debe tener instantáneas almacenadas localmente.
- Debe tener las credenciales de usuario de mantenimiento.

Le recomendamos que haga una copia de seguridad de su máquina virtual antes de aumentar el tamaño de los discos virtuales.

Pasos

1. En el cliente de vSphere, seleccione la máquina virtual de Unified Manager y, a continuación, añada más capacidad de disco a los datos `disk 3`. Consulte la documentación de VMware para obtener más detalles.

   En algunos casos excepcionales, la puesta en funcionamiento de Unified Manager utiliza «disco duro 2» para el disco de datos en lugar de «disco duro 3». Si esto se ha producido en la implementación, aumente el espacio del disco que sea mayor. El disco de datos siempre tendrá más espacio que el otro disco.

2. En el cliente vSphere, seleccione la máquina virtual de Unified Manager y, a continuación, seleccione la pestaña **Console**.
3. Haga clic en en la ventana de la consola y, a continuación, inicie sesión en la consola de mantenimiento con su nombre de usuario y contraseña.
4. En el menú principal, introduzca el número de la opción **Configuración del sistema**.
5. En el menú Configuración del sistema, introduzca el número de la opción **aumentar tamaño del disco de datos**.

Agregar espacio a la unidad lógica del servidor Microsoft Windows

Si necesita aumentar la cantidad de espacio en disco para la base de datos de Unified Manager, puede añadir capacidad a la unidad lógica en la que está instalado Unified

Manager.

Lo que necesitará

Debe tener privilegios de administrador de Windows.

Le recomendamos que realice un backup de la base de datos de Unified Manager antes de agregar espacio en disco.

Pasos

1. Inicie sesión como administrador en el servidor Windows en el que desea agregar espacio en disco.
2. Siga el paso correspondiente al método que desea utilizar para agregar más espacio:

Opción	Descripción
En un servidor físico, añada capacidad a la unidad lógica en la que se ha instalado el servidor de Unified Manager.	Siga los pasos del tema de Microsoft: "Extender un volumen básico"
En un servidor físico, agregue una unidad de disco duro.	Siga los pasos del tema de Microsoft: "Agregar unidades de disco duro"
En un equipo virtual, aumente el tamaño de una partición de disco.	Siga los pasos del tema de VMware: "Aumentar el tamaño de una partición de disco"

Gestión del acceso de usuarios

Es posible crear roles y asignar capacidades para controlar el acceso de los usuarios a Active IQ Unified Manager. Puede identificar los usuarios que tienen las funcionalidades necesarias para acceder a los objetos seleccionados en Unified Manager. Solo los usuarios que tienen estos roles y funcionalidades pueden gestionar los objetos en Unified Manager.

Adición de usuarios

Puede agregar usuarios locales o usuarios de bases de datos mediante la página Users. También puede agregar usuarios o grupos remotos que pertenecen a un servidor de autenticación. Es posible asignar roles a esos usuarios y, según los privilegios de los roles, los usuarios pueden gestionar los objetos de almacenamiento y los datos con Unified Manager, o ver los datos en una base de datos.

Lo que necesitará

- Debe tener la función Administrador de aplicaciones.
- Para agregar un usuario o grupo remoto, debe haber habilitado la autenticación remota y configurado el servidor de autenticación.

- Si planea configurar la autenticación SAML de modo que un proveedor de identidades (IDP) autentique usuarios que acceden a la interfaz gráfica, asegúrese de que estos usuarios se definen como usuarios "relativamente".

  No se permite el acceso a la interfaz de usuario para usuarios de tipo "'local'" o "mantenimiento" cuando se activa la autenticación SAML.

Si agrega un grupo desde Windows Active Directory, todos los miembros directos y subgrupos anidados pueden autenticarse en Unified Manager, a menos que los subgrupos anidados estén deshabilitados. Si agrega un grupo desde OpenLDAP u otros servicios de autenticación, solo los miembros directos de ese grupo pueden autenticarse en Unified Manager.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **usuarios**.
2. En la página usuarios, haga clic en **Agregar**.
3. En el cuadro de diálogo Agregar usuario, seleccione el tipo de usuario que desea agregar e introduzca la información necesaria.

   Al introducir la información de usuario requerida, debe especificar una dirección de correo electrónico que sea exclusiva para el usuario. Debe evitar especificar las direcciones de correo electrónico compartidas por varios usuarios.

4. Haga clic en **Agregar**.

Creación de un usuario de base de datos

Para admitir una conexión entre Workflow Automation y Unified Manager, o bien para acceder a las vistas de la base de datos, primero debe crear un usuario de base de datos con los roles Integration Schema o Report Schema en la interfaz de usuario web de Unified Manager.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Los usuarios de bases de datos proporcionan integración con Workflow Automation y acceso a vistas de base de datos específicas para informes. Los usuarios de la base de datos no tienen acceso a la interfaz de usuario web de Unified Manager o a la consola de mantenimiento, y no pueden ejecutar llamadas de API.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **usuarios**.
2. En la página Users (usuarios), haga clic en **Add**.
3. En el cuadro de diálogo Agregar usuario, seleccione **Usuario de base de datos** en la lista desplegable **Tipo**.
4. Escriba un nombre y una contraseña para el usuario de la base de datos.
5. En la lista desplegable **rol**, seleccione el rol apropiado.

Si está…	Elija este rol
Conexión de Unified Manager con Workflow Automation	Esquema de integración
Acceso a las vistas Informes y otras vistas de bases de datos	Esquema de informes

6. Haga clic en **Agregar**.

Edición de la configuración de usuario

Puede editar la configuración de usuario, como la dirección de correo electrónico y el rol, que se especifican a cada usuario. Por ejemplo, se recomienda cambiar el rol de un usuario que es un operador de almacenamiento y asignar privilegios de administrador de almacenamiento al usuario.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Cuando se modifica el rol asignado a un usuario, los cambios se aplican cuando se produce cualquiera de las siguientes acciones:

- El usuario cierra la sesión y vuelve a iniciar sesión en Unified Manager.
- Se alcanza un tiempo de espera de sesión de 24 horas.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **usuarios**.
2. En la página Users (usuarios), seleccione el usuario para el que desea editar la configuración y haga clic en **Edit**.
3. En el cuadro de diálogo Editar usuario, edite la configuración adecuada que se ha especificado para el usuario.
4. Haga clic en **Guardar**.

Ver usuarios

Puede utilizar la página Users para ver la lista de usuarios que gestionan objetos de almacenamiento y datos mediante Unified Manager. Es posible ver detalles sobre los usuarios, como el nombre de usuario, el tipo de usuario, la dirección de correo electrónico y el rol asignado a los usuarios.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Paso

1. En el panel de navegación izquierdo, haga clic en **General** > **usuarios**.

Eliminación de usuarios o grupos

Puede eliminar uno o varios usuarios de la base de datos del servidor de gestión para evitar que usuarios específicos accedan a Unified Manager. También puede eliminar grupos para que todos los usuarios del grupo ya no puedan acceder al servidor de administración.

Lo que necesitará

- Cuando se eliminan grupos remotos, debe haber reasignado los eventos que se asignan a los usuarios de los grupos remotos.

  Si va a eliminar usuarios locales o usuarios remotos, los eventos asignados a estos usuarios se asignarán automáticamente.

- Debe tener la función Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **usuarios**.
2. En la página Users (usuarios), seleccione los usuarios o grupos que desea eliminar y, a continuación, haga clic en **Delete**.
3. Haga clic en **Sí** para confirmar la eliminación.

Qué es RBAC

El control de acceso basado en roles (RBAC) ofrece la capacidad de controlar quién tiene acceso a diversas funciones y recursos en el servidor Active IQ Unified Manager.

Qué hace el control de acceso basado en roles

El control de acceso basado en roles permite a los administradores gestionar grupos de usuarios definiendo roles. Si necesita restringir el acceso a funciones específicas para administradores seleccionados, debe configurar cuentas de administrador para ellos. Si desea restringir la información que los administradores pueden ver y las operaciones que pueden realizar, debe aplicar roles a las cuentas de administrador que cree.

El servidor de gestión utiliza RBAC para los permisos de inicio de sesión de usuario y roles. Si no ha cambiado la configuración predeterminada del servidor de administración para el acceso de usuarios administrativos, no es necesario iniciar sesión para verlos.

Al iniciar una operación que requiere privilegios específicos, el servidor de administración le solicita que inicie sesión. Por ejemplo, para crear cuentas de administrador, debe iniciar sesión con acceso a la cuenta de Administrador de aplicaciones.

Definiciones de tipos de usuario

Un tipo de usuario especifica el tipo de cuenta que contiene el usuario e incluye usuarios remotos, grupos remotos, usuarios locales, usuarios de base de datos y usuarios de mantenimiento. Cada uno de estos tipos tiene su propia función, que asigna un usuario

con la función Administrador.

Los tipos de usuario de Unified Manager son los siguientes:

- **Usuario de mantenimiento**

  Se crea durante la configuración inicial de Unified Manager. A continuación, el usuario de mantenimiento crea usuarios adicionales y asigna funciones. El usuario de mantenimiento es también el único usuario con acceso a la consola de mantenimiento. Cuando Unified Manager se instala en un sistema Red Hat Enterprise Linux o CentOS, al usuario de mantenimiento se le asigna el nombre de usuario «'umadmin».

- **Usuario local**

  Accede a la interfaz de usuario de Unified Manager y realiza funciones según el rol dado por el usuario de mantenimiento o un usuario con el rol de administrador de aplicaciones.

- **Grupo remoto**

  Un grupo de usuarios que acceden a la interfaz de usuario de Unified Manager con las credenciales almacenadas en el servidor de autenticación. El nombre de esta cuenta debe coincidir con el nombre de un grupo almacenado en el servidor de autenticación. Todos los usuarios del grupo remoto reciben acceso a la interfaz de usuario de Unified Manager usando sus credenciales de usuario individuales. Los grupos remotos pueden realizar funciones según sus roles asignados.

- **Usuario remoto**

  Accede a la interfaz de usuario de Unified Manager con las credenciales almacenadas en el servidor de autenticación. Un usuario remoto realiza funciones basadas en la función proporcionada por el usuario de mantenimiento o un usuario con la función Administrador de aplicaciones.

- **Usuario de base de datos**

  Tiene acceso de solo lectura a los datos en la base de datos de Unified Manager, no tiene acceso a la interfaz web de Unified Manager ni a la consola de mantenimiento, y no puede ejecutar llamadas de API.

Definiciones de roles de usuario

El usuario de mantenimiento o el administrador de aplicaciones asigna una función a todos los usuarios. Cada rol contiene ciertos privilegios. El ámbito de las actividades que se pueden realizar en Unified Manager depende del rol que se tenga asignado y de los privilegios que contiene el rol.

Unified Manager incluye los siguientes roles de usuario predefinidos:

- **Operador**

  Permite ver información sobre el sistema de almacenamiento y otros datos recopilados por Unified Manager, incluidos historiales y tendencias de capacidad. Este rol permite al operador de almacenamiento ver, asignar, reconocer, resolver y añadir notas para los eventos.

- **Administrador de almacenamiento**

  Configura las operaciones de gestión del almacenamiento en Unified Manager. Este rol permite al administrador de almacenamiento configurar umbrales y crear alertas, así como otras opciones y políticas

específicas de la gestión del almacenamiento.

- **Administrador de aplicaciones**

  Configura ajustes que no están relacionados con la administración del almacenamiento. Esta función permite la gestión de usuarios, certificados de seguridad, acceso a la base de datos y opciones administrativas, incluida la autenticación, SMTP, redes y AutoSupport.

  Cuando Unified Manager se instala en sistemas Linux, el usuario inicial con la función de administrador de aplicaciones se denomina automáticamente «'umadmin'».

- **Esquema de integración**

  Este rol permite el acceso de solo lectura a las vistas de la base de datos de Unified Manager con la integración de Unified Manager con OnCommand Workflow Automation (WFA).

- **Esquema del informe**

  Este rol habilita el acceso de solo lectura a los informes y otras vistas de bases de datos directamente desde la base de datos de Unified Manager. Las bases de datos que se pueden ver incluyen:

  - vista_modelo_netapp
  - rendimiento_netapp
  - ocum
  - ocum_report
  - ocum_report_birt
  - opm
  - escalemador

Roles y funcionalidades de usuario de Unified Manager

Según el rol de usuario asignado, puede determinar qué operaciones puede realizar en Unified Manager.

En la siguiente tabla, se muestran las funciones que puede realizar cada rol de usuario:

Función	Operador	Administrador de almacenamiento	Administrador de aplicaciones	Esquema de integración	Esquema de informes
Ver la información del sistema de almacenamiento	•	•	•	•	•
Ver otros datos, como historiales y tendencias de capacidad	•	•	•	•	•

Función	Operador	Administrador de almacenamiento	Administrador de aplicaciones	Esquema de integración	Esquema de informes
Ver, asignar y resolver eventos	•	•	•		
Ver los objetos de servicio de almacenamiento, como las asociaciones de SVM y los pools de recursos	•	•	•		
Ver políticas de umbral	•	•	•		
Gestionar objetos de servicio de almacenamiento, como asociaciones de SVM y pools de recursos		•	•		
Defina las alertas		•	•		
Gestione las opciones de gestión del almacenamiento		•	•		
Gestione las políticas de gestión del almacenamiento		•	•		
Gestionar usuarios			•		
Administrar opciones administrativas			•		

Función	Operador	Administrador de almacenamiento	Administrador de aplicaciones	Esquema de integración	Esquema de informes
Defina las políticas de umbral			•		
Gestionar el acceso a las bases de datos			•		
Gestione la integración con WFA y proporcione acceso a las vistas de la base de datos				•	
Programar y guardar informes		•	•		
Ejecutar las operaciones «'Fix it'» de las acciones de gestión		•	•		
Proporcione acceso de sólo lectura a las vistas de base de datos					•

Gestión de la configuración de autenticación SAML

Después de configurar la configuración de autenticación remota, puede habilitar la autenticación del lenguaje de marcado de aserción de seguridad (SAML) para que los usuarios remotos estén autenticados por un proveedor de identidades (IDP) seguro antes de que puedan acceder a la interfaz de usuario web de Unified Manager.

Tenga en cuenta que solo los usuarios remotos tendrán acceso a la interfaz gráfica de usuario de Unified Manager después de habilitar la autenticación SAML. Los usuarios locales y los usuarios de mantenimiento no podrán acceder a la interfaz de usuario. Esta configuración no afecta a los usuarios que acceden a la consola de mantenimiento.

Requisitos del proveedor de identidades

Al configurar Unified Manager para que utilice un proveedor de identidades (IDP) para realizar la autenticación SAML de todos los usuarios remotos, debe tener en cuenta algunos ajustes de configuración necesarios para que la conexión a Unified Manager se haya realizado correctamente.

Debe introducir el URI y los metadatos de Unified Manager en el servidor IDP. Puede copiar esta información desde la página autenticación de Unified Manager SAML. Unified Manager se considera el proveedor de servicios (SP) en el estándar de lenguaje de marcado de aserción de seguridad (SAML).

Estándares de cifrado compatibles

- Estándar de cifrado avanzado (AES): AES-128 y AES-256
- Secure Hash Algorithm (SHA): SHA-1 y SHA-256

Proveedores de identidades validados

- Shibboleth
- Servicios de Federación de Active Directory (ADFS).

Requisitos de configuración de ADFS

- Debe definir tres reglas de reclamación en el siguiente orden que se requieren para que Unified Manager analice las respuestas SAML de ADFS para esta entrada de confianza de parte confiable.

Regla de reclamación	Valor
SAM-account-name	ID del nombre
SAM-account-name	urn:oid:0.9.2342.19200300.100.1.1
Grupos de token — Nombre no cualificado	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- Debe establecer el método de autenticación en "'autenticación de formularios'" o los usuarios pueden recibir un error al cerrar sesión en Unified Manager . Siga estos pasos:
  a. Abra la Consola de administración de ADFS.
  b. Haga clic en la carpeta Directivas de autenticación de la vista de árbol izquierda.
  c. En acciones a la derecha, haga clic en Editar directiva de autenticación primaria global.
  d. Establezca el método de autenticación de la intranet en "'autenticación de formularios'" en lugar del valor predeterminado "'autenticación de Windows'".
- En algunos casos, se rechaza iniciar sesión mediante el IDP cuando el certificado de seguridad de Unified Manager está firmado por CA. Existen dos soluciones alternativas para resolver este problema:
  - Siga las instrucciones identificadas en el vínculo para deshabilitar la comprobación de revocación en el servidor ADFS para la parte de confianza asociada al certificado de CA encadenada:

    "Desactive el control de revocación por confianza de parte de confianza"

◦ Haga que el servidor de CA resida en el servidor ADFS para firmar la solicitud de certificado del servidor Unified Manager.

Otros requisitos de configuración

- La desviación del reloj de Unified Manager se establece en 5 minutos, por lo que la diferencia de hora entre el servidor IDP y el servidor Unified Manager no puede ser superior a 5 minutos o se producirá un error en la autenticación.

Habilitación de la autenticación SAML

Puede habilitar la autenticación del lenguaje de marcado de aserción de seguridad (SAML) para que los usuarios remotos se autentiquen mediante un proveedor de identidad seguro (IDP) antes de poder acceder a la interfaz de usuario web de Unified Manager.

Lo que necesitará

- Debe haber configurado la autenticación remota y verificado que la autenticación se ha realizado correctamente.
- Debe haber creado al menos un usuario remoto, o un grupo remoto, con la función Administrador de aplicaciones.
- El proveedor de identidades (IDP) debe ser compatible con Unified Manager y debe configurarse.
- Debe tener la URL y los metadatos de IDP.
- Debe tener acceso al servidor IDP.

Después de habilitar la autenticación SAML de Unified Manager, los usuarios no pueden acceder a la interfaz gráfica de usuario hasta que el IDP se haya configurado con la información de host del servidor de Unified Manager. Por lo tanto, debe estar preparado para completar ambas partes de la conexión antes de iniciar el proceso de configuración. El IDP se puede configurar antes o después de configurar Unified Manager.

Solo los usuarios remotos tendrán acceso a la interfaz gráfica de usuario de Unified Manager después de habilitar la autenticación SAML. Los usuarios locales y los usuarios de mantenimiento no podrán acceder a la interfaz de usuario. Esta configuración no afecta a los usuarios que acceden a la consola de mantenimiento, los comandos de Unified Manager o las ZAPI.

Unified Manager se reinicia automáticamente después de completar la configuración de SAML en esta página.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación SAML**.
2. Seleccione la casilla de verificación **Habilitar autenticación SAML**.

   Se mostrarán los campos necesarios para configurar la conexión IDP.

3. Introduzca el URI de IDP y los metadatos de IDP necesarios para conectar el servidor de Unified Manager al servidor de IDP.

   Si se puede acceder al servidor IDP directamente desde el servidor de Unified Manager, puede hacer clic en el botón **Fetch IDP Metadata** después de introducir el URI IDP para rellenar el campo IDP Metadata automáticamente.

4. Copie el URI de metadatos de host de Unified Manager o guarde los metadatos del host en un archivo de texto XML.

   Ahora es posible configurar el servidor IDP con esta información.

5. Haga clic en **Guardar**.

   Aparece un cuadro de mensaje para confirmar que desea completar la configuración y reiniciar Unified Manager.

6. Haga clic en **Confirmar y cerrar sesión** y se reiniciará Unified Manager.

La próxima vez que los usuarios remotos autorizados intenten acceder a la interfaz gráfica de Unified Manager, deberán introducir sus credenciales en la página de inicio de sesión de IDP en lugar de en la página de inicio de sesión de Unified Manager.

Si no se ha completado todavía, acceda a IDP e introduzca el URI del servidor de Unified Manager y los metadatos para completar la configuración.

> Cuando se utiliza ADFS como proveedor de identidades, la interfaz gráfica de usuario de Unified Manager no cumple el tiempo de espera de ADFS y continúa funcionando hasta que se alcanza el tiempo de espera de la sesión de Unified Manager. Puede cambiar el tiempo de espera de la sesión de la GUI haciendo clic en **General** > **Configuración de características** > **tiempo de espera de inactividad**.

Cambiar el proveedor de identidades utilizado para la autenticación SAML

Es posible cambiar el proveedor de identidades (IDP) que Unified Manager utiliza para autenticar usuarios remotos.

Lo que necesitará

- Debe tener la URL y los metadatos de IDP.
- Debe tener acceso al IDP.

El nuevo IDP se puede configurar antes o después de configurar Unified Manager.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación SAML**.
2. Introduzca el URI nuevo de IDP y los metadatos de IDP necesarios para conectar el servidor de Unified Manager al IDP.

   Si se puede acceder al IDP directamente desde el servidor de Unified Manager, puede hacer clic en el botón **Fetch IDP Metadata** después de introducir la URL del IDP para rellenar el campo IDP Metadata automáticamente.

3. Copie el URI de metadatos de Unified Manager o guarde los metadatos en un archivo de texto XML.
4. Haga clic en **Guardar configuración**.

   Aparece un cuadro de mensaje para confirmar que desea cambiar la configuración.

5. Haga clic en **Aceptar**.

Acceda al nuevo IDP e introduzca el URI del servidor de Unified Manager y los metadatos para completar la configuración.

La próxima vez que los usuarios remotos autorizados intenten acceder a la interfaz gráfica de Unified Manager, deberán introducir sus credenciales en la nueva página de inicio de sesión de IDP en lugar de en la página de inicio de sesión de IDP anterior.

Actualizar la configuración de autenticación SAML después de cambiar el certificado de seguridad de Unified Manager

Cualquier cambio en el certificado de seguridad HTTPS instalado en Unified Manager Server requiere actualizar los ajustes de configuración de la autenticación SAML. El certificado se actualiza si cambia el nombre del sistema host, asigna una dirección IP nueva al sistema host o cambia manualmente el certificado de seguridad del sistema.

Después de modificar el certificado de seguridad y se reinicia el servidor de Unified Manager, la autenticación SAML no funcionará y los usuarios no podrán acceder a la interfaz gráfica de Unified Manager. Debe actualizar la configuración de autenticación SAML tanto en el servidor IDP como en el servidor de Unified Manager para volver a habilitar el acceso a la interfaz de usuario.

Pasos

1. Inicie sesión en la consola de mantenimiento.
2. En el **Menú principal**, introduzca el número de la opción **Desactivar autenticación SAML**.

   Aparece un mensaje para confirmar que desea deshabilitar la autenticación SAML y reiniciar Unified Manager.

3. Inicie la interfaz de usuario de Unified Manager con el FQDN o la dirección IP actualizados, acepte el certificado de servidor actualizado en el explorador e inicie sesión con las credenciales de usuario de mantenimiento.
4. En la página **Configuración/autenticación**, seleccione la ficha **autenticación SAML** y configure la conexión IDP.
5. Copie el URI de metadatos de host de Unified Manager o guarde los metadatos del host en un archivo de texto XML.
6. Haga clic en **Guardar**.

   Aparece un cuadro de mensaje para confirmar que desea completar la configuración y reiniciar Unified Manager.

7. Haga clic en **Confirmar y cerrar sesión** y se reiniciará Unified Manager.
8. Acceda al servidor IDP e introduzca el URI del servidor de Unified Manager y los metadatos para completar la configuración.

Proveedor de identidades	Pasos de configuración
ADFS	a. Elimine la entrada de confianza de la parte de confianza existente en la GUI de administración de ADFS. b. Agregue una nueva entrada de confianza de parte de confianza mediante el `saml_sp_metadata.xml` Desde el servidor de Unified Manager actualizado. c. Defina las tres reglas de reclamación necesarias para que Unified Manager analice las respuestas SAML de ADFS para esta entrada de confianza de parte fiable. d. Reinicie el servicio de Windows de ADFS.
Shibboleth	a. Actualice el nuevo FQDN del servidor Unified Manager en el `attribute-filter.xml` y.. `relying-party.xml` archivos. b. Reinicie el servidor Web Apache Tomcat y espere a que el puerto 8005 se vuelva a conectar.

9. Inicie sesión en Unified Manager y verifique que la autenticación SAML funcione como se espera en el IDP.

Deshabilitación de la autenticación SAML

Es posible deshabilitar la autenticación SAML cuando se desea dejar de autenticar usuarios remotos a través de un proveedor de identidad segura (IDP) para poder iniciar sesión en la interfaz de usuario web de Unified Manager. Cuando se deshabilita la autenticación SAML, los proveedores de servicios de directorio configurados, como Active Directory o LDAP, realizan la autenticación de inicio de sesión.

Después de deshabilitar la autenticación SAML, los usuarios locales y los usuarios de mantenimiento podrán acceder a la interfaz gráfica de usuario además de los usuarios remotos configurados.

También puede deshabilitar la autenticación SAML con la consola de mantenimiento de Unified Manager si no tiene acceso a la interfaz gráfica de usuario.

Unified Manager se reinicia automáticamente después de deshabilitar la autenticación de SAML.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación SAML**.
2. Desactive la casilla de verificación **Activar autenticación SAML**.
3. Haga clic en **Guardar**.

   Aparece un cuadro de mensaje para confirmar que desea completar la configuración y reiniciar Unified

Manager.

4. Haga clic en **Confirmar y cerrar sesión** y se reiniciará Unified Manager.

La próxima vez que los usuarios remotos intenten acceder a la interfaz gráfica de Unified Manager, deberán introducir sus credenciales en la página de inicio de sesión de Unified Manager en lugar de en la página de inicio de sesión de IDP.

Acceda a IDP y elimine el URI del servidor de Unified Manager y los metadatos.

Deshabilitar la autenticación SAML de la consola de mantenimiento

Es posible que deba deshabilitar la autenticación SAML desde la consola de mantenimiento cuando no existe acceso a la interfaz gráfica de usuario de Unified Manager. Esto puede suceder en casos de configuración errónea o si no se puede acceder al IDP.

Lo que necesitará

Debe tener acceso a la consola de mantenimiento como usuario de mantenimiento.

Cuando se deshabilita la autenticación SAML, los proveedores de servicios de directorio configurados, como Active Directory o LDAP, realizan la autenticación de inicio de sesión. Los usuarios locales y los usuarios de mantenimiento podrán acceder a la interfaz gráfica de usuario además de los usuarios remotos configurados.

También se puede deshabilitar la autenticación SAML desde la página Setup/Authentication en la interfaz de usuario.

Unified Manager se reinicia automáticamente después de deshabilitar la autenticación de SAML.

Pasos

1. Inicie sesión en la consola de mantenimiento.
2. En el **Menú principal**, introduzca el número de la opción **Desactivar autenticación SAML**.

   Aparece un mensaje para confirmar que desea deshabilitar la autenticación SAML y reiniciar Unified Manager.

3. Escriba **y** y, a continuación, pulse Intro y se reiniciará Unified Manager.

La próxima vez que los usuarios remotos intenten acceder a la interfaz gráfica de Unified Manager, deberán introducir sus credenciales en la página de inicio de sesión de Unified Manager en lugar de en la página de inicio de sesión de IDP.

Si se requiere, acceda a IDP y elimine la URL del servidor de Unified Manager y los metadatos.

Página autenticación SAML

Es posible usar la página autenticación de SAML para configurar Unified Manager para autenticar usuarios remotos mediante SAML a través de un proveedor de identidad seguro (IDP) para que puedan iniciar sesión en la interfaz de usuario web de Unified Manager.

- Debe tener el rol de administrador de aplicaciones para crear o modificar la configuración de SAML.
- Debe haber configurado la autenticación remota.
- Debe haber configurado al menos un usuario remoto o un grupo remoto.

Después de configurar la autenticación remota y los usuarios remotos, puede seleccionar la casilla de comprobación Habilitar autenticación SAML para habilitar la autenticación mediante un proveedor de identidades seguro.

- **URI de IDP**

  El URI para acceder al IDP desde el servidor de Unified Manager. A continuación se enumeran los URI de ejemplo.

  URI de ejemplo de ADFS:

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Ejemplo de URI de Shibboleth:

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **Metadatos IDP**

  Los metadatos de IDP tienen formato XML.

  Si se puede acceder a la URL de IDP desde el servidor de Unified Manager, puede hacer clic en el botón **Fetch IDP Metadata** para rellenar este campo.

- **Sistema host (FQDN)**

  El nombre de dominio completo del sistema host de Unified Manager, tal como se define durante la instalación. Puede cambiar este valor si es necesario.

- **URI de host**

  El URI para acceder al sistema host de Unified Manager desde el IDP.

- **Metadatos del host**

  Los metadatos del sistema host en formato XML.

Gestión de la autenticación

Puede habilitar la autenticación mediante LDAP o Active Directory en el servidor de Unified Manager y configurarla para que funcione con los servidores con el fin de autenticar usuarios remotos.

Para habilitar la autenticación remota, configurar los servicios de autenticación y agregar servidores de autenticación, consulte la sección anterior en **Configuración de Unified Manager para enviar notificaciones de alerta**.

Editar servidores de autenticación

Es posible cambiar el puerto que utiliza Unified Manager Server para comunicarse con el servidor de autenticación.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. Active la casilla **Desactivar búsqueda de grupo anidada**.
3. En el área **servidores de autenticación**, seleccione el servidor de autenticación que desea editar y, a continuación, haga clic en **Editar**.
4. En el cuadro de diálogo **Editar servidor de autenticación**, edite los detalles del puerto.
5. Haga clic en **Guardar**.

Eliminar servidores de autenticación

Puede eliminar un servidor de autenticación si desea impedir que Unified Manager Server se comunique con el servidor de autenticación. Por ejemplo, si desea cambiar un servidor de autenticación con el que el servidor de administración está comunicando, puede eliminar el servidor de autenticación y agregar un nuevo servidor de autenticación.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Cuando se elimina un servidor de autenticación, los usuarios remotos o grupos del servidor de autenticación ya no pueden acceder a Unified Manager.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. Seleccione uno o varios servidores de autenticación que desee eliminar y, a continuación, haga clic en **Eliminar**.
3. Haga clic en **Sí** para confirmar la solicitud de eliminación.

   Si la opción **usar conexión segura** está activada, los certificados asociados con el servidor de autenticación se eliminarán junto con el servidor de autenticación.

Autenticación con Active Directory u OpenLDAP

Es posible habilitar la autenticación remota en el servidor de gestión y configurar el servidor de gestión para que se comunique con los servidores de autenticación, de modo que los usuarios dentro de los servidores de autenticación puedan acceder a Unified Manager.

Puede utilizar uno de los siguientes servicios de autenticación predefinidos o especificar su propio servicio de

autenticación:

- Active Directory de Microsoft

  No puede usar los servicios de directorio ligero de Microsoft.

- OpenLDAP

Puede seleccionar el servicio de autenticación requerido y añadir los servidores de autenticación adecuados para habilitar los usuarios remotos en el servidor de autenticación para acceder a Unified Manager. El servidor de autenticación mantiene las credenciales de los usuarios o grupos remotos. El servidor de gestión usa el protocolo ligero de acceso a directorios (LDAP) para autenticar a los usuarios remotos dentro del servidor de autenticación configurado.

Para los usuarios locales que se crean en Unified Manager, el servidor de gestión mantiene su propia base de datos de nombres de usuario y contraseñas. El servidor de gestión realiza la autenticación y no utiliza Active Directory ni OpenLDAP para la autenticación.

Registro de auditoría

Es posible detectar si los registros de auditoría se ven comprometidos con el uso de registros de auditoría. Todas las actividades realizadas por un usuario se supervisan y registran en los registros de auditoría. Las auditorías se realizan para todas las interfaces de usuario y las funcionalidades de Active IQ Unified Manager de las API expuestas al público.

Puede utilizar **Registro de auditoría: Vista de archivo** para ver y acceder a todos los archivos de registro de auditoría disponibles en Active IQ Unified Manager. Los archivos del Registro de auditoría: Vista de archivo se muestran en función de su fecha de creación. Esta vista muestra información de todo el registro de auditoría capturado desde la instalación o actualización al presente en el sistema. Siempre que se realiza una acción en Unified Manager, la información se actualiza y está disponible en los registros. El estado de cada archivo de registro se captura mediante el atributo "'Estado de integridad de archivo'", que se supervisa activamente para detectar la manipulación o eliminación del archivo de registro. Los registros de auditoría pueden tener uno de los siguientes estados cuando los registros de auditoría están disponibles en el sistema:

Estado	Descripción
ACTIVO	Archivo en el que se registran actualmente los registros.
NORMAL	Archivo inactivo, comprimido y almacenado en el sistema.
MANIPULADO	Archivo que ha sido comprometido por un usuario que ha editado el archivo manualmente.
ELIMINAR_MANUAL	Archivo eliminado por un usuario autorizado.
ROLLOVER_DELETE	Archivo que se eliminó debido a la rodadura basada en la directiva de configuración gradual.

Estado	Descripción
INESPERADO_DELETE	Archivo eliminado por motivos desconocidos.

La página Registro de auditoría incluye los siguientes botones de comando:

- Configurar
- Eliminar
- Descargue

El botón **DELETE** permite eliminar cualquiera de los registros de auditoría enumerados en la vista registros de auditoría. Puede eliminar un registro de auditoría y, opcionalmente, proporcionar un motivo para eliminar el archivo que ayuda en el futuro a determinar una eliminación válida. La columna MOTIVO enumera el motivo junto con el nombre del usuario que realizó la operación de eliminación.

La eliminación de un archivo de registro provocará la eliminación del archivo del sistema, pero la entrada de la tabla DB no se eliminará.

Puede descargar los registros de auditoría de Active IQ Unified Manager con el botón **DOWNLOAD** de la sección registros de auditoría y exportar los archivos de registro de auditoría. Los archivos marcados con «'NORMAL'» o «'MANIPULADO'» se descargan en una compresión `.gzip` formato.

Los archivos de registro de auditoría se archivan periódicamente y se guardan en la base de datos a modo de referencia. Antes del archivado, los registros de auditoría se firman digitalmente para mantener la seguridad y la integridad.

Cuando se genera un paquete AutoSupport completo, el bundle de soporte incluye tanto archivos de registro de auditoría archivados como activos. Pero cuando se genera un bundle de soporte ligero, solo incluye los registros de auditoría activos. No se incluyen los registros de auditoría archivados.

Configuración de registros de auditoría

Puede utilizar el botón **Configurar** de la sección registros de auditoría para configurar la directiva de implementación para archivos de registro de auditoría y también para habilitar el registro remoto para los registros de auditoría.

Puede establecer los valores en **MAX FILE SIZE** y **AUDIT LOG RETENTION PERID** según la cantidad y frecuencia de datos que desee almacenar en el sistema. El valor del campo **TAMAÑO TOTAL del REGISTRO de AUDITORÍA** es el tamaño de los datos totales del registro de auditoría presentes en el sistema. La directiva de recuperación viene determinada por los valores del campo **DÍAS de RETENCIÓN de REGISTRO DE AUDITORÍA**, **TAMAÑO de ARCHIVO MAX** y **TAMAÑO DE REGISTRO DE AUDITORÍA TOTAL**. Cuando el tamaño de la copia de seguridad del registro de auditoría alcanza el valor configurado en **TAMAÑO TOTAL del REGISTRO de AUDITORÍA**, el archivo que se archivó primero se elimina. Esto significa que se ha eliminado el archivo más antiguo. Pero la entrada del fichero sigue estando disponible en la base de datos y está marcada como "'Rollover Delete'". El valor **DÍAS de RETENCIÓN del REGISTRO DE AUDITORÍA** es para el número de días que se conservan los archivos de registro de auditoría. Cualquier archivo anterior al valor establecido en este campo se repasa.

Pasos

1. Haga clic en **registros de auditoría** > > **Configurar**.
2. Introduzca los valores en **MAX FILE SIZE**, **TOTAL AUDIT LOG SIZE** y **DÍAS DE RETENCIÓN DEL**

REGISTRO de AUDITORÍA.

Si desea activar el registro remoto, debe seleccionar **Activar registro remoto**.

Habilitación de registro remoto de registros de auditoría

Puede seleccionar la casilla de verificación **Activar registro remoto** en el cuadro de diálogo Configurar registros de auditoría para habilitar el registro de auditoría remoto. Es posible usar esta función para transferir registros de auditoría a un servidor de syslog remoto. Esto le permitirá gestionar los registros de auditoría cuando haya restricciones de espacio.

El registro remoto de registros de auditoría proporciona una copia de seguridad a prueba de manipulaciones en caso de que se manipulen los archivos de registro de auditoría del servidor Active IQ Unified Manager.

Pasos

1. En el cuadro de diálogo **Configurar registros de auditoría**, seleccione la casilla de verificación **Activar registro remoto**.

   Se mostrarán campos adicionales para configurar el registro remoto.

2. Introduzca el **NOMBRE de HOST** y el **PUERTO** del servidor remoto al que desea conectarse.
3. En el campo **CERTIFICADO de CA de SERVIDOR**, haga clic en **EXAMINAR** para seleccionar un certificado público del servidor de destino.

   El certificado debe cargarse en `.pem` formato. Este certificado debe obtenerse del servidor de syslog de destino y no debe haber caducado. El certificado deberá contener el «'nombre de host'» seleccionado como parte de la `SubjectAltName` (SAN).

4. Introduzca los valores para los siguientes campos: **CHARSET**, **TIEMPO DE ESPERA de CONEXIÓN**, **RETARDO DE RECONEXIÓN**.

   Los valores deben estar en milisegundos para estos campos.

5. Seleccione el formato Syslog requerido y la versión del protocolo TLS en los campos **FORMAT** y **PROTOCOL**.
6. Seleccione la casilla de verificación **Activar autenticación de cliente** si el servidor Syslog de destino requiere autenticación basada en certificados.

   Deberá descargar el certificado de autenticación de cliente y cargarlo en el servidor de syslog antes de guardar la configuración del registro de auditoría; de lo contrario, se producirá un error en la conexión. Según el tipo de servidor de syslog, puede que deba crear un hash del certificado de autenticación de cliente.

   Ejemplo: Syslog-ng requiere que se cree una <hash> del certificado con el comando `openssl x509 -noout -hash -in cert.pem`y, a continuación, debe vincular simbólicamente el certificado de autenticación de cliente a un archivo denominado después de <hash> .0.

7. Haga clic en **Guardar** para configurar la conexión con el servidor y activar el registro remoto.

   Se le redirigirá a la página registros de auditoría.

Autenticación remota

Puede utilizar la página autenticación remota para configurar Unified Manager para comunicarse con el servidor de autenticación con el fin de autenticar a los usuarios remotos que intentan iniciar sesión en la interfaz de usuario web de Unified Manager.

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Después de seleccionar la casilla de verificación Habilitar autenticación remota, puede habilitar la autenticación remota mediante un servidor de autenticación.

- **Servicio de autenticación**

  Permite configurar el servidor de administración para autenticar usuarios en proveedores de servicios de directorio, como Active Directory, OpenLDAP o especificar su propio mecanismo de autenticación. Sólo puede especificar un servicio de autenticación si ha habilitado la autenticación remota.

  - **Active Directory**
    - Nombre del administrador

      Especifica el nombre de administrador del servidor de autenticación.

    - Contraseña

      Especifica la contraseña para acceder al servidor de autenticación.

    - Nombre completo base

      Especifica la ubicación de los usuarios remotos en el servidor de autenticación. Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, entonces el nombre completo base es **cn=ou,dc=domain,dc=com**.

    - Deshabilite la búsqueda de grupo anidada

      Especifica si se habilita o deshabilita la opción de búsqueda de grupos anidados. De forma predeterminada, esta opción está deshabilitada. Si utiliza Active Directory, puede acelerar la autenticación desactivando la compatibilidad con grupos anidados.

    - Utilice Conexión segura

      Especifica el servicio de autenticación utilizado para comunicarse con los servidores de autenticación.

  - **OpenLDAP**
    - Nombre distintivo del enlace

      Especifica el nombre distintivo del enlace que se utiliza junto con el nombre completo de la base para buscar usuarios remotos en el servidor de autenticación.

    - Enlazar contraseña

      Especifica la contraseña para acceder al servidor de autenticación.

    - Nombre completo base

Especifica la ubicación de los usuarios remotos en el servidor de autenticación. Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, entonces el nombre completo base es **cn=ou,dc=domain,dc=com**.

- Utilice Conexión segura

  Especifica que Secure LDAP se utiliza para comunicarse con servidores de autenticación LDAP.

- **Otros**
  - Nombre distintivo del enlace

    Especifica el nombre distintivo del enlace que se utiliza junto con el nombre completo de la base para buscar usuarios remotos en el servidor de autenticación configurado.

  - Enlazar contraseña

    Especifica la contraseña para acceder al servidor de autenticación.

  - Nombre completo base

    Especifica la ubicación de los usuarios remotos en el servidor de autenticación. Por ejemplo, si el nombre de dominio del servidor de autenticación es ou@domain.com, entonces el nombre completo base es **cn=ou,dc=domain,dc=com**.

  - Versión de protocolo

    Especifica la versión LDAP (Lightweight Directory Access Protocol) que admite el servidor de autenticación. Puede especificar si la versión del protocolo se debe detectar automáticamente o si se debe establecer la versión en 2 o 3.

  - Atributo Nombre de usuario

    Especifica el nombre del atributo en el servidor de autenticación que contiene nombres de inicio de sesión de usuario que el servidor de administración debe autenticar.

  - Atributo de pertenencia a grupos

    Especifica un valor que asigna la pertenencia al grupo del servidor de administración a usuarios remotos en función de un atributo y un valor especificado en el servidor de autenticación del usuario.

  - UGID

    Si los usuarios remotos se incluyen como miembros de un objeto GroupOfUniqueNames en el servidor de autenticación, esta opción permite asignar la pertenencia al grupo del servidor de administración a los usuarios remotos basándose en un atributo especificado en ese objeto GroupOfUniqueNames.

  - Deshabilite la búsqueda de grupo anidada

    Especifica si se habilita o deshabilita la opción de búsqueda de grupos anidados. De forma predeterminada, esta opción está deshabilitada. Si utiliza Active Directory, puede acelerar la autenticación desactivando la compatibilidad con grupos anidados.

- Miembro

  Especifica el nombre de atributo que el servidor de autenticación utiliza para almacenar información acerca de los miembros individuales de un grupo.

- Clase de objeto de usuario

  Especifica la clase de objeto de un usuario en el servidor de autenticación remota.

- Clase de objeto de grupo

  Especifica la clase de objeto de todos los grupos del servidor de autenticación remota.

> Los valores que especifique para los atributos *Member*, *User Object Class* y *Group Object Class* deben ser los mismos que los agregados en las configuraciones de Active Directory, OpenLDAP y LDAP. De lo contrario, es posible que se produzca un error en la autenticación.

- Utilice Conexión segura

  Especifica el servicio de autenticación utilizado para comunicarse con los servidores de autenticación.

> Si desea modificar el servicio de autenticación, asegúrese de eliminar los servidores de autenticación existentes y agregar nuevos servidores de autenticación.

Área servidores de autenticación

El área servidores de autenticación muestra los servidores de autenticación con los que se comunica el servidor de administración para buscar y autenticar usuarios remotos. El servidor de autenticación mantiene las credenciales de los usuarios o grupos remotos.

- **Botones de comando**

  Permite añadir, editar o eliminar servidores de autenticación.

  - Agregar

    Permite añadir un servidor de autenticación.

  Si el servidor de autenticación que va a agregar forma parte de un par de alta disponibilidad (con la misma base de datos), también puede agregar el servidor de autenticación asociado. Esto permite que el servidor de administración se comunique con el asociado cuando no se puede acceder a uno de los servidores de autenticación.

  - Editar

    Permite editar la configuración de un servidor de autenticación seleccionado.

  - Eliminar

    Elimina los servidores de autenticación seleccionados.

- **Nombre o dirección IP**

Muestra el nombre de host o la dirección IP del servidor de autenticación que se usa para autenticar al usuario en el servidor de administración.

- **Puerto**

  Muestra el número de puerto del servidor de autenticación.

- **Probar autenticación**

  Este botón valida la configuración del servidor de autenticación autenticando un usuario o grupo remoto.

  Durante las pruebas, si especifica sólo el nombre de usuario, el servidor de administración busca el usuario remoto en el servidor de autenticación, pero no lo autentica. Si especifica tanto el nombre de usuario como la contraseña, el servidor de gestión busca y autentica al usuario remoto.

  No se puede probar la autenticación si la autenticación remota está deshabilitada.

Gestión de certificados de seguridad

Puede configurar HTTPS en el servidor de Unified Manager para supervisar y gestionar los clústeres a través de una conexión segura.

Visualizar el certificado de seguridad HTTPS

Es posible comparar los detalles del certificado HTTPS con el certificado recuperado en el explorador para asegurarse de que la conexión cifrada del explorador con Unified Manager no se intercepte.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

La visualización del certificado permite verificar el contenido de un certificado regenerado o ver los nombres Alt (SAN) sujetos desde los que puede acceder a Unified Manager.

Paso

1. En el panel de navegación izquierdo, haga clic en **General** > **Certificado HTTPS**.

   El certificado HTTPS se muestra en la parte superior de la página

Si necesita ver información más detallada sobre el certificado de seguridad que la que aparece en la página Certificado HTTPS, puede ver el certificado de conexión en el explorador.

Descargar una solicitud de firma de certificación HTTPS

Puede descargar una solicitud de firma de certificación para el certificado de seguridad HTTPS actual para poder proporcionar el archivo a una entidad de certificación para firmar. Un certificado firmado por CA ayuda a evitar ataques de tipo "man in the middle" y proporciona una mejor protección de seguridad que un certificado autofirmado.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Certificado HTTPS**.
2. Haga clic en **Descargar la solicitud de firma de certificado HTTPS**.
3. Guarde la `<hostname>.csr` archivo.

Puede proporcionar el archivo a una entidad de certificación para firmar e instalar el certificado firmado.

Instalar una CA firmada y devolvió un certificado HTTPS

Puede cargar e instalar un certificado de seguridad después de que una entidad de certificación lo haya firmado y devuelto. El archivo que cargue e instale debe ser una versión firmada del certificado autofirmado existente. Un certificado firmado por CA ayuda a evitar los ataques de tipo "man in the middle" y ofrece una mejor protección de seguridad que un certificado autofirmado.

Lo que necesitará

Debe haber completado las siguientes acciones:

- Descargó el archivo de solicitud de firma de certificado y lo firmó una entidad de certificación
- Se guardó la cadena de certificados en formato PEM
- Se incluyeron todos los certificados en la cadena, desde el certificado de servidor de Unified Manager hasta el certificado de firma raíz, incluidos los certificados intermedios presentes

Debe tener la función Administrador de aplicaciones.

Si la validez del certificado para el que se creó una CSR es superior a 397 días, la CA reducirá la validez a 397 días antes de firmar y devolver el certificado

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Certificado HTTPS**.
2. Haga clic en **instalar certificado HTTPS**.
3. En el cuadro de diálogo que aparece, haga clic en **elegir archivo…** para localizar el archivo que se va a cargar.
4. Seleccione el archivo y haga clic en **instalar** para instalarlo.

   Para obtener más información, consulte "Instalar un certificado HTTPS generado con herramientas externas".

Ejemplo de cadena de certificados

El siguiente ejemplo muestra cómo puede aparecer el archivo de cadena de certificados:

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Instalar un certificado HTTPS generado con herramientas externas

Puede instalar certificados que están autofirmados o firmados por CA y que se generan con una herramienta externa como OpenSSL, BoringSSL o LetsEncrypt.

Debe cargar la clave privada junto con la cadena de certificados porque estos certificados son pares de claves pública-privada generados externamente. Los algoritmos de pares de claves permitidos son «'RSA'» y «'EC'». La opción **instalar certificado HTTPS** está disponible en la página certificados HTTPS de la sección General. El archivo que cargue debe tener el siguiente formato de entrada.

1. Clave privada del servidor que pertenece al host Active IQ Unified Manager
2. Certificado del servidor que coincide con la clave privada
3. Certificado de las CA en reverso hasta la raíz, que se utilizan para firmar el certificado anterior

Formato para cargar un certificado con un par de claves EC

Las curvas permitidas son «'prime256v1» y «slecp384r1». Ejemplo de certificado con un par de EC generado externamente:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----
```

Formato para cargar un certificado con un par de claves RSA

Los tamaños de claves permitidos del par de claves RSA que pertenece al certificado de host son 2048, 3072 y 4096. Certificado con un par de claves **RSA** generado externamente:

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

Una vez cargado el certificado, debe reiniciar la instancia de Active IQ Unified Manager para que los cambios se apliquen.

Comprueba la carga de certificados generados externamente

El sistema realiza comprobaciones mientras carga un certificado generado mediante herramientas externas. Si alguna de las comprobaciones falla, se rechaza el certificado. También se incluye una validación para los certificados generados a partir de la CSR dentro del producto y para los certificados generados mediante herramientas externas.

- La clave privada de la entrada se valida contra el certificado de host en la entrada.
- El nombre común (CN) del certificado de host se comprueba con el FQDN del host.

- El nombre común (CN) del certificado de host no debe estar vacío ni en blanco y no debe establecerse en localhost.
- La fecha de inicio de la validez no debe ser posterior y la fecha de caducidad del certificado no debe ser pasada.
- Si existe CA intermedia o CA, la fecha de inicio de validez del certificado no debe ser futura y la fecha de caducidad de validez no debe ser pasada.

La clave privada de la entrada no debe estar cifrada. Si hay claves privadas cifradas, el sistema las rechaza.

Ejemplo 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Ejemplo 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Ejemplo 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Descripciones de página para la gestión de certificados

Puede usar la página HTTPS Certificate para ver los certificados de seguridad actuales y generar certificados HTTPS nuevos.

Página HTTPS Certificate

En la página HTTPS Certificate, puede ver el certificado de seguridad actual, descargar una solicitud de firma de certificación, generar un certificado HTTPS autofirmado nuevo o instalar un certificado HTTPS nuevo.

Si no generó un certificado HTTPS autofirmado nuevo, el certificado que aparece en esta página es el certificado que se generó durante la instalación.

Botones de comando

Los botones de comando le permiten realizar las siguientes operaciones:

- **Descargar la solicitud de firma de certificado HTTPS**

  Descarga una solicitud de certificación para el certificado HTTPS instalado actualmente. El explorador le solicita que guarde el archivo <hostname>.csr para poder proporcionar el archivo a una entidad de certificación que desea firmar.

- **Instalar certificado HTTPS**

  Permite cargar e instalar un certificado de seguridad después de que una entidad de certificación lo haya firmado y devuelto. El nuevo certificado se aplicará después de reiniciar el servidor de gestión.

- **Regenerar certificado HTTPS**

  Permite generar un certificado HTTPS autofirmado nuevo, que reemplaza el certificado de seguridad actual. El nuevo certificado se aplica después de reiniciar Unified Manager.

Cuadro de diálogo Regenerate HTTPS Certificate

El cuadro de diálogo Regenerate HTTPS Certificate permite personalizar la información de seguridad y, a continuación, generar un nuevo certificado HTTPS con esa información.

La información del certificado actual aparece en esta página.

La selección "'Regenerate usando atributos de certificado actuales'" y "'Actualizar atributos de certificado actuales'" le permite regenerar el certificado con la información actual o generar un certificado con nueva información.

- **Nombre común**

  Obligatorio. El nombre de dominio completo (FQDN) que desea proteger.

  En las configuraciones de alta disponibilidad de Unified Manager, utilice la dirección IP virtual.

- **Correo electrónico**

  Opcional. Una dirección de correo electrónico para ponerse en contacto con su empresa; normalmente, la dirección de correo electrónico del administrador del certificado o del departamento DE TI.

- **Empresa**

  Opcional. Normalmente el nombre incorporado de su empresa.

- **Departamento**

  Opcional. El nombre del departamento de su empresa.

- * Ciudad*

  Opcional. Ubicación de la ciudad de su empresa.

- **Estado**

  Opcional. La ubicación del estado o provincia, no abreviada, de la compañía.

- **País**

  Opcional. Ubicación del país de su empresa. Este es típicamente un código ISO de dos letras del país.

- **Nombres alternativos**

  Obligatorio. Nombres de dominio adicionales no primarios que se pueden utilizar para tener acceso a este servidor además del host local u otras direcciones de red existentes. Cada nombre alternativo debe separarse con comas.

  Seleccione la casilla de verificación "'excluir información de identificación local (p. ej., localhost)'" si desea eliminar la información de identificación local del campo nombres alternativos del certificado. Cuando se selecciona esta casilla de verificación, sólo se utiliza el campo nombres alternativos lo que se introduce en el campo. Cuando se deja en blanco, el certificado resultante no tendrá ningún campo nombres alternativos.

- **TAMAÑO DE CLAVE (ALGORITMO DE CLAVE: RSA)**

  El algoritmo de clave está establecido en RSA. Puede seleccionar uno de los tamaños de clave: 2048, 3072 ó 4096 bits. El tamaño de clave predeterminado es de 2048 bits.

- **PERÍODO DE VALIDEZ**

  El período de validez predeterminado es de 397 días. Si ha actualizado desde una versión anterior, es posible que la validez del certificado anterior no cambie.

Para obtener más información, consulte "Generación de certificados HTTPS".

Supervisar y gestionar el almacenamiento

Introducción a Active IQ Unified Manager

Active IQ Unified Manager (anteriormente Unified Manager de OnCommand) le permite supervisar y gestionar el estado y el rendimiento de sus sistemas de almacenamiento de ONTAP desde una única interfaz.

Unified Manager proporciona las siguientes funciones:

- Detección, supervisión y notificaciones de los sistemas instalados con el software ONTAP.
- Panel para mostrar el estado de la capacidad, la seguridad y el rendimiento del entorno.
- Alertas mejoradas, eventos e infraestructura de umbral.
- Muestra gráficos detallados que traza la actividad de las cargas de trabajo con el tiempo; incluidos IOPS (operaciones), Mbps (rendimiento), latencia (tiempo de respuesta), utilización, la capacidad de rendimiento y la proporción de caché.
- Identifica cargas de trabajo que utilizan en exceso los componentes del clúster y las cargas de trabajo cuyo rendimiento se ve afectado por la mayor actividad.
- Proporciona acciones correctivas sugeridas que se pueden realizar para solucionar ciertos incidentes y eventos, y botón "solucionarlo" para algunos eventos, de modo que pueda resolver el problema de inmediato.
- Se integra con OnCommand Workflow Automation para ejecutar flujos de trabajo de protección automatizados.
- Capacidad para crear nuevas cargas de trabajo, como un LUN o un recurso compartido de archivos, directamente desde Unified Manager y asignar un nivel de servicio de rendimiento para definir los objetivos de rendimiento y almacenamiento para los usuarios que acceden a la aplicación utilizando dicha carga de trabajo.

Introducción a la supervisión del estado de Active IQ Unified Manager

Active IQ Unified Manager (anteriormente Unified Manager de OnCommand) le ayuda a supervisar un gran número de sistemas que ejecutan el software ONTAP a través de una interfaz de usuario centralizada. La infraestructura de servidor de Unified Manager proporciona escalabilidad y compatibilidad, así como funcionalidades mejoradas de supervisión y notificación.

Las funciones clave de Unified Manager incluyen la supervisión, la alerta, la gestión de la disponibilidad y la capacidad de los clusters, la gestión de las capacidades de protección, y la agrupación de datos de diagnóstico y el envío de estos a soporte técnico.

Puede usar Unified Manager para supervisar los clústeres. Cuando se producen problemas en el clúster, Unified Manager notifica los detalles de estos problemas mediante eventos. Algunos eventos también le proporcionan una acción correctiva que puede tomar para resolver los problemas. Es posible configurar alertas para eventos que, cuando se produzcan problemas, se le notificarán por correo electrónico y capturas SNMP.

Puede utilizar Unified Manager para gestionar objetos de almacenamiento en el entorno asociándolos con anotaciones. Puede crear anotaciones personalizadas y asociar de forma dinámica clústeres, máquinas

virtuales de almacenamiento (SVM) y volúmenes con las anotaciones mediante las reglas.

También puede planificar los requisitos de almacenamiento de los objetos de clúster mediante la información proporcionada en los gráficos de capacidad y estado del objeto de clúster correspondiente.

Capacidad física y lógica

Unified Manager utiliza los conceptos de espacio físico y lógico utilizados para objetos de almacenamiento de ONTAP.

- Capacidad física: El espacio físico se refiere a los bloques físicos del almacenamiento que se usa en el volumen. La «capacidad física utilizada» suele ser menor que la capacidad lógica utilizada debido a la reducción de datos de las funciones de eficiencia del almacenamiento (como la deduplicación y la compresión).
- Capacidad lógica: El espacio lógico se refiere al espacio utilizable (los bloques lógicos) de un volumen. El espacio lógico hace referencia a cómo se puede utilizar el espacio teórico, sin tener en cuenta los resultados de la deduplicación o la compresión. El “espacio lógico utilizado” es el espacio físico utilizado más el ahorro que se obtiene gracias a las funciones de eficiencia del almacenamiento (como la deduplicación y compresión) que se han configurado. Esta medición suele ser mayor que la capacidad física utilizada porque incluye copias Snapshot, clones y otros componentes, y no refleja la compresión de datos ni otras reducciones del espacio físico. Por lo tanto, la capacidad lógica total podría ser mayor que el espacio aprovisionado.

Unidades de medida de capacidad

Unified Manager calcula la capacidad de almacenamiento en función de unidades binarias de 1024 (2 10) bytes. En ONTAP 9.10.0 y anteriores, estas unidades se mostraban como KB, MB, GB, TB y PB. A partir de ONTAP 9.10.1, se muestran en Unified Manager como KiB, MIB, GIB, TIB y PIB.

Las unidades utilizadas para el rendimiento continúan siendo kilobytes por segundo (Kbps), megabytes por segundo (Mbps), gigabytes por segundo (Gbps) o terabytes por segundo (Tbps), etc., para todas las versiones de ONTAP.

La unidad de capacidad se muestra en Unified Manager para ONTAP 9.10.0 y versiones anteriores	La unidad de capacidad se muestra en Unified Manager para ONTAP 9.10.1	Cálculo	Valor en bytes
KB	KiB	1024	1024 bytes
MB	MIB	1024 * 1024	1,048,576 bytes
GB	GIB	1024 * 1024 * 1024	1,073,741,824 bytes
TB	TIB	1024 * 1024 * 1024 * 1024	1,099,511,627,776 bytes

Introducción a la supervisión del rendimiento de Active IQ Unified Manager

Active IQ Unified Manager (anteriormente Unified Manager de OnCommand) proporciona

funcionalidades de supervisión del rendimiento y análisis de eventos raíz para sistemas que ejecutan el software ONTAP de NetApp.

Unified Manager le ayuda a identificar cargas de trabajo que están utilizando de forma excesiva los componentes del clúster y a reducir el rendimiento de otras cargas de trabajo del clúster. Al definir las políticas de umbral de rendimiento, también se pueden especificar valores máximos de determinados contadores de rendimiento para que los eventos se generen cuando se supera el umbral. Unified Manager le alerta sobre estos eventos de rendimiento para poder realizar acciones correctivas y devolver el rendimiento a los niveles normales de funcionamiento. Los eventos se pueden ver y analizar en la interfaz de usuario de Unified Manager.

Unified Manager supervisa el rendimiento de dos tipos de cargas de trabajo:

- Cargas de trabajo definidas por el usuario

  Estas cargas de trabajo constan de volúmenes de FlexVol y volúmenes de FlexGroup creados en el clúster.

- Cargas de trabajo definidas por el sistema

  Estas cargas de trabajo constan de una actividad interna del sistema.

Usar API de REST de Unified Manager

Active IQ Unified Manager le proporciona API DE REST para ver la información sobre la supervisión y la gestión de su entorno de almacenamiento. Las API también permiten aprovisionar y gestionar objetos de almacenamiento basados en políticas.

También puede ejecutar API de ONTAP en todos los clústeres gestionados por ONTAP usando la puerta de enlace API compatible con Unified Manager.

Para obtener información sobre las API DE REST de Unified Manager, consulte "Primeros pasos con API de REST de Active IQ Unified Manager".

Lo que hace Unified Manager Server

La infraestructura de servidor de Unified Manager consta de una unidad de recogida de datos, una base de datos y un servidor de aplicaciones. Proporciona servicios de infraestructura como detección, supervisión, control de acceso basado en roles (RBAC), auditoría y registro.

Unified Manager recopila información del clúster, almacena los datos en la base de datos y analiza los datos para ver si hay algún problema con el clúster.

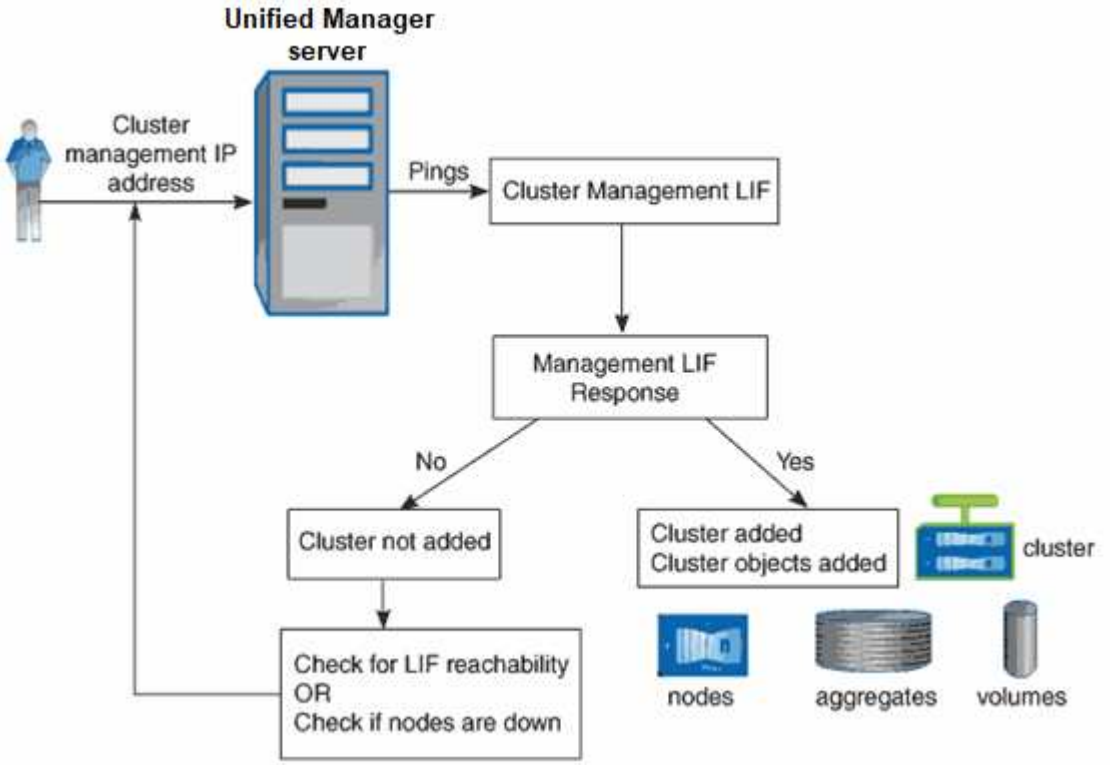
Cómo funciona el proceso de detección

Después de agregar el clúster a Unified Manager, el servidor detecta los objetos del clúster y los añade a su base de datos. Comprender cómo funciona el proceso de detección le permite gestionar los clústeres de su organización y sus objetos.

El intervalo de supervisión predeterminado es de 15 minutos: Si ha agregado un clúster al servidor de Unified

Manager, se tardan 15 minutos en mostrar los detalles del clúster en la interfaz de usuario de Unified Manager.

En la siguiente imagen se muestra el proceso de detección en Active IQ Unified Manager:



La interfaz de usuario

La interfaz de usuario de Unified Manager se compone principalmente de un panel que ofrece una vista general de los objetos supervisados. La interfaz de usuario también proporciona acceso a la visualización de todos los objetos del clúster.

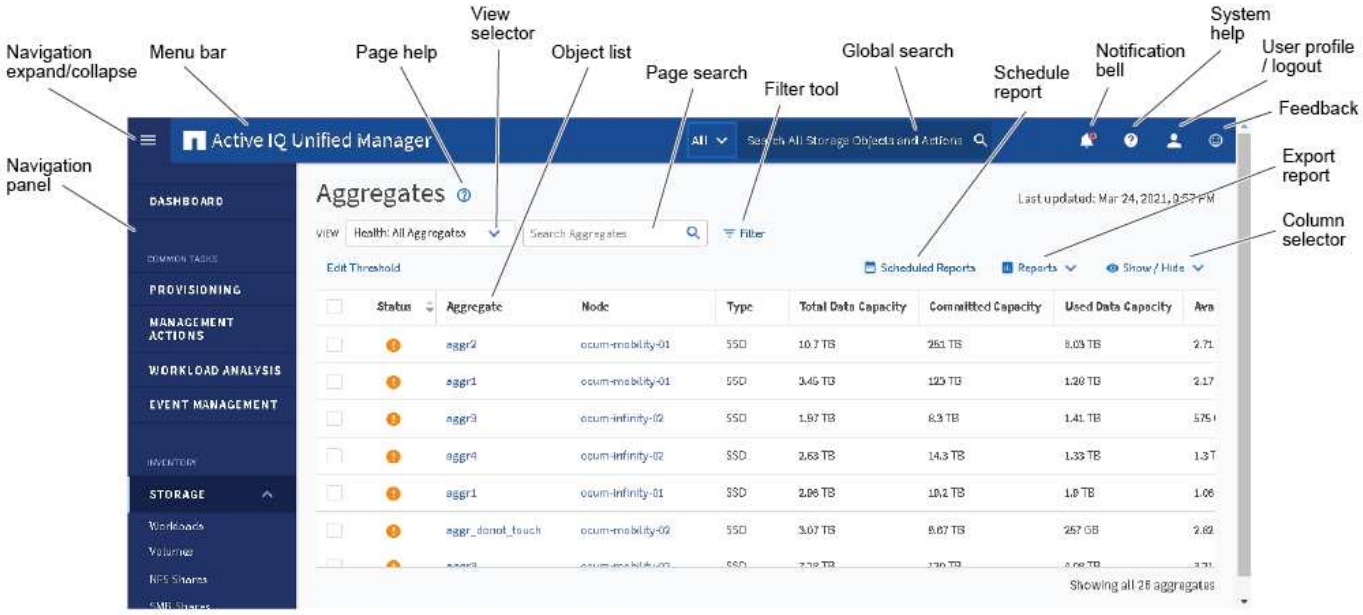
Puede seleccionar una vista preferida y utilizar los botones de acción según sea necesario. La configuración de pantallas se guarda en un espacio de trabajo, de modo que todas las funcionalidades necesarias se encuentren disponibles al iniciar Unified Manager. Sin embargo, es posible que cuando se navega desde una vista a otra y se navega hacia atrás, la vista no sea la misma.

Diseños de ventana típicos

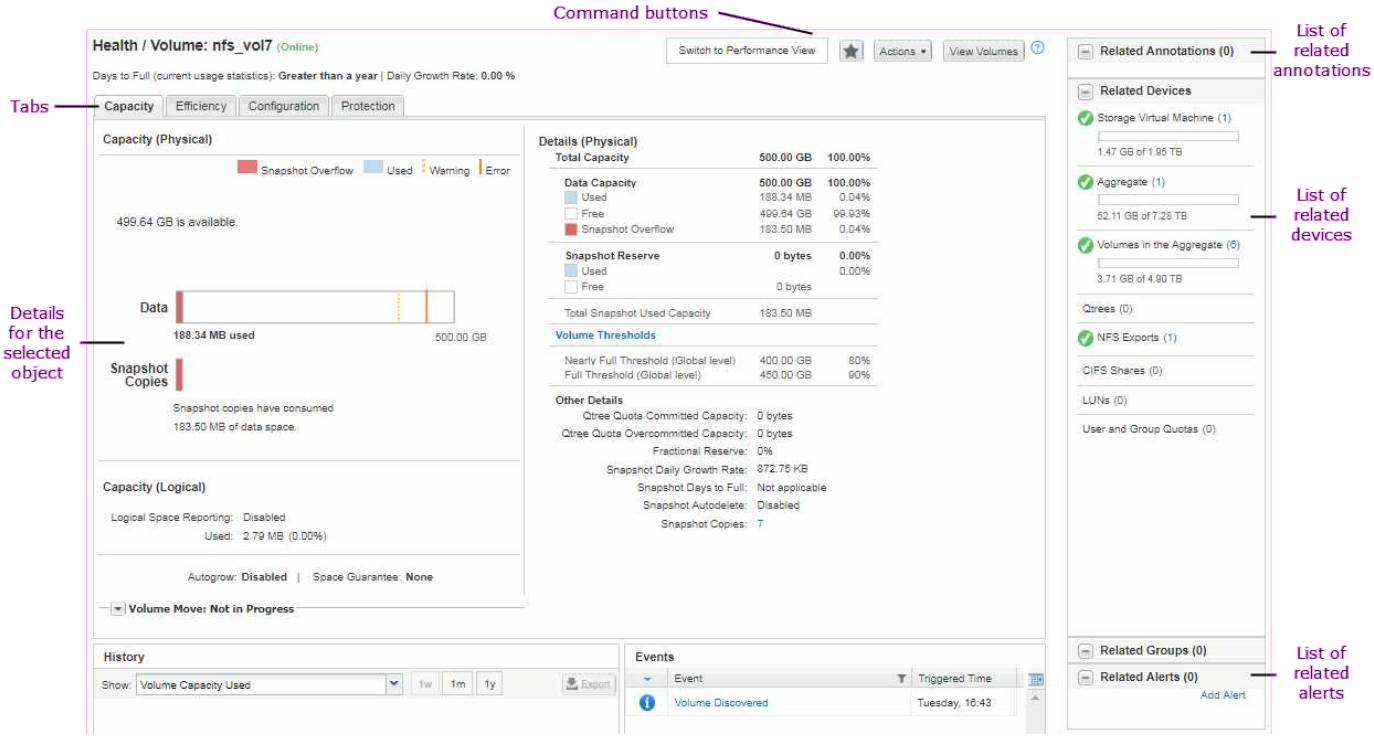
Comprender los diseños de ventana típicos le ayuda a navegar y utilizar Active IQ Unified Manager de forma eficaz. La mayoría de ventanas de Unified Manager son similares a una de dos distribuciones generales: Lista de objetos o detalles. La configuración de visualización recomendada es de al menos 1280 por 1024 píxeles.

No todas las ventanas contienen todos los elementos de los diagramas siguientes.

Diseño de la ventana de lista de objetos



Diseño de la ventana de detalles del objeto



Personalización del diseño de ventanas

Active IQ Unified Manager le permite personalizar el diseño de la información en las páginas de objetos de almacenamiento y red. Al personalizar las ventanas, puede controlar qué datos se ven y cómo se muestran.

- **Clasificación**

  Puede hacer clic en el encabezado de la columna para cambiar el orden de clasificación de las entradas

de la columna. Al hacer clic en el encabezado de la columna, las flechas de ordenación (y..) aparece para esa columna.

- **Filtrado**

  Se puede hacer clic en el icono de filtro ( ) aplicar filtros para personalizar la visualización de información en las páginas de objetos de almacenamiento y red de modo que sólo se muestren las entradas que coincidan con las condiciones proporcionadas. Aplica filtros desde el panel Filtros.

  El panel Filtros permite filtrar la mayoría de las columnas en función de las opciones seleccionadas. Por ejemplo, en la vista Estado: Todos los volúmenes, puede usar el panel Filtros para mostrar todos los volúmenes que están sin conexión. Para ello, seleccione la opción de filtro adecuada en Estado.

  Las columnas relacionadas con la capacidad de cualquier lista siempre muestran datos de capacidad en unidades adecuadas redondeadas a dos puntos decimales. Esto también se aplica al filtrar columnas de capacidad. Por ejemplo, si utiliza el filtro en la columna total Data Capacity de la vista Estado: Todos los agregados para filtrar datos por encima de 20.45 GB, la capacidad real de 20.454 GB se muestra como 20.45 GB. Del mismo modo, si filtra datos de menos de 20.45 GB, la capacidad real de 20.449 GB se muestra como 20.45 GB.

  Si utiliza el filtro de la columna Available Data % en la vista Health: All Aggregates para filtrar datos superiores al 20.45 %, la capacidad real del 20.454 % se muestra como 20.45 %. De la misma manera, si filtra datos menos del 20.45%, la capacidad real del 20.449% se muestra como 20.45%.

- **Ocultar o mostrar las columnas**

  Puede hacer clic en el icono de visualización de columna (**Mostrar/Ocultar**) para seleccionar las columnas que desea mostrar. Una vez que haya seleccionado las columnas adecuadas, puede volver a ordenarlas arrastrándolas con el ratón.

- **Buscando**

  Puede utilizar el cuadro de búsqueda para buscar ciertos atributos de objeto para ayudar a refinar la lista de elementos de la página de inventario. Por ejemplo, puede introducir la palabra "cloud" para refinar la lista de volúmenes de la página del inventario Volumes para ver todos los volúmenes que tienen la palabra "cloud".

- **Exportación de datos**

  Puede hacer clic en el botón **Informes** (o en el botón **Exportar** para exportar datos a valores separados por comas `(.csv)` archivo, `(.pdf)` Document o Microsoft Excel `(.xlsx)` archivar y utilizar los datos exportados para generar informes.

Uso de la ayuda de Unified Manager

La Ayuda incluye información acerca de todas las funciones incluidas en Active IQ Unified Manager. Puede utilizar la tabla de contenido, el índice o la herramienta de búsqueda para buscar información acerca de las funciones y cómo utilizarlas.

La ayuda se encuentra disponible en cada pestaña y en la barra de menú de la interfaz de usuario de Unified Manager.

La herramienta de búsqueda de la Ayuda no funciona para palabras parciales.

- Para obtener información acerca de campos o parámetros específicos, haga clic en .
- Para ver todo el contenido de la Ayuda, haga clic en > **Ayuda/Documentación** en la barra de menús.

  Puede encontrar información más detallada ampliando cualquier parte del índice en el panel de navegación.

- Para buscar en el contenido de la Ayuda, haga clic en la ficha **Buscar** del panel de navegación, escriba la palabra o serie de palabras que desea encontrar y haga clic en **Ir**
- Para imprimir temas de Ayuda, haga clic en el icono de impresora.

Guardado de marcadores de sus temas favoritos de la Ayuda

En la ficha Favoritos de ayuda, puede marcar los temas de Ayuda que utiliza con frecuencia. Ayude a los marcadores a proporcionar un acceso rápido a sus temas favoritos.

Pasos

1. Desplácese al tema de Ayuda que desea agregar como favorito.
2. Haga clic en **Favoritos** y, a continuación, haga clic en **Agregar**.

Buscar objetos de almacenamiento

Para acceder rápidamente a un objeto específico, puede utilizar el campo **Buscar todos los objetos de almacenamiento** situado en la parte superior de la barra de menús. Este método de búsqueda global en todos los objetos le permite localizar rápidamente objetos específicos por tipo. Los resultados de búsqueda se ordenan por tipo de objeto de almacenamiento y puede filtrarlos aún más por objeto mediante el menú desplegable.

Lo que necesitará

- Debe tener una de las siguientes funciones para realizar esta tarea: Operador, Administrador de aplicaciones o Administrador de almacenamiento.
- Una búsqueda válida debe contener al menos tres caracteres.

Al utilizar el valor del menú desplegable "todo", la búsqueda global muestra el número total de resultados encontrados en todas las categorías de objetos; con un máximo de 25 resultados de búsqueda para cada categoría de objetos. Puede seleccionar un tipo de objeto específico en el menú desplegable para restringir la búsqueda dentro de un tipo de objeto específico. En este caso, la lista devuelta no está restringida a los 25 objetos principales.

Entre los tipos de objeto que puede buscar se incluyen:

- De clúster
- Nodos
- Máquinas virtuales de almacenamiento
- Agregados
- Volúmenes
- Qtrees

- Recursos compartidos de SMB
- Recursos compartidos de NFS
- Cuotas de usuarios o grupos
- LUN
- Espacios de nombres de NVMe
- IGroups
- Iniciadores
- Grupo de consistencia

Introducir un nombre de carga de trabajo muestra la lista de cargas de trabajo en la categoría de volúmenes o LUN apropiados.

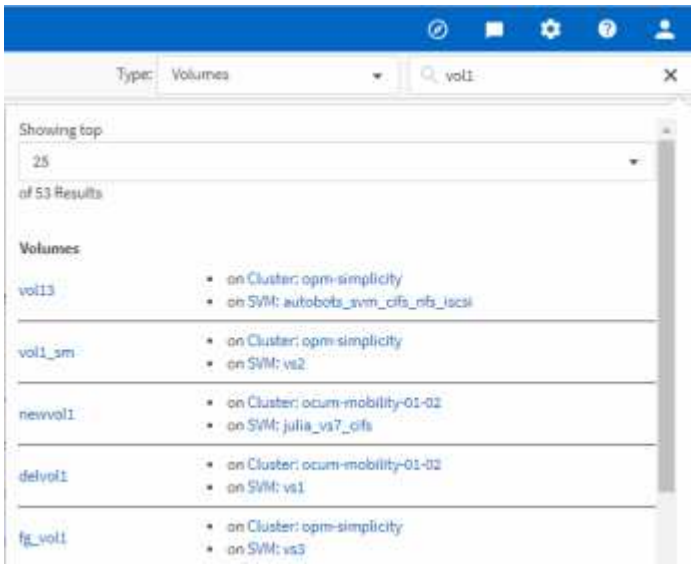
Es posible hacer clic en cualquier objeto de los resultados de búsqueda para ir a la página de detalles Health del objeto. Si no hay ninguna página de estado directa para un objeto, se muestra la página Estado del objeto primario. Por ejemplo, al buscar un LUN específico, se muestra la página de detalles de la SVM en la que reside el LUN.

No se pueden realizar búsquedas en los puertos y las LIF en la barra de búsqueda global.

Pasos

1. Seleccione un tipo de objeto en el menú para afinar los resultados de búsqueda sólo para un único tipo de objeto.
2. Escriba un mínimo de tres caracteres del nombre del objeto en el campo **Buscar todos los objetos de almacenamiento**.

   En este ejemplo, el cuadro desplegable tiene seleccionado el tipo de objeto Volumes. Al escribir "vol1" en el campo **Buscar todos los objetos de almacenamiento** se muestra una lista de todos los volúmenes cuyos nombres contienen estos caracteres.



Exportar datos de almacenamiento como informes

Puede exportar datos de almacenamiento en distintos formatos de salida y, a

continuación, utilizar los datos exportados para generar informes. Por ejemplo, si hay 10 eventos críticos que no se han resuelto, puede exportar los datos desde la página del inventario de Event Management para crear un informe y, a continuación, enviar el informe a los administradores que puedan resolver los problemas.

Puede exportar datos a un `.csv` archivo, `.xlsx` archivo, o. `.pdf` Documente las páginas de inventario **almacenamiento** y **Red** y utilice los datos exportados para generar informes. Hay otras ubicaciones en el producto donde sólo `.csv` o. `.pdf` se pueden generar archivos.

Pasos

1. Ejecute una de las siguientes acciones:

Si desea exportar…	Realice lo siguiente…
Detalles del inventario de objetos de almacenamiento	Haga clic en **almacenamiento** o **Red** en el menú de navegación de la izquierda y, a continuación, seleccione un objeto de almacenamiento. Elija una de las vistas proporcionadas por el sistema o cualquier vista personalizada que haya creado.
Detalles del grupo de políticas de QoS	Haga clic en **almacenamiento** > **grupos de políticas QoS** en el menú de navegación de la izquierda.
Detalles del historial de protección y capacidad de almacenamiento	Haga clic en **almacenamiento** > **agregados** o **almacenamiento** > **volúmenes** y, a continuación, seleccione un único agregado o volumen.
Detalles del evento	Haga clic en **Gestión de eventos** en el menú de navegación de la izquierda.
Objetos de almacenamiento: Detalles de rendimiento de los 10 mejores	Haga clic en **almacenamiento** > **Clusters** > **Performance:All Clusters**, seleccione un clúster y elija la ficha **Top Performers**. A continuación, seleccione un objeto de almacenamiento y un contador de rendimiento.

2. Haga clic en el botón **Informes** (o en el botón **Exportar** de algunas páginas de la interfaz de usuario).
3. Haga clic en **Descargar CSV**, **Descargar PDF** o **Descargar Excel** para confirmar la solicitud de exportación.

   En la pestaña Top Performers, es posible elegir descargar un informe de las estadísticas del clúster único que está viendo o de todos los clústeres del centro de datos.

   Se descarga el archivo.

4. Abra el archivo en la aplicación correspondiente.

Información relacionada

"Página del inventario Health/Clusters"

"Programar un informe"

Filtrado del contenido de la página de inventario

Puede filtrar los datos de las páginas de inventario en Unified Manager para localizar rápidamente datos según criterios específicos. Puede utilizar el filtrado para limitar el contenido de las páginas de Unified Manager a fin de mostrar únicamente los resultados de los que está interesado. Esto proporciona un método muy eficiente para mostrar sólo los datos en los que usted está interesado.

Utilice **filtrado** para personalizar la vista de cuadrícula en función de sus preferencias. Las opciones de filtro disponibles se basan en el tipo de objeto que se está viendo en la cuadrícula. Si se aplican filtros actualmente, el número de filtros aplicados se muestra a la derecha del botón filtro.

Se admiten tres tipos de parámetros de filtro.

Parámetro	Validación
Cadena (texto)	Los operadores son **contiene**, **comienza con**, **termina con** y **no contiene**.
Número	Los operadores son **superiores a**, **inferiores a**, **en el último** y **entre**.
Enumeración (texto)	Los operadores son **is** y **no**.

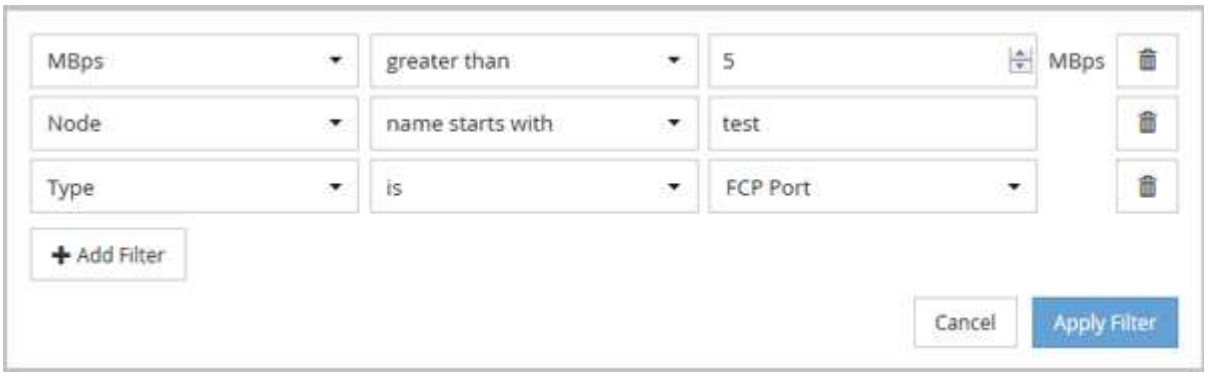
Los campos columna, operador y valor son necesarios para cada filtro; los filtros disponibles reflejan las columnas filtrables en la página actual. El número máximo de filtros que puede aplicar es cuatro. Los resultados filtrados se basan en parámetros de filtro combinados. Los resultados filtrados se aplican a todas las páginas de la búsqueda filtrada, no sólo a la página mostrada actualmente.

Puede agregar filtros mediante el panel filtrado.

1. En la parte superior de la página, haga clic en el botón **filtro**. Aparecerá el panel filtrado.
2. Haga clic en la lista desplegable que se encuentra a la izquierda y seleccione un objeto; por ejemplo, *Cluster* o un contador de rendimiento.
3. Haga clic en la lista desplegable Centro y seleccione el operador que desee utilizar.
4. En la última lista, seleccione o escriba un valor para completar el filtro de ese objeto.
5. Para agregar otro filtro, haga clic en **+Agregar filtro**. Aparecerá un campo de filtro adicional. Complete este filtro utilizando el proceso descrito en los pasos anteriores. Tenga en cuenta que al agregar el cuarto filtro, el botón **+Agregar filtro** ya no aparece.
6. Haga clic en **aplicar filtro**. Las opciones de filtro se aplican a la cuadrícula y el número de filtros se muestra a la derecha del botón filtro.
7. Utilice el panel filtrado para eliminar filtros individuales haciendo clic en el icono de papelera situado a la derecha del filtro que se va a eliminar.
8. Para eliminar todos los filtros, haga clic en **Restablecer** en la parte inferior del panel de filtrado.

Ejemplo de filtrado

La ilustración muestra el panel filtrado con tres filtros. El botón **+Add Filter** aparece cuando tiene menos de cuatro filtros como máximo.



Después de hacer clic en **aplicar filtro**, el panel filtrado se cierra, aplica los filtros y muestra el número de filtros aplicados (3).

Ver eventos activos desde el timbre de notificación

El timbre de notificación ( ) En la barra de menú proporciona una forma rápida de ver los eventos activos más importantes que Unified Manager realiza el seguimiento.

La lista de eventos activos permite ver el número total de eventos críticos, de error, de advertencia y de actualización en todos los clústeres. Esta lista incluye eventos de los 7 días anteriores y no incluye eventos de información. Puede hacer clic en un enlace para mostrar la lista de los eventos que más le interesen.

Tenga en cuenta que, cuando no se puede acceder a un clúster, Unified Manager muestra esta información en esta página. Puede ver información detallada sobre un clúster que no se puede acceder haciendo clic en el botón **Detalles**. Con esta acción se abre la página de detalles Event. En esta página también se muestran los problemas de monitorización de escala, como poco espacio o RAM en la estación de administración.

Pasos

1. En la barra de menú, haga clic en .
2. Para ver los detalles de cualquiera de los eventos activos, haga clic en el enlace de texto del evento, como "2 capacidad" o "4 rendimiento".

Supervisar y gestionar clústeres desde la consola

La consola ofrece información acumulativa de un vistazo sobre el estado actual de los sistemas de ONTAP supervisados. El panel proporciona ""paneles"" que le permiten evaluar la capacidad general, el rendimiento y el estado de seguridad de los clústeres que supervisa.

Además, existen ciertos problemas de ONTAP que se pueden solucionar directamente desde la interfaz de usuario de Unified Manager en lugar de tener que utilizar System Manager de ONTAP o la interfaz de línea de comandos de ONTAP.

En la parte superior de la consola puede seleccionar si los paneles muestran información para todos los clústeres supervisados o para un clúster individual. Para empezar, puede ver el estado de todos los clústeres

y profundizar en cada clúster cuando desea ver información detallada.

Es posible que algunos de los paneles que se enumeran a continuación no aparezcan en la página en función de su configuración.

Paneles	Descripción
Acciones de gestión	Cuando Unified Manager puede diagnosticar y determinar una única resolución de un problema, estas resoluciones se muestran en este panel con un botón **Fix it**.
Capacidad	Muestra la capacidad total y utilizada para el nivel local y el nivel cloud, así como la cantidad de días hasta que la capacidad local alcance el límite superior.
Capacidad de rendimiento	Muestra el valor de la capacidad de rendimiento de cada clúster y el número de días hasta que la capacidad de rendimiento alcanza el límite superior.
IOPS de carga de trabajo	Muestra el número total de cargas de trabajo que se están ejecutando actualmente en un determinado rango de IOPS.
Rendimiento de carga de trabajo	Muestra el número total de cargas de trabajo conformes y no conformes asignadas a cada nivel de servicio de rendimiento definido.
Seguridad	Muestra el número de clústeres que son compatibles o no, el número de SVM que son compatibles o no, y el número de volúmenes cifrados o no.
Protección	Muestra la cantidad de máquinas virtuales de almacenamiento protegidas por la relación SVM-DR, los volúmenes protegidos por la relación de SnapMirror, los volúmenes protegidos por Snapshot y los clústeres protegidos por MetroCluster.
Descripción del uso	Muestra los clústeres ordenados por las IOPS más altas, el rendimiento más alto (Mbps) o la capacidad física utilizada más alta.

Consola

La página Dashboard tiene "paneles" que muestran el estado de alta capacidad, rendimiento y seguridad de los clústeres que se supervisan. Esta página también proporciona un panel Management Actions que enumera las correcciones que Unified Manager puede realizar para resolver ciertos eventos.

La mayoría de los paneles también muestran el número de eventos activos de esa categoría y el número de eventos nuevos añadidos a las 24 horas anteriores. Esta información le ayuda a decidir qué clústeres se podrían necesitar para analizar más a fin de resolver eventos. Al hacer clic en los eventos, se muestran los eventos principales y se proporciona un enlace a la página del inventario Event Management filtrada para mostrar los eventos activos de esa categoría.

En la parte superior de la consola puede seleccionar si los paneles muestran información de todos los clústeres supervisados ("todos los clústeres") o de un clúster individual. Para empezar, puede ver el estado de todos los clústeres y profundizar en cada clúster cuando desea ver información detallada.

Algunos de los paneles que se enumeran a continuación aparecen en el panel de control en función de su configuración.

Panel de acciones de gestión

Hay ciertos problemas que Unified Manager puede diagnosticar a fondo y proporcionar una única resolución. Si están disponibles, estas resoluciones se muestran en este panel con un botón **Fix it** o **Fix All**. Es posible solucionar estos problemas inmediatamente desde Unified Manager, en lugar de tener que utilizar ONTAP System Manager o la CLI de ONTAP. Para ver todos los problemas, haga clic en Ver "Solución de problemas de ONTAP directamente desde Unified Manager" si quiere más información.

Panel capacidad

Al ver todos los clústeres, este panel muestra la capacidad física utilizada (tras aplicar ahorros de eficiencia del almacenamiento) y la capacidad física disponible (sin incluir el potencial ahorro de eficiencia del almacenamiento) para cada clúster, el número de días que se prevé que los discos se llenen, La tasa de reducción de datos basada en la configuración de eficiencia del almacenamiento de ONTAP configurada. También incluye la capacidad utilizada para los niveles de cloud que haya configurado. Al hacer clic en el gráfico de barras irá la página del inventario de agregados para ese clúster. Al hacer clic en el texto "Days to Full" se muestra un mensaje que identifica el agregado con la menor cantidad de días de capacidad restantes; haga clic en el nombre del agregado para ver más detalles.

Al ver un único clúster, este panel muestra la capacidad física utilizada y la capacidad física disponible de los agregados de datos ordenados por cada tipo de disco individual del nivel local y del nivel de cloud. Al hacer clic en el gráfico de barras de un tipo de disco, se abre la página de inventario de volúmenes de los volúmenes que usan ese tipo de disco.

Panel rendimiento capacidad

Cuando se visualizan todos los clústeres, este panel muestra el valor de capacidad de rendimiento de cada clúster (promediado en la 1 hora anterior) y el número de días hasta que la capacidad de rendimiento alcance el límite superior (según la tasa de crecimiento diaria). Al hacer clic en el gráfico de barras, irá la página del inventario de nodos de ese clúster. Tenga en cuenta que la página del inventario de nodos muestra la capacidad de rendimiento media de las 72 horas anteriores. Al hacer clic en el texto "Days to Full" se muestra un mensaje que identifica el nodo con la menor cantidad de días de capacidad de rendimiento restantes; haga clic en el nombre del nodo para ver más detalles.

Al ver un único clúster, este panel muestra los valores de porcentaje de capacidad de rendimiento del clúster utilizada, de IOPS totales y de rendimiento total (MB/s), así como el número de días que tardan en alcanzar el límite superior de cada una de estas tres métricas.

Panel Workload IOPS

Al ver un solo clúster, este panel muestra el número total de cargas de trabajo que se están ejecutando actualmente en un determinado rango de IOPS e indica el número de cada tipo de disco cuando pasa el cursor por encima del gráfico.

Panel Workload Performance

Este panel muestra el número total de cargas de trabajo conformes y no conformes que se asignan a cada política de nivel de servicio de rendimiento (PSL). También muestra la cantidad de cargas de trabajo a las que no se asigna una PSL. Al hacer clic en un gráfico de barras, se le llevan a las cargas de trabajo conformes asignadas a esa política en la página de cargas de trabajo. Al hacer clic en el número que sigue al gráfico de barras, se muestran las cargas de trabajo conformes y no conformes asignadas a esa política.

Panel de seguridad

El panel Seguridad presenta el estado de seguridad de alto nivel para todos los clústeres o un único clúster, según la vista actual. Este panel muestra:

- una lista de los eventos de seguridad recibidos en las últimas 24 horas. Haga clic en un evento para ver los detalles en la página de detalles Event
- el estado de seguridad del clúster (recuento de clústeres compatibles y no compatibles)
- El estado de seguridad de los equipos virtuales de almacenamiento (recuento de equipos virtuales de almacenamiento que cumplen las normativas y no cumplen las normativas).
- el estado de cifrado de volúmenes (número de volúmenes cifrados o no cifrados).
- el estado del volumen antiransomware (recuento de volúmenes con antiransomware que están habilitados o deshabilitados).

Puede hacer clic en los gráficos de barras de los clústeres conformes a la normativa y no conformes a la normativa, VM de almacenamiento, volúmenes cifrados y estado del antivirus de volúmenes, para acceder a las páginas respectivas y ver los detalles de seguridad de los clústeres filtrados, las máquinas virtuales de almacenamiento y los volúmenes.

El cumplimiento se basa en "Guía de fortalecimiento de la seguridad de NetApp para ONTAP 9"la . Haga clic en la flecha derecha de la parte superior del panel para ver los detalles de seguridad de todos los clústeres de la página Seguridad. Para obtener más información, consulte "Visualización detallada del estado de seguridad para clústeres y máquinas virtuales de almacenamiento".

Panel Data Protection

Este panel muestra el resumen de protección de datos de uno o todos los clústeres de un centro de datos. Se muestra el número total de eventos de protección de datos, eventos de MetroCluster y el número de eventos activos generados en las últimas 24 horas en ONTAP. Al hacer clic en el enlace de cada uno de estos eventos, se abre la página de detalles Event. Puede hacer clic en el enlace **Ver todo** para ver todos los eventos de protección activos en la página de inventario de Event Management. El panel muestra:

- La cantidad de volúmenes en un clúster o todos los clústeres de un centro de datos protegido por copias de Snapshot.
- La cantidad de volúmenes en un clúster o todos los clústeres de un centro de datos protegido por relaciones de SnapMirror. Para las relaciones de SnapMirror, se considera el número de volúmenes en el clúster de origen.
- La cantidad de clústeres o todos los clústeres de un centro de datos protegido por la configuración de

MetroCluster sobre IP o FC.

- El número de relaciones de volumen con el objetivo de punto de recuperación (RPO) de SnapMirror está desfase en función del estado de desfase.

Puede pasar el ratón sobre el mismo para ver los recuentos y leyendas correspondientes. Puede hacer clic en la flecha derecha de la parte superior del panel para ver los detalles de uno o todos los clústeres de la página Data Protection. También puede hacer clic en:

- Los gráficos de barras de volúmenes no protegidos y volúmenes protegidos por copias Snapshot para ir a la página Volumes y ver los detalles.
- Los gráficos de barras de los clústeres protegidos o no están protegidos por la configuración de MetroCluster para ir a la página Clusters y ver los detalles.
- Los gráficos de barras de todas las relaciones se van a la página Relaciones, donde se filtran los detalles en función del clúster de origen.

Para obtener más información, consulte "Ver el estado de protección de volumen".

Panel de descripción del uso

Al ver todos los clústeres, puede elegir ver clústeres ordenados por IOPS más alta, mayor rendimiento (MB/s) o mayor capacidad física utilizada.

Al ver un único clúster, puede elegir ver cargas de trabajo ordenadas por IOPS más alta, mayor rendimiento (MB/s) o mayor capacidad lógica utilizada.

Información relacionada

"Solución de problemas mediante soluciones automáticas de Unified Manager"

"Mostrar información acerca de los eventos de rendimiento"

"Gestión del rendimiento mediante la capacidad de rendimiento y la información de IOPS disponible"

"Página de detalles Volume / Health"

"Análisis y notificación de eventos de rendimiento"

"Descripción de los tipos de gravedad de los eventos"

"Fuentes de eventos de rendimiento"

"Gestión de los objetivos de seguridad del clúster"

"Supervisar el rendimiento del clúster en la página Performance Cluster Landing"

"Supervisión del rendimiento mediante las páginas Performance Inventory"

Gestión de problemas o funciones de ONTAP directamente desde Unified Manager

Puede solucionar algunos problemas de ONTAP o gestionar determinadas funciones de ONTAP directamente desde la interfaz de usuario de Unified Manager, en lugar de tener que utilizar ONTAP System Manager o la interfaz de línea de comandos de ONTAP. La opción «Gestión» proporciona correcciones a varios problemas de ONTAP que han

desencadenado eventos de Unified Manager.

Puede corregir problemas directamente desde la página acciones de administración seleccionando la opción **acciones de administración** en el panel de navegación izquierdo. Las acciones de administración también están disponibles en el panel Management Actions (acciones de administración) en el panel Dashboard (Panel), la página de detalles de eventos y la selección Workload Analysis (Análisis de carga de trabajo) en el menú de navegación izquierdo.

Hay ciertos problemas que Unified Manager puede diagnosticar a fondo y proporcionar una única resolución. En el caso de ciertas funciones de ONTAP, como la supervisión antiransomware, Unified Manager realiza comprobaciones internas y recomienda acciones específicas. Si están disponibles, estas resoluciones se muestran en acciones de administración con un botón **Fix it**. Haga clic en el botón **Fix it** para solucionar el problema. Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Unified Manager envía comandos ONTAP al clúster para realizar la corrección solicitada. Cuando finaliza la corrección, el evento se ha obsoleto.

Algunas acciones de administración permiten solucionar el mismo problema en varios objetos de almacenamiento con el botón **Fix All**. Por ejemplo, puede haber 5 volúmenes que tengan el evento "espacio de volumen lleno" que se podría resolver haciendo clic en la acción de administración **solucionar todo** para "Habilitar crecimiento automático de volumen". Mediante un solo clic, puede solucionar este problema en 5 volúmenes.

Para obtener información sobre las funciones y los problemas de ONTAP que puede gestionar mediante la solución automática, consulte "¿Qué problemas puede solucionar Unified Manager".

¿Qué opciones tengo cuando veo el botón reparar o reparar todo

La página Management Actions (acciones de administración) le proporciona el botón **Fix it** o **Fix All** para solucionar los problemas de los que Unified Manager ha sido notificado a través de un evento.

Le recomendamos que haga clic en los botones para solucionar un problema, según sea necesario. Sin embargo, si no está seguro de que desea resolver el problema como recomienda Unified Manager, puede realizar las siguientes acciones:

¿Qué desea hacer?	Acción
Tiene Unified Manager que se solucione el problema en todos los objetos identificados.	Haga clic en el botón **Fix All**.
No solucione el problema de ninguno de los objetos identificados en este momento y oculte esta acción de administración hasta que el evento vuelva a aparecer.	Haga clic en la flecha hacia abajo y haga clic en **descartar todo**.
Solucione el problema sólo en algunos de los objetos identificados.	Haga clic en el nombre de la acción de administración para expandir la lista y mostrar todas las acciones * Fix it* individuales. A continuación, siga los pasos para corregir o descartar acciones de administración individuales.

¿Qué desea hacer?	Acción
Tenga Unified Manager que solucione el problema.	Haga clic en el botón **Fix it**.
No solucione el problema en este momento y oculte esta acción de administración hasta que el evento vuelva a aparecer.	Haga clic en la flecha hacia abajo y haga clic en **descartar**.
Muestre los detalles de este evento para que pueda comprender mejor el problema.	• Haga clic en el botón **Fix it** y revise la corrección que se aplicará en el cuadro de diálogo resultante. • Haga clic en la flecha hacia abajo y haga clic en **Ver detalle de evento** para mostrar la página de detalles evento. A continuación, haga clic en **Fix it** en cualquiera de estas páginas resultantes si desea solucionar el problema.
Muestre los detalles de este objeto de almacenamiento para que pueda comprender mejor el problema.	Haga clic en el nombre del objeto de almacenamiento para mostrar detalles en la página Performance Explorer o Health Details.

En algunos casos, la corrección se refleja en el sondeo de configuración de 15 minutos siguiente. En otros casos, el cambio de configuración puede tardar varias horas en verificarse y en que el evento se quede obsoleto.

Para ver la lista de acciones de administración en curso o completadas, haga clic en el icono de filtro y seleccione **completado** o **en curso**.

Corrija todas las operaciones se ejecutan de forma serial, por lo que cuando vea el panel **en curso** algunos objetos tendrán el estado **en curso** mientras que otros tendrán el estado **programado**; lo que significa que todavía están esperando a ser implementado.

Ver el estado de las acciones de gestión que ha elegido corregir

Es posible ver el estado de todas las acciones de administración seleccionadas para corregir en la página Management Actions. La mayoría de las acciones se muestran como **completado** bastante rápido después de que Unified Manager envía el comando ONTAP al clúster. Sin embargo, algunas acciones, como mover un volumen, pueden tardar más tiempo.

Hay tres filtros disponibles en la página Management Actions:

- **Completado** muestra las dos acciones de administración que se completaron correctamente y las que han fallado. **Las acciones con fallos** proporcionan una razón para el fallo para que pueda solucionar el problema manualmente.
- **En curso** muestra tanto las acciones de administración que se están implementando, como las que están programadas para ser implementadas.
- **Recomendado** muestra todas las acciones de administración que están actualmente activas para todos

los clústeres supervisados.

Pasos

1. Haga clic en **acciones de administración** en el panel de navegación izquierdo. Como alternativa, haga clic en ⋮ En la parte superior del panel **acciones de administración** del **Panel** y seleccione la vista que desee ver.

   Se muestra la página Management Actions.

2. Puede hacer clic en el icono de intercalación junto a la acción de administración en el campo **Descripción** para ver detalles sobre el problema y el comando que se está utilizando para solucionar el problema.
3. Para ver las acciones que **han fallado**, ordene en la columna **Estado** de la vista **completado**. Puede utilizar la herramienta **filtro** para este mismo fin.
4. Si desea ver más información acerca de una acción de administración fallida o si decide que desea corregir una acción de administración recomendada, puede hacer clic en **Ver detalle de evento** en el área expandida después de hacer clic en el icono de intercalación junto a la acción de administración. Un botón **Fix it** está disponible en esa página.

¿Qué problemas puede solucionar Unified Manager

Mediante la función de corrección automática de Active IQ Unified Manager, puede optar por resolver determinados problemas de ONTAP o gestionar de forma efectiva determinadas funciones de ONTAP, como la supervisión antiransomware, a través de Unified Manager.

Esta tabla describe estas funciones o problemas de ONTAP que puede gestionar directamente mediante el botón **Fix it** o **Fix All** de la interfaz de usuario web de Unified Manager.

Nombre y descripción del evento	Acciones de Gestión	Funcionamiento de "reparar"
Espacio de volumen lleno El volumen está casi sin espacio y ha superado el umbral de capacidad completa. De manera predeterminada, este umbral se establece en el 90 % del tamaño del volumen.	Habilitar el crecimiento automático del volumen	Unified Manager determina que el crecimiento automático del volumen no está configurado para este volumen, por lo que habilita esta función para que el volumen aumente su capacidad cuando sea necesario.
Inodos llenos Este volumen se ha quedado sin inodos y no puede aceptar ningún archivo nuevo.	Aumente el número de inodos en el volumen	Aumenta el número de inodos en el volumen en un 2 por ciento.

Nombre y descripción del evento	Acciones de Gestión	Funcionamiento de "reparar"
Se detectó una discrepancia de la política de nivel de almacenamiento El volumen tiene muchos datos inactivos y la política de organización en niveles actual está establecida en "solo copias Snapshot" o "ninguna".	Habilite la organización automática en niveles del cloud	Dado que el volumen ya reside en un FabricPool, cambia la política de organización en niveles a «automática» de modo que los datos inactivos se muevan al nivel de cloud de menor coste.
Se detectó una discrepancia del nivel de almacenamiento El volumen tiene muchos datos inactivos, pero no residen en un nivel de almacenamiento (FabricPool) habilitado para el cloud.	Cambie el nivel de almacenamiento de los volúmenes	Mueve el volumen al nivel de almacenamiento habilitado para el cloud y establece la política de organización en niveles en "automático" para mover los datos inactivos al nivel de cloud.
Registro de auditoría deshabilitado El registro de auditoría no está habilitado para la máquina virtual de almacenamiento	Habilitar el registro de auditoría para la máquina virtual de almacenamiento	Permite el registro de auditoría en la máquina virtual de almacenamiento. Tenga en cuenta que la máquina virtual de almacenamiento ya debe tener configurada una ubicación de registro de auditoría local o remota.
Banner de inicio de sesión deshabilitado Se debe habilitar el banner de inicio de sesión del clúster para aumentar la seguridad al borrar las restricciones de acceso.	Configure el banner de inicio de sesión para el clúster	Establece el banner de inicio de sesión del clúster en "'acceso restringido a usuarios autorizados'".
Banner de inicio de sesión deshabilitado El banner de inicio de sesión de la máquina virtual de almacenamiento se debe habilitar para aumentar la seguridad al borrar las restricciones de acceso.	Configure el banner de inicio de sesión para la máquina virtual de almacenamiento	Configura el banner de inicio de sesión de la máquina virtual de almacenamiento en "acceso restringido a usuarios autorizados".
SSH utiliza claves no seguras Los cifrados con el sufijo "-cbc" se consideran no seguros.	Quite los cifrados no seguros del clúster	Elimina de el clúster los cifrados no seguros, como aes192-cbc y aes128-cbc.

Nombre y descripción del evento	Acciones de Gestión	Funcionamiento de "reparar"
SSH utiliza claves no seguras Los cifrados con el sufijo "-cbc" se consideran no seguros.	Quite los cifrados no seguros de la máquina virtual de almacenamiento	Elimina los cifrados no seguros, como aes192-cbc y aes128-cbc, de la máquina virtual de almacenamiento.
Transporte HTTPS de AutoSupport deshabilitado El protocolo de transporte utilizado para enviar mensajes de AutoSupport al soporte técnico debe estar cifrado.	Establezca HTTPS como el protocolo de transporte para los mensajes de AutoSupport	Establece HTTPS como el protocolo de transporte para los mensajes de AutoSupport en el clúster.
Se superó el umbral de desequilibrio de carga del clúster Indica que la carga está desequilibrado entre los nodos del clúster. Este evento se genera cuando la variación de capacidad de rendimiento utilizada es de más de un 30 % entre nodos.	Equilibre las cargas de trabajo del clúster	Unified Manager identifica el mejor volumen para moverse de un nodo a otro para reducir el desequilibrio y luego mueve el volumen.
Se superó el umbral de desequilibrio de capacidad del clúster Indica que la capacidad está desequilibrado entre los agregados del clúster. Este evento se genera cuando la variación de capacidad utilizada es superior al 70 % entre agregados.	Equilibre la capacidad del clúster	Unified Manager identifica el mejor volumen para moverlo de un agregado a otro con el fin de reducir el desequilibrio y luego lo mueve.
Se superó el umbral de capacidad de rendimiento utilizada Indica que la carga del nodo se podría volver a utilizar si no se reduce el uso en una o más cargas de trabajo altamente activas. Este evento se genera cuando el valor de capacidad de rendimiento del nodo usado es superior al 100 % durante más de 12 horas.	Limite la carga alta en el nodo	Unified Manager identifica el volumen con el IOPS más alto y aplica una política de calidad de servicio utilizando los niveles históricos esperados y pico de IOPS para reducir la carga en el nodo.

Nombre y descripción del evento	Acciones de Gestión	Funcionamiento de "reparar"
Umbral de advertencia de evento dinámico incumplido Indica que el nodo ya está funcionando en estado sobrecargado debido a la carga anormalmente alta de algunas cargas de trabajo.	Reducir la sobrecarga en el nodo	Unified Manager identifica el volumen con el IOPS más alto y aplica una política de calidad de servicio utilizando los niveles históricos esperados y pico de IOPS para reducir la carga en el nodo.
La toma de control no es posible La conmutación al respaldo está deshabilitada actualmente, por lo que el acceso a los recursos del nodo durante una interrupción o reinicio se perderá hasta que el nodo vuelva a estar disponible.	Habilite la conmutación al nodo de respaldo	Unified Manager envía el comando correspondiente para habilitar la conmutación por error en todos los nodos del clúster.
La opción cf.takeover.on_panic está CONFIGURADA COMO DESACTIVADA La opción nodeshell "cf.takeover.on_panic" está establecida en **off**, lo que podría causar un problema en sistemas configurados por ha.	Permita la toma de control en caso de pánico	Unified Manager envía el comando correspondiente al clúster para cambiar esta configuración a **On**.
Deshabilite la opción nodeshell snapmirror.enable La antigua opción nodeshell "snapmirror.enable" está establecida en **on**, lo que podría causar un problema durante el arranque tras actualizar a ONTAP 9.3 o superior.	Establezca la opción snapmirror.enable como off	Unified Manager envía el comando correspondiente al clúster para cambiar esta configuración a **OFF**.
Telnet activado Indica un posible problema de seguridad porque Telnet no es seguro y pasa datos de una manera no cifrada.	Desactivar Telnet	Unified Manager envía el comando correspondiente al clúster para deshabilitar Telnet.

Nombre y descripción del evento	Acciones de Gestión	Funcionamiento de "reparar"
Configure el aprendizaje de la máquina virtual de almacenamiento contra ransomware Comprueba periódicamente si hay clústeres con licencias para supervisar el ransomware. Valida si una máquina virtual de almacenamiento admite solo volúmenes NFS o SMB en este clúster.	Ponga en marcha máquinas virtuales de almacenamiento `learning` modo de supervisión antiransomware	Unified Manager establece la supervisión antiransomware `learning` estado para las máquinas virtuales de almacenamiento a través de la consola de gestión de clústeres. La supervisión antiransomware en todos los volúmenes nuevos creados en la máquina virtual de almacenamiento se mueve automáticamente a un modo de aprendizaje. Con esta habilitación, ONTAP puede aprender el patrón de actividad en los volúmenes y detectar las anomalías debido a posibles ataques maliciosos.
Configure el aprendizaje de volúmenes contra ransomware Comprueba periódicamente si hay clústeres con licencias para supervisar el ransomware. Valida si un volumen solo admite los servicios NFS o SMB en este tipo de clúster.	Coloque volúmenes en `learning` modo de supervisión antiransomware	Unified Manager establece la supervisión antiransomware `learning` estado para los volúmenes a través de la consola de gestión de clústeres. Con esta habilitación, ONTAP puede aprender el patrón de actividad en los volúmenes y detectar las anomalías debido a posibles ataques maliciosos.
Habilite el volumen contra ransomware Comprueba periódicamente si hay clústeres con licencias para supervisar el ransomware. Detecta si los volúmenes se encuentran en el `learning` modo de supervisión antiransomware durante más de 45 días, y determina el posible cliente de ponerlos en modo activo.	Coloque volúmenes en `active` modo de supervisión antiransomware	Unified Manager establece la supervisión antiransomware `active` en los volúmenes a través de la consola de gestión de clústeres. Con esta habilitación, ONTAP puede aprender el patrón de actividad en los volúmenes y detectar las anomalías debido a posibles ataques malintencionados, y crear alertas para las acciones de protección de datos.

Nombre y descripción del evento	Acciones de Gestión	Funcionamiento de "reparar"
Deshabilite el volumen antiransomware Comprueba periódicamente si hay clústeres con licencias para supervisar el ransomware. Detecta notificaciones repetitivos durante la supervisión activa contra el ransomware en los volúmenes (por ejemplo, se devuelven varias advertencias de posibles ataques de ransomware durante 30 días).	Deshabilite la supervisión antiransomware en volúmenes	Unified Manager deshabilita la supervisión antiransomware en los volúmenes a través de la consola de gestión del clúster.

Sobrescribir las acciones de gestión a través de scripts

Puede crear scripts personalizados y asociarlos a alertas para realizar acciones específicas en eventos específicos, y no optar por las acciones de gestión predeterminadas que están disponibles en la página Management Actions o en la consola de Unified Manager.

Si desea realizar acciones específicas para un tipo de evento y elegir no corregirlas como parte de la funcionalidad de acción de gestión proporcionada por Unified Manager, puede configurar un script personalizado para la acción específica. A continuación, puede asociar el script con una alerta para ese tipo de evento y ocuparse de estos eventos individualmente. En este caso, las acciones de gestión no se generan para ese tipo de evento específico en la página Management Actions o la consola de Unified Manager.

Gestionar clústeres

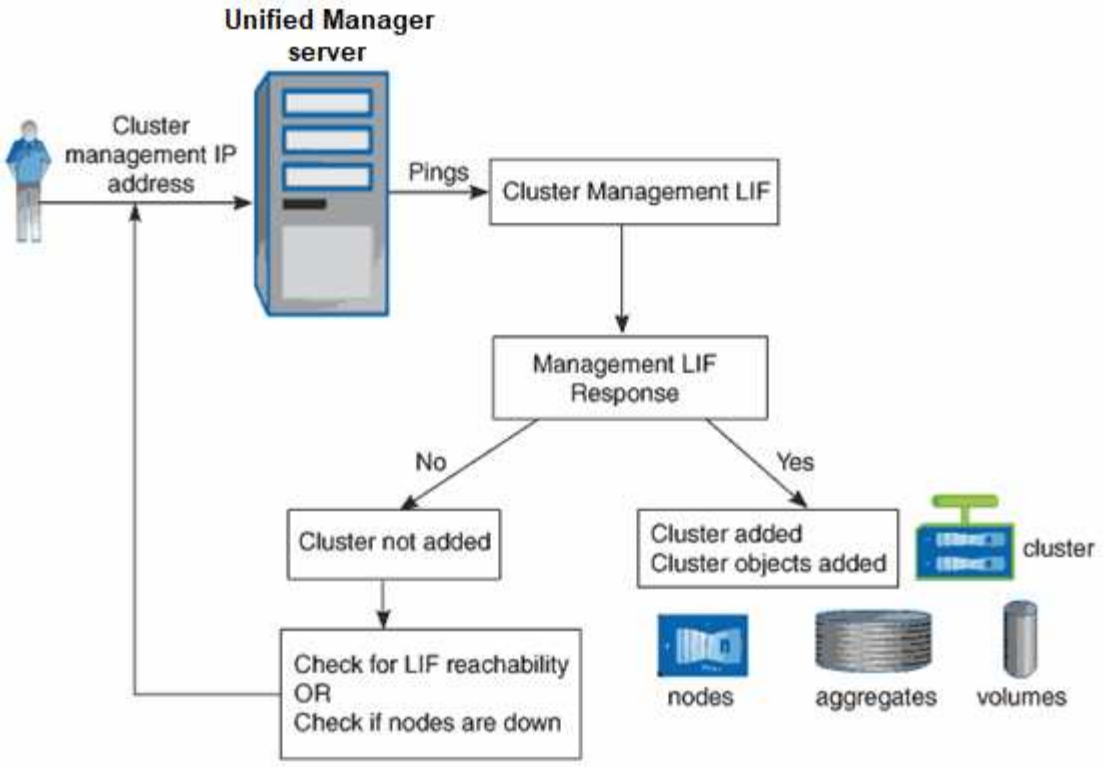
Los clústeres de ONTAP se pueden gestionar mediante Unified Manager para supervisar, añadir, editar y quitar clústeres.

Cómo funciona el proceso de detección del clúster

Después de añadir un clúster a Unified Manager, el servidor detecta los objetos del clúster y los añade a su base de datos. Comprender cómo funciona el proceso de detección le permite gestionar los clústeres de su organización y sus objetos.

El intervalo de supervisión para recoger la información de configuración del clúster es de 15 minutos. Por ejemplo, después de agregar un clúster, tarda 15 minutos en mostrar los objetos del clúster en la interfaz de usuario de Unified Manager. Este plazo también se cumple al realizar cambios en un clúster. Por ejemplo, si se añaden dos volúmenes nuevos a una SVM de un clúster, se ven esos objetos nuevos en la interfaz de usuario después del siguiente intervalo de sondeo, que podría ser de hasta 15 minutos.

En la siguiente imagen se muestra el proceso de detección:



Después de detectar todos los objetos de un clúster nuevo, Unified Manager comienza a recopilar datos históricos de rendimiento de los 15 días anteriores. Estas estadísticas se recopilan mediante la funcionalidad de recogida de continuidad de datos. Esta función le proporciona más de dos semanas de información sobre el rendimiento de un clúster inmediatamente después de añadir. Una vez completado el ciclo de recogida de continuidad de datos, se recogen datos de rendimiento del clúster en tiempo real, de forma predeterminada, cada cinco minutos.

Dado que la recogida de 15 días de datos de rendimiento requiere un uso intensivo de la CPU, se sugiere escalonar la adición de nuevos clústeres de manera que las encuestas de recogida de continuidad de datos no se ejecuten en demasiados clústeres al mismo tiempo.

Se muestra la lista de clústeres supervisados

Puede usar la página Cluster Setup para ver el inventario de clústeres. Es posible ver detalles sobre los clústeres, como su nombre, dirección IP y estado de comunicación.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Paso

1. En el panel de navegación izquierdo, haga clic en **Storage Management** > **Cluster Setup**. + Se mostrarán todos los clústeres de su entorno de almacenamiento gestionados por Unified Manager. La lista de clústeres se ordena según la columna Collection state Severity Level. Puede hacer clic en un encabezado de columna para ordenar los clústeres por columnas diferentes.

Añadir clústeres

Puede añadir un clúster a la Active IQ Unified Manager para poder supervisar el clúster.

Esto incluye la capacidad de obtener información del clúster, como el estado, la capacidad, el rendimiento y la configuración del clúster, para poder encontrar y resolver cualquier problema que pueda ocurrir.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador de almacenamiento.
- Debe tener el nombre de host o la dirección IP de administración del clúster (IPv4 o IPv6) para el clúster.

  Cuando se utiliza el nombre de host, debe resolver la dirección IP de administración del clúster para la LIF de gestión del clúster. Si utiliza un LIF de gestión de nodos, la operación da error.

- Debe tener el nombre de usuario y la contraseña para acceder al clúster.

  Esta cuenta debe tener el rol *admin* con acceso a aplicaciones establecido en *ontapi*, *Console* y *http*.

- Debe conocer el número de puerto para conectarse al clúster mediante el protocolo HTTPS (por lo general, el puerto 443).
- El clúster de debe ejecutar el software ONTAP versión 9.1 o posterior.
- Debe tener espacio suficiente en el servidor de Unified Manager. Se le impide agregar un clúster al servidor cuando más del 90 % del espacio ya está consumido.
- Tiene los certificados necesarios. Unified Manager instala certificados de seguridad al añadir un clúster:

  Certificados de servidor: Este certificado es propiedad de Unified Manager. Se genera un certificado SSL (HTTPS) autofirmado predeterminado con una instalación nueva de Unified Manager. NetApp recomienda actualizarlo a certificado firmado por CA para mejorar la seguridad. Si el certificado de servidor caduca, debe volver a regenerarlo y reiniciar Unified Manager para que los servicios incorporen el nuevo certificado. Para obtener más información acerca de la regeneración del certificado SSL, consulte "Generar un certificado de seguridad HTTPS".

  Certificados para la comunicación mutua con TLS: Se utiliza durante la comunicación mutua con TLS entre Unified Manager y ONTAP. La autenticación basada en certificados está habilitada para un clúster de acuerdo con la versión de ONTAP. Si el clúster que ejecuta la versión de ONTAP es inferior a la versión 9.5, la autenticación basada en certificados no está habilitada.

  La autenticación basada en certificados no se habilita automáticamente para un clúster, si va a actualizar una versión anterior de Unified Manager a Unified Manager 9.12. Sin embargo, puede habilitarla mediante la modificación y el guardado de los detalles del clúster. Si el certificado caduca, debe regenerarlo para incorporar el nuevo certificado. Para obtener más información sobre la visualización y regeneración del certificado, consulte "Editar clústeres".

  - La autenticación basada en certificados se habilita automáticamente si se añade un clúster de la interfaz de usuario web de. Si agrega un clúster desde la consola de mantenimiento, la autenticación basada en certificados no está habilitada.
  - Si la autenticación basada en certificados está habilitada para un clúster, y realiza el backup de Unified Manager desde un servidor y la restauración a otro servidor de Unified Manager donde se cambia el nombre de host o la dirección IP, la supervisión del clúster puede fallar. Para evitar el error, edite y guarde los detalles del clúster. Para obtener más información sobre cómo editar detalles del clúster, consulte "Editar clústeres".

  Certificados de cliente: Se utiliza durante la autenticación de mensajes EMS recibidos de ONTAP. Este

certificado es propiedad de ONTAP y es obligatorio cuando se añade un clúster de ONTAP a Unified Manager. No puede agregar un clúster a Unified Manager con un certificado caducado y si el certificado de cliente ya ha caducado, debe volver a regenerarlo antes de agregar el clúster. Sin embargo, si este certificado caduca en un clúster que ya se ha añadido y está siendo utilizado por Unified Manager, la mensajería de EMS sigue funcionando con el certificado caducado. Para obtener información acerca de la generación de certificados, consulte el artículo de la base de conocimientos (KB) "Cómo renovar un certificado autofirmado de ONTAP en la interfaz de usuario de System Manager".

- Una única instancia de Unified Manager puede admitir un número determinado de nodos. Si necesita supervisar un entorno que supere el número de nodos admitidos, debe instalar una instancia adicional de Unified Manager para supervisar algunos de los clústeres. Para ver la lista del número de nodos admitidos, consulte "Guía de prácticas recomendadas de Unified Manager".

Pasos

1. En el panel de navegación izquierdo, haga clic en **Storage Management** > **Cluster Setup**.
2. En la página Cluster Setup, haga clic en **Add**.
3. En el cuadro de diálogo Agregar clúster, especifique los valores según sea necesario y, a continuación, haga clic en **Enviar**.
4. En el cuadro de diálogo autorizar host, haga clic en **Ver certificado** para ver la información del certificado sobre el clúster.
5. Haga clic en **Sí**.

   En Unified Manager 9.12, después de guardar los detalles del clúster, puede ver el certificado para comunicación mutua TLS para un clúster.

   Si la autenticación basada en certificados no está habilitada, Unified Manager comprueba el certificado solo cuando se añade el clúster inicialmente. Unified Manager no comprueba el certificado para cada llamada API a ONTAP.

Después de detectar todos los objetos de un clúster nuevo, Unified Manager comienza a recopilar datos históricos de rendimiento de los 15 días anteriores. Estas estadísticas se recopilan mediante la funcionalidad de recogida de continuidad de datos. Esta función le proporciona más de dos semanas de información sobre el rendimiento de un clúster inmediatamente después de añadir. Una vez completado el ciclo de recogida de continuidad de datos, se recogen datos de rendimiento del clúster en tiempo real, de forma predeterminada, cada cinco minutos.

Dado que la recogida de 15 días de datos de rendimiento requiere un uso intensivo de la CPU, se sugiere escalonar la adición de nuevos clústeres de manera que las encuestas de recogida de continuidad de datos no se ejecuten en demasiados clústeres al mismo tiempo. Además, si reinicia Unified Manager durante el período de recogida de continuidad de datos, la recogida se detiene y verá vacíos en los gráficos de rendimiento correspondientes al periodo que falta.

Si recibe un mensaje de error que no puede agregar el clúster, compruebe si existen los siguientes problemas:

- Si los relojes de los dos sistemas no están sincronizados y la fecha de inicio del certificado HTTPS de Unified Manager es posterior a la fecha en el clúster. Debe asegurarse de que los relojes se sincronicen con NTP o un servicio similar.
- Si el clúster ha alcanzado la cantidad máxima de destinos de notificaciones de EMS, no se puede añadir la dirección de Unified Manager. De manera predeterminada, solo se pueden definir 20 destinos de notificación de EMS en el clúster.

Información relacionada

"Adición de usuarios"

"Ver la lista del clúster y sus detalles"

"Instalar una CA firmada y devolvió un certificado HTTPS"

Editar clústeres

Puede modificar la configuración de un clúster existente, como el nombre de host o la dirección IP, el nombre de usuario, la contraseña y el puerto, mediante el cuadro de diálogo Edit Cluster.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador de almacenamiento.

A partir de Unified Manager 9.7, los clústeres se pueden añadir solo mediante HTTPS.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Storage Management** > **Cluster Setup**.
2. En la página **Cluster Setup**, seleccione el clúster que desea editar y, a continuación, haga clic en **Edit**.
3. En el cuadro de diálogo **Editar clúster**, modifique los valores según sea necesario. + Si ha modificado los detalles de un clúster agregado a Unified Manager 9.12, puede ver los detalles del certificado para la comunicación Mutual TLS, según la versión de ONTAP. Para obtener más información sobre la versión de ONTAP, consulte "Certificados para comunicación mutua TLS". + para ver los detalles del certificado, haga clic en **Detalles del certificado**. Si el certificado ha caducado, haga clic en el botón **Regenerate** para incorporar el nuevo certificado.
4. Haga clic en **Enviar**.
5. En el cuadro de diálogo autorizar host, haga clic en **Ver certificado** para ver la información del certificado sobre el clúster.
6. Haga clic en **Sí**.

Información relacionada

"Adición de usuarios"

"Ver la lista del clúster y sus detalles"

Quitar clústeres

Puede quitar un clúster de Unified Manager mediante la página Cluster Setup. Por ejemplo, puede quitar un clúster si la detección del clúster falla o cuando desea retirar un sistema de almacenamiento.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador de almacenamiento.

Esta tarea elimina el clúster seleccionado de Unified Manager. Después de eliminar un clúster, este ya no se supervisa. La instancia de Unified Manager registrada en el clúster eliminado también se elimina del clúster.

Al quitar un clúster, también se eliminan todos sus objetos de almacenamiento, datos históricos, servicios de almacenamiento y todos los eventos asociados de Unified Manager. Estos cambios se reflejan en las páginas de inventario y las páginas de detalles después del siguiente ciclo de recopilación de datos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Storage Management** > **Cluster Setup**.
2. En la página Cluster Setup (Configuración del clúster), seleccione el clúster que desea quitar y haga clic en **Remove**.
3. En el cuadro de diálogo del mensaje **Quitar origen de datos**, haga clic en **Quitar** para confirmar la solicitud de eliminación.

Información relacionada

"Adición de usuarios"

"Ver la lista del clúster y sus detalles"

Volver a detectar clústeres

Es posible volver a detectar manualmente un clúster en la página Cluster Setup para obtener la información más reciente del estado, la supervisión del estado y el estado de rendimiento del clúster.

Es posible volver a detectar manualmente un clúster si se desea actualizar el clúster, como aumentar el tamaño de un agregado cuando no hay espacio suficiente, y si desea que Unified Manager detecte los cambios realizados.

Cuando Unified Manager se empareja con OnCommand Workflow Automation (WFA), el emparejamiento activa la readquisición de los datos almacenados en caché mediante WFA.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Storage Management** > **Cluster Setup**.
2. En la página **Cluster Setup**, haga clic en **Rediscover**.

   Unified Manager vuelve a detectar el clúster seleccionado y muestra el estado y el rendimiento más reciente.

Información relacionada

"Ver la lista del clúster y sus detalles"

Supervisión de la infraestructura virtual de VMware

Active IQ Unified Manager proporciona visibilidad de las máquinas virtuales (VM) de su infraestructura virtual, y permite supervisar y solucionar los problemas de almacenamiento y rendimiento del entorno virtual. Es posible usar esta función para determinar cualquier problema de latencia en el entorno de almacenamiento o cuando se

produjo un evento de rendimiento informado en vCenter Server.

Una infraestructura virtual típica puesta en marcha en ONTAP tiene diversos componentes que se distribuyen en las capas informática, de red y de almacenamiento. Cualquier retraso en el rendimiento de una aplicación de equipo virtual puede producirse debido a una combinación de latencias que deben afrontar los distintos componentes de las capas respectivas. Esta función es útil para administradores de almacenamiento y vCenter Server, así como para generalistas DE TI que necesitan analizar un problema de rendimiento en un entorno virtual y entender qué componente ha producido el problema.

Ahora puede acceder a vCenter Server desde el menú de vCenter de la sección VMware. La vista de PEEK de cada máquina virtual enumerada tiene el enlace **VCENTER SERVER** de la VISTA DE TOPOLOGÍA que inicia el vCenter Server en una nueva navegador. También puede usar el botón **Expand Topology** para iniciar la instancia de vCenter Server y hacer clic en el botón **View in vCenter** para ver los almacenes de datos en vCenter Server.

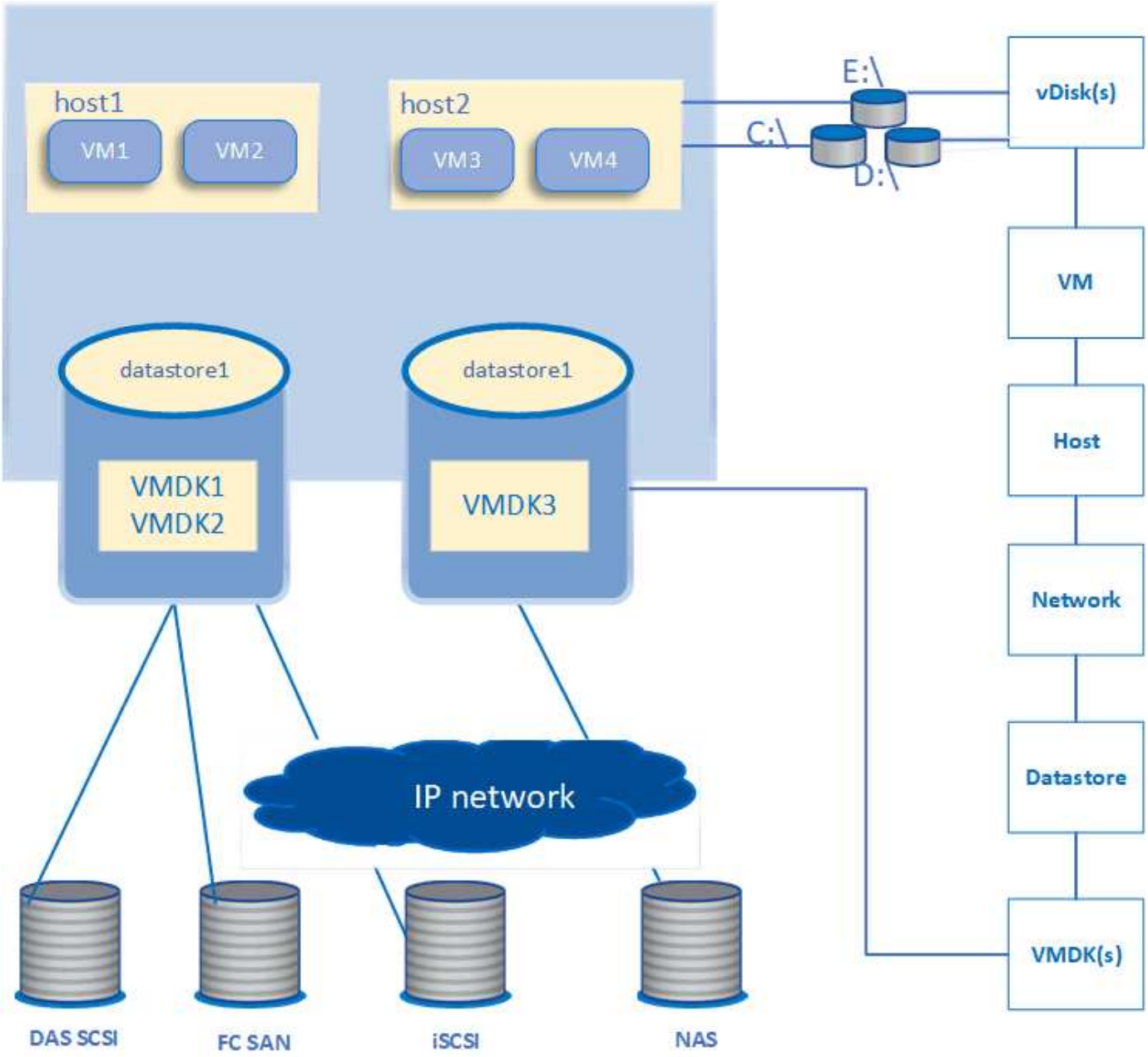
Unified Manager presenta el subsistema subyacente de un entorno virtual en una vista topológica para determinar si se ha producido un problema de latencia en el nodo de computación, la red o el almacenamiento. La vista también destaca el objeto específico que provoca el desfase en el rendimiento a la hora de dar pasos correctivas y solucionar el problema subyacente.

Una infraestructura virtual implementada en el almacenamiento de ONTAP incluye los siguientes objetos:

- VCenter Server: Un plano de control centralizado para gestionar las máquinas virtuales de VMware, los hosts ESXi y todos los componentes relacionados en un entorno virtual. Para obtener más información sobre vCenter Server, consulte la documentación de VMware.
- Host: Un sistema físico o virtual que ejecuta ESXi, el software de virtualización de VMware y aloja la máquina virtual.
- Datastore: Los almacenes de datos son objetos de almacenamiento virtual conectados a los hosts ESXi. Los almacenes de datos son entidades de almacenamiento gestionables de ONTAP, como LUN o volúmenes, que se usan como repositorio para archivos del equipo virtual, como archivos de registro, scripts, archivos de configuración y discos virtuales. Se conectan a los hosts del entorno mediante una conexión DE red SAN o IP. Los almacenes de datos fuera de ONTAP que se asignan a vCenter Server no son compatibles o se muestran en Unified Manager.
- Máquina virtual: Una máquina virtual de VMware.
- Discos virtuales: Los discos virtuales en almacenes de datos que pertenecen a las máquinas virtuales que tienen una extensión como VMDK. Los datos de un disco virtual se almacenan en el VMDK correspondiente.
- VMDK: Un disco de máquina virtual del almacén de datos que proporciona espacio de almacenamiento para discos virtuales. Por cada disco virtual, hay un VMDK correspondiente.

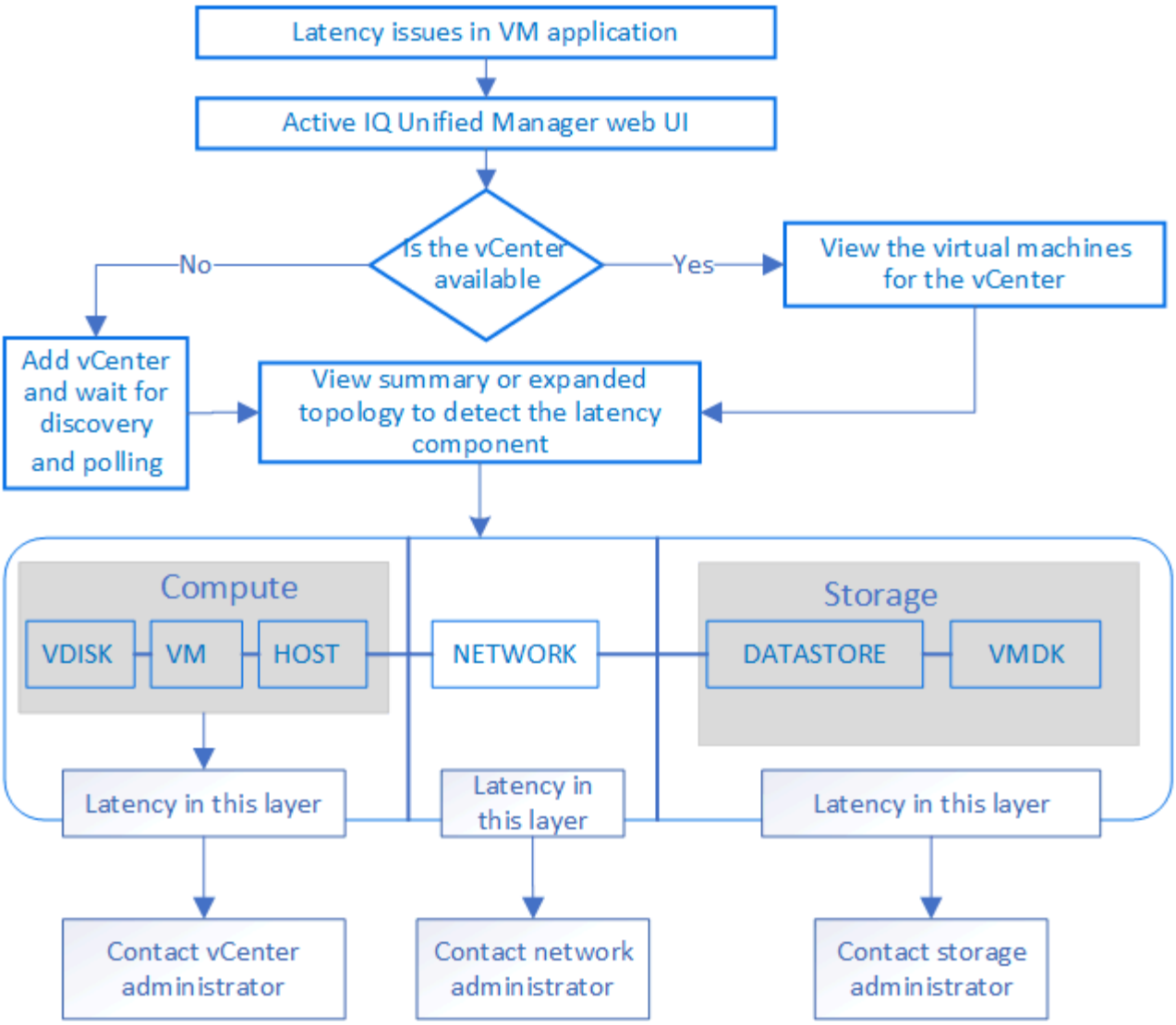
Estos objetos se representan en una vista de topología de máquina virtual.

Virtualización de VMware en ONTAP



Flujo de trabajo del usuario

El siguiente diagrama muestra un caso de uso típico de la vista de topología de la máquina virtual:



Qué no se admite

- Los almacenes de datos que no son de ONTAP y se asignan a las instancias de vCenter Server no son compatibles con Unified Manager. Tampoco se admite cualquier máquina virtual con discos virtuales en esos almacenes de datos.
- No se admite un almacén de datos que abarca varios LUN.
- No se admiten los almacenes de datos que utilizan la traducción de direcciones de red (NAT) para asignar LIF de datos (punto final de acceso).
- No se admite la exportación de volúmenes o LUN como almacenes de datos en diferentes clústeres con las mismas direcciones IP en una configuración de varias LIF, ya que Unified Manager no puede identificar qué almacén de datos pertenece a qué clúster.

  Ejemplo: Supongamos que el clúster A tiene un almacén de datos A. El almacén de datos A se exporta a través de la LIF de datos con la misma dirección IP x.x.x y se crea en este almacén de datos la máquina virtual A. De igual manera, el clúster B tiene un almacén de datos B. El almacén de datos B se exporta a través de la LIF de datos con la misma dirección IP x.x.x.x y el equipo virtual B se crea en el almacén de datos B. UM no podrá asignar el almacén de datos A para la topología De VM A al volumen/LUN de ONTAP correspondiente ni al equipo virtual de asignación B.

- Solo los volúmenes NAS Y SAN (iSCSI y FCP para VMFS) se admiten como almacenes de datos, pero no

los volúmenes virtuales (vVols).

- Solo se admiten discos virtuales iSCSI. No se admiten discos virtuales de los tipos NVMe y SATA.
- Las vistas no permiten generar informes para analizar el rendimiento de los distintos componentes.
- Para la configuración de recuperación ante desastres (DR) de las máquinas virtuales de almacenamiento (máquinas virtuales de almacenamiento), compatible con la única infraestructura virtual en Unified Manager, la configuración se debe cambiar manualmente en vCenter Server para dar lugar a los LUN activos en escenarios de conmutación y conmutación de estado. Sin intervención manual, no se puede acceder a sus almacenes de datos.

Ver y añadir vCenter Server

Para ver y solucionar los problemas del rendimiento de las máquinas virtuales (VM), se deben añadir las instancias de vCenter Server asociadas en la instancia de Active IQ Unified Manager.

Lo que necesitará

Antes de añadir o ver vCenter Server, asegúrese de lo siguiente:

- Conoce los nombres de vCenter Server.
- Conoce la dirección IP de vCenter Server y tiene las credenciales requeridas. Las credenciales deben ser de un administrador de vCenter Server o de un usuario raíz con acceso de solo lectura a vCenter Server.
- La instancia de vCenter Server que desea añadir ejecuta vSphere 6.5 o una versión posterior.
- La configuración de recogida de datos en vCenter Server se establece en el nivel de estadísticas de `Level 3`, garantizar el nivel requerido de recopilación de métricas para todos los objetos supervisados. La duración del intervalo debe ser `5 minutes`, y el período de ahorro debe ser `1 day`.

  Para obtener más información, consulte la sección "niveles de recopilación de datos" de *vSphere Monitoring and Performance Guide* en la documentación de VMware.

- Los valores de latencia en vCenter Server se configuran en milisegundos, no en microsegundos, para los cálculos correctos de los valores de latencia.
- Al añadir el almacén de datos a vCenter Server, puede usar la dirección IP del host o el nombre de dominio completo (FQDN). En caso de añadir el FQDN, asegúrese de que el nombre de dominio pueda resolverse mediante el servidor de Unified Manager. Por ejemplo, para una instalación de Linux, asegúrese de que el nombre de dominio se haya agregado en el `/etc/resolv.conf` archivo.
- La hora actual de vCenter Server está sincronizada con la zona horaria de vCenter Server.
- VCenter Server se puede acceder a una detección correcta.
- Posee el acceso de lectura a SDK de VMware al añadir vCenter Server a Unified Manager. Esto es necesario para el sondeo de configuración.

En cada instancia de vCenter Server que se añadió y se detectó, Unified Manager recopila los datos de configuración, como los detalles de vCenter Server y los servidores ESXi, la asignación de ONTAP, los detalles del almacén de datos y el número de máquinas virtuales alojadas. Además, recopila las métricas de rendimiento de los componentes.

Pasos

1. Vaya a **VMWARE** > **vCenter** y compruebe si su vCenter Server está disponible en la lista.

Si vCenter Server no está disponible, debe añadir vCenter Server.

a. Haga clic en **Agregar**.
b. Añada la dirección IP correcta en vCenter Server y compruebe que el dispositivo sea accesible.
c. Añada el nombre de usuario y la contraseña del administrador o el usuario raíz con acceso de solo lectura a vCenter Server.
d. Agregue el número de puerto personalizado si está utilizando otro puerto que no sea el predeterminado 443.
e. Haga clic en **Guardar**.

Tras la detección correcta, se muestra un certificado de servidor que podrá aceptar.

Cuando acepta el certificado, vCenter Server se añade a la lista de instancias de vCenter Server disponibles. La adición del dispositivo no genera en la recopilación de datos para las máquinas virtuales asociadas y la recogida se produce en los intervalos programados.

2. Si vCenter Server está disponible en la página **vCenter**, compruebe su estado pasando el ratón por el campo **Status** para mostrar si vCenter Server funciona según lo esperado o si hay una advertencia o un error.

Añadir vCenter Server permite ver los siguientes Estados. No obstante, los datos de rendimiento y latencia de los equipos virtuales correspondientes pueden tardar hasta una hora después de agregar vCenter Server para reflejarlo con precisión.

◦ Verde: "Normal", que indica que se ha detectado vCenter Server y que se han recopilado correctamente las métricas de rendimiento
◦ Amarillo: "Advertencia" (por ejemplo, cuando el nivel de estadísticas de vCenter Server no se estableció en 3 o superior para obtener estadísticas de cada objeto)
◦ Naranja: "Error" (indica cualquier error interno, como excepción, fallo en la recogida de datos de configuración o imposibilidad de acceder a vCenter Server) es posible hacer clic en el icono de visualización de la columna (**Mostrar/Ocultar**) para ver el mensaje de estado de un servidor vCenter y solucionar el problema.

3. En caso de que vCenter Server no se pueda acceder a él o que las credenciales hayan cambiado, edite los detalles de vCenter Server seleccionando **vCenter** > **Edit**.
4. Realice los cambios necesarios en la página **Editar VMware vCenter Server**.
5. Haga clic en **Guardar**.

Comienza la recopilación de datos de vCenter Server

VCenter Server recoge muestras de datos de rendimiento en tiempo real de 20 segundos y las enrolla en muestras de hasta 5 minutos. La programación de recogida de datos de rendimiento de Unified Manager se basa en la configuración predeterminada de vCenter Server. Unified Manager procesa las muestras de 5 minutos obtenidas de vCenter Server y calcula un promedio por hora de las IOPS y la latencia de los discos virtuales, los equipos virtuales y los hosts. Para los almacenes de datos, Unified Manager calcula un promedio por hora de IOPS y latencia de muestras obtenidas de ONTAP. Estos valores están disponibles en la parte superior de la hora. Las métricas de rendimiento no están disponibles inmediatamente después de añadir vCenter Server, y solo están disponibles cuando se inicia la siguiente hora. El sondeo de los datos de rendimiento comienza a completar un ciclo de recogida de datos de configuración.

Para los datos de configuración de vCenter Server de sondeo, Unified Manager sigue la misma programación

que para recoger datos de configuración del clúster. Para obtener información sobre la configuración de vCenter Server y la programación de recogida de datos de rendimiento, consulte "actividad de recopilación de datos de rendimiento y configuración del clúster".

Información relacionada

"Actividad de recogida de datos de rendimiento y configuración del clúster"

Supervisar máquinas virtuales

Para cualquier problema de latencia en las aplicaciones de máquinas virtuales (VM), es posible que deba supervisar las VM para analizar la causa y solucionar los problemas de ella. Las máquinas virtuales están disponibles cuando sus clústeres de vCenter Server y ONTAP que alojan el almacenamiento de máquinas virtuales se añaden a Unified Manager.

Puede ver los detalles de los equipos virtuales en la página **VMWARE** > > **Máquinas virtuales**. Se muestra información, como la disponibilidad, el estado, la capacidad utilizada y asignada, la latencia de red, así como las IOPS y la latencia de la máquina virtual, el almacén de datos y el host. Para un equipo virtual que admite varios almacenes de datos, la cuadrícula muestra las métricas del almacén de datos con la peor latencia, con un icono de asterisco (*) que indica almacenes de datos adicionales. Si hace clic en el icono, se muestran las métricas del almacén de datos adicional. Algunas de estas columnas no están disponibles para ordenar y filtrar.

> Para ver una máquina virtual y sus detalles, se debe completar la detección (sondeo o colección de métricas) del clúster de ONTAP. Si el clúster se elimina de Unified Manager, la máquina virtual ya no estará disponible después del próximo ciclo de detección.

En esta página, también puede ver la topología detallada de una máquina virtual, donde se muestran los componentes a los que está relacionada la máquina virtual, por ejemplo, el host, el disco virtual y el almacén de datos que está conectado a ella. La vista de topología muestra los componentes subyacentes en sus capas específicas, en el siguiente orden: **Disco virtual** > **VM** > **Host** > **Red** > **Datastore** > **VMDK**.

Puede determinar la ruta de I/o y las latencias de los componentes desde un aspecto topológico e identificar si el almacenamiento es la causa del problema de rendimiento. La vista de resumen de la topología muestra la ruta de I/o y resalta el componente que tiene problemas de IOPS y latencia para que pueda decidir los pasos para la solución de problemas. También puede tener una vista ampliada de la topología que representa cada componente por separado junto con la latencia de ese componente. Puede seleccionar un componente para determinar la ruta de I/o resaltada en las capas.

Visualización de la topología de resumen

Para determinar los problemas de rendimiento, vea las máquinas virtuales en una topología de resumen:

1. Vaya a **VMWARE** > **Máquinas virtuales**.
2. Busque su máquina virtual escribiendo su nombre en el cuadro de búsqueda. También puede filtrar los resultados de la búsqueda según criterios específicos haciendo clic en el botón **filtro**. Sin embargo, si no puede encontrar la máquina virtual, asegúrese de que se haya añadido y detectado la instancia correspondiente de vCenter Server.

Los servidores vCenter permiten caracteres especiales (como %, &, *, $, #, @, !, \, /, :, *, ?, "', <, >, |, ;, ') en los nombres de entidades vSphere, como VM, cluster, datastore, carpeta, o archivo. VMware vCenter Server y ESX/ESXi Server no escapan a los caracteres especiales utilizados en los nombres mostrados. Sin embargo, cuando se procesa el nombre en Unified Manager, se muestra de forma diferente. Por ejemplo, una máquina virtual llamada como `%$VC_AIQUM_clone_191124%` En vCenter Server se muestra como `%25$VC_AIQUM_clone_191124%25` En Unified Manager. Debe conservar una nota de este problema cuando consulta una máquina virtual con un nombre que tenga caracteres especiales en ella.

3. Compruebe el estado de la máquina virtual. Los Estados de la máquina virtual se recuperan de vCenter Server. Están disponibles los siguientes Estados: Para obtener más información sobre estos Estados, consulte la documentación de VMware.
   - Normal
   - Advertencia
   - Alerta
   - Sin supervisión
   - Desconocido
4. Haga clic en la flecha hacia abajo junto a la máquina virtual para ver la vista de resumen de la topología de los componentes en las capas de computación, red y almacenamiento. Se resalta el nodo que tiene problemas de latencia. La vista de resumen muestra la peor latencia de los componentes. Por ejemplo, si una máquina virtual tiene más de un disco virtual, esta vista muestra el disco virtual que tiene la peor latencia entre todos los discos virtuales.
5. Para analizar la latencia y el rendimiento del almacén de datos durante un período de tiempo, haga clic en el botón **Workload Analyzer** situado en la parte superior del icono del objeto del almacén de datos. Se va a la página Workload Analysis, donde puede seleccionar un rango de tiempo y ver los gráficos de rendimiento del almacén de datos. Para obtener más información acerca del analizador de cargas de trabajo, consulte *solución de problemas de cargas de trabajo mediante el analizador de cargas de trabajo*.

Visualización de topología expandida

Es posible desglosar cada componente por separado para ver la topología expandida de la máquina virtual.

Pasos

1. En la vista de topología de resumen, haga clic en **Expand Topology**. Puede ver la topología detallada de cada componente por separado con los números de latencia de cada objeto. Si hay varios nodos en una categoría, por ejemplo, varios nodos en el almacén de datos o VMDK, el nodo con la peor latencia se resalta en rojo.
2. Para comprobar la ruta de E/S de un objeto específico, haga clic en ese objeto para ver la ruta de E/S y la asignación correspondiente. Por ejemplo, para ver la asignación de un disco virtual, haga clic en el disco virtual para ver su asignación resaltada en el VMDK correspondiente. En caso de desfase en el rendimiento de estos componentes, puede recopilar más datos de ONTAP y solucionar el problema.

No se informan las métricas para VMDK. En la topología, solo se muestran los nombres de VMDK, no las métricas.

Información relacionada

"Solución de problemas de cargas de trabajo mediante Workload Analyzer"

Visualización de la infraestructura virtual en una configuración de recuperación ante desastres

Es posible ver las métricas de configuración y rendimiento de los almacenes de datos alojados en una configuración de MetroCluster o la configuración de la máquina virtual de almacenamiento (VM de almacenamiento) para la recuperación ante desastres (SVM DR).

En Unified Manager, puede ver los volúmenes NAS o LUN en una configuración de MetroCluster conectada como almacenes de datos en vCenter Server. Los almacenes de datos alojados en una configuración de MetroCluster se representan en la misma vista topológica que para un almacén de datos en un entorno estándar.

También puede ver los volúmenes NAS o LUN en una configuración de recuperación ante desastres de máquinas virtuales de almacenamiento que se asignan a los almacenes de datos en vCenter Server.

Ver almacenes de datos en la configuración de MetroCluster

Tenga en cuenta los siguientes requisitos previos antes de ver almacenes de datos en una configuración de MetroCluster:

- En caso de conmutación de sitios y conmutación de estado, será necesario completar el descubrimiento de los clústeres principal y secundario del par de alta disponibilidad y los servidores vCenter.
- Los clústeres primario y secundario del par de alta disponibilidad y las instancias de vCenter Server deben gestionarse mediante Unified Manager.
- La configuración necesaria debe completarse en ONTAP y vCenter Server. Para obtener información, consulte la documentación de ONTAP y vCenter.

  "Centro de documentación de ONTAP 9"

Siga estos pasos para ver los almacenes de datos:

1. En la página **VMWARE** > **Virtual Machines**, haga clic en la máquina virtual que aloja el almacén de datos. Haga clic en el enlace **Workload Analyzer** o datastore. En el escenario estándar cuando el sitio principal que aloja el volumen o LUN funciona como se esperaba, puede ver los detalles del clúster de vServer del sitio principal.
2. En caso de desastre y una conmutación consecutiva al sitio secundario, el enlace del almacén de datos señala a las métricas de rendimiento del volumen o LUN del clúster secundario. Esto se refleja una vez finalizado el siguiente ciclo de clústeres y la detección (adquisición) de vServer.
3. Después de una conmutación de estado exitosa, el enlace del almacén de datos vuelve a reflejar las métricas de rendimiento del volumen o el LUN en el clúster principal. Esto se refleja una vez completado el siguiente ciclo de clústeres y la detección de vServer.

Ver almacenes de datos en la configuración de recuperación ante desastres de la máquina virtual de almacenamiento

Tenga en cuenta los siguientes requisitos previos antes de ver almacenes de datos en una configuración de recuperación ante desastres de una máquina virtual de almacenamiento:

- En caso de conmutación de sitios y conmutación de estado, será necesario completar el descubrimiento de los clústeres principal y secundario del par de alta disponibilidad y los servidores vCenter.

- Unified Manager debe gestionar tanto el clúster de origen como el de destino y las máquinas virtuales de almacenamiento.
- La configuración necesaria debe completarse en ONTAP y vCenter Server.
  - En el caso de almacenes de datos NAS (NFS y VMFS), en caso de desastre, los pasos incluyen la recuperación de la máquina virtual de almacenamiento secundario, la verificación de las LIF y las rutas de datos, el establecimiento de conexiones perdidas en vCenter Server y el inicio de las máquinas virtuales.

    Para una conmutación de regreso al sitio principal, los datos entre los volúmenes deben sincronizarse antes de que el sitio principal comience a servir los datos.
  - Para los almacenes de datos SAN (iSCSI y FC para VMFS), vCenter Server formatea el LUN montado en formato VMFS. En caso de desastre, los pasos incluyen poner en marcha el equipo virtual de almacenamiento secundario, verificar las LIF y las rutas de los datos. Si las IP de destino iSCSI son diferentes de las LIF principales, deben añadirse manualmente. Los nuevos LUN deben estar disponibles como dispositivos bajo el adaptador iSCSI del adaptador de almacenamiento del host. A partir de entonces, se deben crear nuevos almacenes de datos VMFS con las nuevas LUN y los equipos virtuales antiguos se registraron con nuevos nombres. Las máquinas virtuales deben estar en funcionamiento.

    En caso de recuperación, es necesario sincronizar los datos entre los volúmenes. Se deben volver a crear nuevos almacenes de datos VMFS con las LUN y las máquinas virtuales antiguas registradas con nombres nuevos.

    Para obtener información sobre la configuración, consulte la documentación de ONTAP y vCenter Server.

  "Centro de documentación de ONTAP 9"

Siga estos pasos para ver los almacenes de datos:

1. En la página **VMWARE** > **Virtual Machines**, haga clic en el inventario de VM que aloja el almacén de datos. Haga clic en el enlace del objeto de almacén de datos. En el supuesto estándar, puede ver los datos de rendimiento de los volúmenes y las LUN del equipo virtual de almacenamiento principal.
2. En caso de desastre y una conmutación consecutiva al equipo virtual de almacenamiento secundario, el enlace del almacén de datos señala a las métricas de rendimiento del volumen o LUN del equipo virtual de almacenamiento secundario. Esto se refleja una vez finalizado el siguiente ciclo de clústeres y la detección (adquisición) de vServer.
3. Después de una conmutación de estado exitosa, el enlace del almacén de datos vuelve a reflejar las métricas de rendimiento del volumen o el LUN en el equipo virtual de almacenamiento principal. Esto se refleja una vez completado el siguiente ciclo de clústeres y la detección de vServer.

Escenarios no compatibles

- Para una configuración MetroCluster, tenga en cuenta las siguientes limitaciones:
  - Clústeres de solo en `NORMAL` y.. `SWITCHOVER` los estados son tomados. Otros estados, como `PARTIAL_SWITCHOVER, PARTIAL_SWITCHBACK`, y. `NOT_REACHABLE` no son compatibles.
  - A menos que la conmutación automática (ASO) esté habilitada, si el clúster primario cae, no se puede detectar el clúster secundario y la topología sigue apuntar al volumen o LUN del clúster principal.
- Para una configuración de recuperación ante desastres de un equipo virtual de almacenamiento, tenga en

cuenta la siguiente limitación:

- No se admite una configuración con el administrador de recuperación de sitios (SRM) o el adaptador de replicación de almacenamiento (SRA) habilitado para un entorno de almacenamiento DE SAN.

Aprovisionamiento y gestión de cargas de trabajo

La función de gestión activa de Active IQ Unified Manager proporciona niveles de servicio de rendimiento, políticas de eficiencia del almacenamiento y API de proveedores de almacenamiento para aprovisionar, supervisar y gestionar cargas de trabajo de almacenamiento en un centro de datos.

Unified Manager proporciona esta funcionalidad de forma predeterminada. Puede desactivarla desde **Storage Management** > **Configuración de funciones** si no planea utilizar esta funcionalidad.

Cuando se habilita esta opción, puede aprovisionar cargas de trabajo en los clústeres de ONTAP que gestiona la instancia de Unified Manager. También puede asignar políticas, como los niveles de servicio de rendimiento y las políticas de eficiencia del almacenamiento en las cargas de trabajo y gestionar el entorno de almacenamiento basado en dichas políticas.

Esta función habilita las siguientes funciones:

- Detección automática de las cargas de trabajo de almacenamiento en los clústeres añadidos, lo cual facilita la evaluación y la puesta en marcha de las cargas de trabajo de almacenamiento
- Aprovisionamiento de cargas de trabajo NAS con compatibilidad con protocolos NFS y CIFS
- Aprovisionamiento de cargas DE trabajo SAN que admiten los protocolos iSCSI y FCP
- Compatibilidad con los protocolos NFS y CIFS en el mismo recurso compartido de archivos
- Gestión de los niveles de servicio del rendimiento y políticas de eficiencia del almacenamiento
- Asignación de niveles de servicio de rendimiento y políticas de eficiencia del almacenamiento a cargas de trabajo de almacenamiento

Las opciones **Provisioning**, **Storage** > **Workloads** y **Policies** del panel izquierdo de la interfaz de usuario permiten modificar varias configuraciones.

Puede realizar las siguientes funciones con estas opciones:

- Vea las cargas de trabajo de almacenamiento en la página **almacenamiento** > **cargas de trabajo**
- Crear cargas de trabajo de almacenamiento a partir de la página de cargas de trabajo de aprovisionamiento
- Crear y gestionar niveles de servicio de rendimiento desde políticas
- Cree y gestione políticas de eficiencia del almacenamiento desde políticas
- Asigne políticas a las cargas de trabajo de almacenamiento desde la página Workloads

Información relacionada

"Administración del almacenamiento basada en políticas"

Información general de cargas de trabajo

Una carga de trabajo representa las operaciones de entrada/salida (I/o) de un objeto de almacenamiento, como un volumen o LUN. La forma en que se aprovisiona el almacenamiento se basa en los requisitos esperados de la carga de trabajo. Active IQ Unified Manager realiza un seguimiento de las estadísticas de carga de trabajo solo después de que haya tráfico hacia y desde el objeto de almacenamiento. Por ejemplo, los valores de latencia e IOPS de la carga de trabajo están disponibles después de que los usuarios comiencen a utilizar una base de datos o una aplicación de correo electrónico.

La página Workloads muestra un resumen de las cargas de trabajo de almacenamiento de los clústeres de ONTAP que gestiona Unified Manager. Proporciona información acumulativa de un vistazo acerca de las cargas de trabajo de almacenamiento que cumplen con el nivel de servicio de rendimiento, así como las cargas de trabajo de almacenamiento no conformes. También le permite evaluar la capacidad y el rendimiento (IOPS) totales, disponibles y usados de los clústeres en todo el centro de datos.

Se recomienda que evalúe el número de cargas de trabajo de almacenamiento no conformes, no disponibles o no gestionadas por cualquier nivel de servicio de rendimiento y realice las acciones necesarias para garantizar que cumple con sus normativas, su uso de capacidad y las IOPS.

La página Workloads tiene las siguientes dos secciones:

- Información general de cargas de trabajo: Proporciona información general sobre el número de cargas de trabajo de almacenamiento en los clústeres de ONTAP gestionados por Unified Manager.
- Descripción general del centro de datos: Proporciona una descripción general de la capacidad y las IOPS de las cargas de trabajo del almacenamiento en el centro de datos. Los datos correspondientes se muestran a nivel de centro de datos y para individuales .

Sección general de las cargas de trabajo

La sección de información general de las cargas de trabajo ofrece información acumulativa de un vistazo de las cargas de trabajo de almacenamiento. El estado de las cargas de trabajo de almacenamiento se muestra en función de los niveles de servicio de rendimiento asignados y sin asignar.

- **Asignado**: Se informa de los siguientes Estados para las cargas de trabajo de almacenamiento en las que se han asignado niveles de servicio de rendimiento:
  - **Cumplimiento**: El rendimiento de las cargas de trabajo de almacenamiento se basa en los niveles de servicio de rendimiento que se les ha asignado. Si las cargas de trabajo de almacenamiento se encuentran en el umbral de latencia definido en los niveles de servicio de rendimiento asociados, están marcadas como « conformes ». Las cargas de trabajo conformes están marcadas en azul.
  - **No conforme**: Durante la supervisión del rendimiento, las cargas de trabajo de almacenamiento se marcan como «no conformes» si la latencia de las cargas de trabajo de almacenamiento supera el umbral de latencia definido en el nivel de servicio de rendimiento asociado. Las cargas de trabajo no conformes se marcan en naranja.
  - **No disponible**: Las cargas de trabajo de almacenamiento se marcan como "'indisponible'" si están desconectadas o si el clúster correspondiente no es accesible. Las cargas de trabajo no disponibles se marcan en rojo.
- **Sin asignar**: Las cargas de trabajo de almacenamiento que no tienen asignado un nivel de servicio de

rendimiento se indican como "'unassigned'". El número se transmite mediante el icono de información.

El número total de cargas de trabajo es la suma del total de las cargas de trabajo asignadas y sin asignar.

Puede hacer clic en el número total de cargas de trabajo que se muestran en esta sección y visualizarlas en la página cargas de trabajo.

La subsección conformidad por niveles de servicio de rendimiento muestra el número total de cargas de trabajo de almacenamiento disponibles:

- Conforme a cada tipo de nivel de servicio de rendimiento
- Para el cual no hay coincidencia entre los niveles de servicio de rendimiento asignado y recomendado

Sección de información general del centro de datos

En la sección de información general del centro de datos se representa gráficamente la capacidad disponible y utilizada, además de las IOPS para todos los clústeres del centro de datos. Con estos datos, debe gestionar la capacidad y las IOPS de las cargas de trabajo de almacenamiento. En la sección también se muestra la siguiente información de las cargas de trabajo de almacenamiento en todos los clústeres:

- La capacidad total, disponible y utilizada en todos los clústeres del centro de datos
- La tasa de IOPS total, disponible y utilizada para todos los clústeres del centro de datos
- La capacidad disponible y utilizada según cada nivel de servicio de rendimiento
- La tasa de IOPS disponible y utilizada en función de cada nivel de servicio de rendimiento
- El espacio total y las IOPS utilizadas por las cargas de trabajo que no tienen asignado un nivel de servicio de rendimiento

Cómo se calcula la capacidad y el rendimiento del centro de datos en función de los niveles de servicio de rendimiento

La capacidad utilizada y las IOPS se recuperan en términos de la capacidad total utilizada y del rendimiento de todas las cargas de trabajo de almacenamiento de los clústeres.

La IOPS disponible se calcula en función de la latencia esperada y los niveles de servicio de rendimiento recomendados en los nodos. Incluye las IOPS disponibles para todos los niveles de servicio de rendimiento cuya latencia esperada sea menor o igual a su propia latencia esperada.

La capacidad disponible se calcula en función de la latencia esperada y los niveles de servicio de rendimiento recomendados en los agregados. Incluye la capacidad disponible para todos los niveles de servicio de rendimiento cuya latencia esperada es menor o igual a su propia latencia esperada.

Ver cargas de trabajo

Cuando se añaden clústeres a Unified Manager, las cargas de trabajo de almacenamiento de cada clúster se detectan y se muestran automáticamente en la página Workloads.

Unified Manager comienza a analizar las cargas de trabajo para recomendación (PSU recomendados) solo después de que comiencen las operaciones de I/o en las cargas de trabajo de almacenamiento.

Se excluyen los volúmenes de FlexGroup y sus componentes.

Información general de cargas de trabajo

La página Workloads Overview muestra la descripción general de las cargas de trabajo en el centro de datos y la descripción general de espacio y rendimiento del centro de datos.

- Panel **Resumen de cargas de trabajo**: Muestra el número total de cargas de trabajo y el número de cargas de trabajo con o sin las PSLs asignadas en ellas. También se muestra el desglose del número de cargas de trabajo de cada PSL. Al hacer clic en los recuentos, se puede acceder a la vista **todas las cargas de trabajo** con las cargas de trabajo filtradas. También puede ver el número de cargas de trabajo que no se ajustan a la recomendación del sistema y asignar las PSLs recomendadas por el sistema haciendo clic en el botón **asignar PSLs** recomendados por el sistema.
- **Panel de visión general del centro de datos**: Muestra el espacio disponible y utilizado (TIB) y el rendimiento (IOPS) del centro de datos. También se muestra un desglose de los espacios disponibles y utilizados (TIB) y el rendimiento (IOPS) de todas las cargas de trabajo en cada PSL.

Vista All Workloads

La página **almacenamiento > cargas de trabajo > todas las cargas de trabajo** muestra las cargas de trabajo de almacenamiento asociadas con los clústeres de ONTAP gestionados por Unified Manager.

En el caso de las cargas de trabajo de almacenamiento recién descubiertas en las que no se han realizado operaciones de I/o, el estado es «'esperando a que se produzca un I/o». Cuando las operaciones de I/o empiezan en las cargas de trabajo de almacenamiento, Unified Manager inicia el análisis y el estado de la carga de trabajo cambia a «'Aprendizaje…». Una vez completado el análisis (dentro de las 24 horas desde el comienzo de las operaciones de I/o), se muestran los PSU recomendados para las cargas de trabajo de almacenamiento.

La página también permite asignar políticas de eficiencia del almacenamiento (SAP) y niveles de servicio de rendimiento (PSU) a las cargas de trabajo de almacenamiento. Es posible realizar varias tareas:

- Añada o aprovisione cargas de trabajo de almacenamiento
- Ver y filtrar la lista de cargas de trabajo
- Asignación de PSU a las cargas de trabajo de almacenamiento
- Evaluar los archivos PSL recomendados por el sistema y asignarlos a las cargas de trabajo
- Asignación de ASP a cargas de trabajo de almacenamiento

Agregar o aprovisionar cargas de trabajo de almacenamiento

Puede agregar o aprovisionar las cargas de trabajo de almacenamiento a LUN compatibles (compatibles tanto con los protocolos iSCSI como FCP), recursos compartidos de archivos NFS y recursos compartidos SMB.

Pasos

1. Haga clic en **almacenamiento > cargas de trabajo > todas las cargas de trabajo > Crear**.
2. Crear cargas de trabajo. Para obtener más información, consulte "Aprovisionamiento y gestión de cargas de trabajo".

Visualización y filtrado de cargas de trabajo

En la pantalla todas las cargas de trabajo, es posible ver todas las cargas de trabajo del centro de datos o buscar cargas de trabajo de almacenamiento específicas según sus PSU o sus nombres. Puede usar el icono de filtro para introducir condiciones específicas para su búsqueda. Puede buscar por diferentes condiciones de filtro, como por el clúster de hosts o la máquina virtual de almacenamiento. La opción **capacidad total**

permite filtrar por la capacidad total de las cargas de trabajo (por MB). Sin embargo, en este caso, el número de cargas de trabajo que se devuelve puede variar, ya que la capacidad total se compara a nivel de byte.

Para cada carga de trabajo, se muestra información, como el clúster de hosts y la máquina virtual de almacenamiento, junto con el PSL y SEP asignados.

La página también permite ver los detalles de rendimiento de una carga de trabajo. Para ver información detallada sobre las IOPS, la capacidad y la latencia de la carga de trabajo, haga clic en el botón **elegir / columnas de pedido** y seleccione columnas específicas para ver. La columna Performance View muestra la tasa media y máxima de IOPS de una carga de trabajo, y puede hacer clic en el icono del analizador de cargas de trabajo para ver el análisis detallado de IOPS.

Análisis de criterios de rendimiento y capacidad para una carga de trabajo

El botón **analizar carga de trabajo** del menú emergente **Análisis IOPS** le lleva a la página Análisis de carga de trabajo, donde puede seleccionar un intervalo de tiempo y ver las tendencias de latencia, rendimiento y capacidad para la carga de trabajo seleccionada. Para obtener más información acerca del analizador de cargas de trabajo, consulte "Solucionar problemas de cargas de trabajo mediante el analizador de cargas de trabajo".

Puede ver información de rendimiento sobre una carga de trabajo para ayudarle con la solución de problemas haciendo clic en el icono del gráfico de barras en la columna **Vista de rendimiento**. Para ver los gráficos de rendimiento y capacidad en la página Análisis de carga de trabajo para analizar el objeto, haga clic en el botón **analizar carga de trabajo**.

Para obtener más información, consulte "¿Qué datos muestra el analizador de cargas de trabajo".

Asignar políticas a cargas de trabajo

Puede asignar políticas de eficiencia del almacenamiento (ASP) y niveles de servicio de rendimiento (PSLs) a cargas de trabajo de almacenamiento desde la página todas las cargas de trabajo mediante las distintas opciones de navegación.

Asignación de políticas a una sola carga de trabajo

Es posible asignar un PSL, UN SEP o ambos, a una sola carga de trabajo. Siga estos pasos:

1. Seleccionar la carga de trabajo.
2. Haga clic en el icono de edición situado junto a la fila y, a continuación, haga clic en **Editar**.

   Los campos **nivel de servicio de rendimiento asignado** y **Política de eficiencia de almacenamiento** están activados.

3. Seleccione el PSL o SEP requerido, o ambos.
4. Haga clic en el icono de comprobación para aplicar los cambios.

> También puede seleccionar una carga de trabajo y hacer clic en **más acciones** para asignar las políticas.

Asignar políticas a varias cargas de trabajo de almacenamiento

Es posible asignar un PSL o UN SEP a varias cargas de trabajo de almacenamiento juntas. Siga estos pasos:

1. Seleccione las casillas de comprobación de las cargas de trabajo a las que desea asignar la política o seleccione todas las cargas de trabajo del centro de datos.
2. Haga clic en **más acciones**.
3. Para asignar un PSL, seleccione **asignar nivel de servicio de rendimiento**. Para asignar UN SEP, seleccione **asignar directiva de eficiencia del almacenamiento**. Aparecerá una ventana emergente que le permitirá seleccionar la directiva.
4. Seleccione la directiva adecuada y haga clic en **aplicar**. Se muestra el número de cargas de trabajo a las que se asignan las políticas. También se enumeran las cargas de trabajo en las que no se asignan las políticas, con la causa.

> La aplicación de políticas en cargas de trabajo de forma masiva puede tardar algún tiempo, según el número de cargas de trabajo seleccionadas. Puede hacer clic en el botón **Ejecutar en segundo plano** y continuar con otras tareas mientras la operación se ejecuta en segundo plano. Una vez finalizada la asignación masiva, puede ver el estado de finalización. Si se aplica un PSL en varias cargas de trabajo, no es posible activar otra solicitud cuando se ejecuta el trabajo anterior de asignación masiva.

Asignación de PSU recomendados por el sistema a cargas de trabajo

Puede asignar LSP recomendadas por el sistema a estas cargas de trabajo de almacenamiento en un centro de datos que no tiene LSP asignadas o los LSP asignados no coinciden con las recomendaciones del sistema. Para utilizar esta funcionalidad, haga clic en el botón **asignar archivos PSL** recomendados por el sistema. No es necesario seleccionar cargas de trabajo específicas.

La recomendación se determina internamente mediante análisis del sistema y se omite para aquellas cargas de trabajo cuyos IOPS y otros parámetros no coinciden con las definiciones de cualquier PSL disponible. Almacenamiento de cargas de trabajo con `Waiting for I/O` Y los Estados de aprendizaje también están excluidos.

> Existen palabras clave especiales que Unified Manager busca en el nombre de la carga de trabajo para anular el análisis del sistema y recomendar una PSL diferente para la carga de trabajo. Cuando la carga de trabajo tenga las letras "'ora'" en el nombre, se recomienda **Extreme Performance**PSL. Y cuando la carga de trabajo tenga las letras "'vm'" en el nombre, se recomienda **Performance**PSL.

También consulte el artículo de la base de conocimientos (KB) "El valor de ActiveIQ Unified Manager "Assign System recommended Performance Service Level" no es adaptable a una carga de trabajo de alta variable"

Aprovisionar los volúmenes compartidos de archivos

Es posible crear volúmenes de recursos compartidos de archivos compatibles con los protocolos CIFS/SMB y NFS en un clúster existente y Storage Virtual Machine (VM de almacenamiento) desde la página de carga de trabajo de aprovisionamiento.

Lo que necesitará

- El equipo virtual de almacenamiento debe tener espacio para aprovisionar el volumen compartido de archivos.
- Debe habilitarse uno de los servicios de SMB y NFS en el equipo virtual de almacenamiento.
- Para seleccionar y asignar el nivel de servicio de rendimiento (PSL) y la política de eficiencia de

almacenamiento (SEP) en la carga de trabajo, es necesario crear las políticas antes de comenzar a crear la carga de trabajo.

Pasos

1. En la página **Provision Workload**, agregue el nombre de la carga de trabajo que desea crear y, a continuación, seleccione el clúster de la lista Available.
2. En función del clúster que haya seleccionado, el campo **VM de ALMACENAMIENTO** filtra los equipos virtuales de almacenamiento disponibles para ese clúster. Seleccione la máquina virtual de almacenamiento que desee de la lista.

   En función de los servicios SMB y NFS admitidos en la máquina virtual de almacenamiento, la opción NAS se habilita en la sección Host Information.

3. En la sección Storage and Optimization, asigne la capacidad de almacenamiento y PSL, y de manera opcional, UN SEP para la carga de trabajo.

   Las especificaciones para SEP se asignan a la LUN y las definiciones de PSL se aplican a la carga de trabajo cuando se crea.

4. Active la casilla de verificación **imponer límites de rendimiento** si desea aplicar la PSL que se ha asignado a la carga de trabajo.

   Al asignar un PSL a una carga de trabajo, el agregado en el que se crea la carga de trabajo puede admitir los objetivos de rendimiento y capacidad definidos en la política respectiva. Por ejemplo, si se asigna una carga de trabajo "Extreme Performance "PSL", el agregado en el que se aprovisiona la carga de trabajo debe tener la capacidad de admitir los objetivos de rendimiento y capacidad de la política de "rendimiento extremo", como el almacenamiento SSD.

   A menos que se seleccione esta casilla de comprobación, PSL no se aplica a la carga de trabajo y el estado de la carga de trabajo en la consola se muestra como sin asignar.

5. Seleccione la opción **NAS**.

   Si no puede ver la opción **NAS** activada, compruebe si el equipo virtual de almacenamiento que ha seleccionado es compatible con SMB o NFS, o ambos.

   Si el equipo virtual de almacenamiento está habilitado para los servicios SMB y NFS, puede seleccionar las casillas de verificación **Compartir por NFS** y **Compartir por SMB** y crear un recurso compartido de archivos que admita los protocolos NFS y SMB. Si desea crear un recurso compartido SMB o CIFS, seleccione la casilla de comprobación únicamente correspondiente.

6. En el caso de los volúmenes compartidos de archivos NFS, especifique la dirección IP del host o la red para acceder al volumen de recursos compartidos de archivos. Puede introducir valores separados por comas para varios hosts.

   Cuando se añade la dirección IP del host, se ejecuta una comprobación interna para hacer coincidir los detalles del host con la máquina virtual de almacenamiento y la política de exportación de ese host, o bien, en caso de que exista una política existente, se vuelve a utilizar. Si hay varios recursos compartidos NFS creados para el mismo host, se reutilizará una política de exportación disponible para el mismo host con reglas coincidentes para todos los archivos compartidos. La función de especificar reglas de directivas individuales o volver a utilizar directivas proporcionando claves de directiva específicas está disponible cuando se aprovisiona el recurso compartido NFS mediante API.

7. Para un recurso compartido de SMB, especifique qué usuarios o grupos de usuarios pueden acceder al recurso compartido de SMB y asignar los permisos necesarios. Para cada grupo de usuarios, se genera una nueva lista de control de acceso (ACL) durante la creación del recurso compartido de archivos.
8. Haga clic en **Guardar**.

   La carga de trabajo se añade a la lista de cargas de trabajo de almacenamiento.

Aprovisionar las LUN

Puede crear LUN que sean compatibles con los protocolos CIFS/SMB y NFS en un clúster existente y Storage Virtual Machine (Storage VM) desde la página de carga de trabajo de aprovisionamiento.

Lo que necesitará

- La máquina virtual de almacenamiento debe tener espacio para aprovisionar la LUN.
- Tanto iSCSI como FCP deben estar habilitados en la máquina virtual de almacenamiento donde se crea el LUN.
- Para seleccionar y asignar el nivel de servicio de rendimiento (PSL) y la política de eficiencia de almacenamiento (SEP) en la carga de trabajo, es necesario crear las políticas antes de comenzar a crear la carga de trabajo.

Pasos

1. En la página **Provision Workload**, agregue el nombre de la carga de trabajo que desea crear y, a continuación, seleccione el clúster de la lista Available.

   En función del clúster que haya seleccionado, el campo **VM de ALMACENAMIENTO** filtra los equipos virtuales de almacenamiento disponibles para ese clúster.

2. Seleccione la máquina virtual de almacenamiento de la lista que admite los servicios iSCSI y FCP.

   En función de su selección, LA opción SAN está activada en la sección Información del host.

3. En la sección **almacenamiento y optimización**, asigne la capacidad de almacenamiento y PSL, y opcionalmente, EL SEP para la carga de trabajo.

   Las especificaciones para SEP se asignan a la LUN y las definiciones de PSL se aplican a la carga de trabajo cuando se crea.

4. Active la casilla de verificación **imponer límites de rendimiento** si desea aplicar el PSL asignado a la carga de trabajo.

   Al asignar un PSL a una carga de trabajo, el agregado en el que se crea la carga de trabajo puede admitir los objetivos de rendimiento y capacidad definidos en la política respectiva. Por ejemplo, si se asigna una carga de trabajo al PSL de "rendimiento extremo", el agregado en el que se debe aprovisionar la carga de trabajo debe tener la capacidad de admitir los objetivos de rendimiento y capacidad de la política de "rendimiento extremo", como el almacenamiento SSD.

   A menos que se seleccione esta casilla de comprobación, PSL no se aplica a la carga de trabajo y el estado de la carga de trabajo en la consola se muestra como `unassigned`.

5. Seleccione la opción **SAN**. Si no puede ver la opción **SAN** activada, compruebe si la VM de almacenamiento que ha seleccionado es compatible con iSCSI y FCP.
6. Seleccione el sistema operativo host.
7. Especifique la asignación de host para controlar el acceso de los iniciadores a la LUN. Puede asignar grupos de iniciadores existentes (iGroups), o definir y asignar nuevos iGroups.

   Si crea un nuevo igroup mientras aprovisiona la LUN, debe esperar hasta el siguiente ciclo de detección (hasta 15 minutos) para utilizarlo. Por lo tanto, se recomienda utilizar un igroup existente de la lista de iGroups disponibles.

   Si desea crear un nuevo igroup, seleccione el botón **Crear un nuevo iGroup** e introduzca la información del igroup.

8. Haga clic en **Guardar**.

   El LUN se añade a la lista de cargas de trabajo de almacenamiento.

Niveles de servicio de rendimiento

Un nivel de servicio de rendimiento (PSL) permite definir los objetivos de rendimiento y almacenamiento para una carga de trabajo. Es posible asignar un PSL a una carga de trabajo cuando se crea inicialmente la carga de trabajo, o bien luego editarla.

La gestión y la supervisión de los recursos de almacenamiento se basan en los objetivos de nivel de servicio (SLO). Los acuerdos de nivel de servicio se definen mediante acuerdos de nivel de servicio que se basan en el rendimiento y la capacidad necesarios. En Unified Manager, los objetivos de nivel de servicio se refieren a las definiciones de PSL de las aplicaciones que se ejecutan en el almacenamiento de NetApp. Los servicios de almacenamiento se diferencian en función del rendimiento y la utilización de los recursos subyacentes. Un PSL es una descripción de los objetivos de servicio de almacenamiento. Un PSL permite al proveedor de almacenamiento especificar los objetivos de rendimiento y capacidad para la carga de trabajo. Cuando se asigna una PSL en una carga de trabajo, la carga de trabajo correspondiente en ONTAP se gestiona mediante sus objetivos de rendimiento y capacidad. Cada PSL se rige por IOPS máximas, esperadas y mínimas absolutas, y la latencia esperada.

Unified Manager tiene los siguientes tipos de CAL:

- **Definido por el sistema**: Unified Manager proporciona algunas directivas preparadas que no se pueden modificar. Estas PSLs predefinidas son:
  - Rendimiento extremo
  - Rendimiento
  - Valor

    Las PSU de rendimiento extremo, rendimiento y valor son aplicables a la mayoría de las cargas de trabajo de almacenamiento comunes en un centro de datos.

  Unified Manager también ofrece tres niveles de servicio de rendimiento para aplicaciones de bases de datos. Se trata de PSU de rendimiento extremadamente alto que admiten IOPS por ráfagas y son adecuadas para aplicaciones de base de datos con la mayor demanda de rendimiento.

  - Extreme para registros de bases de datos

- Extremo para datos compartidos de bases de datos
- Extremadamente para datos de bases de datos

- **Definido por el usuario**: Si los niveles predefinidos de Servicio de rendimiento no cumplen sus requisitos, puede crear nuevos archivos DLL para satisfacer sus necesidades. Para obtener más información, consulte "Creación y edición de niveles de servicio de rendimiento".
- **Beyond Extreme**: Los archivos DLL de Beyond Extreme son los archivos DLL recomendados por el sistema que se sugieren para cargas de trabajo que requieren IOPS más alto que Extreme. Las cargas de trabajo se analizan internamente en función de sus IOPS, su capacidad y su latencia, y se recomienda un PSL superior a Extreme para cada una de estas cargas de trabajo en la pantalla **almacenamiento > cargas de trabajo > todas las cargas de trabajo**. Puede aplicar las PSU a las cargas de trabajo para garantizar un rendimiento óptimo.

  Los parámetros de IOPS para las cargas de trabajo se generan de forma dinámica, según el comportamiento de la carga de trabajo, y se añaden al nombre de Beyond Extreme PSL en el formato `Beyond Extreme <number-(peak IOPS/TB)> <number(expected IOPS/TB)>`. Por ejemplo, si el sistema determina una carga de trabajo con el pico y el nivel esperado de IOPS como `106345` y.. `37929` Respectivamente, se denomina como Beyond Extreme PSL que se genera para la carga de trabajo `Beyond Extreme 106345 37929`. Aunque el sistema recomienda estos archivos DLL, cuando se asignan a cargas de trabajo, estos archivos se etiquetan como `User-defined` de tipo.

Gestión de cargas de trabajo mediante la asignación de PSU

Puede acceder a los archivos DLL desde la página **políticas** > **niveles de servicio de rendimiento** y utilizando las API del proveedor de almacenamiento. La gestión de las cargas de trabajo de almacenamiento mediante la asignación de PSU a ellas resulta práctica, ya que no tiene que gestionar de forma individual las cargas de trabajo de almacenamiento. Cualquier modificación también se puede gestionar reasignando otro PSL en lugar de administrarlas individualmente. Unified Manager le ayuda a asignar CAL en sus cargas de trabajo en función de la evaluación interna y las recomendaciones.

Para obtener más información sobre la asignación de archivos DLL recomendados por el sistema a las cargas de trabajo, consulte "Asignación de PSU recomendados por el sistema a cargas de trabajo"

La página Performance Service indica las políticas PSL disponibles y permite añadirlas, editarlas y eliminarlas.

> No es posible modificar un PSL definido por el sistema o asignado actualmente a una carga de trabajo. No es posible eliminar un PSL que se asigna a una carga de trabajo o si es el único PSL disponible.

Esta página muestra la siguiente información:

Campo	Descripción
Nombre	Nombre del PSL.
Tipo	Si la política está definida por el sistema o por el usuario.

Campo	Descripción
Tasa prevista de IOPS/TB	Número mínimo de IOPS que se espera que realice una aplicación en un LUN o un recurso compartido de archivos. IOPS esperado especifica las IOPS mínimas esperadas asignadas, según el tamaño del objeto de almacenamiento asignado.
Pico de IOPS/TB	Número máximo de IOPS que puede realizar una aplicación en un LUN o un recurso compartido de archivos. Pico de IOPS especifica el número máximo de IOPS asignadas, según el tamaño del objeto de almacenamiento asignado o el tamaño del objeto de almacenamiento utilizado. El número máximo de IOPS se basa en una política de asignación. La política de asignación es espacio asignado o espacio utilizado. Cuando se establece la política de asignación en espacio asignado, el pico de IOPS se calcula en función del tamaño del objeto de almacenamiento. Cuando se establece la política de asignación en espacio de uso, el IOPS máximo se calcula en función de la cantidad de datos almacenados en el objeto de almacenamiento, teniendo en cuenta las eficiencias de almacenamiento. De forma predeterminada, la directiva de asignación se establece en espacio utilizado.

Campo	Descripción
IOPS mínimo absoluto	El valor mínimo de IOPS absoluto se utiliza como anulación cuando el número de IOPS esperado es inferior a este valor. Los valores predeterminados de las DLL definidas por el sistema son los siguientes: • Rendimiento extremo: Si se espera un IOPS >= 6144/TB, el valor mínimo absoluto de IOPS = 1000 • Rendimiento: Si se espera un IOPS >= 2048/TB y < 6144/TB, el valor mínimo absoluto de IOPS es 500 • Valor: Si se espera IOPS >= 128/TB y < 2048/TB, entonces el mínimo absoluto de IOPS = 75 Los valores predeterminados de las DLL de base de datos definidas por el sistema son los siguientes: • Extreme for Database Logs: Si espera IOPS >= 22528, entonces el valor mínimo absoluto de IOPS = 4000 • Extreme para datos compartidos de bases de datos: Si espera IOPS >= 16384, entonces el valor mínimo absoluto de IOPS = 2000 • Extreme para datos de bases de datos: Si espera IOPS >= 12288, entonces el valor mínimo absoluto de IOPS = 2000 El mayor valor de IOPS mínimo absoluto para las DLL personalizadas puede ser un máximo de 75000. El valor inferior se calcula de la siguiente forma: 1000/latencia esperada
Latencia esperada	Latencia esperada para IOPS de almacenamiento en milisegundos por operación (ms/op).
Capacidad	La capacidad total disponible y utilizada en los clústeres.
Cargas de trabajo	Cantidad de cargas de trabajo de almacenamiento a las que se asigna PSL.

Para obtener más información sobre cómo ayudan las IOPS máximas y los IOPS esperados en lograr un rendimiento diferenciado constante en los clústeres de ONTAP, consulte el siguiente artículo de la base de conocimientos:https://kb.netapp.com/Advice_and_Troubleshooting/Data_Infrastructure_Management/Active_IQ_Unified_Manager/What_is_Performance_Budgeting%3F["¿Qué es la gestión presupuestaria del rendimiento?"]

Los eventos generados para cargas de trabajo que traspasa el umbral definido por los archivos DLL

Tenga en cuenta que si las cargas de trabajo superan el valor de latencia esperado durante el 30 % del tiempo durante la hora anterior, Unified Manager genera uno de los siguientes eventos para notificarle un posible problema de rendimiento:

- Se superó el umbral de latencia del volumen de cargas de trabajo definido por la política de nivel de servicio de rendimiento
- Se superó el umbral de latencia de LUN de carga de trabajo definido por la política de nivel de servicio de rendimiento.

Puede que se desee analizar la carga de trabajo para ver qué puede estar causando los valores de latencia más altos.

Para más información, consulte los siguientes enlaces:

- "Eventos de volumen"
- "Qué sucede cuando se incumple una política de umbral de rendimiento"
- "Cómo Unified Manager utiliza la latencia de carga de trabajo para identificar problemas de rendimiento"
- "¿Qué eventos de rendimiento son"

PSU definidos por el sistema

En la siguiente tabla se proporciona información acerca de las DLL definidas por el sistema:

Nivel de servicio de rendimiento	Descripción y caso de uso	Latencia esperada (ms/op)	Pico de IOPS	IOPS esperada	IOPS mínimo absoluto
Rendimiento extremo	Proporciona un rendimiento extremadamente alto con una latencia muy baja Son perfectas para aplicaciones sensibles a la latencia	1	12288	6144	1000
Rendimiento	Proporciona un alto rendimiento a una baja latencia Ideal para aplicaciones virtualizadas y bases de datos	2	4096	2048	500

Nivel de servicio de rendimiento	Descripción y caso de uso	Latencia esperada (ms/op)	Pico de IOPS	IOPS esperada	IOPS mínimo absoluto
Valor	Proporciona una alta capacidad de almacenamiento y una latencia moderada Ideal para aplicaciones de gran capacidad, como correo electrónico, contenido web, recursos compartidos de archivos y destinos de backup	17	512	128	75
Extreme para registros de bases de datos	Proporciona el máximo rendimiento con la menor latencia. Ideal para aplicaciones de base de datos que admiten registros de bases de datos. Este PSL ofrece el rendimiento más alto porque los registros de bases de datos son extremadamente potentes y el registro está constantemente bajo demanda.	1	45056	22528	4000

Nivel de servicio de rendimiento	Descripción y caso de uso	Latencia esperada (ms/op)	Pico de IOPS	IOPS esperada	IOPS mínimo absoluto
Extremo para datos compartidos de bases de datos	Proporciona un rendimiento muy elevado con la latencia más baja. Ideal para datos de aplicaciones de base de datos que se almacenan en un almacén de datos común, pero que se comparten entre bases de datos.	1	32768	16384	2000
Extremadamente para datos de bases de datos	Proporciona un alto rendimiento con la latencia más baja. Ideal para datos de aplicaciones de base de datos, como metadatos y información de tablas de bases de datos.	1	24576	12288	2000

Creación y edición de niveles de servicio de rendimiento

Cuando los niveles de servicio de rendimiento definidos por el sistema no coinciden con los requisitos de la carga de trabajo, puede crear sus propios niveles de servicio de rendimiento optimizados para sus cargas de trabajo.

Lo que necesitará

- Debe tener la función Administrador de aplicaciones.
- El nombre de nivel de servicio de rendimiento debe ser único y no se pueden utilizar las siguientes palabras clave reservadas:

  `Prime`, `Extreme`, `Performance`, `Value`, `Unassigned`, `Learning`, `Idle`, `Default`, y. `None`.

Se pueden crear y editar niveles de servicio de rendimiento personalizados desde la página niveles de servicio de rendimiento definiendo los objetivos de nivel de servicio necesarios para las aplicaciones que accederán al almacenamiento.

No es posible modificar un nivel de servicio de rendimiento si actualmente se asigna a una carga de trabajo.

Pasos

1. En el panel de navegación izquierdo, en **Configuración**, seleccione **Directivas** > **niveles de servicio de rendimiento**.
2. En la página **niveles de servicio de rendimiento**, haga clic en el botón apropiado en función de si desea crear un nuevo nivel de servicio de rendimiento o si desea editar un nivel de servicio de rendimiento existente.

Para…	Siga estos pasos…
Cree un nuevo nivel de servicio de rendimiento	Haga clic en **Agregar**.
Edite un nivel de servicio de rendimiento existente	Seleccione un nivel de servicio de rendimiento existente y, a continuación, haga clic en **Editar**.

   Se muestra la página para agregar o editar un nivel de servicio de rendimiento.

3. Personalice el nivel de servicio de rendimiento especificando los objetivos de rendimiento y, a continuación, haga clic en **Enviar** para guardar el nivel de servicio de rendimiento.

Puede aplicar el nivel de servicio de rendimiento nuevo o modificado a las cargas de trabajo (LUN, recursos compartidos de archivos NFS, recursos compartidos de CIFS) desde la página de cargas de trabajo o al aprovisionar una nueva carga de trabajo.

Gestión de políticas de eficiencia del almacenamiento

UNA Política de eficiencia del almacenamiento (SEP) permite definir las características de eficiencia del almacenamiento de una carga de trabajo. Se puede asignar UNA SEP a una carga de trabajo al crear inicialmente la carga de trabajo, o después editar la carga de trabajo.

La eficiencia del almacenamiento incluye el uso de tecnologías, como thin provisioning, deduplicación y compresión de datos que aumentan el aprovechamiento del almacenamiento y reducen los costes de almacenamiento. Al crear APP, puede utilizar estas tecnologías que permiten ahorrar espacio de forma individual o conjunta para lograr la máxima eficacia de almacenamiento. Cuando asocia las políticas con las cargas de trabajo de almacenamiento, los ajustes de política especificados se asignan a ellas. Unified Manager le permite asignar SEPS definidos por el sistema y por el usuario para optimizar los recursos de almacenamiento en su centro de datos.

Unified Manager proporciona dos Sep definidos por el sistema: Alto y bajo. Estos Sep son aplicables a la mayoría de las cargas de trabajo de almacenamiento de un centro de datos; sin embargo, puede crear sus propias normas si los PES definidos por el sistema no cumplen sus requisitos.

No puede modificar un SEP que esté definido por el sistema o que esté asignado actualmente a una carga de trabajo. No puede eliminar UN SEP que esté asignado a una carga de trabajo, o si es el único SEP disponible.

La página Directivas de eficiencia del almacenamiento enumera los Sep disponibles y le permite agregar, editar y eliminar datos SEP personalizados. Esta página muestra la siguiente información:

Campo	Descripción
Nombre	Nombre DEL SEP.
Tipo	Si la política está definida por el sistema o por el usuario.
Reserva de espacio	Si el volumen tiene thin provisioning o thick-Provisioning.
Deduplicación	Si la deduplicación está activada en la carga de trabajo: • Inline: La deduplicación se produce mientras se escribe en la carga de trabajo • Fondo: La deduplicación ocurre en la carga de trabajo • Disable: La deduplicación está deshabilitada en la carga de trabajo
Compresión	Si la compresión de datos está habilitada en la carga de trabajo: • Inline: La compresión de datos se produce mientras se escribe en la carga de trabajo • Background: La compresión de datos se produce en la carga de trabajo • Disable: La compresión de datos está deshabilitada en la carga de trabajo
Cargas de trabajo	Número de cargas de trabajo de almacenamiento a LAS que SE asignó SEP

Directrices para crear una Política de eficiencia del almacenamiento personalizada

Si los Sep existentes no cumplen los requisitos de las normativas para las cargas de trabajo de almacenamiento, puede crear UN SEP personalizado. Sin embargo, se recomienda intentar utilizar los SEP definidos por el sistema para las cargas de trabajo de almacenamiento, y solo crear SEP personalizados si es necesario.

Puede ver EL SEP asignado a las cargas de trabajo en la página todas las cargas de trabajo y en la página de detalles Volume / Health. Es posible ver la tasa de reducción de datos a nivel de clúster según estas eficiencias del almacenamiento en el panel capacidad de la consola y en la vista capacidad: All Clusters.

Crear y editar políticas de eficiencia del almacenamiento

Cuando las políticas de eficiencia del almacenamiento definidas por el sistema no coinciden con los requisitos de carga de trabajo, puede crear sus propias políticas de eficiencia del almacenamiento optimizadas para sus cargas de trabajo.

Lo que necesitará

- Debe tener la función Administrador de aplicaciones.
- El nombre de la política de eficiencia de almacenamiento debe ser único y no se pueden utilizar las siguientes palabras clave reservadas:

  `High`, `Low`, `Unassigned`, `Learning`, `Idle`, `Default`, y. `None`.

Puede crear y editar políticas personalizadas de eficiencia del almacenamiento desde la página políticas de eficiencia del almacenamiento definiendo las características de eficiencia del almacenamiento necesarias para las aplicaciones que accederán al almacenamiento.

No puede modificar una Política de eficiencia del almacenamiento si actualmente se asigna a una carga de trabajo.

Pasos

1. En el panel de navegación izquierdo, en **Ajustes**, seleccione **Directivas** > **eficiencia del almacenamiento**.
2. En la página **políticas de eficiencia del almacenamiento**, haga clic en el botón apropiado dependiendo de si desea crear una nueva Política de eficiencia del almacenamiento o si desea editar una Política de eficiencia del almacenamiento existente.

Para…	Siga estos pasos…
Cree una nueva Política de eficiencia del almacenamiento	Haga clic en **Agregar**
Editar una Política de eficiencia del almacenamiento existente	Seleccione una Política de eficiencia del almacenamiento existente y haga clic en **Editar**

   Se muestra la página para añadir o editar una Política de eficiencia del almacenamiento.

3. Personalice la Política de eficiencia del almacenamiento especificando las características de eficiencia del almacenamiento y, a continuación, haga clic en **Enviar** para guardar la Política de eficiencia del almacenamiento.

Puede aplicar la Política de eficiencia del almacenamiento nueva o modificada a las cargas de trabajo (LUN, recursos compartidos de archivos NFS, recursos compartidos de CIFS) desde la página de cargas de trabajo o al aprovisionar una carga de trabajo nueva.

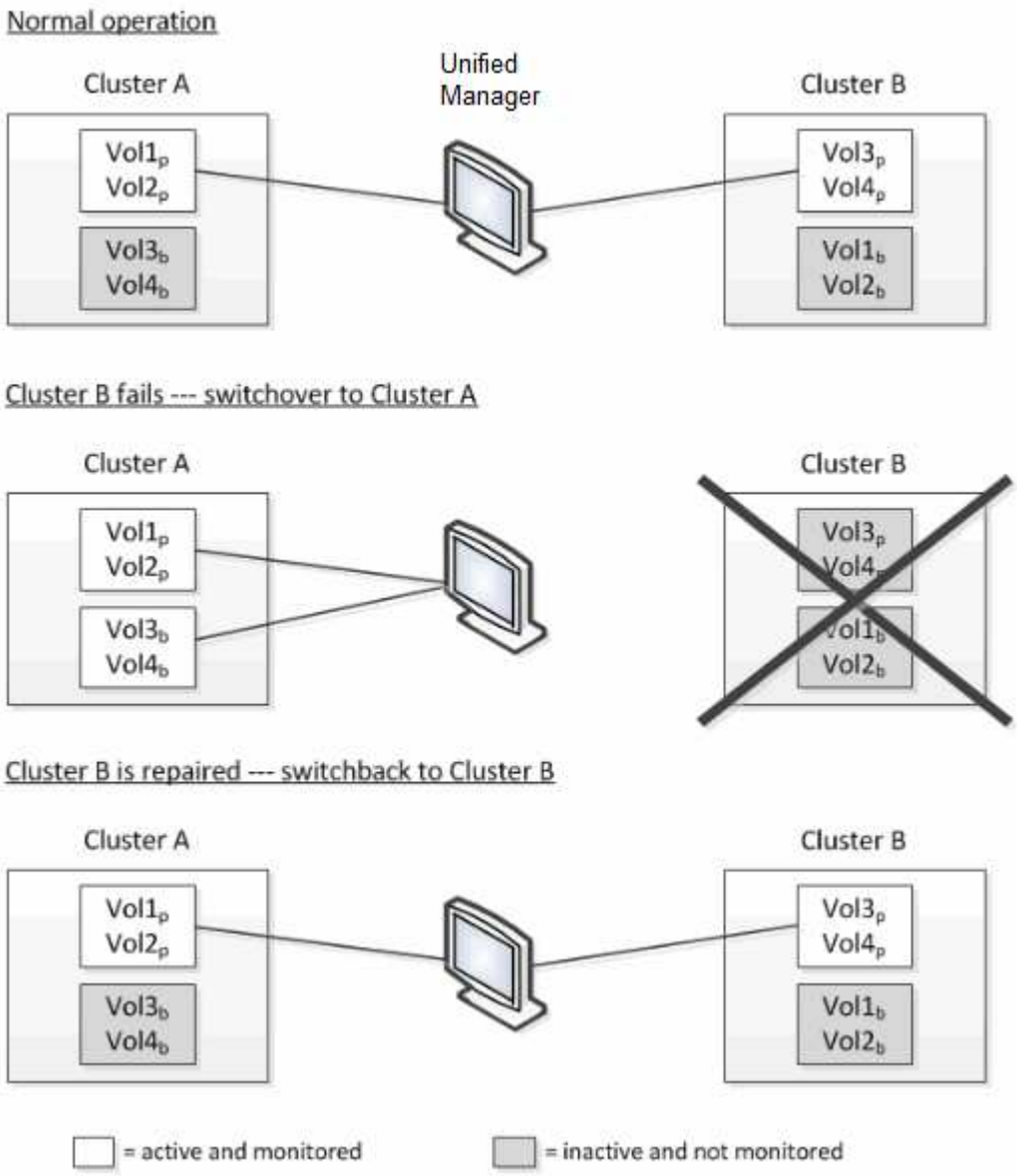
Gestionar y supervisar configuraciones de MetroCluster

La supervisión de la compatibilidad con las configuraciones de MetroCluster en la interfaz de usuario web de Unified Manager le permite comprobar si existen problemas de conectividad en las configuraciones de MetroCluster over FC e IP. Al detectar un problema de conectividad en las primeras etapas, es posible gestionar las configuraciones de MetroCluster de forma eficaz.

Comportamiento del volumen durante la conmutación de sitios y la conmutación de estado

Los eventos que activan una conmutación de sitios o una conmutación de estado hacen que los volúmenes activos se muevan de un clúster a otro en el grupo de recuperación ante desastres. Se detienen los volúmenes del clúster activos y sirven datos a los clientes, y los volúmenes del otro clúster se activan y comienzan a servir datos. Unified Manager supervisa solo los volúmenes que están activos y en ejecución.

Dado que los volúmenes se mueven de un clúster a otro, se recomienda supervisar ambos clústeres. Una única instancia de Unified Manager puede supervisar ambos clústeres en una configuración de MetroCluster, pero en ocasiones la distancia entre las dos ubicaciones requiere el uso de dos instancias de Unified Manager para supervisar ambos clústeres. En la siguiente figura, se muestra una sola instancia de Unified Manager:



Los volúmenes con p en sus nombres indican los volúmenes primarios, y los volúmenes con b en sus nombres son volúmenes de backup reflejados creados por SnapMirror.

Durante el funcionamiento normal:

- El clúster A tiene dos volúmenes activos: Vol1p y Vol2p.
- El clúster B tiene dos volúmenes activos: Vol3p y Vol4p.
- El clúster A tiene dos volúmenes inactivos: Vol3b y Vol4b.
- El clúster B tiene dos volúmenes inactivos: Vol1b y Vol2b.

Unified Manager recopila la información relativa a cada uno de los volúmenes activos (estadísticas, eventos, etc.). Las estadísticas de Vol1p y Vol2p se recogen en el Grupo A, y las estadísticas de Vol3p y Vol4p se recogen en el Grupo B.

Una vez que se produce un fallo catastrófico, se lleva a cabo una conmutación de los volúmenes activos del clúster B al clúster A:

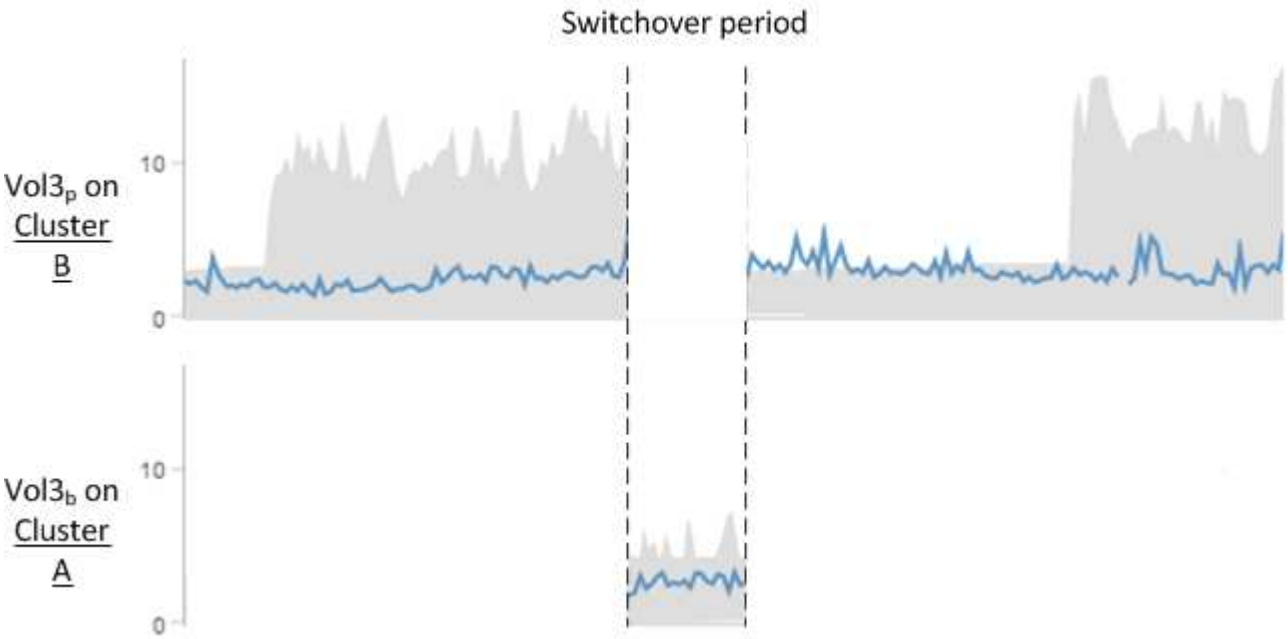
- El clúster A tiene cuatro volúmenes activos: Vol1p, Vol2p, Vol3b y Vol4b.
- El clúster B tiene cuatro volúmenes inactivos: Vol3p, Vol4p, Vol1b y Vol2b.

Como durante el funcionamiento normal, Unified Manager recopila la información relacionada con cada uno de los volúmenes activos. Pero en este caso, las estadísticas de Vol1p y Vol2p son recogidas por el Grupo A, y las estadísticas de Vol3b y Vol4b también son recogidas por el Grupo A.

Tenga en cuenta que Vol3p y Vol3b no son los mismos volúmenes, ya que se encuentran en clústeres diferentes. La información de Unified Manager para Vol3p no es la misma que Vol3b:

- Durante la conmutación al clúster A, las estadísticas y los eventos de Vol3p no se ven.
- En el primer cambio, Vol3b parece un nuevo volumen sin información histórica.

Cuando se repara el clúster B y se realiza una conmutación de regreso, Vol3p vuelve a estar activo en el clúster B, con las estadísticas históricas y una brecha de estadísticas para el período durante el cambio. Vol3b no se puede ver desde el clúster A hasta que se produzca otra conmutación:



- Los volúmenes MetroCluster inactivos, por ejemplo, Vol3b en el clúster A después de la conmutación de estado, se identifican con el mensaje "'este volumen se eliminó'". El volumen no se elimina en realidad, pero Unified Manager no supervisa actualmente porque no es el volumen activo.
- Si una sola instancia de Unified Manager supervisa ambos clústeres en una configuración de MetroCluster, la búsqueda de volúmenes devuelve información de la que esté activo en ese momento. Por ejemplo, una búsqueda para "Vol3" devolverá estadísticas y eventos para Vol3b en el clúster A si se ha producido una conmutación y Vol3 se ha activado en el clúster A.

Definiciones de estado de conectividad de clúster para la configuración de MetroCluster over FC

La conectividad entre los clústeres de una configuración MetroCluster over FC puede ser uno de los siguientes Estados: Optimal, impacted o Down. Comprender los Estados de conectividad permite gestionar las configuraciones de MetroCluster de forma efectiva.

Estado de conectividad	Descripción	Icono mostrado
Óptimo	La conectividad entre los clústeres de la configuración de MetroCluster es normal.	
Afectados	Uno o varios errores comprometen el estado de disponibilidad de conmutación al nodo de respaldo; sin embargo, ambos clústeres de la configuración de MetroCluster siguen en funcionamiento. Por ejemplo, cuando el enlace ISL está inactivo, cuando el enlace IP del interconexión de clústeres está inactivo o cuando no se puede acceder al clúster asociado.	
Abajo	La conectividad entre los clústeres de la configuración de MetroCluster está inactiva debido a que uno o ambos clústeres están inactivos o a que los clústeres se encuentran en modo de conmutación por error. Por ejemplo, cuando el clúster de partners está inactivo a causa de un desastre o cuando hay una conmutación por error planificada para fines de prueba.	Conmutación de sitios con errores: Conmutación de sitios correcta:

Definiciones de estado de mirroring de datos para MetroCluster over FC

Las configuraciones de MetroCluster over FC proporcionan mirroring de datos y la capacidad adicional de iniciar una conmutación por error si deja de estar disponible un sitio completo. El estado de mirroring de datos entre los clústeres de una configuración de MetroCluster over FC puede ser normal o no hay disponibilidad de mirroring. Comprender el estado le permite gestionar su configuración de MetroCluster de forma eficaz.

Estado de mirroring de datos	Descripción	Icono mostrado
Normal	La duplicación de datos entre los clústeres de la configuración de MetroCluster es normal.	
Mirroring no disponible	El mirroring de datos entre los clústeres de la configuración de MetroCluster no está disponible debido a una conmutación de sitios. Por ejemplo, cuando el clúster de partners está inactivo a causa de un desastre o cuando hay una conmutación por error planificada para fines de prueba.	Conmutación de sitios con errores: Conmutación de sitios correcta:

Supervisar las configuraciones de MetroCluster

Puede supervisar los problemas de conectividad en la configuración de MetroCluster. Los detalles incluyen el estado de los componentes y la conectividad dentro de un clúster y el estado de conectividad entre los clústeres de la configuración de MetroCluster. Aquí podrá conocer cómo supervisar los problemas de conectividad en clústeres protegidos por configuraciones MetroCluster over FC e MetroCluster over IP.

Puede supervisar las configuraciones de MetroCluster desde las siguientes vistas en el panel de navegación de la izquierda de Active IQ Unified Manager:

- **Almacenamiento** > **Clusters** > **Protección: Vista MetroCluster**
- **Protección** > **Relaciones** > **relación: MetroCluster** vista

Unified Manager utiliza las alertas de estado del sistema para indicar el estado de los componentes y la conectividad en la configuración de MetroCluster.

Lo que necesitará

- Los clústeres local y remoto de una configuración de MetroCluster deben añadirse a Active IQ Unified Manager.

- En una configuración MetroCluster sobre IP, si se va a admitir un Mediator, el Mediator debe configurarse y agregarse al clúster mediante la API correspondiente.
- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Supervise los problemas de conectividad en la configuración de MetroCluster over FC

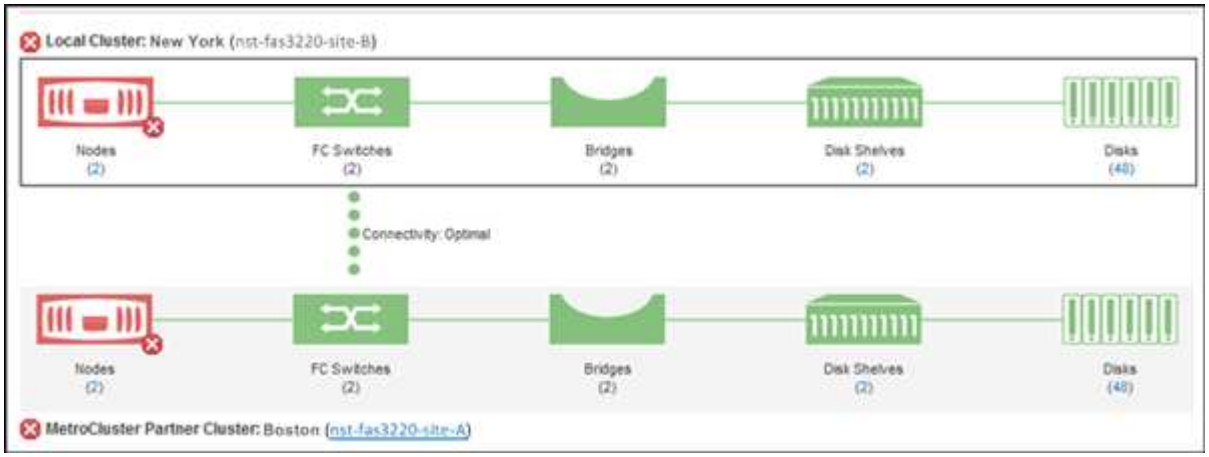
Para los clústeres de una configuración MetroCluster over FC, los gráficos de conectividad se muestran en la página de detalles **Cluster / Health**. Siga estos pasos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **clústeres**.

   Se muestra una lista de todos los clústeres supervisados.

2. En la vista **Protección: MetroCluster**, haga clic en el nombre del clúster para el que desea ver los detalles de configuración de MetroCluster sobre FC. De forma alternativa, puede filtrar por clústeres en una configuración de MetroCluster.
3. En la página de detalles **Cluster / Health**, haga clic en la ficha **conectividad MetroCluster**. La ficha **conectividad MetroCluster** sólo está disponible para configuraciones MetroCluster sobre FC.



   La topología de la configuración de MetroCluster se muestra en el área de objetos del clúster correspondiente. Puede utilizar la información que se muestra en la página de detalles Cluster / Health para corregir cualquier problema de conectividad. Por ejemplo, si la conectividad entre el nodo y el switch de un clúster está inactiva, se muestra el siguiente icono:

Si mueve el puntero sobre el icono, puede ver información detallada sobre el evento generado.

Si detecta problemas de conectividad en la configuración de MetroCluster, debe iniciar sesión en System Manager o acceder a la CLI de ONTAP para resolver los problemas.

Para obtener más información sobre cómo determinar el estado del clúster, consulte "Determinar el estado del clúster en la configuración de MetroCluster over FC".

Supervise los problemas de conectividad en la configuración de MetroCluster over IP

Para los clústeres de una configuración MetroCluster sobre IP, los gráficos de conectividad se muestran en la página **Clusters**. Siga estos pasos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **clústeres**.

   Se muestra una lista de todos los clústeres supervisados.

2. En la vista **Protección: MetroClusters**, haga clic en el nombre del clúster para el que desea ver los detalles de configuración de MetroCluster sobre IP. De forma alternativa, puede filtrar por clústeres en una configuración de MetroCluster.

3. Expanda la fila haciendo clic en el signo de intercalación v . El icono de signo de intercalación aparece solamente para un clúster que esta protección está protegida por configuración de MetroCluster over IP.

   Puede ver la topología de los sitios de origen y réplica, así como el Mediador, si lo hubiera, utilizado para la conexión. Puede ver la siguiente información:

   - Conectividad en todos los sitios
   - Problemas de salud y disponibilidad, si los hay, en ambos sitios
   - Cuestiones relacionadas con el mediador
   - Problemas relacionados con la replicación.

   > Se informa de los siguientes Estados: Crítico (), error (), o normal (). También puede ver el estado de replicación de datos agregados de los datos primarios y de reflejo en la misma topología.

   En el siguiente diagrama, puede ver que la conectividad entre sitios entre los clústeres de origen y destino no está disponible y que el Mediator entre ellos no está configurado.

4. Haga clic en el icono de estado. Se muestra un mensaje con la definición de error. Si se ha producido un evento para el problema en la configuración de MetroCluster over IP, puede hacer clic en el botón **Ver evento** del mensaje y ver los detalles del evento. Cuando haya resuelto el problema y el evento, el icono de estado de esta topología se convierte en normal ().

5. Puede ver más detalles de configuración en las secciones **Descripción general de MetroCluster** y **Protección** de la ficha **Configuración** de la página de detalles **clúster / Salud**.

Sólo para una configuración de MetroCluster sobre IP, puede ver la topología del clúster en la página **Clusters**. Para los clústeres en una configuración MetroCluster over FC, la topología se muestra en la pestaña **conectividad MetroCluster** de la página de detalles **Cluster / Health**.

Información relacionada

- "Página de detalles Cluster / Health"
- Para obtener información acerca de la vista **relación:MetroCluster**, consulte "Supervisar las configuraciones de MetroCluster".
- Para obtener información acerca de **relación: Vista Estado de transferencia de último 1 mes**, consulte "Relación: Vista Estado de transferencia de último 1 mes".
- Para obtener información acerca de **relación: La vista velocidad de transferencia** de último 1 mes, consulte "Relación: Última vista de tarifa de transferencia de 1 mes".
- Para obtener información acerca de la vista **relación: Todas las relaciones**, consulte "Relación: Vista todas las relaciones".

Supervisar la replicación de MetroCluster

Puede supervisar y diagnosticar la condición de estado general de las conexiones lógicas mientras hace mirroring de los datos. Es posible identificar los problemas o cualquier riesgo que interrumpa el mirroring de componentes del clúster, como agregados, nodos y máquinas virtuales de almacenamiento.

Unified Manager utiliza alertas de estado del sistema para supervisar el estado de los componentes y la conectividad en la configuración de MetroCluster.

Lo que necesitará

Tanto el clúster local como el remoto de la configuración de MetroCluster se deben añadir a Unified Manager

Visualización de la replicación para las configuraciones de MetroCluster over IP

En el caso de las configuraciones de MetroCluster over IP, el estado de replicación de datos se muestra en la vista de topología de un clúster protegido por MetroCluster mediante IP desde las siguientes vistas del panel de navegación izquierdo de Unified Manager:

- **Almacenamiento** > **Clusters** > **Protección: Vista MetroCluster**
- **Protección** > **Relaciones** > **relación: MetroCluster** vista

Para obtener más información, consulte "Supervise los problemas de conectividad en MetroCluster por IP".

Visualización de la replicación para configuraciones de MetroCluster over FC

Siga estos pasos para determinar si hay problemas en la replicación de datos para la configuración de MetroCluster over FC.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **clústeres**.

   Se muestra una lista de los clústeres supervisados.

2. En la vista **Estado: Todos los clústeres**, haga clic en el nombre del clúster para el que desea ver los detalles de la replicación de MetroCluster. En la página **Cluster / Health details**, haga clic en la ficha **MetroCluster Replication**.

   La topología de la configuración de MetroCluster que se va a replicar se muestra en el sitio local en el área de objetos del clúster correspondiente con la información sobre el sitio remoto en el que se están reflejando los datos. Si mueve el puntero sobre el icono, puede ver información detallada sobre el evento generado.

Puede utilizar la información que se muestra en la página de detalles Cluster / Health para corregir cualquier problema de replicación. Si detecta problemas de mirroring en la configuración de MetroCluster, debe iniciar sesión en System Manager o acceder a la CLI de ONTAP para resolver los problemas.

Información relacionada

"Página de detalles Cluster / Health"

Gestión de cuotas

Puede utilizar cuotas de usuarios y grupos para limitar la cantidad de espacio en disco o el número de archivos que puede utilizar un usuario o un grupo de usuarios. Es posible ver información de cuotas de usuarios y grupos de usuarios, como el uso de discos y archivos, así como los diversos límites establecidos en los discos.

Qué límites de cuota son

Los límites de cuota de usuario son valores que el servidor de Unified Manager utiliza para evaluar si el consumo de espacio por parte de un usuario está cerca del límite o ha alcanzado el límite establecido por la cuota del usuario. Si se cruza el límite blando o se alcanza el límite rígido, el servidor de Unified Manager genera eventos de cuota de usuario.

De forma predeterminada, el servidor de Unified Manager envía un mensaje de correo electrónico de notificación a los usuarios que han superado el límite de software de cuota o han alcanzado el límite duro de cuota y para los que se han configurado eventos de cuota de usuario. Los usuarios con la función Administrador de aplicaciones pueden configurar alertas que notifican a los destinatarios especificados los eventos de cuota de usuario o de grupo de usuarios.

Puede especificar los límites de cuota mediante ONTAP System Manager o la interfaz de línea de comandos de ONTAP.

Visualización de cuotas de usuarios y grupos de usuarios

La página de detalles Storage VM / Health muestra información sobre las cuotas de grupos de usuarios y usuarios que están configuradas en la SVM. Puede ver el nombre del usuario o grupo de usuarios, los límites establecidos en los discos y archivos, el espacio utilizado en disco y archivo y la dirección de correo electrónico para la notificación.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **Storage VMs**.
2. En la vista **Health: All Storage VMs**, seleccione una máquina virtual de almacenamiento y, a continuación, haga clic en la pestaña **User and Group Quotas**.

Información relacionada

"Adición de usuarios"

Creación de reglas para generar direcciones de correo electrónico

Puede crear reglas para especificar la dirección de correo electrónico según la cuota de usuario asociada con los clústeres, las máquinas virtuales de almacenamiento (SVM), los volúmenes, qtrees, los usuarios o los grupos de usuarios. Se envía una notificación a la dirección de correo electrónico especificada cuando hay una infracción de cuota.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber revisado las directrices de la página Reglas para generar Dirección de correo electrónico de cuota de usuario y grupo.

Debe definir las reglas para las direcciones de correo electrónico de cuota e introducirlas en el orden en el que desea ejecutarlas. Por ejemplo, si desea utilizar la dirección de correo electrónico qtree1@xyz.com para recibir notificaciones acerca de las brechas de cuotas para qtre1 y utilizar la dirección de correo electrónico admin@xyz.com para todos los demás qtrees, las reglas deben aparecer en el siguiente orden:

- Si ($QTREE == 'qtre1') entonces qtree1@xyz.com
- Si ($QTREE == *) entonces admin@xyz.com

Si no se cumple ninguno de los criterios para las reglas especificadas, se utiliza la regla predeterminada:

SI ($USER_OR_GROUP == *) ENTONCES $USER_OR_GROUP@$DOMAIN

Pasos

1. En el panel de navegación de la izquierda, haga clic en **General** > **Reglas de correo electrónico de cuota**.
2. Introduzca la regla en función de sus criterios.
3. Haga clic en **Validar** para validar la sintaxis de la regla.

   Se muestra un mensaje de error si la sintaxis de la regla es incorrecta. Debe corregir la sintaxis y volver a hacer clic en **Validar**.

4. Haga clic en **Guardar**.
5. Compruebe que la dirección de correo electrónico que ha creado se muestra en la pestaña **cuotas de usuario y grupo** de la página de detalles Storage **VM / Health**.

Creación de un formato de notificación por correo electrónico para cuotas de usuarios y grupos de usuarios

Puede crear un formato de notificación para los mensajes de correo electrónico que se envían a un usuario o a un grupo de usuarios cuando hay un problema relacionado con las cuotas (límite de software incumplido o límite rígido alcanzado).

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **General** > **Formato de correo electrónico de cuota**.
2. Introduzca o modifique los detalles en los campos **de**, **asunto** y **Detalles de correo electrónico**.
3. Haga clic en **Vista previa** para obtener una vista previa de la notificación por correo electrónico.
4. Haga clic en **Cerrar** para cerrar la ventana de vista previa.
5. Modifique el contenido de la notificación por correo electrónico, si es necesario.
6. Haga clic en **Guardar**.

Edición de direcciones de correo electrónico de cuotas de usuarios y grupos

Las direcciones de correo electrónico se pueden modificar según la cuota de usuario asociada con los clústeres, las máquinas virtuales de almacenamiento (SVM), los volúmenes, los qtrees, los usuarios o los grupos de usuarios. Puede modificar la dirección de correo electrónico cuando desee reemplazar la dirección de correo electrónico generada por las reglas especificadas en el cuadro de diálogo Reglas para generar Dirección de correo electrónico de usuario y cuota de grupo.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Debe haber revisado el "directrices para la creación de reglas".

Si edita una dirección de correo electrónico, las reglas para generar las direcciones de correo electrónico de usuario y cuota de grupo ya no serán aplicables a la cuota. Para que las notificaciones se envíen a la dirección de correo electrónico generada por las reglas especificadas, deberá eliminar la dirección de correo electrónico y guardar el cambio.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **SVM**.
2. En la vista **Health: All Storage VMs**, seleccione una SVM y, a continuación, haga clic en la pestaña **User and Group Quotas**.
3. Haga clic en **Editar dirección de correo electrónico** debajo de la fila de fichas.
4. En el cuadro de diálogo **Editar dirección de correo electrónico**, realice la acción adecuada:

Si…	Realice lo siguiente…
Desea enviar las notificaciones a la dirección de correo electrónico que generan las reglas especificadas	a. Elimine la dirección de correo electrónico en el campo **Dirección de correo electrónico**. b. Haga clic en **Guardar**. c. Actualice el explorador presionando F5 para volver a cargar el cuadro de diálogo Editar dirección de correo electrónico. La dirección de correo electrónico generada por la regla especificada se muestra en el campo **Dirección de correo electrónico**.
Desea enviar las notificaciones a una dirección de correo electrónico especificada	a. Modifique la dirección de correo electrónico en el campo **Dirección de correo electrónico**. b. Haga clic en **Guardar**. Las reglas para generar las direcciones de correo electrónico de usuario y cuota de grupo ya no se aplican a la cuota.

Más información acerca de las cuotas

Comprender los conceptos de cuotas le ayuda a gestionar de forma eficiente las cuotas de usuario y las cuotas de grupos de usuarios.

Descripción general del proceso de cuotas

Las cuotas pueden ser suaves o duras. Las cuotas blandas hacen que ONTAP envíe una notificación cuando se superen los límites especificados y las cuotas rígidas evitan que una operación de escritura tenga éxito cuando se superen los límites especificados.

Cuando ONTAP recibe una solicitud de un usuario o grupo de usuarios para escribir en un volumen de FlexVol, comprueba si se activan las cuotas en ese volumen para el usuario o el grupo de usuarios y determina lo siguiente:

- Si se alcanzará el límite rígido

  En caso afirmativo, la operación de escritura falla cuando se alcanza el límite rígido y se envía la notificación de cuota dura.

- Si se incumplido el límite blando

  Si la respuesta es sí, la operación de escritura se realiza correctamente cuando se cumple el límite de software y se envía la notificación de cuota de software.

- Si una operación de escritura no superará el límite de software

  Si la respuesta es sí, la operación de escritura es correcta y no se envía ninguna notificación.

Acerca de las cuotas

Las cuotas proporcionan una forma de restringir o realizar un seguimiento del espacio en disco y del número de archivos que usan los usuarios, grupos o qtrees. Las cuotas se especifican con el `/etc/quotas` archivo. Las cuotas se aplican a un volumen o qtree concreto.

Por qué se usan cuotas

Puede utilizar las cuotas para limitar el uso de recursos en volúmenes de FlexVol, para proporcionar una notificación cuando el uso de los recursos alcanza niveles específicos o para realizar un seguimiento del uso de los recursos.

Se especifica una cuota por los siguientes motivos:

- Para limitar la cantidad de espacio en disco o el número de archivos que puede utilizar un usuario o grupo, o que puede contener un qtree
- Para realizar el seguimiento de la cantidad de espacio en disco o del número de archivos que usan los usuarios, un grupo o un qtree, sin fijar un límite
- Para advertir a los usuarios cuando su uso de disco o uso de archivo es alto

Descripción de los cuadros de diálogo cuotas

Puede utilizar la opción adecuada en la pestaña cuotas de usuario y de grupo de la vista Estado: Todas las máquinas virtuales de almacenamiento para configurar el formato de la notificación de correo electrónico que se envía cuando se produce un problema relacionado con la cuota y para configurar reglas para especificar direcciones de correo electrónico basadas en la cuota de usuario.

Formato de notificación por correo electrónico

La página Formato de notificación por correo electrónico muestra las reglas del correo electrónico que se envía a un usuario o a un grupo de usuarios cuando hay un problema relacionado con la cuota (límite de software incumplido o límite rígido alcanzado).

La notificación por correo electrónico se envía sólo cuando se generan los siguientes eventos de cuota de usuario o de grupo de usuarios: Límite de software de espacio de disco de cuota de usuario o de grupo incumplido, límite de software de recuento de archivos de cuota de usuario o de grupo superado, se ha alcanzado el límite duro de recuento de archivos de cuota de usuario o de grupo o se ha alcanzado el límite duro de recuento de archivos de cuota de usuario o de grupo.

- **Desde**

  Muestra la dirección de correo electrónico desde la que se envía el correo electrónico, que se puede modificar. De forma predeterminada, ésta es la dirección de correo electrónico que se especifica en la página Notificaciones.

- **Asunto**

  Muestra el asunto del correo electrónico de notificación.

- **Detalles del correo electrónico**

  Muestra el texto del correo electrónico de notificación. Puede modificar el texto según sus requisitos. Por ejemplo, puede proporcionar información relacionada con los atributos de cuota y reducir el número de palabras clave. Sin embargo, no debe modificar las palabras clave.

  Las palabras clave válidas son las siguientes:

  - $EVENT_NAME

    Especifica el nombre del evento que provocó la notificación por correo electrónico.

  - $QUOTA_TARGET

    Especifica el qtree o el volumen en el que se puede aplicar la cuota.

  - $QUOTA_USED_PERCENT

    Especifica el porcentaje de límite de disco duro, límite de software de disco, límite duro de archivos o límite de software de archivos que utiliza el usuario o grupo de usuarios.

  - $QUOTA_LIMIT

    Especifica el límite de disco duro o el límite de disco duro de archivos que el usuario o el grupo de usuarios alcanzan y se genera uno de los siguientes eventos:

    - Se ha alcanzado el límite duro de espacio en disco de cuota de usuario o de grupo
    - Se ha alcanzado el límite de espacio de disco de cuota de usuario o de grupo
    - Se ha alcanzado el límite duro de recuento de archivos de cuota de usuario o de grupo
    - Se ha alcanzado el límite suave de recuento de archivos de cuota de usuario o de grupo

  - $QUOTA_USED

    Especifica el espacio en disco utilizado o el número de archivos creados por el usuario o el grupo de usuarios.

  - $QUOTA_USER

    Especifica el nombre del usuario o del grupo de usuarios.

Botones de comando

Los botones de comando permiten obtener una vista previa, guardar o cancelar los cambios realizados en el formato de notificación por correo electrónico:

- **Vista previa**

  Muestra una vista previa del correo electrónico de notificación.

- **Restaurar valores predeterminados de fábrica**

  Permite restaurar el formato de notificación a los valores predeterminados de fábrica.

- **Guardar**

Guarda los cambios realizados en el formato de notificación.

Reglas para generar la página Dirección de correo electrónico de cuota de usuario y grupo

La página Reglas para generar Dirección de correo electrónico de cuota de usuario y de grupo permite crear reglas para especificar direcciones de correo electrónico en función de la cuota de usuario asociada a clústeres, SVM, volúmenes, qtrees, usuarios, o grupos de usuarios. Cuando se incumple una cuota, se envía una notificación a la dirección de correo electrónico especificada.

Área Rules

Debe definir las reglas para una dirección de correo electrónico de cuota. También puede agregar comentarios para explicar las reglas.

Cómo se definen las reglas

Debe introducir las reglas en el orden en el que desea ejecutarlas. Si se cumple el criterio de la primera regla, se generará la dirección de correo electrónico según esta regla. Si no se cumple el criterio, se considerará el criterio para la siguiente regla, etc. Cada línea enumera una regla independiente. La regla predeterminada es la última regla de la lista. Es posible cambiar el orden de prioridad de las reglas. Sin embargo, no puede cambiar el orden de la regla predeterminada.

Por ejemplo, si desea utilizar la dirección de correo electrónico qtree1@xyz.com para recibir notificaciones acerca de las brechas de cuotas para qtre1 y utilizar la dirección de correo electrónico admin@xyz.com para todos los demás qtrees, las reglas deben aparecer en el siguiente orden:

- Si ($QTREE == 'qtre1') entonces qtree1@xyz.com
- Si ($QTREE == *) entonces admin@xyz.com

Si no se cumple ninguno de los criterios para las reglas especificadas, se utiliza la regla predeterminada:

SI ($USER_OR_GROUP == *) ENTONCES $USER_OR_GROUP@$DOMAIN

Si más de un usuario tiene la misma cuota, los nombres de los usuarios se muestran como valores separados por comas y las reglas no se aplican para la cuota.

Cómo se añaden comentarios

Puede agregar comentarios para explicar las reglas. Debe usar # al principio de cada comentario y cada línea enumera un comentario separado.

Sintaxis de reglas

La sintaxis de la regla debe ser una de las siguientes:

- si (`valid variableoperator *`) entonces `email ID@domain name`

  si es una palabra clave y está en minúscula. El operador es ==. El ID de correo electrónico puede contener cualquier carácter, las variables válidas $USER_OR_GROUP, $USER o $GROUP, o una combinación de cualquier carácter y las variables válidas $USER_OR_GROUP, $USER o $GROUP. El nombre de dominio puede contener cualquier carácter, la variable válida $DOMAIN o una combinación de cualquier carácter y la variable válida $DOMAIN. Las variables válidas pueden estar en mayúsculas o

minúsculas, pero no deben ser una combinación de ambas. Por ejemplo, $domain y $DOMAIN son válidos, pero $Domain no es una variable válida.

- si (`valid variableoperator `string``) entonces `email ID@domain name`

  si es una palabra clave y es minúscula. El operador puede contener o ==. El ID de correo electrónico puede contener cualquier carácter, las variables válidas $USER_OR_GROUP, $USER o $GROUP, o una combinación de cualquier carácter y las variables válidas $USER_OR_GROUP, $USER o $GROUP. El nombre de dominio puede contener cualquier carácter, la variable válida $DOMAIN o una combinación de cualquier carácter y la variable válida $DOMAIN. Las variables válidas pueden estar en mayúsculas o minúsculas, pero no deben ser una combinación de ambas. Por ejemplo, $domain y $DOMAIN son válidos, pero $Domain no es una variable válida.

Botones de comando

Los botones de comando permiten guardar, validar o cancelar las reglas creadas:

- **Validar**

  Valida la sintaxis de la regla creada. Si hay errores durante la validación, la regla que genera el error se muestra junto con un mensaje de error.

- **Restaurar valores predeterminados de fábrica**

  Permite restaurar las reglas de dirección a los valores predeterminados de fábrica.

- **Guardar**

  Valida la sintaxis de la regla y guarda la regla si no hay errores. Si hay errores durante la validación, la regla que genera el error se muestra junto con un mensaje de error.

Resolución de problemas

La información para la solución de problemas le ayuda a identificar y resolver problemas con los que se encuentra cuando se utiliza Unified Manager.

Agregar espacio en disco al directorio de la base de datos de Unified Manager

El directorio de bases de datos de Unified Manager contiene todos los datos de estado y rendimiento que se recopilan en los sistemas ONTAP. Algunas circunstancias pueden requerir que aumente el tamaño del directorio de la base de datos.

Por ejemplo, el directorio de base de datos se puede llenarse si Unified Manager está recopilando datos de un gran número de clústeres en los que cada clúster tiene muchos nodos. Recibirá un evento de advertencia cuando el directorio de la base de datos esté lleno al 90% y un evento crítico cuando el directorio esté lleno al 95%.

> No se recopilan datos adicionales de los clústeres después de que el directorio se encuentra lleno al 95 %.

Los pasos necesarios para añadir capacidad al directorio de datos son distintos en función de si Unified Manager se ejecuta en un servidor VMware ESXi, en un servidor Red Hat o CentOS Linux o en un servidor

Microsoft Windows.

Adición de espacio al disco de datos de la máquina virtual de VMware

Si necesita aumentar la cantidad de espacio en el disco de datos de la base de datos de Unified Manager, puede añadir capacidad después de la instalación aumentando el espacio en disco mediante la consola de mantenimiento de Unified Manager.

Lo que necesitará

- Debe tener acceso a vSphere Client.
- La máquina virtual no debe tener instantáneas almacenadas localmente.
- Debe tener las credenciales de usuario de mantenimiento.

Le recomendamos que haga una copia de seguridad de su máquina virtual antes de aumentar el tamaño de los discos virtuales.

Pasos

1. En el cliente de vSphere, seleccione la máquina virtual de Unified Manager y, a continuación, añada más capacidad de disco a los datos `disk 3`. Consulte la documentación de VMware para obtener más detalles.

   En algunos casos excepcionales, la instalación de Unified Manager utiliza "disco duro 2" para el disco de datos en lugar de "disco duro 3". Si esto se ha producido en la implementación, aumente el espacio del disco que sea mayor. El disco de datos siempre tendrá más espacio que el otro disco.

2. En el cliente vSphere, seleccione la máquina virtual de Unified Manager y, a continuación, seleccione la pestaña **Console**.
3. Haga clic en en la ventana de la consola y, a continuación, inicie sesión en la consola de mantenimiento con su nombre de usuario y contraseña.
4. En **Menú principal**, introduzca el número de la opción **Configuración del sistema**.
5. En **Menú de configuración del sistema**, introduzca el número de la opción **aumentar tamaño del disco de datos**.

Adición de espacio al directorio de datos del host Linux

Si ha asignado poco espacio en disco a `/opt/netapp/data` directorio para admitir Unified Manager cuando originalmente configuró el host Linux y después instaló Unified Manager, es posible añadir espacio en disco después de la instalación aumentando espacio en disco en la `/opt/netapp/data` directorio.

Lo que necesitará

Debe tener acceso de usuario raíz a la máquina Red Hat Enterprise Linux o CentOS Linux en la que está instalado Unified Manager.

Le recomendamos que realice un backup de la base de datos de Unified Manager antes de aumentar el tamaño del directorio de datos.

Pasos

1. Inicie sesión como usuario root en el equipo Linux en el que desea agregar espacio en disco.
2. Detenga el servicio Unified Manager y el software MySQL asociado en el orden que se muestra: `systemctl stop ocieau ocie mysqld`
3. Crear una carpeta de copia de seguridad temporal (por ejemplo, `/backup-data`) con suficiente espacio en disco para contener los datos de la corriente `/opt/netapp/data` directorio.
4. Copie la configuración de contenido y privilegios de la existente `/opt/netapp/data` directorio en el directorio de datos de copia de seguridad:

   ```
   cp -arp /opt/netapp/data/* /backup-data
   ```

5. Si se Linux está habilitado:

   a. Obtenga el tipo de Linux de se para las carpetas existentes `/opt/netapp/data` carpeta:

      ```
      se_type=`ls -Z /opt/netapp/data| awk '{print $4}'| awk -F: '{print $3}'|
      head -1
      ```

      El sistema devuelve una confirmación similar a la siguiente:

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. Ejecute el `chcon` Comando para establecer el tipo de Linux de se para el directorio de copia de seguridad:

      ```
      chcon -R --type=mysqld_db_t /backup-data
      ```

6. Elimine el contenido del `/opt/netapp/data` directorio:

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

7. Expanda el tamaño de `/opt/netapp/data` directorio a un mínimo de 150 GB a través de comandos de LVM o mediante la adición de discos adicionales.

   > Si ha creado `/opt/netapp/data` desde un disco, no debe intentar montarlo `/opt/netapp/data` Como una unidad NFS o CIFS. Porque, en este caso, si intenta expandir el espacio en disco, algunos comandos de LVM como `resize` y.. `extend` es posible que no funcione como se espera.

8. Confirme que el `/opt/netapp/data` el propietario del directorio (mysql) y el grupo (root) no cambian:

   ```
   ls -ltr /opt/netapp/ | grep data
   ```

   El sistema devuelve una confirmación similar a la siguiente:

   ```
   drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
   ```

9. Si se activa Linux, confirme que el contexto del `/opt/netapp/data` el directorio todavía está establecido en mysqld_db_t:

   a. `touch /opt/netapp/data/abc`

   b. `ls -Z /opt/netapp/data/abc`

      El sistema devuelve una confirmación similar a la siguiente:

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. Elimine el archivo `abc` de forma que este archivo no causa un error de base de datos en el futuro.
11. Copie el contenido de `backup-data` volver al expandido `/opt/netapp/data` directorio:

    `cp -arp /backup-data/* /opt/netapp/data/`

12. Si se Linux está habilitado, ejecute el siguiente comando:

    `chcon -R --type=mysqld_db_t /opt/netapp/data`

13. Inicie el servicio MySQL:

    `systemctl start mysqld`

14. Una vez iniciado el servicio MySQL, inicie los servicios ocie y ocieau en el orden que se muestra:

    `systemctl start ocie ocieau`

15. Después de iniciar todos los servicios, elimine la carpeta de copia de seguridad `/backup-data`:

    `rm -rf /backup-data`

Agregar espacio a la unidad lógica del servidor Microsoft Windows

Si necesita aumentar la cantidad de espacio en disco para la base de datos de Unified Manager, puede añadir capacidad a la unidad lógica en la que está instalado Unified Manager.

Lo que necesitará

Debe tener privilegios de administrador de Windows.

Le recomendamos que realice un backup de la base de datos de Unified Manager antes de agregar espacio en disco.

Pasos

1. Inicie sesión como administrador en el servidor Windows en el que desea agregar espacio en disco.
2. Siga el paso correspondiente al método que desea utilizar para agregar más espacio:

Opción	Descripción
En un servidor físico, añada capacidad a la unidad lógica en la que se ha instalado el servidor de Unified Manager.	Siga los pasos del tema de Microsoft: "Extender un volumen básico"
En un servidor físico, agregue una unidad de disco duro.	Siga los pasos del tema de Microsoft: "Agregar unidades de disco duro"
En un equipo virtual, aumente el tamaño de una partición de disco.	Siga los pasos del tema de VMware: "Aumentar el tamaño de una partición de disco"

Cambiar el intervalo de recogida de estadísticas de rendimiento

El intervalo de recogida predeterminado para las estadísticas de rendimiento es de 5 minutos. Puede cambiar este intervalo a 10 o 15 minutos si descubre que las colecciones de clústeres grandes no están finalizando dentro del tiempo predeterminado. Esta configuración afecta la recogida de estadísticas de todos los clústeres que está supervisando esta instancia de Unified Manager.

Lo que necesitará

Debe tener un ID de usuario y una contraseña autorizados para iniciar sesión en la consola de mantenimiento del servidor de Unified Manager.

La emisión de colecciones de estadísticas de rendimiento no terminado a tiempo se indica mediante los mensajes de mensaje de cabecera `Unable to consistently collect from cluster <cluster_name> or Data collection is taking too long on cluster <cluster_name>.`

Debe cambiar el intervalo de recopilación sólo cuando sea necesario debido a un problema de recopilación de estadísticas. No cambie esta configuración por ningún otro motivo.

> Si se cambia este valor desde el ajuste predeterminado de 5 minutos, puede afectar el número y la frecuencia de los eventos de rendimiento que informa Unified Manager. Por ejemplo, los umbrales de rendimiento definidos por el sistema activan eventos cuando se supera la política durante 30 minutos. Cuando se utilizan colecciones de 5 minutos, se debe superar la política para seis colecciones consecutivas. Para las colecciones de 15 minutos, la directiva debe superarse sólo durante dos períodos de recopilación.

Un mensaje en la parte inferior de la página Cluster Setup indica el intervalo de recogida de datos estadísticos actual.

Pasos

1. Inicie sesión con SSH como usuario de mantenimiento en el host de Unified Manager.

   Se muestran los mensajes de la consola de mantenimiento de Unified Manager.

2. Escriba el número de la opción de menú con la etiqueta **Configuración del intervalo de sondeo de**

rendimiento y, a continuación, pulse Intro.

3. Si se le solicita, vuelva a introducir la contraseña de usuario de mantenimiento.
4. Escriba el número del nuevo intervalo de sondeo que desea establecer y, a continuación, pulse Intro.

Si cambió el intervalo de recogida de Unified Manager a 10 o 15 minutos y tiene una conexión actual con un proveedor de datos externo (como Graphite), debe cambiar el intervalo de transmisión del proveedor de datos de modo que sea igual o mayor que el intervalo de recogida de Unified Manager.

Cambiar el periodo de tiempo, Unified Manager conserva los datos de eventos y rendimiento

De forma predeterminada, Unified Manager almacena datos de eventos y datos de rendimiento durante 6 meses en todos los clústeres supervisados. Una vez transcurrido este tiempo, los datos más antiguos se eliminan automáticamente para dar lugar a los nuevos datos. Este período de tiempo predeterminado funciona bien en la mayoría de las configuraciones, pero es posible que las configuraciones de gran tamaño con muchos clústeres y nodos deban reducir el período de retención para que Unified Manager funcione de forma óptima.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Puede cambiar los períodos de retención de estos dos tipos de datos en la página Data Retention. Esta configuración afecta la retención de datos de todos los clústeres que está supervisando esta instancia de Unified Manager.

> Unified Manager recopila estadísticas de rendimiento cada 5 minutos. Cada día, las estadísticas de 5 minutos se resumen en las estadísticas de rendimiento por hora. Conserva 30 días de datos históricos de rendimiento de 5 minutos y 6 meses de datos de rendimiento resumidos por hora (de forma predeterminada).

Debe reducir el período de retención solo si se está quedando sin espacio o si el backup y otras operaciones tardan mucho tiempo en completarse. La reducción del período de retención tiene los siguientes efectos:

- Los datos de rendimiento antiguos se eliminan de la base de datos de Unified Manager después de las medianoche.
- Los datos de eventos antiguos se eliminan de inmediato de la base de datos de Unified Manager.
- Los eventos anteriores al período de retención ya no estarán disponibles para visualizarlos en la interfaz de usuario.
- Las ubicaciones en la interfaz de usuario de donde se muestren las estadísticas de rendimiento por hora estarán en blanco antes del período de retención.
- Si el período de retención de eventos supera el período de retención de datos de rendimiento, se mostrará un mensaje en la barra deslizante de rendimiento con la advertencia de que los eventos de rendimiento anteriores pueden no tener datos de respaldo en sus gráficos asociados.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Directivas** > **retención de datos**.
2. En la página **retención de datos**, seleccione la herramienta de control deslizante en el área retención de

eventos o retención de datos de rendimiento y muévala al número de meses que deben conservarse los datos y haga clic en **Guardar**.

Error de autenticación desconocido

Al realizar una operación relacionada con la autenticación, como agregar, editar, eliminar o probar usuarios o grupos remotos, puede aparecer el siguiente mensaje de error: `Unknown authentication error.`

Causa

Este problema puede ocurrir si ha establecido un valor incorrecto para las siguientes opciones:

- Nombre del administrador del servicio de autenticación de Active Directory
- Enlazar nombre completo del servicio de autenticación de OpenLDAP

Acción Correctiva

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. En función del servicio de autenticación que haya seleccionado, introduzca la información adecuada para el nombre de administrador o el nombre distintivo de enlace.
3. Haga clic en **probar autenticación** para probar la autenticación con los detalles especificados.
4. Haga clic en **Guardar**.

Usuario no encontrado

Cuando se realiza una operación relacionada con la autenticación, como agregar, editar, eliminar o probar usuarios o grupos remotos, se muestra el siguiente mensaje de error: `User not found.`

Causa

Este problema puede ocurrir si el usuario existe en el servidor AD o en el servidor LDAP y si ha establecido el nombre distintivo base en un valor incorrecto.

Acción Correctiva

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. Introduzca la información adecuada para el nombre distintivo de la base.
3. Haga clic en **Guardar**.

Problema al agregar LDAP mediante otros servicios de autenticación

Cuando selecciona otros como servicio de autenticación, el usuario y la clase de objeto de grupo retienen los valores de la plantilla seleccionada anteriormente. Si el servidor LDAP no utiliza los mismos valores, es posible que se produzca un error en la operación.

Causa

Los usuarios no están configurados correctamente en OpenLDAP.

Acción Correctiva

Puede resolver este problema manualmente utilizando una de las siguientes soluciones.

Si la clase de objeto de usuario LDAP y la clase de objeto de grupo son usuario y grupo, respectivamente, realice los siguientes pasos:

1. En el panel de navegación izquierdo, haga clic en**General** > **autenticación remota**.
2. En el menú desplegable **Servicio de autenticación**, seleccione **Active Directory** y, a continuación, seleccione **otros**.
3. Complete los campos de texto.

Si su clase de objeto de usuario LDAP y su clase de objeto de grupo son posixAccount y posixGroup, respectivamente, realice los siguientes pasos:

1. En el panel de navegación izquierdo, haga clic en **General** > **autenticación remota**.
2. En el menú desplegable **Servicio de autenticación**, seleccione **OpenLDAP** y, a continuación, seleccione **otros**.
3. Complete los campos de texto.

Si las dos primeras soluciones no se aplican, llame al `option-set` API y establezca la `auth.ldap.userObjectClass` y.. `auth.ldap.groupObjectClass` opciones a los valores correctos.

Gestionar eventos y alertas

Gestión de eventos

Los eventos le ayudan a identificar problemas en los clústeres que se supervisan.

¿Qué son los eventos de la plataforma Active IQ

Unified Manager puede mostrar eventos detectados por la plataforma Active IQ. Estos eventos se crean ejecutando un conjunto de reglas contra los mensajes de AutoSupport generados desde todos los sistemas de almacenamiento que supervisa Unified Manager.

Para obtener más información, consulte "Cómo se generan los eventos de la plataforma Active IQ".

Unified Manager comprueba si hay un nuevo archivo de reglas automáticamente y solo descarga un archivo nuevo cuando haya reglas más recientes. En los sitios sin acceso a la red externa, deberá cargar las reglas manualmente desde **Storage Management** > **Event Setup** > **Upload Rules**.

Estos eventos de Active IQ no se superponen con los eventos existentes de Unified Manager e identifican incidentes o riesgos relacionados con la configuración, el cableado, las mejores prácticas y los problemas de disponibilidad del sistema.

Para obtener más información acerca de cómo habilitar eventos de plataforma, consulte "Habilitar los eventos del portal de Active IQ". Para obtener más información sobre cómo cargar el archivo de reglas, consulte "Carga de un nuevo archivo de reglas de Active IQ".

Active IQ de NetApp es un servicio basado en cloud que proporciona análisis predictivos y soporte proactivo para optimizar las operaciones de los sistemas de almacenamiento en el cloud híbrido de NetApp. Consulte "Active IQ de NetApp" si quiere más información.

Qué son los eventos del sistema de gestión de eventos

El sistema de gestión de eventos (EMS) recopila datos de eventos de diferentes partes del kernel de ONTAP y proporciona mecanismos de reenvío de eventos. Estos eventos de ONTAP pueden notificarse como eventos de EMS en Unified Manager. La supervisión y la gestión centralizadas facilita la configuración de eventos de EMS cruciales y notificaciones de alertas basadas en estos eventos de EMS.

La dirección de Unified Manager se añade como destino de notificación al clúster cuando se añade el clúster a Unified Manager. Un evento de EMS se informa en cuanto ocurre el evento en el clúster.

Existen dos métodos para recibir eventos de EMS en Unified Manager:

- Un cierto número de eventos de EMS importantes se informan automáticamente.
- Puede suscribirse para recibir eventos de EMS individuales.

Los eventos de EMS generados por Unified Manager se informan de forma diferente, según el método en el que se generó el evento:

Funcionalidad	Mensajes EMS automáticos	Mensajes EMS suscritos
Eventos de EMS disponibles	Subconjunto de eventos de EMS	Todos los eventos de EMS
Nombre del mensaje EMS cuando se activa	Nombre de evento de Unified Manager (convertido a partir del nombre de evento de EMS)	No específico en el formato "error EMS recibido". El mensaje detallado proporciona el formato de notación de puntos del evento EMS real
Mensajes recibidos	Tan pronto como se haya detectado el clúster	Después de añadir cada evento de EMS requerido a Unified Manager y después del próximo ciclo de sondeo de 15 minutos
Ciclo de vida de evento	Igual que otros eventos de Unified Manager: estados nuevos, reconocidos, resueltos y obsoletos	El evento de EMS se hace obsoleto una vez que se actualiza el clúster, después de 15 minutos, desde el momento en que se creó el evento
Captura eventos durante el tiempo de inactividad de Unified Manager	Sí, cuando el sistema se inicia, se comunica con cada clúster para adquirir los eventos que faltan	No
Detalles del evento	Las acciones correctivas sugeridas se importan directamente de ONTAP para proporcionar resoluciones coherentes	Acciones correctivas no disponibles en la página Event Details

Algunos de los nuevos eventos de EMS automáticos son eventos informativos que indican que se resolvió un evento anterior. Por ejemplo, el evento informativo "todos los componentes de FlexGroup Estado del espacio correcto" indica que el evento de error "los componentes de FlexGroup tienen problemas de espacio" se ha resuelto. Los eventos informativos no se pueden gestionar utilizando el mismo ciclo de vida de evento que otros tipos de gravedad de evento; sin embargo, el evento se vuelve obsoleto automáticamente si el mismo volumen recibe otro evento de error "problemas de velocidad".

Eventos de EMS que se añaden automáticamente a Unified Manager

Los siguientes eventos de EMS de ONTAP se añaden automáticamente a Unified Manager. Estos eventos se generarán cuando se active en cualquier clúster que Unified Manager supervise.

Los siguientes eventos de EMS están disponibles cuando se supervisan clústeres que ejecutan ONTAP 9.5 o una versión posterior del software:

Nombre del evento de Unified Manager	Nombre del evento de EMS	Recurso afectado	Gravedad de Unified Manager
Acceso al nivel de cloud denegado para la reubicación de agregados	arl.netra.ca.check.failed	Agregado	Error
Acceso al nivel de cloud denegado para la reubicación de agregados durante la conmutación al nodo de respaldo del almacenamiento	gb.netra.ca.check.failed	Agregado	Error
Se completó la resincronización de replicación de mirroring de FabricPool	wafl.ca.resync.complete	Clúster	Error
Espacio de FabricPool casi completo	fabricpool.casi.lleno	Clúster	Error
Se inició el periodo de gracia de NVMe-of	nvmf.graceperiod.start	Clúster	Advertencia
NVMe-of Grace Period activo	nvmf.graceperiod.active	Clúster	Advertencia
NVMe-of Grace caducó	nvmf.graceperiod.expired	Clúster	Advertencia
LUN destruida	lun.destroy	LUN	Información
MetaDataConnFail de Cloud AWS	Cloud.aws.metadataConnFail	Nodo	Error
Cloud AWS IAMCredsExpired	Cloud.aws.iamCredsExpired	Nodo	Error
IAMCredsInvalid de Cloud AWS	Cloud.aws.iamCredsInvalid	Nodo	Error
Cloud AWS IAMCredsNotFound	Cloud.aws.iamCredsNotFound	Nodo	Error
IAMCredsNotInitialized Cloud de AWS	Cloud.aws.iamNotInitialized	Nodo	Información

Nombre del evento de Unified Manager	Nombre del evento de EMS	Recurso afectado	Gravedad de Unified Manager
Cloud AWS IAMRoleinválido	Cloud.aws.iamRoleInvalid	Nodo	Error
Cloud AWS IAMRoleNotFound	Cloud.aws.iamRoleNotFound	Nodo	Error
Organización de hosts de nivel cloud sin resolver	objstore.host.no se puede resolver	Nodo	Error
LIF de interconexión de clústeres por niveles en el cloud inactivo	objstore.interclusterlifDown	Nodo	Error
La solicitud no coincide con la firma del nivel de cloud	osc.signaturediscordancia	Nodo	Error
Una de las agrupaciones de NFSv4 agotadas	Nblade.nfsV4PoolEscape	Nodo	Crítico
La memoria del monitor QoS se enceró	qos.monitor.memory.mutile	Nodo	Error
Memoria de monitor QoS abated	qos.monitor.memory.abated	Nodo	Información
Destrucción NVMeNS	NVMeNS.destroy	Espacio de nombres	Información
NVMeNS en línea	NVMeNS.offline	Espacio de nombres	Información
NVMeNS sin conexión	NVMeNS.online	Espacio de nombres	Información
NVMeNS fuera espacio	NVMeNS.out.of.space	Espacio de nombres	Advertencia
Replicación síncrona fuera de sincronización	sms.status.out.of.sync	Relación de SnapMirror	Advertencia
Replicación síncrona restaurada	sms.status.in.sync	Relación de SnapMirror	Información
Error en la resincronización automática de replicación síncrona	sms.resync.intento.error	Relación de SnapMirror	Error

Nombre del evento de Unified Manager	Nombre del evento de EMS	Recurso afectado	Gravedad de Unified Manager
Muchas conexiones CIFS	Nblade.cifsManyAutos	SVM	Error
Se superó la conexión CIFS máxima	Nblade.cifsMaxOpenSameFile	SVM	Error
Se ha excedido el número máximo de conexiones CIFS por usuario	Nblade.cifsMaxSessPerUsrConn	SVM	Error
Conflicto con los nombres NetBIOS de CIFS	Nblade.cifsNbNameConflict	SVM	Error
Intentos de conexión de recursos compartidos CIFS no existentes	Nblade.cifsNoPrivShare	SVM	Crítico
Error en la operación de copia de volúmenes redundantes de CIFS	cifs.shadowcopy.error	SVM	Error
Virus detectado por el servidor AV	Nblade.vscanVirusDetected	SVM	Error
No hay conexión con el servidor AV para el análisis de virus	Nblade.vscanNoScannerConn	SVM	Crítico
No hay ningún servidor AV registrado	Nblade.vscanNoRegdScanner	SVM	Error
Conexión del servidor AV sin respuesta	Nblade.vscanConnInactive	SVM	Información
El servidor AV está muy ocupado para aceptar una nueva solicitud de análisis	Nblade.vscanConnBackPressure	SVM	Error
Un usuario no autorizado intenta utilizar el servidor AV	Nblade.vscanBadUserPrivAccess	SVM	Error
Los componentes de FlexGroup tienen problemas de espacio	flexgroup.constituyentes.have.space.problemas	Volumen	Error

Nombre del evento de Unified Manager	Nombre del evento de EMS	Recurso afectado	Gravedad de Unified Manager
El estado del espacio de los componentes de FlexGroup es correcto	flexgroup.constituyentes.space.status.all.ok	Volumen	Información
Los componentes de FlexGroup tienen problemas de inodos	flexgroup.constituents.have.inodes.issues	Volumen	Error
Los componentes de FlexGroup inodos Estado todo OK	flexgroup.constituents.inodes.status.all.ok	Volumen	Información
Espacio lógico del volumen casi lleno	monitor.vol.nearFull.inc.sav	Volumen	Advertencia
Espacio lógico del volumen lleno	monitor.vol.full.inc.sav	Volumen	Error
Espacio lógico del volumen normal	monitor.vol.one.ok.inc.sav	Volumen	Información
Error al ajustar el tamaño automático del volumen de WAFL	wafl.vol.autoSize.fail	Volumen	Error
Se ha completado el tamaño automático de volúmenes de WAFL	wafl.vol.autoSize.done	Volumen	Información
Tiempo de espera de operación de archivo DE READDIR de WAFL	wafl.readdir.expiraba	Volumen	Error

Suscripción a eventos de EMS de ONTAP

Puede suscribirse para recibir eventos del sistema de gestión de eventos (EMS) generados por sistemas instalados con el software ONTAP. Un subconjunto de eventos de EMS se informa automáticamente a Unified Manager, pero solo se informan eventos de EMS adicionales si se ha suscrito a estos eventos.

Lo que necesitará

No suscribirse a eventos de EMS que ya se hayan añadido a Unified Manager automáticamente, ya que esto puede provocar confusión al recibir dos eventos por el mismo problema.

Puede suscribirse a cualquier número de eventos de EMS. Todos los eventos a los que se suscribe están

validados y solo se aplican los eventos validados a los clústeres que supervisa en Unified Manager. El *ONTAP 9 Catálogo de eventos EMS* proporciona información detallada para todos los mensajes EMS de la versión especificada del software ONTAP 9. Busque la versión adecuada del *Catálogo de eventos EMS* en la página Documentación del producto de ONTAP 9 para obtener una lista de los eventos aplicables.

"Biblioteca de productos de ONTAP 9"

Es posible configurar alertas para los eventos de EMS de ONTAP a los que se suscribe, y puede crear scripts personalizados para su ejecución.

> Si no recibe los eventos de EMS de ONTAP a los que se ha suscrito, puede haber un problema con la configuración de DNS del clúster, lo que impide que el clúster llegue al servidor de Unified Manager. Para resolver este problema, el administrador de clúster debe corregir la configuración de DNS del clúster y, a continuación, reiniciar Unified Manager. Si lo hace, se vacíe los eventos de EMS pendientes en Unified Manager Server.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de eventos**.
2. En la página Event Setup (Configuración de eventos), haga clic en el botón **Subscribe to EMS events** (Suscribirse a eventos EMS).
3. En el cuadro de diálogo Subscribe to EMS Events, introduzca el nombre del evento de EMS de ONTAP al que desea suscribirse.

   Para ver los nombres de los eventos de EMS a los que se puede suscribir, desde el shell del clúster de ONTAP, puede usar la `event route show` (Anterior a ONTAP 9) o el `event catalog show` (ONTAP 9 o posterior).

   "Cómo configurar y recibir alertas de la suscripción a eventos EMS de ONTAP en Active IQ Unified Manager"

4. Haga clic en **Agregar**.

   El evento EMS se agrega a la lista de eventos EMS suscritos, pero la columna aplicable al clúster muestra el estado como "'Desconocido'" para el evento EMS que ha agregado.

5. Haga clic en **Guardar y cerrar** para registrar la suscripción al evento EMS con el clúster.
6. Haga clic en **Subscribe to EMS events** de nuevo.

   El estado «'Yes'» aparece en la columna aplicable al clúster del evento EMS que ha añadido.

   Si el estado no es "'Yes'", compruebe la ortografía del nombre del evento de EMS de ONTAP. Si el nombre se introduce de forma incorrecta, deberá eliminar el evento incorrecto y, a continuación, volver a añadir el evento.

Cuando se produce el evento de ONTAP EMS, el evento se muestra en la página Events. Es posible seleccionar el evento para ver detalles sobre el evento de EMS en la página de detalles Event. También puede gestionar la disposición del evento o crear alertas para el evento.

Qué sucede cuando se recibe un evento

Cuando Unified Manager recibe un evento, se muestra en la página Dashboard, en la

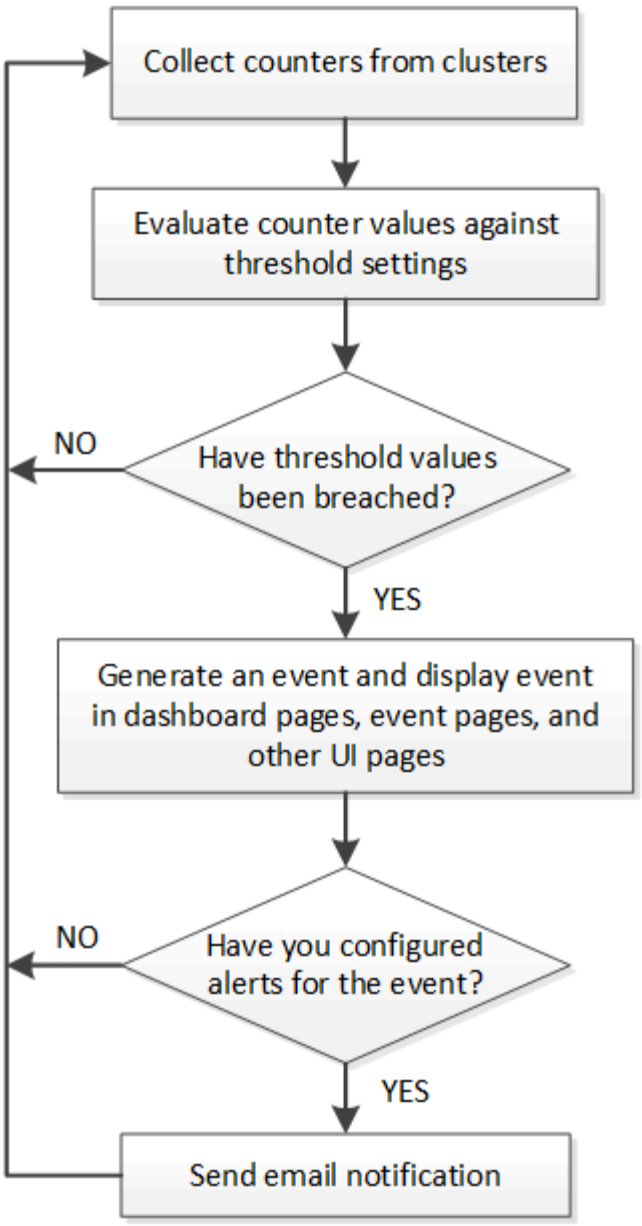
página del inventario Event Management, en las pestañas Summary y Explorer de la página Cluster/Performance y en la página de inventario específico del objeto (por ejemplo, la página Volumes/Health Inventory).

Cuando Unified Manager detecta varias instancias continuas de la misma condición de evento para el mismo componente de clúster, trata todas las ocurrencias como un solo evento, no como eventos independientes. La duración del evento aumenta para indicar que el evento sigue activo.

En función de la configuración de la página Configuración de alertas, puede notificar a otros usuarios acerca de estos eventos. La alerta hace que se inicien las siguientes acciones:

- Todos los usuarios administradores de Unified Manager pueden enviar un correo electrónico acerca del evento.
- El evento se puede enviar a otros destinatarios de correo electrónico.
- Se puede enviar una captura SNMP al receptor de capturas.
- Se puede ejecutar un script personalizado para realizar una acción.

Este flujo de trabajo se muestra en el siguiente diagrama.



Ver eventos y detalles de eventos

Puede ver detalles sobre un evento que ha activado Unified Manager para realizar acciones correctivas. Por ejemplo, si hay un volumen de evento de estado sin conexión, puede hacer clic en ese evento para ver los detalles y ejecutar acciones correctivas.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Los detalles del evento incluyen información como el origen del evento, la causa del evento y cualquier nota relacionada con el evento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Gestión de eventos**.

   De forma predeterminada, la vista todos los eventos activos muestra los eventos nuevos y reconocidos

(activos) que se han generado durante los 7 días anteriores que tienen un nivel de impacto de incidente o riesgo.

2. Si desea ver una categoría concreta de eventos, por ejemplo, eventos de capacidad o eventos de rendimiento, haga clic en **Ver** y seleccione en el menú de tipos de eventos.
3. Haga clic en el nombre del evento para el que desea ver los detalles.

   Los detalles del evento se muestran en la página de detalles Event.

Visualización de eventos sin asignar

Puede ver los eventos no asignados y, a continuación, asignar cada uno de ellos a un usuario que pueda resolverlos.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Gestión de eventos**.

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

2. En el panel **Filtros**, seleccione la opción de filtro **sin asignar** en el área **asignado a**.

Reconocer y resolver eventos

Debe reconocer un evento antes de empezar a trabajar en el problema que generó el evento para que no siga recibiendo notificaciones de alerta de repetición. Después de realizar una acción correctiva para un evento determinado, debe marcar el evento como resuelto.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Puede reconocer y resolver varios eventos al mismo tiempo.

No puede reconocer eventos de información.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Gestión de eventos**.
2. En la lista de eventos, realice las siguientes acciones para reconocer los eventos:

Si desea…	Realice lo siguiente…
Reconozca y marque un solo evento como resuelto	a. Haga clic en el nombre del evento. b. En la página de detalles Event, determine la causa del evento. c. Haga clic en **acuse de recibo**. d. Realice la acción correctiva adecuada. e. Haga clic en **Marcar como solucionado**.
Reconozca y marque varios eventos como resueltos	a. Determine la causa de los eventos desde la página de detalles del evento correspondiente. b. Seleccione los eventos. c. Haga clic en **acuse de recibo**. d. Realice las acciones correctivas necesarias. e. Haga clic en **Marcar como solucionado**.

Una vez que se Marca Resolved el evento, este se mueve a la lista de eventos resueltos.

3. **Opcional**: En el área **Notas y actualizaciones**, añada una nota sobre cómo abordó el evento y, a continuación, haga clic en **Post**.

Asignar eventos a usuarios específicos

Puede asignar eventos sin asignar a usted mismo o a otros usuarios, incluidos los usuarios remotos. Puede reasignar eventos asignados a otro usuario, si es necesario. Por ejemplo, cuando ocurren problemas frecuentes en un objeto de almacenamiento, puede asignar los eventos para estos problemas al usuario que gestiona ese objeto.

Lo que necesitará

- El nombre del usuario y el ID de correo electrónico deben estar configurados correctamente.
- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Gestión de eventos**.
2. En la página de inventario **Event Management**, seleccione uno o más eventos que desee asignar.
3. Asigne el evento seleccionando una de las siguientes opciones:

Si desea asignar el evento a…	Realice lo siguiente…
Usted mismo	Haga clic en **asignar a** > **Me**.

Si desea asignar el evento a…	Realice lo siguiente…
Otro usuario	a. Haga clic en **asignar a** > **otro usuario**. b. En el cuadro de diálogo asignar propietario, introduzca el nombre de usuario o seleccione un usuario de la lista desplegable. c. Haga clic en **asignar**. Se envía una notificación por correo electrónico al usuario. Si no introduce un nombre de usuario o selecciona un usuario de la lista desplegable y hace clic en **asignar**, el evento permanece sin asignar.

Deshabilitar eventos no deseados

Todos los eventos están habilitados de forma predeterminada. Es posible deshabilitar eventos globalmente para evitar la generación de notificaciones para eventos que no tienen importancia en el entorno. Puede habilitar eventos deshabilitados cuando se desea reanudar la recepción de notificaciones.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Si deshabilita eventos, los eventos generados previamente en el sistema se marcan como obsoletos, y no se activan las alertas configuradas para estos eventos. Cuando se habilitan eventos que están deshabilitados, las notificaciones para estos eventos se generan a partir del próximo ciclo de supervisión.

Cuando se deshabilita un evento para un objeto (por ejemplo, el `vol offline` Evento), y posteriormente, usted habilita el evento, Unified Manager no genera nuevos eventos para los objetos que quedan sin conexión cuando el evento estaba en estado deshabilitado. Unified Manager genera un evento nuevo solo cuando hay un cambio en el estado del objeto después de que se rehabilitó el evento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de eventos**.
2. En la página **Event Setup**, deshabilite o habilite eventos seleccionando una de las siguientes opciones:

Si desea…	Realice lo siguiente…
Deshabilite eventos	a. Haga clic en **Desactivar**. b. En el cuadro de diálogo Deshabilitar eventos, seleccione la gravedad del evento. c. En la columna Eventos coincidentes, seleccione los eventos que desea deshabilitar según la gravedad del evento y, a continuación, haga clic en la flecha derecha para mover dichos eventos a la columna Deshabilitar eventos. d. Haga clic en **Guardar y cerrar**. e. Compruebe que los eventos que ha deshabilitado se muestran en la vista de lista de la página Event Setup.
Habilite eventos	a. Seleccione la casilla de comprobación del evento o los eventos que desea habilitar. b. Haga clic en **Activar**.

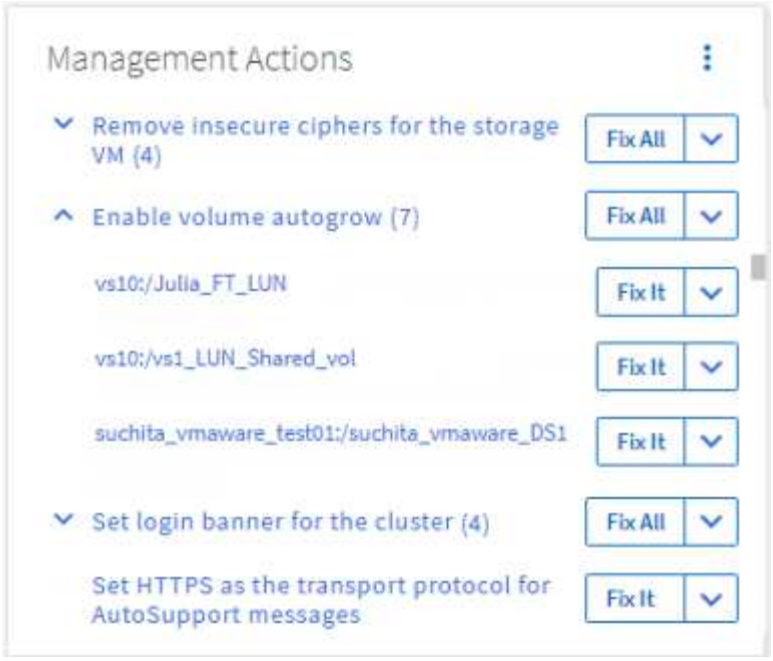
Solución de problemas mediante la solución automática de Unified Manager

Hay ciertos eventos que Unified Manager puede diagnosticar a fondo y proporcionar una única resolución mediante el botón **Fix it**. Si están disponibles, estas resoluciones se muestran en el Panel, en la página de detalles de eventos y en la selección Análisis de carga de trabajo del menú de navegación izquierdo.

La mayoría de los eventos tienen diversas resoluciones posibles que se muestran en la página de detalles del evento de modo que puede implementar la mejor solución con System Manager de ONTAP o la CLI de ONTAP. Una acción **Fix it** está disponible cuando Unified Manager ha determinado que existe una única resolución para solucionar el problema y que se puede resolver mediante un comando CLI de ONTAP.

Pasos

1. Para ver los eventos que se pueden solucionar desde **Panel**, haga clic en **Panel**.



2. Para resolver cualquiera de los problemas que Unified Manager puede solucionar, haga clic en el botón **Fix it**. Para solucionar un problema que existe en varios objetos, haga clic en el botón **solucionar todo**.

Para obtener información sobre los problemas que pueden solucionarse automáticamente con la solución de problemas, consulte "¿Qué problemas puede solucionar Unified Manager".

Habilitar y deshabilitar la generación de informes de eventos de Active IQ

Los eventos de la plataforma Active IQ se generan y se muestran de forma predeterminada en la interfaz de usuario de Unified Manager. Si considera que estos eventos son demasiado "ruidosos" o que no desea ver estos eventos en Unified Manager, puede deshabilitar la generación de estos eventos. Puede habilitarlos más adelante si desea reanudar la recepción de estas notificaciones.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Cuando deshabilita esta función, Unified Manager deja de recibir eventos de la plataforma Active IQ de inmediato.

Cuando habilita esta función, Unified Manager comienza a recibir eventos de la plataforma Active IQ poco después de medianoche según la zona horaria del clúster. La hora de inicio se basa en el momento en el que Unified Manager recibe mensajes de AutoSupport de cada clúster.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Configuración de funciones**.
2. En la página **Configuración de característica**, desactive o active los eventos de la plataforma Active IQ seleccionando una de las siguientes opciones:

Si desea…	Realice lo siguiente…
Deshabilite los eventos de la plataforma Active IQ	En el panel **Eventos del portal Active IQ**, mueva el botón deslizante hacia la izquierda.
Habilite los eventos de la plataforma de Active IQ	En el panel **Eventos del portal Active IQ**, mueva el botón deslizante hacia la derecha.

Carga de un nuevo archivo de reglas de Active IQ

Unified Manager comprueba si hay un nuevo archivo de eventos (reglas) de Active IQ de forma automática y descarga un nuevo archivo cuando hay reglas más recientes. Sin embargo, en sitios sin acceso a la red externa, es necesario cargar el archivo de reglas manualmente.

Las reglas de Active IQ también se conocen como reglas seguras de Config Advisor (CA).

Cuando se instala Unified Manager o se actualiza a una versión específica de un sitio sin conectividad de red, las reglas de Active IQ incluidas se encuentran disponibles automáticamente para su carga. Sin embargo, se recomienda descargar un nuevo archivo de reglas aproximadamente una vez al mes del sitio de soporte de NetApp para asegurarse de que los eventos actualizados se generan y sus sistemas de almacenamiento continúan funcionando de forma óptima.

Lo que necesitará

- La generación de informes de eventos del portal de Active IQ debe estar habilitada. Esta función está habilitada de forma predeterminada. Para obtener más información, consulte "Habilitar los eventos del portal de Active IQ".
- Debe descargar el archivo de reglas del sitio de soporte de NetApp.

  El archivo de reglas está ubicado en el directorio: https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure_rules.zip

Pasos

1. En un equipo con acceso a la red, desplácese hasta el sitio de soporte de NetApp y descargue las reglas actuales `.zip` archivo.

   El paquete de reglas agrupadas incluye el repositorio de reglas, orígenes de datos y un artículo de la base de conocimientos de NetApp.

   En los sistemas Windows, en un sitio sin conectividad de red, el artículo de la base de conocimientos de NetApp no se incluye de forma predeterminada con el instalador. Puede descargar el archivo *secure_rules.zip* del sitio de soporte y cargarlo para ver el artículo de KB de todas las reglas.

2. Transfiera el archivo de reglas a algún medio que pueda introducir en el área segura y, a continuación, cópielo en un sistema del área segura.
3. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de eventos**.

4. En la página **Event Setup**, haga clic en el botón **Upload Rules**.
5. En el cuadro de diálogo **Reglas de carga**, desplácese hasta y seleccione las reglas `.zip` Archivo que ha descargado y haga clic en **cargar**.

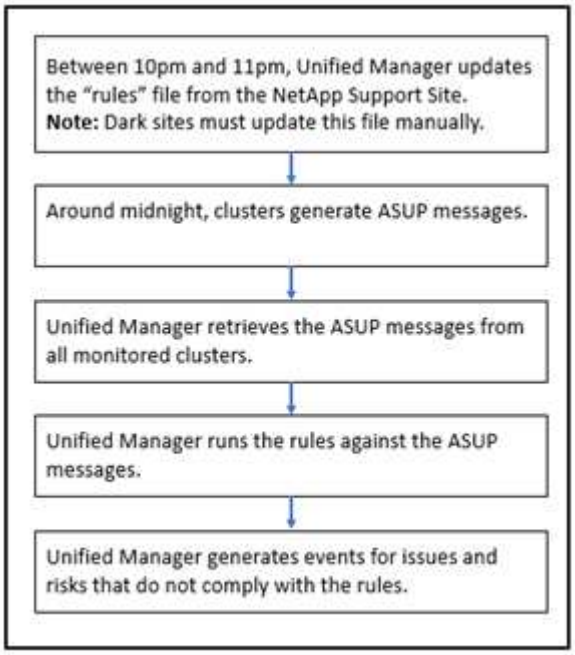
   Este proceso puede tardar varios minutos.

El archivo de reglas se descomprime en el servidor de Unified Manager. Después de que los clústeres gestionados generen un archivo AutoSupport después de la medianoche, Unified Manager comprueba los clústeres con respecto al archivo de reglas y genera nuevos eventos de riesgo e incidentes según sea necesario.

Para obtener más información, consulte este artículo de la base de conocimientos (KB): "Cómo actualizar manualmente las reglas de AIQUASecure en Active IQ Unified Manager".

Cómo se generan los eventos de la plataforma Active IQ

Los incidentes y riesgos de la plataforma de Active IQ se convierten en eventos de Unified Manager, como se muestra en el siguiente diagrama.



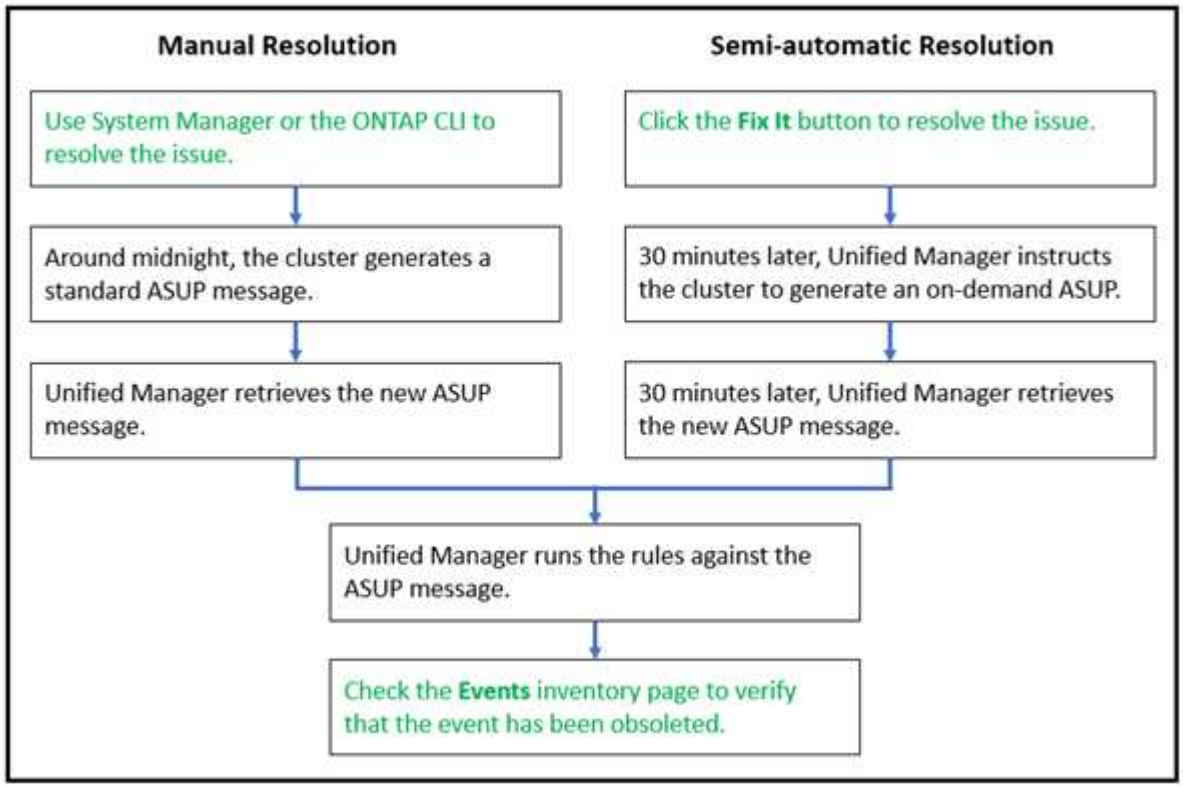
Como se puede ver, el archivo de reglas compilado en la plataforma de Active IQ se mantiene actualizado, los mensajes de AutoSupport de clúster se generan a diario y Unified Manager actualiza la lista de eventos a diario.

Resolver eventos de la plataforma Active IQ

Los incidentes y los riesgos de la plataforma Active IQ son similares a los de otros eventos de Unified Manager, ya que se pueden asignar a otros usuarios para su resolución y tienen los mismos estados disponibles. Sin embargo, cuando se resuelven estos tipos de eventos con el botón **Fix it**, puede verificar la resolución en cuestión de horas.

El siguiente diagrama muestra las acciones que debe realizar (en verde) y la acción que Unified Manager

realiza (en negro) al resolver eventos generados a partir de la plataforma de Active IQ.



Al realizar una resolución manual, debe iniciar sesión en System Manager o en la interfaz de línea de comandos de ONTAP para solucionar el problema. Solo podrá verificar el problema después de que el clúster genere un nuevo mensaje de AutoSupport a medianoche.

Al realizar una resolución semiautomática con el botón **Fix it**, puede comprobar que la corrección se ha realizado correctamente en cuestión de horas.

Configuración de los ajustes de retención de eventos

Es posible especificar el número de meses que se conserva un evento en el servidor de Unified Manager antes de eliminarlo automáticamente.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Conservar eventos durante más de 6 meses puede afectar al rendimiento del servidor y no es recomendable.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **retención de datos**.
2. En la página **retención de datos**, seleccione el control deslizante en el área retención de eventos y muévalos al número de meses que deben retener los eventos y haga clic en **Guardar**.

Qué es una ventana de mantenimiento de Unified Manager

La ventana de mantenimiento de Unified Manager se define para suprimir eventos y alertas de un plazo específico cuando se ha programado el mantenimiento del clúster y

no se desea recibir un gran número de notificaciones no deseadas.

Cuando se inicia la ventana de mantenimiento, se publica un evento "ventana de mantenimiento de objetos iniciada" en la página de inventario Gestión de eventos. Este evento se vuelve obsoleto automáticamente cuando finaliza la ventana de mantenimiento.

Durante una ventana de mantenimiento, aún se generan los eventos relacionados con todos los objetos de ese clúster, pero no aparecen en ninguna de las páginas de la interfaz de usuario y no se envían alertas ni otros tipos de notificaciones para estos eventos. Sin embargo, es posible ver los eventos generados para todos los objetos de almacenamiento durante una ventana de mantenimiento. Para ello, seleccione una de las opciones Ver de la página del inventario Event Management.

Puede programar una ventana de mantenimiento que se iniciará en el futuro, puede cambiar las horas de inicio y de finalización de una ventana de mantenimiento programada y puede cancelar una ventana de mantenimiento programada.

Programar una ventana de mantenimiento para deshabilitar las notificaciones de eventos del clúster

Si tiene un tiempo de inactividad planificado para un clúster, por ejemplo, para actualizar el clúster o mover uno de los nodos, puede eliminar los eventos y alertas que normalmente se generan durante ese periodo de tiempo mediante la programación de una ventana de mantenimiento de Unified Manager.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Durante una ventana de mantenimiento, aún se generan los eventos relacionados con todos los objetos de ese clúster, pero no aparecen en la página de eventos y no se envían alertas ni otros tipos de notificaciones para estos eventos.

El momento que introduzca para la ventana de mantenimiento se basa en la hora en el servidor de Unified Manager.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Storage Management** > **Cluster Setup**.
2. En la columna **modo de mantenimiento** del clúster, seleccione el botón deslizante y muévase a la derecha.

   Se muestra la ventana de calendario.

3. Seleccione la fecha y hora de inicio y finalización de la ventana de mantenimiento y haga clic en **aplicar**.

   Aparece el mensaje "programado" junto al botón deslizante.

Cuando se llega a la hora de inicio, el clúster pasa al modo de mantenimiento y se genera un evento "ventana de mantenimiento de objetos iniciada".

Cambiar o cancelar una ventana de mantenimiento programado

Si configuró una ventana de mantenimiento de Unified Manager para que se produzca en el futuro, puede cambiar las horas de inicio y de finalización o cancelar la ventana de

mantenimiento.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Cancelar una ventana de mantenimiento que se está ejecutando actualmente es útil si ha completado el mantenimiento del clúster antes de la hora de finalización de la ventana de mantenimiento programada, y desea volver a recibir eventos y alertas del clúster.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Storage Management** > **Cluster Setup**.
2. En la columna **modo de mantenimiento** del clúster:

Si desea…	Realice este paso…
Cambie el plazo de tiempo de un plazo de mantenimiento programado	a. Haga clic en el texto "scheduled" junto al botón del control deslizante. b. Cambie la fecha y la hora de inicio y finalización y haga clic en **aplicar**.
Ampliar la longitud de una ventana de mantenimiento activa	a. Haga clic en el texto "activo" junto al botón del control deslizante. b. Cambie la fecha y la hora de finalización y haga clic en **aplicar**.
Cancelar una ventana de mantenimiento programado	Seleccione el botón deslizante y muévase hacia la izquierda.
Cancelar una ventana de mantenimiento activa	Seleccione el botón deslizante y muévase hacia la izquierda.

Ver los eventos que se produjeron durante una ventana de mantenimiento

Si es necesario, puede ver los eventos generados para todos los objetos de almacenamiento durante una ventana de mantenimiento de Unified Manager. La mayoría de los eventos aparecerán en el estado Obsoleto una vez que se haya completado la ventana de mantenimiento y todos los recursos del sistema estén de respaldo y en ejecución.

Lo que necesitará

Debe haber al menos una ventana de mantenimiento completada antes de que haya algún evento disponible.

Los eventos que se produjeron durante una ventana de mantenimiento no aparecen de forma predeterminada en la página del inventario Event Management.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Eventos**.

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

2. En el panel Ver, seleccione la opción **todos los eventos generados durante el mantenimiento**.

   Se muestra la lista de eventos desencadenados durante los últimos 7 días de todas las sesiones de la ventana de mantenimiento y de todos los clusters.

3. Si ha habido varias ventanas de mantenimiento para un único clúster, puede hacer clic en el icono de calendario **tiempo activado** y seleccionar el período de tiempo para los eventos de la ventana de mantenimiento que le interesa ver.

Gestionar eventos de recursos del sistema host

Unified Manager incluye un servicio que supervisa problemas de recursos en el sistema host en el que está instalado Unified Manager. Problemas como falta de espacio en disco disponible o falta de memoria en el sistema host pueden desencadenar eventos de estación de gestión que se muestran como mensajes de banner en toda la parte superior de la interfaz de usuario.

Los eventos de la estación de gestión indican un problema con el sistema host en el que está instalado Unified Manager. Algunos ejemplos de problemas de la estación de gestión son que el espacio en disco se ejecuta poco en el sistema host, que Unified Manager carece de un ciclo de recogida de datos normal y que no se completa o se completó tarde un análisis de estadísticas porque se inició el siguiente sondeo de recopilación.

A diferencia de todos los demás mensajes de eventos de Unified Manager, estos eventos críticos y de advertencia de la estación de gestión concretos se muestran en mensajes de banner.

Paso

1. Para ver la información de eventos de la estación de administración, realice estas acciones:

Si desea…	Realice lo siguiente…
Ver detalles del evento	Haga clic en el banner del evento para mostrar la página de detalles Event que incluye soluciones sugeridas para el problema.
Ver todos los eventos de la estación de administración	a. En el panel de navegación izquierdo, haga clic en **Gestión de eventos**. b. En el panel Filters de la página del inventario Event Management, haga clic en el cuadro para Management Station en la lista Source Type.

Más información acerca de los eventos

Comprender los conceptos sobre eventos le ayuda a gestionar los clústeres y los objetos del clúster de forma eficiente y a definir las alertas de manera adecuada.

Definiciones de estado de eventos

El estado de un evento le ayuda a identificar si es necesaria una acción correctiva adecuada. Un evento puede ser Nuevo, reconocido, resuelto u Obsoleto. Tenga en cuenta que tanto los eventos nuevos como los reconocidos se consideran eventos activos.

los estados del evento son los siguientes:

- **Nuevo**

  El estado de un nuevo evento.

- **Reconocido**

  El estado de un evento cuando lo ha reconocido.

- **Resuelto**

  Estado de un evento cuando se Marca como solucionado.

- **Obsoleto**

  El estado de un evento cuando se corrige automáticamente o cuando la causa del evento ya no es válida.

  No puede reconocer ni resolver un evento obsoleto.

Ejemplo de diferentes estados de un evento

Los siguientes ejemplos ilustran los cambios de estado de eventos manuales y automáticos.

Cuando se activa el clúster de eventos no accesible, el estado del evento es New. Cuando reconoce el evento, el estado del evento cambia a reconocido. Cuando haya realizado una acción correctiva adecuada, debe marcar el evento como solucionado. El estado del evento cambia a resuelto.

Si el evento del clúster no accesible se genera debido a una interrupción del suministro eléctrico, cuando se restaura la alimentación, el clúster comienza a funcionar sin ninguna intervención del administrador. Por lo tanto, el evento clúster no accesible ya no es válido y el estado del evento cambia a Obsoleto en el siguiente ciclo de supervisión.

Unified Manager envía una alerta cuando un evento está en el estado Obsoleto o resuelto. La línea del asunto y el contenido del correo electrónico de una alerta ofrecen información acerca del estado del evento. Una captura SNMP también incluye información sobre el estado del evento.

Descripción de los tipos de gravedad de los eventos

Cada evento está asociado con un tipo de gravedad para ayudarle a priorizar los eventos que requieren una acción correctiva inmediata.

- **Crítico**

  Se produjo un problema que podría provocar una interrupción del servicio si no se toman acciones correctivas de inmediato.

Los eventos de rendimiento críticos se envían únicamente desde los umbrales definidos por el usuario.

- **Error**

  El origen del evento sigue en funcionamiento; sin embargo, se requiere una acción correctiva para evitar una interrupción del servicio.

- **Advertencia**

  El origen de eventos ha experimentado un suceso que debe conocer o un contador de rendimiento de un objeto de clúster está fuera del rango normal y debe supervisarse para asegurarse de que no alcance la gravedad crucial. Los eventos de esta gravedad no provocan interrupciones del servicio y podría no ser necesario realizar una acción correctiva inmediata.

  Los eventos de advertencia de rendimiento se envían desde umbrales definidos por el usuario, definidos por el sistema o dinámicos.

- **Información**

  El evento se produce cuando se descubre un nuevo objeto o cuando se realiza una acción del usuario. Por ejemplo, cuando se elimina un objeto de almacenamiento o cuando hay cambios de configuración, se genera el evento con tipo gravedad Information.

  Los eventos de información se envían directamente desde ONTAP cuando detecta un cambio de configuración.

Descripción de los niveles de impacto de eventos

Cada evento está asociado a un nivel de impacto (incidente, riesgo, evento o actualización) para ayudarle a priorizar los eventos que requieren una acción correctiva inmediata.

- **Incidente**

  Un incidente es un conjunto de eventos que pueden provocar que un clúster deje de servir datos al cliente y se quede sin espacio para almacenar datos. Los eventos con un nivel de impacto de incidente son los más graves. Se deberían tomar medidas correctivas inmediatas para evitar la interrupción del servicio.

- **Riesgo**

  Un riesgo es un conjunto de eventos que pueden provocar que un clúster deje de servir datos al cliente y se quede sin espacio para almacenar datos. Los eventos con un nivel de impacto de riesgo pueden causar interrupción del servicio. Puede que sea necesaria la acción correctiva.

- **Evento**

  Un evento es un cambio de estado o estado de los objetos de almacenamiento y sus atributos. Los eventos con un nivel de impacto de evento son informativos y no requieren acción correctiva.

- **Actualización**

  Los eventos de actualización son un tipo específico de evento que se informa en la plataforma Active IQ. Estos eventos identifican problemas en los que la resolución requiere actualizar el software ONTAP, el firmware del nodo o el software del sistema operativo (para avisos de seguridad). Quizás desee realizar

una acción correctiva inmediata para algunos de estos problemas, mientras que otros pueden esperar hasta el siguiente mantenimiento programado.

Descripción de las áreas de impacto de eventos

Los eventos se clasifican en seis áreas de impacto (disponibilidad, capacidad, configuración, rendimiento, protección, y seguridad) para permitirle concentrarse en los tipos de eventos de los que usted es responsable.

- **Disponibilidad**

  Los eventos de disponibilidad le notifican si un objeto de almacenamiento se desconecta, si un servicio de protocolo se desactiva, si se produce un problema con una conmutación al respaldo del almacenamiento o si se produce un problema con el hardware.

- **Capacidad**

  Los eventos de capacidad le notifican si los agregados, volúmenes, LUN o espacios de nombres se acercan o han alcanzado un umbral de tamaño, o si la tasa de crecimiento es inusual en el entorno.

- **Configuración**

  Los eventos de configuración informan de la detección, la eliminación, la adición, la eliminación o el nombre de los objetos de almacenamiento. Los eventos de configuración tienen un nivel de impacto de evento y un tipo de gravedad de información.

- **Rendimiento**

  Los eventos de rendimiento le notifican de las condiciones de recursos, configuración o actividad de su clúster que pueden afectar negativamente a la velocidad de la entrada o recuperación del almacenamiento de datos en los objetos de almacenamiento supervisados.

- **Protección**

  Los eventos de protección le notifican los incidentes o riesgos que implican las relaciones de SnapMirror, problemas con la capacidad de destino, problemas con las relaciones de SnapVault o problemas con trabajos de protección. Cualquier objeto de ONTAP (especialmente agregados, volúmenes y SVM) que alojen volúmenes secundarios y relaciones de protección se categorizan en el área de impacto de protección.

- **Seguridad**

  Los eventos de seguridad le notifican de qué forma se protegen los clústeres de ONTAP, las máquinas virtuales de almacenamiento (SVM) y los volúmenes en función de los parámetros definidos en la "Guía de fortalecimiento de la seguridad de NetApp para ONTAP 9".

  Además, esta área incluye los eventos de actualización notificados desde la plataforma Active IQ.

Cómo se calcula el estado del objeto

El estado del objeto está determinado por el evento más grave que actualmente tiene un estado Nuevo o reconocido. Por ejemplo, si el estado de un objeto es error, uno de los eventos del objeto tiene un tipo de gravedad de error. Cuando se ha realizado la acción

correctiva, el estado del evento pasa a resuelto.

Detalles de gráficos de eventos de rendimiento dinámicos

Para eventos de rendimiento dinámicos, en la sección Diagnóstico del sistema de la página de detalles de eventos, se enumeran las principales cargas de trabajo con la mayor latencia o uso del componente del clúster que es objeto de disputa.

Las estadísticas de rendimiento se basan en la hora en la que se detectó el evento de rendimiento hasta la última vez que se analizó el evento. Los gráficos también muestran estadísticas de rendimiento históricas del componente de clúster que está en disputa.

Por ejemplo, puede identificar cargas de trabajo con una alta utilización de un componente para determinar qué carga de trabajo se debe mover a un componente menos utilizado. Mover la carga de trabajo reduciría la cantidad de trabajo del componente actual, lo que posiblemente haría que el componente no fuera de contención. En la parte superior de esta sección se encuentra el intervalo de hora y fecha en que se detectó un evento y se analizó por última vez. Para los eventos activos (nuevos o reconocidos), se actualiza la última hora analizada.

Los gráficos de latencia y actividades muestran los nombres de las cargas de trabajo principales cuando pasa el cursor por encima del gráfico. Al hacer clic en el menú Workload Type (Tipo de carga de trabajo) situado a la derecha del gráfico, podrá ordenar las cargas de trabajo según su rol en el evento, incluido *tiburones*, *bravucons* o *Victimas*, y se mostrarán detalles sobre su latencia y su uso en el componente del clúster en disputa. Es posible comparar el valor real con el valor esperado para ver cuándo la carga de trabajo estaba fuera de su rango esperado de latencia o uso. Para obtener más información, consulte "Tipos de cargas de trabajo supervisadas por Unified Manager".

> Cuando se ordena según la desviación máxima en latencia, las cargas de trabajo definidas por el sistema no se muestran en la tabla, ya que la latencia solo se aplica a las cargas de trabajo definidas por el usuario. Las cargas de trabajo con valores bajos de latencia no se muestran en la tabla.

Para obtener más información sobre los umbrales de rendimiento dinámico, consulte "Analizar eventos de umbrales dinámicos de rendimiento".

Para obtener información acerca de cómo Unified Manager clasifica las cargas de trabajo y determina el orden de clasificación, consulte "La forma en que Unified Manager determina el impacto en el rendimiento de un evento".

Los datos en los gráficos muestran 24 horas de estadísticas de rendimiento antes de la última vez que se analizó el evento. Los valores reales y esperados para cada carga de trabajo se basan en el momento en el que participó la carga de trabajo en el evento. Por ejemplo, es posible que una carga de trabajo participe en un evento después de que se detecte el evento, por lo que es posible que sus estadísticas de rendimiento no coincidan con los valores en el momento de la detección de eventos. De forma predeterminada, las cargas de trabajo se ordenan por desviación máxima (mayor) en la latencia.

> Dado que Unified Manager conserva un máximo de 30 días de rendimiento histórico y datos de eventos de 5 minutos, si el evento tiene más de 30 días de antigüedad, no se muestran datos de rendimiento.

- **Columna de clasificación de carga de trabajo**
  - **Tabla de latencia**

Muestra el impacto del evento en la latencia de la carga de trabajo durante el último análisis.

- **Columna de uso de componentes**

  Muestra detalles acerca del uso de la carga de trabajo del componente de clúster en disputa. En los gráficos, el uso real es una línea azul. Una barra roja resalta la duración del evento, desde el tiempo de detección hasta el último tiempo analizado. Para obtener más información, consulte "Valores de medición del rendimiento de la carga de trabajo".

  Para el componente de red, ya que las estadísticas de rendimiento de red provienen de la actividad del clúster, esta columna no se muestra.

- **Uso de componentes**

  Muestra el historial de uso, en porcentaje, del procesamiento de red, el procesamiento de datos y los componentes agregados, o el historial de la actividad, en porcentaje, del componente del grupo de políticas de QoS. El gráfico no se muestra para los componentes de red o de interconexión. Puede apuntar a las estadísticas para ver las estadísticas de uso en un momento específico.

- **Escritura total MB/s Historial**

  Únicamente para el componente Recursos de MetroCluster, muestra el rendimiento de escritura total, en megabytes por segundo (Mbps), para todas las cargas de trabajo de volúmenes que se están reflejando en el clúster de partners en una configuración de MetroCluster.

- **Historial de eventos**

  Muestra líneas sombreadas en rojo para indicar los eventos históricos del componente en disputa. Para los eventos obsoletos, el gráfico muestra los eventos que ocurrieron antes de que se detectara el evento seleccionado y después de haberlo resuelto.

Cambios de configuración detectados por Unified Manager

Unified Manager supervisa sus clústeres para detectar cambios de configuración con el fin de ayudarle a determinar si un cambio podría haber causado o contribuido a un evento de rendimiento. Las páginas Performance Explorer muestran un icono de evento de cambio (●) para indicar la fecha y la hora en que se detectó el cambio.

Puede revisar los gráficos de rendimiento en las páginas Performance Explorer y en la página Workload Analysis para ver si el evento de cambio afecta al rendimiento del objeto de clúster seleccionado. Si el cambio se detectó en o aproximadamente al mismo tiempo que un evento de rendimiento, el cambio podría haber contribuido al problema, lo que provocó que se disparara la alerta de evento.

Unified Manager puede detectar los siguientes eventos de cambio, que se clasifican como eventos informativos:

- Un volumen se mueve entre agregados.

  Unified Manager puede detectar cuando el movimiento está en curso, completado o con errores. Si Unified Manager está inactivo durante un movimiento de volúmenes, cuando se realiza el backup, detecta el movimiento del volumen y muestra un evento de cambio para él.

- El límite de rendimiento (MB/s o IOPS) de un grupo de políticas de calidad de servicio que contiene uno o

más cambios en las cargas de trabajo supervisadas.

Cambiar el límite de un grupo de políticas puede provocar picos intermitentes en la latencia (tiempo de respuesta), que también podrían desencadenar eventos del grupo de políticas. La latencia vuelve a la normalidad de forma gradual y los eventos causados por los picos quedan obsoletos.

- Un nodo de un par de alta disponibilidad toma el control o devuelve el almacenamiento de su otro nodo.

  Unified Manager puede detectar cuándo se ha completado la operación de toma de control, toma de control parcial o retorno al nodo primario. Si la toma de control está provocada por un nodo de pánico, Unified Manager no detecta el evento.

- Se ha completado correctamente una actualización o una operación de reversión de ONTAP.

  Se muestran la versión anterior y la nueva.

Lista de eventos y tipos de gravedad

Puede usar la lista de eventos para familiarizarse con las categorías de eventos, los nombres de eventos y el tipo de gravedad de cada evento que puede ver en Unified Manager. Los eventos se muestran en orden alfabético por categoría de objeto.

Eventos agregados

Los eventos de agregado le proporcionan información sobre el estado de los agregados para poder supervisar posibles problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Disponibilidad

Un asterisco (*) identifica los eventos de EMS que se han convertido a eventos de Unified Manager.

Nombre del evento(nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Agregado sin conexión (ocumEvtagregateStateOffline)	Incidente	Agregado	Crítico
Error de agregado (ocumEvtagregateStateFailed)	Incidente	Agregado	Crítico
Agregado restringido (ocumEvtagregateStateRestricted)	Riesgo	Agregado	Advertencia

Nombre del evento(nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Reconstrucción de agregados (ocumEvtagregateRaidStateReconstructing)	Riesgo	Agregado	Advertencia
Agregado degradado (ocumEvtagregateRaidStaegraded)	Riesgo	Agregado	Advertencia
Nivel de cloud parcialmente accesible (ocumEventCloudTierPartiallyReacable)	Riesgo	Agregado	Advertencia
Nivel de cloud inaccesible (ocumEventCloudTierUnreacables)	Riesgo	Agregado	Error
Acceso denegado por el nivel de cloud para la reubicación de agregados *(arlNetraCaCheckFailed)	Riesgo	Agregado	Error
Acceso denegado por el nivel de cloud para la reubicación de agregados durante la conmutación por error de almacenamiento *(gbNetraCaCheckFailed)	Riesgo	Agregado	Error
Agregado de MetroCluster dejado atrás(ocumEvtMetroClusteragregateLeftBehind)	Riesgo	Agregado	Error
Mirroring de agregado de MetroCluster degradado(ocumEvtMetroClusteraggregateMirrorDeGruted)	Riesgo	Agregado	Error

Área de impacto: Capacidad

Nombre del evento(nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Espacio de agregado casi completo (ocumEvtagregateNearlyFull)	Riesgo	Agregado	Advertencia
Espacio agregado completo (ocumEvtagregateFull)	Riesgo	Agregado	Error
Días agregados hasta Full (ocumEvtagregateDaysUntilFullSoon)	Riesgo	Agregado	Error
Agregado sobrecomprometido(ocumEvtagregateOverkanty)	Riesgo	Agregado	Error
Agregado casi sobrecomprometido(ocumEvtagregateAlmostOverdted)	Riesgo	Agregado	Advertencia
Reserva de Snapshot de agregado completa(ocumEvtagregateSnapReserveFull)	Riesgo	Agregado	Advertencia
Tasa de crecimiento agregado anormal (ocumEvtagregarGrowthRateAbnormal)	Riesgo	Agregado	Advertencia

Área de impacto: Configuración

Nombre del evento(nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Agregado detectado (no aplicable)	Evento	Agregado	Información
Agregado cambiado de nombre (no aplicable)	Evento	Agregado	Información

Nombre del evento(nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Agregado eliminado (no aplicable)	Evento	Nodo	Información

Área de impacto: Rendimiento

Nombre del evento(nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se ha incumplido el umbral crítico de IOPS de agregado (ocumagregateIopsIncident)	Incidente	Agregado	Crítico
Se ha incumplido el umbral de advertencia de IOPS del agregado (ocumagregateIopsWarning)	Riesgo	Agregado	Advertencia
Se ha incumplido el umbral crítico de los MB/s agregados(ocumagregateMbpsIncident)	Incidente	Agregado	Crítico
Umbral de advertencia agregado MB/s incumplido (ocumagregateMbpsWarning)	Riesgo	Agregado	Advertencia
Se ha incumplido el umbral crítico de latencia de agregado (ocumagregateLatencyIncident)	Incidente	Agregado	Crítico
Umbral de advertencia de latencia agregada incumplido (ocumagregateLatencyWarning)	Riesgo	Agregado	Advertencia

Nombre del evento(nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se ha incumplido el umbral crítico de capacidad de rendimiento del agregado (ocumagregatePerfCapacidad UsedIncident).	Incidente	Agregado	Crítico
Se ha incumplido el umbral de advertencia de capacidad de rendimiento agregado utilizada (ocumagregatePerfCapacidad UsedWarning)	Riesgo	Agregado	Advertencia
Se ha incumplido el umbral crítico de utilización del agregado (ocumagregateUtilationIncident)	Incidente	Agregado	Crítico
Umbral de advertencia de utilización de agregado incumplido (ocumagregateUtillationWarning)	Riesgo	Agregado	Advertencia
Umbral sobreutilizado de discos agregados (ocumagregarDisksOverUtilizedWarning)	Riesgo	Agregado	Advertencia
Umbral dinámico agregado incumplido (ocumDynamicAgregEventWarning)	Riesgo	Agregado	Advertencia

Eventos del clúster

Los eventos del clúster proporcionan información sobre el estado de los clústeres, lo que permite supervisar los clústeres para detectar posibles problemas. Los eventos se agrupan por área de impacto, e incluyen el nombre del evento, el nombre de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Disponibilidad

Un asterisco (*) identifica los eventos de EMS que se han convertido a eventos de Unified Manager.

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
El clúster carece de discos de repuesto (ocumEvtDisksNoRepuestos)	Riesgo	Clúster	Advertencia
No se puede acceder al clúster (ocumEvtClusterUnacable).	Riesgo	Clúster	Error
Error de supervisión de clúster (fallo de ocumEvtClusterMonitoringFailed)	Riesgo	Clúster	Advertencia
Se incumplen los límites de capacidad de licencia de Cluster FabricPool (ocumEvtExternalCapacidad TierSpaceFull)	Riesgo	Clúster	Advertencia
Periodo de gracia que se inició NVMe-of * (nvmfGracePeriodStart)	Riesgo	Clúster	Advertencia
NVMe-of Grace Active *(nvmfGracePeriodActive)	Riesgo	Clúster	Advertencia
Periodo de gracia de NVMe-of expirado *(nvmfGracePeriodExpired)	Riesgo	Clúster	Advertencia
Ventana de mantenimiento de objetos iniciada (objectMaintenanceWindowStarted)	Evento	Clúster	Crítico
Ventana de mantenimiento de objetos finalizada (objectMaintenanceWindowEnded)	Evento	Clúster	Información

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Discos de repuesto MetroCluster dejados atrás (ocumEvtSpareDiskLeftBehind)	Riesgo	Clúster	Error
Conmutación de sitios automática no planificada de MetroCluster deshabilitada (ocumEvnedTMAutomaticUnplanSwitchOverDisabled).	Riesgo	Clúster	Advertencia
Se cambió la contraseña de usuario del clúster *(cluster.passwd.changed)	Evento	Clúster	Información

Área de impacto: Capacidad

Nombre del evento(nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Umbral de desequilibrio de capacidad del clúster incumplido (ocumConformanceNodeImbalanceWarning)	Riesgo	Clúster	Advertencia
Planificación del nivel de cloud del clúster (clusterCloudTierPlanningWarning)	Riesgo	Clúster	Advertencia
Resincronización de duplicación de FabricPool completada *(waflCaResyncComplete)	Evento	Clúster	Advertencia
Espacio FabricPool casi completo * (laestructura completo)	Riesgo	Clúster	Error

Área de impacto: Configuración

Nombre del evento(nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Nodo agregado (no aplicable)	Evento	Clúster	Información
Nodo eliminado (no aplicable)	Evento	Clúster	Información
Clúster eliminado (no aplicable)	Evento	Clúster	Información
Error al agregar el clúster (no aplicable)	Evento	Clúster	Error
Nombre del clúster cambiado (no aplicable)	Evento	Clúster	Información
EMS de emergencia recibido (no aplicable)	Evento	Clúster	Crítico
EMS crítico recibido (no aplicable)	Evento	Clúster	Crítico
Aviso EMS recibido (no aplicable)	Evento	Clúster	Error
Error EMS recibido (no aplicable)	Evento	Clúster	Advertencia
Aviso EMS recibido (no aplicable)	Evento	Clúster	Advertencia
Depurar EMS recibido (no aplicable)	Evento	Clúster	Advertencia
Aviso EMS recibido (no aplicable)	Evento	Clúster	Advertencia
EMS informativo recibido (no aplicable)	Evento	Clúster	Advertencia

Los eventos de EMS de ONTAP se clasifican en tres niveles de gravedad de evento de Unified Manager.

Nivel de gravedad de eventos de Unified Manager	Nivel de gravedad de evento de EMS de ONTAP

Crítico	Emergencia Crítico
Error	Alerta
Advertencia	Error Advertencia Depurar Aviso Informativo

Área de impacto: Rendimiento

Nombre del evento(nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Umbral de desequilibrio de carga de clúster incumplido()	Riesgo	Clúster	Advertencia
Se ha incumplido el umbral crítico de IOPS del clúster (ocumClusterIopsIncident).	Incidente	Clúster	Crítico
Se superó el umbral de advertencia de IOPS del clúster (ocumClusterIopsWarning).	Riesgo	Clúster	Advertencia
Se ha incumplido el umbral crítico del clúster MB/s (ocumClusterMbpsIncident).	Incidente	Clúster	Crítico
Umbral de advertencia de clúster MB/s incumplido(ocumClusterMbpsWarning)	Riesgo	Clúster	Advertencia

Nombre del evento(nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se ha incumplido el umbral dinámico del clúster (ocumClusterDynamicEventWarning)	Riesgo	Clúster	Advertencia

Área de impacto: Seguridad

Nombre del evento(nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Transporte HTTPS de AutoSupport deshabilitado (ocumClusterASUPHtpsConfiguredDisabled)	Riesgo	Clúster	Advertencia
Reenvío de registros no cifrado (ocumClusterAuditLogUnEncrypted)	Riesgo	Clúster	Advertencia
Usuario de administración local predeterminado habilitado (ocumClusterDefaultAdminEnabled)	Riesgo	Clúster	Advertencia
Modo FIPS desactivado (ocumClusterFipsDeshabilitado)	Riesgo	Clúster	Advertencia
Banner de inicio de sesión deshabilitado (ocumClusterLoginBannerDisabled)	Riesgo	Clúster	Advertencia
Se ha cambiado el banner de inicio de sesión (ocumClusterLoginBannerChanged)	Riesgo	Clúster	Advertencia

Nombre del evento(nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Destinos de reenvío de registros cambiados (ocumLogForwardDestinationsChanged)	Riesgo	Clúster	Advertencia
Nombres de servidores NTP modificados(ocumNtpServerNamesChanged)	Riesgo	Clúster	Advertencia
El recuento de servidores NTP es bajo (securityConfigNTPServerCountLowRisk)	Riesgo	Clúster	Advertencia
Comunicación punto del clúster sin cifrado (ocumClusterPeerEncryptionDisabled)	Riesgo	Clúster	Advertencia
SSH utiliza Ciphers no seguros(ocumClusterSSHInsecure).	Riesgo	Clúster	Advertencia
Protocolo Telnet habilitado(ocumClusterTelnetEnabled)	Riesgo	Clúster	Advertencia
Las contraseñas de algunas cuentas de usuario de ONTAP utilizan la función hash MD5 menos segura (ocumClusterMD5PasswordHashUsed)	Riesgo	Clúster	Advertencia
Cluster utiliza certificado autofirmado(ocumClusterSelfSignedCertificate)	Riesgo	Clúster	Advertencia
El shell remoto del clúster está habilitado (ocumClusterRshDisabled).	Riesgo	Clúster	Advertencia

Nombre del evento(nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Certificado de clúster a punto de expirar (ocumEvtClusterCertificateAboutToExpire)	Riesgo	Clúster	Advertencia
Certificado de clúster caducado (ocumEvtClusterCertificateExpired)	Riesgo	Clúster	Error

Eventos de discos

Los eventos de discos le proporcionan información sobre el estado de los discos para que pueda supervisar si existen problemas potenciales. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Discos flash: Bloques de repuesto casi consumidos(ocumEvtClusterFlashDiskFewerSpareBlockError)	Riesgo	Clúster	Error
Discos flash: Sin bloques de repuesto (ocumEvtClusterFlashDiskNoSpareBlockCritical)	Incidente	Clúster	Crítico
Algunos discos sin asignar(ocumEvtClusterUndeDesasignosAlgunos)	Riesgo	Clúster	Advertencia
Algunos discos con errores (ocumEvtDisksSomeFailed)	Incidente	Clúster	Crítico

Eventos de compartimentos

Los eventos de compartimentos le proporcionan información sobre el estado de los

compartimentos de bandejas de discos en el centro de datos para poder supervisar posibles problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Error de los ventiladores de la bandeja de discos (ocumEvtShelfFanFailed)	Incidente	Bandeja de almacenamiento	Crítico
Error en los suministros de alimentación de la bandeja de discos (ocumEvtShelfPowerSupplyFailed)	Incidente	Bandeja de almacenamiento	Crítico
Bandeja de discos multivía no configurada (ocumDiskShelfShelfcNotInMultiPath) Este evento no se aplica a: • Clústeres que están en una configuración de MetroCluster • Las siguientes plataformas: FAS2554, FAS2552, FAS2520 y FAS2240	Riesgo	Nodo	Advertencia
Fallo de ruta de bandeja de discos (ocumDiskShelfDiskShelfP PathFailure)	Riesgo	Bandeja de almacenamiento	Advertencia

Área de impacto: Configuración

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Bandeja de discos detectada (no aplicable)	Evento	Nodo	Información
Bandejas de discos eliminadas (no aplicable)	Evento	Nodo	Información

Eventos de ventiladores

Los eventos de ventiladores le ofrecen información acerca de los ventiladores de estado de los nodos en su centro de datos para que pueda supervisar si existen problemas potenciales. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Uno o más ventiladores fallidos (ocumEvtFanssOneOrMoreFailed)	Incidente	Nodo	Crítico

Eventos de tarjeta Flash

Los eventos de tarjeta Flash le proporcionan información sobre el estado de las tarjetas flash instaladas en los nodos en su centro de datos para poder supervisar posibles problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Tarjetas flash sin conexión (ocumEvtFlashCardOffline)	Incidente	Nodo	Crítico

Eventos Inodes

Los eventos de inodo proporcionan información cuando el inodo está lleno o casi lleno para poder supervisar de posibles problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Capacidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Inodos casi lleno(ocumEvtInodesAlmostFull)	Riesgo	Volumen	Advertencia

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Inodes Full (ocumEvtInodesFull)	Riesgo	Volumen	Error

Eventos de la interfaz de red (LIF)

Los eventos de la interfaz de red proporcionan información acerca del estado de su interfaz de red (LIF), para poder supervisar posibles problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Estado de la interfaz de red abajo (ocumEvtLifStatusDown)	Riesgo	Interfaz	Error
Estado de la interfaz de red FC/FCoE inactivo (ocumEvtFCLifStatusDown)	Riesgo	Interfaz	Error
Conmutación por error de la interfaz de red no posible (ocumEvtLifFailoverNotPossible)	Riesgo	Interfaz	Advertencia
Interfaz de red no en el puerto de inicio (ocumEvtLifNotAtHomePort)	Riesgo	Interfaz	Advertencia

Área de impacto: Configuración

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Ruta de interfaz de red no configurada (no aplicable)	Evento	Interfaz	Información

Área de impacto: Rendimiento

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se ha incumplido el umbral crítico de la interfaz de red MB/s(ocumNetworkLifMbpsIncident)	Incidente	Interfaz	Crítico
Se ha incumplido el umbral de advertencia de la interfaz de red MB/s (ocumNetworkLifMbpsWarning)	Riesgo	Interfaz	Advertencia
Se ha incumplido el umbral crítico de la interfaz de red FC MB/s (ocumFcpLifMbpsIncident)	Incidente	Interfaz	Crítico
Se ha incumplido el umbral de advertencia de la interfaz de red FC MB/s (ocumFcpLifMbpsWarning)	Riesgo	Interfaz	Advertencia
Se ha incumplido el umbral crítico de la interfaz de red FC de nVMF (OcumNvmfcLifMbpsIncident)	Incidente	Interfaz	Crítico
Se ha incumplido el umbral de advertencia de la interfaz de red FC de nVMF MB/s (ocumNvmfcLifMbpsWarning)	Riesgo	Interfaz	Advertencia

Eventos de LUN

Los eventos de LUN le ofrecen información acerca del estado de sus LUN, para que pueda supervisar de posibles problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Disponibilidad

Un asterisco (*) identifica los eventos de EMS que se han convertido a eventos de Unified Manager.

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
LUN sin conexión (ocumEvtLunOffline)	Incidente	LUN	Crítico
LUN destruida *(lunDestroy)	Evento	LUN	Información
LUN asignada con sistema operativo no compatible en un igroup (O4.UnsupportedOsType)	Incidente	LUN	Advertencia
Ruta activa única para acceder a LUN(ocumEvtLunSingleActivePath)	Riesgo	LUN	Advertencia
Sin rutas activas para acceder a la LUN (ocumEvtLunNotReacable)	Incidente	LUN	Crítico
No hay rutas optimizadas para acceder a la LUN (ocumEvtLunOptimizedPathInactive)	Riesgo	LUN	Advertencia
Sin rutas para acceder a la LUN desde un partner de alta disponibilidad (ocumEvtLunHaPathInactive)	Riesgo	LUN	Advertencia
Sin ruta para acceder a la LUN desde un nodo en el par de alta disponibilidad (ocumEvtLunNodePathStatusDown)	Riesgo	LUN	Error

Área de impacto: Capacidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Espacio insuficiente para la copia Snapshot de la LUN(ocumEvtLunSnapshotNotPossible)	Riesgo	Volumen	Advertencia

Área de impacto: Configuración

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
LUN asignada con sistema operativo no compatible en un igroup (O4.UnsupportedOsType)	Riesgo	LUN	Advertencia

Área de impacto: Rendimiento

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se superó el umbral crítico de IOPS de LUN(ocumLunIopsIncident)	Incidente	LUN	Crítico
Se superó el umbral de advertencia de IOPS de LUN (ocumLunIopsWarning).	Riesgo	LUN	Advertencia
Se ha incumplido el umbral crítico de LUN MB/s (ocumLunMbpsIncident)	Incidente	LUN	Crítico
Se ha incumplido el umbral de advertencia de LUN MB/s (ocumLunMbpsWarning)	Riesgo	LUN	Advertencia
Se ha incumplido el umbral crítico de latencia ms/op de LUN (ocumLunLatencyIncident)	Incidente	LUN	Crítico

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se ha incumplido el umbral de advertencia de latencia de ms/op de LUN (ocumLunLatencyWarning)	Riesgo	LUN	Advertencia
Se insuperó la latencia de LUN y el umbral crítico de IOPS (ocumLunLatencyIopsIncident).	Incidente	LUN	Crítico
Se superó el umbral de advertencia de latencia de LUN y IOPS (ocumLunencyIopsWarning)	Riesgo	LUN	Advertencia
Se ha incumplido el umbral crítico de latencia de LUN y MB/s (ocumLunLatencyMbpsIncident)	Incidente	LUN	Crítico
Se ha incumplido el umbral de advertencia de latencia y MB/s de LUN (ocumLunLatencyMbpsWarning)	Riesgo	LUN	Advertencia
Latencia de LUN y capacidad de rendimiento agregado utilizada umbral crítico incumplido (ocumLunencyAggregatePerfCapacidadUsedIncident)	Incidente	LUN	Crítico
Latencia de LUN y capacidad de rendimiento agregado utilizada umbral de advertencia incumplido (ocumLunencyAggregatePerfCapacidadUsedWarning)	Riesgo	LUN	Advertencia

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se ha incumplido el umbral crítico de latencia de LUN y uso del agregado (OculunLatencyAggregate adición de utilidades)	Incidente	LUN	Crítico
Se ha incumplido el umbral de advertencia de latencia de LUN y utilización de agregados (ocumLunarCentral agregationUtilationWarning)	Riesgo	LUN	Advertencia
Latencia de LUN y capacidad de rendimiento de nodos utilizada umbral crítico incumplido (ocumLunencyNodePerfCapacidad UsedIncident)	Incidente	LUN	Crítico
Latencia de LUN y capacidad de rendimiento de nodos utilizada umbral de advertencia incumplido (ocumLunencyNodePerfCapacidad UsedWarning)	Riesgo	LUN	Advertencia
Latencia de LUN y capacidad de rendimiento de nodos utilizados: Se superó el umbral crucial de la toma de control (ocumLunLatencyAggregate PerfCapityUsedTakeOverIncident)	Incidente	LUN	Crítico
Latencia de LUN y capacidad de rendimiento de nodos utilizados: Se superó el umbral de advertencia de toma de control (ocumLunencyAggregate PerfCapityUsedTakeOver Warning)	Riesgo	LUN	Advertencia

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se superó el umbral crítico de latencia de LUN y uso de nodos (ocumLunNodeUtilationIncident)	Incidente	LUN	Crítico
Umbral de advertencia de latencia de LUN y uso de nodos incumplido (ocumLunNodeUtilationWarning)	Riesgo	LUN	Advertencia
Se superó el umbral de advertencia de IOPS máximo de LUN de QoS (ocumQosLunMaxIopsWarning)	Riesgo	LUN	Advertencia
Se ha incumplido el umbral de advertencia máximo MB/s de LUN de QoS (ocumQosLunMaxMbpsWarning)	Riesgo	LUN	Advertencia
Se superó el umbral de latencia de LUN de cargas de trabajo definido por la política de nivel de servicio de rendimiento (ocumConforceLatencyWarning)	Riesgo	LUN	Advertencia

Eventos de la estación de gestión

Los eventos de la estación de gestión le proporcionan información sobre el estado del servidor en el que está instalado Unified Manager para poder supervisar posibles problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Configuración

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Espacio en disco del servidor de gestión casi completo (ocumEvtUnifiedManagerDiskNearSpacelyFull)	Riesgo	Estación de gestión	Advertencia
Espacio completo en disco del servidor de administración (ocumEvtUnifiedManagerDiskSpaceFull)	Incidente	Estación de gestión	Crítico
Memoria de servidor de administración baja (ocumEvtUnifiedManagerMemoryLow)	Riesgo	Estación de gestión	Advertencia
Servidor de administración casi sin memoria (ocumEvtUnifiedManagerMemoriaAlmostOut)	Incidente	Estación de gestión	Crítico
Se ha aumentado el tamaño del archivo de registro de MySQL; se requiere un reinicio (ocumEvtMysqlLogFileSizeWarning)	Incidente	Estación de gestión	Advertencia
La asignación de tamaño total de registro de auditoría está a cerca de estar lleno	Riesgo	Estación de gestión	Advertencia
Certificado de servidor de syslog a punto de expirar	Riesgo	Estación de gestión	Advertencia
El certificado de servidor de syslog caducó	Riesgo	Estación de gestión	Error
Archivo de registro de auditoría alterado	Riesgo	Estación de gestión	Advertencia
Se eliminó el archivo de registro de auditoría	Riesgo	Estación de gestión	Advertencia

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Error de conexión del servidor de syslog	Riesgo	Estación de gestión	Error
Se cambió la configuración del servidor de syslog	Evento	Estación de gestión	Advertencia

Área de impacto: Rendimiento

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
El análisis de datos de rendimiento se ve afectado(ocumEvtUnifiedManagerDataMissingAnalyze)	Riesgo	Estación de gestión	Advertencia
La recopilación de datos de rendimiento se ve afectada (ocumEvtUnifiedManagerDataMissingCollection)	Incidente	Estación de gestión	Crítico

Estos dos últimos eventos de rendimiento solo estaban disponibles para Unified Manager 7.2. Si alguno de estos eventos se encuentra en el estado New y se actualiza a una versión más reciente del software Unified Manager, los eventos no se depuran automáticamente. Deberá mover los eventos al estado Resolved manualmente.

Eventos del puente MetroCluster

Los eventos de puente de MetroCluster le proporcionan información sobre el estado de los puentes para que pueda supervisar si existen problemas potenciales en una configuración de MetroCluster over FC. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Puente no accesible(ocumEvtBridgeUnacable)	Incidente	Puente MetroCluster	Crítico

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Temperatura del puente anormal (ocumEvtBridgeTemperatureAbnormal)	Incidente	Puente MetroCluster	Crítico

Eventos de conectividad de MetroCluster

Los eventos de conectividad le proporcionan información sobre la conectividad entre los componentes de un clúster y entre los clústeres de MetroCluster over FC y MetroCluster over IP, para poder supervisar posibles problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Eventos comunes en ambas configuraciones

Estos eventos de conectividad son comunes para configuraciones de MetroCluster over FC y MetroCluster over IP.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Todos los enlaces entre socios de MetroCluster Down(ocumEvtMetroClusterAllLinksBetweenPartnersDown)	Incidente	Relación de MetroCluster	Crítico
No se puede acceder a los partners de MetroCluster sobre la red de relaciones entre iguales (ocumEvtMetroClusterPartnersNotReachableOverPeeringNetwork)	Incidente	Relación de MetroCluster	Crítico
La funcionalidad de recuperación ante desastres de MetroCluster se vio afectada (ocumEvtMetroClusterDRStatusImped)	Riesgo	Relación de MetroCluster	Crítico

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Configuración de MetroCluster conmutada(ocumEvtMetroClusterDRStatusImped)	Riesgo	Relación de MetroCluster	Advertencia

Configuración de MetroCluster over FC

Estos eventos tienen que ver con las configuraciones de MetroCluster over FC.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Todos los enlaces Inter-Switch Down(ocumEvtMetroClusterAllISLBetweenSwitchesDown)	Incidente	Conexión entre switches MetroCluster	Crítico
Puente FC-SAS hacia la pila de almacenamiento hacia abajo (ocumEvtBridgeSasPortDown)	Incidente	Conexión de pila de puente de MetroCluster	Crítico
Configuración de MetroCluster parcialmente conmutada(ocumEvtMetroClusterDRStatusPartiallyImped)	Riesgo	Relación de MetroCluster	Error
Del nodo al switch FC todos los enlaces de interconexión de FC-VI están inactivos (ocumEvtMcNodeSwitchFcviLinksDown)	Incidente	Conexión de switch del nodo MetroCluster	Crítico
Del nodo al switch FC uno o varios vínculos FC-Initiator Down (ocumEvtMcNodeSwitchFcLinksOneOrMoreDown)	Riesgo	Conexión de switch del nodo MetroCluster	Advertencia

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Del nodo al switch FC todos los enlaces de iniciador FC abajo (ocumEvtMcNodeSwitchFcLinksDown)	Incidente	Conexión de switch del nodo MetroCluster	Crítico
Conmutador a enlace FC Bridge FC Down (ocumEvtMcSwitchBridgeFcLinksDown)	Incidente	Conexión del puente del conmutador MetroCluster	Crítico
Inter Node todos los enlaces de interconexión FC VI abajo (ocumEvtMcInterNodeLinksDown)	Incidente	Conexión entre nodos	Crítico
Inter Node uno o más enlaces de interconexión FC VI hacia abajo (ocumEvtMcInterNodeLinksOneOrMoreDown)	Riesgo	Conexión entre nodos	Advertencia
Enlace de nodo a puente hacia abajo (ocumEvtMcNodeBridgeLinksDown)	Incidente	Conexión de puente de nodo	Crítico
Nodo a pila de almacenamiento todos los enlaces SAS abajo (ocumEvtMcNodeStackLinksDown)	Incidente	Conexión de pila de nodos	Crítico
Nodo a pila de almacenamiento uno o varios enlaces SAS abajo (ocumEvtMcNodeStackLinksOneOrMoreDown)	Riesgo	Conexión de pila de nodos	Advertencia

Configuración de MetroCluster over IP

Estos eventos tienen que ver con las configuraciones de MetroCluster por IP.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
El estado de la conectividad entre sitios IP de MetroCluster está inactivo (cc IntersiteStatusDown).	Riesgo	Relación de MetroCluster	Crítico
Conexión del nodo MetroCluster-IP al switch sin conexión (mccIpPortStatusOffline)	Riesgo	Nodo	Error

Eventos del switch de MetroCluster

Los eventos de switch de MetroCluster para configuraciones de MetroCluster over FC le proporcionan información sobre el estado de los switches MetroCluster de modo que pueda supervisar si existen posibles problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Temperatura del interruptor anormal (ocumEvtSwitchTemperatureAnormal)	Incidente	Switch MetroCluster	Crítico
Interruptor no accesible (ocumEvtSwitchUnacable)	Incidente	Switch MetroCluster	Crítico
Fallo de los ventiladores del conmutador (ocumEvtSwitchFansOneOrMoreFailed)	Incidente	Switch MetroCluster	Crítico
Error en las fuentes de alimentación del switch (fallo de ocumEvtPowerSwitchSupplesOneOrMoreFailed)	Incidente	Switch MetroCluster	Crítico

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Fallo en los sensores de temperatura del interruptor (ocumEvtSwitchTemperatureSensorFailed) Este evento se aplica únicamente a switches Cisco.	Incidente	Switch MetroCluster	Crítico

Eventos de espacio de nombres de NVMe

Los eventos de espacio de nombres de NVMe ofrecen información sobre el estado de los espacios de nombres para poder supervisar si existen problemas potenciales. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Un asterisco (*) identifica los eventos de EMS que se han convertido a eventos de Unified Manager.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
NVMeNS sin conexión * (nvmeNamespaceStatusOffline)	Evento	Espacio de nombres	Información
NVMeNS Online * (nvmeNamespaceStatusOnline)	Evento	Espacio de nombres	Información
NVMeNS fuera del espacio * (nvmeNamespaceSpaceOutOfSpace)	Riesgo	Espacio de nombres	Advertencia
NVMeNS Destroy * (nvmeNamespaceDestroy)	Evento	Espacio de nombres	Información

Área de impacto: Rendimiento

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se superó el umbral crucial de IOPS del espacio de nombres de NVMe (ocumNvmeNamespaceIopsIncident)	Incidente	Espacio de nombres	Crítico
Se superó el umbral de advertencia de IOPS del espacio de nombres de NVMe (ocumNvmeNamespaceIopsWarning)	Riesgo	Espacio de nombres	Advertencia
Se ha incumplido el umbral crítico del espacio de nombres NVMe MB/s (ocumNvmeNamespaceMbpsIncident)	Incidente	Espacio de nombres	Crítico
Se ha incumplido el umbral de advertencia de espacio de nombres NVMe MB/s (ocumNvmeNamespaceMbpsWarning)	Riesgo	Espacio de nombres	Advertencia
Se ha incumplido el umbral crítico de latencia del espacio de nombres NVMe ms/op (ocumNvmeNamespaceLatencyIncident)	Incidente	Espacio de nombres	Crítico
Se insuperó el umbral de advertencia de latencia de espacio de nombres de NVMe en ms/op (ocumNvmeNamespaceLatencyWarning)	Riesgo	Espacio de nombres	Advertencia
Se ha incumplido la latencia del espacio de nombres de NVMe y el umbral crítico de IOPS (ocumNvmeNamespaceLatencyIopsIncident)	Incidente	Espacio de nombres	Crítico

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se insuperó el umbral de advertencia de latencia de espacio de nombres y de IOPS de NVMe (ocumNvmeNamespaceLatencyIopsWarning)	Riesgo	Espacio de nombres	Advertencia
Se insuperó la latencia del espacio de nombres de NVMe y el umbral crítico de MB/s(ocumNvmeNamespaceLatencyMbpsIncident)	Incidente	Espacio de nombres	Crítico
Se insuperó el umbral de advertencia de latencia del espacio de nombres de NVMe y MB/s(ocumNvmeNamespaceLatencyMbpsWarning)	Riesgo	Espacio de nombres	Advertencia

Eventos de nodo

Los eventos de nodo le proporcionan información acerca del estado del nodo para poder supervisar posibles problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Un asterisco (*) identifica los eventos de EMS que se han convertido a eventos de Unified Manager.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Espacio de volumen raíz del nodo casi completo (ocumEvtClusterNodeRootVolumeNearSpacelyFull)	Riesgo	Nodo	Advertencia
Cloud AWS MetaDataConnFail *(ocumCloudAwsMetadataConnFail)	Riesgo	Nodo	Error

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
IAMCredsExpired de Cloud AWS *(ocumCloudAwsIamCredsExpired)	Riesgo	Nodo	Error
IAMCredsInvalid de Cloud AWS *(ocumCloudAwsIamCredsInvalid)	Riesgo	Nodo	Error
IAMCredsNotFound de Cloud AWS *(ocumCloudAwsIamCredsNotFound)	Riesgo	Nodo	Error
IAMCredsNotInitialized * de Cloud AWS(ocumCloudAwsIamCredsNotInitialized)	Evento	Nodo	Información
IAMRoleinválido de Cloud AWS *(ocumCloudAwsIamRoleInvalid)	Riesgo	Nodo	Error
IAMRoleNotFound de Cloud AWS *(ocumCloudAwsIamRoleNotFound)	Riesgo	Nodo	Error
Host de nivel de cloud no resoluble *(ocumObjstoreHostUnresoluble)	Riesgo	Nodo	Error
LIF de interconexión de clústeres en el cloud Down *(ocumObjstoreInterClusterLifDown)	Riesgo	Nodo	Error
Uno de los pools de NFSv4 agotados *(nbladeNfsv4PoolEXhaust)	Incidente	Nodo	Crítico

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
La solicitud no coincide con la firma del nivel de cloud * (oscilatrediscordancia)	Riesgo	Nodo	Error

Área de impacto: Capacidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Memoria del monitor QoS en formato *(ocumQosmonitoryMauned)	Riesgo	Nodo	Error
Memoria de monitorización de QoS * (ocumQosmonitoryMemoriaAbada)	Evento	Nodo	Información

Área de impacto: Configuración

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Nodo cambiado de nombre (no aplicable)	Evento	Nodo	Información

Área de impacto: Rendimiento

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se superó el umbral crucial de IOPS de nodo (ocumNodeIopsIncident)	Incidente	Nodo	Crítico
Se superó el umbral de advertencia de IOPS del nodo (ocumNodeIopsWarning)	Riesgo	Nodo	Advertencia
Umbral crítico del nodo MB/s incumplido(ocumNodeMbpsIncident)	Incidente	Nodo	Crítico

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Umbral de advertencia de nodo MB/s incumplido (ocumNodeMbpsWarning)	Riesgo	Nodo	Advertencia
Se ha incumplido el umbral crítico de latencia de los nodos ms/op (ocumNodeLatencyIncident).	Incidente	Nodo	Crítico
Umbral de advertencia de latencia de nodos ms/op violado (ocumNodeLatencyWarning)	Riesgo	Nodo	Advertencia
Se infringió la capacidad de rendimiento del nodo utilizado el umbral crítico (ocumNodePerfCapacidad UsedIncident)	Incidente	Nodo	Crítico
Se superó el umbral de advertencia de capacidad de rendimiento del nodo usado (ocumNodePerfCapacidad UsedWarning).	Riesgo	Nodo	Advertencia
Capacidad de rendimiento del nodo utilizada: Se ha infringido el umbral crítico de la toma de control (ocumNodePerfCapacidad UsedTakeoverIncident)	Incidente	Nodo	Crítico
Capacidad de rendimiento del nodo utilizada: Se superó el umbral de advertencia de toma de control (ocumNodePerfCapacidad UsedTakeoverWarning)	Riesgo	Nodo	Advertencia
Se superó el umbral crítico de uso de nodos (ocumNodeUtilationIncident)	Incidente	Nodo	Crítico

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se superó el umbral de advertencia de utilización de nodos (ocumNodeUtilationWarning)	Riesgo	Nodo	Advertencia
Umbral sobreutilizado de par de alta disponibilidad de nodo incumplido (ocumNodeHaPairOverUtilizedInformation)	Evento	Nodo	Información
Umbral de fragmentación de disco de nodo infringido (ocumNodeDiskFragmentationWarning)	Riesgo	Nodo	Advertencia
Umbral de capacidad de rendimiento utilizada infringido (ocumNodeOverUtilizedWarning)	Riesgo	Nodo	Advertencia
Umbral dinámico del nodo incumplido (ocumDynamicEventWarning)	Riesgo	Nodo	Advertencia

Área de impacto: Seguridad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
ID de asesoría: NTAP-<*Advisory ID*>(ocumx)	Riesgo	Nodo	Crítico

Eventos de la batería NVRAM

Los eventos de batería de NVRAM le ofrecen información acerca del estado de las baterías para que pueda supervisar si existen problemas potenciales. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Batería NVRAM baja (ocumEvtNvramBatteryLow)	Riesgo	Nodo	Advertencia
Batería NVRAM descargada (ocumEvtNvramBatteryDiscared)	Riesgo	Nodo	Error
Batería NVRAM demasiado cargada (ocumEvtNvramBatteryOverCharged)	Incidente	Nodo	Crítico

Eventos del puerto

Los eventos de puerto le ofrecen el estado acerca de los puertos del clúster para que pueda supervisar los cambios o los problemas en el puerto, como si el puerto está inactivo.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Estado del puerto inactivo (ocumEvtPortStatusDown)	Incidente	Nodo	Crítico

Área de impacto: Rendimiento

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se ha incumplido el umbral crítico del puerto de red MB/s(ocumNetworkPortMbpsIncident)	Incidente	Puerto	Crítico
Umbral de advertencia de puerto de red MB/s incumplido(ocumNetworkPortMbpsWarning)	Riesgo	Puerto	Advertencia

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se ha incumplido el umbral crítico del puerto FCP MB/s(ocumFcpPortMbpsIncident)	Incidente	Puerto	Crítico
Umbral de advertencia de puerto FCP MB/s incumplido(ocumFcpPortMbpsWarning)	Riesgo	Puerto	Advertencia
Se ha incumplido el umbral crítico de utilización de puertos de red (ocumNetworkPortUtilationIncident)	Incidente	Puerto	Crítico
Umbral de advertencia de utilización de puerto de red incumplido (ocumNetworkPortUtilationWarning)	Riesgo	Puerto	Advertencia
Se ha incumplido el umbral crítico de utilización de puertos FCP (ocumFcpPortUtilizationIncident)	Incidente	Puerto	Crítico
Se ha incumplido el umbral de advertencia de utilización de puertos FCP (ocumFcpPortUtilizationWarning)	Riesgo	Puerto	Advertencia

Eventos de suministro de alimentación

Los eventos de suministros de alimentación le proporcionan información sobre el estado del hardware para poder supervisar si existen problemas potenciales. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Una o más fuentes de alimentación con fallos (ocumEvtPowerSupplyOneOrMoreFailed)	Incidente	Nodo	Crítico

Eventos de protección

Los eventos de protección le indican si un trabajo se ha producido un error o se ha anulado para poder supervisar si hay problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Zona de impacto: Protección

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Error de trabajo de protección (ocumEvtProtectionJobTaskFailed)	Incidente	Servicio de volumen o almacenamiento	Crítico
Trabajo de protección anulado (ocumEvtProtectionJobAborted)	Riesgo	Servicio de volumen o almacenamiento	Advertencia

Eventos para qtrees

Los eventos para qtrees proporcionan información sobre la capacidad para qtrees y los límites de archivos y discos para poder realizar un seguimiento de posibles problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Capacidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Espacio Qtree casi completo (ocumEvtQtreeSpaceNearlyFull)	Riesgo	Qtree	Advertencia

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Espacio completo para Qtree (ocumEvtQtreeSpaceFull)	Riesgo	Qtree	Error
Espacio de Qtree normal (ocumEvtQtreeSpaceThresholdOk)	Evento	Qtree	Información
Se ha alcanzado el límite duro de archivos Qtree (ocumEvtQtreeFilesHardLimitReached)	Incidente	Qtree	Crítico
Límite de software de archivos Qtree incumplido (ocumEvtQtreeFilesSoftLimitBreached)	Riesgo	Qtree	Advertencia
Se ha alcanzado el límite duro de espacio de Qtree (ocumEvtQtreeSpaceHardLimitReached)	Incidente	Qtree	Crítico
Se violó el límite de espacio blando de Qtree (ocumEvtQtreeSpaceSoftLimitBreached)	Riesgo	Qtree	Advertencia

Eventos del procesador de servicios

Los eventos de procesador de servicios le proporcionan información sobre el estado de su procesador para que pueda supervisar si existen posibles problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Procesador de servicios no configurado (ocumEvtServiceProcessorNotConfigred)	Riesgo	Nodo	Advertencia

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Procesador de servicios sin conexión (ocumEvtServiceProcessorOffline)	Riesgo	Nodo	Error

Eventos de relaciones con SnapMirror

Los eventos de relaciones de SnapMirror le proporcionan información sobre el estado de sus relaciones de SnapMirror asíncrono y síncrono para que pueda supervisar posibles problemas. Los eventos de relación de SnapMirror asíncrono se generan tanto para máquinas virtuales de almacenamiento como para volúmenes, pero los eventos de relación de SnapMirror síncrono solo se generan para las relaciones de volumen. No se ha generado ningún evento para los volúmenes que forman parte de las relaciones de recuperación ante desastres de Storage VM. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Zona de impacto: Protección

Un asterisco (*) identifica los eventos de EMS que se han convertido a eventos de Unified Manager.

Los eventos de las relaciones de SnapMirror se generan para equipos virtuales de almacenamiento protegidos mediante la recuperación ante desastres de Storage VM, pero no para las relaciones de objetos constituyentes.

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Replicación de mirror insalubre (ocumEvtSnapmirrorRelationshipUnheaded)	Riesgo	Relación de SnapMirror	Advertencia
Replicación de mirroring rota-off (ocumEvtSnapmirrorRelationshipStateBrokenoff)	Riesgo	Relación de SnapMirror	Error
Error al inicializar la replicación de reflejo (ocumEvtSnapmirrorRerelationshipInitializeFailed)	Riesgo	Relación de SnapMirror	Error

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Error en la actualización de replicación de reflejo (ocumEvtSnapmirrorRelationship shipUpdateFailed)	Riesgo	Relación de SnapMirror	Error
Error de desfase de replicación de réplica (ocumEvtSnapMirrorRelationship shipLagError)	Riesgo	Relación de SnapMirror	Error
Aviso de desfase de replicación de réplica (ocumEvtSnapMirrorRelationship shillWarning)	Riesgo	Relación de SnapMirror	Advertencia
Error en la resincronización de replicación de reflejo (ocumEvtSnapmirrorRelationshipResyncFailed)	Riesgo	Relación de SnapMirror	Error
Replicación síncrona fuera de sincronización *(syncSnapmirrorRelationship shipOutofsync)	Riesgo	Relación de SnapMirror	Advertencia
Replicación síncrona restaurada *(syncSnapmirrorRelationshipInSync)	Evento	Relación de SnapMirror	Información
Error en la resincronización automática de replicación síncrona *(syncSnapmirrorRelationshipAutoSyncRetryFailed)	Riesgo	Relación de SnapMirror	Error
ONTAP Mediator se añade al cluster (snapmirrorMediator)	Evento	Clúster	Información
Mediador ONTAP se quita del clúster (snapmirrorMediatorRemoved)	Evento	Clúster	Información

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
No se puede acceder al Mediador ONTAP desde el clúster (snapmirrorMediatorUnable)	Riesgo	Mediador	Advertencia
No se puede acceder al Mediador ONTAP desde el clúster (snapmirrorMediatorMisconfigured)	Riesgo	Mediador	Error
Se ha restablecido la conectividad de Mediator de ONTAP, y está preparado para SMBC (snapmirrorMediatorInQuorum)	Evento	Mediador	Información

Eventos de relaciones de reflejo asíncrono y almacén

Los eventos de relaciones de mirroring y almacén asíncronos le proporcionan información sobre el estado de las relaciones de SnapMirror y almacén asíncronas para poder realizar una supervisión de posibles problemas. Los eventos de relación de reflejo asíncrono y almacén se admiten tanto para las relaciones de protección de máquinas virtuales de almacenamiento como de volúmenes. Pero solo no se admiten las relaciones de almacén para la recuperación ante desastres de la máquina virtual de almacenamiento. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Zona de impacto: Protección

Los eventos de relaciones de SnapMirror y almacén también se generan para equipos virtuales de almacenamiento protegidos mediante la recuperación ante desastres de Storage VM pero no para las relaciones de objetos constituyentes.

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Reflejo asíncrono y almacén en mal estado(ocumEvtMirrorRelationship relación depósito Unheavy)	Riesgo	Relación de SnapMirror	Advertencia

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Reflejo asíncrono y almacén roto-off (ocumEvtMirrorRelationship ationshipStateBrokenoff)	Riesgo	Relación de SnapMirror	Error
Error en el reflejo asíncrono y la inicialización del almacén (error de ocumEvtMirrorRelationship InitializeFailed)	Riesgo	Relación de SnapMirror	Error
Error en la actualización de reflejo asíncrono y almacén (ocumEvtMirrorRelationship UpdateFailed)	Riesgo	Relación de SnapMirror	Error
Error de desfase de reflejo asíncrono y almacén (ocumEvtMirrorRelationship shipLagError)	Riesgo	Relación de SnapMirror	Error
Advertencia de desfase de reflejo asíncrono y almacén (ocumEvtMirrorRelationship relación shipLagWarning)	Riesgo	Relación de SnapMirror	Advertencia
Error en la resincronización de reflejo asíncrono y almacén (ocumEvtMirrorRelationshipResyncFailed)	Riesgo	Relación de SnapMirror	Error

El evento "fallo de actualización de SnapMirror" se produce en el portal de Active IQ (Config Advisor).

Eventos Snapshot

Los eventos Snapshot ofrecen información sobre el estado de las copias Snapshot, lo que permite supervisar las copias Snapshot para detectar posibles problemas. Los eventos se agrupan por área de impacto, e incluyen el nombre del evento, el nombre de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Eliminación automática de Snapshot deshabilitada (no aplicable)	Evento	Volumen	Información
Eliminación automática de copias Snapshot habilitada (no aplicable)	Evento	Volumen	Información
Configuración de eliminación automática de copias Snapshot modificada (no aplicable)	Evento	Volumen	Información

Eventos de relaciones con SnapVault

Los eventos de relaciones con SnapVault le proporcionan información sobre el estado de sus relaciones de SnapVault para poder supervisar posibles problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Zona de impacto: Protección

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Vault asíncrono insalubre(ocumEvtSnapVaultationshipUnheaded)	Riesgo	Relación de SnapMirror	Advertencia
Vault Broken-off asíncrono(ocumEvtSnapRelationshipStateBrokenoff)	Riesgo	Relación de SnapMirror	Error
Error al inicializar el almacén asíncrono (error de ocumEvtSnapVaultRelationship InitializeFailed)	Riesgo	Relación de SnapMirror	Error
Error en la actualización asíncrona del almacén (ocumEvtSnapVaultRelationship UpdateFailed)	Riesgo	Relación de SnapMirror	Error

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Error de desfase en el almacén asíncrono (ocumEvtSnapVaultRelationship shipLagError)	Riesgo	Relación de SnapMirror	Error
Advertencia de desfase en el almacén asíncrono (ocumEvtSnapVaultRelationship shipLagWarning)	Riesgo	Relación de SnapMirror	Advertencia
Error en la resincronización de Vault asíncrona (ocumEvtSnapvaultRelationshipResyncFailed)	Riesgo	Relación de SnapMirror	Error

Eventos de configuración de conmutación por error de almacenamiento

Los eventos de configuración de conmutación por error del almacenamiento (SFO) le proporcionan información acerca de si su recuperación tras fallos del almacenamiento está deshabilitada o no configurada para que pueda supervisar si existen problemas potenciales. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Interconexión de recuperación tras fallos de almacenamiento uno o varios enlaces hacia abajo (ocumEvtSfoInterconnectOneOrMoreLinksDown)	Riesgo	Nodo	Advertencia
Conmutación por error de almacenamiento desactivada (ocumEvtSfoSettingsDisabled).	Riesgo	Nodo	Error
Conmutación por error de almacenamiento no configurada(ocumEvtSfoSettingsNotConfigred)	Riesgo	Nodo	Error

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Estado de conmutación por error del almacenamiento: Toma de control (ocumEvtSfoStateTakeover)	Riesgo	Nodo	Advertencia
Estado de conmutación por error de almacenamiento - devolución parcial (ocumEvtSfoStatePartialGiveback)	Riesgo	Nodo	Error
Estado inactivo del nodo de conmutación por error del almacenamiento (ocumEvtSfoNodeStatusDown)	Riesgo	Nodo	Error
No es posible la toma de control de conmutación por error del almacenamiento (ocumEvtSfoOverTakeoNotPossible)	Riesgo	Nodo	Error

Eventos de servicios de almacenamiento

Los eventos de servicios de almacenamiento le proporcionan información sobre la creación y suscripción de servicios de almacenamiento para poder realizar una supervisión de posibles problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Configuración

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Servicio de almacenamiento creado (no aplicable)	Evento	Servicio de almacenamiento	Información
Servicio de almacenamiento suscrito(no aplicable)	Evento	Servicio de almacenamiento	Información

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Suscripción al servicio de almacenamiento (no aplicable)	Evento	Servicio de almacenamiento	Información

Zona de impacto: Protección

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Eliminación inesperada de Managed SnapMirror RelationshipocumEvtStorageServiceUnsupportedRelationshipDeletion	Riesgo	Servicio de almacenamiento	Advertencia
Eliminación inesperada del volumen miembro del servicio de almacenamiento (ocumEvtStorageServiceUnexpectedVolumeDeletion)	Incidente	Servicio de almacenamiento	Crítico

Eventos de la bandeja de almacenamiento

Los eventos de la bandeja de almacenamiento le indican si su bandeja de almacenamiento presenta anomalías de forma que pueda supervisar posibles problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Rango de tensión anormal (ocumEvtShelfVoltageAbnormal)	Riesgo	Bandeja de almacenamiento	Advertencia
Rango de corriente anormal (ocumEvtSheltrosABnormal)	Riesgo	Bandeja de almacenamiento	Advertencia

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Temperatura anormal (ocumEvtShelTemperatureAbnormal)	Riesgo	Bandeja de almacenamiento	Advertencia

Eventos de máquinas virtuales de almacenamiento

Los eventos de máquina virtual de almacenamiento (también conocidos como SVM) le proporcionan información sobre el estado de sus máquinas virtuales de almacenamiento (SVM) para poder supervisar posibles problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Un asterisco (*) identifica los eventos de EMS que se han convertido a eventos de Unified Manager.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Service Down de SVM (ocumEvtVserverCifsServiceStatusDown)	Incidente	SVM	Crítico
Servicio CIFS SVM no configurado (no aplicable)	Evento	SVM	Información
Intentos de conectar recursos compartidos CIFS no existentes *(nbladeCifsNoPrivShare)	Incidente	SVM	Crítico
Conflicto de nombres NetBIOS CIFS *(nbladeCifsNbNameConflict)	Riesgo	SVM	Error
Error en la operación de copia de volúmenes redundantes de CIFS *(cifsShadowCopyFailure)	Riesgo	SVM	Error
Muchas conexiones CIFS *(nbladeCifsManyAuths)	Riesgo	SVM	Error

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se superó la conexión CIFS máxima *(nbladeCifsMaxOpenSametime)	Riesgo	SVM	Error
Se ha superado el máximo número de conexiones CIFS por usuario *(nbladeCiffsMaxSessPerUsrConn)	Riesgo	SVM	Error
Servicio FC/FCoE de SVM inactivo (ocumEvtVserverFcServiceStatusDown)	Incidente	SVM	Crítico
Servicio iSCSI de SVM inactivo (ocumEvtVserverIscsiServiceStatusDown)	Incidente	SVM	Crítico
Servicio NFS de SVM inactivo (ocumEvtVserverNfsServiceStatusDown)	Incidente	SVM	Crítico
Servicio SVM FC/FCoE no configurado (no aplicable)	Evento	SVM	Información
Servicio iSCSI de SVM no configurado (no aplicable)	Evento	SVM	Información
Servicio SVM NFS no configurado (no aplicable)	Evento	SVM	Información
SVM detenido (ocumEvtVserverDown)	Riesgo	SVM	Advertencia
El servidor AV está demasiado ocupado como para aceptar una nueva solicitud de análisis *(nbladeVscanConnBackPressure)	Riesgo	SVM	Error

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
No hay conexión de servidor AV para virus Scan *(nbladebvscanNoScannerConn)	Incidente	SVM	Crítico
No hay ningún servidor AV registrado *(nbladeVscanNoRegdScanner)	Riesgo	SVM	Error
Conexión de servidor AV * sin respuesta (nbladeVscanConnInactive)	Evento	SVM	Información
Intento de usuario no autorizado de AV Server *(nbladeVscanBadUserPrivAccess)	Riesgo	SVM	Error
Virus encontrado por AV Server *(nbladeVscanVirusDetected)	Riesgo	SVM	Error

Área de impacto: Configuración

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
SVM detectada (no aplicable)	Evento	SVM	Información
SVM eliminada (no aplicable)	Evento	Clúster	Información
SVM cuyo nombre ha cambiado (no corresponde)	Evento	SVM	Información

Área de impacto: Rendimiento

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se superó el umbral crítico de IOPS de SVM (ocumSvmIopsIncident)	Incidente	SVM	Crítico
Se superó el umbral de advertencia de IOPS de SVM (ocumSvmIopsWarning)	Riesgo	SVM	Advertencia
Se ha incumplido el umbral crítico de SVM MB/s (ocumSvmMbpsIncident)	Incidente	SVM	Crítico
Se ha incumplido el umbral de advertencia de SVM MB/s (ocumSvmMbpsWarning)	Riesgo	SVM	Advertencia
Se superó el umbral crucial de latencia de SVM (ocumSvmLatencyIncident)	Incidente	SVM	Crítico
Se superó el umbral de advertencia de latencia de SVM (ocumSvmLatencyWarning)	Riesgo	SVM	Advertencia

Área de impacto: Seguridad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Registro de auditoría desactivado (ocumVserverAuditLogdeshabilitado)	Riesgo	SVM	Advertencia
Banner de inicio de sesión deshabilitado (ocumVserverLoginBannerDisabled)	Riesgo	SVM	Advertencia

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
SSH está utilizando Ciphers no seguros(ocumVserverSSHInsecure)	Riesgo	SVM	Advertencia
Banner de inicio de sesión cambiado (ocumVserverLoginBannerChanged)	Riesgo	SVM	Advertencia
La supervisión antiransomware de la máquina virtual de almacenamiento está deshabilitada (antireomwareSvmStateDisabled).	Riesgo	SVM	Advertencia
La supervisión antiransomware de la máquina virtual de almacenamiento está habilitada (modo de aprendizaje) (antiRansomwareSvmStateDryrun)	Evento	SVM	Información
Storage VM es adecuado para la supervisión antiransomware (modo de aprendizaje) (ocumEvtSvmArwCandidate)	Evento	SVM	Información

Eventos de cuota de usuarios y grupos

Los eventos de cuota de usuario y grupo le proporcionan información acerca de la capacidad de la cuota de usuario y grupo de usuarios, así como los límites de archivos y discos para poder supervisar posibles problemas. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Capacidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Límite de software de espacio en disco de cuota de usuario o de grupo incumplido(ocumEvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	Riesgo	Cuota de usuario o de grupo	Advertencia
Se ha alcanzado el límite duro de espacio en disco de cuota de usuario o de grupo (ocumEvtUserOrGroupQuotaDiskSpaceHardLimitReached)	Incidente	Cuota de usuario o de grupo	Crítico
Límite de software de recuento de archivos de cuota de usuario o de grupo incumplido(ocumEvtUserOrGroupQuotaFileCountSoftLimitBreached)	Riesgo	Cuota de usuario o de grupo	Advertencia
Se ha alcanzado el límite duro de recuento de archivos de cuota de usuario o de grupo (ocumEvtUserOrGroupQuotaFileCountHardLimitReached)	Incidente	Cuota de usuario o de grupo	Crítico

Eventos de volumen

Los eventos de volumen ofrecen información sobre el estado de los volúmenes que permite supervisar si existen problemas potenciales. Los eventos se agrupan por área de impacto, e incluyen el nombre del evento, el nombre de captura, el nivel de impacto, el tipo de origen y la gravedad.

Un asterisco (*) identifica los eventos de EMS que se han convertido a eventos de Unified Manager.

Área de impacto: Disponibilidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Volumen restringido (ocumEvtVolumeRestricted)	Riesgo	Volumen	Advertencia
Volumen sin conexión (ocumEvtVolumeoffline)	Incidente	Volumen	Crítico
Volumen parcialmente disponible(ocumEvtVolumePartiallyAvailable)	Riesgo	Volumen	Error
Volumen desmontado (no aplicable)	Evento	Volumen	Información
Volumen montado (no aplicable)	Evento	Volumen	Información
Volumen remontado (no aplicable)	Evento	Volumen	Información
Ruta de unión de volumen inactiva (ocumEvtVolumeJunctionPathInactive)	Riesgo	Volumen	Advertencia
Tamaño automático de volumen habilitado (no aplicable)	Evento	Volumen	Información
Tamaño automático del volumen - deshabilitado (no aplicable)	Evento	Volumen	Información
Capacidad máxima modificada de tamaño automático de los volúmenes (no aplicable)	Evento	Volumen	Información
Tamaño de incremento de tamaño automático del volumen modificado (no aplicable)	Evento	Volumen	Información

Área de impacto: Capacidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Espacio de volumen en riesgo aprovisionado por thin-provisioning (ocumThinProvisionVolumeSpaceAtRisco)	Riesgo	Volumen	Advertencia
Espacio de volumen completo (ocumEvtVolumeFull)	Riesgo	Volumen	Error
Espacio del volumen casi completo (ocumEvtVolumeNearlyFull)	Riesgo	Volumen	Advertencia
Espacio lógico de volumen completo *(volumeLogicalSpaceFull)	Riesgo	Volumen	Error
Espacio lógico de volumen casi completo *(volumeLogicalSpaceNearlyFull)	Riesgo	Volumen	Advertencia
Espacio lógico de volumen normal *(volumeLogicalSpaceAllOK)	Evento	Volumen	Información
Espacio completo de la reserva de copias Snapshot para volúmenes (ocumEvtSnapshotFull)	Riesgo	Volumen	Advertencia
Hay demasiadas copias Snapshot (ocumEvtSnapshotTooMany)	Riesgo	Volumen	Error
Exceso de cuota de Volume Qtree (ocumEvtVolumeQtreeQuotaOvercomprometidos)	Riesgo	Volumen	Error

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
La cuota de qtree del volumen casi está comprometida en exceso (ocumEvtVolumeQtreeQuotaAlmostOvercomprometidos)	Riesgo	Volumen	Advertencia
Tasa de crecimiento del volumen anormal (ocumEvtVolumeGrowthRateAbnormal)	Riesgo	Volumen	Advertencia
Días de volumen hasta completo (ocumEvtVolumeDaysUntilFullSoon)	Riesgo	Volumen	Error
Garantía de espacio de volumen deshabilitada (no aplicable)	Evento	Volumen	Información
Garantía de espacio de volumen activada (no aplicable)	Evento	Volumen	Información
Garantía de espacio de volumen modificada (no aplicable)	Evento	Volumen	Información
Copias Snapshot de volumen días de reserva hasta Full(ocumEvtVolumeSnapshotReserveDaysUntilFullSoon)	Riesgo	Volumen	Error
Los componentes de FlexGroup tienen problemas de espacio * (flexGroupConstituentsHaveSpaceIssues)	Riesgo	Volumen	Error
Estado del espacio de los componentes de FlexGroup todo OK * (flexGroupConstituentsSpaceStatusAllOK)	Evento	Volumen	Información

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Los componentes de FlexGroup tienen problemas de inodos *(flexGroupConstituentsHaveInodesIssues)	Riesgo	Volumen	Error
Componentes FlexGroup inodos Estado todo OK * (flexGroupConstituentsInodesStatusAllOK)	Evento	Volumen	Información
Error de AutoSize de volumen WAFL *(waflVolAutoSizeFail)	Riesgo	Volumen	Error
Ajuste de tamaño automático de volúmenes de WAFL terminado * (waflVolAutoSizeone)	Evento	Volumen	Información
El volumen de FlexGroup es superior al 80% utilizado*	Incidente	Volumen	Error
El volumen de FlexGroup es superior al 90% utilizado*	Incidente	Volumen	Crítico
Anomalía en la eficiencia del almacenamiento de volúmenes (ocumVolumeAbnormalStorageEfficiencyWarning)	Riesgo	Volumen	Advertencia
Reserva de instantáneas de volumen infrautilizada (volumeSnaphotReserveUnderutilizedWarning)	Evento	Volumen	Advertencia
Reserva de instantáneas de volumen infrautilizada (volumeSnaphotReserveUnderutilizedClean)	Evento	Volumen	Advertencia

Área de impacto: Configuración

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Volumen cambiado de nombre (no aplicable)	Evento	Volumen	Información
Volumen detectado (no aplicable)	Evento	Volumen	Información
Volumen eliminado (no aplicable)	Evento	Volumen	Información

Área de impacto: Rendimiento

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se superó el umbral de advertencia de IOPS máx. De volumen de calidad de servicio (ocumQosVolumeMaxIopsWarning)	Riesgo	Volumen	Advertencia
Se ha incumplido el umbral de advertencia máximo de MB/s de volumen de QoS (ocumQosVolumeMaxMbpsWarning)	Riesgo	Volumen	Advertencia
Se superó el umbral de advertencia de valor máximo de IOPS/TB de volumen de calidad de servicio (ocumQosVolumeMaxIopsPerTbWarning).	Riesgo	Volumen	Advertencia
Se incumplido el umbral de latencia del volumen de carga de trabajo según se define por la política de nivel de servicio de rendimiento (ocumConforceLatencyWarning)	Riesgo	Volumen	Advertencia

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se superó el umbral crítico de IOPS de volumen (incidente de ocumVolumeIopsIncident) .	Incidente	Volumen	Crítico
Se superó el umbral de advertencia de IOPS de volumen (ocumVolumeIopsWarning).	Riesgo	Volumen	Advertencia
Umbral crítico de volumen MB/s incumplido(ocumVolumeMbpsIncident)	Incidente	Volumen	Crítico
Umbral de advertencia de volumen MB/s incumplido(ocumVolumeMbpsWarning)	Riesgo	Volumen	Advertencia
Se ha incumplido el umbral crítico de latencia de volumen ms/op (ocumVolumeLatencyIncident).	Incidente	Volumen	Crítico
Umbral de advertencia de latencia de volumen ms/op incumplido (ocumVolumeLatencyWarning)	Riesgo	Volumen	Advertencia
Se ha incumplido el umbral crítico de la relación de Srta. de caché de volumen (ocumVolumeCacheMissRatioIncident)	Incidente	Volumen	Crítico
Umbral de advertencia de relación de falta de caché de volumen incumplido (ocumVolumeCacheMissRatioWarning)	Riesgo	Volumen	Advertencia

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se incumplido el umbral crítico de latencia de los volúmenes y IOPS (ocumVolumeLatencyIops Incident).	Incidente	Volumen	Crítico
Se insuperó el umbral de advertencia de latencia de volúmenes y IOPS (ocumVolumeLatencyIops Warning)	Riesgo	Volumen	Advertencia
Se incumplido el umbral crítico de latencia de los volúmenes y MB/s(ocumVolumeLatencyMbpsIncident)	Incidente	Volumen	Crítico
Se ha incumplido el umbral de advertencia de latencia de volumen y MB/s (ocumVolumeLatencyMbpsWarning)	Riesgo	Volumen	Advertencia
Latencia de volumen y capacidad de rendimiento del agregado utilizada umbral crítico incumplido (ocumVolumeLatencyAggregate PerfCapacidad UsedIncident)	Incidente	Volumen	Crítico
Latencia de volumen y capacidad de rendimiento agregado utilizada umbral de advertencia incumplido (ocumVolumeLatencyAggregate PerfCapacidad UsedWarning)	Riesgo	Volumen	Advertencia
Se ha incumplido el umbral crítico de latencia de volumen y utilización del agregado (ocumVolumeLatencyAggregate adición de utilidades)	Incidente	Volumen	Crítico

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se ha incumplido el umbral de advertencia de latencia del volumen y utilización del agregado (ocumVolumeLatencyaggregationUtilationWarning)	Riesgo	Volumen	Advertencia
Latencia de volumen y capacidad de rendimiento de nodos utilizada umbral crítico incumplido (ocumVolumeLatencyNodePerfCapacidadUsedIncident)	Incidente	Volumen	Crítico
Latencia de volumen y capacidad de rendimiento de nodos utilizada umbral de advertencia incumplido (ocumVolumeLatencyNodePerfCapacidadUsedWarning)	Riesgo	Volumen	Advertencia
Latencia de volúmenes y capacidad de rendimiento de nodos utilizados: Se superó el umbral crucial de la toma de control (ocumVolumeLatencyAggregate PerfCapityUsedTakeOverIncident)	Incidente	Volumen	Crítico
Latencia de volúmenes y capacidad de rendimiento de nodos utilizados: Se superó el umbral de advertencia de toma de control (ocumVolumeLatencyAggregate PerfCapityUsedTakeOverWarning)	Riesgo	Volumen	Advertencia

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Se superó el umbral crítico de latencia de volúmenes y uso de nodos (ocumVolumeLatencyNodeUtilationIncident)	Incidente	Volumen	Crítico
Umbral de advertencia de latencia de volumen y utilización de nodos incumplido (ocumVolumeLatencyNodeUtilationWarning)	Riesgo	Volumen	Advertencia

Área de impacto: Seguridad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
La supervisión del volumen contra ransomware está habilitada (modo activo) (antiRansomwareVolumeStateEnabled).	Evento	Volumen	Información
La supervisión del volumen antiransomware está deshabilitada (antiRansomwareVolumeStateDisabled).	Riesgo	Volumen	Advertencia
La supervisión del volumen antiransomware está habilitada (modo de aprendizaje) (antiRansomwareVolumeStateDryrun)	Evento	Volumen	Información
La supervisión del volumen antiransomware se detiene (modo de aprendizaje) (antiRansomwareVolumeStateDryrunPaused)	Riesgo	Volumen	Advertencia

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
La supervisión del volumen antiransomware se detiene (modo activo) (antiRansomwareVolumeStateEnablePaused)	Riesgo	Volumen	Advertencia
La supervisión del volumen antiransomware se está desactivando (antiRansomwareVolumeStateDisableInProgress).	Riesgo	Volumen	Advertencia
Actividad de ransomware vista (callHomeRansowareActivitySeen)	Incidente	Volumen	Crítico
Volumen adecuado para la supervisión antiransomware (modo de aprendizaje) (ocumEvtVolumeArwCandidate)	Evento	Volumen	Información
Volumen adecuado para la monitorización antiransomware (modo activo) (ocumVolumeSuitedForActiveAntiRansomwareDetection)	Riesgo	Volumen	Advertencia
El volumen muestra alertas ruidosas contra el ransomware (antiRansowarFeatureNoisyVolume)	Riesgo	Volumen	Advertencia

Área de impacto: Protección de datos

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
El volumen tiene insuficiente protección local Snapshot (volumeLacksLocalProtectionWarning)	Riesgo	Volumen	Advertencia
El volumen tiene insuficiente protección local de Snapshot (volumeLacksLocalProtectionCleed)	Riesgo	Volumen	Advertencia

Eventos de estado del movimiento de volúmenes

Los eventos de estado del movimiento de volúmenes le indican acerca del estado del movimiento de volúmenes para poder supervisar si existen problemas potenciales. Los eventos se agrupan por área de impacto e incluyen el nombre del evento y de captura, el nivel de impacto, el tipo de origen y la gravedad.

Área de impacto: Capacidad

Nombre del evento (nombre de la captura)	Nivel de impacto	Tipo de origen	Gravedad
Estado del movimiento de volumen: En curso (no aplicable)	Evento	Volumen	Información
Estado de movimiento del volumen - failed (ocumEvtVolumeMoveFailed)	Riesgo	Volumen	Error
Estado del movimiento de volumen: Completado (no aplicable)	Evento	Volumen	Información
Movimiento de volumen - transición diferida (ocumEvtVolumeMoveCutoverDetransferido)	Riesgo	Volumen	Advertencia

Descripción de ventanas de eventos y cuadros de diálogo

Los eventos le notifican cualquier problema de su entorno. Es posible usar la página del inventario Event Management y la página de detalles Event Management para supervisar

todos los eventos. Puede utilizar el cuadro de diálogo Opciones de configuración de notificaciones para configurar la notificación. Se puede usar la página Event Setup para deshabilitar o habilitar eventos.

Notificaciones

Puede configurar Unified Manager Server para que envíe notificaciones cuando se genera un evento o cuando se asigna a un usuario. También puede configurar los mecanismos de notificación. Por ejemplo, las notificaciones se pueden enviar como correos electrónicos o capturas SNMP.

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Correo electrónico

Esta área permite configurar las siguientes opciones de correo electrónico para las notificaciones de alertas:

- **Desde la dirección**

  Especifica la dirección de correo electrónico desde la cual se envía la notificación de alertas. Este valor también se utiliza como dirección de origen de un informe cuando se comparte. Si la dirección de origen se ha rellenado previamente con la dirección "ActiveIQUnifiedManager@localhost.com", debe cambiarla a una dirección de correo electrónico real para asegurarse de que todas las notificaciones de correo electrónico se han entregado correctamente.

Servidor SMTP

Esta área permite configurar los siguientes ajustes del servidor SMTP:

- **Nombre de host o Dirección IP**

  Especifica el nombre de host del servidor de host SMTP, que se utiliza para enviar la notificación de alerta a los destinatarios especificados.

- **Nombre de usuario**

  Especifica el nombre de usuario SMTP. El nombre de usuario SMTP sólo es necesario cuando SMTPAUTH está habilitado en el servidor SMTP.

- **Contraseña**

  Especifica la contraseña SMTP. El nombre de usuario SMTP sólo es necesario cuando SMTPAUTH está habilitado en el servidor SMTP.

- **Puerto**

  Especifica el puerto que utiliza el servidor de host SMTP para enviar notificaciones de alerta.

  El valor predeterminado es 25.

- **Use START/TLS**

  Al activar esta casilla se proporciona una comunicación segura entre el servidor SMTP y el servidor de administración mediante los protocolos TLS/SSL (también conocidos como start_tls y StartTLS).

- **Use SSL**

  Si activa esta casilla, se proporciona una comunicación segura entre el servidor SMTP y el servidor de administración mediante el protocolo SSL.

SNMP

Esta área permite configurar las siguientes opciones de captura SNMP:

- **Versión**

  Especifica la versión de SNMP que desea utilizar en función del tipo de seguridad que necesite. Las opciones incluyen la versión 1, la versión 3, la versión 3 con autenticación y la versión 3 con autenticación y cifrado. El valor predeterminado es Versión 1.

- **Host de destino de captura**

  Especifica el nombre de host o la dirección IP (IPv4 o IPv6) que recibe las capturas SNMP que envía el servidor de gestión. Para especificar varios destinos de capturas, separe cada host con una coma.

  > Todas las demás configuraciones de SNMP, como "Versión" y "Puerto saliente", deben ser las mismas para todos los hosts de la lista.

- **Puerto de captura de salida**

  Especifica el puerto a través del cual el servidor SNMP recibe las capturas que envía el servidor de administración.

  El valor predeterminado es 162.

- **Comunidad**

  La cadena de comunidad para acceder al host.

- **ID del motor**

  Especifica el identificador único del agente SNMP y el servidor de administración lo genera automáticamente. El Id. Del motor está disponible con SNMP versión 3, SNMP versión 3 con autenticación y SNMP versión 3 con autenticación y cifrado.

- **Nombre de usuario**

  Especifica el nombre de usuario SNMP. El nombre de usuario está disponible con SNMP versión 3, SNMP versión 3 con autenticación y SNMP versión 3 con autenticación y cifrado.

- **Protocolo de autenticación**

  Especifica el protocolo utilizado para autenticar un usuario. Las opciones de protocolo incluyen MD5 y SHA. MD5 es el valor predeterminado. El protocolo de autenticación está disponible en SNMP Versión 3 con autenticación y SNMP Versión 3 con autenticación y cifrado.

- **Contraseña de autenticación**

  Especifica la contraseña utilizada al autenticar un usuario. La contraseña de autenticación está disponible en SNMP Versión 3 con autenticación y SNMP Versión 3 con autenticación y cifrado.

- **Protocolo de Privacidad**

  Especifica el protocolo de privacidad utilizado para cifrar mensajes SNMP. Las opciones de protocolo incluyen AES 128 y DES. El valor predeterminado es AES 128. El protocolo de privacidad está disponible en SNMP Versión 3 con autenticación y cifrado.

- **Contraseña de privacidad**

  Especifica la contraseña cuando se utiliza el protocolo de privacidad. La contraseña de privacidad está disponible en SNMP Versión 3 con autenticación y cifrado.

Para obtener más información acerca de los objetos y capturas SNMP, puede descargar la "MIB de Active IQ Unified Manager" En el sitio de soporte de NetApp.

Página del inventario Event Management

La página de inventario Gestión de eventos permite ver una lista de los eventos actuales y sus propiedades. Puede realizar tareas como reconocer, resolver y asignar eventos. También puede añadir una alerta para eventos específicos.

La información de esta página se actualiza automáticamente cada 5 minutos para garantizar que se muestren los eventos nuevos más recientes.

Componentes del filtro

Le permite personalizar la información que aparece en la lista de eventos. Puede refinar la lista de eventos que se muestran utilizando los siguientes componentes:

- Menú Ver para seleccionar una lista predefinida de selecciones de filtro.

  Esto incluye elementos como todos los eventos activos (nuevos y reconocidos), eventos de rendimiento activos, eventos asignados a mí (el usuario que ha iniciado sesión) y todos los eventos generados durante todas las ventanas de mantenimiento.

- Panel de búsqueda para refinar la lista de eventos introduciendo términos completos o parciales.
- Botón filtro que inicia el panel Filtros para poder seleccionar de todos los atributos de campo y campo disponibles para afinar la lista de eventos.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Asignar a**

  Permite seleccionar el usuario al que se asigna el evento. Al asignar un evento a un usuario, el nombre de usuario y la hora a la que asignó el evento se agregan a la lista de eventos para los eventos seleccionados.

  - Yo

    Asigna el evento al usuario que ha iniciado sesión actualmente.

  - Otro usuario

Muestra el cuadro de diálogo asignar propietario, que permite asignar o reasignar el evento a otros usuarios. También puede anular la asignación de eventos si deja en blanco el campo de propiedad.

- **Acuse de recibo**

  Confirma los eventos seleccionados.

  Al reconocer un evento, el nombre de usuario y la hora a la que reconoció el evento se agregan a la lista de eventos para los eventos seleccionados. Cuando reconoce un evento, es responsable de gestionarlo.

  No puede reconocer eventos de información.

- **Marcar como solucionado**

  Permite cambiar el estado del evento a Resolved.

  Al resolver un evento, el nombre de usuario y la hora a la que resolvió el evento se agregan a la lista de eventos para los eventos seleccionados. Después de realizar una acción correctiva para el evento, debe marcar el evento como resuelto.

- **Agregar alerta**

  Muestra el cuadro de diálogo Agregar alerta, que le permite agregar alertas para los eventos seleccionados.

- **Informes**

  Permite exportar detalles de la vista de eventos actual a un archivo de valores separados por comas (.csv) o un documento PDF.

- **Mostrar/Ocultar selector de columna**

  Permite elegir las columnas que se muestran en la página y seleccionar el orden en el que se muestran.

Lista Events

Muestra detalles de todos los eventos ordenados por tiempo activado.

De forma predeterminada, se muestra la vista todos los eventos activos para mostrar los eventos nuevos y confirmados de los siete días anteriores que tienen un nivel de impacto de incidente o riesgo.

- **Tiempo activado**

  Hora en la que se generó el evento.

- **Gravedad**

  La gravedad del evento: Crítico ( ), error ( ), Advertencia ( ), e Información ( ).

- **Estado**

  Estado del evento: Nuevo, reconocido, resuelto u Obsoleto.

- **Nivel de impacto**

El nivel de impacto del evento: Incidente, riesgo, evento o actualización.

- * Área de impacto*

  El área de impacto de eventos: Disponibilidad, capacidad, rendimiento, protección, configuración, O Seguridad.

- **Nombre**

  Nombre del evento. Puede seleccionar el nombre para mostrar la página de detalles Event para ese evento.

- **Fuente**

  Nombre del objeto en el que se ha producido el evento. Puede seleccionar el nombre para mostrar la página de detalles Health o Performance de ese objeto.

  Cuando se produce una filtración de política de calidad de servicio compartida, solo se muestra en este campo el objeto de carga de trabajo que consume la mayor cantidad de IOPS o MB/s. Las cargas de trabajo adicionales que utilizan esta política se muestran en la página de detalles Event.

- **Tipo de fuente**

  El tipo de objeto (por ejemplo, Storage VM, Volume o Qtree) con el que está asociado el evento.

- **Asignado a**

  Nombre del usuario al que se asigna el evento.

- **Origen del evento**

  Tanto si el evento se originó a partir del "Portal de Active IQ" como directamente desde "Active IQ Unified Manager".

- **Nombre de anotación**

  Nombre de la anotación que se asigna al objeto de almacenamiento.

- **Notas**

  El número de notas que se agregan para un evento.

- **Días pendientes**

  El número de días desde que se generó inicialmente el evento.

- **Tiempo asignado**

  El tiempo transcurrido desde que se asignó el evento a un usuario. Si el tiempo transcurrido supera una semana, se muestra la Marca de tiempo cuando se asignó el evento a un usuario.

- **Reconocido por**

  Nombre del usuario que ha reconocido el evento. El campo está en blanco si el evento no se reconoce.

- **Tiempo reconocido**

El tiempo transcurrido desde que se reconoció el evento. Si el tiempo transcurrido supera una semana, se muestra la Marca de tiempo cuando se reconoció el evento.

- **Resuelto por**

  Nombre del usuario que resolvió el evento. El campo está en blanco si el evento no se resuelve.

- **Tiempo resuelto**

  El tiempo transcurrido desde que se resolvió el evento. Si el tiempo transcurrido supera una semana, se muestra la Marca de tiempo cuando se resolvió el evento.

- **Tiempo Obsoletado**

  Hora a la que el estado del evento se convirtió en Obsoleto.

Página de detalles Event

En la página de detalles Event, puede ver los detalles de un evento seleccionado, como la gravedad del evento, el nivel de impacto, el área de impacto y el origen del evento. También puede ver información adicional sobre posibles soluciones para resolver el problema.

- **Nombre del evento**

  El nombre del evento y la hora en que se vio el evento por última vez.

  Para los eventos que no son de rendimiento, mientras que el evento está en el estado Nuevo o reconocido, la última información vista no es conocida y, por lo tanto, está oculta.

- **Descripción del evento**

  Una breve descripción del evento.

  En algunos casos, en la descripción del evento se proporciona un motivo para el desencadenante.

- **Componente en disputa**

  Para eventos de rendimiento dinámicos, esta sección muestra iconos que representan los componentes lógicos y físicos del clúster. Si un componente es objeto de disputa, su icono está en un círculo y se resalta en rojo.

  Consulte *Cluster Components y por qué pueden estar en disputa* para obtener una descripción de los componentes que se muestran aquí.

Las secciones Información de sucesos, Diagnóstico del sistema y acciones sugeridas se describen en otros temas.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Icono Notas**

Permite agregar o actualizar una nota acerca del evento y revisar todas las notas que dejan otros usuarios.

Menú acciones

- **Asignar a mí**

  Le asigna el evento.

- **Asignar a otros**

  Abre el cuadro de diálogo asignar propietario, que permite asignar o reasignar el evento a otros usuarios.

  Al asignar un evento a un usuario, el nombre del usuario y la hora a la que se asignó el evento se agregan a la lista de eventos para los eventos seleccionados.

  También puede anular la asignación de eventos si deja en blanco el campo de propiedad.

- **Acuse de recibo**

  Confirma los eventos seleccionados para que no continúe recibiendo notificaciones de alerta de repetición.

  Cuando reconoce un evento, el nombre de usuario y la hora a la que ha reconocido el evento se agregan a la lista de eventos (reconocida por) para los eventos seleccionados. Cuando usted reconoce un evento, usted toma la responsabilidad de administrar ese evento.

- **Marcar como solucionado**

  Permite cambiar el estado del evento a Resolved.

  Al resolver un evento, el nombre de usuario y la hora a la que resolvió el evento se agregan a la lista de eventos (resuelto por) para los eventos seleccionados. Después de realizar una acción correctiva para el evento, debe marcar el evento como resuelto.

- **Agregar alerta**

  Muestra el cuadro de diálogo Agregar alerta, que permite agregar una alerta para el evento seleccionado.

Qué se muestra en la sección Información del evento

Utilice la sección Información de eventos de la página de detalles Event para ver los detalles de un evento seleccionado, como la gravedad del evento, el nivel de impacto, el área de impacto y el origen del evento.

Los campos que no se aplican al tipo de evento están ocultos. Puede ver los siguientes detalles del evento:

- **Tiempo de activación del evento**

  Hora en la que se generó el evento.

- **Estado**

  Estado del evento: Nuevo, reconocido, resuelto u Obsoleto.

- **Causa obsoleta**

  Las acciones que causaron que el evento se quede obsoleto, por ejemplo, el problema se solucionó.

- **Duración del evento**

  Para los eventos activos (nuevos y reconocidos), este es el tiempo entre la detección y el momento en que se analizó el evento por última vez. Para los eventos obsoletos, éste es el tiempo entre la detección y el momento en que se resolvió el evento.

  Este campo se muestra para todos los eventos de rendimiento y para otros tipos de eventos sólo después de que se hayan resuelto o se hayan vuelto obsoletos.

- **Última vista**

  La fecha y la hora en que el evento fue visto por última vez como activo.

  Para los eventos de rendimiento, este valor puede ser más reciente que el tiempo de activación de eventos, ya que este campo se actualiza después de cada nueva colección de datos de rendimiento siempre que el evento esté activo. Para otros tipos de eventos, cuando se encuentra en el estado Nuevo o reconocido, este contenido no se actualiza y, por lo tanto, el campo está oculto.

- **Gravedad**

  La gravedad del evento: Crítico ( ), error ( ), Advertencia ( ), e Información ( ).

- **Nivel de impacto**

  El nivel de impacto del evento: Incidente, riesgo, evento o actualización.

- * Área de impacto*

  El área de impacto de eventos: Disponibilidad, capacidad, rendimiento, protección, configuración, O Seguridad.

- **Fuente**

  Nombre del objeto en el que se ha producido el evento.

  Cuando se visualizan los detalles de un evento de política de calidad de servicio compartida, se enumeran en este campo hasta tres de los objetos de carga de trabajo que consumen la mayor cantidad de IOPS o Mbps.

  Puede hacer clic en el enlace de nombre de origen para mostrar la página de detalles de estado o rendimiento de ese objeto.

- **Anotaciones Fuente**

  Muestra el nombre y el valor de la anotación del objeto al que está asociado el evento.

  Este campo solo se muestra para eventos de estado en clústeres, SVM y volúmenes.

- **Grupos de fuentes**

  Muestra los nombres de todos los grupos a los que pertenece el objeto afectado.

Este campo solo se muestra para eventos de estado en clústeres, SVM y volúmenes.

- **Tipo de fuente**

  El tipo de objeto (por ejemplo, SVM, Volume o Qtree) con el que está asociado el evento.

- **En Cluster**

  Nombre del clúster en el que ocurrió el evento.

  Puede hacer clic en el enlace de nombre del clúster para mostrar la página de detalles Health o Performance de ese clúster.

- **Recuento de objetos afectados**

  Número de objetos afectados por el evento.

  Puede hacer clic en el enlace del objeto para ver la página de inventario rellena con los objetos que afecta actualmente a este evento.

  Este campo solo se muestra para eventos de rendimiento.

- **Volúmenes afectados**

  La cantidad de volúmenes que se ven afectados por este evento.

  Este campo solo se muestra para eventos de rendimiento en nodos o agregados.

- **Política activada**

  Nombre de la directiva de umbral que emitió el evento.

  Puede pasar el cursor sobre el nombre de la política para ver los detalles de la política de umbral. Para las políticas de calidad de servicio adaptativas, también se muestra la política definida, el tamaño del bloque y el tipo de asignación (espacio asignado o espacio usado).

  Este campo solo se muestra para eventos de rendimiento.

- **ID de regla**

  Para los eventos de la plataforma Active IQ, éste es el número de la regla que se ha activado para generar el evento.

- **Reconocido por**

  El nombre de la persona que reconoció el evento y la hora en que se reconoció el evento.

- **Resuelto por**

  El nombre de la persona que resolvió el evento y la hora a la que se resolvió el evento.

- **Asignado a**

  El nombre de la persona asignada para trabajar en el evento.

- **Ajustes de alerta**

Se muestra la siguiente información sobre las alertas:

- Si no hay alertas asociadas con el evento seleccionado, aparecerá un enlace **Agregar alerta**.

  Para abrir el cuadro de diálogo Agregar alerta, haga clic en el enlace.

- Si hay una alerta asociada con el evento seleccionado, se muestra el nombre de alerta.

  Para abrir el cuadro de diálogo Editar alerta, haga clic en el enlace.

- Si existe más de una alerta asociada con el evento seleccionado, se muestra el número de alertas.

  Para abrir la página Alert Setup, haga clic en el enlace para ver más detalles sobre estas alertas.

No se muestran las alertas deshabilitadas.

- **Última notificación enviada**

  La fecha y la hora en que se envió la notificación de alerta más reciente.

- **Enviar por**

  El mecanismo que se utilizó para enviar la notificación de alerta: Correo electrónico o captura SNMP.

- **Secuencia de comandos anterior**

  Nombre del script que se ejecutó cuando se generó la alerta.

Aparece la sección acciones recomendadas

La sección acciones sugeridas de la página de detalles evento proporciona posibles motivos para el evento y sugiere algunas acciones para que pueda intentar resolver el evento por su cuenta. Las acciones sugeridas se personalizan en función del tipo de evento o tipo de umbral que se ha incumplido.

Esta área solo se muestra para algunos tipos de eventos.

En algunos casos se proporcionan enlaces de **Ayuda** en la página que hacen referencia a información adicional para muchas acciones sugeridas, incluidas instrucciones para realizar una acción específica. Algunas de estas acciones pueden requerir el uso de Unified Manager, System Manager de ONTAP, OnCommand Workflow Automation, comandos de la CLI de ONTAP o una combinación de estas herramientas.

Debe tener en cuenta las acciones sugeridas aquí como solo una guía para resolver este evento. La acción que se toma para resolver este evento debe basarse en el contexto de su entorno.

Si desea analizar el objeto y el evento con más detalle, haga clic en el botón **analizar carga de trabajo** para mostrar la página Análisis de carga de trabajo.

Hay ciertos eventos que Unified Manager puede diagnosticar a fondo y proporcionar una única resolución. Si están disponibles, estas resoluciones se muestran con un botón **Fix it**. Haga clic en este botón para que Unified Manager solucione el problema que causa el evento.

Para los eventos de plataforma Active IQ, esta sección puede contener un enlace a un artículo de la base de

conocimientos de NetApp, cuando esté disponible, que describe el problema y posibles resoluciones. En los sitios sin acceso a red externa, se abre localmente un PDF del artículo de la base de conocimientos; el PDF forma parte del archivo de reglas que se descarga manualmente en la instancia de Unified Manager.

En qué se muestra la sección Diagnóstico del sistema

La sección Diagnóstico del sistema de la página de detalles del evento proporciona información que puede ayudarle a diagnosticar problemas que pueden haber sido responsables del evento.

Esta área solo se muestra para algunos eventos.

Algunos eventos de rendimiento proporcionan gráficos relevantes para el evento concreto que se ha activado. Normalmente, esto incluye un gráfico IOPS o Mbps y un gráfico de latencia de los diez días anteriores. Cuando se organiza de esta manera, se puede ver qué componentes de almacenamiento afectan en mayor medida a la latencia o se ven afectados por la latencia, cuando el evento está activo.

Para los eventos de rendimiento dinámicos, se muestran los siguientes gráficos:

- Latencia de carga de trabajo: Muestra el historial de latencia de las cargas de trabajo principales de víctimas, abusones o tiburones en el componente en disputa.
- Workload Activity: Se muestran detalles sobre el uso de la carga de trabajo del componente de clúster en disputa.
- Actividad de recursos: Muestra las estadísticas de rendimiento históricas del componente del clúster en disputa.

Los otros gráficos se muestran cuando algunos componentes del clúster son objeto de disputa.

Otros eventos proporcionan una breve descripción del tipo de análisis que realiza el sistema en el objeto de almacenamiento. En algunos casos habrá una o más líneas; una para cada componente que se ha analizado, para las políticas de rendimiento definidas por el sistema que analizan varios contadores de rendimiento. En este caso, aparece un icono verde o rojo junto al diagnóstico para indicar si se ha encontrado o no un problema en ese diagnóstico en particular.

Página Event Setup

En la página Event Setup, se muestra la lista de eventos deshabilitados y se proporciona información como el tipo de objeto asociado y la gravedad del evento. También es posible realizar tareas como deshabilitar o habilitar eventos de forma global.

Sólo puede acceder a esta página si tiene la función Administrador de aplicaciones o Administrador de almacenamiento.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas para los eventos seleccionados:

- **Desactivar**

  Abre el cuadro de diálogo Deshabilitar eventos, que se puede utilizar para deshabilitar eventos.

- **Activar**

Activa los eventos seleccionados que ha elegido desactivar anteriormente.

- **Reglas de carga**

  Inicia el cuadro de diálogo Upload Rules, lo que permite que los sitios sin acceso a red externo suban manualmente el archivo de reglas de Active IQ en Unified Manager. Las reglas se ejecutan en mensajes de Cluster AutoSupport para generar eventos de configuración, cableado, prácticas recomendadas y disponibilidad del sistema, según lo definido por la plataforma Active IQ.

- **Suscríbete a eventos EMS**

  Inicia el cuadro de diálogo Subscribe to EMS Events, que permite suscribirse para recibir eventos específicos del sistema de gestión de eventos (EMS) desde los clústeres que supervisa. EMS recopila información sobre los eventos que se producen en el clúster. Cuando se recibe una notificación para un evento de EMS suscrito, se genera un evento de Unified Manager con la gravedad correspondiente.

Vista de lista

La vista Lista muestra (en formato tabular) información sobre los eventos que están desactivados. Puede utilizar los filtros de columnas para personalizar los datos que se muestran.

- **Evento**

  Muestra el nombre del evento que está desactivado.

- **Gravedad**

  Muestra la gravedad del evento. La gravedad puede ser crítica, error, advertencia o información.

- **Tipo de fuente**

  Muestra el tipo de origen para el que se genera el evento.

Cuadro de diálogo Disable Events

El cuadro de diálogo Deshabilitar eventos muestra la lista de tipos de eventos para los que puede deshabilitar eventos. Puede deshabilitar eventos para un tipo de evento según una gravedad determinada o para un conjunto de eventos.

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Área Event Properties

El área Propiedades de evento especifica las siguientes propiedades de evento:

- **Gravedad del suceso**

  Permite seleccionar eventos según el tipo de gravedad, que puede ser crítico, error, advertencia o Información.

- **Nombre del evento contiene**

  Permite filtrar eventos cuyo nombre contenga los caracteres especificados.

- **Eventos coincidentes**

  Muestra la lista de eventos que coinciden con el tipo de gravedad de evento y la cadena de texto que especifica.

- **Desactivar eventos**

  Muestra la lista de eventos seleccionados para deshabilitar.

  La gravedad del evento también se muestra junto con el nombre del evento.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas para los eventos seleccionados:

- **Guardar y cerrar**

  Deshabilita el tipo de evento y cierra el cuadro de diálogo.

- **Cancelar**

  Descarta los cambios y cierra el cuadro de diálogo.

Gestión de alertas

Es posible configurar alertas para que envíen notificaciones automáticamente cuando se produzcan eventos o eventos específicos de determinados tipos de gravedad. También puede asociar una alerta a un script que se ejecuta cuando se activa una alerta.

¿Qué alertas son

Aunque los eventos se producen de forma continua, Unified Manager genera una alerta solo cuando un evento cumple los criterios de filtro especificados. Puede elegir los eventos para los que se deben generar las alertas; por ejemplo, cuando se supera un umbral de espacio o se desconecta un objeto. También puede asociar una alerta a un script que se ejecuta cuando se activa una alerta.

Entre los criterios de filtro se incluyen la clase de objeto, el nombre o la gravedad del evento.

Qué información se incluye en un correo electrónico de alerta

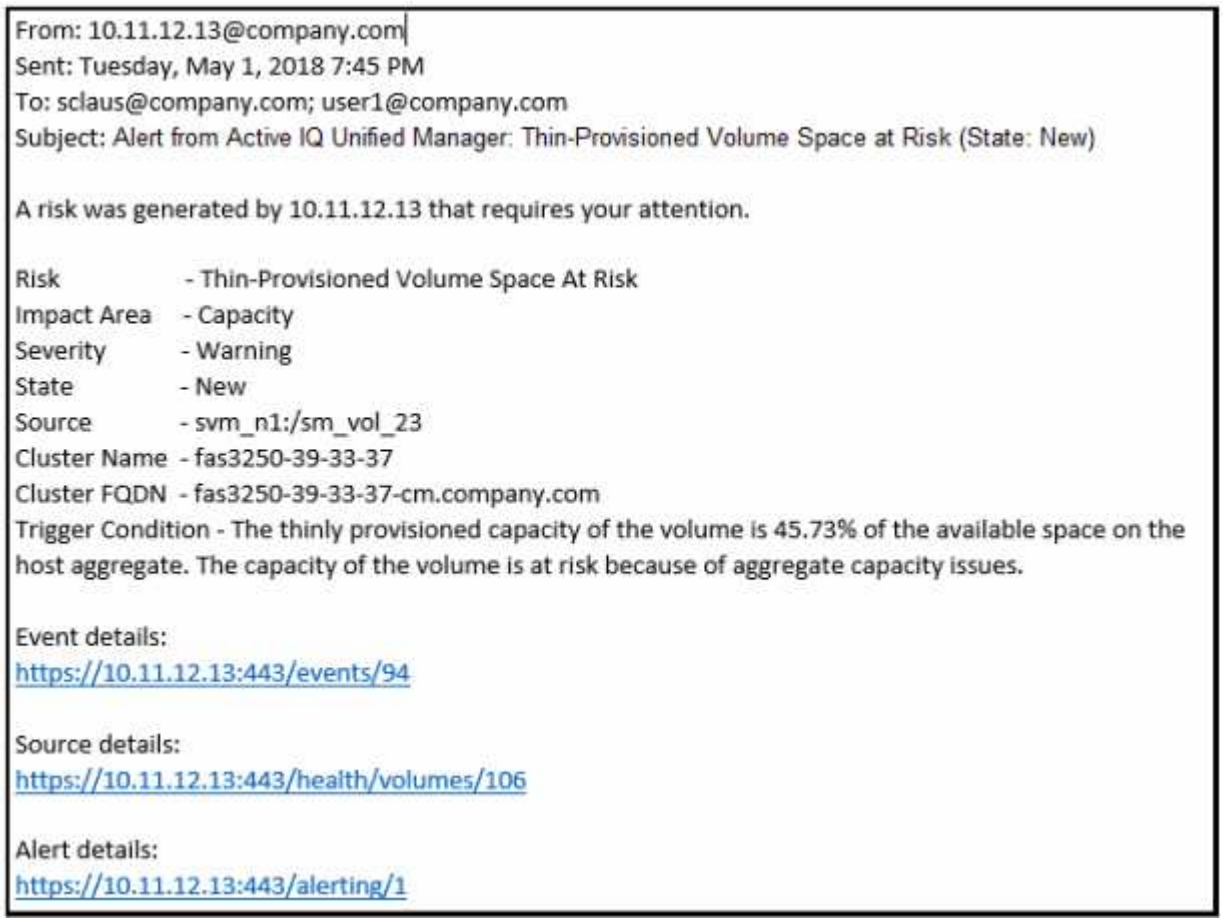
Los mensajes de correo electrónico de alertas de Unified Manager proporcionan el tipo de evento, la gravedad del evento, el nombre de la política o umbral que se violó para provocar el evento y una descripción del evento. El mensaje de correo electrónico también proporciona un hipervínculo a cada evento que le permite ver la página de detalles del evento en la interfaz de usuario de.

Los correos electrónicos de alerta se envían a todos los usuarios que se han suscrito para recibir alertas.

Si un contador de rendimiento o un valor de capacidad tiene un cambio grande durante un período de

recopilación, puede provocar que se active un evento crítico y uno de advertencia al mismo tiempo para la misma política de umbral. En este caso, podrá recibir un correo electrónico para el evento de advertencia y otro para el evento crítico. Esto se debe a que Unified Manager permite suscribirse por separado para recibir alertas de advertencia y incumplimiento de umbrales críticos.

A continuación se muestra un ejemplo de correo electrónico de alerta:


From: 10.11.12.13@company.com
Sent: Tuesday, May 1, 2018 7:45 PM
To: sclaus@company.com; user1@company.com
Subject: Alert from Active IQ Unified Manager: Thin-Provisioned Volume Space at Risk (State: New)

A risk was generated by 10.11.12.13 that requires your attention.

Risk - Thin-Provisioned Volume Space At Risk
Impact Area - Capacity
Severity - Warning
State - New
Source - svm_n1:/sm_vol_23
Cluster Name - fas3250-39-33-37
Cluster FQDN - fas3250-39-33-37-cm.company.com
Trigger Condition - The thinly provisioned capacity of the volume is 45.73% of the available space on the host aggregate. The capacity of the volume is at risk because of aggregate capacity issues.

Event details:
https://10.11.12.13:443/events/94

Source details:
https://10.11.12.13:443/health/volumes/106

Alert details:
https://10.11.12.13:443/alerting/1

Adición de alertas

Puede configurar alertas para que le notifiquen un evento determinado. Es posible configurar alertas para un solo recurso, para un grupo de recursos o para eventos de un tipo de gravedad determinado. Puede especificar la frecuencia con la que desea que se le notifique y asociar un script a la alerta.

Lo que necesitará

- Debe haber configurado los ajustes de notificación, como la dirección de correo electrónico de usuario, el servidor SMTP y el host de captura SNMP, con el fin de permitir que el servidor Active IQ Unified Manager utilice estos ajustes para enviar notificaciones a los usuarios cuando se genera un evento.
- Debe conocer los recursos y los eventos sobre los que desea activar la alerta, así como los nombres de usuario o las direcciones de correo electrónico de los usuarios a los que desea notificar.
- Si desea que un script se ejecute según el evento, debe haber añadido el script a Unified Manager mediante la página Scripts.
- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Puede crear una alerta directamente desde la página de detalles Event después de recibir un evento además de crear una alerta desde la página Alert Setup, tal y como se describe aquí.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de alertas**.
2. En la página **Configuración de alertas**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar alerta**, haga clic en **Nombre** e introduzca un nombre y una descripción para la alerta.
4. Haga clic en **Recursos** y seleccione los recursos que se incluirán o excluirán de la alerta.

   Puede establecer un filtro especificando una cadena de texto en el campo **Nombre contiene** para seleccionar un grupo de recursos. Según la cadena de texto que especifique, la lista de recursos disponibles solo muestra los recursos que coinciden con la regla de filtro. La cadena de texto que especifique distingue mayúsculas y minúsculas.

   Si un recurso cumple las reglas de inclusión y exclusión especificadas, la regla de exclusión tiene prioridad sobre la regla de inclusión y no se genera la alerta para los eventos relacionados con el recurso excluido.

5. Haga clic en **Eventos** y seleccione los eventos según el nombre del evento o el tipo de gravedad del evento para el que desea activar una alerta.

   Para seleccionar más de un evento, pulse la tecla Ctrl mientras realiza las selecciones.

6. Haga clic en **acciones** y seleccione los usuarios a los que desea notificar, elija la frecuencia de notificación, elija si se enviará una captura SNMP al receptor de capturas y asigne una secuencia de comandos para que se ejecute cuando se genere una alerta.

   Si modifica la dirección de correo electrónico especificada para el usuario y vuelve a abrir la alerta para su edición, el campo Nombre aparecerá en blanco porque la dirección de correo electrónico modificada ya no está asignada al usuario que se seleccionó previamente. Además, si modificó la dirección de correo electrónico del usuario seleccionado desde la página usuarios, la dirección de correo electrónico modificada no se actualizará para el usuario seleccionado.

   También puede optar por notificar a los usuarios a través de las capturas SNMP.

7. Haga clic en **Guardar**.

Ejemplo de añadir una alerta

Este ejemplo muestra cómo crear una alerta que cumpla con los siguientes requisitos:

- Nombre de alerta: HealthTest
- Recursos: Incluye todos los volúmenes cuyo nombre contiene "abc" y excluye todos los volúmenes cuyo nombre contiene "xyz".
- Eventos: Incluye todos los eventos críticos de salud
- Acciones: Incluye "sample@domain.com", una secuencia de comandos "Test" y el usuario debe ser notificado cada 15 minutos

Realice los siguientes pasos en el cuadro de diálogo Agregar alerta:

1. Haga clic en **Nombre** e introduzca **`HealthTest`** En el campo **Nombre de alerta**.
2. Haga clic en **Recursos** y, en la ficha incluir, seleccione **volúmenes** en la lista desplegable.
   a. Introduzca **`abc`** En el campo **Nombre contiene** para mostrar los volúmenes cuyo nombre contiene "abc".
   b. Seleccione **<<All Volumes whose name contains 'abc'>>** en el área Recursos disponibles y muévalos al área Recursos seleccionados.
   c. Haga clic en **excluir** e introduzca **`xyz`** En el campo **Nombre contiene** y, a continuación, haga clic en **Agregar**.
3. Haga clic en **Eventos** y seleccione **críticos** en el campo gravedad del evento.
4. Seleccione **todos los eventos críticos** en el área Eventos coincidentes y muévalos al área Eventos seleccionados.
5. Haga clic en **acciones** e introduzca **`sample@domain.com`** En el campo Alerta a estos usuarios.
6. Seleccione **Recordar cada 15 minutos** para notificar al usuario cada 15 minutos.

   Puede configurar una alerta para que envíe repetidamente notificaciones a los destinatarios durante un período de tiempo específico. Debe determinar la hora desde la cual está activa la notificación de eventos para la alerta.
7. En el menú Select Script to Execute, seleccione **Test** script.
8. Haga clic en **Guardar**.

Directrices para añadir alertas

Puede añadir alertas basadas en un recurso, como un clúster, nodo, agregado o volumen, y eventos de un tipo de gravedad determinado. Como práctica recomendada, puede añadir una alerta para cualquiera de los objetos críticos después de haber agregado el clúster al que pertenece el objeto.

Puede utilizar las siguientes directrices y consideraciones para crear alertas y gestionar los sistemas de forma eficaz:

- Descripción de alertas

  Debe proporcionar una descripción de la alerta para ayudarle a realizar un seguimiento de las alertas de forma eficaz.

- Recursos

  Debe decidir qué recurso físico o lógico requiere una alerta. Puede incluir y excluir recursos, según sea necesario. Por ejemplo, si desea supervisar de cerca los agregados mediante la configuración de una alerta, debe seleccionar los agregados necesarios de la lista de recursos.

  Si selecciona una categoría de recursos, por ejemplo, **<<All User or Group Quotas>>**, entonces recibirá alertas para todos los objetos de esa categoría.

  Al seleccionar un clúster, ya que el recurso no selecciona de forma automática los objetos de almacenamiento de ese clúster. Por ejemplo, si crea una alerta para todos los eventos críticos de todos los clústeres, recibirá alertas solo para los eventos críticos del clúster. No recibirá alertas sobre eventos críticos en nodos, agregados, etc.

- Gravedad del evento

  Debe decidir si un evento de un tipo de gravedad especificado (crítico, error, advertencia) debe activar la alerta y, de ser así, qué tipo de gravedad.

- Eventos seleccionados

  Si añade una alerta según el tipo de evento generado, debe decidir qué eventos requieren una alerta.

  Si selecciona una gravedad de evento, pero no selecciona ningún evento individual (si deja vacía la columna "Eventos seleccionados"), recibirá alertas para todos los eventos de la categoría.

- Acciones

  Debe indicar los nombres de usuario y las direcciones de correo electrónico de los usuarios que reciben la notificación. También puede especificar una captura SNMP como un modo de notificación. Puede asociar los scripts a una alerta para que se ejecuten cuando se genere una alerta.

- Frecuencia de notificación

  Puede configurar una alerta para que envíe repetidamente notificaciones a los destinatarios durante un tiempo específico. Debe determinar la hora desde la cual está activa la notificación de eventos para la alerta. Si desea que la notificación de eventos se repita hasta que se reconozca el evento, debe determinar la frecuencia con la que desea que se repita la notificación.

- Ejecutar secuencia de comandos

  Puede asociar la secuencia de comandos con una alerta. La secuencia de comandos se ejecuta cuando se genera la alerta.

Adición de alertas para eventos de rendimiento

Es posible configurar alertas para eventos de rendimiento individuales, como cualquier otro evento que reciba Unified Manager. Además, si desea tratar todos los eventos de rendimiento por igual y enviar correo electrónico a la misma persona, puede crear una única alerta para notificarle cuando se active cualquier evento de rendimiento crítico o de advertencia.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

El siguiente ejemplo muestra cómo crear un evento para todos los eventos de latencia crítica, IOPS y Mbps. Puede utilizar esta misma metodología para seleccionar eventos de todos los contadores de rendimiento y de todos los eventos de advertencia.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de alertas**.
2. En la página **Configuración de alertas**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar alerta**, haga clic en **Nombre** e introduzca un nombre y una descripción para la alerta.

4. No seleccione ningún recurso en la página **Recursos**.

   Dado que no se selecciona ningún recurso, la alerta se aplica a todos los clústeres, agregados, volúmenes, etc., en los cuales se reciben estos eventos.

5. Haga clic en **Eventos** y realice las siguientes acciones:
   a. En la lista gravedad del evento, seleccione **crítico**.
   b. En el campo Event Name contiene, introduzca `latency` y, a continuación, haga clic en la flecha para seleccionar todos los eventos coincidentes.
   c. En el campo Event Name contiene, introduzca `iops` y, a continuación, haga clic en la flecha para seleccionar todos los eventos coincidentes.
   d. En el campo Event Name contiene, introduzca `mbps` y, a continuación, haga clic en la flecha para seleccionar todos los eventos coincidentes.
6. Haga clic en **acciones** y, a continuación, seleccione el nombre del usuario que recibirá el correo electrónico de alerta en el campo **Alerta a estos usuarios**.
7. Configure cualquier otra opción de esta página para emitir capturas SNMP y ejecutar un script.
8. Haga clic en **Guardar**.

Probar alertas

Puede probar una alerta para verificar que la ha configurado correctamente. Cuando se activa un evento, se genera una alerta y se envía un correo electrónico de alerta a los destinatarios configurados. Puede comprobar si se envía la notificación y si la secuencia de comandos se ejecuta mediante la alerta de prueba.

Lo que necesitará

- Debe haber configurado ajustes de notificación, como la dirección de correo electrónico de los destinatarios, el servidor SMTP y la captura SNMP.

  Unified Manager Server puede utilizar esta configuración para enviar notificaciones a los usuarios cuando se genera un evento.

- Debe haber asignado un script y configurado el script para que se ejecute cuando se genere la alerta.
- Debe tener la función Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de alertas**.
2. En la página **Configuración de alertas**, seleccione la alerta que desea probar y, a continuación, haga clic en **Prueba**.

   Se envía un correo electrónico de alerta de prueba a las direcciones de correo electrónico especificadas durante la creación de la alerta.

Habilitar y deshabilitar alertas para eventos resueltos y obsoletos

Para todos los eventos que haya configurado para enviar alertas, se enviará un mensaje

de alerta cuando esos eventos pasen por todos los estados disponibles: Nuevo, reconocido, resuelto y Obsoleto. Si no desea recibir alertas de eventos a medida que se trasladan a los estados resueltos y Obsoleto, puede configurar una configuración global para suprimir dichas alertas.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

De forma predeterminada, las alertas no se envían para los eventos a medida que se mueven a los estados resueltos y Obsoleto.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de alertas**.
2. En la página **Configuración de alertas**, realice una de las siguientes acciones mediante el control deslizante situado junto al elemento **Alertas para eventos resueltos y obsoletos**:

Para…	Realice lo siguiente…
Deje de enviar alertas cuando los eventos se resuelvan o se vuelven obsoletos	Mueva el control deslizante hacia la izquierda
Comience a enviar alertas como eventos que se resuelven o se vuelven obsoletos	Mueva el control deslizante hacia la derecha

No se incluye el hecho de que los volúmenes de destino de recuperación ante desastres generen alertas

Al configurar alertas de volumen, es posible especificar una cadena en el cuadro de diálogo Alert que identifica un volumen o un grupo de volúmenes. Si configuró la recuperación ante desastres para las SVM, sin embargo, los volúmenes de origen y destino tienen el mismo nombre, por lo que recibirá alertas para ambos volúmenes.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Si desea deshabilitar alertas para los volúmenes de destino de recuperación ante desastres, se deben excluir los volúmenes que tienen el nombre de la SVM de destino. Esto es posible porque el identificador de los eventos del volumen contiene el nombre de SVM y el nombre del volumen con el formato "<svm_name>:/<volume_name>".

El siguiente ejemplo muestra cómo crear alertas para el volumen "vol1" en la SVM principal "vs1", pero excluya la alerta de la generación en un volumen con el mismo nombre en SVM "vs1-dr".

Realice los siguientes pasos en el cuadro de diálogo Agregar alerta:

Pasos

1. Haga clic en **Nombre** e introduzca un nombre y una descripción para la alerta.

2. Haga clic en **Recursos** y, a continuación, seleccione la ficha **incluir**.
   a. Seleccione **volumen** en la lista desplegable y, a continuación, introduzca **`vol1`** En el campo **Nombre contiene** para mostrar los volúmenes cuyo nombre contiene "vol1".
   b. Seleccione **<<All Volumes whose name contains 'vol1'>>** desde el área **Recursos disponibles**, y muévalos al área **Recursos seleccionados**.
3. Seleccione la ficha **excluir**, seleccione **volumen**, introduzca **`vs1-dr`** En el campo **Nombre contiene** y, a continuación, haga clic en **Agregar**.

   De este modo, se excluye la generación de alertas para el volumen «vol1» en la SVM «vs1-dr».
4. Haga clic en **Eventos** y seleccione el evento o eventos que desea aplicar al volumen o volúmenes.
5. Haga clic en **acciones** y, a continuación, seleccione el nombre del usuario que recibirá el correo electrónico de alerta en el campo **Alerta a estos usuarios**.
6. Configure cualquier otra opción de esta página para emitir capturas SNMP y ejecutar una secuencia de comandos y, a continuación, haga clic en **Guardar**.

Visualizar alertas

Es posible ver la lista de alertas que se crean para varios eventos en la página Alert Setup. También es posible ver propiedades de alerta como la descripción de alertas, el método de notificación y la frecuencia, los eventos que activan la alerta, los destinatarios de correo electrónico de las alertas y los recursos afectados, como clústeres, agregados y volúmenes.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Paso

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de alertas**.

   La lista de alertas se muestra en la página Alert Setup.

Editar alertas

Puede editar propiedades de alerta como el recurso con el que está asociada la alerta, eventos, destinatarios, opciones de notificación, frecuencia de notificación, y los scripts asociados.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de alertas**.
2. En la página **Configuración de alertas**, seleccione la alerta que desea editar y haga clic en **Editar**.

3. En el cuadro de diálogo **Editar alerta**, edite las secciones nombre, recursos, eventos y acciones, según sea necesario.

   Es posible cambiar o quitar el script asociado a la alerta.

4. Haga clic en **Guardar**.

Eliminar alertas

Es posible eliminar una alerta cuando ya no se necesita. Por ejemplo, puede eliminar una alerta que se creó para un recurso particular cuando Unified Manager ya no supervisa ese recurso.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de alertas**.
2. En la página **Configuración de alertas**, seleccione las alertas que desea eliminar y haga clic en **Eliminar**.
3. Haga clic en **Sí** para confirmar la solicitud de eliminación.

Descripción de ventanas de alerta y cuadros de diálogo

Si desea configurar alertas para recibir notificaciones acerca de los eventos, utilice el cuadro de diálogo Add Alert. También puede ver la lista de alertas desde la página Alert Setup.

Página Alert Setup

La página Alert Setup muestra una lista de alertas y proporciona información sobre el nombre de alerta, el estado, el método de notificación y la frecuencia de notificaciones. En esta página, también es posible añadir, editar, quitar, habilitar o deshabilitar alertas.

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Botones de comando

- **Agregar**

  Muestra el cuadro de diálogo Agregar alerta, que permite añadir alertas nuevas.

- **Edición**

  Muestra el cuadro de diálogo Editar alerta, que permite editar las alertas seleccionadas.

- **Eliminar**

  Elimina las alertas seleccionadas.

- **Activar**

  Habilita las alertas seleccionadas para que envíen notificaciones.

- **Desactivar**

  Deshabilita las alertas seleccionadas cuando desea detener temporalmente el envío de notificaciones.

- **Prueba**

  Prueba las alertas seleccionadas para verificar su configuración después de agregarlas o editarlas.

- **Alertas de Eventos resueltos y obsoletos**

  Permite habilitar o deshabilitar el envío de alertas cuando los eventos se mueven a los estados resueltos o Obsoleto. Esto puede ayudar a los usuarios a recibir notificaciones innecesarias.

Vista de lista

La vista de lista muestra, en formato de tabla, información sobre las alertas que se crean. Puede utilizar los filtros de columnas para personalizar los datos que se muestran. También puede seleccionar una alerta para ver más información sobre ella en el área de detalles.

- **Estado**

  Especifica si una alerta está habilitada ( ) o desactivado ( ).

- **Alerta**

  Muestra el nombre de la alerta.

- **Descripción**

  Muestra una descripción de la alerta.

- **Método de notificación**

  Muestra el método de notificación seleccionado para la alerta. Es posible notificar a los usuarios a través de correo electrónico o capturas SNMP.

- **Frecuencia de notificación**

  Especifica la frecuencia (en minutos) con la que el servidor de administración continúa enviando notificaciones hasta que el evento se confirma, se resuelve o se mueve al estado Obsoleto.

El área Detalles

El área de detalles proporciona más información sobre la alerta seleccionada.

- **Nombre de alerta**

  Muestra el nombre de la alerta.

- **Descripción de alerta**

Muestra una descripción de la alerta.

- **Eventos**

  Muestra los eventos en los que desea activar la alerta.

- **Recursos**

  Muestra los recursos sobre los que desea activar la alerta.

- **Incluye**

  Muestra el grupo de recursos sobre los que desea activar la alerta.

- **Excluye**

  Muestra el grupo de recursos para los que no desea activar la alerta.

- **Método de notificación**

  Muestra el método de notificación de la alerta.

- **Frecuencia de notificación**

  Muestra la frecuencia con la que el servidor de administración continúa enviando notificaciones de alerta hasta que el evento se confirma, se resuelve o se mueve al estado Obsoleto.

- **Nombre del script**

  Muestra el nombre del script asociado a la alerta seleccionada. Este script se ejecuta cuando se genera una alerta.

- **Destinatarios de correo electrónico**

  Muestra las direcciones de correo electrónico de los usuarios que reciben la notificación de alerta.

Cuadro de diálogo Agregar alerta

Puede crear alertas para notificarle cuando se genera un evento determinado, de modo que pueda abordar el problema rápidamente y, por lo tanto, minimizar el impacto en el entorno. Puede crear alertas para un solo recurso o un conjunto de recursos, así como para eventos de un tipo de gravedad determinado. También puede especificar el método de notificación y la frecuencia de las alertas.

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Nombre

Esta área le permite especificar un nombre y una descripción para la alerta:

- **Nombre de alerta**

  Permite especificar un nombre de alerta.

- **Descripción de alerta**

  Permite especificar una descripción de la alerta.

Recursos

Esta área le permite seleccionar un recurso individual o agrupar los recursos en función de una regla dinámica para la que desea activar la alerta. Una *regla dinámica* es el conjunto de recursos filtrados según la cadena de texto que especifique. Puede buscar recursos seleccionando un tipo de recurso de la lista desplegable o puede especificar el nombre exacto del recurso para mostrar un recurso específico.

Si va a crear una alerta desde cualquiera de las páginas de detalles del objeto de almacenamiento, el objeto de almacenamiento se incluye automáticamente en la alerta.

- **Incluir**

  Le permite incluir los recursos para los que desea activar alertas. Puede especificar una cadena de texto para agrupar recursos que coincidan con la cadena y seleccionar este grupo que se incluirá en la alerta. Por ejemplo, puede agrupar todos los volúmenes cuyo nombre contiene la cadena "abc".

- **Excluir**

  Permite excluir recursos para los que no desea activar alertas. Por ejemplo, puede excluir todos los volúmenes cuyo nombre contenga la cadena "xyz".

  La ficha excluir sólo se muestra cuando se seleccionan todos los recursos de un tipo de recurso en particular: Por ejemplo, <<All Volumes>> o. <<All Volumes whose name contains 'xyz'>>.

  Si un recurso cumple las reglas de inclusión y exclusión especificadas, la regla de exclusión tiene prioridad sobre la regla de inclusión y no se genera la alerta para el evento.

Eventos

Este área le permite seleccionar los eventos para los que desea crear las alertas. Puede crear alertas para los eventos según una gravedad determinada o para un conjunto de eventos.

Para seleccionar más de un evento, mantenga pulsada la tecla Ctrl mientras realiza las selecciones.

- **Gravedad del suceso**

  Le permite seleccionar eventos según el tipo de gravedad, que puede ser crítico, error o advertencia.

- **Nombre del evento contiene**

  Permite seleccionar eventos cuyo nombre contenga caracteres especificados.

Acciones

Esta área le permite especificar los usuarios a los que desea notificar cuando se activa una alerta. También puede especificar el método de notificación y la frecuencia de la notificación.

- **Avisar a estos usuarios**

  Permite especificar la dirección de correo electrónico o el nombre de usuario del usuario para recibir

notificaciones.

Si modifica la dirección de correo electrónico especificada para el usuario y vuelve a abrir la alerta para su edición, el campo Nombre aparecerá en blanco porque la dirección de correo electrónico modificada ya no está asignada al usuario que se seleccionó previamente. Además, si ha modificado la dirección de correo electrónico del usuario seleccionado desde la página usuarios, la dirección de correo electrónico modificada no se actualizará para el usuario seleccionado.

- **Frecuencia de notificación**

  Permite especificar la frecuencia con la cual el servidor de gestión envía notificaciones hasta que el evento se confirma, se resuelve o se mueve al estado obsoleto.

  Se pueden elegir los siguientes métodos de notificación:

  - Notificar sólo una vez
  - Notificar a una frecuencia específica
  - Notificar a una frecuencia especificada dentro del intervalo de tiempo especificado
- **Emitir SNMP Trap**

  Al seleccionar esta casilla, se permite especificar si se deben enviar capturas SNMP al host SNMP configurado globalmente.

- **Ejecutar script**

  Permite agregar el script personalizado a la alerta. Este script se ejecuta cuando se genera una alerta.

> Si no ve esta capacidad disponible en la interfaz de usuario, se debe a que el administrador ha desactivado la funcionalidad. Si es necesario, puede activar esta funcionalidad desde **Storage Management** > **Configuración de funciones**.

Botones de comando

- **Guardar**

  Crea una alerta y cierra el cuadro de diálogo.

- **Cancelar**

  Descarta los cambios y cierra el cuadro de diálogo.

Cuadro de diálogo Edit Alert

Puede editar propiedades de alerta, como el recurso con el que está asociada la alerta, eventos, script y opciones de notificación.

Nombre

Esta área le permite editar el nombre y la descripción de la alerta.

- **Nombre de alerta**

Permite editar el nombre de alerta.

- **Descripción de alerta**

  Permite especificar una descripción de la alerta.

- **Estado de alerta**

  Permite habilitar o deshabilitar la alerta.

Recursos

Esta área le permite seleccionar un recurso individual o agrupar los recursos en función de una regla dinámica para la que desea activar la alerta. Puede buscar recursos seleccionando un tipo de recurso de la lista desplegable o puede especificar el nombre exacto del recurso para mostrar un recurso específico.

- **Incluir**

  Le permite incluir los recursos para los que desea activar alertas. Puede especificar una cadena de texto para agrupar recursos que coincidan con la cadena y seleccionar este grupo que se incluirá en la alerta. Por ejemplo, puede agrupar todos los volúmenes cuyo nombre contenga la cadena "'vol0'".

- **Excluir**

  Permite excluir recursos para los que no desea activar alertas. Por ejemplo, puede excluir todos los volúmenes cuyo nombre contenga la cadena "'xyz'".

> La ficha excluir sólo se muestra cuando se seleccionan todos los recursos de un tipo de recurso en particular, por ejemplo, <<All Volumes>> o <<All Volumes whose name contains 'xyz'>>.

Eventos

Este área le permite seleccionar los eventos para los que desea activar las alertas. Puede activar una alerta para eventos según una gravedad determinada o para un conjunto de eventos.

- **Gravedad del suceso**

  Le permite seleccionar eventos según el tipo de gravedad, que puede ser crítico, error o advertencia.

- **Nombre del evento contiene**

  Permite seleccionar eventos cuyo nombre contenga los caracteres especificados.

Acciones

Esta área permite especificar el método de notificación y la frecuencia de las notificaciones.

- **Avisar a estos usuarios**

  Permite editar la dirección de correo electrónico o el nombre de usuario, o bien especificar una nueva dirección de correo electrónico o nombre de usuario para recibir notificaciones.

- **Frecuencia de notificación**

Permite editar la frecuencia con la cual el servidor de gestión envía notificaciones hasta que el evento se confirma, se resuelve o se mueve al estado obsoleto.

Se pueden elegir los siguientes métodos de notificación:

- Notificar sólo una vez
- Notificar a una frecuencia específica
- Notificar a una frecuencia especificada dentro del intervalo de tiempo especificado

- **Emitir SNMP Trap**

  Permite especificar si se deben enviar capturas SNMP al host SNMP configurado globalmente.

- **Ejecutar script**

  Permite asociar un script con la alerta. Este script se ejecuta cuando se genera una alerta.

Botones de comando

- **Guardar**

  Guarda los cambios y cierra el cuadro de diálogo.

- **Cancelar**

  Descarta los cambios y cierra el cuadro de diálogo.

Administrar scripts

Es posible usar scripts para modificar o actualizar automáticamente varios objetos de almacenamiento en Unified Manager. El script está asociado a una alerta. Cuando un evento activa una alerta, se ejecuta el script. Puede cargar scripts personalizados y probar su ejecución cuando se genera una alerta.

La capacidad de cargar scripts en Unified Manager y ejecutarlas está habilitada de forma predeterminada. Si su organización no desea permitir esta funcionalidad debido a razones de seguridad, puede desactivar esta funcionalidad desde **Storage Management** > **Configuración de funciones**.

Información relacionada

"Habilitar y deshabilitar la capacidad para cargar scripts"

Cómo funcionan los scripts con alertas

Es posible asociar una alerta a la secuencia de comandos para que se ejecute el script cuando se genera una alerta para un evento en Unified Manager. Puede usar los scripts para resolver problemas con objetos de almacenamiento o identificar qué objetos de almacenamiento generan los eventos.

Cuando se genera una alerta para un evento en Unified Manager, se envía un correo electrónico de alerta a los destinatarios especificados. Si asoció una alerta a un script, se ejecuta el script. Puede obtener los detalles

de los argumentos pasados al script desde el correo electrónico de alerta.

> Si ha creado una secuencia de comandos personalizada y la ha asociado con una alerta para un tipo de evento específico, las acciones se realizan en función de su secuencia de comandos personalizada para ese tipo de evento y las acciones **Fix it** no están disponibles de forma predeterminada en la página acciones de administración o en el panel de Unified Manager.

El script utiliza los siguientes argumentos para su ejecución:

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

Puede utilizar los argumentos de las secuencias de comandos y recopilar información de eventos relacionada o modificar objetos de almacenamiento.

Ejemplo para obtener argumentos de scripts

```
`print "$ARGV[0] : $ARGV[1]\n"`
`print "$ARGV[7] : $ARGV[8]\n"`
```

Cuando se genera una alerta, se ejecuta este script y se muestra el siguiente resultado:

```
-`eventID : 290`
-`eventSourceID : 4138`
```

Añadiendo scripts

Puede añadir scripts en Unified Manager y asociarlos con alertas. Estos scripts se ejecutan automáticamente cuando se genera una alerta, y le permiten obtener información sobre los objetos de almacenamiento para los que se genera el evento.

Lo que necesitará

- Debe haber creado y guardado los scripts que desea añadir al servidor de Unified Manager.
- Los formatos de archivo compatibles con scripts son Perl, Shell, PowerShell, Python y. `.bat` archivos.

Plataforma en la que se ha instalado Unified Manager	Idiomas compatibles
VMware	Scripts Perl y Shell
Linux	Scripts Perl, Python y Shell
Windows	PowerShell, Perl, Python y scripts .bat

- Para los scripts Perl, se debe instalar Perl en el servidor Unified Manager. Para instalaciones de VMware, se instala Perl 5 de forma predeterminada y los scripts solo admiten lo que admite Perl 5. Si se instaló Perl después de Unified Manager, debe reiniciar el servidor de Unified Manager.
- Para los scripts de PowerShell, se debe establecer la directiva de ejecución de PowerShell correspondiente en el servidor Windows para poder ejecutar los scripts.

Si el script crea archivos de registro para realizar un seguimiento del progreso del script de alertas, debe asegurarse de que no se creen los archivos de registro en ningún lugar de la carpeta de instalación de Unified Manager.

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Puede cargar scripts personalizados y recopilar detalles de eventos acerca de la alerta.

Si no ve esta capacidad disponible en la interfaz de usuario, se debe a que el administrador ha desactivado la funcionalidad. Si es necesario, puede activar esta funcionalidad desde **Storage Management** > **Configuración de funciones**.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Storage Management** > **Scripts**.
2. En la página **Scripts**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar script**, haga clic en **examinar** para seleccionar el archivo de secuencia de comandos.
4. Introduzca una descripción para la secuencia de comandos que seleccione.
5. Haga clic en **Agregar**.

Información relacionada

"Habilitar y deshabilitar la capacidad para cargar scripts"

Eliminar scripts

Es posible eliminar un script de Unified Manager cuando el script ya no se requiere o no es válido.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- El script no debe estar asociado a una alerta.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Storage Management** > **Scripts**.
2. En la página **Scripts**, seleccione la secuencia de comandos que desea eliminar y, a continuación, haga clic en **Eliminar**.
3. En el cuadro de diálogo **Advertencia**, confirme la eliminación haciendo clic en **Sí**.

Prueba de la ejecución de scripts

Puede verificar que el script se ejecute correctamente cuando se genera una alerta para un objeto de almacenamiento.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber cargado un script en el formato de archivo compatible a Unified Manager.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Storage Management** > **Scripts**.
2. En la página **Scripts**, agregue el script de prueba.
3. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de alertas**.
4. En la página **Configuración de alertas**, realice una de las siguientes acciones:

Para…	Realice lo siguiente…
Añadir una alerta	a. Haga clic en **Agregar**. b. En la sección acciones, asocie la alerta al script de prueba.
Editar una alerta	a. Seleccione una alerta y, a continuación, haga clic en **Editar**. b. En la sección acciones, asocie la alerta al script de prueba.

5. Haga clic en **Guardar**.
6. En la página **Configuración de alertas**, seleccione la alerta que ha agregado o modificado y, a continuación, haga clic en **Prueba**.

   El script se ejecuta con el argumento "-test" y se envía una alerta de notificación a las direcciones de correo electrónico que se especificaron al crear la alerta.

Comandos de CLI de Unified Manager compatibles

Como administrador de almacenamiento, puede usar los comandos de la CLI para realizar consultas en los objetos de almacenamiento; por ejemplo, en clústeres, agregados, volúmenes, Qtrees y LUN. Puede utilizar los comandos de la CLI para consultar la base de datos interna de Unified Manager y la base de datos de ONTAP.

También puede utilizar los comandos de la CLI en scripts que se ejecutan al principio o al final de una operación, o bien se ejecutan cuando se activa una alerta.

Todos los comandos deben ir precedidos por el comando `um cli login` y un nombre de usuario y una contraseña válidos para la autenticación.

Para ejecutar el comando *um run*, asegúrese de que su cuenta tiene acceso a la aplicación *Console*.

Comando de la CLI	Descripción	Salida
`um cli login -u <username> [-p <password>]`	Inicia sesión en la CLI. Debido a las implicaciones de seguridad, debe introducir sólo el nombre de usuario que sigue la opción "-u". Cuando se utilice de esta forma, se le pedirá la contraseña y la contraseña no se capturará en la tabla de historial o proceso. La sesión caduca a las tres horas del inicio de sesión, después de las cuales el usuario debe iniciar sesión de nuevo.	Muestra el mensaje correspondiente.
`um cli logout`	Cierra sesión en la CLI.	Muestra el mensaje correspondiente.
`um help`	Muestra todos los subcomandos de primer nivel.	Muestra todos los subcomandos de primer nivel.
`um run cmd [ -t <timeout> ] <cluster> <command>`	La forma más sencilla de ejecutar un comando en uno o más hosts. Se utiliza principalmente para generar scripts de alertas para obtener o realizar una operación en ONTAP. El argumento de tiempo de espera opcional establece un límite de tiempo máximo (en segundos) para que el comando se complete en el cliente. El valor predeterminado es 0 (espere siempre).	Según lo recibido de ONTAP.
`um run query <sql command>`	Ejecuta una consulta SQL. Sólo se permiten las consultas que se leen en la base de datos. No se admiten operaciones de actualización, inserción o eliminación.	Los resultados se muestran en una forma tabular. Si se devuelve un conjunto vacío, o si hay algún error de sintaxis o solicitud incorrecta, muestra el mensaje de error correspondiente.

Comando de la CLI	Descripción	Salida
`um datasource add -u <username> -P <password> [ -t <protocol> ] [ -p <port> ] <hostname-or-ip>`	Agrega un origen de datos a la lista de sistemas de almacenamiento gestionados. Un origen de datos describe cómo se establecen las conexiones con los sistemas de almacenamiento. Las opciones -u (nombre de usuario) y -P (contraseña) se deben especificar al agregar un origen de datos. La opción -t (protocolo) especifica el protocolo que se utiliza para comunicarse con el clúster (http o https). Si no se especifica el protocolo, se intentará ambos protocolos la opción -p (puerto) especifica el puerto que se utiliza para comunicarse con el clúster. Si no se especifica el puerto, se intentará el valor predeterminado del protocolo adecuado. Este comando solo el administrador de almacenamiento puede ejecutarlo.	Las solicitudes del usuario aceptan el certificado e imprimen el mensaje correspondiente.
`um datasource list [ <datasource-id>]`	Muestra los orígenes de datos para los sistemas de almacenamiento gestionados.	Muestra los siguientes valores en formato tabular: `ID Address Port, Protocol Acquisition Status, Analysis Status, Communication status, Acquisition Message, and Analysis Message.`
`um datasource modify [ -h <hostname-or-ip> ] [ -u <username> ] [ -P <password> ] [ -t <protocol> ] [ -p <port> ] <datasource-id>`	Modifica una o varias opciones de origen de datos. Solo el administrador de almacenamiento puede ejecutarlo.	Muestra el mensaje correspondiente.
`um datasource remove <datasource-id>`	Elimina el origen de datos (clúster) de Unified Manager.	Muestra el mensaje correspondiente.
`um option list [ <option> .. ]`	Muestra todas las opciones que puede configurar mediante el comando SET.	Muestra los siguientes valores en formato tabular: `Name, Value, Default Value, and Requires Restart.`

Comando de la CLI	Descripción	Salida
`um option set <option-name>=<option-value> [ <option-name>=<option-value> … ]`	Establece una o más opciones. Solo el administrador de almacenamiento puede ejecutar el comando.	Muestra el mensaje correspondiente.
`um version`	Muestra la versión del software Unified Manager.	`Version ("9.6")`
`um lun list [-q] [ -ObjectType <object-id>]`	Muestra las LUN después de filtrar en el objeto especificado. -q es aplicable para que todos los comandos no muestren ningún encabezado. El tipo de objeto puede ser lun, qtree, clúster, volumen, cuota, o svm. Por ejemplo: **`um lun list -cluster 1`** En este ejemplo, "-cluster" es el objecttype y "1" es el objectId. El comando enumera todas las LUN del clúster con el ID 1.	Muestra los siguientes valores en formato tabular: `ID and LUN path.`
`um svm list [-q] [ -ObjectType <object-id>]`	Muestra las máquinas virtuales de almacenamiento después de filtrar el objeto especificado. El tipo de objeto puede ser lun, qtree, clúster, volumen, cuota, o svm. Por ejemplo: **`um svm list -cluster 1`** En este ejemplo, "-cluster" es el objecttype y "1" es el objectId. El comando enumera todas las máquinas virtuales de almacenamiento del clúster con el ID 1.	Muestra los siguientes valores en formato tabular: `Name and Cluster ID.`

Comando de la CLI	Descripción	Salida
`um qtree list [-q] [ -ObjectType <object-id>]`	Enumera los qtrees después de filtrar en el objeto especificado. -q es aplicable para que todos los comandos no muestren ningún encabezado. El tipo de objeto puede ser lun, qtree, clúster, volumen, cuota, o svm. Por ejemplo: **`um qtree list -cluster 1`** En este ejemplo, "-cluster" es el objecttype y "1" es el objectId. El comando enumera todos los qtrees dentro del clúster con el ID 1.	Muestra los siguientes valores en formato tabular: `Qtree ID and Qtree Name.`
`um disk list [-q] [-ObjectType <object-id>]`	Enumera los discos después de filtrar en el objeto especificado. El tipo de objeto puede ser disco, aggr, nodo o clúster. Por ejemplo: **`um disk list -cluster 1`** En este ejemplo, "-cluster" es el objecttype y "1" es el objectId. El comando enumera todos los discos del clúster con el ID 1.	Muestra los siguientes valores en formato tabular `ObjectType and object-id`.
`um cluster list [-q] [-ObjectType <object-id>]`	Muestra los clústeres después de filtrar en el objeto especificado. El tipo de objeto puede ser disco, aggr, nodo, clúster, lun, qtree, volumen, cuota o svm. Por ejemplo: **`um cluster list -aggr 1`** En este ejemplo, "-aggr" es el objecttype y "1" es el objectId. El comando enumera el clúster al que pertenece el agregado con el ID 1.	Muestra los siguientes valores en formato tabular: `Name, Full Name, Serial Number, Datasource Id, Last Refresh Time, and Resource Key.`

Comando de la CLI	Descripción	Salida
`um cluster node list [-q] [-ObjectType <object-id>]`	Muestra los nodos del clúster después de filtrar el objeto especificado. El tipo de objeto puede ser disco, aggr, nodo o clúster. Por ejemplo: **`um cluster node list -cluster 1`** En este ejemplo, "-cluster" es el objecttype y "1" es el objectId. El comando enumera todos los nodos del clúster con el ID 1.	Muestra los siguientes valores en formato tabular `Name and Cluster ID`.
`um volume list [-q] [-ObjectType <object-id>]`	Enumera los volúmenes después de filtrar en el objeto especificado. El tipo de objeto puede ser lun, qtree, clúster, volumen, cuota, svm o agregado. Por ejemplo: **`um volume list -cluster 1`** En este ejemplo, "-cluster" es el objecttype y "1" es el objectId. El comando enumera todos los volúmenes del clúster con el ID 1.	Muestra los siguientes valores en formato tabular `Volume ID and Volume Name`.
`um quota user list [-q] [-ObjectType <object-id>]`	Muestra los usuarios de la cuota después de filtrar en el objeto especificado. El tipo de objeto puede ser qtree, clúster, volumen, cuota o svm. Por ejemplo: **`um quota user list -cluster 1`** En este ejemplo, "-cluster" es el objecttype y "1" es el objectId. El comando enumera todos los usuarios de cuota del clúster con el ID 1.	Muestra los siguientes valores en formato tabular `ID, Name, SID and Email`.

Comando de la CLI	Descripción	Salida
`um aggr list [-q] [-ObjectType <object-id>]`	Enumera los agregados después de filtrar en el objeto especificado. El tipo de objeto puede ser disco, aggr, nodo, clúster o volumen. Por ejemplo: **`um aggr list -cluster 1`** En este ejemplo, "-cluster" es el objecttype y "1" es el objectId. El comando enumera todos los agregados del clúster con el ID 1.	Muestra los siguientes valores en formato tabular `Aggr ID, and Aggr Name`.
`um event ack <event-ids>`	Reconoce uno o más eventos.	Muestra el mensaje correspondiente.
`um event resolve <event-ids>`	Resuelve uno o varios eventos.	Muestra el mensaje correspondiente.
`um event assign -u <username> <event-id>`	Asigna un evento a un usuario.	Muestra el mensaje correspondiente.
`um event list [ -s <source> ] [ -S <event-state-filter-list>.. ] [ <event-id> .. ]`	Muestra los eventos generados por el sistema o el usuario. Filtra eventos según el origen, el estado y los ID.	Muestra los siguientes valores en formato tabular `Source, Source type, Name, Severity, State, User and Timestamp`.
`um backup restore -f <backup_file_path_and_name>`	Restaura un backup de la base de datos MySQL con archivos .7z.	Muestra el mensaje correspondiente.

Descripción de ventanas de script y cuadros de diálogo

La página Scripts permite añadir scripts a Unified Manager.

Scripts

La página Scripts permite añadir sus scripts personalizados a Unified Manager. Puede asociar estos scripts con alertas para habilitar la reconfiguración automática de los objetos de almacenamiento.

La página Scripts permite añadir o eliminar scripts de Unified Manager.

Botones de comando

- **Agregar**

Muestra el cuadro de diálogo Agregar script, que permite agregar scripts.

- **Eliminar**

  Elimina la secuencia de comandos seleccionada.

Vista de lista

La vista de lista muestra, en formato de tabla, los scripts que se añadieron a Unified Manager.

- **Nombre**

  Muestra el nombre del script.

- **Descripción**

  Muestra la descripción del script.

Cuadro de diálogo Add Script

El cuadro de diálogo Add Script permite añadir scripts a Unified Manager. Es posible configurar alertas con los scripts para resolver automáticamente los eventos generados para los objetos de almacenamiento.

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

- **Seleccione Archivo de secuencia de comandos**

  Permite seleccionar un script para la alerta.

- **Descripción**

  Permite especificar una descripción para el script.

Supervise y gestione el rendimiento de los clústeres

Introducción a la supervisión del rendimiento de Active IQ Unified Manager

Active IQ Unified Manager (anteriormente Unified Manager de OnCommand) proporciona funcionalidades de supervisión del rendimiento y análisis de eventos raíz para sistemas que ejecutan el software ONTAP de NetApp.

Unified Manager le ayuda a identificar cargas de trabajo que están utilizando de forma excesiva los componentes del clúster y a reducir el rendimiento de otras cargas de trabajo del clúster. Al definir las políticas de umbral de rendimiento, también se pueden especificar valores máximos de determinados contadores de rendimiento para que los eventos se generen cuando se supera el umbral. Unified Manager le alerta sobre estos eventos de rendimiento para poder realizar acciones correctivas y devolver el rendimiento a los niveles normales de funcionamiento. Los eventos se pueden ver y analizar en la interfaz de usuario de Unified Manager.

Unified Manager supervisa el rendimiento de dos tipos de cargas de trabajo:

- Cargas de trabajo definidas por el usuario

  Estas cargas de trabajo constan de volúmenes de FlexVol y volúmenes de FlexGroup creados en el clúster.

- Cargas de trabajo definidas por el sistema

  Estas cargas de trabajo constan de una actividad interna del sistema.

Funciones de supervisión del rendimiento de Unified Manager

Unified Manager recopila y analiza estadísticas de rendimiento de sistemas que ejecutan el software ONTAP. Utiliza umbrales dinámicos de rendimiento y umbrales definidos por el usuario para supervisar diversos contadores de rendimiento sobre muchos componentes del clúster.

Un tiempo de respuesta alto (latencia) indica que el objeto de almacenamiento, por ejemplo, un volumen, tiene un rendimiento más lento de lo normal. Este problema también indica que el rendimiento ha disminuido para las aplicaciones cliente que utilizan el volumen. Unified Manager identifica el componente de almacenamiento donde reside el problema de rendimiento y proporciona una lista de acciones sugeridas para resolver el problema de rendimiento.

Unified Manager incluye las siguientes funciones:

- Supervisa y analiza las estadísticas de rendimiento de la carga de trabajo desde un sistema que ejecuta el software ONTAP.
- Realiza un seguimiento de los contadores de rendimiento de clústeres, nodos, agregados, puertos, SVM, Volúmenes, LUN, espacios de nombres NVMe e interfaces de red (LIF).
- Muestra gráficos detallados que traza la actividad de las cargas de trabajo a lo largo del tiempo; incluidos

IOPS (operaciones), MB/s (rendimiento), latencia (tiempo de respuesta), utilización, la capacidad de rendimiento y la proporción de caché.

- Le permite crear políticas de umbral de rendimiento definidas por el usuario que activan eventos y envían alertas por correo electrónico cuando se incumplen los umbrales.
- Utiliza umbrales definidos por el sistema y umbrales de rendimiento dinámicos que aprenden acerca de la actividad de la carga de trabajo para identificar y avisarle de problemas de rendimiento.
- Identifica las políticas de calidad de servicio (QoS) y las políticas de nivel de servicio (PSU) de rendimiento que se aplican a los volúmenes y las LUN.
- Identifica claramente el componente del clúster que está en disputa.
- Identifica cargas de trabajo que utilizan en exceso los componentes del clúster y las cargas de trabajo cuyo rendimiento se ve afectado por la mayor actividad.

Las interfaces de Unified Manager que se utilizan para gestionar el rendimiento del sistema de almacenamiento

Estas secciones contienen información acerca de las dos interfaces de usuario que Active IQ Unified Manager proporciona para la solución de problemas de capacidad de almacenamiento de datos, disponibilidad y protección. Las dos IU son la interfaz de usuario web de Unified Manager y la consola de mantenimiento.

Si desea utilizar las funciones de protección en Unified Manager, también debe instalar y configurar OnCommand Workflow Automation (WFA).

Interfaz de usuario web de Unified Manager

La interfaz de usuario web de Unified Manager permite a un administrador supervisar y solucionar los problemas de los clústeres relacionados con la capacidad de almacenamiento de datos, la disponibilidad y la protección.

Estas secciones describen algunos flujos de trabajo comunes que un administrador puede seguir para solucionar problemas de capacidad de almacenamiento, disponibilidad de datos o protección que se muestran en la interfaz de usuario web de Unified Manager.

Consola de mantenimiento

La consola de mantenimiento de Unified Manager permite a un administrador supervisar, diagnosticar y solucionar problemas del sistema operativo, problemas de actualización de la versión, problemas de acceso del usuario y problemas de red relacionados con el propio servidor de Unified Manager. Si la interfaz de usuario web de Unified Manager no está disponible, la consola de mantenimiento es el único formato de acceso a Unified Manager.

Puede usar esta información para acceder a la consola de mantenimiento y utilizarla para resolver los problemas relacionados con el funcionamiento del servidor de Unified Manager.

Actividad de recogida de datos de rendimiento y configuración del clúster

El intervalo de recopilación para *cluster Configuration data* es de 15 minutos. Por ejemplo, después de agregar un clúster, tarda 15 minutos en mostrar los detalles del clúster en la interfaz de usuario de Unified Manager. Este intervalo se aplica cuando se realizan cambios también en un clúster.

Por ejemplo, si se añaden dos volúmenes nuevos a una SVM de un clúster, se ven esos objetos nuevos en la interfaz de usuario después del siguiente intervalo de sondeo, que podría ser de hasta 15 minutos.

Unified Manager recopila las *estadísticas de rendimiento* actuales de todos los clústeres supervisados cada cinco minutos. Analiza estos datos para identificar eventos de rendimiento y problemas potenciales. Conserva 30 días de datos de rendimiento históricos de cinco minutos y 180 días de datos de rendimiento históricos de una hora. Esto permite ver detalles de rendimiento muy granulares para el mes actual y las tendencias generales de rendimiento de hasta un año.

Los sondeos de recogida se compensan por unos minutos para que los datos de cada clúster no se envíen al mismo tiempo, lo que podría afectar al rendimiento.

En la siguiente tabla se describen las actividades de recogida que Unified Manager realiza:

Actividad	Intervalo de tiempo	Descripción
Sondeo de estadísticas de rendimiento	Cada 5 minutos	Recopila datos de rendimiento en tiempo real de cada clúster.
Análisis estadístico	Cada 5 minutos	Después de cada sondeo de las estadísticas, Unified Manager compara los datos recopilados con los umbrales definidos por el usuario, definidos por el sistema y dinámicos. Si se ha incumplido algún umbral de rendimiento, Unified Manager genera eventos y envía un correo electrónico a los usuarios especificados, si se han configurado para hacerlo.
Sondeo de configuración	Cada 15 minutos	Recopila información detallada de inventario de cada clúster para identificar todos los objetos de almacenamiento (nodos, SVM, volúmenes, etc.).
Resumen	Cada hora	Resume las últimas 12 recopilaciones de datos de rendimiento de cinco minutos en promedios por hora. Los valores promedio por hora se usan en algunas de las páginas de la interfaz de usuario y se conservan durante 180 días.

Actividad	Intervalo de tiempo	Descripción
Análisis de previsión y eliminación de datos	Todos los días después de medianoche	Analiza datos de clúster para establecer umbrales dinámicos para la latencia de volúmenes y IOPS en las próximas 24 horas. Elimina de la base de datos los datos los datos de rendimiento de cinco minutos que tengan más de 30 días.
Eliminar datos	Todos los días después de las 2 de la mañana	Elimina de la base de datos todos los eventos anteriores a 180 días y los umbrales dinámicos mayores de 180 días.
Eliminar datos	Todos los días después de las 3:30 a.m.	Elimina de la base de datos todos los datos de rendimiento de una hora que tengan más de 180 días.

Qué es un ciclo de recopilación de continuidad de datos

Un ciclo de recopilación de continuidad de datos recupera datos de rendimiento fuera del ciclo de recopilación de rendimiento del clúster en tiempo real que se ejecuta, de forma predeterminada, cada cinco minutos. Las recopilaciones de continuidad de datos permiten a Unified Manager llenar los vacíos de datos estadísticos que se producen cuando no pudo recopilar datos en tiempo real.

Unified Manager realiza encuestas de recogida de continuidad de datos de datos históricos de rendimiento cuando se producen los siguientes eventos:

- Inicialmente, un clúster se añade a Unified Manager.

  Unified Manager recopila datos de rendimiento históricos de los 15 días anteriores. Esto le permite ver dos semanas de información histórica sobre el rendimiento de un clúster unas horas después de agregar.

  Además, si existe alguno, se notifican los eventos de umbral definidos por el sistema durante el período anterior.

- El ciclo de recogida de datos de rendimiento actual no termina a tiempo.

  Si el sondeo de rendimiento en tiempo real supera el período de recopilación de cinco minutos, se inicia un ciclo de recopilación de continuidad de datos para recopilar esa información que falta. Sin la recopilación de continuidad de datos, se omite el siguiente período de recopilación.

- Unified Manager no se ha podido acceder durante un periodo de tiempo y vuelve a estar en línea, como en las siguientes situaciones:
  - Se ha reiniciado.
  - Se cerró durante una actualización de software o al crear un archivo de copia de seguridad.

    - Se repara una interrupción de la red.
- Un clúster ha sido inaccesible durante un periodo de tiempo y después vuelve a estar en línea, como en las siguientes situaciones:
    - Se repara una interrupción de la red.
    - Una conexión de red de área amplia lenta retrasó la recopilación normal de datos de rendimiento.

Un ciclo de recogida de continuidad de datos puede recopilar un máximo de 24 horas de datos históricos. Si Unified Manager se reduce durante más de 24 horas, se muestra una brecha en los datos de rendimiento en las páginas de interfaz de usuario.

Un ciclo de recopilación de continuidad de datos y un ciclo de recopilación de datos en tiempo real no se pueden ejecutar al mismo tiempo. El ciclo de recopilación de continuidad de datos debe finalizar antes de que se inicie la recopilación de datos de rendimiento en tiempo real. Cuando se necesita la recogida de continuidad de datos para recopilar más de una hora de datos históricos, aparece un mensaje de banner para ese clúster en la parte superior del panel Notificaciones.

Lo que significa la Marca de hora en los datos y eventos recopilados

La Marca de hora que aparece en los datos de estado y rendimiento recopilados, o que aparece como hora de detección de un evento, se basa en la hora del clúster de ONTAP, ajustada a la zona horaria establecida en el explorador web.

Se recomienda usar un servidor de protocolo de tiempo de redes (NTP) para sincronizar la hora en los servidores de Unified Manager, en los clústeres de ONTAP y en los exploradores web.

Si ve marcas de tiempo que buscan incorrectas para un clúster determinado, quizás desee comprobar que la hora del clúster se ha establecido correctamente.

Navegar por los flujos de trabajo de rendimiento en la interfaz gráfica de usuario de Unified Manager

La interfaz de Unified Manager proporciona muchas páginas para la recogida y visualización de información de rendimiento. Utilice el panel de navegación izquierdo para desplazarse a las páginas de la GUI y utilice fichas y vínculos de las páginas para ver y configurar información.

Se utilizan todas las siguientes páginas para supervisar y solucionar problemas con la información de rendimiento del clúster:

- consola
- páginas de inventario de objetos de red y almacenamiento
- páginas de detalles de objetos de almacenamiento (incluido el explorador de rendimiento)
- páginas de configuración y configuración
- páginas de eventos

Iniciar sesión en la interfaz de usuario de

Puede iniciar sesión en la interfaz de usuario de Unified Manager mediante un explorador web compatible.

Lo que necesitará

- El navegador web debe cumplir los requisitos mínimos.

  Consulte la matriz de interoperabilidad en "mysupport.netapp.com/matrix" para ver la lista completa de versiones compatibles del navegador.

- Debe tener la dirección IP o la URL del servidor de Unified Manager.

Se cerrará automáticamente la sesión después de 1 hora de inactividad. Este periodo de tiempo se puede configurar en **General** > **Configuración de funciones**.

Pasos

1. Introduzca la URL en el explorador web, donde URL es la dirección IP o el nombre de dominio completo (FQDN) de Unified Manager Server:
   - Para IPv4: `https://URL/`
   - Para IPv6: `https://[URL]/`

Si el servidor utiliza un certificado digital autofirmado, es posible que el explorador muestre una advertencia que indica que el certificado no es de confianza. Puede reconocer el riesgo de continuar con el acceso o instalar un certificado digital firmado por una entidad de certificación (CA) para la autenticación del servidor. . En la pantalla de inicio de sesión, introduzca su nombre de usuario y contraseña.

Si el inicio de sesión en la interfaz de usuario de Unified Manager se protege mediante la autenticación SAML, se deben introducir las credenciales en la página de inicio de sesión del proveedor de identidades (IDP) en lugar de la página de inicio de sesión de Unified Manager.

Aparecerá la página Dashboard.

> Si no se inicializa Unified Manager Server, una nueva ventana del navegador muestra el asistente First Experience. Es necesario introducir un destinatario de correo electrónico inicial para el cual se enviarán las alertas por correo electrónico, el servidor SMTP que se encargará de las comunicaciones por correo electrónico y si AutoSupport está habilitado para enviar información sobre la instalación de Unified Manager al soporte técnico. La interfaz de usuario de Unified Manager se muestra después de completar esta información.

Interfaz gráfica y rutas de navegación

Unified Manager cuenta con una gran flexibilidad y permite realizar varias tareas de distintas formas. Existen muchas rutas de navegación que se detectarán cuando trabaje en Unified Manager. Aunque no se pueden mostrar todas las combinaciones posibles de navegaciones, debería estar familiarizado con algunos de los escenarios más comunes.

Supervise la navegación de objetos del clúster

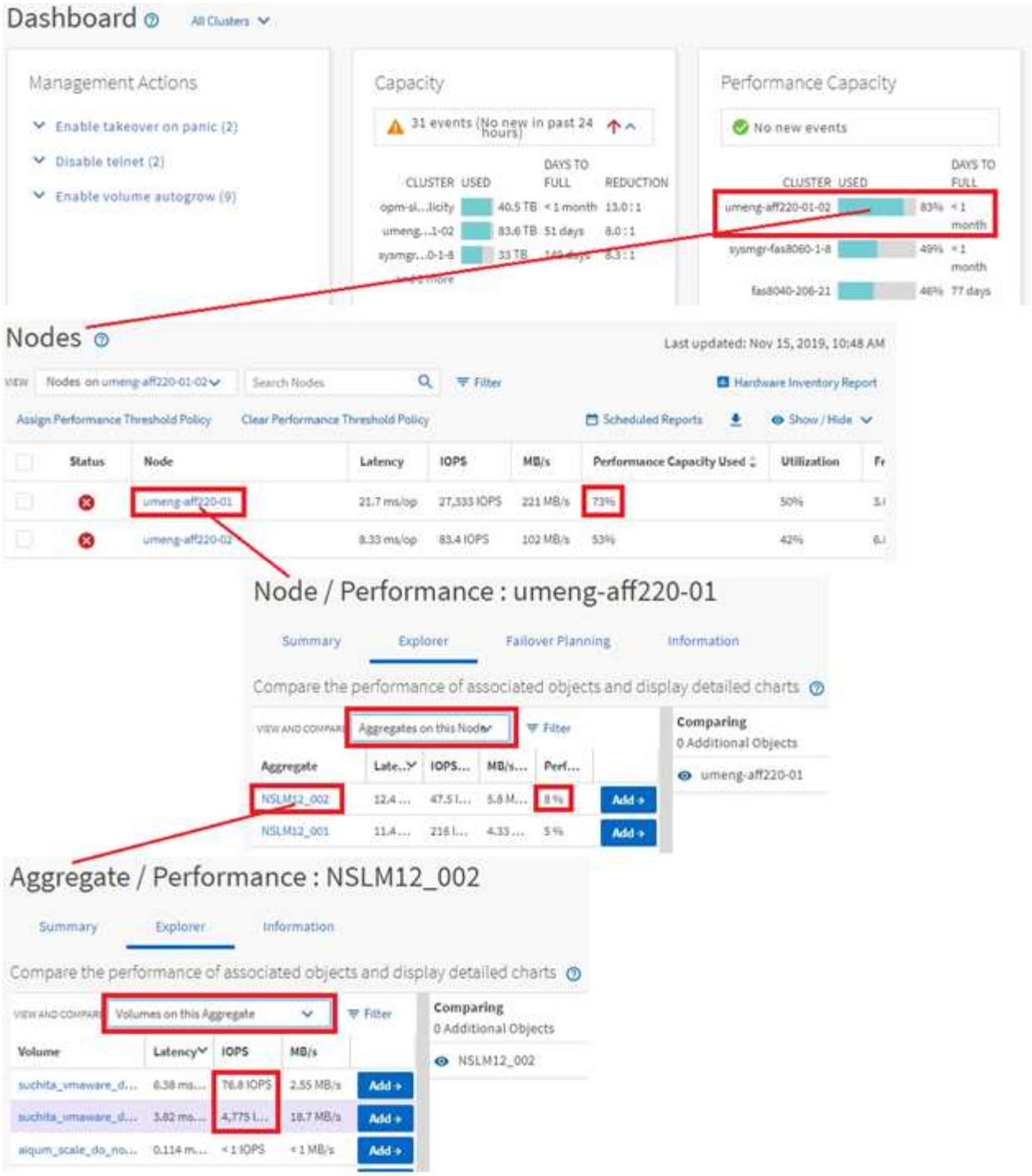
Es posible supervisar el rendimiento de todos los objetos en cualquier clúster gestionado

por Unified Manager. La supervisión de objetos de almacenamiento le proporciona una descripción general del rendimiento del clúster y los objetos, e incluye supervisión de eventos de rendimiento. Es posible ver los eventos y el rendimiento a un nivel alto o estudiar aún más detalles sobre los eventos de rendimiento y rendimiento de objetos.

Este es un ejemplo de muchas posibles navegaciones de objetos de clúster:

1. En la página Dashboard, revise los detalles en el panel rendimiento capacidad para identificar el clúster que utiliza la mayor capacidad de rendimiento y haga clic en el gráfico de barras para ir a la lista de nodos de ese clúster.
2. Identifique el nodo con el valor de capacidad de rendimiento más alto usado y haga clic en ese nodo.
3. En la página Explorador de nodos / rendimiento, haga clic en **agregados en este nodo** en el menú Ver y comparar.
4. Identifique el agregado que utiliza la mayor capacidad de rendimiento y haga clic en ese agregado.
5. En la página Aggregate / Performance Explorer, haga clic en **Volumes on this aggregate** en el menú View and Compare.
6. Identifique los volúmenes que utilizan más IOPS.

Debe investigar estos volúmenes para ver si debe aplicar una política de calidad de servicio o una política de nivel de servicio de rendimiento, o cambiar la configuración de la política, de modo que esos volúmenes no usen un porcentaje de IOPS tan grande en el clúster.



Supervise la navegación del rendimiento del clúster

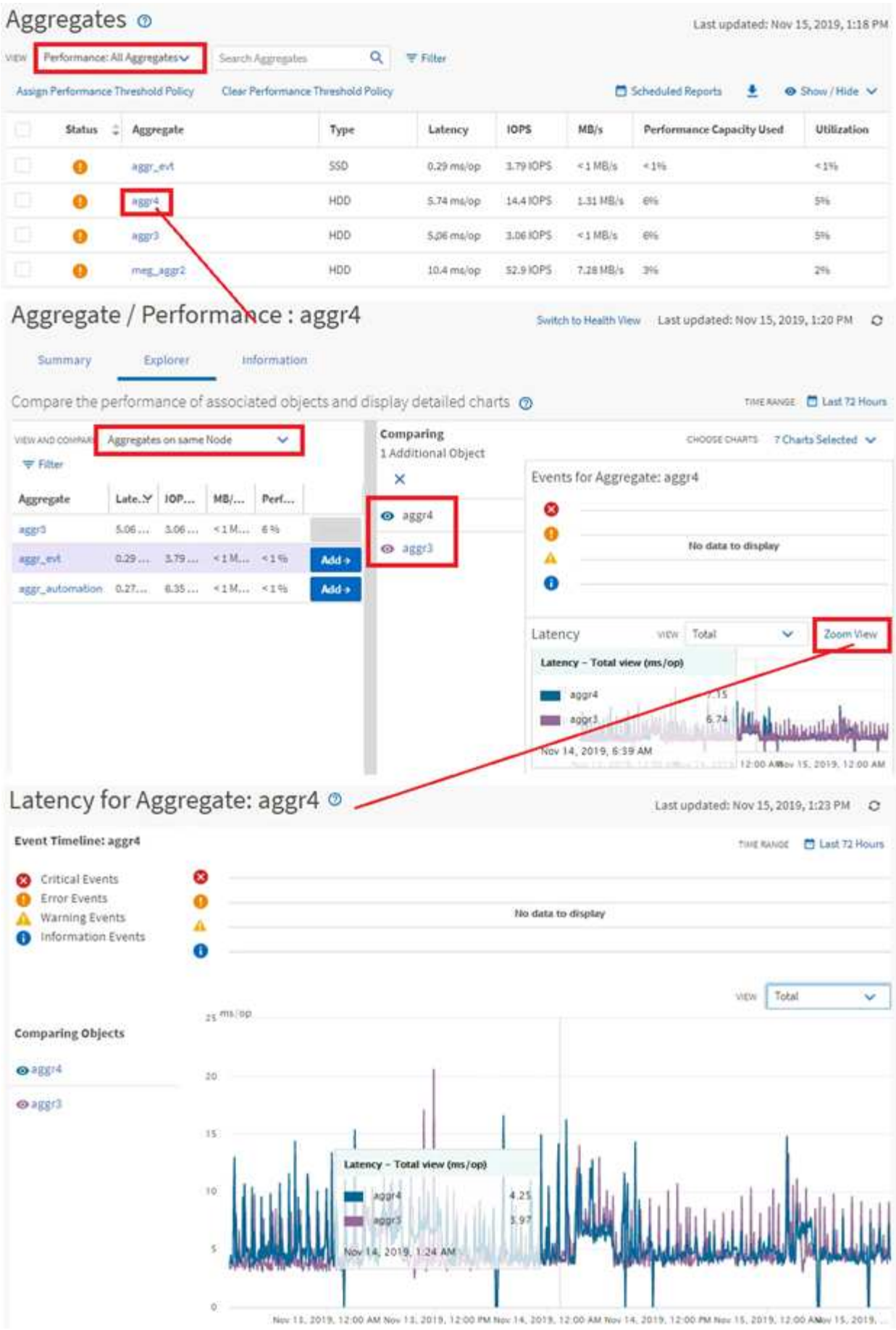
Es posible supervisar el rendimiento de todos los clústeres gestionados por Unified Manager. La supervisión de los clústeres ofrece una descripción general del rendimiento del clúster y el objeto, e incluye supervisión de eventos de rendimiento. Es posible ver los eventos y el rendimiento a un nivel alto o bien investigar más sobre cualquier detalle de los eventos de rendimiento y rendimiento de objetos y clústeres.

Este es un ejemplo de muchas posibles rutas de navegación del rendimiento del clúster:

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **agregados**.
2. Para ver información sobre el rendimiento de esos agregados, seleccione la vista rendimiento: All Aggregates.
3. Identifique el agregado que desea investigar y haga clic en el nombre del agregado para desplazarse a la página Aggregate / Performance Explorer.
4. Opcionalmente, seleccione otros objetos para comparar con este agregado en el menú Ver y comparar y, a continuación, agregue uno de los objetos al panel comparación.

   Las estadísticas de ambos objetos aparecerán en los gráficos de contadores para realizar la comparación.

5. En el panel de comparación situado a la derecha de la página del explorador, haga clic en **Zoom View** en uno de los gráficos de contadores para ver detalles sobre el historial de rendimiento de ese agregado.


Aggregates
Last updated: Nov 15, 2019, 1:18 PM
VIEW
Performance: All Aggregates
Search Aggregates
Filter
Assign Performance Threshold Policy
Clear Performance Threshold Policy
Scheduled Reports
Show / Hide
Status
Aggregate
Type
Latency
IOPS
MB/s
Performance Capacity Used
Utilization
aggr_evt
SSD
0.29 ms/op
3.79 IOPS
< 1 MB/s
< 1%
aggr4
HDD
5.74 ms/op
14.4 IOPS
1.31 MB/s
6%
5%
aggr3
HDD
5.06 ms/op
3.06 IOPS
< 1 MB/s
6%
5%
meg_aggr2
HDD
10.4 ms/op
52.9 IOPS
7.28 MB/s
3%
2%
Aggregate / Performance : aggr4
Switch to Health View
Last updated: Nov 15, 2019, 1:20 PM
Summary
Explorer
Information
Compare the performance of associated objects and display detailed charts
TIME RANGE
Last 72 Hours
VIEW AND COMPARE
Aggregates on same Node
Filter
Aggregate
Late...
IOP...
MB/...
Perf...
aggr3
5.06 ...
3.06 ...
< 1 M...
6 %
aggr_evt
0.29 ...
3.79 ...
< 1 M...
< 1 %
Add
aggr_automation
0.27...
6.35 ...
< 1 M...
< 1 %
Add
Comparing
1 Additional Object
CHOOSE CHARTS
7 Charts Selected
aggr4
aggr3
Events for Aggregate: aggr4
No data to display
Latency
VIEW
Total
Zoom View
Latency – Total view (ms/op)
aggr4
7.15
aggr3
6.74
Nov 14, 2019, 6:39 AM
12:00 AM
Nov 15, 2019, 12:00 AM
Latency for Aggregate: aggr4
Last updated: Nov 15, 2019, 1:23 PM
Event Timeline: aggr4
TIME RANGE
Last 72 Hours
Critical Events
Error Events
Warning Events
Information Events
No data to display
VIEW
Total
Comparing Objects
aggr4
aggr3
ms/op
25
20
15
10
5
0
Latency – Total view (ms/op)
aggr4
4.25
aggr3
3.97
Nov 14, 2019, 1:24 AM
Nov 13, 2019, 12:00 AM
Nov 13, 2019, 12:00 PM
Nov 14, 2019, 12:00 AM
Nov 14, 2019, 12:00 PM
Nov 15, 2019, 12:00 AM
Nov 15, 2019,

Navegación de investigación de eventos

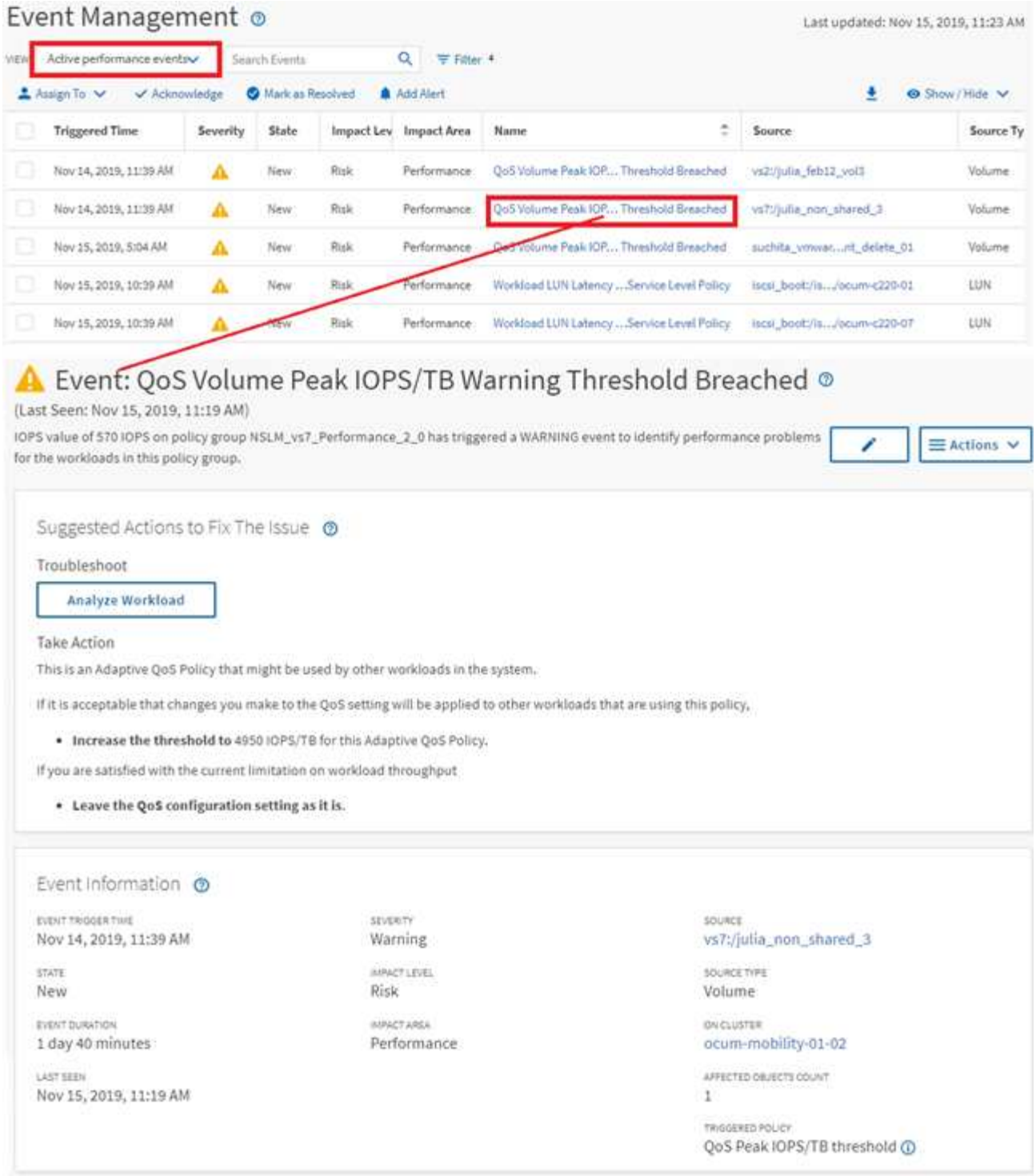
Las páginas de detalles de eventos de Unified Manager le ofrecen una perspectiva en profundidad de cualquier evento de rendimiento. Esto resulta beneficioso cuando se analizan eventos de rendimiento, cuando se realiza la solución de problemas y cuando se perfecciona el rendimiento del sistema.

Según el tipo de evento de rendimiento, es posible que vea uno de dos tipos de páginas de detalles de eventos:

- Página de detalles Event para eventos definidos por el usuario y definidos por el sistema
- Página de detalles Event para eventos de política de umbral dinámico

Este es un ejemplo de una navegación de investigación de eventos.

1. En el panel de navegación izquierdo, haga clic en **Gestión de eventos**.
2. En el menú Ver, haga clic en **Eventos de rendimiento activos**.
3. Haga clic en el nombre del evento que desea investigar y se mostrará la página de detalles Event.
4. Vea la Descripción del evento y revise las acciones sugeridas (si están disponibles) para ver más detalles sobre el evento que puede ayudarle a resolver el problema. Puede hacer clic en el botón **analizar carga de trabajo** para mostrar gráficos de rendimiento detallados que le ayudarán a analizar el problema.



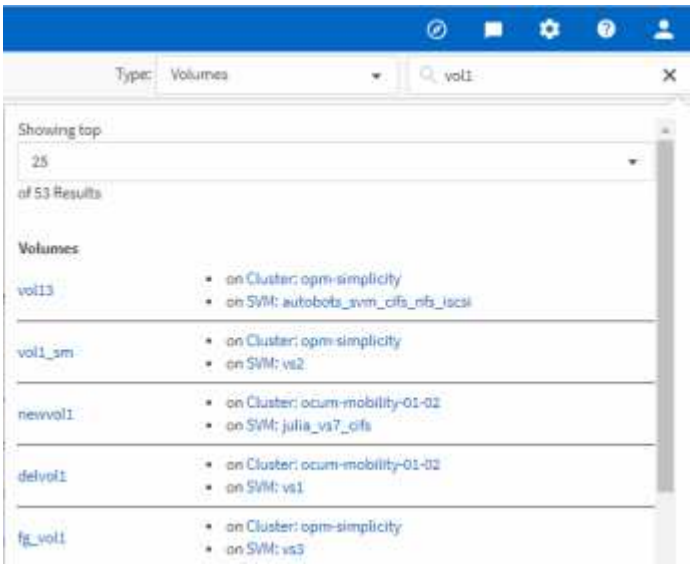
Buscar objetos de almacenamiento

Para acceder rápidamente a un objeto específico, puede utilizar el campo **Buscar todos los objetos de almacenamiento** situado en la parte superior de la barra de menús. Este método de búsqueda global en todos los objetos le permite localizar rápidamente objetos específicos por tipo. Los resultados de búsqueda se ordenan por tipo de objeto de almacenamiento y se pueden filtrar mediante el menú desplegable. Una búsqueda válida debe contener al menos tres caracteres.

La búsqueda global muestra el número total de resultados, pero sólo se puede acceder a los 25 resultados de búsqueda principales. Debido a esto, la funcionalidad de búsqueda global se puede considerar como una herramienta de acceso directo para buscar elementos específicos si conoce los elementos que desea localizar rápidamente. Para obtener resultados completos de la búsqueda, puede utilizar la búsqueda en las páginas de inventario de objetos y su funcionalidad de filtrado asociada.

Puede hacer clic en el cuadro desplegable y seleccionar **todo** para buscar simultáneamente en todos los objetos y eventos. También puede hacer clic en el cuadro desplegable para especificar el tipo de objeto. Escriba un mínimo de tres caracteres del nombre del objeto o evento en el campo **Buscar todos los objetos de almacenamiento** y, a continuación, pulse **Intro** para mostrar los resultados de la búsqueda, como:

- Cluster: Nombres de clúster
- Nodes: Nombres de nodos
- Agregados: Nombres de agregados
- SVM: Nombres de SVM
- Volúmenes: Nombres de volúmenes
- LUN: Rutas de LUN



Los LIF y puertos no pueden realizar búsquedas en la barra de búsqueda global.

En este ejemplo, el cuadro desplegable tiene el tipo de objeto Volume seleccionado. Al escribir "'vol'" en el campo **Buscar todos los objetos de almacenamiento** se muestra una lista de todos los volúmenes cuyos nombres contienen estos caracteres. En el caso de las búsquedas de objetos, puede hacer clic en cualquier resultado de búsqueda para desplazarse a la página Performance Explorer del objeto. Para las búsquedas de eventos, al hacer clic en un elemento del resultado de búsqueda se desplaza a la página Detalles del evento.

Filtrado del contenido de la página de inventario

Puede filtrar los datos de las páginas de inventario en Unified Manager para localizar rápidamente datos según criterios específicos. Puede utilizar el filtrado para limitar el contenido de las páginas de Unified Manager a fin de mostrar únicamente los resultados de los que está interesado. Esto proporciona un método muy eficiente para mostrar sólo los datos en los que usted está interesado.

Utilice **filtrado** para personalizar la vista de cuadrícula en función de sus preferencias. Las opciones de filtro disponibles se basan en el tipo de objeto que se está viendo en la cuadrícula. Si se aplican filtros actualmente, el número de filtros aplicados se muestra a la derecha del botón filtro.

Se admiten tres tipos de parámetros de filtro.

Parámetro	**Validación**
Cadena (texto)	Los operadores son **contiene**, **comienza con**, **termina con** y **no contiene**.
Número	Los operadores son **superiores a**, **inferiores a**, **en el último** y **entre**.
Enumeración (texto)	Los operadores son **is** y **no**.

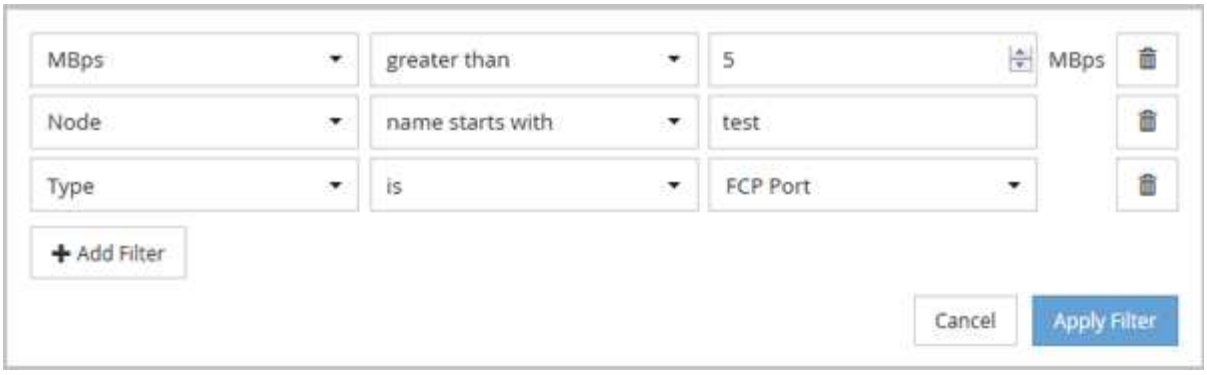
Los campos columna, operador y valor son necesarios para cada filtro; los filtros disponibles reflejan las columnas filtrables en la página actual. El número máximo de filtros que puede aplicar es cuatro. Los resultados filtrados se basan en parámetros de filtro combinados. Los resultados filtrados se aplican a todas las páginas de la búsqueda filtrada, no sólo a la página mostrada actualmente.

Puede agregar filtros mediante el panel filtrado.

1. En la parte superior de la página, haga clic en el botón **filtro**. Aparecerá el panel filtrado.
2. Haga clic en la lista desplegable que se encuentra a la izquierda y seleccione un objeto; por ejemplo, *Cluster* o un contador de rendimiento.
3. Haga clic en la lista desplegable Centro y seleccione el operador que desee utilizar.
4. En la última lista, seleccione o escriba un valor para completar el filtro de ese objeto.
5. Para agregar otro filtro, haga clic en **+Agregar filtro**. Aparecerá un campo de filtro adicional. Complete este filtro utilizando el proceso descrito en los pasos anteriores. Tenga en cuenta que al agregar el cuarto filtro, el botón **+Agregar filtro** ya no aparece.
6. Haga clic en **aplicar filtro**. Las opciones de filtro se aplican a la cuadrícula y el número de filtros se muestra a la derecha del botón filtro.
7. Utilice el panel filtrado para eliminar filtros individuales haciendo clic en el icono de papelera situado a la derecha del filtro que se va a eliminar.
8. Para eliminar todos los filtros, haga clic en **Restablecer** en la parte inferior del panel de filtrado.

Ejemplo de filtrado

La ilustración muestra el panel filtrado con tres filtros. El botón **+Add Filter** aparece cuando tiene menos de cuatro filtros como máximo.



Después de hacer clic en **aplicar filtro**, el panel filtrado se cierra, aplica los filtros y muestra el número de filtros aplicados (3).

Supervisar el rendimiento del clúster en la consola de

La consola de Unified Manager proporciona algunos paneles que muestran el estado de rendimiento de alto nivel de todos los clústeres que supervisa esta instancia de Unified Manager. Le permite evaluar el rendimiento general de los clústeres gestionados y anotar, localizar o asignar rápidamente para solucionar cualquier evento específico identificado.

Descripción de los paneles de rendimiento de la consola

La consola de Unified Manager proporciona algunos paneles que muestran el estado de rendimiento de alto nivel para todos los clústeres que se supervisan en el entorno. Puede elegir ver el estado de todos los clústeres o de un clúster individual.

Además de mostrar la información de rendimiento, la mayoría de los paneles también muestran el número de eventos activos de esa categoría y el número de eventos nuevos añadidos durante las 24 horas anteriores. Esta información le ayuda a decidir qué clústeres se podrían necesitar para analizar más a fin de resolver los eventos notificados. Al hacer clic en los eventos, se muestran los primeros eventos y se proporciona un enlace a la página del inventario Event Management filtrada para mostrar los eventos de esa categoría.

Los siguientes paneles proporcionan el estado del rendimiento.

- **Panel de capacidad de rendimiento**

  Cuando se visualizan todos los clústeres, este panel muestra el valor de capacidad de rendimiento de cada clúster (promediado en la 1 hora anterior) y el número de días hasta que la capacidad de rendimiento alcance el límite superior (según la tasa de crecimiento diaria). Al hacer clic en el gráfico de barras, irá la página del inventario de nodos de ese clúster. Tenga en cuenta que la página del inventario de nodos muestra la capacidad de rendimiento media durante las 72 horas anteriores, de modo que es posible que este valor no coincida con el valor del panel.

  Al ver un único clúster, este panel muestra la capacidad de rendimiento del clúster, las IOPS totales y los valores de rendimiento totales.

- **Panel de IOPS de carga de trabajo**

  Cuando se habilita la gestión de cargas de trabajo activas y, al ver un solo clúster, este panel muestra el

número total de cargas de trabajo que se están ejecutando actualmente en un determinado rango de IOPS.

- **Panel de rendimiento de carga de trabajo**

  Cuando la gestión activa de la carga de trabajo está habilitada, este panel muestra el número total de cargas de trabajo conformes y no conformes asignadas a cada nivel de servicio de rendimiento definido. Al hacer clic en un gráfico de barras se llevan a las cargas de trabajo asignadas a esa política en la página cargas de trabajo.

- **Panel de visión general del uso**

  Cuando se ven todos los clústeres, es posible ver clústeres ordenados por mayor IOPS o rendimiento (MB/s).

  Al ver un único clúster, puede elegir ver cargas de trabajo en ese clúster ordenadas por IOPS o rendimiento (MB/s) más alto.

Mensajes y descripciones de banner de rendimiento

Unified Manager puede mostrar mensajes de banner en la página Notificaciones (de la campana de notificación) para alertarle de los problemas de estado de un clúster en particular.

Mensaje de banner	Descripción	Resolución
`No performance data is being collected from cluster` *`cluster_name`*`. Restart Unified Manager to correct this issue.`	El servicio de recogida de Unified Manager se ha detenido y no se recopilan datos de rendimiento de ningún clúster.	Reinicie Unified Manager para corregir este problema. Si esto no corrige el problema, póngase en contacto con el soporte técnico.
`More than x hour(s) of historical data is being collected from cluster` *`cluster_name`*`. Current data collections will start after all historical data is collected.`	Actualmente se ejecuta un ciclo de recogida de continuidad de datos para recuperar datos de rendimiento fuera del ciclo de recogida de rendimiento de clúster en tiempo real.	No se requiere ninguna acción. Los datos de rendimiento actuales se recogerán una vez completado el ciclo de recopilación de continuidad de datos. Un ciclo de recogida de continuidad de datos se ejecuta cuando se añade un nuevo clúster o cuando Unified Manager no pudo recoger los datos de rendimiento actuales por algún motivo.

Cambiar el intervalo de recogida de estadísticas de rendimiento

El intervalo de recogida predeterminado para las estadísticas de rendimiento es de 5 minutos. Puede cambiar este intervalo a 10 o 15 minutos si descubre que las colecciones de clústeres grandes no están finalizando dentro del tiempo predeterminado. Esta configuración afecta la recogida de estadísticas de todos los clústeres que está

supervisando esta instancia de Unified Manager.

Lo que necesitará

Debe tener un ID de usuario y una contraseña autorizados para iniciar sesión en la consola de mantenimiento del servidor de Unified Manager.

La emisión de colecciones de estadísticas de rendimiento no terminado a tiempo se indica mediante los mensajes de mensaje de cabecera `Unable to consistently collect from cluster <cluster_name>` o. `Data collection is taking too long on cluster <cluster_name>`.

Debe cambiar el intervalo de recopilación sólo cuando sea necesario debido a un problema de recopilación de estadísticas. No cambie esta configuración por ningún otro motivo.

> Si se cambia este valor desde el ajuste predeterminado de 5 minutos, puede afectar el número y la frecuencia de los eventos de rendimiento que informa Unified Manager. Por ejemplo, los umbrales de rendimiento definidos por el sistema activan eventos cuando se supera la política durante 30 minutos. Cuando se utilizan colecciones de 5 minutos, se debe superar la política para seis colecciones consecutivas. Para las colecciones de 15 minutos, la directiva debe superarse sólo durante dos períodos de recopilación.

Un mensaje en la parte inferior de la página Cluster Setup indica el intervalo de recogida de datos estadísticos actual.

Pasos

1. Inicie sesión con SSH como usuario de mantenimiento en el host de Unified Manager.

   Se muestran los avisos de la consola de mantenimiento de Unified Manager.

2. Escriba el número de la opción de menú con la etiqueta **Configuración del intervalo de sondeo de rendimiento** y, a continuación, pulse Intro.
3. Si se le solicita, vuelva a introducir la contraseña de usuario de mantenimiento.
4. Escriba el número del nuevo intervalo de sondeo que desea establecer y, a continuación, pulse Intro.

Si cambió el intervalo de recogida de Unified Manager a 10 o 15 minutos y tiene una conexión actual con un proveedor de datos externo (como Graphite), debe cambiar el intervalo de transmisión del proveedor de datos de modo que sea igual o mayor que el intervalo de recogida de Unified Manager.

Solucionar problemas de cargas de trabajo mediante el analizador de cargas de trabajo

El analizador de cargas de trabajo proporciona una forma de ver criterios importantes de estado y rendimiento para una única carga de trabajo en una sola página, con el fin de ayudar a resolver problemas. Al ver todos los eventos actuales y anteriores de una carga de trabajo, se puede obtener una mejor idea de por qué la carga de trabajo puede tener un problema de rendimiento o capacidad ahora.

El uso de esta herramienta también puede ayudarle a determinar si el almacenamiento es la causa de cualquier problema de rendimiento de una aplicación o si el problema está causado por una red u otro problema relacionado.

Puede iniciar esta funcionalidad desde varios lugares de la interfaz de usuario:

- En la selección Workload Analysis (Análisis de carga de trabajo) del menú de navegación izquierdo
- En la página Detalles del evento, haga clic en el botón **analizar carga de trabajo**
- Desde cualquier página de inventario de cargas de trabajo (volumen, LUN, carga de trabajo, recursos compartidos NFS o recursos compartidos SMB/CIFS), haciendo clic en el icono más , Luego **analizar la carga de trabajo**
- En la página Virtual Machines, haga clic en el botón **analizar carga de trabajo** de cualquier objeto Datastore

Al iniciar la herramienta desde el menú de navegación izquierdo, puede introducir el nombre de cualquier carga de trabajo que desee analizar y seleccionar el intervalo de tiempo para el que desea solucionar problemas. Cuando se inicia la herramienta desde cualquiera de las páginas de carga de trabajo o de inventario de máquinas virtuales, el nombre de la carga de trabajo se rellena automáticamente y los datos de la carga de trabajo se presentan con el intervalo de tiempo predeterminado de 2 horas. Cuando se inicia la herramienta desde la página de detalles Event, el nombre de la carga de trabajo se rellena automáticamente y se muestran los datos de 10 días.

¿Qué datos muestra el analizador de cargas de trabajo

La página del analizador de cargas de trabajo muestra información sobre los eventos actuales que podrían afectar a la carga de trabajo, recomendaciones para resolver potencialmente el problema que causa el evento y gráficos para analizar el historial de rendimiento y capacidad.

En la parte superior de la página, se debe especificar el nombre de la carga de trabajo (volumen o LUN) que se desea analizar y el período de tiempo sobre el que se desean ver las estadísticas. Puede cambiar el período de tiempo en cualquier momento si desea ver un período de tiempo más corto o más largo.

Las otras áreas de la página muestran los resultados del análisis y los gráficos de rendimiento y capacidad.

> Los gráficos de cargas de trabajo de las LUN no proporcionan el mismo nivel de estadísticas que esos gráficos de los volúmenes, por lo que notará diferencias al analizar estos dos tipos de cargas de trabajo.

- **Área de resumen de eventos**

  Muestra una breve descripción general del número y los tipos de eventos que se han producido a lo largo del periodo de tiempo. Cuando existen eventos de diferentes áreas de impacto (por ejemplo, rendimiento y capacidad), se muestra esta información para poder seleccionar detalles del tipo de evento en el que está interesado. Haga clic en el tipo de evento para ver una lista de los nombres de evento.

  Si solo hay un evento durante el periodo de tiempo, en algunos eventos se muestra una lista de recomendaciones para corregir el problema.

- **Línea de tiempo del evento**

  Muestra todas las ocurrencias de eventos durante el periodo especificado. Pase el cursor sobre cada evento para ver el nombre del evento.

  Si ha llegado a esta página haciendo clic en el botón **analizar carga de trabajo** de la página Detalles del evento, el icono del evento seleccionado aparece más grande para poder identificar el evento.

- **Área de gráficos de rendimiento**

  Muestra gráficos de latencia, rendimiento (tanto IOPS como MB/s) y aprovechamiento (tanto para el nodo como para el agregado) en función del periodo de tiempo seleccionado. Puede hacer clic en el enlace Ver detalles de rendimiento para mostrar la página Performance Explorer de la carga de trabajo, en caso de que desea realizar más análisis.

  - **Latencia** muestra la latencia de la carga de trabajo en el periodo de tiempo seleccionado. El gráfico tiene tres vistas que le permiten ver:
    - **Latencia total**
    - **Interrupción** de la latencia (desglosada por lecturas, escrituras y otros procesos)
    - **Latencia de los componentes del clúster** (se ha roto por el componente del clúster)

Consulte "Los componentes del clúster y el motivo por los que pueden estar en contención" para obtener una descripción de los componentes del clúster que se muestran aquí. **Rendimiento muestra tanto IOPS como MB/s de rendimiento para la carga de trabajo durante el periodo de tiempo seleccionado. El gráfico tiene cuatro vistas que le permiten ver:** * **Total** rendimiento *** desglose rendimiento (dividido por lecturas, escrituras y otros procesos)** * **rendimiento de la nube** (los MB/s que se utilizan para escribir datos y leer datos de la nube; Para las cargas de trabajo que están organizando en niveles la capacidad en el cloud) *** IOPS con Forecast (una predicción de los valores de rendimiento de IOPS superior e inferior esperados en el período de tiempo) este gráfico también muestra los ajustes del umbral de rendimiento máximo y mínimo de calidad de servicio (QoS), si se han configurado, Puede ver dónde se puede encontrar que el sistema limite el rendimiento de forma intencionada con políticas de calidad de servicio. Utilización** muestra la utilización tanto para el agregado como para el nodo en el que se ejecuta la carga de trabajo durante el periodo de tiempo seleccionado. A partir de aquí puede ver si su agregado o nodo está sobrecargado, lo que puede causar una alta latencia. Al analizar volúmenes FlexGroup, en los gráficos de uso aparecen varios nodos y varios agregados.

- * Área de la carta de capacidad*

  Muestra gráficos de la capacidad de datos y la capacidad de Snapshot de los últimos un mes de la carga de trabajo.

  Para los volúmenes, es posible hacer clic en el enlace Ver detalles de capacidad para mostrar la página Health Details de la carga de trabajo en caso de que desea realizar más análisis. Las LUN no proporcionan este enlace porque no hay ninguna página Health Details para las LUN.

  - **Vista de capacidad** muestra el espacio total disponible asignado para la carga de trabajo y el espacio lógico utilizado (después de todas las optimizaciones de NetApp).
  - **Vista de instantánea** muestra el espacio total reservado para copias Snapshot y la cantidad de espacio que se está utilizando actualmente. Tenga en cuenta que las LUN no proporcionan una vista Snapshot.
  - **Cloud Tier View** muestra la cantidad de capacidad que se está utilizando en el nivel de rendimiento local y cuánto se está utilizando en el nivel de nube. Estos gráficos incluyen una estimación de la cantidad de tiempo que queda antes de que se llene la capacidad para esta carga de trabajo. Esta información se basa en el uso histórico. Además, requiere un mínimo de 10 días de datos. Cuando quedan menos de 30 días de capacidad, Unified Manager identifica el almacenamiento como «'casi completo'».

¿Cuándo se debe utilizar el analizador de cargas de trabajo

Por lo general, se usaría el analizador de cargas de trabajo para solucionar un problema

de latencia notificado por un usuario, para analizar más a fondo un evento o una alerta informados, o para explorar una carga de trabajo que observe que funciona de forma anormal.

En el caso en el que los usuarios se han puesto en contacto con usted para decir que la aplicación que utilizan se está ejecutando muy lentamente, puede comprobar los gráficos de latencia, rendimiento y uso de la carga de trabajo en la cual se está ejecutando la aplicación para ver si el almacenamiento es la causa del problema de rendimiento. Puede utilizar el gráfico de capacidad también para ver si la capacidad es baja, ya que un sistema ONTAP en el que se utiliza más del 85% puede ocasionar problemas de rendimiento. Estas tablas le ayudarán a determinar si el problema está causado por el almacenamiento, una red u otro problema relacionado.

En el caso de que Unified Manager haya generado un evento de rendimiento y desee revisar la causa del problema de forma más exhaustiva, puede iniciar el analizador de cargas de trabajo desde la página de detalles del evento haciendo clic en el botón **analizar carga de trabajo** para investigar parte de la latencia, el rendimiento, y las tendencias de capacidad para la carga de trabajo.

En caso de observar una carga de trabajo que parece estar funcionando de forma anormal al ver cualquier página de inventario de la carga de trabajo (volumen, LUN, carga de trabajo, recurso compartido NFS o recurso compartido SMB/CIFS), se puede hacer clic en el icono más , A continuación **analizar carga de trabajo** para abrir la página Análisis de carga de trabajo para examinar más la carga de trabajo.

Mediante el analizador de cargas de trabajo

Hay muchas formas de iniciar el analizador de cargas de trabajo desde la interfaz de usuario. Aquí describimos el lanzamiento de la herramienta desde el panel de navegación izquierdo.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Análisis de carga de trabajo**.

   Se muestra la página Workload Analysis.

2. Si conoce el nombre de la carga de trabajo, introduzca el nombre. Si no está seguro del nombre completo, introduzca un mínimo de 3 caracteres y el sistema mostrará una lista de cargas de trabajo que coincidan con la cadena.
3. Seleccione el intervalo de tiempo si desea ver las estadísticas durante más de las 2 horas predeterminadas y haga clic en **aplicar**.
4. Consulte el área Resumen para ver los eventos que se han producido durante el periodo de tiempo.
5. Consulte los gráficos de rendimiento y capacidad para ver cuándo alguna de las métricas es anormal y consulte si algún evento se alinea con la entrada anormal.

Supervisar el rendimiento del clúster en la página Performance Cluster Landing

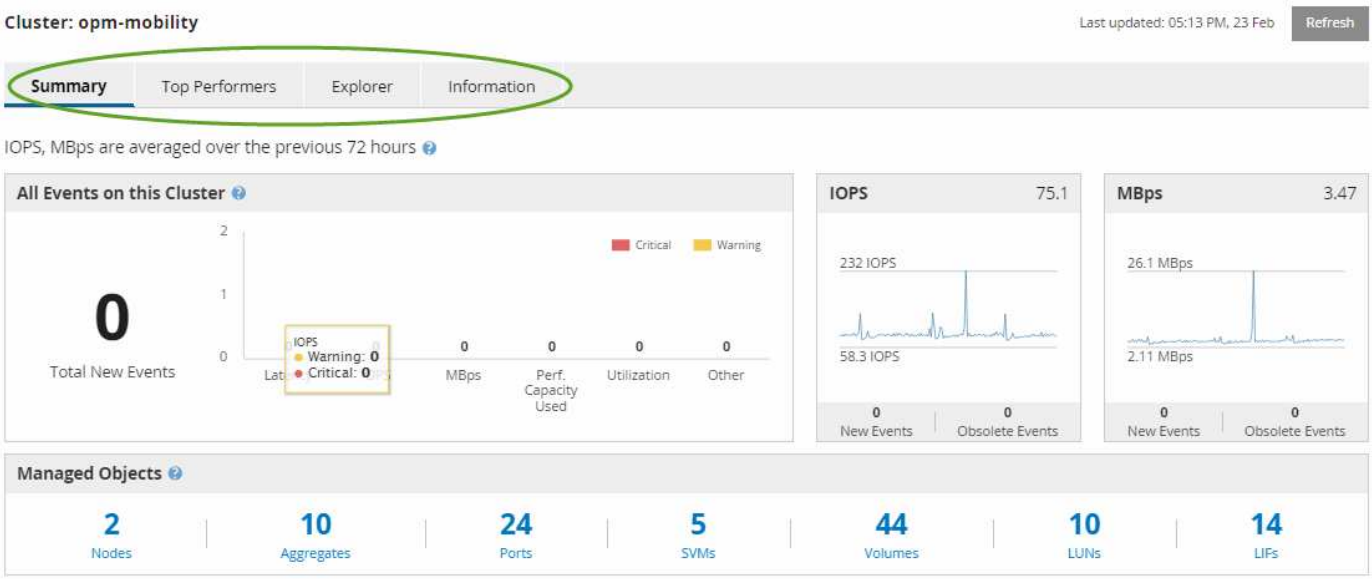
La página Performance Cluster Landing muestra el estado de alto nivel de rendimiento de un clúster seleccionado que está supervisando por una instancia de Unified Manager. Esta página le permite evaluar el rendimiento general de un clúster específico y anotar, localizar o asignar con rapidez para solucionar cualquier evento específico del clúster

identificado.

Descripción de la página de destino del clúster de rendimiento

La página de destino de Performance Cluster proporciona una descripción general del rendimiento de un clúster seleccionado, donde se hace hincapié en el estado del rendimiento de los 10 objetos más importantes del clúster. Los problemas de rendimiento se muestran en la parte superior de la página, en el panel All Events en este clúster.

La página de destino de clúster de rendimiento proporciona una descripción general de todos los clústeres que gestiona una instancia de Unified Manager. Esta página proporciona información sobre eventos y rendimiento, y permite supervisar y solucionar problemas de los clústeres. En la siguiente imagen, se muestra un ejemplo de la página de destino de Performance Cluster para el clúster denominado opm-motion:



El recuento de eventos en la página Cluster Summary puede no coincidir con el recuento de eventos en la página Performance Event Inventory. Esto se debe a que la página Cluster Summary puede mostrar un evento cada una de las barras de latencia y uso cuando se han incumplido las políticas de umbral de combinación, mientras que la página Performance Event Inventory muestra solo un evento cuando se ha incumplido una política de combinación.

Si Unified Manager ha eliminado un clúster de su gestión, el estado **eliminado** se muestra a la derecha del nombre del clúster en la parte superior de la página.

Página de destino de Cluster de rendimiento

La página Performance Cluster Landing muestra el estado de rendimiento de alto nivel de un clúster seleccionado. La página le permite acceder a detalles completos de cada contador de rendimiento para los objetos de almacenamiento en el clúster seleccionado.

La página de destino de clúster de rendimiento incluye cuatro pestañas para separar los detalles del clúster en cuatro áreas de información:

- Resumen

    - Panel Cluster Events
    - Gráficos de rendimiento MB/s e IOPS
    - Panel Managed Objects
- Página Top Performers
- Explorador
- Página de información

Página Performance Cluster Summary

La página Performance Cluster Summary ofrece un resumen de los eventos activos, el rendimiento de IOPS y el rendimiento de MB/s para un clúster. Esta página también incluye el número total de objetos de almacenamiento en el clúster.

Panel de eventos de rendimiento del clúster

El panel Cluster Performance Events muestra estadísticas de rendimiento y todos los eventos activos para el clúster. Esto resulta más útil cuando se supervisan los clústeres y todos los eventos y el rendimiento relacionados con el clúster.

Todos los eventos en este panel Cluster

En el panel todos los eventos de este clúster se muestran todos los eventos de rendimiento de clúster activos durante las 72 horas anteriores. El total de eventos activos se muestra en el extremo izquierdo; este número representa el total de todos los eventos nuevos y reconocidos para todos los objetos de almacenamiento de este clúster. Puede hacer clic en el enlace total Active Events para ir a la página Events Inventory, que se ha filtrado para mostrar estos eventos.

El gráfico de barras total Active Events del clúster muestra el número total de eventos críticos y de advertencia activos:

- Latencia (total para nodos, agregados, SVM, volúmenes, LUN, y espacios de nombres)
- IOPS (total para clústeres, nodos, agregados, SVM, volúmenes LUN y espacios de nombres)
- MB/s (total para clústeres, nodos, agregados, SVM, volúmenes LUN, espacios de nombres, puertos y LIF)
- Capacidad de rendimiento utilizada (total para nodos y agregados)
- Utilización (total para nodos, agregados y puertos)
- Otros (ratio de pérdidas de caché en volúmenes)

La lista contiene eventos de rendimiento activos activados a partir de políticas de umbral definidas por el usuario, políticas de umbral definidas por el sistema y umbrales dinámicos.

Los datos del gráfico (barras de contador verticales) se muestran en rojo ( ) para eventos críticos, y amarillo ( ) para eventos de advertencia. Coloque el cursor sobre cada barra vertical de contadores para ver el tipo y el número reales de eventos. Puede hacer clic en **Actualizar** para actualizar los datos del panel de contadores.

Puede mostrar u ocultar eventos críticos y de advertencia en el gráfico de rendimiento total de eventos activos haciendo clic en los iconos **críticos** y **Advertencia** de la leyenda. Si oculta ciertos tipos de eventos, los iconos de leyenda se muestran en gris.

Paneles de contadores

Los paneles de contadores muestran eventos de actividad y rendimiento del clúster de las 72 horas anteriores e incluyen los siguientes contadores:

- * Panel de contadores IOPS*

  IOPS indica la velocidad operativa del clúster en el número de operaciones de entrada/salida por segundo. Este panel de contadores proporciona una descripción general de alto nivel del estado de IOPS del clúster durante el período de 72 horas anterior. Puede colocar el cursor sobre la línea de tendencias del gráfico para ver el valor de IOPS de un tiempo específico.

- * MB/s panel de contadores*

  MB/s indica la cantidad de datos que se han transferido al clúster y desde él en megabytes por segundo. Este panel de contadores proporciona una descripción general de alto nivel del estado del clúster MB/s durante el período anterior de 72 horas. Puede colocar el cursor sobre la línea de tendencias del gráfico para ver el valor de MB/s de un tiempo específico.

El número situado en la parte superior derecha del gráfico en la barra gris es el valor medio del último período de 72 horas. Los números que se muestran en la parte inferior y superior del gráfico de líneas de tendencia son los valores mínimo y máximo del último período de 72 horas. La barra gris debajo del gráfico contiene el recuento de eventos activos (nuevos y reconocidos) y eventos obsoletos del último período de 72 horas.

Los paneles de contadores contienen dos tipos de eventos:

- **Activo**

  Indica que el evento de rendimiento está activo (nuevo o reconocido). El problema que causa el evento no se ha corregido solo o no se ha resuelto. El contador de rendimiento del objeto de almacenamiento sigue por encima del umbral de rendimiento.

- **Obsoleto**

  Indica que el evento no está activo. El problema que causa el evento se ha corregido solo o se ha resuelto. El contador de rendimiento del objeto de almacenamiento ya no está por encima del umbral de rendimiento.

En **Eventos activos**, si hay un evento, puede colocar el cursor sobre el icono del evento y hacer clic en el número del evento para enlazar a la página Detalles del evento correspondiente. Si hay más de un evento, puede hacer clic en **Ver todos los eventos** para mostrar la página Inventario de eventos, que se filtra para mostrar todos los eventos del tipo de contador de objeto seleccionado.

Panel Managed Objects

El panel Managed Objects de la pestaña Performance Summary proporciona una información general de nivel superior sobre los tipos de objetos de almacenamiento y los números para el clúster. Este panel le permite realizar el seguimiento del estado de los objetos de cada clúster.

El recuento de objetos gestionados son datos puntuales a partir del último período de recopilación. Los objetos nuevos se detectan a intervalos de 15 minutos.

Al hacer clic en el número vinculado para cualquier tipo de objeto, se muestra la página de inventario de

rendimiento de objetos para ese tipo de objeto. La página del inventario de objetos se filtra para mostrar únicamente los objetos de este clúster.

Los objetos administrados son:

- **Nodos**

  Un sistema físico en un clúster.

- **Agregados**

  Conjunto de varios grupos de discos independientes (RAID) redundantes que se pueden gestionar como una sola unidad de protección y aprovisionamiento.

- **Puertos**

  Punto de conexión física en nodos que se utiliza para conectarse a otros dispositivos de una red.

- **Almacenamiento de VMs**

  Máquina virtual que proporciona acceso de red a través de direcciones de red únicas. Una SVM puede servir datos a partir de un espacio de nombres distinto y se puede administrar por separado del resto del clúster.

- **Volúmenes**

  Entidad lógica que mantiene datos de usuario accesibles a través de uno o varios de los protocolos de acceso admitidos. El recuento incluye tanto volúmenes FlexVol como volúmenes FlexGroup, no incluye los componentes FlexGroup.

- **LUN**

  El identificador de una unidad lógica Fibre Channel (FC) o una unidad lógica iSCSI. Una unidad lógica normalmente corresponde a un volumen de almacenamiento y se representa dentro de un sistema operativo de ordenador como dispositivo.

- **Interfaces de red**

  Interfaz de red lógica que representa un punto de acceso de red a un nodo. El recuento incluye todos los tipos de interfaz.

Página Top Performers

La página Top Performers muestra los objetos de almacenamiento con el rendimiento más alto o el más bajo según el contador de rendimiento seleccionado. Por ejemplo, en la categoría de máquinas virtuales de almacenamiento, puede mostrar las SVM que tienen las IOPS más altas, o la latencia más alta, o los MB/s más bajos Esta página también muestra si alguno de los mejores ejecutantes tiene eventos de rendimiento activos (nuevos o reconocidos).

La página Top Performers muestra un máximo de 10 de cada objeto. Es preciso tener en cuenta que el objeto Volume incluye tanto los volúmenes FlexVol como los volúmenes FlexGroup.

- **Intervalo de tiempo**

Puede seleccionar un intervalo de tiempo para ver los ejecutantes superiores; el intervalo de tiempo seleccionado se aplica a todos los objetos de almacenamiento. Intervalos de tiempo disponibles:

- Última hora
- Últimas 24 horas
- Últimas 72 horas (predeterminado)
- Últimos 7 días

- **Sistema métrico**

  Haga clic en el menú **Métrico** para seleccionar un contador diferente. Las opciones de contador son únicas para el tipo de objeto. Por ejemplo, los contadores disponibles para el objeto **Volumes** son **latencia**, **IOPS** y **MB/s**. Al cambiar el contador se cargan de nuevo los datos del panel con los ejecutantes superiores según el contador seleccionado.

  Contadores disponibles:

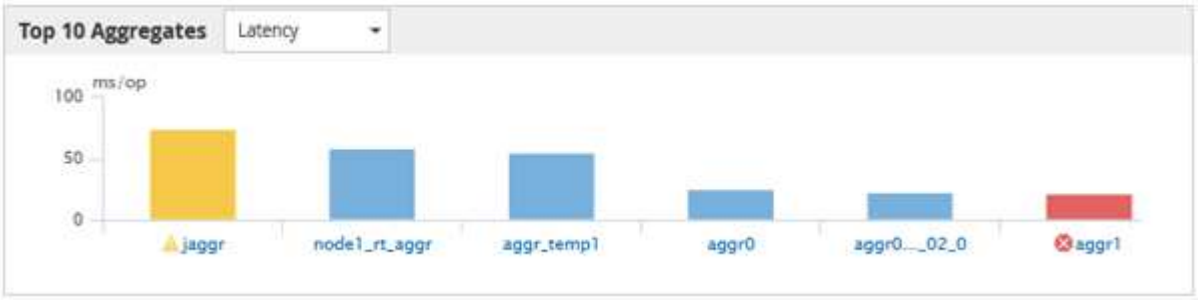
  - Latencia
  - IOPS
  - MB/s
  - Capacidad de rendimiento utilizada (para nodos y agregados)
  - Utilización (para nodos y agregados)

- **Ordenar**

  Haga clic en el menú **Ordenar** para seleccionar un orden ascendente o descendente para el objeto y el contador seleccionados. Las opciones son **más altas a más bajas** y **más bajas a más altas**. Estas opciones le permiten ver los objetos con el rendimiento más alto o el más bajo.

- **Barra de contador**

  La barra de contador del gráfico muestra las estadísticas de rendimiento de cada objeto, representada como una barra para ese elemento. Los gráficos de barras están codificados con colores. Si el contador no está violando un umbral de rendimiento, la barra de contador se muestra en azul. Si una infracción de umbral está activa (un evento nuevo o confirmado), la barra se muestra en color para el evento: Los sucesos de advertencia se muestran en amarillo ( ) y los sucesos críticos se muestran en rojo ( ). Las infracciones de umbral se indican aún más mediante iconos de indicadores de eventos de gravedad para los eventos de advertencia y críticos.



Para cada gráfico, el eje X muestra los ejecutantes superiores del tipo de objeto seleccionado. El eje y muestra las unidades aplicables al contador seleccionado. Al hacer clic en el enlace del nombre del objeto debajo de cada elemento de gráfico de barras vertical, se desplaza hasta la página de inicio de rendimiento del objeto seleccionado.

- **Indicador de sucesos de gravedad**

  El icono del indicador **evento de gravedad** se muestra a la izquierda del nombre de un objeto para el valor crítico activo ( ) o advertencia ( ) eventos en los gráficos de alto rendimiento. Haga clic en el icono del indicador **evento de gravedad** para ver:

  - **Un evento**

    Navega hasta la página de detalles del evento correspondiente a ese evento.

  - **Dos o más eventos**

    Navega hasta la página de inventario de eventos, que se filtra para mostrar todos los eventos del objeto seleccionado.

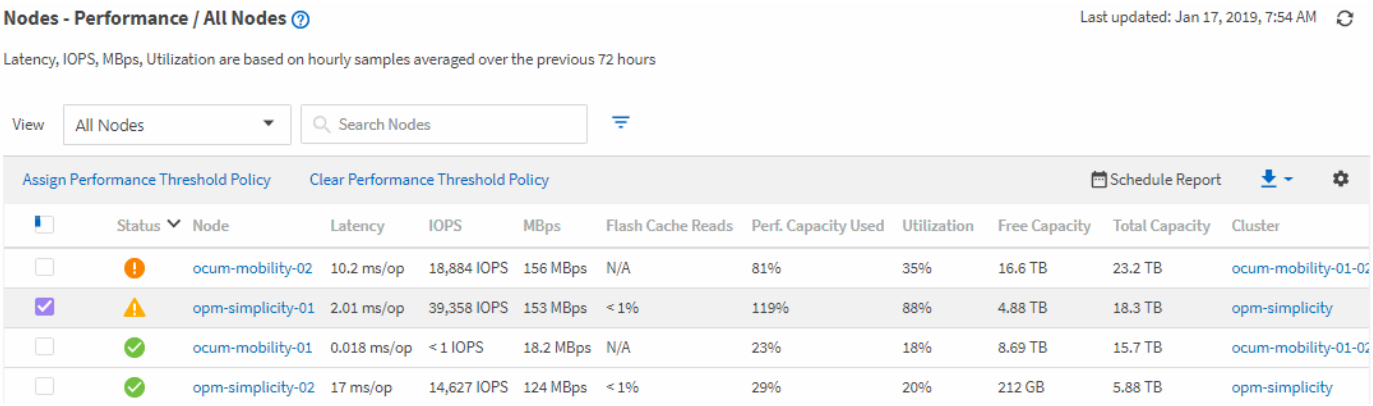
- **Botón Exportar**

  Crea un `.csv` archivo que contiene los datos que aparecen en la barra de contador. Puede optar por crear el archivo para el único clúster que esté viendo o para todos los clústeres del centro de datos.

Supervisión del rendimiento mediante las páginas Performance Inventory

Las páginas de rendimiento del inventario de objetos muestran información de rendimiento, eventos de rendimiento y estado de objetos para todos los objetos de una categoría de tipo de objeto. Esto proporciona una descripción general rápida del estado de rendimiento de cada objeto dentro de un clúster, por ejemplo, de todos los nodos o todos los volúmenes.

Las páginas de rendimiento del inventario de objetos proporcionan una descripción general de alto nivel del estado del objeto, lo que permite evaluar el rendimiento general de todos los objetos y comparar los datos de rendimiento del objeto. Para refinar el contenido de páginas de inventario de objetos, realice búsquedas, ordenaciones y filtros. Esto resulta beneficioso para la supervisión y la gestión del rendimiento de objetos, ya que permite localizar rápidamente objetos con problemas de rendimiento y comenzar el proceso de solución de problemas.



De forma predeterminada, los objetos de las páginas del inventario de rendimiento se ordenan en función del nivel de importancia del rendimiento del objeto. Los objetos con nuevos eventos críticos de rendimiento se enumeran primero y los objetos con eventos de advertencia se muestran en segundo lugar. Esto proporciona una indicación visual inmediata de los problemas que deben abordarse. Todos los datos de rendimiento se

basan en un promedio de 72 horas.

Es posible desplazarse fácilmente desde la página de rendimiento del inventario de objetos a la página de detalles de un objeto si se hace clic en el nombre del objeto en la columna nombre del objeto. Por ejemplo, en la página de inventario Performance/All Nodes , haga clic en un objeto de nodo en la columna **Nodes** . La página de detalles del objeto proporciona información detallada y detalles sobre el objeto seleccionado, incluida la comparación en paralelo de los eventos activos.

Ver las páginas de inventario de rendimiento para todos los objetos de almacenamiento

Las páginas de inventario de rendimiento se utilizan para ver un resumen de la información sobre el rendimiento de cada uno de los objetos de almacenamiento disponibles, como los clústeres, los agregados, los volúmenes, etc. Puede establecer un enlace a las páginas de detalles del objeto Performance para ver información detallada de un objeto determinado.

De forma predeterminada, los objetos de las páginas de vista se ordenan en función de la gravedad del evento. Los objetos con eventos críticos se enumeran primero y los objetos con eventos de advertencia aparecen en segundo lugar. Esto proporciona una indicación visual inmediata de los problemas que deben abordarse.

Puede exportar datos de estas páginas a valores separados por comas (`.csv`), archivo de Microsoft Excel (`.xlsx`), o. (`.pdf`) Documente utilizando el botón **Informes** y, a continuación, utilice los datos exportados para generar informes. Además, puede personalizar la página y, a continuación, programar un informe para que se cree y envíe por correo electrónico regularmente mediante el botón **Informes programados**.

Todos los campos de estas páginas se pueden utilizar en vistas personalizadas y en informes. Algunos de los campos están vinculados a páginas relacionadas, lo que permite una vista más detallada.

Rendimiento: Vista All Clusters

La vista Performance: All Clusters muestra una descripción general de los eventos de rendimiento, los datos y la información de configuración para cada clúster supervisado por una instancia de Unified Manager. Esta página permite supervisar el rendimiento de los clústeres y solucionar problemas de rendimiento y eventos de umbral.

Puede asignar directivas de umbral de rendimiento a cualquier objeto de las páginas de inventario de objetos o borrar directivas de umbral mediante los botones **asignar directiva de umbral de rendimiento** y **Borrar directiva de umbral de rendimiento**.

A continuación se muestran algunos campos importantes en la vista Performance: All Clusters.

- Cluster FQDN: El nombre de dominio completo (FQDN) del clúster.
- IOPS: Las operaciones de entrada/salida por segundo en el clúster.
- MB/s: El rendimiento en el clúster, medido en MIB por segundo.
- Campos de capacidad: Capacidad libre y total en GIB.
- Host Name or IP Address: El nombre de host o la dirección IP (IPv4 o IPv6) de la LIF de gestión del clúster.
- OS Version: La versión del software ONTAP que se instala en el clúster.

Si se instalan diferentes versiones del software ONTAP en los nodos del clúster, se muestra el número de versión más bajo. Puede ver la versión de ONTAP que se instala en cada nodo desde la vista rendimiento: Todos los nodos.

- Política de umbral: La política de umbral de rendimiento definida por el usuario o políticas que están activas en este objeto de almacenamiento. Puede colocar el cursor sobre los nombres de directivas que contienen puntos suspensivos (…). para ver el nombre completo de la directiva o la lista de nombres de directivas asignadas. Los botones asignar directiva de umbral de rendimiento y Borrar directiva de umbral de rendimiento permanecen deshabilitados hasta que seleccione uno o más objetos haciendo clic en las casillas de verificación situadas en el extremo izquierdo.

Rendimiento: Vista de todos los volúmenes

Performance: All Volumes View muestra información general de los eventos de rendimiento, los datos de contador y la información de configuración de cada volumen FlexVol y volumen FlexGroup que supervisa una instancia de Unified Manager. Esto permite supervisar rápidamente el rendimiento de los volúmenes y solucionar problemas de rendimiento y eventos de umbral.

Si desea analizar la latencia y el rendimiento de un objeto específico, haga clic en el botón más opciones ⋮ A continuación **analizar carga de trabajo** y puede ver gráficos de rendimiento y capacidad en la página Análisis de carga de trabajo. Puede ver los detalles en System Manager si tiene credenciales válidas para System Manager.

Para los volúmenes de protección de datos (DP), solo se muestran los valores de contador del tráfico generado por el usuario. Los volúmenes raíz no se muestran en esta página.

A continuación se muestran algunos campos importantes en la vista rendimiento: Todos los volúmenes.

- Estilo: FlexVol o FlexGroup.
- Latencia: Para los volúmenes FlexVol, es el tiempo de respuesta medio del volumen para todas las solicitudes de I/o, expresado en milisegundos por operación. Para los volúmenes FlexGroup, esta es la latencia media de todos los volúmenes constituyentes.
- IOPS/TB: El número de operaciones de entrada/salida procesadas por segundo según el espacio total que consume la carga de trabajo, en terabytes. Este contador mide el rendimiento que ofrece una cantidad de capacidad de almacenamiento determinada.
- IOPS: Para los volúmenes FlexVol, este es el número de operaciones de entrada/salida por segundo del volumen. Para los volúmenes FlexGroup, esta es la suma de IOPS para todos los volúmenes constituyentes.
- MB/s: Para volúmenes FlexVol, el rendimiento en el volumen, medido en megabytes por segundo. Para los volúmenes FlexGroup, esta es la suma de MB/s para todos los volúmenes constituyentes.
- Campos de capacidad: Capacidad libre y total en GIB.

Consulte los siguientes enlaces para obtener más información:

- "Asignación de políticas de umbral de rendimiento a objetos de almacenamiento"
- "Eliminación de políticas de umbral de rendimiento de objetos de almacenamiento"
- "Tipos de cargas de trabajo supervisadas por Unified Manager"
- "Ver la configuración del grupo de políticas de calidad de servicio aplicable a volúmenes o LUN específicos"

- "Descripción de las recomendaciones de Unified Manager para organizar los datos en niveles en el cloud"
- "Ver los gráficos de rendimiento para comparar volúmenes o LUN que están en el mismo grupo de políticas de calidad de servicio"

Rendimiento: Vista de todos los agregados

La vista rendimiento: Todos los agregados muestra una descripción general de los eventos de rendimiento, los datos y la información de configuración de cada agregado supervisado por una instancia de Unified Manager. Esta página le permite supervisar el rendimiento de los agregados y solucionar problemas de rendimiento y eventos de umbral.

A continuación se muestran algunos campos importantes en la vista Performance: All Aggregates.

- Tipo: El tipo de agregado:
  - HDD
  - Híbrido. Combina HDD y SSD, pero Flash Pool no se ha habilitado.
  - Híbrido (Flash Pool). Combina HDD y SSD y Flash Pool se ha habilitado.
  - SSD
  - SSD (FabricPool). Combina SSD y un nivel de cloud
  - Unidad de disco duro (FabricPool). Combina HDD y un nivel de cloud
  - VMDisk (SDS). Discos virtuales en una máquina virtual
  - Disco de VMware (FabricPool). Combina discos virtuales y un nivel de cloud
  - LUN (FlexArray)
- Generación de informes de datos inactivos: Si la funcionalidad de generación de informes de datos inactivos está habilitada o deshabilitada en este agregado. Cuando se encuentra habilitada, los volúmenes de este agregado muestran la cantidad de datos inactivos en la vista rendimiento: Todos los volúmenes. El valor de este campo es "N/A" cuando la versión de ONTAP no admite la generación de informes de datos inactivos.
- Política de umbral: La política de umbral de rendimiento definida por el usuario o políticas que están activas en este objeto de almacenamiento. Puede colocar el cursor sobre los nombres de directivas que contienen puntos suspensivos (…). para ver el nombre completo de la directiva o la lista de nombres de directivas asignadas. Los botones asignar directiva de umbral de rendimiento y Borrar directiva de umbral de rendimiento permanecen deshabilitados hasta que seleccione uno o más objetos haciendo clic en las casillas de verificación situadas en el extremo izquierdo. Consulte los siguientes enlaces para obtener más información:
- "Asignación de políticas de umbral de rendimiento a objetos de almacenamiento"
- "Eliminación de políticas de umbral de rendimiento de objetos de almacenamiento"

Rendimiento: Vista de todos los nodos

La vista rendimiento: Todos los nodos muestra información general de los eventos de rendimiento, los datos y la información de configuración de cada nodo que supervisa una instancia de Unified Manager. Esto permite supervisar rápidamente el rendimiento de los nodos y solucionar problemas de rendimiento y eventos de umbral.

Las lecturas de Flash Cache muestran el porcentaje de operaciones de lectura del nodo que se satisfacen con la caché, en lugar de ser devueltas del disco. Los datos de Flash Cache solo se muestran para nodos, y solo cuando se instala un módulo Flash Cache en el nodo.

En el menú **Informes**, la opción **Informe de inventario de hardware** se proporciona cuando Unified Manager, y los clústeres que administra, se instalan en un sitio sin conectividad de red externa. Este botón genera un archivo .csv que contiene una lista completa de información de clústeres y nodos; como números de modelo de hardware y números de serie, tipos y números de discos, licencias instaladas, etc. Esta funcionalidad de generación de informes resulta útil para renovar el contrato en sitios seguros que no están conectados a la plataforma Active IQ de NetApp. Puede asignar directivas de umbral de rendimiento a cualquier objeto de las páginas de inventario de objetos o borrar directivas de umbral mediante los botones **asignar directiva de umbral de rendimiento** y **Borrar directiva de umbral de rendimiento**.

Consulte los siguientes enlaces para obtener más información:

- "Asignación de políticas de umbral de rendimiento a objetos de almacenamiento"
- "Eliminación de políticas de umbral de rendimiento de objetos de almacenamiento"
- "Generar un informe de inventario de hardware para la renovación de contrato"

Rendimiento: Vista de todas las máquinas virtuales de almacenamiento

La vista rendimiento: All Storage VMs muestra información general sobre los eventos de rendimiento, los datos y la información de configuración para cada máquina virtual de almacenamiento (SVM) que supervisa una instancia de Unified Manager. Esto le permite supervisar rápidamente el rendimiento de las SVM y solucionar problemas de rendimiento y eventos de umbral. En el campo latencia de esta página, se informa del tiempo de respuesta medio de todas las solicitudes de I/o, expresadas en milisegundos por operación.

Las SVM que aparecen en esta página incluyen solo SVM de datos y clúster. Unified Manager no utiliza ni muestra las SVM de administrador ni de nodo.

Consulte los siguientes enlaces para obtener más información:

- "Asignación de políticas de umbral de rendimiento a objetos de almacenamiento"
- "Eliminación de políticas de umbral de rendimiento de objetos de almacenamiento"

Rendimiento: Vista de todas las LUN

La vista rendimiento: Todas las LUN muestra información general de los eventos de rendimiento, los datos y la información de configuración de cada LUN que supervisa una instancia de Unified Manager. Esto le permite supervisar rápidamente el rendimiento de sus LUN y solucionar problemas de rendimiento y eventos de umbral.

Si desea analizar la latencia y el rendimiento de un objeto específico, haga clic en el icono más ⋮, Luego **analizar la carga de trabajo** y puede ver los gráficos de rendimiento y capacidad en la página **Análisis de carga de trabajo**.

Consulte los siguientes enlaces para obtener más información:

- "Supervisar las LUN en una relación de grupo de consistencia"
- "Aprovisionar las LUN"
- "Asignación de políticas de umbral de rendimiento a objetos de almacenamiento"

- "Eliminación de políticas de umbral de rendimiento de objetos de almacenamiento"
- "Ver volúmenes o LUN que estén en el mismo grupo de políticas de calidad de servicio".
- "Ver la configuración del grupo de políticas de calidad de servicio aplicable a volúmenes o LUN específicos"
- "Aprovisionamiento de LUN mediante API"

Performance: Toda la vista NVMe Namespaces

La vista Performance: All NVMe Namespaces muestra información general sobre los eventos de rendimiento, los datos y la información de configuración de cada espacio de nombres de NVMe que se supervisa mediante una instancia de Unified Manager. Esto permite supervisar rápidamente el rendimiento y el estado de los espacios de nombres, así como resolver problemas y eventos de umbral.

Se informa de la siguiente información, entre otras: El estado actual del espacio de nombres. * Sin conexión: No se permite el acceso de lectura o escritura al espacio de nombres. * Online: Se permite el acceso de lectura y escritura al espacio de nombres. * NVFAIL: El espacio de nombres se desconectó automáticamente debido a un fallo de NVRAM. * Error de espacio: El espacio de nombres se ha quedado sin espacio.

Consulte los siguientes enlaces para obtener más información:

- "Asignación de políticas de umbral de rendimiento a objetos de almacenamiento"
- "Eliminación de políticas de umbral de rendimiento de objetos de almacenamiento"

Performance: Vista de todas las interfaces de red

La vista Performance: All Network interfaces muestra una descripción general de los eventos de rendimiento, los datos y la información de configuración de cada interfaz de red (LIF) que está supervisando mediante esta instancia de Unified Manager. Esta página le permite supervisar rápidamente el rendimiento de las interfaces y solucionar problemas de rendimiento y eventos de umbral. A continuación se muestran algunos campos importantes en la vista Performance: All Network interfaces.

- IOPS: Las operaciones de entrada/salida por segundo. IOPS no es aplicable a los LIF NFS ni a los LIF CIFS, y se muestra como N/A para estos tipos.
- Latencia: El tiempo de respuesta medio de todas las solicitudes de I/o, expresado en milisegundos por operación. La latencia no es aplicable a los LIF NFS y los LIF CIFS, y se muestra como N/A para estos tipos.
- Ubicación de inicio: La ubicación de inicio de la interfaz, mostrada como nombre de nodo y nombre de puerto, separados por dos puntos (:). Si la ubicación se muestra con puntos suspensivos (…), puede colocar el cursor sobre el nombre de la ubicación para ver la ubicación completa.
- Ubicación actual: La ubicación actual de la interfaz, mostrada como nombre de nodo y nombre de puerto, separados por dos puntos (:). Si la ubicación se muestra con puntos suspensivos (…), puede colocar el cursor sobre el nombre de la ubicación para ver la ubicación completa.
- Role: El rol de interfaz: Data, Cluster, Node Management o Intercluster.

Las interfaces que se enumeran en esta página incluyen LIF de datos, LIF de clúster, LIF de gestión de nodos y LIF de interconexión de clústeres. Unified Manager no utiliza ni muestra las LIF del sistema.

Rendimiento: Vista de todos los puertos

La vista rendimiento: Todos los puertos muestra una descripción general de los eventos de rendimiento, los datos y la información de configuración de cada puerto que supervisa una instancia de Unified Manager. Esto permite supervisar rápidamente el rendimiento de los puertos y solucionar problemas de rendimiento y eventos de umbral. Para un rol de puerto, se muestra la función de puerto de red, ya sea Data o Cluster. Los puertos FCP no pueden tener un rol y el rol se muestra como N/A.

> Los valores de contador de rendimiento solo se muestran para los puertos físicos. Los valores de contador no se muestran para las VLAN ni los grupos de interfaces.

Consulte los siguientes enlaces para obtener más información:

- "Asignación de políticas de umbral de rendimiento a objetos de almacenamiento"
- "Eliminación de políticas de umbral de rendimiento de objetos de almacenamiento"

Rendimiento: Vista QoS Policy Groups

La vista QoS Policy Groups muestra los grupos de políticas de calidad de servicio disponibles en los clústeres que supervisa Unified Manager. Esto incluye las políticas de calidad de servicio tradicionales, las políticas de calidad de servicio adaptativas y las políticas de calidad de servicio asignadas mediante los niveles de servicio de rendimiento.

A continuación, se muestran algunos campos importantes en la vista Performance: QoS Policy Groups.

- QoS Policy Group: El nombre del grupo de políticas de calidad de servicio. Para las políticas de Service Level Manager (NSLM) 1.3 de NetApp que se han importado a Unified Manager 9.7 o posterior, el nombre que se muestra aquí incluye el nombre de SVM y otra información que no aparece en el nombre cuando se definió Performance Service Levelwas en NSLM. Por ejemplo, el nombre "NSLM_vs6_Performance_2_0" significa que esta es la política "Performance" de NSLM definida por el sistema creada en la SVM "vs6" con una latencia esperada de "2 ms/op".
- SVM: La máquina virtual de almacenamiento (SVM) a la que pertenece el grupo de políticas de calidad de servicio. Es posible hacer clic en el nombre de la máquina virtual de almacenamiento para acceder a la página de detalles de esa máquina virtual de almacenamiento. Tenga en cuenta que este campo está vacío si la política de calidad de servicio se ha creado en la máquina virtual de almacenamiento Admin, ya que este tipo de máquina virtual de almacenamiento representa el clúster.
- Min rendimiento: El rendimiento mínimo, en IOPS, que se garantizará que proporcione el grupo de políticas. Para las políticas adaptativas, se trata del número mínimo esperado de IOPS por TB asignado al volumen o LUN, según el tamaño del objeto de almacenamiento asignado.
- Rendimiento máximo: El rendimiento, en IOPS y/o MB/s, que el grupo de políticas no debe superar. Cuando este campo está en blanco, significa que el máximo definido en ONTAP es infinito. Para las políticas adaptativas, es el número máximo (pico) de IOPS posible por TB asignado al volumen o LUN, en función del tamaño del objeto de almacenamiento asignado o del tamaño del objeto de almacenamiento utilizado.
- Absolute Minimum IOPS: Para las políticas adaptativas, es el valor mínimo absoluto de IOPS que se utiliza como anulación cuando el IOPS esperado es inferior a este valor.
- Block Size: El tamaño de bloque especificado para la política adaptativa de calidad de servicio.
- Asignación mínima: Se utiliza si el "espacio asignado" o el "espacio utilizado" para determinar el rendimiento máximo de IOPS (pico).
- Latencia esperada: La latencia media esperada para operaciones de entrada/salida de almacenamiento.

- Compartido: Para las políticas de calidad de servicio tradicionales, si los valores de rendimiento definidos en el grupo de políticas se comparten entre varios objetos.
- Associated Objects: La cantidad de cargas de trabajo que se asignan al grupo de políticas de calidad de servicio. Puede hacer clic en el botón expandir ( ) Junto al Nombre del grupo de políticas QoS para ver más detalles acerca del grupo de políticas.
- Capacidad asignada: La cantidad de espacio que usan los objetos del grupo de políticas de calidad de servicio actualmente.
- Asociados Objects: El número de cargas de trabajo que se asignan al grupo de políticas de calidad de servicio, separadas en volúmenes y LUN. Puede hacer clic en el número para desplazarse a una página que proporciona más detalles sobre los volúmenes o LUN seleccionados.

Para obtener más información, consulte los temas en "Gestione el rendimiento mediante información del grupo de políticas de calidad de servicio".

Afinar el contenido de la página del inventario de rendimiento

Las páginas de inventario de objetos de rendimiento contienen herramientas que ayudan a refinar el contenido de datos de inventario de objetos, lo que permite localizar datos específicos de forma rápida y sencilla.

La información contenida en las páginas de inventario de objetos Performance puede ser extensa y a menudo abarca varias páginas. Este tipo de datos completos son excelentes para la supervisión, el seguimiento y la mejora del rendimiento; sin embargo, ubicar datos específicos requiere herramientas que le permitan localizar rápidamente los datos que busca. Por lo tanto, las páginas de inventario de objetos Performance contienen funcionalidades para realizar búsquedas, ordenar y filtrar. Además, las búsquedas y el filtrado pueden funcionar conjuntamente para reducir aún más los resultados.

Buscar en páginas rendimiento de inventario de objetos

Puede buscar cadenas en páginas rendimiento de inventario de objetos. Utilice el campo **Buscar** situado en la parte superior derecha de la página para localizar rápidamente los datos basados en el nombre del objeto o el nombre de la política. Esto permite localizar rápidamente objetos específicos y sus datos asociados, o bien localizar rápidamente políticas y ver los datos de objetos de políticas asociados.

Paso

1. Realice una de las siguientes opciones según sus requisitos de búsqueda:

Para localizar esto…	Escriba esto…
Un objeto específico	El nombre del objeto en el campo **Buscar** y haga clic en **Buscar**. Se muestra el objeto por el que ha buscado y sus datos relacionados.
Una política de umbral de rendimiento definida por el usuario	Todo o parte del nombre de la política en el campo **Buscar** y haga clic en **Buscar**. Se muestran los objetos asignados a la política en la que se realizó la búsqueda.

Ordenar en las páginas rendimiento de inventario de objetos

Puede ordenar todos los datos de las páginas rendimiento de inventario de objetos por cualquier columna en orden ascendente o descendente. Esto permite localizar rápidamente datos de inventario de objetos, lo cual resulta útil para examinar el rendimiento o iniciar un proceso de resolución de problemas.

La columna seleccionada para ordenar se indica mediante un nombre de encabezado de columna resaltado y un icono de flecha que indica la dirección de ordenación a la derecha del nombre. Una flecha hacia arriba indica el orden ascendente; una flecha hacia abajo indica el orden descendente. El orden predeterminado es por **Estado** (criticidad de evento) en orden descendente, con los eventos de rendimiento más críticos listados primero.

Paso

1. Puede hacer clic en el nombre de una columna para alternar el orden de clasificación de la columna en orden ascendente o descendente.

   El contenido de la página rendimiento del inventario de objetos se ordena en orden ascendente o descendente, según la columna seleccionada.

Filtrar datos en las páginas rendimiento de inventario de objetos

Puede filtrar datos en las páginas rendimiento de inventario de objetos para localizar rápidamente datos según criterios específicos. Puede utilizar el filtrado para restringir el contenido de las páginas rendimiento de inventario de objetos para mostrar sólo los resultados especificados. Esto proporciona un método muy eficiente para mostrar solo los datos de rendimiento de los que le interesa.

Puede utilizar el panel filtrado para personalizar la vista de cuadrícula en función de sus preferencias. Las opciones de filtro disponibles se basan en el tipo de objeto que se está viendo en la cuadrícula. Si se aplican filtros actualmente, el número de filtros aplicados se muestra a la derecha del botón filtro.

Se admiten tres tipos de parámetros de filtro.

Parámetro	Validación
Cadena (texto)	Los operadores son **contiene**, **comienza con**, **termina con** y **no contiene**.
Número	Los operadores son **superiores a**, **inferiores a**, **en el último** y **entre**.
Enumeración (texto)	Los operadores son **is** y **no**.

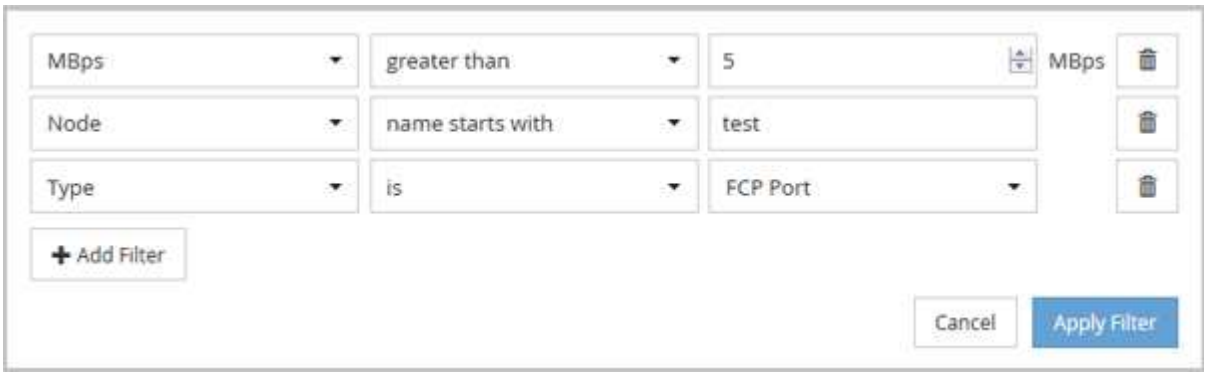
Los campos columna, operador y valor son necesarios para cada filtro; los filtros disponibles reflejan las columnas filtrables en la página actual. El número máximo de filtros que puede aplicar es cuatro. Los resultados filtrados se basan en parámetros de filtro combinados. Los resultados filtrados se aplican a todas las páginas de la búsqueda filtrada, no sólo a la página mostrada actualmente.

Puede agregar filtros mediante el panel filtrado.

1. En la parte superior de la página, haga clic en el botón **filtro**. Aparecerá el panel filtrado.
2. Haga clic en la lista desplegable que se encuentra a la izquierda y seleccione un objeto; por ejemplo, *Cluster* o un contador de rendimiento.
3. Haga clic en la lista desplegable Centro y seleccione el operador que desee utilizar.
4. En la última lista, seleccione o escriba un valor para completar el filtro de ese objeto.
5. Para agregar otro filtro, haga clic en **+Agregar filtro**. Aparecerá un campo de filtro adicional. Complete este filtro utilizando el proceso descrito en los pasos anteriores. Tenga en cuenta que al agregar el cuarto filtro, el botón **+Agregar filtro** ya no aparece.
6. Haga clic en **aplicar filtro**. Las opciones de filtro se aplican a la cuadrícula y el número de filtros se muestra a la derecha del botón filtro.
7. Utilice el panel filtrado para eliminar filtros individuales haciendo clic en el icono de papelera situado a la derecha del filtro que se va a eliminar.
8. Para eliminar todos los filtros, haga clic en **Restablecer** en la parte inferior del panel de filtrado.

Ejemplo de filtrado

La ilustración muestra el panel filtrado con tres filtros. El botón **+Add Filter** aparece cuando tiene menos de cuatro filtros como máximo.



Después de hacer clic en **aplicar filtro**, el panel filtrado se cierra, aplica los filtros y muestra el número de filtros aplicados (3).

Descripción de las recomendaciones de Unified Manager para organizar los datos en niveles en el cloud

El rendimiento: Todos los volúmenes muestran información relacionada con el tamaño de los datos de usuario almacenados en el volumen que está inactivo (frío). En algunos casos, Unified Manager identifica ciertos volúmenes que se beneficiarían mediante la organización en niveles de los datos inactivos en el nivel de cloud (proveedor de cloud o StorageGRID) de un agregado habilitado para FabricPool.

FabricPool se introdujo en ONTAP 9.2, por lo que si utiliza una versión del software ONTAP anterior a 9.2, la recomendación de Unified Manager para almacenar datos en niveles requiere actualizar el software ONTAP. Además, el **`auto`** La política de organización en niveles se introdujo en ONTAP 9.4 y en la **`all`** La política de organización en niveles se introdujo en ONTAP 9.6, de modo que si se recomienda utilizar la política de organización en niveles automática, debe actualizar a ONTAP 9.4 o superior.

Los siguientes tres campos de rendimiento: La vista de todos los volúmenes ofrece información sobre si puede mejorar la utilización de discos del sistema de almacenamiento y ahorrar espacio en el nivel de rendimiento al mover los datos inactivos al nivel de cloud.

- **Política de organización en niveles**

  La política de organización en niveles determina si los datos del volumen permanecen en el nivel de rendimiento o si algunos de los datos se mueven del nivel de rendimiento al nivel de cloud.

  El valor de este campo indica la política de organización en niveles establecida en el volumen, aunque el volumen no resida actualmente en un agregado de FabricPool. La política de organización en niveles solo se aplica cuando el volumen se encuentra en un agregado de FabricPool.

- **Datos fríos**

  Los datos fríos muestran el tamaño de los datos de usuario almacenados en el volumen inactivo (en frío).

  Un valor se muestra aquí solo cuando se utiliza software ONTAP 9.4 o superior porque requiere que el agregado en el que se implementa el volumen tenga **`inactive data reporting parameter`** establezca en **`enabled`**, y que se ha cumplido el umbral mínimo de días de enfriamiento (para volúmenes que utilizan **`snapshot-only`** o. **`auto`** política de organización en niveles). En caso contrario, el valor se indica como «'N/A'».

- **Recomendación sobre la nube**

  Después de que se haya capturado información suficiente sobre la actividad de datos en el volumen, Unified Manager puede determinar que no se requiere ninguna acción o bien podría ahorrar espacio en el nivel de rendimiento al organizar en niveles los datos inactivos en el nivel de cloud.

El campo de datos fríos se actualiza cada 15 minutos, pero el campo recomendación de cloud se actualiza cada 7 días cuando se realiza el análisis de datos inactivos en el volumen. Por lo tanto, la cantidad exacta de datos fríos puede diferir entre los campos. El campo recomendación de cloud muestra la fecha en la que se ejecutó el análisis.

Cuando se activa la función de generación de informes de datos inactivos, el campo datos fríos muestra la cantidad exacta de datos inactivos. Sin la funcionalidad de generación de informes de datos inactivos, Unified Manager utiliza las estadísticas de rendimiento para determinar si los datos están inactivos en un volumen. La cantidad de datos inactivos no se muestra en el campo datos fríos en este caso, pero se muestra cuando se pasa el cursor por encima de la palabra **Tier** para ver la recomendación de la nube.

Las recomendaciones de cloud que verá son:

- **Aprendizaje**. No se han recopilado datos suficientes para hacer una recomendación.
- **Tier**. El análisis ha determinado que el volumen contiene datos inactivos (fríos) y que debe configurar el volumen para moverlos al nivel de cloud. En algunos casos, esto puede requerir en primer lugar mover el volumen a un agregado habilitado para FabricPool. En otros casos en los que el volumen ya está en un agregado de FabricPool, basta con cambiar la política de organización en niveles.
- **Sin acción**. O bien el volumen tiene muy pocos datos inactivos, el volumen ya está establecido en la política de organización en niveles «'auto» de un agregado de FabricPool o el volumen es un volumen de protección de datos. Este valor también se muestra cuando el volumen está sin conexión o cuando se utiliza en una configuración de MetroCluster.

Para mover un volumen, o cambiar la política de organización en niveles de volúmenes o la configuración de

la generación de informes de datos inactivos del agregado, utilice System Manager de ONTAP, los comandos de la CLI de ONTAP o una combinación de estas herramientas.

Si ha iniciado sesión en Unified Manager con la función Administrador de aplicaciones o Administrador de almacenamiento, el enlace **Configurar volumen** está disponible en la recomendación de nube al pasar el cursor por encima de la palabra **nivel**. Haga clic en este botón para abrir la página volúmenes en System Manager y realizar el cambio recomendado.

Supervisión del rendimiento mediante las páginas Performance Explorer

Las páginas Performance Explorer muestran información detallada sobre el rendimiento de cada objeto de un clúster. La página proporciona una vista detallada del rendimiento de todos los objetos del clúster, lo que permite seleccionar y comparar los datos de rendimiento de objetos específicos durante varios periodos de tiempo.

También puede evaluar el rendimiento general de todos los objetos y comparar los datos de rendimiento de los objetos en un formato paralelo.

Descripción del objeto raíz

El objeto raíz es la línea de base con la que se realizan otras comparaciones de objetos. Esto permite ver y comparar los datos de otros objetos con el objeto raíz, lo cual proporciona análisis de datos de rendimiento que le ayudan a resolver problemas y mejorar el rendimiento de los objetos.

El nombre del objeto raíz aparece en la parte superior del panel de comparación. Los objetos adicionales se muestran debajo del objeto raíz. Aunque no hay límite en el número de objetos adicionales que puede agregar al panel de comparación, sólo se permite un objeto raíz. Los datos del objeto raíz se muestran automáticamente en los gráficos del panel ContraCharts.

No puede cambiar el objeto raíz; siempre está establecido en la página de objetos que está viendo. Por ejemplo, si abre la página Volume Performance Explorer de Volume1, Volume1 es el objeto raíz y no puede cambiarse. Si desea realizar una comparación con otro objeto raíz, debe hacer clic en el vínculo de un objeto y abrir su página de destino.

Los eventos y umbrales se muestran solo para los objetos raíz.

Aplicar filtrado para reducir la lista de objetos correlacionados de la cuadrícula

El filtrado le permite mostrar un subconjunto más pequeño y bien definido de objetos en la cuadrícula. Por ejemplo, si tiene 25 volúmenes en la cuadrícula, el filtrado le permite ver sólo aquellos volúmenes con un rendimiento inferior a 90 Mbps o una latencia superior a 1 ms/op.

Especificación de un intervalo de tiempo para objetos correlacionados

El selector de intervalo de tiempo de la página Performance Explorer permite especificar el intervalo de tiempo para la comparación de datos de objetos. Si se especifica un

intervalo de tiempo, se refina el contenido de las páginas Performance Explorer para mostrar solo los datos del objeto dentro del intervalo de tiempo especificado.

Afinar el intervalo de tiempo proporciona un método eficiente para mostrar solo los datos de rendimiento que le interesan. Puede seleccionar un intervalo de tiempo predefinido o especificar un intervalo de tiempo personalizado. El intervalo de tiempo predeterminado es las 72 horas anteriores.

Selección de un intervalo de tiempo predefinido

Seleccionar un intervalo de tiempo predefinido es una forma rápida y eficiente de personalizar y centrar el resultado de los datos cuando se ven los datos de rendimiento del objeto del clúster. Al seleccionar un intervalo de tiempo predefinido, se dispone de datos de hasta 13 meses.

Pasos

1. En la parte superior derecha de la página **Performance Explorer**, haga clic en **intervalo de tiempo**.
2. En el lado derecho del panel **selección de intervalo de tiempo**, seleccione un intervalo de tiempo predefinido.
3. Haga clic en **aplicar rango**.

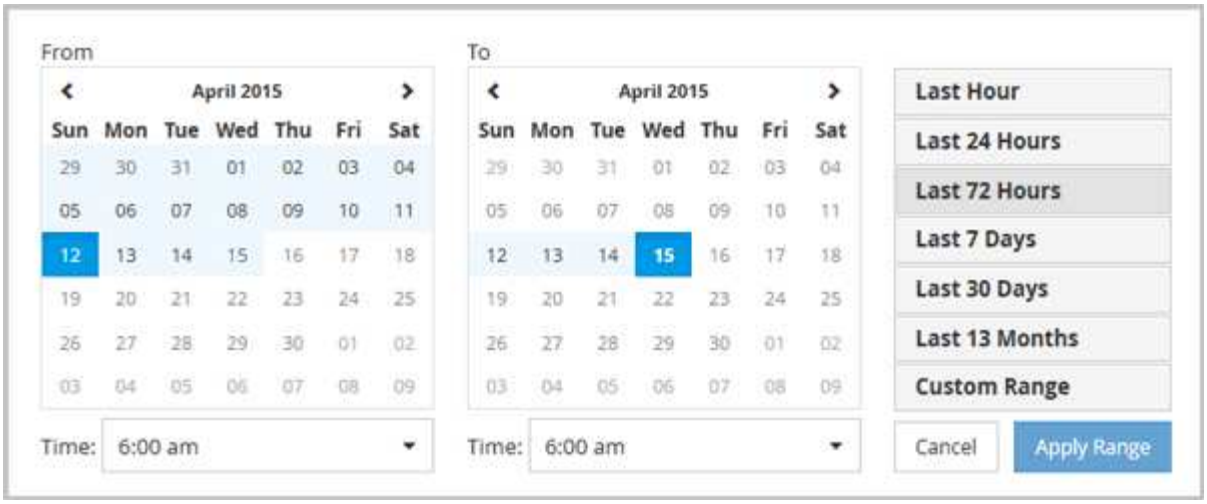
Especificación de un intervalo de tiempo personalizado

La página Performance Explorer permite especificar el intervalo de fecha y hora para los datos de rendimiento. Especificar un rango de tiempo personalizado proporciona mayor flexibilidad que el uso de intervalos de tiempo predefinidos al afinar los datos de objetos del clúster.

Puede seleccionar un intervalo de tiempo entre una hora y 390 días. 13 meses equivale a 390 días porque cada mes se cuenta como 30 días. La especificación de un intervalo de fechas y horas proporciona más detalles y le permite ampliar determinados eventos de rendimiento o series de eventos. La especificación de un intervalo de tiempo también ayuda a solucionar problemas potenciales de rendimiento, ya que al especificar un intervalo de fecha y tiempo se muestran los datos que rodean el evento de rendimiento con más detalle. Utilice el control **intervalo de tiempo** para seleccionar intervalos de fecha y hora predefinidos o especifique su propio intervalo de fecha y hora personalizado de hasta 390 días. Los botones de los intervalos de tiempo predefinidos varían de **última hora** a **últimos 13 meses**.

Al seleccionar la opción **últimos 13 meses** o especificar un intervalo de fechas personalizado superior a 30 días, se muestra un cuadro de diálogo en el que se informa de que los datos de rendimiento mostrados durante un período superior a 30 días se registran utilizando promedios por hora y no un sondeo de datos de 5 minutos. Por lo tanto, podría producirse una pérdida de granularidad visual de la línea de tiempo. Si hace clic en la opción **no volver a mostrar** del cuadro de diálogo, el mensaje no aparece cuando selecciona la opción **últimos 13 meses** o especifica un intervalo de fechas personalizado superior a 30 días. Los datos de resumen también se aplican en un intervalo de tiempo menor, si el intervalo de tiempo incluye una hora/fecha que es superior a 30 días a partir de hoy.

Al seleccionar un intervalo de tiempo (personalizado o predefinido), los intervalos de tiempo de 30 días o menos se basan en muestras de datos de intervalo de 5 minutos. Los intervalos de tiempo superiores a 30 días se basan en muestras de datos de intervalo de una hora.



1. Haga clic en el cuadro desplegable **intervalo de tiempo** y aparecerá el panel intervalo de tiempo.
2. Para seleccionar un intervalo de tiempo predefinido, haga clic en uno de los botones **última…** situados a la derecha del panel **intervalo de tiempo**. Al seleccionar un intervalo de tiempo predefinido, se dispone de datos de hasta 13 meses. El botón de intervalo de tiempo predefinido que ha seleccionado se resalta y los días y la hora correspondientes se muestran en los calendarios y selectores de tiempo.
3. Para seleccionar un intervalo de fechas personalizado, haga clic en la fecha de inicio en el calendario **de** de la izquierda. Haga clic en **<** o **>** para navegar hacia delante o hacia atrás en el calendario. Para especificar la fecha de finalización, haga clic en una fecha del calendario **a** de la derecha. Tenga en cuenta que la fecha de finalización predeterminada es hoy a menos que especifique una fecha de finalización diferente. El botón **intervalo personalizado** situado a la derecha del panel intervalo de tiempo está resaltado, lo que indica que ha seleccionado un intervalo de fechas personalizado.
4. Para seleccionar un intervalo de tiempo personalizado, haga clic en el control **Time** situado debajo del calendario **from** y seleccione la hora de inicio. Para especificar la hora de finalización, haga clic en el control **Time** situado debajo del calendario **to** de la derecha y seleccione la hora de finalización. El botón **intervalo personalizado** situado a la derecha del panel intervalo de tiempo está resaltado, lo que indica que ha seleccionado un intervalo de tiempo personalizado.
5. Opcionalmente, puede especificar las horas de inicio y finalización al seleccionar un intervalo de fechas predefinido. Seleccione el intervalo de fechas predefinido como se ha descrito anteriormente y, a continuación, seleccione las horas de inicio y de finalización como se ha descrito anteriormente. Las fechas seleccionadas se resaltan en los calendarios, las horas de inicio y finalización especificadas aparecen en los controles **Time** y el botón **Custom Range** se resalta.
6. Después de seleccionar el intervalo de fecha y hora, haga clic en **aplicar rango**. Las estadísticas de rendimiento de ese intervalo de tiempo se muestran en los gráficos y en la línea de tiempo Eventos.

Definir la lista de objetos correlacionados para la representación gráfica de comparación

Puede definir una lista de objetos correlacionados para la comparación de datos y rendimiento en el panel Diagrama de contador. Por ejemplo, si la máquina virtual de almacenamiento (SVM) tiene un problema de rendimiento, es posible comparar todos los volúmenes de la SVM para identificar qué volumen podría estar provocando el problema.

Puede agregar cualquier objeto de la cuadrícula de objetos correlacionados a los paneles comparación y Diagrama de contador. Esto permite ver y comparar datos de varios objetos y con el objeto raíz. Puede agregar y quitar objetos a y desde la cuadrícula de objetos correlacionados; sin embargo, el objeto raíz del panel de comparación no se puede quitar.

Al agregar muchos objetos al panel comparativo, puede afectar negativamente al rendimiento. Para mantener el rendimiento, debe seleccionar un número limitado de gráficos para la comparación de datos.

Pasos

1. En la cuadrícula de objetos, busque el objeto que desea agregar y haga clic en el botón **Agregar**.

   El botón **Agregar** se vuelve gris y el objeto se agrega a la lista de objetos adicionales del panel de comparación. Los datos del objeto se añaden a los gráficos de los paneles Counter Charts. El color del icono de ojo del objeto ( ) coincide con el color de la línea de tendencias de datos del objeto en los gráficos.

2. **Opcional:** Ocultar o mostrar datos para los objetos seleccionados:

Para hacer esto…	Realice esta acción…
Ocultar un objeto seleccionado	Haga clic en el icono de ojo del objeto seleccionado ( ) En el panel de comparación. Los datos del objeto están ocultos y el icono de ojo de ese objeto se vuelve gris.
Muestra un objeto oculto	Haga clic en el icono de ojo gris del objeto seleccionado en el panel de comparación. El icono de ojo vuelve a su color original y los datos del objeto se vuelven a añadir a los gráficos del panel ContraCharts.

3. **Opcional:** elimine los objetos seleccionados del panel **comparando**:

Para hacer esto…	Realice esta acción…
Quitar un objeto seleccionado	Coloque el puntero sobre el nombre del objeto seleccionado en el panel de comparación para mostrar el botón de eliminación de objeto (**X**) y, a continuación, haga clic en el botón. El objeto se elimina del panel comparativo y sus datos se borran de los gráficos de contadores.
Quite todos los objetos seleccionados	Haga clic en el botón para eliminar todos los objetos (**X**) situado en la parte superior del panel de comparación. Se quitan todos los objetos seleccionados y sus datos, dejando sólo el objeto raíz.

Gráficos de contadores

Los gráficos del panel gráficos de contador permiten ver y comparar los datos de rendimiento del objeto raíz y de los objetos agregados a partir de la cuadrícula de objetos correlacionados. Esto puede ayudarle a comprender las tendencias de rendimiento y

aislar y resolver problemas de rendimiento.

Los gráficos de contadores que se muestran de forma predeterminada son Events, Latency, IOPS y Mbps. Los gráficos opcionales que puede decidir mostrar son la utilización, la capacidad de rendimiento utilizada, las IOPS disponibles, las IOPS/TB y la ratio de excepciones de caché. Además, puede elegir ver valores totales o valores de desglose de los gráficos latencia, IOPS, Mbps y capacidad de rendimiento utilizados.

El Explorador de rendimiento muestra ciertos gráficos de contadores de forma predeterminada, si el objeto de almacenamiento lo admite todo o no. Cuando no se admite un contador, el gráfico de contadores está vacío y el mensaje `Not applicable for <object>` aparece en pantalla.

Los gráficos muestran las tendencias de rendimiento del objeto raíz y de todos los objetos seleccionados en el panel de comparación. Los datos de cada gráfico se organizan de la siguiente manera:

- **Eje X**

  Muestra el período de tiempo especificado. Si no ha especificado un intervalo de tiempo, el valor predeterminado es el período anterior de 72 horas.

- **Eje y**

  Muestra las unidades de contador únicas para el objeto u objetos seleccionados.

Los colores de las líneas de tendencias coinciden con el color del nombre del objeto tal como se muestra en el panel de comparación. Puede colocar el cursor sobre un punto de cualquier línea de tendencia para ver detalles de tiempo y valor para ese punto.

Si desea investigar un período de tiempo específico dentro de un gráfico, puede utilizar uno de los siguientes métodos:

- Utilice el botón **<** para expandir el panel Contador de gráficos para extender el ancho de la página.
- Utilice el cursor (cuando se pase a una lupa) para seleccionar una parte del período de tiempo de la carta para enfocar y ampliar esa área. Puede hacer clic en Restablecer zoom gráfico para devolver el gráfico al período de tiempo predeterminado.
- Utilice el botón **Zoom View** para mostrar un gran gráfico de contador único que contiene detalles ampliados e indicadores de umbral.

> En ocasiones, aparecen separaciones en las líneas de tendencias. Estos vacíos indican que Unified Manager no pudo recoger datos de rendimiento del sistema de almacenamiento o que Unified Manager podría haber estado inactivo.

Tipos de gráficos de contadores de rendimiento

Hay gráficos de rendimiento estándar que muestran los valores de contador para el objeto de almacenamiento seleccionado. Cada uno de los gráficos de contadores de desglose muestra los valores totales separados en categorías de lectura, escritura y otras. Además, algunos gráficos de contadores de desglose muestran detalles adicionales cuando el gráfico se muestra en la vista Zoom.

La siguiente tabla muestra los gráficos de contadores de rendimiento disponibles.

Gráficos disponibles	Descripción del gráfico
Eventos	Muestra eventos críticos, de error, de advertencia e información correlacionados con los gráficos estadísticos del objeto raíz. Los eventos de estado se muestran además de los eventos de rendimiento para proporcionar una imagen completa de las razones por las que el rendimiento puede verse afectado.
Latencia: Total	Número de milisegundos necesarios para responder a las solicitudes de aplicaciones. Tenga en cuenta que los valores medios de latencia se ponderan las I/O.
Latencia: Desglose	La misma información que se muestra en Latency total, pero con los datos de rendimiento separados en latencia de lectura, escritura y otra. Esta opción de gráfico solo se aplica cuando el objeto seleccionado es una SVM, nodo, agregado, volumen, LUN, o espacio de nombres.
Latencia: Componentes del clúster	La misma información que se muestra en latencia total, pero con los datos de rendimiento separados en latencia por componente del clúster. Esta opción de gráfico se aplica solo cuando el objeto seleccionado es un volumen.
IOPS - total	Número de operaciones de entrada/salida procesadas por segundo. Cuando se muestra para un nodo, al seleccionar «'total'» se muestra la tasa de IOPS de los datos que se transfieren a través de este nodo que pueden residir en el nodo local o en el remoto, y al seleccionar «'total (local)'» se muestra la tasa de IOPS de los datos que residen únicamente en el nodo actual.

Gráficos disponibles	Descripción del gráfico
Desglose de IOPS	La misma información que se muestra en IOPS total, pero con los datos de rendimiento separados en IOPS de lectura, escritura y otras IOPS. Esta opción de gráfico solo se aplica cuando el objeto seleccionado es una SVM, nodo, agregado, volumen, LUN, o espacio de nombres. Cuando se muestra en la vista Zoom, el gráfico volúmenes muestra los valores de rendimiento mínimo y máximo de la calidad de servicio si está configurado en ONTAP. Cuando se muestra para un nodo, al seleccionar «'desglose» se muestra el desglose de IOPS de los datos que se transfieren a través de este nodo que pueden residir en el nodo local o el remoto, y al seleccionar «'desglose (local)» se muestra el desglose de IOPS de los datos que únicamente residen en el nodo actual.
IOPS: Protocolos	La misma información que se muestra en IOPS total, pero los datos de rendimiento están separados en gráficos individuales para tráfico de protocolos CIFS, NFS, FCP, NVMe e iSCSI. Esta opción de gráfico se aplica solo cuando el objeto seleccionado es una SVM.
IOPS/TB: Total	Número de operaciones de entrada/salida procesadas por segundo según el espacio total que consume la carga de trabajo, en terabytes. También denominado densidad de I/o, este contador mide el rendimiento que ofrece una cantidad de capacidad de almacenamiento determinada. Cuando se muestra en la vista Zoom, el gráfico volúmenes muestra los valores esperado de calidad de servicio y máximo rendimiento, si se configuran en ONTAP. Esta opción de gráfico se aplica solo cuando el objeto seleccionado es un volumen.
MB/s - total	Número de megabytes de datos que se transfieren al objeto y desde él por segundo.

Gráficos disponibles	Descripción del gráfico
MB/s: Desglose	La misma información que se muestra en el gráfico MB/s, pero con los datos de rendimiento separados en lecturas de disco, lecturas de Flash Cache, escrituras y otro. Cuando se muestra en la vista Zoom, el gráfico de volúmenes muestra los valores de rendimiento máximo de la calidad de servicio si se configuró en ONTAP. Esta opción de gráfico solo se aplica cuando el objeto seleccionado es una SVM, nodo, agregado, volumen, LUN, o espacio de nombres. Los datos de Flash Cache solo se muestran para nodos, y solo cuando se instala un módulo Flash Cache en el nodo.
Capacidad de rendimiento utilizada - total	Porcentaje de la capacidad de rendimiento que consume el nodo o el agregado.
Capacidad de rendimiento utilizada: Desglose	La capacidad de rendimiento utilizada de datos separados en los protocolos de usuario y los procesos en segundo plano del sistema. Además, se muestra la cantidad de capacidad de rendimiento libre.
IOPS disponible - total	Número de operaciones de entrada/salida por segundo que están actualmente disponibles (libres) en este objeto. Este número es el resultado de restar las IOPS actualmente usadas a las IOPS totales que Unified Manager calcula que el objeto puede realizar. Esta opción de gráfico sólo se aplica cuando el objeto seleccionado es un nodo o un agregado.
Utilización - total	Porcentaje de recursos disponibles del objeto que se está utilizando. El aprovechamiento indica la utilización de nodos para nodos, utilización de discos para agregados y uso de ancho de banda para puertos. Esta opción de gráfico sólo se aplica cuando el objeto seleccionado es un nodo, agregado o puerto.
Ratio de falta de caché: Total	Porcentaje de solicitudes de lectura de aplicaciones cliente que se devuelven del disco en lugar de ser devueltas de la caché. Esta opción de gráfico se aplica solo cuando el objeto seleccionado es un volumen.

Selección de gráficos de rendimiento para mostrar

La lista desplegable Choose Chart permite seleccionar los tipos de gráficos de contadores de rendimiento para mostrar en el panel Counter Charts. Esto le permite ver datos y contadores específicos según sus requisitos de rendimiento.

Pasos

1. En el panel **Cartas de contador**, haga clic en la lista desplegable **elegir gráficos**.
2. Agregar o quitar gráficos:

Para…	Realice lo siguiente…
Agregar o quitar gráficos individuales	Haga clic en las casillas de verificación situadas junto a los gráficos que desee mostrar u ocultar
Agregue todos los gráficos	Haga clic en **Seleccionar todo**
Eliminar todos los gráficos	Haga clic en **Desseleccionar todo**

Las selecciones del gráfico se muestran en el panel Contador de gráficos. Tenga en cuenta que al agregar gráficos, los nuevos gráficos se insertan en el panel gráficos de contador para que coincidan con el orden de los gráficos enumerados en la lista desplegable elegir gráficos. La selección de gráficos adicionales puede requerir un desplazamiento adicional.

Ampliación del panel Contador de gráficos

Puede expandir el panel de gráficos de contador para que los gráficos sean más grandes y más legibles.

Una vez definidos los objetos de comparación y el intervalo de tiempo de los contadores, puede ver un panel de gráficos de contador más grande. Utilice el botón **<** en la parte central de la ventana del Explorador de rendimiento para expandir el panel.

Paso

1. Expanda o reduzca el panel * Contador Charts*.

Para…	Realice lo siguiente…
Expanda el panel Contador de gráficos para ajustar el ancho de la página	Haga clic en el botón **<**
Reduzca el panel Contador de gráficos a la mitad derecha de la página	Haga clic en el botón **>**

Cambiar el enfoque de los gráficos de contador a un período de tiempo más corto

Puede utilizar el ratón para reducir el intervalo de tiempo para centrarse en un período de tiempo específico en el panel Diagrama de contador o en la ventana Vista de zoom de

gráficos de contador. Esto permite ver una vista más granular y microscópica de cualquier parte de la línea de tiempo de los datos de rendimiento, los eventos y los umbrales.

Lo que necesitará

El cursor debe haber cambiado a una lupa para indicar que esta funcionalidad está activa.

> Cuando se utiliza esta función, que altera la línea de tiempo para mostrar los valores que corresponden a la visualización más granular, el intervalo de fecha y hora del selector **intervalo de tiempo** no cambia de los valores originales del gráfico.

Pasos

1. Para ampliar un período de tiempo específico, haga clic en la lupa y arrastre el ratón para resaltar el área que desea ver en detalle.

   Los valores de contador del período de tiempo que seleccione rellenarán el gráfico de contadores.

2. Para volver al período de tiempo original establecido en el selector **intervalo de tiempo**, haga clic en el botón **Restablecer zoom gráfico**.

   El gráfico de contadores aparece en su estado original.

Visualización de detalles de eventos en la línea de tiempo de eventos

Puede ver todos los eventos y sus detalles relacionados en el panel línea de tiempo de eventos del Explorador de rendimiento. Se trata de un método rápido y eficiente para ver todos los eventos de estado y rendimiento que se produjeron en el objeto raíz durante un intervalo de tiempo especificado, lo que puede ser útil para solucionar problemas de rendimiento.

El panel línea de tiempo de eventos muestra eventos críticos, de error, de advertencia e informativos que se produjeron en el objeto raíz durante el intervalo de tiempo seleccionado. Cada gravedad de evento tiene su propia línea de tiempo. Los eventos únicos y múltiples se representan mediante un punto de evento en la línea de tiempo. Es posible colocar el cursor sobre un punto de evento para ver los detalles del evento. Para aumentar la granularidad visual de varios eventos, puede reducir el intervalo de tiempo. De esta forma, se propagan varios eventos en eventos individuales, lo que le permite ver e investigar por separado cada evento.

Cada punto de evento de rendimiento de la línea de tiempo de eventos se alinea verticalmente con un pico correspondiente en las líneas de tendencias de los gráficos de contadores que se muestran debajo de la línea de tiempo de eventos. Esto proporciona una correlación visual directa entre los eventos y el rendimiento general. Los eventos de salud también se muestran en la línea de tiempo, pero estos tipos de eventos no necesariamente se alinean con un pico en uno de los gráficos de rendimiento.

Pasos

1. En el panel **escala de tiempo de eventos**, coloque el cursor sobre un punto de evento en una línea de tiempo para ver un resumen del evento o eventos en ese punto de evento.

   Un cuadro de diálogo emergente muestra información sobre los tipos de evento, la fecha y la hora en que ocurrieron los eventos, el estado y la duración del evento.

2. Vea los detalles completos de un evento o varios:

Para hacer esto…	Haga clic en esto…
Ver detalles de un solo evento	**Ver detalles del evento** en el cuadro de diálogo emergente.
Ver detalles de varios eventos	**Ver detalles del evento** en el cuadro de diálogo emergente. Al hacer clic en un solo evento en el cuadro de diálogo varios eventos, se muestra la página correspondiente Event Details.

Vista de zoom de las cartas de contador

Los gráficos de contador proporcionan una vista Zoom que le permite ampliar los detalles de rendimiento durante el período de tiempo especificado. Esto permite ver detalles y eventos de rendimiento con una granularidad mucho más alta, lo que es beneficioso cuando se solucionan problemas de rendimiento.

Cuando se muestra en Zoom View, algunos de los gráficos de desglose proporcionan información adicional de la que aparece cuando el gráfico no está en Zoom View. Por ejemplo, el gráfico de desglose de IOPS, IOPS/TB y Mbps las páginas Zoom View muestran los valores de políticas de calidad de servicio de los volúmenes y LUN si se establecen en ONTAP.

En el caso de las políticas de umbral de rendimiento definidas por el sistema, en la lista **políticas** sólo están disponibles las políticas «'Recursos nodo sobreutilizados'» y «'límite de rendimiento QoS incumplido'». Las demás políticas de umbral definidas por el sistema no están disponibles en este momento.

Visualización de la vista Zoom de las cartas del contador

La vista de zoom de Counter Charts proporciona un nivel más preciso de detalle para el gráfico de contadores seleccionado y su línea de tiempo asociada. Esto amplía los datos del gráfico de contadores, lo que le permite tener una visión más nítida de los eventos de rendimiento y sus causas subyacentes.

Puede visualizar la vista de zoom de las cartas de contador para cualquier gráfico de contadores.

Pasos

1. Haga clic en **Zoom View** para abrir la carta seleccionada una nueva ventana del explorador.
2. Si está viendo un gráfico de desglose y, a continuación, hace clic en **Zoom View**, el gráfico de desglose se muestra en Zoom View. Puede seleccionar **total** mientras está en Zoom View si desea cambiar la opción de vista.

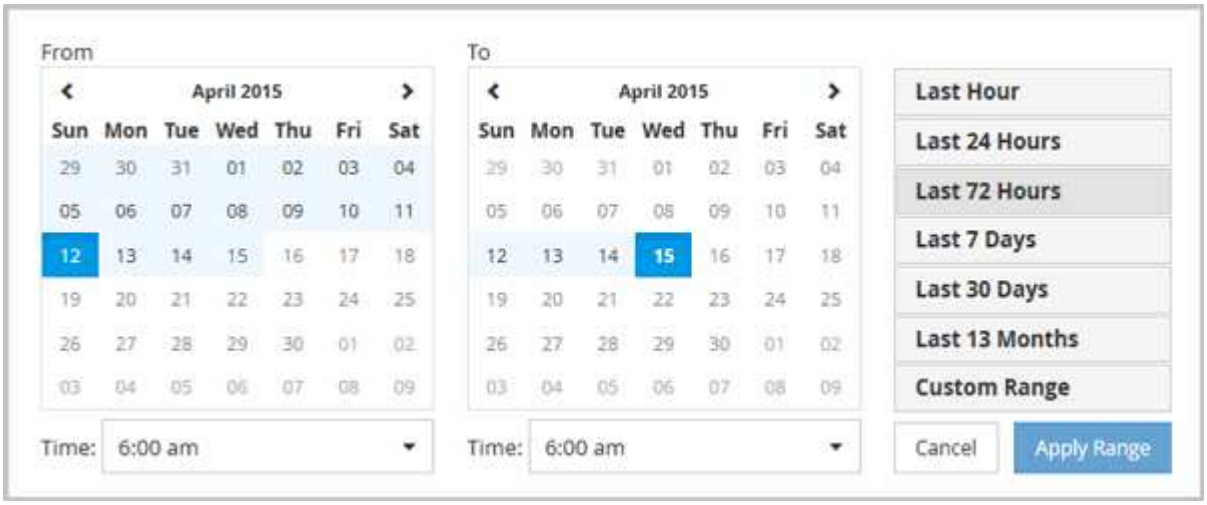
Especificación del intervalo de tiempo en la vista Zoom

El control **intervalo de tiempo** de la ventana de vista de zoom de los gráficos de contador permite especificar un intervalo de fecha y hora para el gráfico seleccionado. Esto le permite localizar rápidamente datos específicos según un intervalo de tiempo preestablecido o bien su propio intervalo de tiempo personalizado.

Puede seleccionar un intervalo de tiempo entre una hora y 390 días. 13 meses equivale a 390 días porque cada mes se cuenta como 30 días. La especificación de un intervalo de fechas y horas proporciona más detalles y le permite ampliar determinados eventos de rendimiento o series de eventos. La especificación de un intervalo de tiempo también ayuda a solucionar problemas potenciales de rendimiento, ya que al especificar un intervalo de fecha y tiempo se muestran los datos que rodean el evento de rendimiento con más detalle. Utilice el control **intervalo de tiempo** para seleccionar intervalos de fecha y hora predefinidos o especifique su propio intervalo de fecha y hora personalizado de hasta 390 días. Los botones de los intervalos de tiempo predefinidos varían de **última hora** a **últimos 13 meses**.

Al seleccionar la opción **últimos 13 meses** o especificar un intervalo de fechas personalizado superior a 30 días, se muestra un cuadro de diálogo en el que se informa de que los datos de rendimiento mostrados durante un período superior a 30 días se registran utilizando promedios por hora y no un sondeo de datos de 5 minutos. Por lo tanto, podría producirse una pérdida de granularidad visual de la línea de tiempo. Si hace clic en la opción **no volver a mostrar** del cuadro de diálogo, el mensaje no aparece cuando selecciona la opción **últimos 13 meses** o especifica un intervalo de fechas personalizado superior a 30 días. Los datos de resumen también se aplican en un intervalo de tiempo menor, si el intervalo de tiempo incluye una hora/fecha que es superior a 30 días a partir de hoy.

Al seleccionar un intervalo de tiempo (personalizado o predefinido), los intervalos de tiempo de 30 días o menos se basan en muestras de datos de intervalo de 5 minutos. Los intervalos de tiempo superiores a 30 días se basan en muestras de datos de intervalo de una hora.



1. Haga clic en el cuadro desplegable **intervalo de tiempo** y aparecerá el panel intervalo de tiempo.
2. Para seleccionar un intervalo de tiempo predefinido, haga clic en uno de los botones **última…** situados a la derecha del panel **intervalo de tiempo**. Al seleccionar un intervalo de tiempo predefinido, se dispone de datos de hasta 13 meses. El botón de intervalo de tiempo predefinido que ha seleccionado se resalta y los días y la hora correspondientes se muestran en los calendarios y selectores de tiempo.
3. Para seleccionar un intervalo de fechas personalizado, haga clic en la fecha de inicio en el calendario **de** de la izquierda. Haga clic en **<** o **>** para navegar hacia delante o hacia atrás en el calendario. Para especificar la fecha de finalización, haga clic en una fecha del calendario **a** de la derecha. Tenga en cuenta que la fecha de finalización predeterminada es hoy a menos que especifique una fecha de finalización

diferente. El botón **intervalo personalizado** situado a la derecha del panel intervalo de tiempo está resaltado, lo que indica que ha seleccionado un intervalo de fechas personalizado.

4. Para seleccionar un intervalo de tiempo personalizado, haga clic en el control **Time** situado debajo del calendario **from** y seleccione la hora de inicio. Para especificar la hora de finalización, haga clic en el control **Time** situado debajo del calendario **to** de la derecha y seleccione la hora de finalización. El botón **intervalo personalizado** situado a la derecha del panel intervalo de tiempo está resaltado, lo que indica que ha seleccionado un intervalo de tiempo personalizado.
5. Opcionalmente, puede especificar las horas de inicio y finalización al seleccionar un intervalo de fechas predefinido. Seleccione el intervalo de fechas predefinido como se ha descrito anteriormente y, a continuación, seleccione las horas de inicio y de finalización como se ha descrito anteriormente. Las fechas seleccionadas se resaltan en los calendarios, las horas de inicio y finalización especificadas aparecen en los controles **Time** y el botón **Custom Range** se resalta.
6. Después de seleccionar el intervalo de fecha y hora, haga clic en **aplicar rango**. Las estadísticas de rendimiento de ese intervalo de tiempo se muestran en los gráficos y en la línea de tiempo Eventos.

Selección de umbrales de rendimiento en la vista Zoom de gráficos de contador

La aplicación de umbrales en la vista Zoom de gráficos de contador proporciona una vista detallada de las ocurrencias de eventos de umbral de rendimiento. Esto le permite aplicar o eliminar umbrales y ver inmediatamente los resultados, lo cual puede ser útil a la vez que decide si la solución de problemas debe ser el siguiente paso.

La selección de umbrales en la vista de zoom de gráficos de contador permite ver datos precisos acerca de los eventos de umbral de rendimiento. Puede aplicar cualquier umbral que aparezca en el área **políticas** de la vista de zoom de los gráficos de contador.

Sólo se puede aplicar una directiva cada vez al objeto en la vista Zoom de los gráficos de contador.

Paso

1. Seleccione o anule la selección de esto está asociado a una política.

   El umbral seleccionado se aplica a la vista de zoom de Counter Charts. Los umbrales críticos se muestran como una línea roja; los umbrales de advertencia se muestran como una línea amarilla.

Ver la latencia de volumen por componente del clúster

Puede ver información detallada sobre la latencia de un volumen mediante la página Volume Performance Explorer. El gráfico de contadores Latency - total muestra la latencia total en el volumen, y el gráfico de contadores Latency - Breakdown es útil para determinar el impacto de la latencia de lectura y escritura en el volumen.

Además, el gráfico latencia - componentes del clúster muestra una comparación detallada de la latencia de cada componente del clúster para ayudar a determinar cómo contribuye cada componente a la latencia total del volumen. Se muestran los siguientes componentes del clúster:

- Red
- Límite máximo de QoS
- Límite mín. De QoS
- Procesamiento de red

- Interconexión en clúster
- Procesamiento de datos
- Operaciones de agregado
- Activación del volumen
- Recursos de MetroCluster
- Latencia del cloud
- SnapMirror sincronizado

Pasos

1. En la página **Explorador de rendimiento de volumen** del volumen seleccionado, en el gráfico latencia, seleccione **componentes de clúster** en el menú desplegable.

   Se muestra el gráfico latencia - componentes del clúster.

2. Para ver una versión más grande del gráfico, seleccione **Zoom View**.

   Se muestra el gráfico comparativo de componentes del clúster. Puede restringir la comparación anulando o seleccionando la que se asocia con cada componente del clúster.

3. Para ver los valores específicos, mueva el cursor hacia el área del gráfico para ver la ventana emergente.

Ver tráfico de IOPS de SVM por protocolo

Puede ver información detallada sobre las IOPS de una SVM mediante la página Performance/SVM Explorer. El gráfico de contadores IOPS - total muestra el uso total de IOPS en la SVM, y el gráfico de contadores IOPS - Breakdown es útil para determinar el impacto de las operaciones de lectura, escritura y otras IOPS en la SVM.

Además, en el gráfico IOPS - Protocolos se muestra una comparación detallada del tráfico de IOPS de cada protocolo que se utiliza en la SVM. Están disponibles los siguientes protocolos:

- CIFS
- NFS
- FCP
- ISCSI
- NVMe

Pasos

1. En la página **Performance/SVM Explorer** de la SVM seleccionada, en el gráfico IOPS, seleccione **Protocolos** en el menú desplegable.

   Se muestra el gráfico IOPS - Protocolos.

2. Para ver una versión más grande del gráfico, seleccione **Zoom View**.

   Se muestra el gráfico comparativo del protocolo IOPS avanzado. Puede restringir la comparación anulando o seleccionando la que está asociado a un protocolo.

3. Para ver los valores específicos, mueva el cursor al área de gráfico de cualquier gráfico para ver la

ventana emergente.

Vea los gráficos de latencia de volúmenes y LUN para verificar la garantía de rendimiento

Puede ver los volúmenes y LUN que ha suscrito al programa «'Garantía de rendimiento» para comprobar que la latencia no ha superado el nivel que se le ha garantizado.

La garantía de rendimiento de latencia es un valor de milisegundos por operación que no se debe superar. Se basa en un promedio por hora, no en el período predeterminado de recopilación de rendimiento de cinco minutos.

Pasos

1. En la vista **rendimiento: Todos los volúmenes** o **rendimiento: Todas las LUN**, seleccione el volumen o LUN en el que esté interesado.
2. En la página **Explorador de rendimiento** para el volumen o LUN seleccionados, elija **Promedio por hora** en el selector **Ver estadísticas en**.

   La línea horizontal del gráfico latencia mostrará una línea más suave ya que las colecciones de cinco minutos se sustituyen por la media por hora.

3. Si tiene otros volúmenes en el mismo agregado que están bajo la garantía de rendimiento, puede añadir esos volúmenes para ver su valor de latencia en el mismo gráfico.

Visualización del rendimiento de los clústeres de cabinas All SAN

Es posible usar la vista Performance: All Clusters para mostrar el estado de rendimiento de los clústeres de cabina All SAN.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Se puede ver información general de todos los clústeres de cabina SAN en la vista Performance: All Clusters y detalles en la página Cluster / Performance Explorer.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **clústeres**.
2. Asegúrese de que la columna "'Personality'" se muestra en la vista **Salud: Todos los clusters**, o añádala utilizando el control **Mostrar / Ocultar**.

   Esta columna muestra «"cabina All SAN»» de los clústeres de la cabina All SAN.

3. Para ver información sobre el rendimiento en esos clústeres, seleccione la vista **rendimiento: Todos los clústeres**.

   Consulte la información de rendimiento del clúster de la cabina All SAN.

4. Para ver información detallada sobre el rendimiento de esos clústeres, haga clic en el nombre de un clúster de cabina All SAN.
5. Haga clic en la ficha **Explorer**.

6. En la página **Cluster / Performance Explorer**, seleccione **Nodes en este clúster** en el menú **Ver y Comparar**.

   Puede comparar las estadísticas de rendimiento de ambos nodos en este clúster para asegurarse de que la carga es casi idéntica en ambos nodos. Si existen grandes discrepancias entre los dos nodos, puede añadir el segundo nodo a los gráficos y comparar los valores a lo largo de un periodo de tiempo más largo para identificar cualquier problema de configuración.

Ver las IOPS de los nodos según las cargas de trabajo que solo residen en el nodo local

El gráfico de contadores IOPS del nodo puede destacar dónde las operaciones solo pasan por el nodo local mediante una LIF de red para realizar operaciones de lectura/escritura en volúmenes de un nodo remoto. Los gráficos IOPS: «'total (local)'» y «'desglose (local)'» muestran la tasa de IOPS de los datos almacenados en volúmenes locales únicamente en el nodo actual.

Las versiones «local» de estos gráficos de contadores son similares a los gráficos de nodos de la capacidad de rendimiento y la utilización porque también muestran solo las estadísticas de los datos que residen en volúmenes locales.

Comparando las versiones "'local'" de estos gráficos de contadores con las versiones totales normales de estos gráficos de contadores, puede ver si hay mucho tráfico que se mueve por el nodo local para acceder a los volúmenes del nodo remoto. Esta situación podría ocasionar problemas de rendimiento, que se podrían indicar con un uso elevado en el nodo, si hay demasiadas operaciones que pasan por el nodo local para llegar a un volumen en un nodo remoto. En estos casos puede que desee mover un volumen al nodo local o crear una LIF en el nodo remoto donde se pueda conectar el tráfico de hosts que acceden a ese volumen.

Pasos

1. En la página **Performance/Node Explorer** del nodo seleccionado, en el gráfico IOPS, seleccione **total** en el menú desplegable.

   Se muestra el gráfico IOPS - total.

2. Haga clic en **Zoom View** para mostrar una versión más grande del gráfico en una nueva pestaña del navegador.
3. De nuevo en la página **Performance/Node Explorer**, en el gráfico IOPS, seleccione **total (local)** en el menú desplegable.

   Se muestra el gráfico IOPS - total (local).

4. Haga clic en **Zoom View** para mostrar una versión más grande del gráfico en una nueva pestaña del navegador.
5. Vea los dos gráficos junto a los otros e identifique áreas donde los valores de IOPS parecen ser muy diferentes.
6. Mueva el cursor por estas áreas para comparar la tasa de IOPS local y total de un momento específico.

Componentes de las páginas de destino de objetos

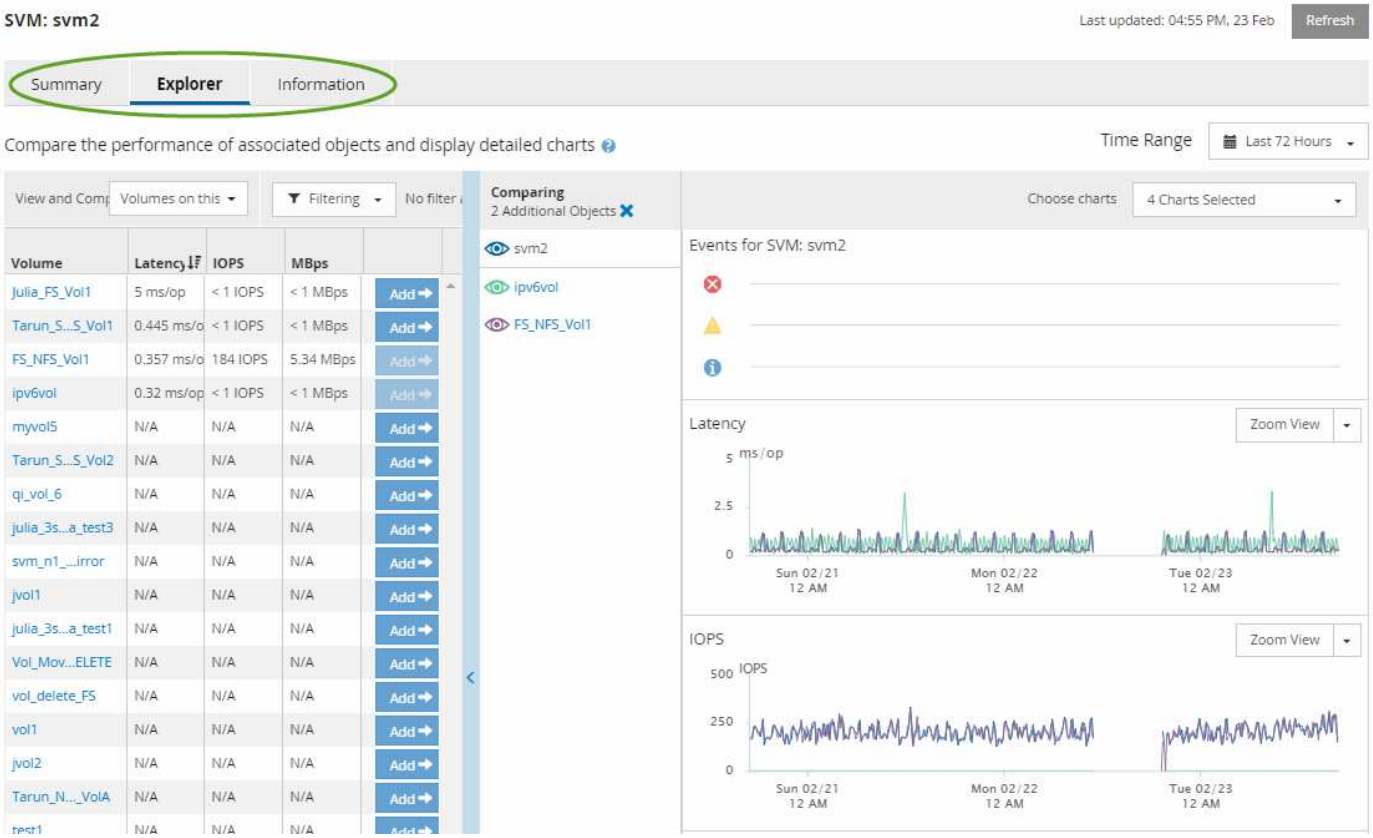
Las páginas de destino de objetos proporcionan información sobre todos los eventos críticos, de advertencia e informativos. Proporcionan una vista detallada del rendimiento

de todos los objetos del clúster, lo que permite seleccionar y comparar objetos individuales durante varios periodos de tiempo.

Las páginas de destino de objetos permiten examinar el rendimiento general de todos los objetos y comparar los datos de rendimiento de los objetos en un formato paralelo. Esto es beneficioso para evaluar el rendimiento y para resolver problemas de eventos.

> Los datos mostrados en los paneles de resumen de contadores y en los gráficos de contador se basan en un intervalo de muestreo de cinco minutos. Los datos que se muestran en la cuadrícula de inventario de objetos situada en la parte izquierda de la página se basan en un intervalo de muestreo de una hora.

En la siguiente imagen se muestra un ejemplo de una página de destino de objetos que muestra la información del explorador:



Dependiendo del objeto de almacenamiento que se esté viendo, la página de inicio de objetos puede tener las siguientes pestañas que proporcionan datos de rendimiento acerca del objeto:

- Resumen

  Muestra tres o cuatro gráficos de contadores que contienen los eventos y el rendimiento por objeto durante el período anterior de 72 horas, incluida una línea de tendencia que muestra los valores alto y bajo durante ese período.

- Explorador

  Muestra una cuadrícula de objetos de almacenamiento relacionados con el objeto actual, lo que permite comparar los valores de rendimiento del objeto actual con los de los objetos relacionados. Esta ficha incluye hasta once contadores gráficos y un selector de rango de tiempo, que le permiten realizar una

variedad de comparaciones.

- Información

  Muestra los valores de los atributos de configuración que no tienen rendimiento acerca del objeto de almacenamiento, incluida la versión instalada del software ONTAP, el nombre del partner de alta disponibilidad y el número de puertos y LIF.

- Mejores artistas

  Para los clústeres: Muestra los objetos de almacenamiento con el mayor rendimiento o el menor, según el contador de rendimiento que seleccione.

- Planificación de conmutación por error

  Para los nodos: Muestra la estimación del impacto sobre el rendimiento de un nodo si el partner de alta disponibilidad del nodo falla.

- Detalles

  Para volúmenes: Se muestran estadísticas detalladas de rendimiento de toda la actividad de I/o y las operaciones de la carga de trabajo de volumen seleccionada. Esta pestaña está disponible para volúmenes FlexVol, volúmenes FlexGroup y componentes de FlexGroups.

Resumen

La página Summary muestra gráficos de contadores que contienen detalles sobre los eventos y el rendimiento por objeto durante el período de 72 horas anterior. Estos datos no se actualizan automáticamente, pero están actualizados a partir de la última carga de página. Los gráficos de la página Resumen responden a la pregunta *do I need to look foulterior?*

Gráficos y estadísticas de contadores

Los gráficos resumidos proporcionan una visión general rápida de alto nivel para el último período de 72 horas y le ayudan a identificar posibles problemas que requieren una investigación adicional.

Las estadísticas del contador de páginas Summary se muestran en los gráficos.

Puede colocar el cursor sobre la línea de tendencias de un gráfico para ver los valores de contador de un momento específico. Los gráficos resumidos también muestran el número total de eventos críticos y de advertencia activos para el período anterior de 72 horas para los siguientes contadores:

- **Latencia**

  Tiempo de respuesta medio para todas las solicitudes de I/o; se expresa en milisegundos por operación.

  Se muestra para todos los tipos de objeto.

- **IOPS**

  Velocidad media de funcionamiento; expresada en operaciones de entrada/salida por segundo.

  Se muestra para todos los tipos de objeto.

- **MB/s**

  Rendimiento medio; expresado en megabytes por segundo.

  Se muestra para todos los tipos de objeto.

- **Capacidad de rendimiento utilizada**

  Porcentaje de la capacidad de rendimiento que consume un nodo o un agregado.

  Visualización solo para nodos y agregados.

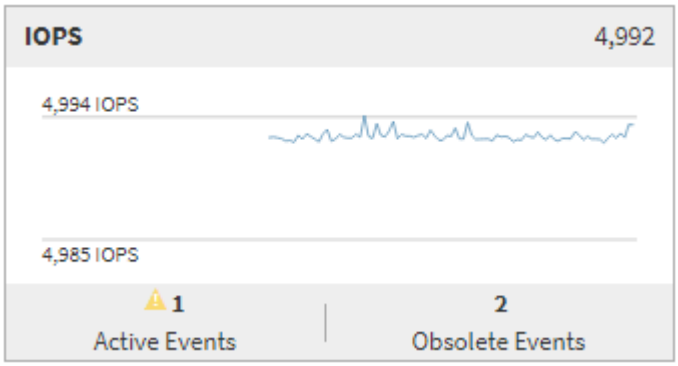
- **Utilización**

  Porcentaje de utilización de objetos para nodos y agregados, o uso de ancho de banda para puertos.

  Se muestra solo para nodos, agregados y puertos.

Al colocar el cursor sobre el número de eventos de eventos activos, se muestra el tipo y el número de eventos. Los eventos críticos se muestran en rojo ( ) y los sucesos de advertencia aparecen en amarillo ( ).

El número situado en la parte superior derecha del gráfico en la barra gris es el valor medio del último período de 72 horas. Los números que se muestran en la parte inferior y superior del gráfico de líneas de tendencia son los valores mínimo y máximo del último período de 72 horas. La barra gris debajo del gráfico contiene el recuento de eventos activos (nuevos y reconocidos) y eventos obsoletos del último período de 72 horas.



- **Tabla de contadores de latencia**

  El gráfico de contadores latencia proporciona una información general de alto nivel de la latencia de objetos para el período de 72 horas anterior. La latencia se refiere al tiempo de respuesta medio para todas las solicitudes de I/o; se expresa en milisegundos por operación, el tiempo de servicio, el tiempo de espera o los dos que tiene un paquete o un bloque de datos en el componente de almacenamiento del clúster que se está considerando.

  Arriba (valor de contador): el número en el cabezal muestra el promedio para el período anterior de 72 horas.

- Medio (gráfico de rendimiento):* el número en la parte inferior del gráfico muestra la menor latencia, y el número en la parte superior del gráfico muestra la latencia más alta para el período anterior de 72 horas. Sitúe el cursor sobre la línea de tendencias del gráfico para ver el valor de latencia de un tiempo específico.
- Inferior (eventos):* al pasar el ratón, el elemento emergente muestra los detalles de los eventos. Haga clic

en el enlace **Eventos activos** situado debajo del gráfico para ir a la página Inventario de eventos para ver los detalles completos del evento.

- **Tabla de contadores IOPS**

  El gráfico de contadores IOPS proporciona una información general de alto nivel del estado IOPS del objeto durante el período de 72 horas anterior. IOPS indica la velocidad del sistema de almacenamiento en el número de operaciones de entrada/salida por segundo.

  Arriba (valor de contador): el número en el cabezal muestra el promedio para el período anterior de 72 horas.

- Medio (gráfico de rendimiento):* el número en la parte inferior del gráfico muestra la tasa de IOPS más baja y el número en la parte superior del gráfico muestra la tasa de IOPS más alta para el período de 72 horas anterior. Sitúe el cursor sobre la línea de tendencias del gráfico para ver el valor de IOPS de un tiempo específico.
- Inferior (eventos):* al pasar el ratón, el elemento emergente muestra los detalles de los eventos. Haga clic en el enlace **Eventos activos** situado debajo del gráfico para ir a la página Inventario de eventos para ver los detalles completos del evento.
- * MB/s counter chart*

  El gráfico de contadores MB/s muestra el rendimiento del objeto MB/s e indica la cantidad de datos que se han transferido al objeto y desde él en megabytes por segundo. El gráfico de contadores MB/s proporciona una descripción general de alto nivel del estado del objeto MB/s durante el período anterior de 72 horas.

  Arriba (valor de contador): el número en el encabezado muestra el número medio de MB/s para el período anterior de 72 horas.

- Medio (gráfico de rendimiento):* el valor en la parte inferior del gráfico muestra el número más bajo de MB/s, y el valor en la parte superior del gráfico muestra el número más alto de MB/s para el período anterior de 72 horas. Sitúe el cursor sobre la línea de tendencias del gráfico para ver el valor de MB/s de un tiempo específico.
- Inferior (eventos):* al pasar el ratón, el elemento emergente muestra los detalles de los eventos. Haga clic en el enlace **Eventos activos** situado debajo del gráfico para ir a la página Inventario de eventos para ver los detalles completos del evento.
- * Capacidad de rendimiento usada tabla de contadores*

  El gráfico de contadores Performance Capacity used muestra el porcentaje de la capacidad de rendimiento que consume el objeto.

  Arriba (valor de contador): el número en el cabezal muestra la capacidad de rendimiento media usada para el período anterior de 72 horas.

  Medio (gráfico de rendimiento): el valor en la parte inferior del gráfico muestra el porcentaje de capacidad de rendimiento más bajo utilizado y el valor en la parte superior del gráfico muestra el porcentaje de capacidad de rendimiento más alto utilizado para el período anterior de 72 horas. Coloque el cursor sobre la línea de tendencias del gráfico para ver el valor de capacidad de rendimiento usado durante un tiempo específico.

- Inferior (eventos):* al pasar el ratón, el elemento emergente muestra los detalles de los eventos. Haga clic en el enlace **Eventos activos** situado debajo del gráfico para ir a la página Inventario de eventos para ver los detalles completos del evento.

- **Tabla de contadores de utilización**

  El gráfico de contadores de uso muestra el porcentaje de utilización del objeto. El gráfico de contadores de utilización proporciona una descripción general de alto nivel del porcentaje del objeto o del uso de ancho de banda durante el período de 72 horas anterior.

  Arriba (valor de contador): el número en el encabezado muestra el porcentaje de utilización promedio para el período anterior de 72 horas.

- Medio (gráfico de rendimiento):* el valor en la parte inferior del gráfico muestra el porcentaje de utilización más bajo, y el valor en la parte superior del gráfico muestra el porcentaje de utilización más alto para el período de 72 horas anterior. Sitúe el cursor sobre la línea de tendencias del gráfico para ver el valor de utilización de un tiempo específico.
- Inferior (eventos):* al pasar el ratón, el elemento emergente muestra los detalles de los eventos. Haga clic en el enlace **Eventos activos** situado debajo del gráfico para ir a la página Inventario de eventos para ver los detalles completos del evento.

Eventos

En la tabla del historial de eventos, donde corresponda, se enumeran los eventos más recientes que se han producido en ese objeto. Al hacer clic en el nombre del evento se muestran los detalles del evento en la página Event Details.

Componentes de la página Performance Explorer

La página Performance Explorer le permite comparar el rendimiento de objetos similares en un clúster, por ejemplo, todos los volúmenes de un clúster. Esto resulta beneficioso para la solución de problemas de eventos de rendimiento y el ajuste preciso del rendimiento de objetos. También puede comparar objetos con el objeto raíz, que es la línea base con la que se realizan otras comparaciones de objetos.

Puede hacer clic en el botón **Cambiar a vista de estado** para mostrar la página de detalles de estado de este objeto. En algunos casos, puede obtener información importante sobre la configuración de almacenamiento para el objeto que podría ayudarle a resolver problemas.

La página Performance Explorer muestra una lista de objetos del clúster y sus datos de rendimiento. Esta página muestra todos los objetos de clúster del mismo tipo (por ejemplo, volúmenes y sus estadísticas de rendimiento específicas para objeto) en una tabla de resultados. Esta vista proporciona una descripción eficiente del rendimiento de objetos del clúster.

Si «'N/A'» aparece en cualquier celda de la tabla, significa que un valor para ese contador no está disponible porque no hay E/S en ese objeto en este momento.

La página Performance Explorer contiene los siguientes componentes:

- **Intervalo de tiempo**

  Le permite seleccionar un intervalo de tiempo para los datos del objeto.

  Puede elegir un rango predefinido o especificar un intervalo de tiempo personalizado.

- **Ver y comparar**

Permite seleccionar qué tipo de objeto correlacionado se muestra en la cuadrícula.

Las opciones disponibles dependen del tipo de objeto raíz y sus datos disponibles. Puede hacer clic en la lista desplegable Ver y comparar para seleccionar un tipo de objeto. El tipo de objeto seleccionado se muestra en la lista.

- **Filtrado**

  Le permite limitar la cantidad de datos que recibe, en función de sus preferencias.

  Puede crear filtros que se apliquen a los datos del objeto, por ejemplo, IOPS de mayor de 4. Puede agregar hasta cuatro filtros simultáneos.

- **Comparando**

  Muestra una lista de los objetos seleccionados para su comparación con el objeto raíz.

  Los datos de los objetos del panel de comparación se muestran en los gráficos de contador.

- **Ver estadísticas en**

  Para los volúmenes y los LUN, permite seleccionar si las estadísticas se muestran después de cada ciclo de recogida (predeterminado 5 minutos), o si las estadísticas se muestran como una media por hora. Esta funcionalidad le permite ver el gráfico de latencia al apoyar el programa "Garantía de rendimiento" de NetApp.

- * Contador gráficos*

  Muestra datos gráficos para cada categoría de rendimiento de objeto.

  Normalmente, sólo se muestran tres o cuatro gráficos de forma predeterminada. El componente elegir gráficos permite mostrar gráficos adicionales u ocultar gráficos específicos. También puede elegir mostrar u ocultar la línea de tiempo de los eventos.

- **Calendario de eventos**

  Muestra los eventos de rendimiento y estado que se producen en la línea de tiempo seleccionada en el componente intervalo de tiempo.

Gestione el rendimiento mediante información del grupo de políticas de calidad de servicio

Unified Manager permite ver los grupos de políticas de calidad de servicio (QoS) disponibles en todos los clústeres que supervisa. Las políticas pueden haberse definido mediante el software ONTAP (System Manager o la CLI de ONTAP) o mediante políticas de nivel de servicio de rendimiento de Unified Manager. Unified Manager también muestra qué volúmenes y LUN tienen asignado un grupo de políticas de calidad de servicio.

Para obtener más información sobre el ajuste de la configuración de QoS, consulte "Información general sobre gestión del rendimiento"

Cómo la calidad de servicio de almacenamiento puede controlar el rendimiento de la carga de trabajo

Puede crear un grupo de políticas de calidad de servicio (QoS) para controlar el límite de I/o por segundo (IOPS) o rendimiento (MB/s) para las cargas de trabajo que contiene. Si las cargas de trabajo se encuentran en un grupo de políticas sin un límite establecido, como el grupo de políticas predeterminado, o el límite establecido no cumple con sus necesidades, puede aumentar el límite o mover las cargas de trabajo a un grupo de políticas nuevo o existente que tenga el límite deseado.

Los grupos de políticas de calidad de servicio «¿tradicional» se pueden asignar a cargas de trabajo individuales; por ejemplo, un volumen o una LUN únicos. En este caso, la carga de trabajo puede utilizar el límite de rendimiento completo. También se pueden asignar grupos de políticas de calidad de servicio a varias cargas de trabajo; en cuyo caso, el límite de rendimiento es «esencial» entre las cargas de trabajo. Por ejemplo, un límite de calidad de servicio de 9,000 IOPS asignadas a tres cargas de trabajo restringiría el número de IOPS combinadas de más de 9,000 IOPS.

Los grupos de políticas de calidad de servicio «adaptativas» también pueden asignarse a cargas de trabajo individuales o a varias cargas de trabajo. Sin embargo, incluso cuando se asignan a varias cargas de trabajo, cada carga de trabajo obtiene el límite de rendimiento completo en lugar de compartir el valor de rendimiento con otras cargas de trabajo. Además, las políticas de calidad de servicio adaptativas ajustan automáticamente el valor de rendimiento en función del tamaño del volumen, por carga de trabajo, de modo que se mantenga la ratio de IOPS por terabytes a medida que cambie el tamaño del volumen. Por ejemplo, si el pico se establece en 5,000 IOPS/TB en una política de calidad de servicio adaptativa, un volumen de 10 TB tendrá un rendimiento máximo de 50,000 IOPS. Si el tamaño del volumen cambia más adelante a 20 TB, la calidad de servicio adaptativa ajusta el máximo a 100,000 IOPS.

A partir de ONTAP 9.5, se puede incluir el tamaño de bloque al definir una política de calidad de servicio adaptativa. Esto convierte de forma efectiva la política de un umbral IOPS/TB a un umbral de MB/s para casos en los que las cargas de trabajo utilizan tamaños de bloque muy grandes y, en última instancia, utilizan un gran porcentaje de rendimiento.

En el caso de las políticas de calidad de servicio de los grupos compartidos, cuando las IOPS o MB/s de todas las cargas de trabajo de un grupo de políticas superan el límite establecido, el grupo de políticas limita las cargas de trabajo para restringir su actividad, lo que puede reducir el rendimiento de todas las cargas de trabajo del grupo de políticas. Si la limitación de grupo de políticas genera un evento de rendimiento dinámico, la descripción del evento muestra el nombre del grupo de políticas implicado.

En la vista rendimiento: Todos los volúmenes, es posible ordenar los volúmenes afectados por IOPS y MB/s para ver qué cargas de trabajo tienen el uso más alto que puede haber contribuido al evento. En la página Performance/Volumes Explorer, puede seleccionar otros volúmenes o LUN en el volumen para compararlos con el uso de rendimiento de Mbps o de IOPS de la carga de trabajo afectada.

Al asignar las cargas de trabajo que están utilizando en exceso los recursos del nodo a una configuración de grupo de políticas más restrictiva, el grupo de políticas limita las cargas de trabajo a restringir su actividad, lo que puede reducir el uso de los recursos en ese nodo. Sin embargo, si desea que la carga de trabajo pueda usar más recursos del nodo, puede aumentar el valor del grupo de políticas.

Puede usar System Manager, los comandos de ONTAP o los niveles de servicio de rendimiento de Unified Manager para gestionar grupos de políticas, incluidas las siguientes tareas:

- Crear un grupo de políticas
- Agregar o eliminar cargas de trabajo en un grupo de políticas

- Mover una carga de trabajo entre grupos de políticas
- Cambiar el límite de rendimiento de un grupo de políticas
- Mover una carga de trabajo a otro agregado o nodo

Ver todos los grupos de políticas de calidad de servicio disponibles en todos los clústeres

Puede mostrar una lista de todos los grupos de políticas de calidad de servicio disponibles en los clústeres que Unified Manager supervisa. Esto incluye políticas de calidad de servicio tradicionales, políticas de calidad de servicio adaptativas y políticas de calidad de servicio gestionadas por las políticas de nivel de servicio de Unified Manager Performance.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **grupos de políticas QoS**.

   La vista rendimiento: Grupos de políticas de calidad de servicio tradicionales se muestra de forma predeterminada.

2. Consulte la configuración detallada de cada grupo de políticas tradicional de calidad de servicio disponible.
3. Haga clic en el botón expandir ( ) Junto al nombre del grupo de políticas QoS para ver más detalles sobre el grupo de políticas.
4. En el menú View, seleccione una de las opciones adicionales para ver todos los grupos de políticas de calidad de servicio adaptativos o para ver todos los grupos de políticas de calidad de servicio creados mediante los niveles de servicio de Unified Manager Performance Service.

Ver volúmenes o LUN que estén en el mismo grupo de políticas de calidad de servicio

Puede mostrar una lista de los volúmenes y LUN que se hayan asignado al mismo grupo de políticas de calidad de servicio.

En el caso de los grupos de políticas de calidad de servicio tradicionales «que son » entre varios volúmenes, puede resultar útil ver si determinados volúmenes están utilizando en exceso el rendimiento definido para el grupo de políticas. También puede ser útil para decidir si puede añadir otros volúmenes al grupo de políticas sin un impacto negativo sobre los otros volúmenes.

En el caso de políticas de calidad de servicio adaptativas y de niveles de servicio de Unified Manager Performance, Esto puede ser útil para ver todos los volúmenes o LUN que utilizan un grupo de políticas, de modo que pueda ver qué objetos se verían afectados si cambia la configuración de la política de calidad de servicio.

Pasos

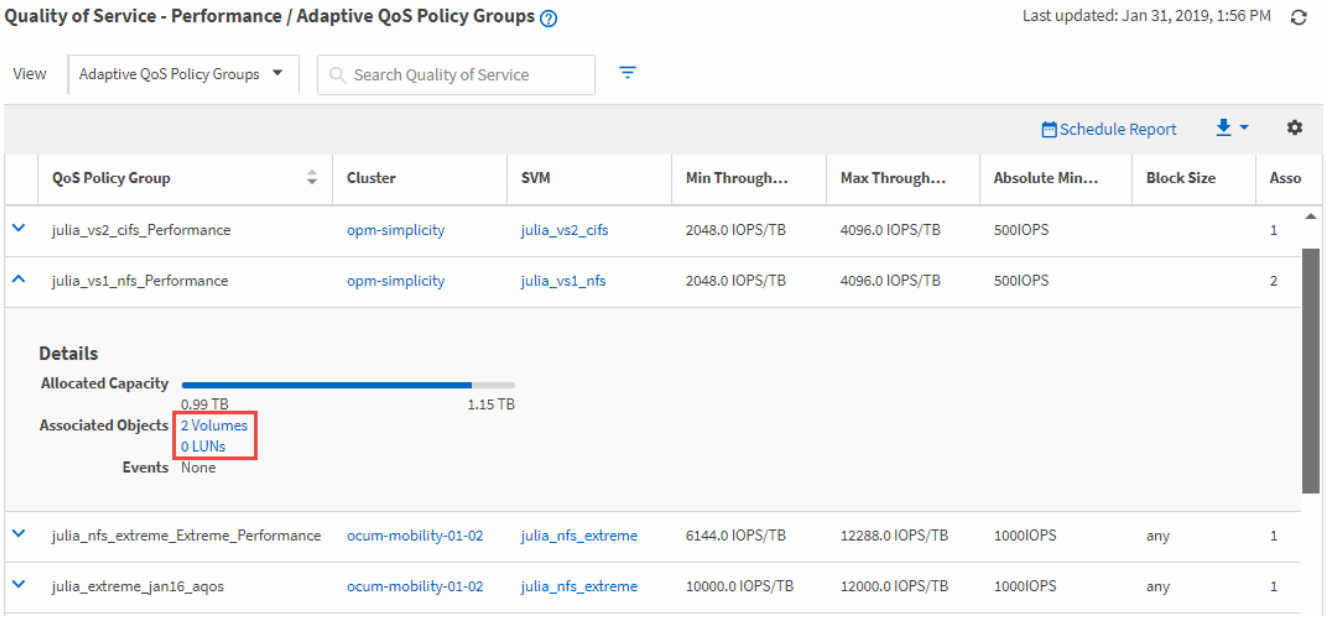
1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **grupos de políticas QoS**.

   La vista rendimiento: Grupos de políticas de calidad de servicio tradicionales se muestra de forma predeterminada.

2. Si usted está interesado en el grupo de políticas tradicionales, quédese en esta página. De lo contrario, seleccione una de las opciones adicionales Ver para mostrar todos los grupos de políticas de calidad de

servicio adaptativos o todos los grupos de políticas de calidad de servicio creados por los niveles de servicio de rendimiento de Unified Manager.

3. En la política QoS que le interesa, haga clic en el botón expandir ( ) Junto al nombre del grupo de políticas QoS para ver más
detalles.



4. Haga clic en el enlace Volumes o LUN para ver los objetos con esta política de calidad de servicio.

   La página Performance Inventory de los volúmenes o LUN se muestra con la lista ordenada de los objetos que está utilizando la política de calidad de servicio.

Ver la configuración del grupo de políticas de calidad de servicio aplicable a volúmenes o LUN específicos

Puede ver los grupos de políticas de calidad de servicio que se aplican a sus volúmenes y LUN y puede vincular a la vista Performance/QoS Policy Groups para mostrar las opciones de configuración detalladas para cada política de calidad de servicio.

A continuación se muestran los pasos para ver la política de calidad de servicio que se aplica a un volumen. Los pasos para ver esta información de una LUN son similares.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.

   El estado: Toda la vista de volúmenes se muestra de forma predeterminada.

2. En el menú Ver, seleccione **rendimiento: Volúmenes en QoS Policy Group**.
3. Localice el volumen que desea revisar y desplácese a la derecha hasta que vea la columna **Grupo de políticas de QoS**.
4. Haga clic en el nombre del grupo de políticas de calidad de servicio.

   La página Quality of Service correspondiente se muestra en función de si es una política de calidad de servicio tradicional, una política de calidad de servicio adaptativa o una política de calidad de servicio que se creó mediante los niveles de servicio de Unified Manager Performance.

5. Consulte los ajustes de configuración detallados del grupo de políticas de QoS.
6. Haga clic en el botón expandir ( ) Junto al nombre del grupo de políticas QoS para ver más detalles sobre el grupo de políticas.

Ver los gráficos de rendimiento para comparar volúmenes o LUN que están en el mismo grupo de políticas de calidad de servicio

Puede ver los volúmenes y las LUN que se encuentran en los mismos grupos de políticas de calidad de servicio y, a continuación, comparar el rendimiento en un único gráfico de IOPS, MB/s o IOPS/TB para identificar cualquier problema.

Los pasos para comparar el rendimiento de los volúmenes en el mismo grupo de políticas de calidad de servicio se muestran a continuación. Los pasos para ver esta información de una LUN son similares.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.

   El estado: Toda la vista de volúmenes se muestra de forma predeterminada.

2. En el menú Ver, seleccione **rendimiento: Volúmenes en QoS Policy Group**.
3. Haga clic en el nombre del volumen que desea revisar.

   Se muestra la página Performance Explorer para el volumen.

4. En el menú Ver y comparar, seleccione **volúmenes en el mismo grupo de políticas QoS**.

   En la tabla siguiente se enumeran los demás volúmenes que comparten la misma política de calidad de servicio.

5. Haga clic en el botón **Agregar** para agregar esos volúmenes a los gráficos para que pueda comparar las IOPS, MB/s, IOPS/TB y otros contadores de rendimiento de todos los volúmenes seleccionados en los gráficos.

   Es posible cambiar el intervalo de tiempo para ver el rendimiento durante diferentes intervalos de tiempo distintos a los predeterminados de 72 horas.

Cómo se muestran los diferentes tipos de políticas de calidad de servicio en los gráficos de rendimiento

Puede ver la configuración de la política de calidad de servicio (QoS) definida por ONTAP que se aplicó a un volumen o LUN en los gráficos Performance Explorer y Workload Analysis IOPS, IOPS/TB y MB/s. La información que se muestra en los gráficos es diferente según el tipo de política de calidad de servicio que se haya aplicado a la carga de trabajo.

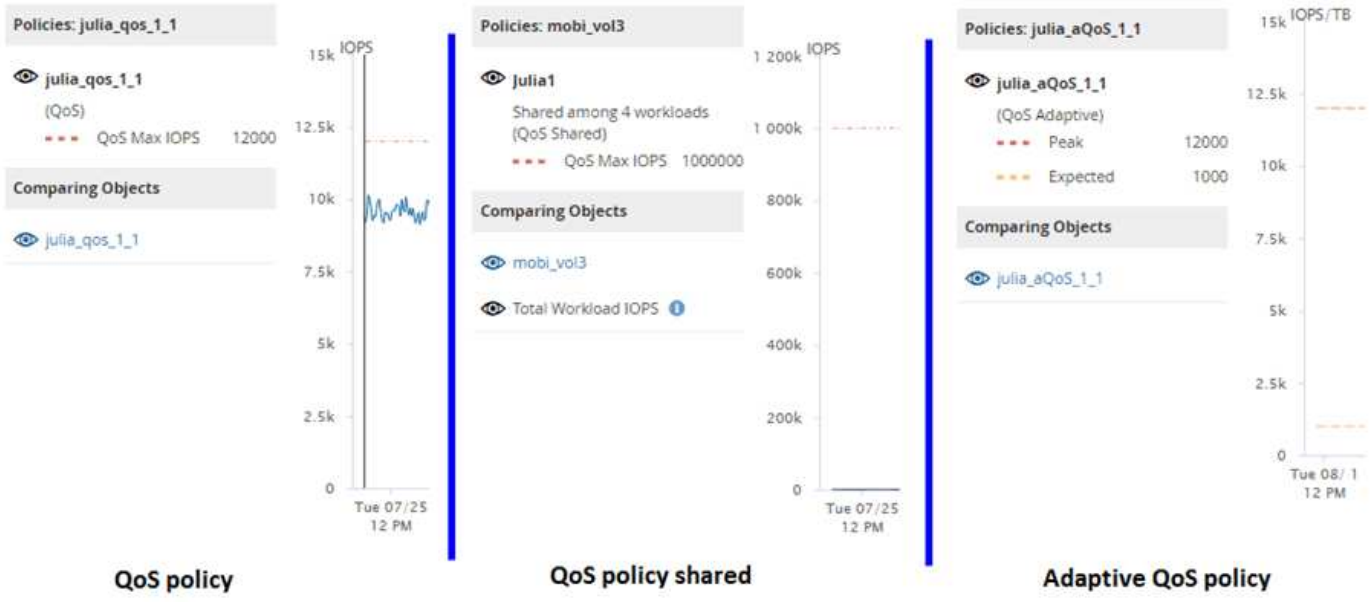
Un ajuste de rendimiento máximo (o «'pico») define el rendimiento máximo que puede consumir la carga de trabajo y, por lo tanto, limita el impacto en las cargas de trabajo de la competencia para los recursos del sistema. La configuración de un rendimiento mínimo (o ««previsto») define el rendimiento mínimo que debe estar disponible para la carga de trabajo de forma que una carga de trabajo crítica satisfaga los objetivos de rendimiento mínimos con independencia de la demanda de otras cargas de trabajo de la competencia.

Las políticas de calidad de servicio compartidas y no compartidas para IOPS y MB/s utilizan los términos «minimum» y «maximum» para definir el suelo y el techo. Las políticas de calidad de servicio adaptativas para IOPS/TB, que se introdujeron en ONTAP 9.3, utilizan los términos «'previsto'» y «'pico» para definir el suelo y el techo.

Aunque ONTAP permite crear estos dos tipos de políticas de calidad de servicio, en función de cómo se apliquen a las cargas de trabajo, hay tres maneras en que la política de calidad de servicio se mostrará en los gráficos de rendimiento.

Tipo de política	Funcionalidad	Indicador en la interfaz de Unified Manager
La política de calidad de servicio compartida se asigna a una sola carga de trabajo, o la política de calidad de servicio no compartida se asigna a una sola carga de trabajo o a varias cargas de trabajo	Cada carga de trabajo puede consumir la configuración de rendimiento especificada	Muestra «»(QoS)».
La política de calidad de servicio compartida se asigna a varias cargas de trabajo	Todas las cargas de trabajo comparten el valor de rendimiento especificado	Muestra «»(QoS compartido)».
La política de calidad de servicio adaptativa asignada a una sola carga de trabajo o a varias cargas de trabajo	Cada carga de trabajo puede consumir la configuración de rendimiento especificada	Muestra «»(QoS adaptativo)».

En la siguiente figura, se muestra un ejemplo de cómo se muestran las tres opciones en los gráficos de contadores.



Cuando se muestra una política de calidad de servicio normal definida en IOPS en el gráfico IOPS/TB para una carga de trabajo, ONTAP convierte el valor de IOPS en un valor de IOPS/TB y Unified Manager muestra esa política en el gráfico IOPS/TB junto con el texto «"QoS, definida en IOPS».

Cuando se muestra una política de calidad de servicio adaptativa que se ha definido en IOPS/TB en el gráfico de IOPS de una carga de trabajo, ONTAP convierte el valor de IOPS/TB en un valor de IOPS y Unified Manager muestra esa política en el gráfico de IOPS junto con el texto "'Adaptive QoS - used, Se define en IOPS/TB' o «"calidad de servicio adaptativa, asignada, definida en IOPS/TB» en función de cómo se configure el valor de asignación pico de IOPS. Cuando el valor de asignación se establece en "'espacio asignado'", el pico de IOPS se calcula en función del tamaño del volumen. Cuando el ajuste de asignación se establece en «'espacio utilizado», el IOPS máximo se calcula en función de la cantidad de datos almacenados en el volumen, teniendo en cuenta las eficiencias del almacenamiento.

El gráfico IOPS/TB muestra los datos de rendimiento solo cuando la capacidad lógica utilizada por el volumen es mayor o igual a 128 GB. Los vacíos se muestran en el gráfico cuando la capacidad utilizada desciende por debajo de los 128 GB durante el periodo de tiempo seleccionado.

Ver la configuración mínima y máxima de calidad de servicio de la carga de trabajo en el Explorador de rendimiento

Puede ver la configuración de la política de calidad de servicio (QoS) definida por ONTAP en un volumen o LUN en los gráficos Performance Explorer. Un ajuste máximo del rendimiento limita el impacto de las cargas de trabajo concurrentes en los recursos del sistema. Un ajuste mínimo de rendimiento garantiza que una carga de trabajo crítica cumpla los objetivos de rendimiento mínimos, sin importar la demanda de otras cargas de trabajo en competencia.

Los valores de rendimiento de QoS «minum» y «m ximum» de IOPS y MB/s se muestran en los gráficos de contadores solo si se han configurado en ONTAP. Los ajustes mínimos de rendimiento están disponibles solo en sistemas que ejecuten el software ONTAP 9.2 o posterior, solo en sistemas AFF. Estos ajustes solo se pueden establecer para IOPS en este momento.

Las políticas de calidad de servicio adaptativas están disponibles a partir de ONTAP 9.3 y se expresan mediante IOPS/TB en lugar de IOPS. Estas políticas ajustan de forma automática el valor de la política de calidad de servicio en función del tamaño del volumen, por carga de trabajo, de modo que se mantenga la ratio de IOPS por terabytes a medida que cambie el tamaño del volumen. Solo puede aplicar un grupo de políticas de calidad de servicio adaptativo en los volúmenes. La terminología «esperada» y «pico» de QoS se utiliza para políticas de QoS adaptables en lugar de como mínimo y máximo.

Unified Manager genera eventos de advertencia para incumplimientos de políticas de calidad de servicio cuando el rendimiento de la carga de trabajo superó la configuración máxima de política de calidad de servicio definida durante cada periodo de recogida de rendimiento de la hora anterior. El rendimiento de la carga de trabajo puede superar el umbral de calidad de servicio durante un breve periodo de tiempo durante cada periodo de recogida, pero Unified Manager muestra el rendimiento «medio» durante el periodo de recogida en el gráfico. Por este motivo, es posible que vea eventos de calidad de servicio mientras el rendimiento de una carga de trabajo no haya superado el umbral de política que se muestra en el gráfico.

Pasos

1. En la página **Explorador de rendimiento** del volumen o LUN seleccionados, realice las siguientes acciones para ver los ajustes de techo y piso de QoS:

Si desea…	Realice lo siguiente…
Ver el techo de IOPS (la calidad de servicio máx.)	En el gráfico total de IOPS o desglose, haga clic en **Zoom View**.
Ver el techo de MB/s (QoS máx.)	En el gráfico total o desglosado MB/s, haga clic en **Zoom View**.
Ver la planta de IOPS (la calidad de servicio mín.)	En el gráfico total de IOPS o desglose, haga clic en **Zoom View**.
Vea el techo de IOPS/TB (la pico de calidad de servicio)	Para los volúmenes, en el gráfico IOPS/TB, haga clic en **Zoom View**.
Ver la superficie de IOPS/TB (calidad de servicio esperada)	Para los volúmenes, en el gráfico IOPS/TB, haga clic en **Zoom View**.

La línea horizontal discontinua indica el valor de rendimiento máximo o mínimo establecido en ONTAP. También puede ver cuándo se han implementado los cambios en los valores de calidad de servicio.

2. Para ver los valores específicos de IOPS y MB/s en comparación con la configuración de QoS, mueva el cursor al área del gráfico para ver la ventana emergente.

Si observa que ciertos volúmenes o LUN tienen un número muy elevado de IOPS o MB/s y están destacando los recursos del sistema, puede usar System Manager o la interfaz de línea de comandos ONTAP para ajustar la configuración de calidad de servicio de forma que estas cargas de trabajo no afecten al rendimiento de otras cargas de trabajo.

Para obtener más información sobre el ajuste de la configuración de QoS, consulte "Información general sobre gestión del rendimiento"

Gestión del rendimiento mediante la capacidad de rendimiento y la información de IOPS disponible

Performance Capacity indica la cantidad de rendimiento que se puede obtener de un recurso sin sobrepasar el rendimiento útil de dicho recurso. Cuando se visualizan a través de los contadores de rendimiento existentes, la capacidad de rendimiento es el punto en el que se obtiene el uso máximo de un nodo o de un agregado antes de que la latencia empeore.

Unified Manager recopila estadísticas de capacidad de rendimiento de nodos y agregados en cada clúster. *Performance Capacity used* es el porcentaje de la capacidad de rendimiento que se está utilizando actualmente y *Performance Capacity Free* es el porcentaje de la capacidad de rendimiento que sigue estando disponible.

Aunque la capacidad de rendimiento libre proporciona un porcentaje del recurso que sigue disponible, *Available IOPS* indica el número de IOPS que se pueden añadir al recurso antes de alcanzar la capacidad de rendimiento máxima. Al utilizar esta métrica, puede asegurarse de poder añadir cargas de trabajo de un número predeterminado de IOPS a un recurso.

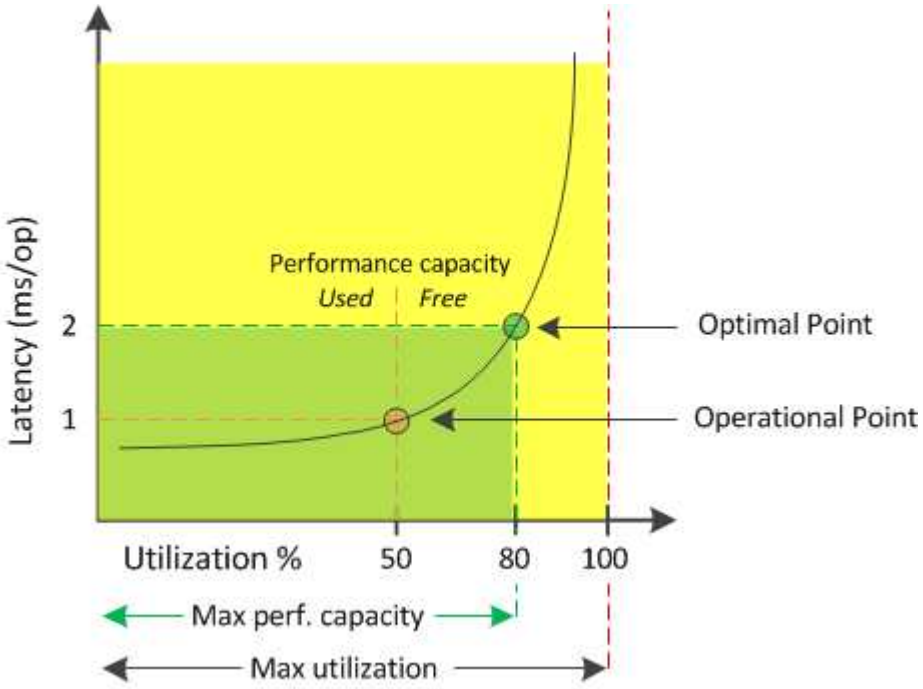
La supervisión de la información de capacidad del rendimiento tiene las siguientes ventajas:

- Ayuda en el aprovisionamiento y equilibrio de flujos de trabajo.
- Ayuda a evitar la sobrecarga de un nodo o la inserción de sus recursos más allá del punto óptimo, lo que reduce la necesidad de solucionar el problema.
- Le ayuda a determinar con mayor precisión dónde puede ser necesario un equipo de almacenamiento adicional.

La capacidad de rendimiento utilizada

La capacidad de rendimiento utilizada contador ayuda a identificar si el rendimiento de un nodo o de un agregado está llegando a un punto en el que el rendimiento puede degradarse si las cargas de trabajo aumentan. También puede mostrarle si un nodo o agregado se está utilizando en exceso durante periodos de tiempo específicos. La capacidad de rendimiento utilizada es similar al de la utilización, pero el primero proporciona más información acerca de las funcionalidades de rendimiento disponibles en un recurso físico para una carga de trabajo específica.

La capacidad de rendimiento óptima utilizada es el punto en el que un nodo o un agregado tienen una utilización y una latencia óptimas (tiempo de respuesta) y se utiliza con eficiencia. En la siguiente figura, se muestra una muestra de latencia frente a utilización de un agregado.



En este ejemplo, el *operational point* identifica que el agregado está funcionando actualmente con una utilización del 50% con una latencia de 1.0 ms/op. A partir de las estadísticas extraídas del agregado, Unified Manager determina que se dispone de capacidad de rendimiento adicional para este agregado. En este ejemplo, el *optimal point* se identifica como el punto en el que el agregado está a 80% de utilización con una latencia de 2.0 ms/op. Por tanto, puede añadir más volúmenes y LUN a este agregado para que sus sistemas se utilicen de forma más eficiente.

Se espera que el contador de capacidad de rendimiento utilizada sea un número mayor que el contador de «'utilización» porque la capacidad de rendimiento aumenta el impacto en la latencia. Por ejemplo, si se utiliza

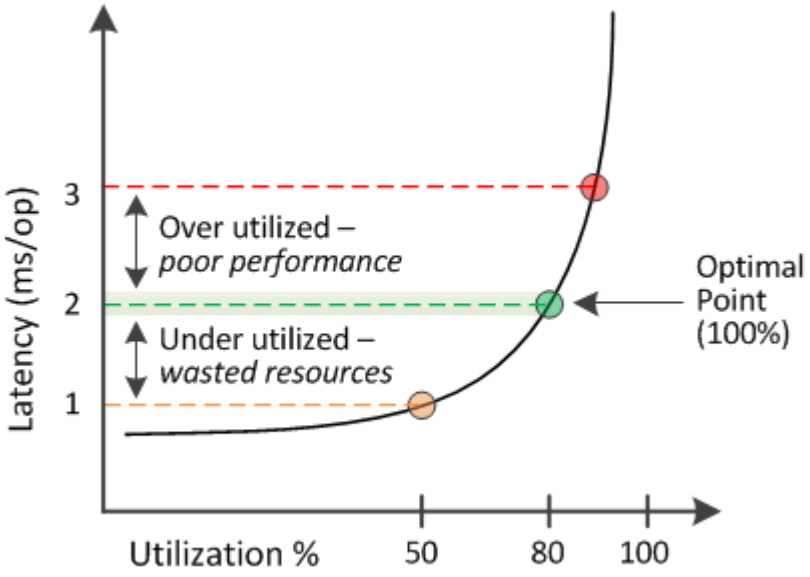
un nodo o un agregado el 70 %, el valor de capacidad de rendimiento puede estar entre el 80 % y el 100 %, según el valor de latencia.

Sin embargo, en algunos casos, el contador de utilización puede ser más alto en la página Dashboard. Esto es normal porque la consola actualiza los valores de contador actuales en cada período de recogida; no muestra promedios durante un periodo de tiempo como las otras páginas de la interfaz de usuario de Unified Manager. El contador de capacidad de rendimiento utilizada se utiliza mejor como indicador de rendimiento promediado durante un período de tiempo, mientras que el contador de utilización se utiliza mejor para determinar el uso instantáneo de un recurso.

Qué significa el valor de capacidad de rendimiento utilizada

El valor de capacidad de rendimiento utilizada le ayuda a identificar los nodos y los agregados que se están utilizando en exceso o están desaprovechados. Esto permite redistribuir las cargas de trabajo para hacer que los recursos de almacenamiento sean más eficientes.

En la siguiente figura, se muestra la curva de latencia frente a utilización de un recurso e se identifican, con puntos de color, tres áreas en las que se podría ubicar el punto operativo actual.



- Un porcentaje de capacidad de rendimiento utilizada igual a 100 se encuentra en el punto óptimo.

  En este momento se están utilizando los recursos de manera eficiente.

- Un porcentaje de capacidad de rendimiento usado superior a 100 indica que el nodo o el agregado están desaprovechados y que las cargas de trabajo están recibiendo un rendimiento inferior al óptimo.

  No se deben agregar cargas de trabajo nuevas al recurso y es posible que sea necesario redistribuir las cargas de trabajo existentes.

- Un porcentaje de capacidad de rendimiento usado inferior a 100 indica que el nodo o el agregado están desaprovechados y que los recursos no se están utilizando correctamente.

  Es posible añadir más cargas de trabajo al recurso.

A diferencia de la utilización, el porcentaje de capacidad de rendimiento utilizada puede ser superior al 100 %. No existe un porcentaje máximo, pero los recursos típicamente estarán en el rango del 110% al 140% cuando se están sobreutilizando. Los porcentajes superiores indicarían un recurso con problemas graves.

Qué es IOPS disponible

El contador de IOPS disponible identifica el número restante de IOPS que se pueden añadir a un nodo o a un agregado antes de que el recurso alcance su límite.

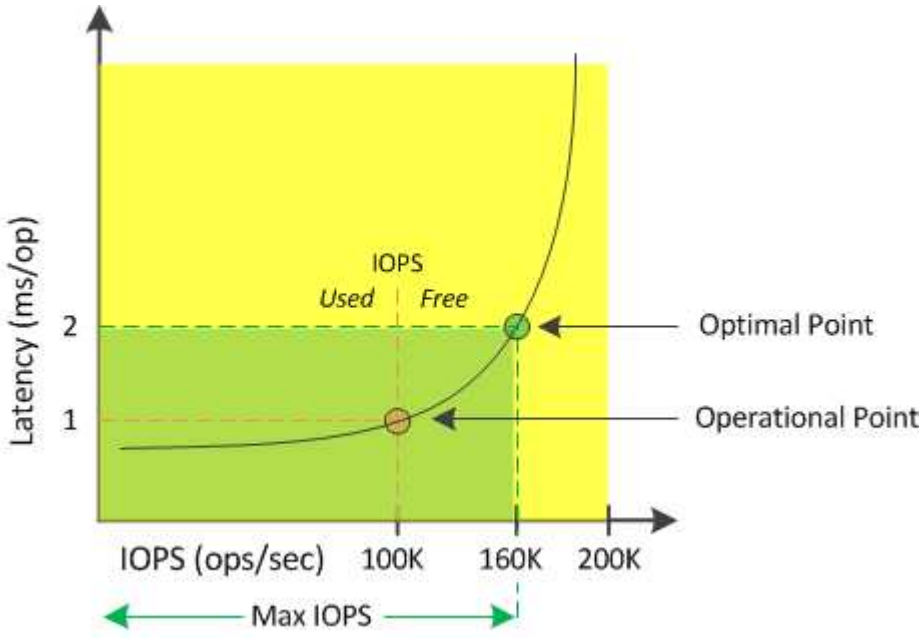
El número total de IOPS que puede proporcionar un nodo se basa en las características físicas del nodo, por ejemplo, el número de CPU, la velocidad de CPU y la cantidad de RAM. El número total de IOPS que puede proporcionar un agregado está basado en las propiedades físicas de los discos, por ejemplo, un disco SATA, SAS o SSD.

El IOPS total de todos los volúmenes de un agregado podría no coincidir con el IOPS total del agregado. Esto se trata en el siguiente artículo de la base de conocimientos: KB "¿Por qué la suma de todas las IOPS de volumen de un agregado no coincide con la IOPS del agregado?"

Aunque el contador libre de capacidad de rendimiento ofrece el porcentaje de un recurso que sigue disponible, el contador de IOPS disponible indica el número exacto de IOPS (cargas de trabajo) puede añadirse a un recurso antes de alcanzar la capacidad de rendimiento máxima.

Por ejemplo, si se utiliza un par de sistemas de almacenamiento FAS2520 y FAS8060, un valor libre de capacidad de rendimiento del 30 % significa que tiene cierta capacidad de rendimiento libre. Sin embargo, ese valor no proporciona visibilidad sobre cuántas cargas de trabajo se pueden implementar en esos nodos. El contador de IOPS disponible puede mostrar que tiene 500 IOPS disponibles en FAS8060, pero solo 100 IOPS disponibles en FAS2520.

En la siguiente figura, se muestra una muestra de latencia frente a curva de IOPS de un nodo.



El número máximo de IOPS que puede proporcionar un recurso es el número de IOPS cuando la capacidad de rendimiento utilizada es del 100 % (el punto óptimo). El punto operativo identifica que el nodo funciona actualmente a 100 000 IOPS con una latencia de 1.0 ms/op. Según las estadísticas capturadas del nodo,

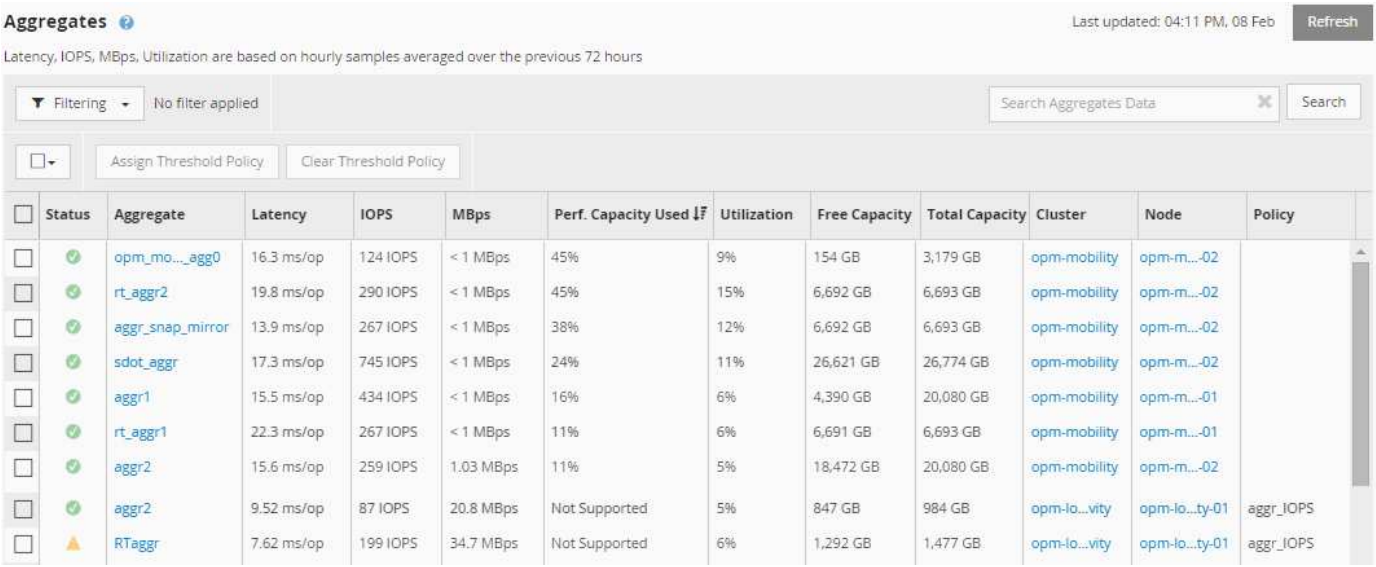
Unified Manager determina que la tasa de IOPS máxima para el nodo es de 160K, lo que significa que hay 60K de IOPS libre o disponible. Por lo tanto, puede añadir más cargas de trabajo a este nodo para que sus sistemas se usen con mayor eficiencia.

Cuando hay una actividad mínima del usuario en el recurso, el valor de IOPS disponible se calcula asumiendo una carga de trabajo genérica en función de aproximadamente 4,500 IOPS por núcleo de CPU. Esto es debido a que Unified Manager carece de los datos para calcular con precisión las características de la carga de trabajo a la que se sirve.

Ver los valores de capacidad de rendimiento de los nodos y los agregados

Puede supervisar los valores de capacidad de rendimiento usada para todos los nodos o todos los agregados de un clúster, o bien puede ver detalles de un solo nodo o de un agregado.

Los valores de capacidad utilizada de rendimiento se muestran en las páginas Dashboard, Performance Inventory, Top Performers, la página Create Threshold Policy, las páginas Performance Explorer y los gráficos detallados. Por ejemplo, la página Performance: All Aggregates proporciona una columna Performance capacidad utilizada para ver el valor de capacidad de rendimiento utilizada para todos los agregados.



Status	Aggregate	Latency	IOPS	MBps	Perf. Capacity Used	Utilization	Free Capacity	Total Capacity	Cluster	Node	Policy
	opm_mo..._agg0	16.3 ms/op	124 IOPS	< 1 MBps	45%	9%	154 GB	3,179 GB	opm-mobility	opm-m...-02	
	rt_aggr2	19.8 ms/op	290 IOPS	< 1 MBps	45%	15%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
	aggr_snap_mirror	13.9 ms/op	267 IOPS	< 1 MBps	38%	12%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
	sdot_aggr	17.3 ms/op	745 IOPS	< 1 MBps	24%	11%	26,621 GB	26,774 GB	opm-mobility	opm-m...-02	
	aggr1	15.5 ms/op	434 IOPS	< 1 MBps	16%	6%	4,390 GB	20,080 GB	opm-mobility	opm-m...-01	
	rt_aggr1	22.3 ms/op	267 IOPS	< 1 MBps	11%	6%	6,691 GB	6,693 GB	opm-mobility	opm-m...-01	
	aggr2	15.6 ms/op	259 IOPS	1.03 MBps	11%	5%	18,472 GB	20,080 GB	opm-mobility	opm-m...-02	
	aggr2	9.52 ms/op	87 IOPS	20.8 MBps	Not Supported	5%	847 GB	984 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS
	RTaggr	7.62 ms/op	199 IOPS	34.7 MBps	Not Supported	6%	1,292 GB	1,477 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS

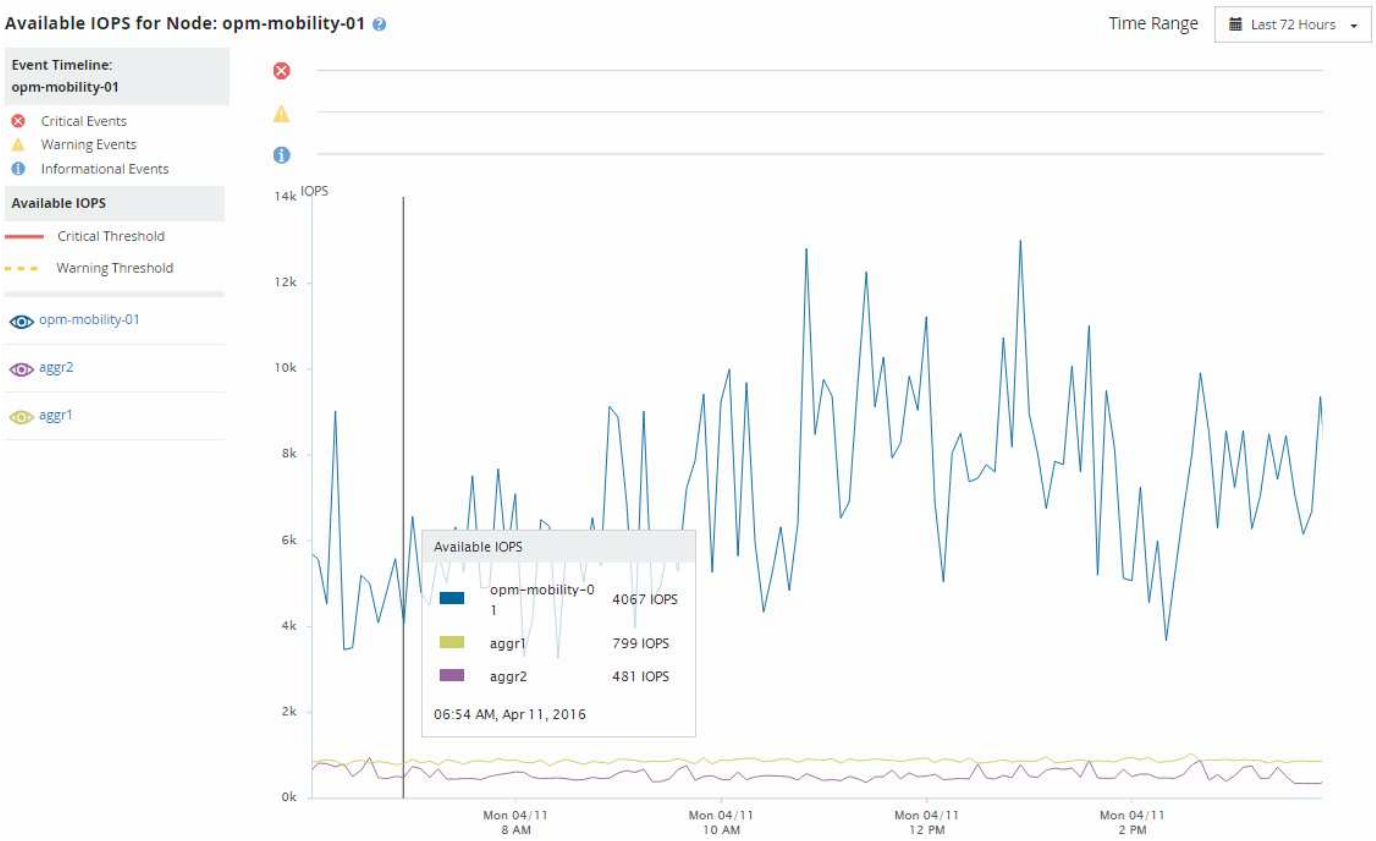
La supervisión de la capacidad de rendimiento utilizada contador permite identificar los siguientes aspectos:

- Si algún nodo o agregado de algún clúster tiene un valor de capacidad de alto rendimiento utilizado
- Si algún nodo o agregado de algún clúster tiene eventos de capacidad de rendimiento activos
- Los nodos y los agregados que tienen el valor de capacidad de rendimiento más alto y bajo en un clúster
- Valores de contador de latencia y uso, junto con nodos o agregados que tienen valores de capacidad de rendimiento elevados utilizados
- Cómo se verá afectada la capacidad de rendimiento utilizada para los nodos en un par de alta disponibilidad si falla uno de los nodos
- Los volúmenes y LUN más activos de un agregado con un valor de capacidad de alto rendimiento utilizada

Ver los valores de IOPS disponibles de los nodos y los agregados

Puede supervisar los valores de IOPS disponibles para todos los nodos o todos los agregados de un clúster, o bien puede ver detalles de un único nodo o agregado.

Los valores de IOPS disponibles se muestran en las páginas Performance Inventory y en los gráficos de página Performance Explorer para nodos y agregados. Por ejemplo, al ver un nodo en la página Node/Performance Explorer, puede seleccionar el gráfico de contadores «'Available IOPS'» de la lista para poder comparar los valores de IOPS disponibles para el nodo y varios agregados de ese nodo.



La supervisión del contador de IOPS disponible le permite identificar:

- Los nodos o agregados que tienen los mayores valores de IOPS disponibles para ayudar a determinar dónde se pueden poner en marcha futuras cargas de trabajo.
- Los nodos o agregados que tienen los valores de IOPS disponibles más pequeños para identificar los recursos que debe supervisar para detectar posibles problemas de rendimiento en el futuro.
- Los volúmenes y LUN más activos en un agregado con un pequeño valor de IOPS disponible.

Ver los gráficos de contadores de capacidad de rendimiento para identificar los problemas

En la página Performance Explorer, se pueden ver los gráficos de capacidad de rendimiento utilizados para nodos y agregados. Esto permite ver datos detallados de capacidad de rendimiento de los nodos y los agregados seleccionados para un periodo específico.

El gráfico de contadores estándar muestra los valores de capacidad de rendimiento utilizados para los nodos

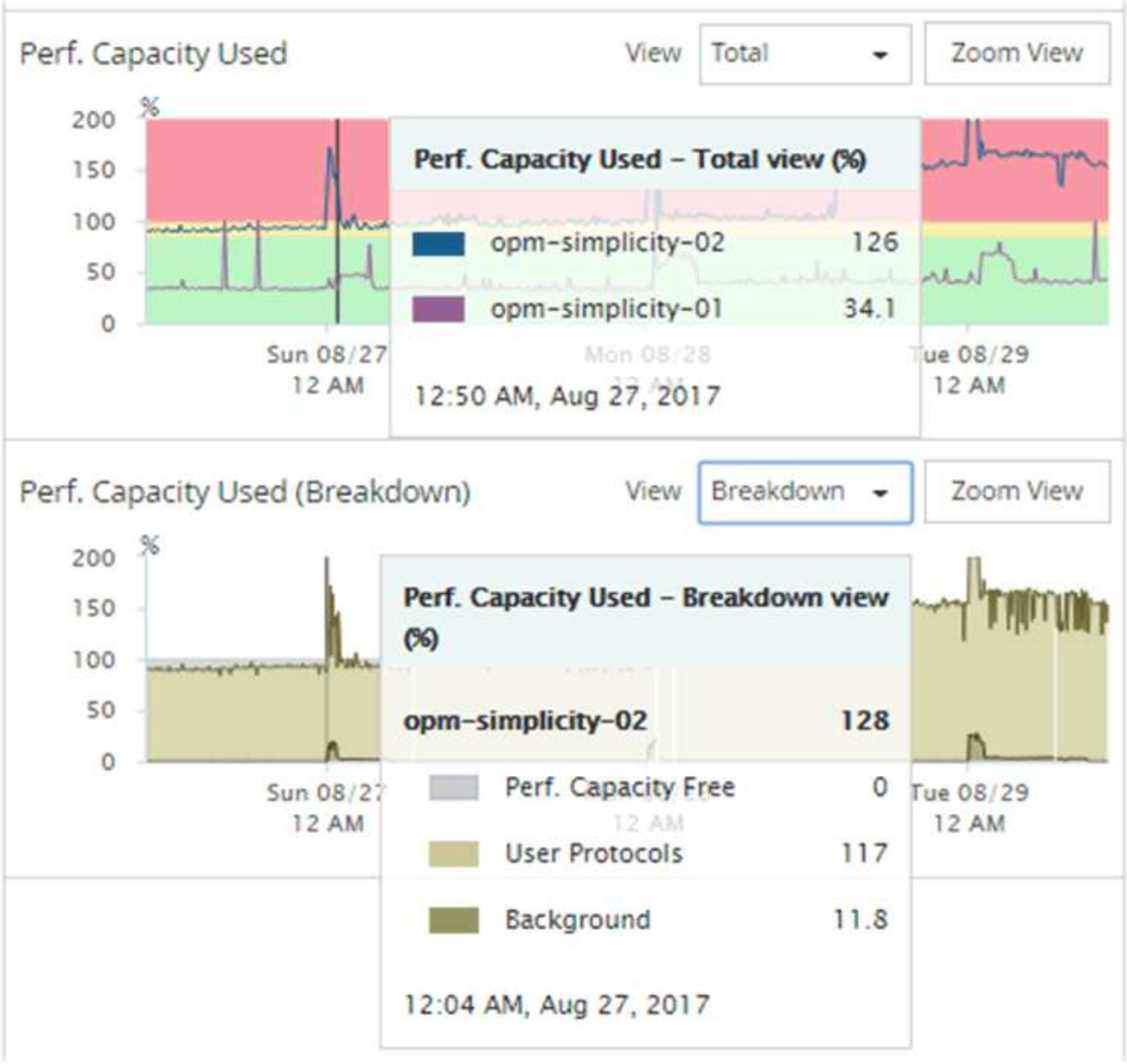
o los agregados seleccionados. El gráfico de contadores Breakdown muestra los valores de capacidad de rendimiento totales para el objeto raíz separados en el uso según los protocolos de usuario frente a los procesos del sistema en segundo plano. Además, también se muestra la cantidad de capacidad de rendimiento libre.

> Dado que algunas actividades en segundo plano asociadas a la gestión de datos y del sistema se identifican como cargas de trabajo de usuario y se clasifican como protocolos de usuario, el porcentaje de protocolos de usuario puede parecer artificialmente alto cuando se ejecutan dichos procesos. Estos procesos normalmente se ejecutan a la medianoche cuando el uso del clúster es bajo. Si ve un pico en la actividad de protocolo del usuario alrededor de la medianoche, compruebe si los trabajos de backup del clúster u otras actividades que se realizan en segundo plano están configurados para ejecutarse en ese momento.

Pasos

1. Seleccione la ficha **Explorer** de una página de nodo o agregado **aterrizaje**.
2. En el panel **Cartas de contador**, haga clic en **elegir gráficos** y, a continuación, seleccione **Perf. Gráfico capacidad utilizada**.
3. Desplácese hacia abajo hasta que pueda ver el gráfico.

   Los colores del gráfico estándar muestran cuando el objeto está en el rango óptimo (amarillo), cuando el objeto está subutilizado (verde) y cuando el objeto está sobreutilizado (rojo). El gráfico detallado muestra detalles detallados de capacidad de rendimiento solo para el objeto raíz.



4. Si desea ver cualquiera de los gráficos en formato de tamaño completo, haga clic en **Zoom View**.

   De esta forma, se pueden abrir varios gráficos de contadores en ventanas diferentes para comparar los valores de capacidad de rendimiento utilizados con los valores de IOPS o Mbps en el mismo periodo de tiempo.

La capacidad de rendimiento utilizada condiciones de umbral de rendimiento

Es posible crear políticas de umbral de rendimiento definidas por el usuario para que los eventos se activen cuando la capacidad de rendimiento utilizada para un nodo o un agregado supera la configuración de umbral de capacidad de rendimiento utilizada definida por el usuario.

Además, los nodos pueden configurarse con una política de umbral «"capacidad de rendimiento utilizada por la adquisición"». Esta política de umbral suma las estadísticas de rendimiento utilizadas en ambos nodos de una pareja de alta disponibilidad para determinar si alguno de los nodos carecerá de capacidad suficiente si

falla el otro nodo. Puesto que la carga de trabajo durante la conmutación por error es la combinación de las cargas de trabajo de los dos nodos asociados, se puede aplicar la misma capacidad de rendimiento utilizada la política de toma de control a ambos nodos.

> Esta equivalencia en capacidad de rendimiento se utiliza, por lo general, entre nodos. Sin embargo, si hay mucho más tráfico entre nodos destinado para uno de los nodos a través de su partner de conmutación por error, la capacidad de rendimiento total utilizada al ejecutar todas las cargas de trabajo en un nodo del partner en comparación con el otro nodo del partner puede ser ligeramente diferente en función del cual ha fallado.

Las condiciones de capacidad de rendimiento utilizadas también se pueden utilizar como configuración de umbral de rendimiento secundario para crear una política de umbral de combinación al definir umbrales para las LUN y los volúmenes. La condición de capacidad de rendimiento utilizada se aplica al agregado o el nodo en el que reside el volumen o la LUN. Por ejemplo, puede crear una política de umbral de combinación utilizando los siguientes criterios:

Objeto de almacenamiento	Contador de rendimiento	Umbral de advertencia	Umbral crítico	Duración
Volumen	Latencia	15 ms/op	25 ms/op	20 minutos
Agregado	Capacidad de rendimiento utilizada	80 %	95 %	

Las políticas de umbral de combinación hacen que se genere un evento solo cuando se incumplen ambas condiciones durante toda la duración.

Uso del contador de capacidad de rendimiento utilizada para gestionar el rendimiento

Por lo general, las organizaciones quieren operar con una capacidad de rendimiento utilizada por debajo de 100 para que los recursos se utilicen de forma eficiente al tiempo que se reserva cierta capacidad de rendimiento adicional para acomodar las demandas de periodo pico. Se pueden utilizar políticas de umbral para personalizar la fecha de envío de alertas de valores de capacidad utilizada de alto rendimiento.

Puede establecer objetivos específicos según sus requisitos de rendimiento. Por ejemplo, las empresas de servicios financieros podrían reservar más capacidad de desempeño para garantizar la ejecución oportuna de las operaciones. Tal vez estas empresas quieran definir los umbrales de capacidad de rendimiento utilizada en el intervalo del 70-80 por ciento. Las empresas de fabricación con márgenes más pequeños pueden optar por reservar una menor capacidad de rendimiento si están dispuestas a arriesgar el rendimiento para gestionar mejor los costes DE TECNOLOGÍA. Estas empresas pueden definir umbrales de capacidad de rendimiento utilizados en el intervalo del 85-95 por ciento.

Cuando el valor de la capacidad de rendimiento utilizada supera el porcentaje configurado en una política de umbral definida por el usuario, Unified Manager envía un correo electrónico de alerta y añade el evento a la página Event Inventory. De este modo, puede gestionar posibles problemas antes de que afecten al rendimiento. Estos eventos también se pueden utilizar como indicadores que se necesitan para mover la carga de trabajo y cambiar dentro de los nodos y agregados.

Comprender y utilizar la página Node Failover Planning

La página Performance/Node Failover Planning calcula el impacto en el rendimiento de un nodo si se produce un error en el nodo de partner de alta disponibilidad (ha) del nodo. Unified Manager basa las estimaciones en el rendimiento histórico de los nodos en la pareja de alta disponibilidad.

Estimar el impacto en el rendimiento de una conmutación por error le permite planificar en las siguientes situaciones:

- Si una conmutación al respaldo degrada de forma consistente el rendimiento estimado del nodo de toma de control a un nivel inaceptable, puede considerar tomar acciones correctivas para reducir el impacto en el rendimiento debido a la conmutación al nodo de respaldo.
- Antes de iniciar una conmutación por error manual para realizar tareas de mantenimiento del hardware, puede calcular cómo la conmutación por error afecta al rendimiento del nodo que toma el control para determinar cuál es el mejor momento para llevar a cabo la tarea.

Uso de la página Planificación de conmutación por error de nodos para determinar las acciones correctivas

Basándose en la información que se muestra en la página Performance/Node Failover Planning, puede realizar acciones para garantizar que una conmutación por error no haga que el rendimiento de un par de alta disponibilidad caiga por debajo de un nivel aceptable.

Por ejemplo, para reducir el impacto en el rendimiento estimado de una conmutación al nodo de respaldo, puede mover algunos volúmenes o LUN de un nodo del par de alta disponibilidad a otros nodos del clúster. Al hacerlo se garantiza que el nodo primario pueda seguir ofreciendo un rendimiento aceptable tras un fallo.

Componentes de la página Node Failover Planning

Los componentes de la página Performance/Node Failover Planning se muestran en una cuadrícula y en el panel comparativo. Estas secciones le permiten evaluar el impacto de la conmutación por error de un nodo en el rendimiento del nodo de respaldo.

Cuadrícula de estadísticas de rendimiento

La página Performance/Node Failover Planning muestra un grid que contiene estadísticas de latencia, IOPS, utilización y capacidad de rendimiento utilizadas.

> Los valores de latencia e IOPS que se muestran en esta página y en la página Performance/Node Performance Explorer pueden no coincidir porque se utilizan diferentes contadores de rendimiento para calcular los valores para predecir la conmutación al nodo de respaldo.

En el grid, se asigna a cada nodo uno de los siguientes roles:

- Primario

  El nodo que toma el relevo al partner de alta disponibilidad cuando el partner falla. El objeto raíz siempre

es el nodo primario.

- Como partner

  El nodo que falla en el escenario de conmutación por error.

- Toma de control estimada

  Igual que el nodo primario. Las estadísticas de rendimiento que se muestran para este nodo muestran el rendimiento del nodo de toma de control después de que este asuma el control del partner que ha fallado.

> Aunque la carga de trabajo del nodo de respaldo es equivalente a las cargas de trabajo combinadas de ambos nodos después de una conmutación al respaldo, las estadísticas del nodo de respaldo estimado no son la suma de las estadísticas del nodo primario y del nodo Partner. Por ejemplo, si la latencia del nodo primario es de 2 ms/op y la latencia del nodo Partner es de 3 ms/op, el nodo de toma de control estimado podría tener una latencia de 4 ms/op. Este valor es un cálculo que Unified Manager realiza.

Puede hacer clic en el nombre del nodo Partner si desea que se convierta en el objeto raíz. Después de que se muestre la página Performance Explorer, puede hacer clic en la ficha **Planificación de conmutación por error** para ver cómo cambia el rendimiento en este escenario de fallo de nodo. Por ejemplo, si Node1 es el nodo primario y Node2 es el nodo asociado, puede hacer clic en Node2 para convertirse en el nodo primario. De esta forma, puede ver cómo cambia el rendimiento estimado en función de qué nodo falle.

Panel de comparación

La siguiente lista describe los componentes que se muestran en el panel comparar de forma predeterminada:

- **Gráficos de eventos**

  Se muestran con el mismo formato que los de la página Performance Explorer. Sólo pertenecen al nodo principal.

- * Contrafolios*

  Muestran estadísticas históricas del contador de rendimiento que se muestra en la cuadrícula. En cada gráfico, el gráfico del nodo de toma de control estimado muestra el rendimiento estimado si se había producido una conmutación por error en un momento dado.

  Por ejemplo, supongamos que el gráfico de utilización muestra un 73% para el nodo de toma de control estimado a las 11:00 El 8 de febrero. Si se hubiera producido una conmutación por error en ese momento, la utilización del nodo de respaldo habría sido del 73%.

  Las estadísticas históricas ayudan a encontrar el tiempo óptimo para iniciar una conmutación al respaldo, lo que minimiza la posibilidad de sobrecargar el nodo de respaldo. Solo puede programar una conmutación por error en momentos en los que se acepte el rendimiento previsto del nodo que toma el control.

De forma predeterminada, las estadísticas del objeto raíz y del nodo asociado se muestran en el panel de comparación. A diferencia de la página Performance/Node Performance Explorer, esta página no muestra el botón **Add** para que agregue objetos para la comparación de estadísticas.

Puede personalizar el panel de comparación de la misma manera que lo hace en la página Performance/Node Performance Explorer. La siguiente lista muestra ejemplos de personalización de los gráficos:

- Haga clic en un nombre de nodo para mostrar u ocultar las estadísticas del nodo en los gráficos Contador.
- Haga clic en **Zoom View** para mostrar un gráfico detallado de un contador en particular en una ventana nueva.

Uso de una directiva de umbral con la página Planificación de conmutación por error de nodos

Puede crear una política de umbral de nodo para que se le notifique en la página Performance/Node Failover Planning cuando una posible recuperación tras fallos degradara el rendimiento del nodo de respaldo a un nivel inaceptable.

La política de umbral de rendimiento definida por el sistema denominada "'par ha de nodos sobreutilizado'" genera un evento de advertencia si se supera el umbral durante seis periodos de recopilación consecutivos (30 minutos). El umbral se considera superado si la capacidad de rendimiento combinada utilizada de los nodos en un par de alta disponibilidad supera el 200 %.

El evento de la política de umbral definida por el sistema le avisa de que una conmutación al nodo de respaldo provocará que la latencia del nodo de toma de control aumente a un nivel inaceptable. Cuando ve un evento generado por esta política para un nodo en particular, puede desplazarse a la página Performance/Node Failover Planning de ese nodo para ver el valor de latencia previsto debido a una conmutación por error.

Además de utilizar esta política de umbral definida por el sistema, puede crear políticas de umbral utilizando el contador «'capacidad de rendimiento utilizada - adquisición'» y, a continuación, aplicar la política a los nodos seleccionados. Especificar un umbral inferior al 200 % le permite recibir un evento antes de superar el umbral de la política definida por el sistema. También puede especificar el período mínimo de tiempo durante el cual se supera el umbral a menos de 30 minutos si desea recibir una notificación antes de generar el evento de política definido por el sistema.

Por ejemplo, puede definir una política de umbral para generar un evento de advertencia si la capacidad de rendimiento combinado utilizada de los nodos de un par de alta disponibilidad supera el 175 % durante más de 10 minutos. Puede aplicar esta política a Node1 y Node2, que forman un par de alta disponibilidad. Después de recibir una notificación de evento de advertencia para Node1 o Node2, puede ver la página Performance/Node Failover Planning para ese nodo a fin de evaluar el impacto estimado en el rendimiento en el nodo de toma de control. Puede tomar acciones correctivas para evitar sobrecargar el nodo de toma de control si se produce una conmutación al respaldo. Si realiza alguna acción cuando la capacidad de rendimiento combinado que se utiliza de los nodos es inferior al 200 %, la latencia del nodo que toma el control no alcanza un nivel inaceptable incluso si se produce una conmutación por error durante este tiempo.

Usar el gráfico de desglose de capacidad de rendimiento utilizada para la planificación de conmutación por error

El gráfico detallado capacidad de rendimiento utilizada - desglose muestra la capacidad de rendimiento utilizada para el nodo principal y el nodo del partner. También muestra la cantidad de capacidad de rendimiento libre en el nodo de toma de control estimado. Esta información le ayuda a determinar si podría tener un problema de rendimiento si falla el nodo del partner.

Además de mostrar la capacidad de rendimiento total utilizada para los nodos, el gráfico Breakdown los valores para cada nodo en los protocolos de usuario y procesos en segundo plano.

- Los protocolos de usuario son las operaciones de I/o desde las aplicaciones de usuario hacia y desde el clúster.

- Los procesos en segundo plano son los procesos internos del sistema implicados en la eficiencia del almacenamiento, la replicación de datos y el estado del sistema.

Este nivel adicional de detalle permite determinar si un problema de rendimiento está provocado por la actividad de las aplicaciones de usuario o por los procesos del sistema en segundo plano, como la deduplicación, la reconstrucción de RAID, el filtrado de discos y las copias SnapMirror.

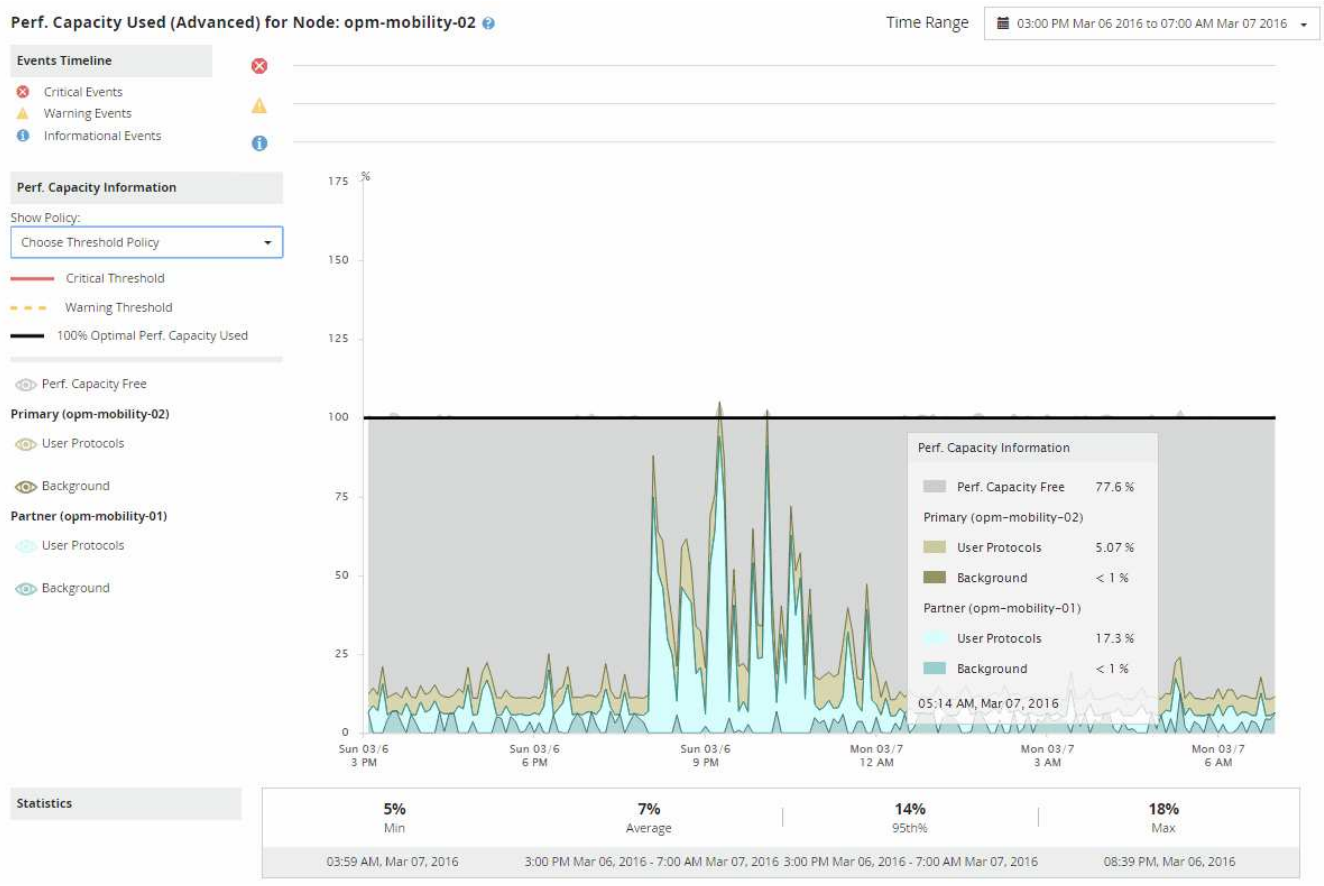
Pasos

1. Vaya a la página **Performance/Node Failover Planning** para el nodo que servirá como nodo de toma de control estimado.
2. En el selector **intervalo de tiempo**, elija el período de tiempo durante el cual se muestran las estadísticas históricas en la cuadrícula de contadores y en los gráficos de contadores.

   Se muestran los gráficos de contadores con estadísticas del nodo principal, nodo del partner y nodo de toma de control estimado.

3. En la lista **elegir gráficos**, seleccione **Perf. Capacidad utilizada**.
4. En el campo **Perf. Gráfico Capacity used**, seleccione **Breakdown** y haga clic en **Zoom View**.

   El gráfico detallado de rendimiento. Se muestra la capacidad utilizada.



5. Mueva el cursor por el gráfico detallado para ver la información sobre capacidad de rendimiento utilizada en la ventana emergente.

   Rendim. El porcentaje libre de capacidad es la capacidad de rendimiento disponible en el nodo de toma de control estimado. Indica la cantidad de capacidad de rendimiento que queda en el nodo que toma el control tras una conmutación al respaldo. Si es 0 %, una conmutación al nodo de respaldo provocará que

la latencia aumente hasta un nivel inaceptable en el nodo de respaldo.

6. Considere tomar medidas correctivas para evitar un porcentaje libre de capacidad de rendimiento baja.

   Si tiene pensado iniciar una conmutación al respaldo para el mantenimiento de nodos, elija una hora para conmutar al nodo del partner cuando el porcentaje libre de capacidad de rendimiento no sea 0.

Recogida de datos y supervisión del rendimiento de carga de trabajo

Unified Manager recopila y analiza la actividad de la carga de trabajo cada 5 minutos para identificar eventos de rendimiento y detecta cambios de configuración cada 15 minutos. Conserva un máximo de 30 días de datos históricos de eventos y rendimiento de 5 minutos, y utiliza estos datos para prever el rango de latencia esperado para todas las cargas de trabajo supervisadas.

Unified Manager debe recoger como mínimo 3 días de actividad de carga de trabajo antes de que pueda iniciar su análisis y antes de que la previsión de latencia del tiempo de respuesta de I/o pueda mostrarse en la página Workload Analysis y en la página de detalles Event. Mientras se recoge esta actividad, la previsión de latencia no muestra todos los cambios que se producen en la actividad de la carga de trabajo. Después de recoger 3 días de actividad, Unified Manager ajusta el pronóstico de latencia cada 24 horas a las 12:00 a.m. para reflejar los cambios en la actividad de la carga de trabajo y establecer un umbral dinámico de rendimiento más preciso.

Durante los primeros 4 días en los que Unified Manager supervisa una carga de trabajo, si han transcurrido más de 24 horas desde la última recogida de datos, los gráficos de latencia no mostrarán el pronóstico de latencia de esa carga de trabajo. Los eventos detectados antes de la última recogida siguen estando disponibles.

> El horario de verano cambia la hora del sistema, lo que altera el pronóstico de latencia de las estadísticas de rendimiento para las cargas de trabajo supervisadas. Unified Manager empieza a corregir el pronóstico de latencia de forma inmediata y tarda unos 15 días en completarlo. Durante este tiempo, puede seguir usando Unified Manager, pero, dado que Unified Manager utiliza el pronóstico de latencia para detectar eventos dinámicos, es posible que algunos eventos no sean precisos. Los eventos detectados antes del cambio de hora no se verán afectados.

Tipos de cargas de trabajo supervisadas por Unified Manager

Es posible utilizar Unified Manager para supervisar el rendimiento de dos tipos de cargas de trabajo: Definidas por el usuario y definidas por el sistema.

- ***cargas de trabajo definidas por el usuario***

  El rendimiento de I/o de las aplicaciones al clúster. Estos son procesos implicados en solicitudes de lectura y escritura. Un volumen, LUN, recurso compartido NFS, recurso compartido SMB/CIFS y una carga de trabajo es una carga de trabajo definida por el usuario.

  > Unified Manager solo supervisa la actividad de las cargas de trabajo en el clúster. No supervisa las aplicaciones, los clientes ni las rutas entre las aplicaciones y el clúster.

Si se cumple uno o varios de los siguientes aspectos con relación a una carga de trabajo, Unified Manager no se podrá supervisar:

  - Se trata de una copia de protección de datos (DP) en modo de solo lectura. (Los volúmenes DP se supervisan para el tráfico generado por el usuario).
  - Se trata de un clon de datos sin conexión.
  - Es un volumen reflejado en una configuración MetroCluster.

- ***cargas de trabajo definidas por el sistema***

  Los procesos internos implicados en la eficiencia del almacenamiento, la replicación de datos y el estado del sistema, incluidos:

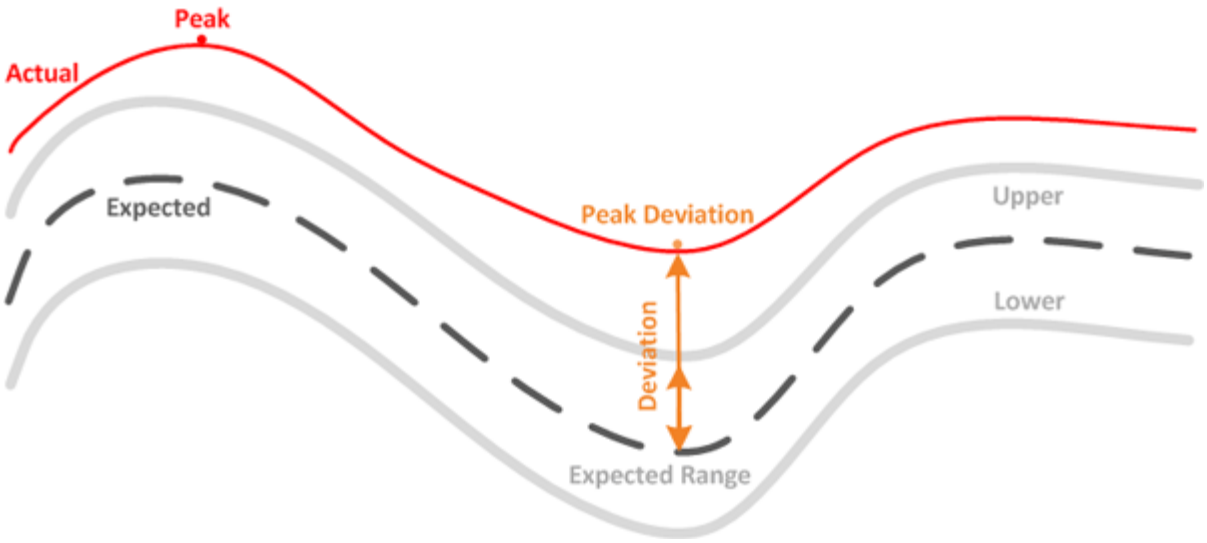
  - Eficiencia del almacenamiento, como la deduplicación
  - Estado del disco, que incluye la reconstrucción de RAID, el filtrado de discos, etc.
  - La replicación de datos, como las copias SnapMirror
  - Actividades de gestión
  - Estado del sistema de archivos, que incluye diversas actividades de WAFL
  - Escáneres del sistema de archivos, como WAFL scan
  - Descarga de copias, como las operaciones de eficiencia del almacenamiento descargados de hosts VMware
  - Estado del sistema, como movimientos de volúmenes, compresión de datos, etc.
  - Volúmenes sin supervisar

Los datos de rendimiento de las cargas de trabajo definidas por el sistema se muestran en la interfaz gráfica de usuario solo cuando el componente del clúster utilizado por estas cargas de trabajo es objeto de disputa. Por ejemplo, no se puede buscar el nombre de una carga de trabajo definida por el sistema para ver sus datos de rendimiento en la interfaz gráfica de usuario.

Valores de medición del rendimiento de la carga de trabajo

Unified Manager mide el rendimiento de las cargas de trabajo en un clúster en función de los valores estadísticos históricos y esperados, lo que forma el pronóstico de latencia de los valores de las cargas de trabajo. Compara los valores estadísticos de la carga de trabajo real con el pronóstico de latencia para determinar cuándo el rendimiento de la carga de trabajo es demasiado alto o demasiado bajo. Una carga de trabajo que no se ejecuta según lo esperado activa un evento de rendimiento dinámico para notificarle.

En la siguiente ilustración, el valor real, en rojo, representa las estadísticas de rendimiento reales en el plazo. El valor real ha superado el umbral de rendimiento, que es los límites superiores del pronóstico de latencia. El pico es el valor real más alto del lapso. La desviación mide el cambio entre los valores esperados (el pronóstico) y los valores reales, mientras que la desviación máxima indica el mayor cambio entre los valores esperados y los valores reales.



En la siguiente tabla, se enumeran los valores de medición del rendimiento de la carga de trabajo.

Medida	Descripción
Actividad	El porcentaje del límite de calidad de servicio que utilizan las cargas de trabajo del grupo de políticas. Si Unified Manager detecta un cambio en un grupo de políticas, como añadir o quitar un volumen o cambiar el límite de calidad de servicio, los valores reales y esperados pueden superar el 100 % del límite establecido. Si un valor supera el 100% del límite establecido, se muestra como >100%. Si un valor es inferior al 1% del límite establecido, se muestra como <1%.
Real	El valor de rendimiento medido en un momento específico para una carga de trabajo determinada.
Desviación	El cambio entre los valores esperados y los valores reales. Es la relación entre el valor real menos el valor esperado y el valor superior del rango esperado menos el valor esperado. Un valor de desviación negativo indica que el rendimiento de la carga de trabajo es menor de lo esperado, mientras que un valor positivo indica que el rendimiento de la carga de trabajo es mayor de lo esperado.

Medida	Descripción
Esperado	Los valores esperados se basan en el análisis de los datos de rendimiento históricos de una carga de trabajo determinada. Unified Manager analiza estos valores estadísticos para determinar el rango esperado (previsión de latencia) de valores.
Previsión de latencia (rango esperado)	La previsión de latencia es una predicción de los valores de rendimiento superior e inferior esperados en un momento determinado. Para la latencia de la carga de trabajo, los valores superiores forman el umbral de rendimiento. Cuando el valor real supera el umbral de rendimiento, Unified Manager activa un evento de rendimiento dinámico.
Pico	Valor máximo medido a lo largo de un período de tiempo.
Desviación máxima	El valor máximo de desviación medido a lo largo de un período de tiempo.
Profundidad de cola	El número de solicitudes de I/o pendientes que están esperando en el componente de interconexión.
Utilización	Para los componentes de procesamiento de red, procesamiento de datos y agregado, el porcentaje de tiempo ocupado para completar las operaciones de carga de trabajo durante un período de tiempo. Por ejemplo, el porcentaje de tiempo durante el procesamiento de la red o los componentes de procesamiento de datos para procesar una solicitud de I/o o o para que un agregado cumpla una solicitud de lectura o escritura.
Rendimiento de escritura	La cantidad de rendimiento de escritura, en megabytes por segundo (MB/s), desde cargas de trabajo en un clúster local hasta el clúster asociado en una configuración MetroCluster.

Qué rango esperado de rendimiento es

La previsión de latencia es una predicción de los valores de rendimiento superior e inferior esperados en un momento determinado. Para la latencia de la carga de trabajo, los valores superiores forman el umbral de rendimiento. Cuando el valor real supera el umbral de rendimiento, Unified Manager activa un evento de rendimiento dinámico.

Por ejemplo, durante el horario normal de trabajo entre las 9:00 a.m. y a las 5:00 p.m., la mayoría de los empleados podrían revisar su correo electrónico entre las 9:00 a.m. y las 10:30 El aumento de la demanda de los servidores de correo electrónico implica un aumento de la actividad de las cargas de trabajo en el

almacenamiento de entorno de administración durante este tiempo. Los empleados pueden notar que el tiempo de respuesta es lento por parte de los clientes de correo electrónico.

Durante la hora del almuerzo entre las 12:00 p.m. y la 1:00 y al final del día de trabajo después de las 5:00 p.m., la mayoría de los empleados están probablemente lejos de sus computadoras. La demanda de los servidores de correo electrónico suele disminuir y, por lo tanto, se reduce la demanda de almacenamiento de entorno administrativo. Como alternativa, podrían programarse operaciones con la carga de trabajo, como backups de almacenamiento o análisis de virus, que comiencen a las 5:00 p. m. y aumente la actividad en el almacenamiento de gestión.

Durante varios días, el aumento y la disminución de la actividad de las cargas de trabajo determinan el rango esperado (pronóstico de latencia) de la actividad, con los límites superior e inferior de una carga de trabajo. Cuando la actividad de carga de trabajo real de un objeto está fuera de los límites superior o inferior, y permanece fuera de los límites durante un periodo de tiempo, puede indicar que el objeto se está utilizando en exceso o infrautilizado.

Cómo se forma la previsión de latencia

Unified Manager debe recoger como mínimo 3 días de actividad de carga de trabajo antes de que pueda iniciar su análisis y antes de que la previsión de latencia del tiempo de respuesta de I/o pueda mostrarse en la interfaz gráfica de usuario. La recopilación de datos mínimos requeridos no tiene en cuenta todos los cambios que se producen en la actividad de la carga de trabajo. Después de recoger los primeros 3 días de actividad, Unified Manager ajusta el pronóstico de latencia cada 24 horas a las 12:00 para reflejar los cambios en la actividad de las cargas de trabajo y establecer un umbral dinámico de rendimiento más preciso.

El horario de verano cambia la hora del sistema, lo que altera el pronóstico de latencia de las estadísticas de rendimiento para las cargas de trabajo supervisadas. Unified Manager empieza a corregir el pronóstico de latencia de forma inmediata y tarda unos 15 días en completarlo. Durante este tiempo, puede seguir usando Unified Manager, pero, dado que Unified Manager utiliza el pronóstico de latencia para detectar eventos dinámicos, es posible que algunos eventos no sean precisos. Los eventos detectados antes del cambio de hora no se verán afectados.

Cómo se utiliza el pronóstico de latencia en el análisis de rendimiento

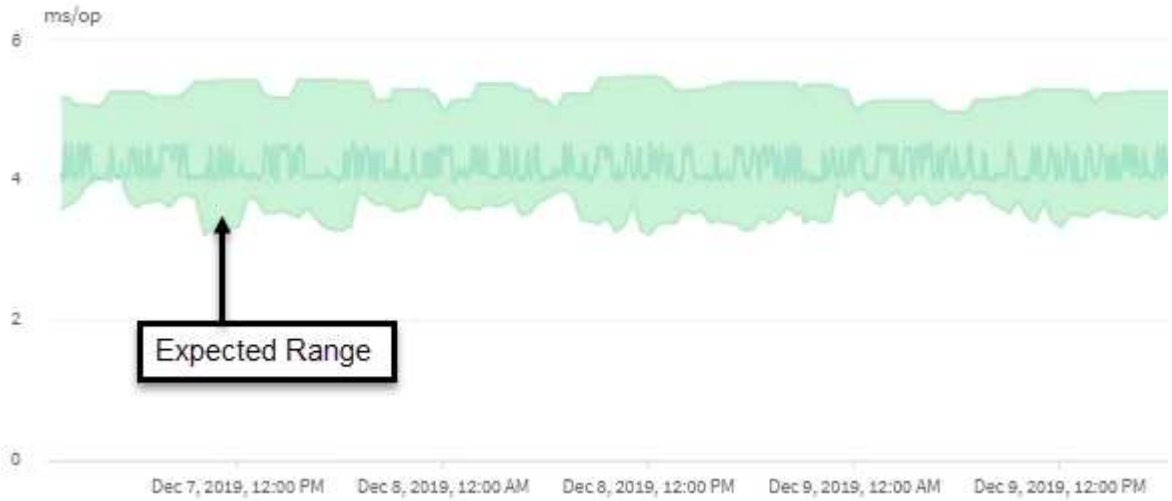
Unified Manager usa el pronóstico de latencia para representar la actividad de latencia de I/o típica (tiempo de respuesta) para las cargas de trabajo supervisadas. Le avisa cuando la latencia real de una carga de trabajo se encuentra por encima de los límites superiores de la previsión de latencia, que activa un evento de rendimiento dinámico, para que pueda analizar el problema de rendimiento y tomar medidas correctivas para resolverlo.

El pronóstico de latencia establece la línea de base de rendimiento para la carga de trabajo. Con el tiempo, Unified Manager aprende de las mediciones de rendimiento anteriores para pronosticar los niveles de rendimiento y actividad esperados para la carga de trabajo. El límite superior del rango esperado establece el umbral de rendimiento dinámico. Unified Manager utiliza la base para determinar cuándo la latencia real está por encima o por debajo de un umbral, o fuera de los límites de su rango esperado. La comparación entre los valores reales y los valores esperados crea un perfil de rendimiento para la carga de trabajo.

Cuando la latencia real de una carga de trabajo supera el umbral de rendimiento dinámico, debido a la contención en un componente de clúster, la latencia es alta y la carga de trabajo se ejecuta más lentamente de lo esperado. El rendimiento de otras cargas de trabajo que comparten los mismos componentes del clúster también puede ser más lento de lo esperado.

Unified Manager analiza el evento de umbral que cruza y determina si la actividad es un evento de rendimiento. Si la actividad de alta carga de trabajo continúa siendo coherente durante un largo periodo de tiempo, como varias horas, Unified Manager considera que la actividad es normal y ajusta de forma dinámica el pronóstico de latencia para formar el nuevo umbral de rendimiento dinámico.

Es posible que algunas cargas de trabajo tengan una actividad baja constante, donde la previsión de latencia no tiene una tasa alta de cambio con el tiempo. Para minimizar el número de eventos durante el análisis de eventos de rendimiento, Unified Manager activa un evento solo en volúmenes de baja actividad cuyas operaciones y latencias son mucho más elevadas de lo esperado.



En este ejemplo, la latencia de un volumen tiene un pronóstico de latencia, en gris, de 3.5 milisegundos por operación (ms/op) a su nivel más bajo y de 5.5 ms/op a su nivel más alto. Si la latencia real, en azul, aumenta de repente a 10 ms/op, debido a un pico intermitente en el tráfico de la red o contención en un componente del clúster, supera la previsión de latencia y ha superado el umbral de rendimiento dinámico.

Cuando se redujo el tráfico de red o el componente del clúster ya no es objeto de disputa, la latencia devuelve dentro de la previsión de latencia. Si la latencia permanece en o por encima de los 10 ms/op durante un largo periodo de tiempo, es posible que deba tomar la acción correctiva para resolver el evento.

Cómo Unified Manager utiliza la latencia de carga de trabajo para identificar problemas de rendimiento

La latencia de las cargas de trabajo (tiempo de respuesta) es el tiempo que tarda un volumen en un clúster en responder a las solicitudes de I/o de las aplicaciones cliente. Unified Manager utiliza la latencia para detectar eventos de rendimiento y alertarle de ellos.

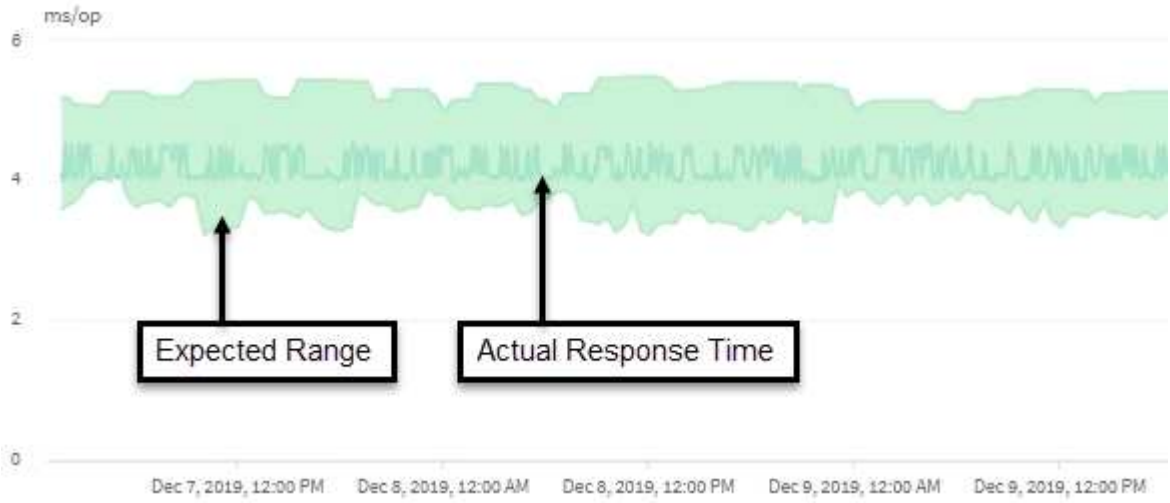
Una alta latencia significa que las solicitudes de aplicaciones a un volumen de un clúster tardan más de lo habitual. La causa de la alta latencia podría estar en el clúster mismo, debido a la contención en uno o más componentes del clúster. La alta latencia también podría deberse a problemas externos al clúster, como cuellos de botella de red, problemas con el cliente que aloja las aplicaciones, o problemas con las propias aplicaciones.

Unified Manager solo supervisa la actividad de las cargas de trabajo en el clúster. No supervisa las aplicaciones, los clientes ni las rutas entre las aplicaciones y el clúster.

Las operaciones en el clúster, como la realización de backups o la ejecución de la deduplicación, que

aumenten su demanda de los componentes del clúster compartidos por otras cargas de trabajo, también pueden contribuir a una alta latencia. Si la latencia real supera el umbral de rendimiento dinámico del rango esperado (previsión de latencia), Unified Manager analiza el evento para determinar si es un evento de rendimiento que podría necesitar resolver. La latencia se mide en milisegundos por operación (ms/op).

En el gráfico Latency total de la página Workload Analysis, es posible ver un análisis de las estadísticas de latencia para ver cómo la actividad de procesos individuales, como solicitudes de lectura y escritura, se compara con las estadísticas de latencia generales. La comparación ayuda a determinar qué operaciones tienen la actividad más alta o si operaciones específicas tienen actividad anormal que afecta la latencia de un volumen. Al analizar los eventos de rendimiento, puede utilizar las estadísticas de latencia para determinar si un evento fue causado por un problema en el clúster. También puede identificar las actividades de carga de trabajo específicas o los componentes del clúster que participan en el evento.



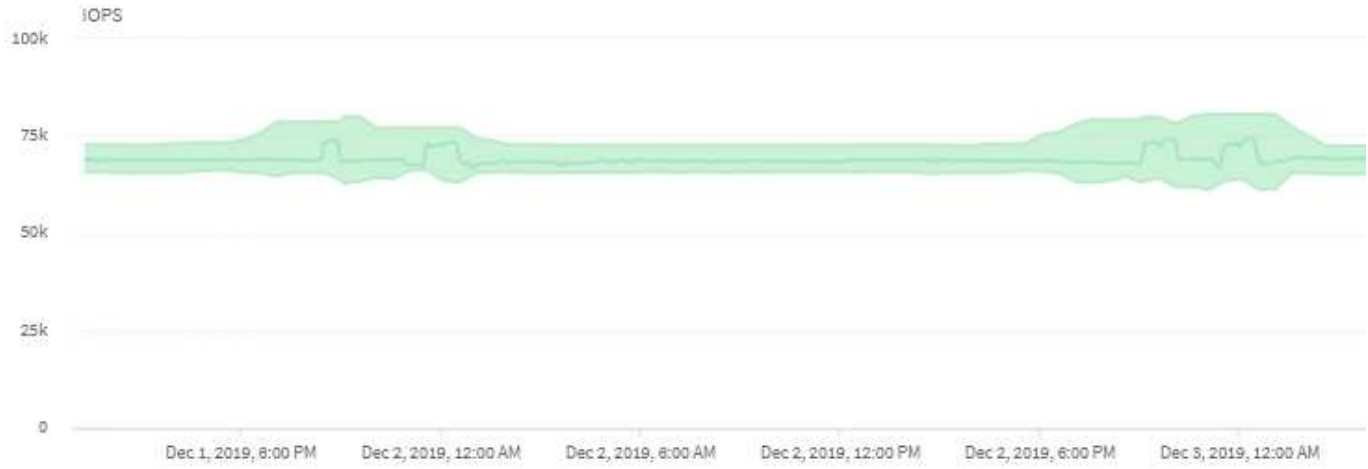
En este ejemplo se muestra el gráfico latencia . La actividad de tiempo de respuesta real (latencia) es una línea azul y la previsión de latencia (rango esperado) es verde.

Puede haber vacíos en la línea azul si Unified Manager no pudo recopilar datos. Esto puede ocurrir porque el clúster o el volumen no se pudo acceder, Unified Manager se apagó durante esa hora o la recogida fue más prolongada que el período de recogida de 5 minutos.

Cómo las operaciones del clúster pueden afectar a la latencia de carga de trabajo

Las operaciones (IOPS) representan la actividad de todas las cargas de trabajo definidas por el usuario y definidas por el sistema en un clúster. Las estadísticas de IOPS le ayudan a determinar si los procesos del clúster, como hacer backups o ejecutar deduplicación, están afectando a la latencia de las cargas de trabajo (tiempo de respuesta) o podrían haber provocado o contribuido a un evento de rendimiento.

Al analizar los eventos de rendimiento, puede utilizar las estadísticas de IOPS para determinar si un evento de rendimiento fue causado por un problema en el clúster. Es posible identificar las actividades de carga de trabajo específicas que pueden haber contribuido principalmente al evento de rendimiento. Las IOPS se miden en operaciones por segundo (OPS/s).



Este ejemplo muestra el gráfico IOPS. Las estadísticas de operaciones reales son una línea azul y las estadísticas de operaciones de IOPS se muestran en verde.

En algunos casos en los que se sobrecarga un clúster, es posible que Unified Manager muestre el mensaje `Data collection is taking too long on Cluster` *`cluster_name`*. Esto significa que no se han recopilado suficientes estadísticas para que Unified Manager las analice. Debe reducir los recursos que está utilizando el clúster para poder recopilar las estadísticas.

Supervisión del rendimiento de las configuraciones de MetroCluster

Unified Manager permite supervisar el rendimiento de escritura entre clústeres en una configuración de MetroCluster para identificar cargas de trabajo con un alto nivel de rendimiento de escritura.

Si estas cargas de trabajo de alto rendimiento hacen que otros volúmenes en el clúster local tengan tiempos de respuesta de I/o elevados, Unified Manager activa los eventos de rendimiento para notificarle.

Unified Manager trata los clústeres de una configuración de MetroCluster como clústeres individuales. No distingue entre clústeres que son partners ni relaciona el rendimiento de escritura de cada clúster.

Cuando un clúster local en una configuración MetroCluster refleja sus datos en el clúster del partner, los datos se escriben en NVRAM y, después, se transfieren mediante los vínculos interswitch (ISL) a los agregados remotos. Unified Manager analiza la NVRAM para identificar las cargas de trabajo cuyo alto rendimiento de escritura está utilizando demasiado la NVRAM, poniendo en contención a la NVRAM.

Las cargas de trabajo cuya desviación en el tiempo de respuesta ha superado el umbral de rendimiento se denominan *víctimas* y las cargas de trabajo cuya desviación en el rendimiento de escritura en la NVRAM es mayor de lo habitual, lo que provoca la contención, se denominan *abusones*. Dado que solo se reflejan las solicitudes de escritura en el clúster de partners, Unified Manager no analiza el rendimiento de lectura.

Puede ver el rendimiento de cualquiera de los clústeres de una configuración de MetroCluster analizando las cargas de trabajo de los LUN y volúmenes correspondientes desde las siguientes pantallas. Puede filtrar los resultados por el clúster. Desde el panel de navegación de la izquierda:

- **Almacenamiento > clústeres > rendimiento: Vista todos los clústeres**. Consulte

- **Almacenamiento > volúmenes > rendimiento: Vista todos los volúmenes**.
- **Almacenamiento > LUN > rendimiento: Vista de todas las LUN**.
- **Análisis de cargas de trabajo > todas las cargas de trabajo**

Información relacionada

"Análisis y notificación de eventos de rendimiento"

"Análisis de eventos de rendimiento para una configuración de MetroCluster"

"Funciones de las cargas de trabajo involucradas en un evento de rendimiento"

"Identificar las cargas de trabajo de las víctimas involucradas en un evento de rendimiento"

"Identificar las cargas de trabajo abusivas que están involucradas en un evento de rendimiento"

"Identificar las cargas de trabajo de tiburones en un evento de rendimiento"

Comprender los eventos y las alertas de rendimiento

Los eventos de rendimiento son incidentes relacionados con el rendimiento de la carga de trabajo en un clúster. Le ayudan a identificar cargas de trabajo con tiempos de respuesta lentos. Junto con los eventos de salud que ocurrieron al mismo tiempo, usted puede determinar los problemas que podrían haber causado, o contribuido a, los tiempos de respuesta lentos.

Cuando Unified Manager detecta varias apariciones de la misma condición de evento para el mismo componente del clúster, trata todas las ocurrencias como un solo evento, no como eventos independientes.

Es posible configurar alertas para que envíen notificaciones por correo electrónico automáticamente cuando se produzcan eventos de rendimiento de ciertos tipos de gravedad.

Fuentes de eventos de rendimiento

Los eventos de rendimiento son problemas relacionados con el rendimiento de la carga de trabajo en un clúster. Le ayudan a identificar objetos de almacenamiento con tiempos de respuesta lentos, también conocidos como alta latencia. Junto con otros eventos de salud que ocurrieron al mismo tiempo, usted puede determinar los problemas que podrían haber causado, o contribuido a, los tiempos de respuesta lentos.

Unified Manager recibe eventos de rendimiento de los siguientes orígenes:

- **Sucesos de política de umbral de rendimiento definidos por el usuario**

  Problemas de rendimiento basados en valores de umbral personalizados que se han configurado. Puede configurar las políticas de umbral de rendimiento para los objetos de almacenamiento; por ejemplo, agregados y volúmenes, para que los eventos se generen cuando se ha incumplido un valor de umbral de un contador de rendimiento.

  Para recibir estos eventos, debe definir una política de umbral de rendimiento y asignarla a un objeto de almacenamiento.

- **Sucesos de política de umbral de rendimiento definidos por el sistema**

  Problemas de rendimiento basados en valores de umbral definidos por el sistema. Estas políticas de umbral se incluyen en la instalación de Unified Manager para cubrir problemas de rendimiento habituales.

  Estas políticas de umbral se habilitan de forma predeterminada, por lo que es posible que vea eventos poco después de agregar un clúster.

- **Eventos de umbral de rendimiento dinámico**

  Problemas de rendimientos provocados por errores en una infraestructura INFORMÁTICA o por cargas de trabajo que realizan un uso excesivo de los recursos del clúster. La causa de estos eventos podría ser un problema sencillo que se corrija por sí solo pasado un tiempo, o que se podría solucionar con una reparación o un cambio de configuración. Un evento de umbral dinámico indica que las cargas de trabajo de un sistema ONTAP son lentas debido a que hay otras cargas de trabajo que realizan un uso intensivo de los componentes del clúster compartidos.

  Estos umbrales se habilitan de forma predeterminada, por lo que es posible que vea eventos tras tres días de recoger datos en un nuevo clúster.

Tipos de gravedad de eventos de rendimiento

Cada evento de rendimiento está asociado con un tipo de gravedad para ayudarle a priorizar los eventos que requieren una acción correctiva inmediata.

- **Crítico**

  Se produjo un evento de rendimiento que podría provocar una interrupción del servicio si no se emprenderse inmediatamente una acción correctiva.

  Los eventos críticos se envían únicamente desde umbrales definidos por el usuario.

- **Advertencia**

  Un contador de rendimiento de un objeto de clúster está fuera del rango normal y se debe supervisar para asegurarse de que no alcanza la gravedad crucial. Los eventos de esta gravedad no provocan interrupciones del servicio y podría no ser necesario realizar una acción correctiva inmediata.

  Los eventos de advertencia se envían desde umbrales definidos por el usuario, definidos por el sistema o dinámicos.

- **Información**

  El evento se produce cuando se descubre un nuevo objeto o cuando se realiza una acción del usuario. Por ejemplo, cuando se elimina un objeto de almacenamiento o cuando hay cambios de configuración, se genera el evento con tipo gravedad Information.

  Los eventos de información se envían directamente desde ONTAP cuando detecta un cambio de configuración.

Para más información, consulte los siguientes enlaces:

- "Qué sucede cuando se recibe un evento"

- "Qué información se incluye en un correo electrónico de alerta"
- "Adición de alertas"
- "Adición de alertas para eventos de rendimiento"

Cambios de configuración detectados por Unified Manager

Unified Manager supervisa sus clústeres para detectar cambios de configuración con el fin de ayudarle a determinar si un cambio podría haber causado o contribuido a un evento de rendimiento. Las páginas Performance Explorer muestran un icono de evento de cambio ( ) para indicar la fecha y la hora en que se detectó el cambio.

Puede revisar los gráficos de rendimiento en las páginas Performance Explorer y en la página Workload Analysis para ver si el evento de cambio afecta al rendimiento del objeto de clúster seleccionado. Si el cambio se detectó en o aproximadamente al mismo tiempo que un evento de rendimiento, el cambio podría haber contribuido al problema, lo que provocó que se disparara la alerta de evento.

Unified Manager puede detectar los siguientes eventos de cambio, que se clasifican como eventos informativos:

- Un volumen se mueve entre agregados.

  Unified Manager puede detectar cuando el movimiento está en curso, completado o con errores. Si Unified Manager está inactivo durante un movimiento de volúmenes, cuando se realiza el backup, detecta el movimiento del volumen y muestra un evento de cambio para él.

- El límite de rendimiento (MB/s o IOPS) de un grupo de políticas de calidad de servicio que contiene uno o más cambios en las cargas de trabajo supervisadas.

  Cambiar el límite de un grupo de políticas puede provocar picos intermitentes en la latencia (tiempo de respuesta), que también podrían desencadenar eventos del grupo de políticas. La latencia vuelve a la normalidad de forma gradual y los eventos causados por los picos quedan obsoletos.

- Un nodo de un par de alta disponibilidad toma el control o devuelve el almacenamiento de su otro nodo.

  Unified Manager puede detectar cuándo se ha completado la operación de toma de control, toma de control parcial o retorno al nodo primario. Si la toma de control está provocada por un nodo de pánico, Unified Manager no detecta el evento.

- Se ha completado correctamente una actualización o una operación de reversión de ONTAP.

  Se muestran la versión anterior y la nueva.

Tipos de políticas de umbral de rendimiento definidas por el sistema

Unified Manager proporciona algunas políticas de umbral estándar que supervisan el rendimiento de un clúster y generan eventos automáticamente. Estas políticas se habilitan de forma predeterminada, por lo que generan eventos de información o advertencia cuando se incumplen los umbrales de rendimiento supervisados.

Las políticas de umbral de rendimiento definidas por el sistema no se habilitan en sistemas Cloud Volumes ONTAP, ONTAP Edge o ONTAP Select.

Si recibe eventos innecesarios de cualquier política de umbral de rendimiento definida por el sistema, puede deshabilitar los eventos para políticas individuales en la página Event Setup.

Políticas de umbral de clúster

Las políticas de umbral de rendimiento del clúster definidas por el sistema se asignan, de forma predeterminada, a cada clúster que supervisa Unified Manager:

- **Desequilibrio de carga de clúster**

  Identifica situaciones en las que un nodo está funcionando con una carga mucho más alta que otros nodos del clúster y, por lo tanto, afecta potencialmente a las latencias de las cargas de trabajo.

  Para ello, compara la capacidad de rendimiento utilizada en todos los nodos de un clúster para ver si algún nodo ha superado el valor de umbral del 30 % durante más de 24 horas. Este es un evento de advertencia.

- **Desequilibrio de la capacidad del clúster**

  Identifica situaciones en las que un agregado tiene una capacidad utilizada mucho mayor que otros agregados del clúster y, por lo tanto, afecta potencialmente al espacio necesario para las operaciones.

  Para ello, compara el valor de capacidad utilizada de todos los agregados del clúster para ver si hay una diferencia del 70 % entre cualquier agregado. Este es un evento de advertencia.

Políticas de umbral de nodo

Las políticas de umbral de rendimiento de nodo definidas por el sistema se asignan, de forma predeterminada, a cada nodo en los clústeres que supervisa Unified Manager:

- **Se ha incumplido el umbral de capacidad de rendimiento utilizada**

  Identifica situaciones en las que un solo nodo está funcionando por encima de los límites de su eficiencia operativa y, por lo tanto, afecta potencialmente a las latencias de la carga de trabajo.

  Para ello, busca nodos que usan más del 100 % de su capacidad de rendimiento durante más de 12 horas. Este es un evento de advertencia.

- **Par de nodos de alta disponibilidad sobreutilizado**

  Identifica situaciones en las que los nodos de una pareja de ha están funcionando por encima de los límites de la eficiencia operativa de la pareja de ha.

  Para ello, se debe observar el valor de capacidad de rendimiento utilizada para los dos nodos de la pareja de alta disponibilidad. Si la capacidad de rendimiento combinado que se usa de los dos nodos supera el 200 % durante más de 12 horas, la conmutación por error de una controladora afectará a las latencias de carga de trabajo. Este es un evento informativo.

- **Fragmentación de disco en nodo**

  Identifica situaciones en las que un disco o los discos de un agregado están fragmentados, lo cual ralentiza servicios del sistema clave y afecta potencialmente a las latencias de carga de trabajo de un nodo.

  Para ello, se fijan determinadas tasas de operaciones de lectura y escritura en todos los agregados de un

nodo. Esta política también se puede activar durante la resincronización de SyncMirror o cuando se encuentran errores durante las operaciones de limpieza de discos. Este es un evento de advertencia.

> La política de «fragmentación de disco de nodo» analiza agregados de solo HDD; los agregados de Flash Pool, SSD y FabricPool no se analizan.

Políticas de umbral de agregado

La política de umbral de rendimiento de agregado definida por el sistema se asigna de forma predeterminada a cada agregado de los clústeres que supervisa Unified Manager:

- **Exceso de uso de discos agregados**

  Identifica situaciones en las que un agregado está funcionando por encima de los límites de su eficiencia operativa y, de este modo, afecta potencialmente a las latencias de la carga de trabajo. Identifica estas situaciones buscando agregados en los que los discos del agregado están más del 95% utilizados durante más de 30 minutos. A continuación, esta directiva de varias condiciones realiza el siguiente análisis para ayudar a determinar la causa del problema:

  - ¿Un disco del agregado está realizando actualmente una actividad de mantenimiento en segundo plano?

    Algunas de las actividades de mantenimiento en segundo plano en las que se podría realizar un disco son la reconstrucción de discos, la limpieza de discos, la resincronización de SyncMirror y la reparidad.

  - ¿Hay un cuello de botella de comunicaciones en la interconexión Fibre Channel de la bandeja de discos?
  - ¿Hay demasiado espacio libre en el agregado? Se emite un evento de advertencia para esta directiva sólo si una (o más) de las tres directivas subordinadas también se consideran inrelacionadas. Un evento de rendimiento no se desencadena si solo se utilizan los discos del agregado superior al 95%.

> La política de «discos agregados agregados «sobreutilizados» analiza agregados de solo HDD y agregados de Flash Pool (híbridos); los agregados SSD y FabricPool no se analizan.

Políticas de umbral de latencia de carga de trabajo

Las políticas de umbral de latencia de carga de trabajo definidas por el sistema se asignan a cualquier carga de trabajo que tenga una política de nivel de servicio de rendimiento configurada que tenga un valor definido de «latencia esperada»:

- **Umbral de latencia de volumen de carga de trabajo/LUN incumplido según lo definido por nivel de servicio de rendimiento**

  Identifica volúmenes (recursos compartidos de archivos) y LUN que han superado su límite de «latencia esperada» y que afectan al rendimiento de la carga de trabajo. Este es un evento de advertencia.

  Para ello, se buscan cargas de trabajo que hayan superado el valor de latencia esperado durante un 30 % del tiempo durante la hora anterior.

Políticas de umbral de calidad de servicio

Las políticas de umbral de rendimiento de calidad de servicio definidas por el sistema se asignan a cualquier carga de trabajo que tenga una política de rendimiento máximo de calidad de servicio de ONTAP configurada

(IOPS, IOPS/TB o MB/s). Unified Manager activa un evento cuando el valor de rendimiento de la carga de trabajo es un 15 % menor que el valor de calidad de servicio configurado:

- **QoS máx IOPS o MB/s umbral**

  Identifica volúmenes y LUN que han superado el límite máximo de rendimiento de IOPS o MB/s de la calidad de servicio, y que afectan a la latencia de la carga de trabajo. Este es un evento de advertencia.

  Cuando se asigna una sola carga de trabajo a un grupo de políticas, para ello, se deben buscar cargas de trabajo que hayan superado el umbral de rendimiento máximo definido en el grupo de políticas de calidad de servicio asignado durante cada periodo de recogida en la hora anterior.

  Cuando varias cargas de trabajo comparten una sola política de calidad de servicio, lo hace añadiendo las IOPS o MB/s de todas las cargas de trabajo de la política y comprobando ese total respecto al umbral.

- **QoS pico IOPS/TB o IOPS/TB con umbral de tamaño de bloque**

  Identifica volúmenes que han superado su límite de rendimiento máximo de IOPS/TB de la calidad de servicio adaptativa (o IOPS/TB con límite de tamaño de bloque) y que afectan a la latencia de las cargas de trabajo. Este es un evento de advertencia.

  Para ello, convierte el umbral máximo de IOPS/TB definido en la política de calidad de servicio adaptativa en un valor de IOPS máximo de calidad de servicio en función del tamaño de cada volumen y, a continuación, busca volúmenes que hayan superado el IOPS máximo de calidad de servicio durante cada periodo de recogida de rendimiento de la hora anterior.

  > Esta política se aplica a los volúmenes solo cuando el clúster se ha instalado con el software ONTAP 9.3 y versiones posteriores.

  Cuando se ha definido el elemento «'tamaño de bloque'» en la política de calidad de servicio adaptativa, el umbral se convierte en un valor máximo de MB/s de calidad de servicio en función del tamaño de cada volumen. A continuación, busca volúmenes que hayan superado el máximo de MB/s de calidad de servicio durante cada periodo de recogida de rendimiento de la hora anterior.

  > Esta política se aplica a los volúmenes solo cuando el clúster se ha instalado con el software ONTAP 9.5 y versiones posteriores.

Análisis y notificación de eventos de rendimiento

Los eventos de rendimiento le notifican problemas de rendimiento de I/o en una carga de trabajo provocada por la contención en un componente de clúster. Unified Manager analiza el evento para identificar todas las cargas de trabajo involucradas, el componente en disputa y si el evento sigue siendo un problema que podría necesitar resolver.

Unified Manager supervisa la latencia de I/o (tiempo de respuesta) y las IOPS (operaciones) para volúmenes en un clúster. Cuando otras cargas de trabajo realizan un uso excesivo de un componente del clúster, por ejemplo, el componente es objeto de disputa y no puede funcionar en un nivel óptimo para satisfacer las demandas de las cargas de trabajo. El rendimiento de otras cargas de trabajo que utilizan el mismo componente puede verse afectado, lo que provoca el aumento de las latencias. Si la latencia supera el umbral de rendimiento dinámico, Unified Manager activa un evento de rendimiento para notificarle.

Análisis de eventos

Unified Manager realiza los siguientes análisis utilizando los 15 días anteriores de estadísticas de rendimiento para identificar las cargas de trabajo víctimas, las cargas de trabajo abusivas y el componente del clúster implicados en un evento:

- Identifica las cargas de trabajo víctimas cuya latencia ha superado el umbral de rendimiento dinámico, que es el límite superior de la previsión de latencia:
  - Para volúmenes en agregados híbridos HDD o Flash Pool (nivel local), los eventos solo se activan cuando la latencia es superior a 5 milisegundos (ms) y las IOPS son superiores a 10 operaciones por segundo (OPS/s).
  - Para volúmenes en agregados íntegramente de SSD o agregados de FabricPool (nivel de cloud), los eventos solo se activan cuando la latencia es superior a 1 ms y el IOPS supera las 100 OPS/s.
- Identifica el componente del clúster en disputa.

  Si la latencia de las cargas de trabajo víctimas en la interconexión del clúster es superior a 1 ms, Unified Manager lo considera importante y activa un evento para la interconexión del clúster.

- Identifica las cargas de trabajo abusivas que están sobreutilizando el componente del clúster y que hacen que estén en contención.
- Clasifica las cargas de trabajo involucradas, en función de su desviación en utilización o actividad de un componente del clúster, para determinar qué elementos agresores tienen el mayor cambio de uso del componente del clúster y qué víctimas son las más afectadas.

Es posible que se produzca un evento solo durante un breve momento y, a continuación, corregirlo después de que el componente que está utilizando ya no sea objeto de disputa. Un evento continuo es un evento que se vuelve a producir para el mismo componente del clúster en un intervalo de cinco minutos y permanece en el estado activo. En el caso de eventos continuos, Unified Manager activa una alerta tras detectar el mismo evento en dos intervalos de análisis consecutivos.

Cuando se resuelve un evento, este sigue disponible en Unified Manager como parte del registro de problemas de rendimiento anteriores de un volumen. Cada evento tiene un ID único que identifica el tipo de evento y los componentes de volúmenes, clúster y clúster implicados.

Un único volumen puede participar en más de un evento a la vez.

Estado del evento

Los eventos pueden estar en uno de los siguientes estados:

- **Activo**

  Indica que el evento de rendimiento está activo (nuevo o reconocido). El problema que causa el evento no se ha corregido solo o no se ha resuelto. El contador de rendimiento del objeto de almacenamiento sigue por encima del umbral de rendimiento.

- **Obsoleto**

  Indica que el evento no está activo. El problema que causa el evento se ha corregido solo o se ha resuelto. El contador de rendimiento del objeto de almacenamiento ya no está por encima del umbral de rendimiento.

Notificación de eventos

Los eventos se muestran en la página Dashboard y en muchas otras páginas de la interfaz de usuario, y las alertas de esos eventos se envían a direcciones de correo electrónico especificadas. Puede ver información detallada sobre un evento y obtener sugerencias para resolverlo en la página de detalles Event y en la página Workload Analysis.

Interacción de eventos

En la página de detalles Event y en la página Workload Analysis, puede interactuar con los eventos de las siguientes maneras:

- Al mover el ratón sobre un evento se muestra un mensaje que muestra la fecha y la hora en que se detectó el evento.

  Si hay varios eventos para el mismo período de tiempo, el mensaje muestra el número de eventos.

- Al hacer clic en un solo evento se muestra un cuadro de diálogo que muestra información más detallada sobre el evento, incluidos los componentes del clúster implicados.

  El componente objeto de la contención está en un círculo y se resalta en rojo. Puede hacer clic en **Ver análisis completo** para ver el análisis completo en la página de detalles del evento. Si hay varios eventos para el mismo período de tiempo, el cuadro de diálogo muestra detalles acerca de los tres eventos más recientes. Puede hacer clic en un evento para ver el análisis de eventos en la página de detalles Event.

La forma en que Unified Manager determina el impacto en el rendimiento de un evento

Unified Manager utiliza la desviación de la actividad, la utilización, el rendimiento de escritura, el uso de componentes del clúster o la latencia de l/o (tiempo de respuesta) en una carga de trabajo para determinar el nivel de impacto en el rendimiento de la carga de trabajo. Esta información determina el rol de cada carga de trabajo del evento y su clasificación en la página de detalles Event.

Unified Manager compara los valores del último análisis de una carga de trabajo con el rango esperado (pronóstico de latencia) de valores. La diferencia entre los valores que se analizaron por última vez y el rango esperado de valores identifica las cargas de trabajo cuyo rendimiento tuvo un mayor impacto en el evento.

Por ejemplo, supongamos que un clúster contiene dos cargas de trabajo: La carga de trabajo A y la carga de trabajo B. El pronóstico de latencia de la carga de trabajo A es de 5-10 milisegundos por operación (ms/op) y su latencia real suele ser de aproximadamente 7 ms/op. El pronóstico de latencia para la carga de trabajo B es de 10-20 ms/op y su latencia real suele ser de aproximadamente 15 ms/op. Ambas cargas de trabajo están dentro de sus previsiones de latencia. Debido a una contención en el clúster, la latencia de ambas cargas de trabajo aumenta a 40 ms/op, que cruza el umbral de rendimiento dinámico, que es los límites superiores del pronóstico de latencia y se activan eventos. La desviación en latencia, de los valores esperados a los valores por encima del umbral de rendimiento, para la carga De trabajo A es aproximadamente de 33 ms/op y la desviación de la carga de trabajo B es de unos 25 ms/op. La latencia de ambas cargas de trabajo se dispara hasta los 40 ms/op, pero la carga De trabajo A tuvo un impacto en el rendimiento mayor porque tuvo la mayor desviación de latencia en 33 ms/op.

En la página de detalles Event, en la sección System Diagnosis, se pueden ordenar las cargas de trabajo por su desviación de la actividad, la utilización o el rendimiento de un componente del clúster. También es posible ordenar las cargas de trabajo por latencia. Cuando se selecciona una opción de ordenación, Unified Manager

analiza la desviación de la actividad, la utilización, el rendimiento o la latencia desde que se detectó el evento de los valores esperados para determinar el orden de clasificación de la carga de trabajo. Para la latencia, los puntos rojos (🔴) indica un umbral de rendimiento que cruza una carga de trabajo víctima y el impacto posterior en la latencia. Cada punto rojo indica un nivel más alto de desviación en latencia, lo que ayuda a identificar las cargas de trabajo víctimas cuya latencia más se vio afectada por un evento.

Los componentes del clúster y el motivo por los que pueden estar en contención

Puede identificar los problemas de rendimiento del clúster cuando un componente del clúster entra en disputa. El rendimiento de las cargas de trabajo que utilizan el componente disminuye y aumenta su tiempo de respuesta (latencia) para las solicitudes de clientes, lo que activa un evento en Unified Manager.

Un componente que está en disputa no puede ejecutarse en un nivel óptimo. Su rendimiento ha disminuido, y el rendimiento de otros componentes del clúster y las cargas de trabajo, llamado *Victimas*, puede haber aumentado la latencia. Para eliminar un componente de la contención, debe reducir su carga de trabajo o aumentar su capacidad para gestionar más trabajo, de modo que el rendimiento pueda volver a los niveles normales. Dado que Unified Manager recopila y analiza el rendimiento de la carga de trabajo en intervalos de cinco minutos, solo detecta cuando un componente de clúster se utiliza de forma coherente en exceso. No se detectan picos transitorios de sobreutilización que duran solo una corta duración dentro del intervalo de cinco minutos.

Por ejemplo, un agregado de almacenamiento puede ser objeto de disputa porque una o más cargas de trabajo en él están compitiendo por sus solicitudes de I/O. Otras cargas de trabajo del agregado pueden verse afectadas, lo que provoca una disminución del rendimiento. Para reducir la cantidad de actividad del agregado, hay diferentes pasos que se pueden realizar, como mover una o varias cargas de trabajo a agregados o nodos menos ocupados para reducir la demanda general de la carga de trabajo en el agregado actual. En el caso de un grupo de políticas de calidad de servicio, puede ajustar el límite de rendimiento o mover cargas de trabajo a otro grupo de políticas, de modo que las cargas de trabajo ya no se aceleren.

Unified Manager supervisa los siguientes componentes del clúster para alertarle cuando los hay en disputa:

- **Red**

  Representa el tiempo de espera de las solicitudes de I/o de los protocolos de red externos del clúster. El tiempo de espera transcurrido para que las transacciones «'están listas para la transferencia» finalicen antes de que el clúster pueda responder a una solicitud de I/O. Si el componente de red es objeto de disputa, significa que un tiempo de espera elevado en la capa de protocolo está afectando a la latencia de una o más cargas de trabajo.

- **Procesamiento de red**

  Representa el componente de software del clúster involucrado en el procesamiento de I/o entre la capa de protocolo y el clúster. Es posible que el nodo que gestiona el procesamiento de red haya cambiado desde que se detectó el evento. Si el componente de red es objeto de disputa, significa que un uso elevado en el nodo de procesamiento de red está afectando a la latencia de una o más cargas de trabajo.

  Cuando se utiliza un clúster de cabina All SAN en una configuración activo-activo, el valor de latencia de procesamiento de red se muestra en ambos nodos para poder verificar que los nodos comparten la carga igualmente.

- **Límite de QoS máx.**

  Representa la configuración máxima de rendimiento (pico) del grupo de políticas de calidad de servicio del

almacenamiento asignado a la carga de trabajo. Si el componente del grupo de políticas es objeto de disputa, significa que el límite de rendimiento establecido está acelerando todas las cargas de trabajo del grupo de políticas, lo que afecta a la latencia de una o más cargas de trabajo.

- **Límite de QoS mín.**

  Representa la latencia de una carga de trabajo causada por la configuración de rendimiento mínimo de calidad de servicio (esperado) asignada a otras cargas de trabajo. Si el valor mínimo de calidad de servicio establecido en ciertas cargas de trabajo utiliza la mayoría del ancho de banda para garantizar el rendimiento prometido, se aceleran otras cargas de trabajo y muestran más latencia.

- **Interconexión en cluster**

  Representa los cables y los adaptadores que conectan de forma física los nodos en clúster. Si el componente de interconexión del clúster es objeto de disputa, significa que un tiempo de espera elevado para las solicitudes de I/o en la interconexión del clúster está afectando a la latencia de una o más cargas de trabajo.

- **Procesamiento de datos**

  Representa el componente de software del clúster involucrado en el procesamiento de I/o entre el clúster y el agregado de almacenamiento que contiene la carga de trabajo. Es posible que el nodo que gestiona el procesamiento de datos haya cambiado desde que se detectó el evento. Si el componente de procesamiento de datos es objeto de disputa, significa que un uso elevado en el nodo de procesamiento de datos está afectando a la latencia de una o más cargas de trabajo.

- **Activación de volumen**

  Representa el proceso que realiza un seguimiento del uso de todos los volúmenes activos. En entornos de gran tamaño en los que hay más de 1000 volúmenes activos, este proceso realiza un seguimiento de la cantidad de volúmenes críticos que se necesitan para acceder a los recursos a través del nodo al mismo tiempo. Cuando el número de volúmenes activos simultáneos supera el umbral máximo recomendado, algunos de los volúmenes no críticos experimentan latencia según se identifica aquí.

- **Recursos de MetroCluster**

  Representa los recursos de MetroCluster, incluidos NVRAM y los vínculos interswitch (ISL), que se usan para reflejar datos entre los clústeres de una configuración de MetroCluster. Si el componente MetroCluster es objeto de disputa, significa que el alto rendimiento de escritura de las cargas de trabajo del clúster local o un problema de estado del enlace afectan a la latencia de una o más cargas de trabajo del clúster local. Si el clúster no está en una configuración MetroCluster, este icono no se muestra.

- **Operaciones globales o agregados de SSD**

  Representa el agregado de almacenamiento en el que se ejecutan las cargas de trabajo. Si el componente de agregado es objeto de disputa, significa que un uso elevado en el agregado está afectando a la latencia de una o más cargas de trabajo. Un agregado está formado por todos los HDD, o una combinación de HDD y SSD (un agregado de Flash Pool), o una combinación de HDD y un nivel de cloud (un agregado de FabricPool). Un «agregado SD» está compuesto por todos los SSD (un agregado all-flash) o una combinación de SSD y un nivel de cloud (un agregado de FabricPool).

- **Latencia de cloud**

  Representa el componente de software del clúster involucrado en el procesamiento de I/o entre el clúster y el nivel de cloud en el que se almacenan los datos del usuario. Si el componente de latencia del cloud es objeto de disputa, significa que una gran cantidad de lecturas de volúmenes que están alojados en el nivel

de cloud están afectando a la latencia de una o más cargas de trabajo.

- **SnapMirror** sincronizado

  Representa el componente de software del clúster involucrado en la replicación de datos de usuario del volumen primario al secundario en una relación de SnapMirror Synchronous. Si el componente Sync SnapMirror es objeto de disputa, significa que la actividad de las operaciones de SnapMirror Synchronous está afectando a la latencia de una o más cargas de trabajo.

Funciones de las cargas de trabajo involucradas en un evento de rendimiento

Unified Manager utiliza roles para identificar la implicación de una carga de trabajo en un evento de rendimiento. Entre las funciones se encuentran las víctimas, los agresores y los tiburones. Una carga de trabajo definida por el usuario puede ser víctima, abusador o tiburón al mismo tiempo.

Función	Descripción
Víctima	Carga de trabajo definida por el usuario cuyo rendimiento ha disminuido debido a otras cargas de trabajo, denominadas verdugos, que usan en exceso un componente de clúster. Solo las cargas de trabajo definidas por el usuario se identifican como víctimas. Unified Manager identifica las cargas de trabajo víctimas en función de su desviación en la latencia, donde la latencia real, durante un evento, ha aumentado considerablemente de su previsión de latencia (rango esperado).
Matón	Una carga de trabajo definida por el usuario o el sistema cuyo uso excesivo de un componente del clúster ha provocado la reducción del rendimiento de otras cargas de trabajo denominadas víctimas. Unified Manager identifica cargas de trabajo problemáticas según su desviación en el uso de un componente del clúster, donde el uso real, durante un evento, ha aumentado considerablemente desde su rango de uso esperado.
IBM	Carga de trabajo definida por el usuario con el mayor uso de un componente del clúster en comparación con todas las cargas de trabajo involucradas en un evento. Unified Manager identifica cargas de trabajo de tiburón en función de su uso de un componente de clúster durante un evento.

Las cargas de trabajo de un clúster pueden compartir muchos de los componentes del clúster, como agregados y la CPU, para el procesamiento de datos y red. Cuando una carga de trabajo, como un volumen, aumenta el uso de un componente del clúster hasta el punto de que el componente no puede satisfacer de forma eficiente las demandas de las cargas de trabajo, el componente es objeto de disputa. La carga de trabajo que utiliza en exceso un componente del clúster es un problema. Las otras cargas de trabajo que

comparten esos componentes y cuyo rendimiento afecta al abusador son las víctimas. La actividad de las cargas de trabajo definidas por el sistema, como la deduplicación o las copias Snapshot, también puede convertirse en «bullying».

Cuando Unified Manager detecta un evento, identifica todas las cargas de trabajo y los componentes del clúster implicados, incluidas las cargas de trabajo abusivas que causaron el evento, el componente de clúster que está en disputa y las cargas de trabajo víctimas cuyo rendimiento ha disminuido debido al aumento de la actividad de las cargas de trabajo abusivas.

Si Unified Manager no puede identificar las cargas de trabajo abusivas, solo envía alertas sobre las cargas de trabajo víctimas y el componente de clúster correspondiente.

Unified Manager puede identificar cargas de trabajo que son víctimas de cargas de trabajo abusivas y, además, identificar cuándo esas mismas cargas de trabajo pasan a ser cargas de trabajo abusivas. Una carga de trabajo puede ser un problema para sí misma. Por ejemplo, una carga de trabajo de alto rendimiento que está acelerando por el límite de un grupo de políticas provoca que se aceleren todas las cargas de trabajo del grupo de políticas, incluso la propia. Una carga de trabajo que sea intimidatada o víctima en un evento de rendimiento continuo puede cambiar su función o ya no ser participante en el evento.

Gestión de los umbrales de rendimiento

Las políticas de umbral de rendimiento le permiten determinar el punto en el que Unified Manager genera un evento que informa a los administradores del sistema sobre problemas que podrían afectar al rendimiento de la carga de trabajo. Estas políticas de umbral se conocen como umbrales de rendimiento *definidos por el usuario*.

Esta versión admite umbrales de rendimiento definidos por el usuario, definidos por el sistema y dinámicos. Con los umbrales dinámicos y definidos por el sistema, Unified Manager analiza la actividad de la carga de trabajo para determinar el valor de umbral adecuado. Con los umbrales definidos por el usuario, puede definir los límites superiores de rendimiento para muchos contadores de rendimiento y para muchos objetos de almacenamiento.

Los umbrales de rendimiento definidos por el sistema y los umbrales de rendimiento dinámico los establece Unified Manager y no se pueden configurar. Si recibe eventos innecesarios de alguna política de umbral de rendimiento definida por el sistema, puede deshabilitar políticas individuales de la página Event Setup.

Cómo funcionan las políticas de umbral de rendimiento definidas por el usuario

Puede establecer políticas de umbral de rendimiento en objetos de almacenamiento (por ejemplo, en agregados y volúmenes) para que se pueda enviar un evento al administrador de almacenamiento con el fin de informar al administrador de que el clúster está experimentando un problema de rendimiento.

Puede crear una política de umbral de rendimiento para un objeto de almacenamiento mediante:

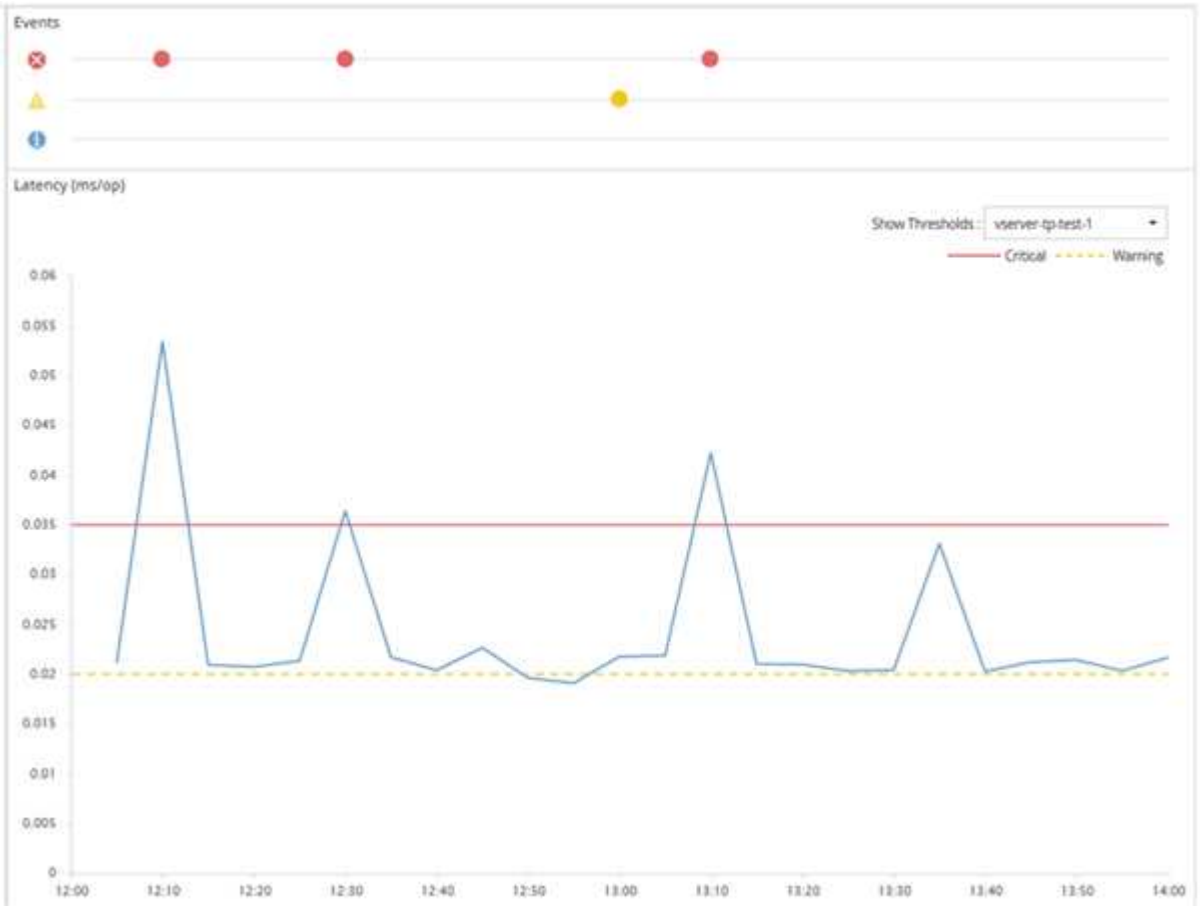
- Seleccionar un objeto de almacenamiento
- Seleccionar un contador de rendimiento asociado con ese objeto
- Especificación de valores que definen los límites superiores del contador de rendimiento que se consideran situaciones críticas y de advertencia

- Especificación de un período de tiempo que define el tiempo que el contador debe superar el límite superior

Por ejemplo, puede establecer una política de umbral de rendimiento en un volumen, de modo que se reciba una notificación de evento crucial siempre que las IOPS de ese volumen superen las 750 operaciones por segundo durante 10 minutos consecutivos. Esta misma política de umbral también puede especificar que se envíe un evento de advertencia cuando IOPS supere las 500 operaciones por segundo durante 10 minutos.

La versión actual proporciona umbrales que envían eventos cuando un valor de contador supera el valor del umbral. No se pueden establecer umbrales que envíen eventos cuando un valor de contador esté por debajo de un valor de umbral.

Se muestra un gráfico de contadores de ejemplo aquí, lo que indica que se incumplido un umbral de advertencia (icono amarillo) a las 1:00, y que se violó un umbral crítico (icono rojo) a las 12:10, 12:30 y 1:10:



Se debe producir una infracción de umbral continuamente durante la duración especificada. Si el umbral cae por debajo de los valores límite por cualquier motivo, una infracción posterior se considera el inicio de una nueva duración.

Algunos objetos del clúster y contadores de rendimiento permiten crear una política de umbral de combinación que requiere dos contadores de rendimiento para superar sus límites máximos antes de que se genere un evento. Por ejemplo, puede crear una política de umbral con los siguientes criterios:

Objeto de clúster	Contador de rendimiento	Umbral de advertencia	Umbral crítico	Duración
Volumen	Latencia	10 milisegundos	20 milisegundos	15 minutos
Agregado	Utilización	65 %	85 %	

Las políticas de umbral que utilizan dos objetos de clúster hacen que se genere un evento solo cuando se incumplen ambas condiciones. Por ejemplo, utilizando la política de umbral definida en la tabla:

Si la latencia de un volumen está promediando…	Y el uso del disco agregado es…	Realice lo siguiente…
15 milisegundos	50 %	No se informa de ningún evento.
15 milisegundos	75 %	Se informa de un evento de advertencia.
25 milisegundos	75 %	Se informa de un evento de advertencia.
25 milisegundos	90 %	Se informa de un evento crítico.

Qué sucede cuando se incumple una política de umbral de rendimiento

Cuando un valor de contador supera su valor de umbral de rendimiento definido para la cantidad de tiempo especificada en la duración, se supera el umbral y se informa de un evento.

El evento hace que se inicien las siguientes acciones:

- El evento se muestra en la página Dashboard, Performance Cluster Summary, la página Events y la página Performance Inventory específica para cada objeto.
- (Opcional) puede enviarse una alerta de correo electrónico sobre el evento a uno o más destinatarios de correo electrónico y puede enviarse una captura SNMP a un receptor de capturas.
- (Opcional) se puede ejecutar un script para modificar o actualizar automáticamente objetos de almacenamiento.

La primera acción se ejecuta siempre. Puede configurar si las acciones opcionales se realizan en la página Configuración de alertas. Puede definir acciones únicas en función de si se incumplen una política de advertencia o de umbral crítico.

Una vez que se ha producido una infracción de política de umbral de rendimiento en un objeto de almacenamiento, no se generan más eventos para esa política hasta que el valor del contador no supere el valor del umbral, momento en el que la duración se restablece para ese límite. Mientras se sigue excediendo el umbral, la hora de finalización del evento se actualiza continuamente para reflejar que este evento está en curso.

Un evento de umbral captura o congela la información relacionada con la gravedad y la definición de la política

de modo que la información de umbral única se muestre con el evento, incluso si la política de umbral se modifica en el futuro.

Se puede realizar un seguimiento de los contadores de rendimiento mediante umbrales

Algunos contadores de rendimiento comunes, como IOPS y MB/s, pueden tener umbrales definidos para todos los objetos de almacenamiento. Hay otros contadores que pueden tener umbrales establecidos para determinados objetos de almacenamiento.

Contadores de rendimiento disponibles

Objeto de almacenamiento	Contador de rendimiento	Descripción
Clúster	IOPS	Promedio de operaciones de entrada/salida que el clúster procesa por segundo.
MB/s	Número medio de megabytes de datos que se transfieren a y desde este clúster por segundo.	Nodo
IOPS	Promedio de operaciones de entrada/salida que el nodo procesa por segundo.	MB/s
Número medio de megabytes de datos que se transfieren a y desde este nodo por segundo.	Latencia	Número medio de milisegundos que tarda el nodo en responder a las solicitudes de las aplicaciones.
Utilización	Porcentaje medio de la CPU y la RAM del nodo que se está utilizando.	Capacidad de rendimiento utilizada
Porcentaje promedio de capacidad de rendimiento que está consumiendo el nodo.	Capacidad de rendimiento utilizada: Respaldo	Porcentaje medio de la capacidad de rendimiento que está consumiendo el nodo, más la capacidad de rendimiento de su nodo asociado.
Agregado	IOPS	Número medio de operaciones de entrada/salida de procesos agregados por segundo.
MB/s	Cantidad media de megabytes de datos que se transfieren a y desde este agregado por segundo.	Latencia

Objeto de almacenamiento	Contador de rendimiento	Descripción
Número medio de milisegundos que tarda el agregado en responder a las solicitudes de aplicaciones.	Utilización	Porcentaje medio de los discos del agregado que se están utilizando.
Capacidad de rendimiento utilizada	Porcentaje medio de capacidad de rendimiento que consume el agregado.	Máquina virtual de almacenamiento
IOPS	Número medio de operaciones de entrada/salida que los procesos de SVM por segundo.	MB/s
Número medio de megabytes de datos que se transfieren a y desde esta SVM por segundo.	Latencia	Número medio de milisegundos que la SVM tarda en responder a las solicitudes de aplicaciones.
Volumen	IOPS	Número medio de operaciones de entrada/salida que procesa el volumen por segundo.
MB/s	Número medio de megabytes de datos que se transfieren a y desde este volumen por segundo.	Latencia
Número medio de milisegundos que el volumen tarda en responder a las solicitudes de las aplicaciones.	Ratio de pérdidas de caché	Porcentaje medio de solicitudes de lectura de aplicaciones cliente que regresan de el volumen, en lugar de que regresan de la caché.
LUN	IOPS	Número medio de operaciones de entrada/salida que los procesos de LUN por segundo.
MB/s	Número medio de megabytes de datos que se transfieren a y desde esta LUN por segundo.	Latencia
Número medio de milisegundos que tarda la LUN en responder a las solicitudes de aplicaciones.	Espacio de nombres	IOPS
Número medio de operaciones de entrada/salida que procesa el espacio de nombres por segundo.	MB/s	Número medio de megabytes de datos que se transfieren a y desde este espacio de nombres por segundo.

Objeto de almacenamiento	Contador de rendimiento	Descripción
Latencia	Número medio de milisegundos que el espacio de nombres tarda en responder a las solicitudes de las aplicaciones.	Puerto
Uso del ancho de banda	El porcentaje medio de ancho de banda disponible del puerto que se está utilizando.	MB/s
Número medio de megabytes de datos que se transfieren a y desde este puerto por segundo.	Interfaz de red (LIF)	MB/s

Qué objetos y contadores pueden utilizarse en políticas de umbral de combinación

Sólo algunos contadores de rendimiento se pueden utilizar juntos en políticas de combinación. Cuando se especifican contadores de rendimiento primario y secundario, ambos contadores de rendimiento deben superar sus límites máximos antes de que se genere un evento.

Objeto y contador de almacenamiento principal	Objeto de almacenamiento secundario y contador
Latencia del volumen	IOPS de volumen
Volumen MB/s	Utilización de agregados
Capacidad de rendimiento de agregados utilizada	Uso de nodos
Capacidad de rendimiento de nodo utilizada	Capacidad de rendimiento del nodo utilizada: Respaldo
Latencia de LUN	IOPS DE LUN
LUN MB/s	Utilización de agregados
Capacidad de rendimiento de agregados utilizada	Uso de nodos
Capacidad de rendimiento de nodo utilizada	Capacidad de rendimiento del nodo utilizada: Respaldo

Cuando se aplica una política de combinación de volúmenes a un volumen FlexGroup, en lugar de a un volumen FlexVol, solo pueden seleccionarse como contador secundario los atributos «'IOPS de volumen» y «'MB/s» de volumen. Si la política de umbral contiene uno de los atributos del nodo o de agregado, la política no se aplicará al volumen de FlexGroup y recibirá un mensaje de error en el que se describe este caso. Esto se debe a que los volúmenes FlexGroup pueden existir en más de un nodo o agregado.

Creación de políticas de umbral de rendimiento definidas por el usuario

Es posible crear políticas de umbral de rendimiento para los objetos de almacenamiento, de manera tal que se envíen notificaciones cuando un contador de rendimiento supere un valor específico. La notificación de eventos identifica que el clúster está experimentando un problema de rendimiento.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Para crear políticas de umbral de rendimiento, se deben introducir los valores de umbral en la página Create Performance Threshold Policy. Puede crear nuevas políticas definiendo todos los valores de la política en esta página o puede hacer una copia de una política existente y cambiar los valores de la copia (denominada *clone*).

Los valores de umbral válidos son de 0.001 a 10,000,000 para números, 0.001-100 para porcentajes y 0.001-200 para porcentajes de capacidad de rendimiento utilizados.

La versión actual proporciona umbrales que envían eventos cuando un valor de contador supera el valor del umbral. No se pueden establecer umbrales que envíen eventos cuando un valor de contador esté por debajo de un valor de umbral.

Pasos

1. En el panel de navegación izquierdo, seleccione **umbrales de evento** > **rendimiento**.

   Se muestra la página Performance Thresholds.

2. Haga clic en el botón apropiado en función de si desea crear una nueva política o si desea clonar una política similar y modificar la versión clonada.

Para…	Haga clic en…
Crear una nueva política	**Crear**
Clonar una política existente	Seleccione una directiva existente y haga clic en **Clonar**

   Se mostrarán la página Create Performance Threshold Policy o Clone Performance Threshold Policy.

3. Defina la política de umbral especificando los valores de umbral de contador de rendimiento que desea establecer para objetos de almacenamiento específicos:

   a. Seleccione el tipo de objeto de almacenamiento y especifique un nombre y una descripción para la

política.

b. Seleccione el contador de rendimiento que se va a realizar el seguimiento y especifique los valores de límite que definen los eventos de advertencia y críticos.

   Debe definir al menos un límite de advertencia o crítico. No es necesario definir ambos tipos de límites.

c. Seleccione un contador de rendimiento secundario, si es necesario, y especifique los valores de límite para eventos críticos y de advertencia.

   Para incluir un contador secundario, ambos contadores superan los valores de límite antes de superar el umbral y se informa de un evento. Sólo se pueden configurar determinados objetos y contadores mediante una directiva de combinación.

d. Seleccione la duración del tiempo durante el cual deben incumplir los valores límite para que se envíe un evento.

Al clonar una política existente, debe introducir un nombre nuevo para la política.

4. Haga clic en **Guardar** para guardar la directiva.

   El resultado es la página Performance Thresholds. Un mensaje de éxito en la parte superior de la página confirma que la política de umbral se ha creado y proporciona un enlace a la página Inventory de ese tipo de objeto para que pueda aplicar la nueva política a los objetos de almacenamiento inmediatamente.

Si desea aplicar la nueva directiva de umbral a objetos de almacenamiento en este momento, puede hacer clic en el vínculo **Ir a objeto_TYPE Now** para ir a la página Inventario.

Asignación de políticas de umbral de rendimiento a objetos de almacenamiento

Se asigna una política de umbral de rendimiento definida por el usuario a un objeto de almacenamiento de modo que Unified Manager informe un evento si el valor del contador de rendimiento supera el valor de la política.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Debe existir la política de umbral de rendimiento, o las políticas, que desea aplicar al objeto.

Solo se puede aplicar una política de rendimiento a la vez a un objeto o a un grupo de objetos.

Es posible asignar un máximo de tres políticas de umbral a cada objeto de almacenamiento. Cuando se asignan políticas a varios objetos, si alguno de ellos ya tiene el número máximo de políticas asignadas, Unified Manager realiza las siguientes acciones:

- Aplica la política a todos los objetos seleccionados que no han alcanzado su máximo
- Ignora los objetos que han alcanzado el número máximo de políticas
- Muestra un mensaje que indica que la directiva no se ha asignado a todos los objetos

Pasos

1. En la página Performance Inventory de cualquier objeto de almacenamiento, seleccione el objeto o los objetos a los que desea asignar una política de umbral:

Para asignar umbrales a…	Haga clic en…
Un solo objeto	La casilla de verificación situada a la izquierda de ese objeto.
Varios objetos	La casilla de verificación situada a la izquierda de cada objeto.
Todos los objetos de la página	La ☐▾ Y seleccione **Seleccionar todos los objetos de esta página**.
Todos los objetos del mismo tipo	La ☐▾ Y seleccione **Seleccionar todos los objetos**.

Puede utilizar la funcionalidad de ordenación y filtrado para refinar la lista de objetos de la página de inventario para facilitar la aplicación de políticas de umbral a muchos objetos.

2. Realice su selección y, a continuación, haga clic en **asignar directiva de umbral de rendimiento**.

   Se muestra la página Assign Performance Threshold Policy, donde se muestra una lista de las políticas de umbral que existen para ese tipo específico de objeto de almacenamiento.

3. Haga clic en cada política para mostrar los detalles de la configuración de umbral de rendimiento a fin de verificar que ha seleccionado la política de umbral correcta.
4. Después de seleccionar la directiva de umbral adecuada, haga clic en **asignar directiva**.

   Un mensaje de éxito en la parte superior de la página confirma que la política de umbral se ha asignado al objeto u objetos y proporciona un enlace a la página Alertas para que pueda configurar las opciones de alerta para este objeto y esta política.

Si desea que las alertas se envíen por correo electrónico o como captura SNMP, para notificarle que se ha generado un evento de rendimiento en particular, debe configurar los ajustes de alerta en la página Alert Setup.

Ver las políticas de umbral de rendimiento

Es posible ver todas las políticas de umbral de rendimiento definidas actualmente en la página Performance Thresholds.

La lista de políticas de umbral se ordena alfabéticamente por nombre de política, y incluye política para todo tipo de objetos de almacenamiento. Puede hacer clic en un encabezado de columna para ordenar las políticas según esa columna. Si busca una política específica, utilice los mecanismos de filtro y búsqueda para refinar la lista de políticas de umbral que aparecen en la lista de inventario.

Puede pasar el cursor sobre el nombre de la política y el nombre de la condición para ver los detalles de configuración de la política. Además, puede utilizar los botones proporcionados para crear, clonar, editar y eliminar políticas de umbral definidas por el usuario.

Paso

1. En el panel de navegación izquierdo, seleccione **umbrales de evento** > **rendimiento**.

Se muestra la página Performance Thresholds.

Editar políticas de umbral de rendimiento definidas por el usuario

La configuración del umbral se puede editar para las políticas de umbral de rendimiento existentes. Esto puede ser útil si descubre que está recibiendo demasiadas alertas o muy pocas para ciertas condiciones de umbral.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

No es posible cambiar el nombre de la política ni el tipo de objeto de almacenamiento que se supervisa para las políticas de umbral existentes.

Pasos

1. En el panel de navegación izquierdo, seleccione **umbrales de evento** > **rendimiento**.

   Se muestra la página Performance Thresholds.

2. Seleccione la directiva de umbral que desea cambiar y haga clic en **Editar**.

   Se muestra la página Edit Performance Threshold Policy.

3. Realice los cambios realizados en la directiva de umbral y haga clic en **Guardar**.

   El resultado es la página Performance Thresholds.

Después de guardar, los cambios se actualizan inmediatamente en todos los objetos de almacenamiento que usan la política.

En función del tipo de cambios realizados en la directiva, es posible que desee revisar la configuración de alerta configurada para los objetos que utilizan la directiva en la página Configuración de alertas.

Eliminación de políticas de umbral de rendimiento de objetos de almacenamiento

Es posible quitar una política de umbral de rendimiento definida por el usuario de un objeto de almacenamiento cuando ya no se desea que Unified Manager supervise el valor del contador de rendimiento.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

Solo puede eliminar una política cada vez de un objeto seleccionado.

Puede quitar una política de umbral de varios objetos de almacenamiento si selecciona más de un objeto de la lista.

Pasos

1. En la página **Inventory** de cualquier objeto de almacenamiento, seleccione uno o más objetos que tengan al menos una política de umbral de rendimiento aplicada.

Para borrar umbrales de…	Realice lo siguiente…
Un solo objeto	Seleccione la casilla de verificación situada a la izquierda de ese objeto.
Varios objetos	Seleccione la casilla de verificación situada a la izquierda de cada objeto.
Todos los objetos de la página	Haga clic en en el encabezado de la columna.

2. Haga clic en **Borrar Directiva de umbral de rendimiento**.

   Se muestra la página Clear Threshold Policy, que muestra una lista de las políticas de umbral asignadas actualmente a los objetos de almacenamiento.

3. Seleccione la directiva de umbral que desea eliminar de los objetos y haga clic en **Borrar directiva**.

   Al seleccionar una directiva de umbral, se muestran los detalles de la directiva para que pueda confirmar que ha seleccionado la directiva adecuada.

Qué ocurre cuando se cambia una política de umbral de rendimiento

Si ajusta el valor de contador o la duración de una política de umbral de rendimiento existente, el cambio de política se aplica a todos los objetos de almacenamiento que usan la política. El nuevo ajuste se realiza de inmediato y Unified Manager comienza a comparar los valores de contador de rendimiento con la nueva configuración de umbral de todos los datos de rendimiento recientemente recopilados.

Si existe algún evento activo para los objetos que utilizan la política de umbral modificada, los eventos se marcan como obsoletos y la política de umbral comienza a supervisar el contador como una política de umbral recientemente definida.

Al ver el contador en el que se ha aplicado el umbral en la vista detallada de los gráficos de contador, las líneas de umbral críticas y de advertencia reflejan la configuración de umbral actual. La configuración de umbral original no aparece en esta página aunque vea los datos históricos cuando la configuración de umbral anterior estaba en vigor.

Puesto que las configuraciones de umbral más antiguas no aparecen en la vista detallada de los gráficos de contador, es posible que aparezcan eventos históricos que aparecen debajo de las líneas de umbral actuales.

Qué sucede con las políticas de umbral de rendimiento cuando se mueve un objeto

Dado que las políticas de umbral de rendimiento se asignan a los objetos de almacenamiento, si se mueve un objeto, todas las políticas de umbral asignadas se conservan asociadas al objeto después de completar el movimiento. Por ejemplo, si mueve un volumen o una LUN a otro agregado, las políticas de umbral seguirán activas para el volumen o LUN del nuevo agregado.

Si existe una condición de contador secundario para la política de umbral (una política de combinación), por ejemplo, si se asigna una condición adicional a un agregado o a un nodo, la condición de contador secundario se aplica al nuevo agregado o nodo al que se ha movido el volumen o LUN.

Si existe algún evento activo nuevo para los objetos que utilizan la política de umbral modificado, los eventos se marcan como obsoletos y la política de umbral comienza a supervisar el contador como una política de umbral recientemente definida.

Una operación de movimiento de volúmenes hace que ONTAP envíe un evento de cambio informativo. Aparece un icono de evento de cambio en la línea de tiempo Events en la página Performance Explorer y en la página Workload Analysis para indicar la hora a la que se completó la operación de movimiento.

> Si mueve un objeto a un clúster diferente, la política de umbral definida por el usuario se elimina del objeto. Si es necesario, debe asignar una política de umbral al objeto una vez completada la operación de movimiento. Sin embargo, las políticas de umbral dinámicas y definidas por el sistema se aplican automáticamente a un objeto después de mover este a un nuevo clúster.

Funcionalidad de política de umbral durante la toma de control y el retorno al nodo primario de ha

Cuando una operación de toma de control o devolución se produce en una configuración de alta disponibilidad (ha), los objetos que se mueven de un nodo al otro nodo conservan sus políticas de umbral del mismo modo que en las operaciones de movimiento manual. Dado que Unified Manager comprueba si hay cambios en la configuración del clúster cada 15 minutos, el impacto de la conmutación al nuevo nodo no se identifica hasta el siguiente sondeo de la configuración del clúster.

> Si se produce una operación de toma de control y devolución dentro del período de recogida de cambios de configuración de 15 minutos, es posible que no vea cómo se mueven las estadísticas de rendimiento de un nodo al otro nodo.

Funcionalidad de políticas de umbral durante la reubicación de agregados

Si mueve un agregado de un nodo a otro mediante el `aggregate relocation start` comando, tanto las políticas de umbral de combinación como las únicas se conservan en todos los objetos y la parte de nodo de la política de umbral se aplica al nuevo nodo.

Funcionalidad de políticas de umbral durante la conmutación de MetroCluster

Los objetos que se mueven de un clúster a otro de una configuración de MetroCluster no conservan su configuración de política de umbral definida por el usuario. Si es necesario, puede aplicar políticas de umbral en los volúmenes y LUN que se han movido al clúster de partners. Después de que un objeto se haya movido de nuevo a su clúster original, la política de umbral definida por el usuario se vuelve a aplicar automáticamente.

Para obtener más información, consulte "Comportamiento del volumen durante la conmutación de sitios y la conmutación de estado".

Análisis de eventos de rendimiento

Puede analizar los eventos de rendimiento para identificar cuándo se detectaron, si están activos (nuevos o reconocidos) o obsoletos, las cargas de trabajo y los componentes del clúster afectados, y las opciones para resolver los eventos por su cuenta.

Mostrar información acerca de los eventos de rendimiento

La página del inventario Event Management se puede usar para ver una lista de todos los eventos de rendimiento en los clústeres que se supervisan Unified Manager. Al ver esta información, puede determinar los eventos más críticos y, a continuación, profundizar en información detallada para determinar la causa del evento.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

La lista de eventos se ordena por hora detectada, con los eventos más recientes listados primero. Puede hacer clic en un encabezado de columna para ordenar los eventos según esa columna. Por ejemplo, puede ordenar por la columna Estado para ver los eventos por gravedad. Si está buscando un evento específico o un tipo de evento específico, puede utilizar el filtro y los mecanismos de búsqueda para afinar la lista de eventos que aparecen en la lista.

Los eventos de todos los orígenes se muestran en esta página:

- Política de umbral de rendimiento definida por el usuario
- Política de umbral de rendimiento definida por el sistema
- Umbral de rendimiento dinámico

La columna Tipo de evento enumera el origen del evento. Puede seleccionar un evento para ver detalles sobre él en la página de detalles Event.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Gestión de eventos**.
2. En el menú Ver, seleccione **Eventos de rendimiento activos**.

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

3. Busque un evento que desee analizar y haga clic en el nombre del evento.

   Se muestra la página de detalles del evento.

> También puede mostrar la página de detalles de un evento si se hace clic en el enlace del nombre del evento de la página Performance Explorer y también desde un correo electrónico de alerta.

Análisis de eventos de umbrales de rendimiento definidos por el usuario

Los eventos generados a partir de umbrales definidos por el usuario indican que un contador de rendimiento de un determinado objeto de almacenamiento, por ejemplo, un agregado o un volumen, ha superado el umbral definido en la política. Esto indica que el objeto del clúster está experimentando un problema de rendimiento.

La página de detalles Event se utiliza para analizar el evento de rendimiento y realizar las acciones correctivas necesarias para devolver el rendimiento a la normalidad.

Respuesta a eventos de umbral de rendimiento definidos por el usuario

Puede utilizar Unified Manager para investigar los eventos de rendimiento causados por un contador de rendimiento que cruza un umbral crítico o de advertencia definido por el usuario. También puede usar Unified Manager para comprobar el estado del componente del clúster a fin de ver si los eventos de estado recientes detectados en el componente contribuyeron al evento de rendimiento.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Debe haber eventos de rendimiento nuevos o obsoletos.

Pasos

1. Abra la página **Detalles del evento** para ver información sobre el evento.
2. Revise la **Descripción**, que describe la brecha de umbral que provocó el evento.

   Por ejemplo, el mensaje "'valor de latencia de 456 ms/op ha activado un evento DE ADVERTENCIA basado en el valor de umbral de 400 ms/op'" indica que se ha producido un evento de advertencia de latencia para el objeto.

3. Pase el cursor sobre el nombre de la política para mostrar detalles sobre la política de umbral que activó el evento.

   Esto incluye el nombre de la política, el contador de rendimiento que se está evaluando, el valor del contador que debe incumplir para considerarse un evento crítico o de advertencia y la duración mediante la cual el contador debe superar el valor.

4. Tome nota del **tiempo de activación del evento** para que pueda investigar si se han producido otros eventos al mismo tiempo que podrían haber contribuido a este evento.
5. Siga una de las siguientes opciones para investigar más a fondo el evento y determinar si necesita realizar alguna acción para resolver el problema de rendimiento:

Opción	Posibles acciones de investigación
Haga clic en el nombre del objeto Source para mostrar la página Explorer de ese objeto.	Esta página permite ver los detalles del objeto y comparar este objeto con otros objetos de almacenamiento similares para ver si otros objetos de almacenamiento tienen un problema de rendimiento al mismo tiempo. Por ejemplo, para ver si otros volúmenes del mismo agregado están teniendo también un problema de rendimiento.
Haga clic en el nombre del clúster para mostrar la página Cluster Summary.	Esta página le permite ver los detalles del clúster en el que reside el objeto para ver si existen otros problemas de rendimiento a la vez.

Analizar eventos de umbrales de rendimiento definidos por el sistema

Los eventos generados a partir de umbrales de rendimiento definidos por el sistema

indican que un contador de rendimiento, o un conjunto de contadores de rendimiento, para un determinado objeto de almacenamiento ha superado el umbral de una política definida por el sistema. Esto indica que el objeto de almacenamiento, por ejemplo, un agregado o nodo, está experimentando un problema de rendimiento.

La página de detalles Event se utiliza para analizar el evento de rendimiento y realizar las acciones correctivas necesarias para devolver el rendimiento a la normalidad.

Las políticas de umbral definidas por el sistema no se habilitan en sistemas Cloud Volumes ONTAP, ONTAP Edge o ONTAP Select.

Respuesta a eventos de umbral de rendimiento definidos por el sistema

Es posible utilizar Unified Manager para investigar los eventos de rendimiento provocados por un contador de rendimiento que cruce un umbral de advertencia definido por el sistema. También puede usar Unified Manager para comprobar el estado del componente del clúster a fin de ver si los eventos recientes detectados en el componente contribuyeron al evento de rendimiento.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Debe haber eventos de rendimiento nuevos o obsoletos.

Pasos

1. Abra la página **Detalles del evento** para ver información sobre el evento.
2. Revise la **Descripción**, que describe la brecha de umbral que provocó el evento.

   Por ejemplo, el mensaje "'valor de utilización de nodos del 90 % ha activado un evento DE ADVERTENCIA basado en el valor de umbral del 85 %'" indica que se ha producido un evento de advertencia de utilización de nodos para el objeto de clúster.

3. Tome nota del **tiempo de activación del evento** para que pueda investigar si se han producido otros eventos al mismo tiempo que podrían haber contribuido a este evento.
4. En **Diagnóstico del sistema**, revise la breve descripción del tipo de análisis que la directiva definida por el sistema está realizando en el objeto de clúster.

   En algunos casos se muestra un icono verde o rojo junto al diagnóstico para indicar si se ha encontrado un problema en ese diagnóstico en particular. Para otros tipos de gráficos de contadores de eventos definidos por el sistema, se muestra el rendimiento del objeto.

5. En **acciones sugeridas**, haga clic en el enlace **Ayúdame a hacer esto** para ver las acciones sugeridas que puede realizar para intentar resolver el evento de rendimiento por su cuenta.

Responder a los eventos de rendimiento del grupo de políticas de calidad de servicio

Unified Manager genera eventos de advertencia sobre las políticas de calidad de servicio cuando el rendimiento de las cargas de trabajo (IOPS, IOPS/TB o Mbps) superó la configuración de la política de calidad de servicio de ONTAP definida y la latencia de las cargas de trabajo se ve cada vez más afectada. Estos eventos definidos por el sistema

proporcionan la oportunidad para corregir posibles problemas de rendimiento antes de que muchas cargas de trabajo se vean afectadas por la latencia.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Debe haber eventos de rendimiento nuevos, reconocidos o obsoletos.

Unified Manager genera eventos de advertencia para incumplimiento de políticas de calidad de servicio cuando el rendimiento de la carga de trabajo superó la configuración de la política de calidad de servicio definida durante cada periodo de recogida de rendimiento de la hora anterior. El rendimiento de la carga de trabajo puede superar el umbral de calidad de servicio durante un breve periodo de tiempo durante cada periodo de recogida, pero Unified Manager muestra únicamente el rendimiento «medio» durante el periodo de recogida del gráfico. Por este motivo, puede recibir eventos de calidad de servicio mientras que el rendimiento de una carga de trabajo puede no haber superado el umbral de política que se muestra en el gráfico.

Puede usar System Manager o los comandos de la ONTAP para gestionar los grupos de políticas, incluidas las siguientes tareas:

- Crear un grupo de políticas nuevo para la carga de trabajo
- Agregar o eliminar cargas de trabajo en un grupo de políticas
- Mover una carga de trabajo entre grupos de políticas
- Cambiar el límite de rendimiento de un grupo de políticas
- Mover una carga de trabajo a un agregado o nodo diferente

Pasos

1. Abra la página **Detalles del evento** para ver información sobre el evento.
2. Revise la **Descripción**, que describe la brecha de umbral que provocó el evento.

   Por ejemplo, el mensaje "'IOPS value of 1,352 IOPS on vol1_NFS1 ha activado un evento DE ADVERTENCIA para identificar problemas potenciales de rendimiento para la carga de trabajo'" indica que se ha producido un evento QoS Max IOPS en el volumen vol1_NFS1.

3. Consulte la sección **Información de evento** para obtener más información sobre cuándo se produjo el evento y cuánto tiempo ha estado activo.

   Además, para los volúmenes o LUN que comparten el rendimiento de una política de calidad de servicio, puede ver los nombres de las tres cargas de trabajo principales que consumen más IOPS o Mbps.

4. En la sección **Diagnóstico del sistema**, revise los dos gráficos: Uno para el promedio total de IOPS o Mbps (dependiendo del evento) y uno para latencia. Cuando se organiza de esta forma, se pueden ver los componentes del clúster que afectan en mayor medida a la latencia cuando la carga de trabajo se acercó al límite máximo de calidad de servicio.

   Para un evento de política de calidad de servicio compartida, las tres cargas de trabajo principales se muestran en el gráfico de rendimiento. Si más de tres cargas de trabajo comparten la política de calidad de servicio, se añaden cargas de trabajo adicionales en una categoría «¿otras cargas de trabajo». Además, el gráfico latencia muestra la latencia media de todas las cargas de trabajo que forman parte de la política de calidad de servicio.

   Tenga en cuenta que, para los eventos de política de calidad de servicio adaptativos, los gráficos IOPS y Mbps muestran los valores de IOPS o Mbps que ONTAP ha convertido de la política de umbral de

IOPS/TB asignada en función del tamaño del volumen.

5. En la sección **acciones sugeridas**, revise las sugerencias y determine qué acciones debe realizar para evitar un aumento en la latencia de la carga de trabajo.

   Si es necesario, haga clic en el botón **Ayuda** para ver más detalles sobre las acciones sugeridas que puede realizar para intentar resolver el evento de rendimiento.

Eventos de políticas de calidad de servicio adaptativas que tienen un tamaño de bloque definido

Los grupos de políticas de calidad de servicio adaptativos escalan automáticamente el techo o el piso de rendimiento según el tamaño del volumen y mantienen la ratio de IOPS en TB a medida que cambie el tamaño del volumen. A partir de ONTAP 9.5 puede especificar el tamaño de bloque en la política de calidad de servicio para aplicar eficazmente un umbral de MB/s al mismo tiempo.

Al asignar un umbral de IOPS en una política de calidad de servicio adaptativa, solo se establece un límite en el número de operaciones que se producen en cada carga de trabajo. Según el tamaño de bloque que se establece en el cliente que genera las cargas de trabajo, algunas IOPS incluyen muchos más datos y, por lo tanto, colocan una carga mucho más grande en los nodos que procesan las operaciones.

El valor MB/s para una carga de trabajo se genera con la siguiente fórmula:

```
MB/s = (IOPS * Block Size) / 1000
```

Si la carga de trabajo tiene una media de 3,000 IOPS y el tamaño de bloque en el cliente se establece en 32 KB, los MB/s efectivos para esta carga de trabajo son 96. Si esta misma carga de trabajo tiene una media de 3,000 IOPS y el tamaño de bloque en el cliente se establece en 48 KB, el tamaño de bloque efectivo para esta carga de trabajo es de 144 MB/s. Puede ver que el nodo está procesando un 50 % más de datos cuando el tamaño de bloque es mayor.

Echemos un vistazo a la siguiente política de calidad de servicio adaptativa que tiene un tamaño de bloque definido y cómo se activan los eventos en función del tamaño de bloque que se establece en el cliente.

Cree una política y establezca el rendimiento máximo en 2,500 IOPS/TB con un tamaño de bloque de 32 KB. De este modo, el umbral de MB/s se establece en 80 MB/s ((2500 IOPS * 32 KB) / 1000) para un volumen con 1 TB de capacidad utilizada. Tenga en cuenta que Unified Manager genera un evento de advertencia cuando el valor de rendimiento es un 10 % inferior al umbral definido. Los eventos se generan en las siguientes situaciones:

Capacidad utilizada	**El evento se genera cuando el rendimiento supera este número de …**	
	IOPS	MB/s
1 TB	2,250 000 IOPS	72 MB/s
2 TB	4,500 000 IOPS	144 MB/s
5 TB	11,250 000 IOPS	360 MB/s

Si el volumen utiliza 2 TB del espacio disponible y la tasa de IOPS es 4,000 y el tamaño de bloque de calidad de servicio está establecido en 32 KB en el cliente, el rendimiento de MB/ps es 128 MB/s ((4,000 IOPS * 32 KB) / 1000). No se genera ningún evento en este caso, ya que tanto 4,000 IOPS como 128 MB/s están por debajo del umbral para un volumen que utiliza 2 TB de espacio.

Si el volumen utiliza 2 TB del espacio disponible, y la tasa de IOPS es 4,000, y el tamaño de bloque de calidad de servicio está configurado como 64 KB en el cliente, el rendimiento de MB/s es de 256 MB/s ((4,000 IOPS * 64 KB) / 1000). En este caso, las 4,000 IOPS no generan un evento, pero el valor de MB/s de 256 MB/s se encuentra por encima del umbral de 144 MB/s y se genera un evento.

Por esta razón, cuando se activa un evento basado en una infracción MB/s de una directiva de QoS adaptativa que incluye el tamaño de bloque, se muestra un gráfico MB/s en la sección Diagnóstico del sistema de la página de detalles evento. Si el evento se activa en función de una filtración de IOPS para la política de calidad de servicio adaptativa, se muestra un gráfico de IOPS en la sección System Diagnosis. Si se produce una infracción tanto para IOPS como para MB/s, recibirá dos eventos.

Para obtener más información sobre el ajuste de la configuración de QoS, consulte "Información general sobre gestión del rendimiento".

Respuesta a eventos de rendimiento sobreutilizados de recursos de nodos

Unified Manager genera eventos de advertencia sobreutilizados de los recursos de nodos cuando un único nodo está funcionando por encima de los límites de su eficiencia operativa y, por lo tanto, afecta potencialmente a las latencias de las cargas de trabajo. Estos eventos definidos por el sistema proporcionan la oportunidad para corregir posibles problemas de rendimiento antes de que muchas cargas de trabajo se vean afectadas por la latencia.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Debe haber eventos de rendimiento nuevos o obsoletos.

Unified Manager genera eventos de advertencia para las infracciones de políticas de recursos de nodos sobreutilizadas buscando nodos que utilicen más del 100 % de su capacidad de rendimiento durante más de 30 minutos.

Puede usar System Manager o los comandos de la ONTAP para corregir este tipo de problema de rendimiento, incluidas las siguientes tareas:

- Crear y aplicar una política de calidad de servicio a cualquier volumen o LUN que utilicen en exceso los recursos del sistema
- Reducir el límite máximo de rendimiento de la calidad de servicio de un grupo de políticas al cual se aplican cargas de trabajo
- Mover una carga de trabajo a un agregado o nodo diferente
- Aumentar la capacidad añadiendo discos al nodo o actualizando a un nodo con una CPU más rápida y más RAM

Pasos

1. Abra la página **Detalles del evento** para ver información sobre el evento.
2. Revise la **Descripción**, que describe la brecha de umbral que provocó el evento.

Por ejemplo, el mensaje "'Perf. Valor de capacidad utilizada del 139 % en Simplicity-02 ha activado un evento DE ADVERTENCIA para identificar problemas de rendimiento potenciales en la unidad de procesamiento de datos». indica que la capacidad de rendimiento de los nodos simplicity-02 está sobreutilizada y afecta negativamente al rendimiento de los nodos.

3. En la sección **Diagnóstico del sistema**, revise los tres gráficos: Uno para la capacidad de rendimiento utilizada en el nodo, otro para la tasa media de IOPS de almacenamiento que utilizan las cargas de trabajo principales y uno para la latencia en las cargas de trabajo principales. Cuando se organizan de este modo, se pueden ver qué cargas de trabajo son la causa de la latencia en el nodo.

   Puede ver qué cargas de trabajo tienen políticas de calidad de servicio aplicadas, y cuáles no, moviendo el cursor sobre el gráfico IOPS.

4. En la sección **acciones sugeridas**, revise las sugerencias y determine qué acciones debe realizar para evitar un aumento en la latencia de la carga de trabajo.

   Si es necesario, haga clic en el botón **Ayuda** para ver más detalles sobre las acciones sugeridas que puede realizar para intentar resolver el evento de rendimiento.

Responder a los eventos de rendimiento de desequilibrio de clústeres

Unified Manager genera eventos de advertencia de desequilibrio en el clúster cuando un nodo de un clúster está funcionando con una carga mucho más alta que otros nodos y, por lo tanto, afecta potencialmente a las latencias de las cargas de trabajo. Estos eventos definidos por el sistema proporcionan la oportunidad para corregir posibles problemas de rendimiento antes de que muchas cargas de trabajo se vean afectadas por la latencia.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Unified Manager genera eventos de advertencia para incumplimiento de políticas de umbral de desequilibrio de clúster mediante la comparación del valor de capacidad de rendimiento utilizada para todos los nodos del clúster para ver si hay una diferencia de carga del 30 % entre cualquier nodo.

Estos pasos le ayudan a identificar los siguientes recursos para poder mover cargas de trabajo de alto rendimiento a un nodo más bajo utilizado:

- Los nodos del mismo clúster que se utilizan menos
- Los agregados del nuevo nodo que menos se utilizan
- Los volúmenes de mayor rendimiento en el nodo actual

Pasos

1. Abra la página de detalles **Event** para ver información sobre el evento.
2. Revise la **Descripción**, que describe la brecha de umbral que provocó el evento.

   Por ejemplo, el mensaje "'la capacidad de rendimiento utilizada contador indica una diferencia de carga del 62 % entre los nodos del clúster Dallas-1-8 y ha activado un evento de ADVERTENCIA basado en el umbral del sistema del 30 %'" indica que la capacidad de rendimiento de uno de los nodos está sobreutilizada y afecta al rendimiento del nodo.

3. Revise el texto de las **acciones sugeridas** para mover un volumen de alto rendimiento del nodo con el valor de alta capacidad de rendimiento usado a un nodo con el valor de menor capacidad de rendimiento usado.
4. Identifique los nodos con la capacidad de rendimiento más alta y mínima utilizada:
   a. En la sección **Información de evento**, haga clic en el nombre del clúster de origen.
   b. En la página **Cluster / Performance Summary**, haga clic en **Nodes** en el área **Managed Objects**.
   c. En la página de inventario **Nodes**, ordene los nodos por la columna **capacidad de rendimiento utilizada**.
   d. Identifique los nodos con la capacidad de rendimiento más alta y mínima utilizada, y escriba esos nombres.
5. Identifique el volumen que utiliza el mayor número de IOPS del nodo que tiene el valor de capacidad de rendimiento más alto utilizado:
   a. Haga clic en el nodo con el valor de capacidad de rendimiento más alto que se utiliza.
   b. En la página **Node / Performance Explorer**, seleccione **agregaciones en este nodo** en el menú **Ver y Comparar**.
   c. Haga clic en el agregado con el valor de capacidad de rendimiento más alto utilizada.
   d. En la página **aggregate / Performance Explorer**, seleccione **Volumes en este agregado** en el menú **Ver y Comparar**.
   e. Ordene los volúmenes según la columna **IOPS**, escriba el nombre del volumen con el mayor número de IOPS y el nombre del agregado en el que reside el volumen.
6. Identifique el agregado con el uso más bajo en el nodo que tiene el valor de capacidad de rendimiento más bajo utilizado:
   a. Haga clic en **almacenamiento** > **agregados** para abrir la página de inventario **agregados**.
   b. Seleccione la vista **rendimiento: Todos los agregados**.
   c. Haga clic en el botón **filtro** y agregue un filtro donde "'nodo'" sea igual al nombre del nodo con la capacidad de rendimiento más baja utilizada que escribió en el paso 4.
   d. Escriba el nombre del agregado que tenga el valor de capacidad de rendimiento más bajo utilizada.
7. Mueva el volumen del nodo sobrecargado al agregado que ha identificado como que tiene un uso bajo en el nodo nuevo.

   Puede llevar a cabo la operación de transferencia con System Manager de ONTAP, OnCommand Workflow Automation, comandos de ONTAP o una combinación de estas herramientas.

Después de unos días, compruebe si está recibiendo el mismo evento de desequilibrio de clúster de este clúster.

Analizar eventos de umbrales dinámicos de rendimiento

Los eventos generados a partir de los umbrales dinámicos indican que el tiempo de respuesta real (latencia) de una carga de trabajo es demasiado alto o demasiado bajo, en comparación con el intervalo de tiempo de respuesta esperado. La página de detalles Event se utiliza para analizar el evento de rendimiento y realizar las acciones correctivas necesarias para devolver el rendimiento a la normalidad.

Los umbrales de rendimiento dinámico no están habilitados en sistemas Cloud Volumes ONTAP, ONTAP Edge o ONTAP Select.

Identificar las cargas de trabajo de las víctimas involucradas en un evento de rendimiento dinámico

En Unified Manager, es posible identificar qué cargas de trabajo de volumen tienen la mayor desviación en tiempo de respuesta (latencia) provocada por un componente de almacenamiento en disputa. La identificación de estas cargas de trabajo le ayuda a comprender por qué las aplicaciones cliente que acceden a ellas han tenido un rendimiento más lento de lo habitual.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Debe haber eventos de rendimiento dinámicos nuevos, reconocidos o obsoletos.

La página de detalles Event muestra una lista de las cargas de trabajo definidas por el usuario y definidas por el sistema, clasificadas por la mayor desviación de la actividad o el uso del componente, o más afectadas por el evento. Los valores se basan en los picos identificados por Unified Manager cuando detectó y analizó por última vez el evento.

Pasos

1. Abra la página **Detalles del evento** para ver información sobre el evento.
2. En los gráficos latencia de carga de trabajo y actividad de carga de trabajo, seleccione **cargas de trabajo de víctimas**.
3. Pase el cursor por los gráficos para ver las principales cargas de trabajo definidas por el usuario que afectan al componente y el nombre de la carga de trabajo víctima.

Identificar las cargas de trabajo abusivas involucradas en un evento de rendimiento dinámico

En Unified Manager, es posible identificar qué cargas de trabajo tienen la mayor desviación en uso para un componente de clúster en disputa. Al identificar estas cargas de trabajo, entiende por qué algunos volúmenes del clúster tienen tiempos de respuesta lentos (latencia).

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Debe haber eventos de rendimiento dinámicos nuevos, reconocidos o obsoletos.

La página de detalles Event muestra una lista de las cargas de trabajo definidas por el usuario y definidas por el sistema con la clasificación del uso más alto del componente o más afectado por el evento. Los valores se basan en los picos identificados por Unified Manager cuando detectó y analizó por última vez el evento.

Pasos

1. Abra la página de detalles Event para ver información sobre el evento.
2. En los gráficos latencia de carga de trabajo y actividad de carga de trabajo, seleccione **carga de trabajo bully**.
3. Pase el cursor por los gráficos para ver las principales cargas de trabajo problemáticas definidas por el

usuario que afectan al componente.

Identificar cargas de trabajo de tiburón involucradas en un evento de rendimiento dinámico

En Unified Manager, es posible identificar qué cargas de trabajo tienen la mayor desviación de uso para un componente de almacenamiento en contención. La identificación de estas cargas de trabajo le ayuda a determinar si estas cargas de trabajo se deben mover a un clúster menos utilizado.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Hay un evento dinámico de rendimiento nuevo, reconocido o obsoleto.

La página de detalles Event muestra una lista de las cargas de trabajo definidas por el usuario y definidas por el sistema con la clasificación del uso más alto del componente o más afectado por el evento. Los valores se basan en los picos identificados por Unified Manager cuando detectó y analizó por última vez el evento.

Pasos

1. Abra la página **Detalles del evento** para ver información sobre el evento.
2. En los gráficos Workload Latency y Workload Activity, seleccione **Shark Workloads**.
3. Pase el cursor por los gráficos para ver las principales cargas de trabajo definidas por el usuario que afectan al componente y el nombre de la carga de trabajo de tiburón.

Análisis de eventos de rendimiento para una configuración de MetroCluster

Es posible utilizar Unified Manager para analizar un evento de rendimiento de una configuración de MetroCluster. Es posible identificar las cargas de trabajo involucradas en el evento y revisar las acciones sugeridas para resolverlo.

Los eventos de rendimiento de MetroCluster pueden deberse a cargas de trabajo *intimidator* que usan en exceso los enlaces interswitches (ISL) entre los clústeres, o debido a problemas de estado del enlace. Unified Manager supervisa cada clúster en una configuración de MetroCluster de forma independiente, sin considerar eventos de rendimiento en un clúster de partners.

Los eventos de rendimiento de ambos clústeres de la configuración de MetroCluster también se muestran en la página Unified Manager Dashboard. También puede ver las páginas Health de Unified Manager para comprobar el estado de cada clúster y ver su relación.

Analizar un evento de rendimiento dinámico en un clúster en una configuración de MetroCluster

Puede utilizar Unified Manager para analizar el clúster en una configuración de MetroCluster en la que se detectó un evento de rendimiento. Puede identificar el nombre del clúster, la hora de detección del evento y las cargas de trabajo implicadas en *intimid* y *Victim*.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Debe haber eventos de rendimiento nuevos, reconocidos o obsoletos para una configuración de

MetroCluster.

- Los dos clústeres de la configuración de MetroCluster deben supervisarse con la misma instancia de Unified Manager.

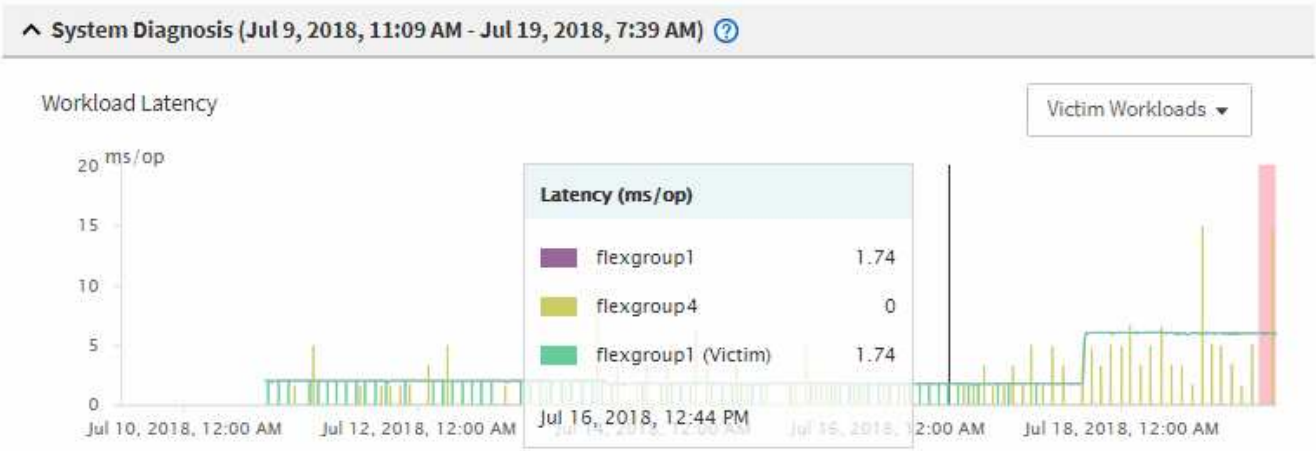
Pasos

1. Abra la página **Detalles del evento** para ver información sobre el evento.
2. Revise la descripción del evento para ver los nombres de las cargas de trabajo involucradas y el número de cargas de trabajo involucradas.

   En este ejemplo, el icono Recursos de MetroCluster es de color rojo, lo que indica que los recursos de MetroCluster están en disputa. Coloque el cursor sobre el icono para mostrar una descripción del icono.

3. Anote el nombre del clúster y la hora de detección del evento que puede utilizar para analizar los eventos de rendimiento en el clúster de partners.
4. En los gráficos, revise las cargas de trabajo *Victim* para confirmar que sus tiempos de respuesta son superiores al umbral de rendimiento.

   En este ejemplo, la carga de trabajo de la víctima se muestra en el texto de desplazamiento. Los gráficos de latencia muestran, a alto nivel, un patrón de latencia constante para las cargas de trabajo víctimas involucradas. Aunque la latencia anormal de las cargas de trabajo víctimas haya activado el evento, un patrón de latencia consistente podría indicar que las cargas de trabajo están funcionando dentro de su rango esperado, pero que un pico en la I/o aumentó la latencia y activó el evento.



   Si instaló recientemente una aplicación en un cliente que accede a estas cargas de trabajo de volumen y esa aplicación envía una gran cantidad de I/o, es posible que anticipe que aumentan las latencias. Si la latencia de las cargas de trabajo se devuelve dentro del rango esperado, el estado del evento cambia a obsoleto y permanece en este estado durante más de 30 minutos, es probable que pueda ignorar el evento. Si el evento está en curso y permanece en el estado nuevo, puede investigarlo aún más para determinar si otros problemas causaron el evento.

5. En el gráfico de rendimiento de cargas de trabajo, seleccione **Bully Workloads** para mostrar las cargas de

trabajo abusivas.

La presencia de cargas de trabajo abusivas indica que el evento podría haber sido causado por una o más cargas de trabajo en el clúster local haciendo un uso excesivo de los recursos de MetroCluster. Las cargas de trabajo abusivas tienen una alta desviación en rendimiento de escritura (MB/s).

En este gráfico, se muestra el patrón de rendimiento de escritura (MB/s) de las cargas de trabajo en el nivel superior. Es posible revisar el patrón de escritura MB/s para identificar un rendimiento anormal, que puede indicar que una carga de trabajo está haciendo un uso excesivo de los recursos de MetroCluster.

Si en este evento no hay cargas de trabajo matones, es posible que el evento haya estado causado por un problema de estado con el enlace entre los clústeres o un problema de rendimiento en el clúster de partners. Puede usar Unified Manager para comprobar el estado de ambos clústeres en una configuración de MetroCluster. También puede utilizar Unified Manager para comprobar y analizar eventos de rendimiento en el clúster de partners.

Analizar un evento de rendimiento dinámico para un clúster remoto en una configuración de MetroCluster

Es posible utilizar Unified Manager para analizar eventos dinámicos de rendimiento en un clúster remoto en una configuración de MetroCluster. El análisis le ayuda a determinar si un evento en el clúster remoto provocó un evento en su clúster de partners.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Es necesario haber analizado un evento de rendimiento en un clúster local en una configuración de MetroCluster y obtenido la hora de detección del evento.
- Debe haber comprobado el estado del clúster local y de su clúster de partners implicados en el evento de rendimiento y que ha obtenido el nombre del clúster de partners.

Pasos

1. Inicie sesión en la instancia de Unified Manager que supervisa el clúster de partners.
2. En el panel de navegación de la izquierda, haga clic en **Eventos** para mostrar la lista de eventos.
3. En el selector **intervalo de tiempo**, seleccione **última hora** y, a continuación, haga clic en **aplicar rango**.
4. En el selector **Filtering**, seleccione **Cluster** en el menú desplegable de la izquierda, escriba el nombre del clúster asociado en el campo de texto y, a continuación, haga clic en **aplicar filtro**.

   Si no existen eventos para el clúster seleccionado durante la última hora, esto indica que el clúster no ha experimentado ningún problema de rendimiento durante el momento en que se detectó el evento en su partner.

5. Si el clúster seleccionado tiene eventos detectados en la última hora, compare el tiempo de detección de eventos con la hora de detección de eventos para el evento en el clúster local.

   Si estos eventos requieren cargas de trabajo abusivas que causan contención en el componente de procesamiento de datos, uno o más de estos factores podrían haber provocado el evento en el clúster local. Puede hacer clic en el evento para analizarlo y revisar las acciones sugeridas para resolverlo en la página de detalles Event.

   Si estos eventos no requieren cargas de trabajo abusivas, no provoquen el evento de rendimiento en el clúster local.

Responder a un evento de rendimiento dinámico causado por la limitación del grupo de políticas de calidad de servicio

Puede utilizar Unified Manager para investigar un evento de rendimiento provocado por un grupo de políticas de calidad de servicio (QoS) que regula el rendimiento de la carga de trabajo (MB/s). La aceleración aumentó los tiempos de respuesta (latencia) de las cargas de trabajo de volúmenes en el grupo de políticas. Puede utilizar la información de eventos para determinar si son necesarios nuevos límites en los grupos de políticas para detener la limitación.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Debe haber eventos de rendimiento nuevos, reconocidos o obsoletos.

Pasos

1. Abra la página **Detalles del evento** para ver información sobre el evento.
2. Lea la **Descripción**, que muestra el nombre de las cargas de trabajo afectadas por la limitación.

   La descripción puede mostrar la misma carga de trabajo para la víctima y el matón, porque la limitación hace que la carga de trabajo sea víctima de sí misma.

3. Registre el nombre del volumen con una aplicación como, por ejemplo, un editor de texto.

   Puede buscar en el nombre del volumen para buscarlo más adelante.

4. En los gráficos de latencia de carga de trabajo y utilización de carga de trabajo, seleccione **Bully Workloads**.
5. Pase el cursor por los gráficos para ver las principales cargas de trabajo definidas por el usuario que están afectando al grupo de políticas.

   La carga de trabajo en la parte superior de la lista tiene la mayor desviación y causó la aceleración. La actividad es el porcentaje del límite del grupo de políticas que utiliza cada carga de trabajo.

6. En el área **acciones sugeridas**, haga clic en el botón **analizar carga de trabajo** para la carga de trabajo superior.
7. En la página Workload Analysis, establezca el gráfico latencia para ver todos los componentes del clúster y el gráfico de rendimiento para ver el desglose.

   Los gráficos de desglose se muestran en el gráfico latencia y el gráfico IOPS.

8. Compare los límites de QoS en el gráfico **latencia** para ver qué cantidad de limitación afectó a la latencia en el momento del evento.

   El grupo de políticas de calidad de servicio tiene un rendimiento máximo de 1,000 operaciones por segundo (op/s), que las cargas de trabajo que contiene no pueden superar en conjunto. En el momento del evento, las cargas de trabajo del grupo de políticas tenían un rendimiento combinado de más de 1,200 operaciones por segundo, lo que hizo que el grupo de políticas reacelerara su actividad de vuelta a los 1,000 operaciones por segundo

9. Compare los valores de **latencia de lecturas/escrituras** con los valores **lecturas/escrituras/otros**.

Ambos gráficos muestran un número elevado de solicitudes de lectura con alta latencia, pero el número de solicitudes y la cantidad de latencia para las solicitudes de escritura es bajo. Estos valores le ayudan a determinar si hay una gran cantidad de rendimiento o cantidad de operaciones que aumentaron la latencia. Puede usar estos valores al decidir poner un límite de grupo de políticas en el rendimiento o las operaciones.

10. Use el Administrador del sistema de ONTAP para aumentar el límite actual del grupo de políticas a 1,300 operaciones/s.
11. Después de un día, vuelva a Unified Manager e introduzca la carga de trabajo que registró en el paso 3 en la página **Análisis de carga de trabajo**.
12. Seleccione el gráfico de desglose de rendimiento.

    Se muestra el gráfico de lecturas/escrituras/otro.

13. En la parte superior de la página, coloque el cursor en el icono de evento de cambio ( ) para el cambio de límite del grupo de políticas.
14. Compare el gráfico **Lecturas/Escrituras/Other** con el gráfico **latencia**.

    Las solicitudes de lectura y escritura son las mismas, pero se ha detenido la limitación y se ha reducido la latencia.

Responder a un evento de rendimiento dinámico causado por un fallo del disco

Puede utilizar Unified Manager para investigar un evento de rendimiento provocado por cargas de trabajo que utilizan en exceso un agregado. También puede usar Unified Manager para comprobar el estado del agregado a fin de ver si los eventos de estado recientes detectados en el agregado contribuyeron al evento de rendimiento.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Debe haber eventos de rendimiento nuevos, reconocidos o obsoletos.

Pasos

1. Abra la página **Detalles del evento** para ver información sobre el evento.
2. Lea la **Descripción**, que describe las cargas de trabajo implicadas en el evento y el componente de clúster en disputa.

   Hay varios volúmenes victimas cuya latencia se vio afectada por el componente del clúster en disputa. El agregado, que está en medio de una reconstrucción de RAID para sustituir el disco con error por un disco de repuesto, es el componente del clúster en disputa. En componente en disputa, el icono del agregado se resalta en rojo y el nombre del agregado se muestra entre paréntesis.

3. En el gráfico de utilización de la carga de trabajo, seleccione **Bully Workloads**.
4. Pase el cursor por encima del gráfico para ver las cargas de trabajo principales problemáticas que afectan al componente.

   En la parte superior del gráfico se muestran las principales cargas de trabajo con el máximo aprovechamiento desde que se detectó el evento. Una de las principales cargas de trabajo es el estado del disco de carga de trabajo definido por el sistema, que indica una reconstrucción de RAID. Una reconstrucción es el proceso interno relacionado con la reconstrucción del agregado con el disco de

repuesto. La carga de trabajo de estado del disco, junto con otras cargas de trabajo del agregado, probablemente provocó la contención en el agregado y el evento asociado.

5. Después de confirmar que la actividad de la carga de trabajo del estado del disco provocó el evento, espere aproximadamente 30 minutos hasta que finalice la reconstrucción y que Unified Manager analice el evento y detecte si el agregado sigue en disputa.
6. Actualice **Detalles del evento**.

   Una vez finalizada la reconstrucción de RAID, compruebe que el estado sea obsoleto para indicar que se ha resuelto el evento.

7. En el gráfico de utilización de la carga de trabajo, seleccione **Bully Workloads** para ver las cargas de trabajo en el agregado por su utilización máxima.
8. En el área **acciones sugeridas**, haga clic en el botón **analizar carga de trabajo** para la carga de trabajo superior.
9. En la página **Análisis de carga de trabajo**, establezca el intervalo de tiempo para mostrar las últimas 24 horas (1 día) de los datos del volumen seleccionado.

   En la línea de tiempo del evento, un punto rojo (🔴) indica cuándo se produjo el evento de fallo del disco.

10. En el gráfico utilización nodo y agregado, oculte la línea de las estadísticas nodo para que sólo permanezca la línea agregada.
11. Compare los datos de este gráfico con los datos en el momento del evento en el gráfico **latencia**.

    En el momento del evento, el uso del agregado muestra una gran cantidad de actividad de lectura y escritura causada por los procesos de reconstrucción de RAID, que aumentó la latencia del volumen seleccionado. Unas horas después del evento, tanto las lecturas como las escrituras y la latencia han disminuido, lo que confirma que el agregado ya no está en disputa.

Responder a un evento de rendimiento dinámico causado por la toma de control de alta disponibilidad

Puede utilizar Unified Manager para investigar un evento de rendimiento causado por un alto procesamiento de datos en un nodo de clúster que se encuentra en un par de alta disponibilidad (ha). También puede usar Unified Manager para comprobar el estado de los nodos a fin de ver si algún evento de estado reciente detectado en los nodos contribuyó al evento de rendimiento.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Debe haber eventos de rendimiento nuevos, reconocidos o obsoletos.

Pasos

1. Abra la página **Detalles del evento** para ver información sobre el evento.
2. Lea la **Descripción**, que describe las cargas de trabajo implicadas en el evento y el componente de clúster en disputa.

   Hay un volumen víctima cuya latencia se vio afectada por el componente del clúster en disputa. El nodo de procesamiento de datos, que adquirió todas las cargas de trabajo del nodo asociado, es el componente de clúster en disputa. En componente en disputa, el icono procesamiento de datos se resalta en rojo y el nombre del nodo que estaba gestionando el procesamiento de datos en el momento del evento se

muestra entre paréntesis.

3. En **Descripción**, haga clic en el nombre del volumen.

   Se muestra la página Volume Performance Explorer. En la parte superior de la página, en la línea de tiempo Eventos, un icono de evento de cambio ( ) Indica la hora a la que Unified Manager detectó el inicio de la toma de control de alta disponibilidad.

4. Dirija su cursor al icono de evento de cambio para la toma de control de ha y los detalles sobre la toma de control de ha se muestran en el texto de la vista sobre el ratón.

   En el gráfico latencia, un evento indica que el volumen seleccionado superó el umbral de rendimiento debido a una alta latencia aproximadamente el mismo tiempo que la toma de control de alta disponibilidad.

5. Haga clic en **Zoom View** para mostrar el gráfico de latencia en una página nueva.
6. En el menú Ver, seleccione **componentes del clúster** para ver la latencia total por componente del clúster.
7. Dirija el cursor del ratón al icono de evento de cambio para el inicio de la toma de control de ha y compare la latencia del procesamiento de datos con la latencia total.

   En el momento de la toma de control de alta disponibilidad, se produjo un pico en el procesamiento de datos frente a la creciente demanda de carga de trabajo sobre el nodo de procesamiento de datos. El mayor uso de la CPU aumentó la latencia y activó el evento.

8. Después de corregir el nodo con errores, use System Manager de ONTAP para realizar un retorno de alta disponibilidad, que mueve las cargas de trabajo del nodo asociado al nodo fijo.
9. Una vez completada la devolución de ha, tras el siguiente descubrimiento de configuración en Unified Manager (aproximadamente 15 minutos), busque el evento y la carga de trabajo desencadenados por la toma de control de ha en la página de inventario de **Event Management**.

   El evento activado por la toma de control de alta disponibilidad ahora tiene un estado obsoleto, lo que indica que se ha resuelto el evento. La latencia en el componente de procesamiento de datos ha disminuido, lo que ha reducido la latencia total. El evento se ha resuelto en el nodo que el volumen seleccionado ahora utiliza para el procesamiento de datos.

Resolver eventos de rendimiento

Puede utilizar las acciones recomendadas para intentar resolver los eventos de rendimiento por su cuenta. Siempre se muestran las tres primeras sugerencias y las acciones de la cuarta sugerencia son específicas del tipo de evento mostrado.

Los enlaces **Ayuda para hacer esto** proporcionan información adicional para cada acción sugerida, incluidas instrucciones para realizar una acción específica. Algunas de estas acciones pueden requerir el uso de Unified Manager, System Manager de ONTAP, OnCommand Workflow Automation, comandos de la CLI de ONTAP o una combinación de estas herramientas.

Confirmación de que la latencia se encuentra dentro del rango esperado

Cuando un componente de clúster es objeto de disputa, es posible que las cargas de trabajo de volúmenes que lo utilizan hayan reducido el tiempo de respuesta (latencia). Es posible revisar la latencia de cada carga de trabajo víctima en el componente en disputa

para confirmar que la latencia real está dentro del rango esperado. También puede hacer clic en el nombre de un volumen para ver los datos históricos del volumen.

Si el evento de rendimiento está en estado obsoleto, es posible que la latencia de cada víctima involucrada en el evento haya devuelto dentro de su rango esperado.

Revise el impacto de los cambios de configuración en el rendimiento de la carga de trabajo

Los cambios de configuración en el clúster, como un disco con fallos, conmutación de alta disponibilidad o un volumen movido, pueden afectar de forma negativa al rendimiento del volumen y provocar un aumento de la latencia.

En Unified Manager, es posible revisar la página Análisis de cargas de trabajo para ver cuándo se produjo un cambio de configuración reciente y compararlo con las operaciones y la latencia (tiempo de respuesta) para ver si hubo un cambio en la actividad de la carga de trabajo del volumen seleccionada.

Las páginas de rendimiento de Unified Manager solo pueden detectar un número limitado de eventos de cambio. Las páginas de estado proporcionan alertas de otros eventos provocados por cambios de configuración. Se puede buscar el volumen en Unified Manager para ver el historial de eventos.

Opciones para mejorar el rendimiento de las cargas de trabajo desde el cliente

Puede comprobar sus cargas de trabajo de cliente, como aplicaciones o bases de datos, que envían I/o a volúmenes involucrados en un evento de rendimiento para determinar si un cambio en el cliente puede corregir el evento.

Cuando los clientes que están conectados a volúmenes en un clúster aumentan sus solicitudes de I/o, el clúster debe esforzarse más para satisfacer la demanda. Si sabe qué clientes tienen un gran número de solicitudes de I/o a un volumen determinado del clúster, puede mejorar el rendimiento del clúster ajustando el número de clientes que acceden al volumen o reduciendo la cantidad de I/o al volumen. También puede aplicar o aumentar un límite en el grupo de políticas de calidad de servicio del que pertenece el volumen.

Puede investigar los clientes y sus aplicaciones para determinar si los clientes envían más I/o de lo normal, que podría estar provocando la contención en un componente de clúster. En la página de detalles Event, la sección System Diagnosis muestra las cargas de trabajo de volumen principales que utilizan el componente en disputa. Si sabe qué cliente accede a un volumen determinado, puede ir al cliente para determinar si el hardware del cliente o una aplicación no están funcionando como se esperaba o si está realizando más trabajo de lo habitual.

En una configuración MetroCluster, las solicitudes de escritura a un volumen en un clúster local se reflejan en un volumen en el clúster remoto. Mantener el volumen de origen en el clúster local sincronizado con el volumen de destino en el clúster remoto, también se puede aumentar la demanda de ambos clústeres en la configuración de MetroCluster. Al reducir las solicitudes de escritura a estos volúmenes reflejados, los clústeres pueden realizar menos operaciones de sincronización, lo que reduce el impacto en el rendimiento de otras cargas de trabajo.

Compruebe si existen problemas con los clientes o la red

Cuando los clientes que están conectados a volúmenes en un clúster aumentan sus solicitudes de I/o, el clúster debe esforzarse más para satisfacer la demanda. La mayor demanda del clúster puede poner un componente en contención, aumentar la latencia de

las cargas de trabajo que lo utilizan y activar un evento en Unified Manager.

En la página de detalles Event, la sección System Diagnosis muestra las cargas de trabajo de volumen principales que utilizan el componente en disputa. Si sabe qué cliente accede a un volumen determinado, puede ir al cliente para determinar si el hardware del cliente o una aplicación no están funcionando como se esperaba o si está realizando más trabajo de lo habitual. Es posible que deba ponerse en contacto con el administrador de clientes o con el proveedor de aplicaciones para obtener ayuda.

Puede comprobar su infraestructura de red para determinar si hay problemas de hardware, cuellos de botella o cargas de trabajo en la competencia que puedan haber provocado que las solicitudes de I/o entre el clúster y los clientes conectados tengan un rendimiento más lento de lo esperado. Es posible que deba ponerse en contacto con el administrador de red para obtener ayuda.

Verifique si otros volúmenes del grupo de políticas de calidad de servicio tienen una actividad inusualmente alta

Es posible revisar las cargas de trabajo del grupo de políticas de calidad de servicio (QoS) con el cambio más alto en la actividad para determinar si más de una carga de trabajo provocó el evento. También se puede ver si otras cargas de trabajo siguen superando el límite de rendimiento establecido o si vuelven a estar dentro del rango esperado de actividad.

En la página de detalles Event, en la sección System Diagnosis, se pueden ordenar las cargas de trabajo por desviación máxima en la actividad para mostrar las cargas de trabajo con el mayor cambio en la actividad de la parte superior de la tabla. Estas cargas de trabajo podrían ser las "'verdugos'" cuya actividad superara el límite establecido y podría haber causado el evento.

Es posible ir a la página Análisis de cargas de trabajo de cada carga de trabajo de volumen para revisar la actividad de IOPS. Si la carga de trabajo tiene periodos de actividad de operaciones muy alta, es posible que haya contribuido al evento. Es posible cambiar la configuración del grupo de políticas para la carga de trabajo o mover la carga de trabajo a otro grupo.

Puede usar los comandos de la CLI de ONTAP System Manager o de ONTAP para gestionar los grupos de políticas de la siguiente manera:

- Crear un grupo de políticas.
- Añada o quite cargas de trabajo de un grupo de políticas.
- Mover una carga de trabajo entre grupos de políticas.
- Cambiar el límite de rendimiento de un grupo de políticas.

Mover interfaces lógicas (LIF)

Mover las interfaces lógicas (LIF) a un puerto menos ocupado puede ayudar a mejorar el equilibrio de carga, ayudar con las operaciones de mantenimiento y el ajuste del rendimiento, y reducir el acceso indirecto.

El acceso indirecto puede reducir la eficiencia del sistema. Se produce cuando una carga de trabajo de un volumen utiliza diferentes nodos para el procesamiento de red y el procesamiento de datos. Para reducir el acceso indirecto, puede reorganizar las LIF, lo que implica mover las LIF para utilizar el mismo nodo para el procesamiento de la red y el procesamiento de datos. Puede configurar el equilibrio de carga para que ONTAP mueva automáticamente los LIF ocupados a un puerto diferente o puede mover una LIF manualmente.

Beneficios	Consideraciones
• Mejore el equilibrio de carga. • Reduzca el acceso indirecto.	Al mover una LIF conectada a recursos compartidos CIFS, los clientes que acceden a los recursos compartidos CIFS están desconectados. Cualquier solicitud de lectura o escritura a los recursos compartidos CIFS se interrumpe.

Es posible utilizar los comandos de la ONTAP para configurar el equilibrio de carga. Para obtener más información, consulte la documentación de redes de ONTAP.

Utilice System Manager de ONTAP y los comandos de la CLI de ONTAP para mover las LIF manualmente.

Ejecute operaciones de eficiencia del almacenamiento en momentos de menor actividad

Puede modificar la política o la programación que maneja las operaciones de eficiencia del almacenamiento para ejecutarse cuando las cargas de trabajo de los volúmenes afectados están menos ocupadas.

Las operaciones de eficiencia del almacenamiento pueden utilizar una gran cantidad de recursos de CPU del clúster y convertirse en un problema para los volúmenes en los que se ejecutan las operaciones. Si los volúmenes víctimas tienen una actividad alta al mismo tiempo que se ejecutan las operaciones de eficiencia del almacenamiento, su latencia puede aumentar y desencadenar un evento.

En la página de detalles Event, la sección System Diagnosis muestra las cargas de trabajo en el grupo de políticas QoS por desviación máxima en la actividad para identificar las cargas de trabajo problemáticas. Si aparece «eficiencia del almacenamiento» cerca de la parte superior de la tabla, estas operaciones intimidan a las cargas de trabajo víctimas. Al modificar la política o la programación de eficiencia para que se ejecute cuando estas cargas de trabajo estén menos ocupadas, puede impedir que las operaciones de eficiencia del almacenamiento provoquen la contención en un clúster.

Puede usar System Manager de ONTAP para gestionar políticas de eficiencia. Puede usar los comandos de ONTAP para gestionar las políticas y las programaciones de eficiencia.

Qué es la eficiencia del almacenamiento

La eficiencia del almacenamiento le permite almacenar la cantidad máxima de datos al menor coste y alberga un rápido crecimiento de datos mientras consume menos espacio. La estrategia de eficiencia del almacenamiento de NetApp se basa en la virtualización del almacenamiento y el almacenamiento unificado que proporciona su sistema operativo ONTAP principal y el sistema de archivos WAFL (Write Anywhere File Layout).

La eficiencia del almacenamiento incluye tecnologías como thin provisioning, copia Snapshot, deduplicación, compresión de datos, FlexClone, Thin replication con SnapVault y SnapMirror de volúmenes, RAID-DP, Flash Cache, agregados de Flash Pool y agregados habilitados para FabricPool que ayudan a aumentar la utilización del almacenamiento y a reducir los costes de almacenamiento.

La arquitectura de almacenamiento unificado le permite consolidar de forma eficaz una red de área de

almacenamiento (SAN), un almacenamiento conectado a la red (NAS) y un almacenamiento secundario en una única plataforma.

Las unidades de disco de alta densidad, como las unidades de conexión de tecnología avanzada en serie (SATA) configuradas en el agregado de Flash Pool o con la tecnología Flash Cache y RAID-DP, aumentan la eficiencia sin que ello afecte al rendimiento ni a la flexibilidad.

Un agregado habilitado para FabricPool incluye todo un agregado de SSD o un agregado de HDD (a partir de ONTAP 9.8) como nivel de rendimiento local y un almacén de objetos que especifique como nivel de cloud. La configuración de FabricPool le ayuda a gestionar qué nivel de almacenamiento (el nivel local o el nivel cloud) deben almacenarse en función de si se accede a los datos con frecuencia.

Las tecnologías como thin provisioning, copia Snapshot, deduplicación, compresión de datos, thin replication con SnapVault y SnapMirror para volúmenes y FlexClone ofrecen un mejor ahorro. Puede usar estas tecnologías por separado o juntas para lograr la máxima eficiencia del almacenamiento.

Añada discos y reasigne datos

Puede añadir discos a un agregado para aumentar la capacidad de almacenamiento y el rendimiento de dicho agregado. Tras agregar los discos, verá una mejora en el rendimiento de lectura únicamente tras reasignar los datos en los discos que haya agregado.

Puede utilizar estas instrucciones cuando Unified Manager haya recibido eventos de agregado activados por umbrales dinámicos o por umbrales de rendimiento definidos por el sistema:

- Cuando haya recibido un evento de umbral dinámico, en la página de detalles Event, el icono del componente del clúster que representa el agregado en disputa se resalta en rojo.

  Debajo del icono, entre paréntesis, es el nombre del agregado, que identifica el agregado al que se pueden añadir discos.

- Cuando ha recibido un evento de umbral definido por el sistema, en la página de detalles Event, el texto de descripción del evento enumera el nombre del agregado que tiene el problema.

  Puede añadir discos y reasignar datos en este agregado.

Los discos que agregue al agregado ya deben existir en el clúster. Si el clúster no tiene discos adicionales disponibles, puede que tenga que ponerse en contacto con su administrador o adquirir más discos. Puede usar System Manager o los comandos de la ONTAP de ONTAP para añadir discos a un agregado.

Debe reasignar los datos cuando se utilizan únicamente agregados de HDD y Flash Pool. No reasignar datos en agregados de SSD o FabricPool.

Cómo habilitar Flash Cache en un nodo puede mejorar el rendimiento de la carga de trabajo

Puede mejorar el rendimiento de la carga de trabajo activando la caché inteligente de datos Flash Cache™ en cada nodo del clúster.

Un módulo Flash Cache o un módulo de memoria basado en PCIe Performance Acceleration Module optimizan el rendimiento de cargas de trabajo de lectura aleatoria intensiva al funcionar como una caché de

lectura externa inteligente. Este hardware funciona conjuntamente con el componente de software de caché externa WAFL de ONTAP.

En Unified Manager, en la página de detalles Event, el icono del componente del clúster que representa el agregado en disputa se resalta en rojo. Debajo del icono, entre paréntesis, se encuentra el nombre del agregado, que identifica el agregado. Puede habilitar Flash Cache en el nodo en el que reside el agregado.

Puede usar System Manager de ONTAP o los comandos de ONTAP para ver si Flash Cache está instalado o habilitado y para habilitarla si todavía no está habilitado. El siguiente comando indica si Flash Cache está habilitado en un nodo específico: **`cluster::> run local options flexscale.enable`**

Para obtener más información sobre Flash Cache y los requisitos para su uso, consulte el siguiente informe técnico:

"Informe técnico 3832: Guía de prácticas recomendadas de Flash Cache"

Cómo habilitar Flash Pool en un agregado de almacenamiento puede mejorar el rendimiento de la carga de trabajo

Puede mejorar el rendimiento de la carga de trabajo al habilitar la función Flash Pool en un agregado. Un Flash Pool es un agregado que incorpora tanto HDD como SSD. Los HDD se utilizan para almacenamiento principal y las SSD proporcionan una caché de lectura y escritura de alto rendimiento que mejora el rendimiento del agregado.

En Unified Manager, la página de detalles Event muestra el nombre del agregado en disputa. Puede usar System Manager de ONTAP o los comandos de la ONTAP para ver si Flash Pool está habilitado para un agregado. Si tiene instalados SSD, puede usar la interfaz de línea de comandos para habilitarla. Si tiene discos SSD instalados, puede ejecutar el siguiente comando en el agregado para ver si Flash Pool está habilitado: **`cluster::> storage aggregate show -aggregate aggr_name -field hybrid-enabled`**

En este comando, *`aggr_name`* es el nombre del agregado, como el agregado en disputa.

Para obtener más información sobre Flash Pool y los requisitos para su uso, consulte la *Guía de gestión de almacenamiento físico de Clustered Data ONTAP*.

Comprobación del estado de la configuración de MetroCluster

Puede usar Unified Manager para revisar el estado de los clústeres en una configuración de MetroCluster por IP o FC. El estado y los eventos le ayudan a determinar si existen problemas de hardware o software que podrían afectar al rendimiento de sus cargas de trabajo.

Si configura Unified Manager para que envíe alertas por correo electrónico, puede comprobar su correo electrónico por si tiene problemas de estado en el clúster local o remoto que puedan haber contribuido a un evento de rendimiento. En la GUI de Unified Manager, puede seleccionar **Gestión de eventos** para ver una lista de eventos actuales y, a continuación, utilizar los filtros para mostrar únicamente eventos de configuración de MetroCluster.

Para obtener más información, consulte "Comprobar el estado de los clústeres en una configuración de MetroCluster"

Verificación de la configuración de MetroCluster

Puede evitar problemas de rendimiento para cargas de trabajo duplicadas en una configuración de MetroCluster over FC e IP, garantizando que la configuración de MetroCluster se configure correctamente. También puede mejorar el rendimiento de la carga de trabajo cambiando la configuración o actualizando componentes de software o hardware.

Consulte "Documentación de MetroCluster" Para obtener las instrucciones de configurar los clústeres en la configuración de MetroCluster, incluidos los switches Fibre Channel (FC), los cables y los enlaces entre switches (ISL). También es útil configurar el software MetroCluster para que los clústeres local y remoto puedan comunicarse con los datos de volúmenes reflejados. Para obtener información específica sobre la configuración de MetroCluster over IP, consulte "Instale una configuración de IP de MetroCluster".

Es posible comparar la configuración de MetroCluster con los requisitos en "Documentación de MetroCluster" Para determinar si cambiar o actualizar componentes de su configuración de MetroCluster puede mejorar el rendimiento de la carga de trabajo. Esta comparación puede ayudarle a responder a las siguientes preguntas:

- ¿Las controladoras son adecuadas para sus cargas de trabajo?
- ¿Necesita actualizar sus paquetes ISL a un ancho de banda mayor para poder gestionar más rendimiento?
- ¿Puede ajustar los créditos de búfer a búfer (BBC) en los switches para aumentar el ancho de banda?
- Si sus cargas de trabajo tienen un rendimiento de escritura elevado para almacenamiento de unidades de estado sólido (SSD), ¿necesita actualizar sus puentes de FC a SAS para adaptarse al rendimiento?

Información relacionada

- Para obtener información acerca de cómo reemplazar o actualizar componentes de MetroCluster, consulte "Documentación de MetroCluster".
- Para obtener información sobre la actualización de las controladoras, consulte "Actualización de controladoras en una configuración MetroCluster FC mediante conmutación de sitios y conmutación de estado" y.. "Actualización de controladoras en una configuración IP de MetroCluster mediante conmutación de sitios y conmutación de estado"

Mover las cargas de trabajo a otro agregado

Puede usar Unified Manager para ayudar a identificar un agregado con un menor nivel de actividad que el agregado en el que residen actualmente las cargas de trabajo y, a continuación, puede mover volúmenes o LUN seleccionados a ese agregado. Mover las cargas de trabajo de alto rendimiento a un agregado menos ocupado o a un agregado con almacenamiento flash habilitado permite que la carga de trabajo tenga un rendimiento más eficiente.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Debe haber registrado el nombre del agregado que está teniendo un problema de rendimiento.
- Debe haber registrado la fecha y la hora en que el agregado recibió el evento.
- Unified Manager debe haber recopilado y analizado un mes o más de datos de rendimiento.

Estos pasos le ayudan a identificar los siguientes recursos para mover cargas de trabajo de alto rendimiento a un agregado más bajo utilizado:

- Los agregados del mismo clúster que menos se utilizan
- Los volúmenes de mayor rendimiento en el agregado actual

Pasos

1. Identifique el agregado del clúster que es el más utilizado:
   a. En la página de detalles **Event**, haga clic en el nombre del clúster en el que reside el agregado.

      Los detalles del clúster se muestran en la página Performance/Cluster Landing.

   b. En la página **Resumen**, haga clic en **agregados** en el panel **objetos gestionados**.

      Se muestra la lista de agregados de este clúster.

   c. Haga clic en la columna **utilización** para ordenar los agregados por menos utilizados.

      También puede identificar aquellos agregados que tengan la capacidad libre * más grande. De este modo, se proporciona una lista de agregados potenciales a los que se pueden mover cargas de trabajo.

   d. Escriba el nombre del agregado al que desea mover las cargas de trabajo.
2. Identifique los volúmenes de alto rendimiento del agregado que ha recibido el evento:
   a. Haga clic en el agregado que está teniendo un problema de rendimiento.

      Los detalles del agregado se muestran en la página Performance/Aggregate Explorer.

   b. En el selector **intervalo de tiempo**, seleccione **últimos 30 días** y, a continuación, haga clic en **aplicar rango**.

      Esto permite ver un período del historial de rendimiento más largo que las 72 horas predeterminadas. Desea mover un volumen que utilice muchos recursos de forma coherente, no solo en las últimas 72 horas.

   c. En el control **Ver y Comparar**, seleccione **volúmenes en este agregado**.

      Se muestra una lista de los volúmenes FlexVol y los volúmenes que forman FlexGroup en este agregado.

   d. Ordene los volúmenes en los MB/s más altos y, luego, en la tasa de IOPS más alta, para ver los volúmenes con el rendimiento más alto.
   e. Escriba los nombres de los volúmenes que desea mover a otro agregado.
3. Mueva los volúmenes de alto rendimiento al agregado que ha identificado como con un bajo aprovechamiento.

   Puede llevar a cabo la operación de transferencia con System Manager de ONTAP, OnCommand Workflow Automation, comandos de ONTAP o una combinación de estas herramientas.

Tras unos días, compruebe si está recibiendo el mismo tipo de eventos de este nodo o agregado.

Mover las cargas de trabajo a un nodo diferente

Puede usar Unified Manager para ayudar a identificar un agregado en un nodo diferente que esté menos ocupado que el nodo en el que se están ejecutando las cargas de trabajo en ese momento y, a continuación, puede mover los volúmenes seleccionados a ese agregado. Mover cargas de trabajo de alto rendimiento a un agregado en un nodo menos ocupado permite que las cargas de trabajo de ambos nodos tengan un rendimiento más eficiente.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Debe haber registrado el nombre del nodo que está teniendo actualmente un problema de rendimiento.
- Debe haber registrado la fecha y la hora en que el nodo recibió el evento de rendimiento.
- Unified Manager debe haber recopilado y analizado los datos de rendimiento por un mes o más.

Este procedimiento le ayuda a identificar los siguientes recursos para poder mover cargas de trabajo de alto rendimiento a un nodo más bajo utilizado:

- Los nodos en el mismo clúster que tienen la mayor capacidad de rendimiento libre
- Los agregados del nodo nuevo que tienen la mayor capacidad de rendimiento libre
- Los volúmenes de mayor rendimiento en el nodo actual

Pasos

1. Identifique un nodo del clúster que tenga la mayor capacidad de rendimiento libre:
   a. En la página **Detalles de evento**, haga clic en el nombre del clúster en el que reside el nodo.

      Los detalles del clúster se muestran en la página Performance/Cluster Landing.

   b. En la ficha **Resumen**, haga clic en **nodos** en el panel **objetos gestionados**.

      Se muestra la lista de nodos de este clúster.

   c. Haga clic en la columna **capacidad de rendimiento utilizada** para ordenar los nodos por porcentaje mínimo utilizado.

      Proporciona una lista de nodos potenciales a los que se podría mover cargas de trabajo.

   d. Escriba el nombre del nodo al que desea mover las cargas de trabajo.
2. Identifique un agregado en el nuevo nodo que sea lo menos utilizado:
   a. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **agregados** y seleccione **rendimiento** > **todos los agregados** en el menú Ver.

      Se muestra la vista rendimiento: Todos los agregados.

   b. Haga clic en **filtrado**, seleccione **nodo** en el menú desplegable de la izquierda, escriba el nombre del nodo en el campo de texto y, a continuación, haga clic en **aplicar filtro**.

      La vista rendimiento: Todos los agregados se vuelve a mostrar con la lista de agregados disponibles en este nodo.

c. Haga clic en la columna **capacidad de rendimiento utilizada** para ordenar los agregados por menos utilizados.

   De este modo, se proporciona una lista de agregados potenciales a los que se pueden mover cargas de trabajo.

d. Escriba el nombre del agregado al que desea mover las cargas de trabajo.

3. Identifique las cargas de trabajo de alto rendimiento del nodo que recibió el evento:
   a. Vuelva a la página **Detalles del evento** del evento.
   b. En el campo **volúmenes afectados**, haga clic en el enlace del número de volúmenes.

      El rendimiento: Toda la vista de volúmenes se muestra con una lista filtrada de volúmenes en ese nodo.

   c. Haga clic en la columna **capacidad total** para ordenar los volúmenes por el espacio asignado más grande.

      Proporciona una lista de los volúmenes potenciales que puede querer mover.

   d. Escriba los nombres de los volúmenes que desea mover y los nombres de los agregados actuales en los que residen.
4. Mueva los volúmenes a los agregados que ha identificado como con la mayor capacidad de rendimiento libre del nuevo nodo.

   Puede llevar a cabo la operación de transferencia con System Manager de ONTAP, OnCommand Workflow Automation, comandos de ONTAP o una combinación de estas herramientas.

Tras unos días, puede comprobar si está recibiendo el mismo tipo de eventos de este nodo o agregado.

Mover las cargas de trabajo a un agregado en un nodo diferente

Puede usar Unified Manager para ayudar a identificar un agregado en un nodo diferente menos ocupado que el nodo en el que se están ejecutando las cargas de trabajo y, a continuación, puede mover los volúmenes seleccionados a ese agregado. Mover cargas de trabajo de alto rendimiento a un agregado en un nodo menos ocupado permite que las cargas de trabajo de ambos nodos funcionen de forma más eficiente.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Debe haber registrado el nombre del nodo que está teniendo actualmente un problema de rendimiento.
- Debe haber registrado la fecha y la hora en que el nodo recibió el evento de rendimiento.
- Unified Manager debe haber recopilado y analizado un mes o más de datos de rendimiento.

Estos pasos le ayudan a identificar los siguientes recursos para poder mover cargas de trabajo de alto rendimiento a un nodo más bajo utilizado:

- Los nodos del mismo clúster que se utilizan menos
- Los agregados del nuevo nodo que menos se utilizan

- Los volúmenes de mayor rendimiento en el nodo actual

Pasos

1. Identifique un nodo del clúster que sea el que menos se utilice:
   a. En la página de detalles **Event**, haga clic en el nombre del clúster en el que reside el nodo.

      Los detalles del clúster se muestran en la página Performance/Cluster Landing.

   b. En la página **Resumen**, haga clic en **nodos** en el panel **objetos gestionados**.

      Se muestra la lista de nodos de este clúster.

   c. Haga clic en la columna **utilización** para ordenar los nodos por menos utilizados.

      También puede identificar aquellos nodos que tengan la capacidad libre * más grande. Proporciona una lista de nodos potenciales a los que se podría mover cargas de trabajo.

   d. Escriba el nombre del nodo al que desea mover las cargas de trabajo.
2. Identifique un agregado en el nuevo nodo que sea lo menos utilizado:
   a. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **agregados** y seleccione **rendimiento** > **todos los agregados** en el menú Ver.

      Se muestra la vista rendimiento: Todos los agregados.

   b. Haga clic en **filtrado**, seleccione **nodo** en el menú desplegable de la izquierda, escriba el nombre del nodo en el campo de texto y, a continuación, haga clic en **aplicar filtro**.

      La vista rendimiento: Todos los agregados se vuelve a mostrar con la lista de agregados disponibles en este nodo.

   c. Haga clic en la columna **utilización** para ordenar los agregados por menos utilizados.

      También puede identificar aquellos agregados que tengan la capacidad libre * más grande. De este modo, se proporciona una lista de agregados potenciales a los que se pueden mover cargas de trabajo.

   d. Escriba el nombre del agregado al que desea mover las cargas de trabajo.
3. Identifique las cargas de trabajo de alto rendimiento del nodo que recibió el evento:
   a. Vuelva a la página de detalles **evento** del evento.
   b. En el campo **volúmenes afectados**, haga clic en el enlace del número de volúmenes.

      El rendimiento: Toda la vista de volúmenes se muestra con una lista filtrada de volúmenes en ese nodo.

   c. Haga clic en la columna **capacidad total** para ordenar los volúmenes por el espacio asignado más grande.

      Proporciona una lista de los volúmenes potenciales que puede querer mover.

   d. Escriba los nombres de los volúmenes que desea mover y los nombres de los agregados actuales en los que residen.
4. Mueva los volúmenes a los agregados que ha identificado como si tuviera una utilización baja en el nodo

nuevo.

Puede llevar a cabo la operación de transferencia con System Manager de ONTAP, OnCommand Workflow Automation, comandos de ONTAP o una combinación de estas herramientas.

Tras unos días, compruebe si está recibiendo el mismo tipo de eventos de este nodo o agregado.

Mover cargas de trabajo a un nodo en un par de alta disponibilidad diferente

Puede usar Unified Manager para ayudar a identificar un agregado en un nodo en una pareja de alta disponibilidad (ha) diferente con más capacidad de rendimiento libre que la pareja de alta disponibilidad en la que se ejecutan actualmente las cargas de trabajo. A continuación, puede mover los volúmenes seleccionados a agregados en la nueva pareja de ha.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Su clúster debe estar formado por un mínimo de dos parejas de alta disponibilidad

  No puede utilizar este proceso de corrección si solo tiene un par de alta disponibilidad en su clúster.
- Debe haber registrado los nombres de los dos nodos de la pareja de ha que están teniendo actualmente un problema de rendimiento.
- Debe haber registrado la fecha y la hora en que los nodos recibieron el evento de rendimiento.
- Unified Manager debe haber recopilado y analizado los datos de rendimiento por un mes o más.

Mover cargas de trabajo de alto rendimiento a un agregado en un nodo con una capacidad de rendimiento más libre permite que las cargas de trabajo de ambos nodos tengan un rendimiento más eficiente. Este procedimiento le ayuda a identificar los siguientes recursos para que pueda mover cargas de trabajo de alto rendimiento a un nodo con más capacidad de rendimiento libre en un par de alta disponibilidad diferente:

- Los nodos de una pareja de alta disponibilidad diferente en el mismo clúster que tienen la mayor capacidad de rendimiento libre
- Los agregados de los nuevos nodos con la mayor capacidad de rendimiento libre
- Los volúmenes de mayor rendimiento en los nodos actuales

Pasos

1. Identifique los nodos que forman parte de una pareja de alta disponibilidad diferente en el mismo clúster:
   a. En la página **Detalles de evento**, haga clic en el nombre del clúster en el que residen los nodos.

      Los detalles del clúster se muestran en la página Performance/Cluster Landing.

   b. En la página **Resumen**, haga clic en **nodos** en el panel **objetos gestionados**.

      La lista de nodos de este clúster se muestra en la vista rendimiento: All Nodes.

   c. Escriba los nombres de los nodos que están en parejas de ha diferentes de la pareja de ha que tiene actualmente un problema de rendimiento.
2. Identifique un nodo en la nueva pareja de alta disponibilidad que tenga la mayor capacidad de rendimiento

libre:

a. En la vista **rendimiento: Todos los nodos**, haga clic en la columna **capacidad de rendimiento utilizada** para ordenar los nodos por el porcentaje mínimo utilizado.

   Proporciona una lista de nodos potenciales a los que se podría mover cargas de trabajo.

b. Escriba el nombre del nodo en un par de alta disponibilidad diferente al que desea mover las cargas de trabajo.

3. Identifique un agregado en el nodo nuevo que tenga la mayor capacidad de rendimiento libre:
   a. En la vista **rendimiento: Todos los nodos**, haga clic en el nodo.

      Los detalles del nodo se muestran en la página Performance/Node Explorer.

   b. En el menú **Ver y comparar**, seleccione **agregados en este nodo**.

      Los agregados de este nodo se muestran en la cuadrícula.

   c. Haga clic en la columna **capacidad de rendimiento utilizada** para ordenar los agregados por menos utilizados.

      De este modo, se proporciona una lista de agregados potenciales a los que se pueden mover cargas de trabajo.

   d. Escriba el nombre del agregado al que desea mover las cargas de trabajo.
4. Identifique las cargas de trabajo de alto rendimiento desde los nodos que recibieron el evento:
   a. Vuelva a la página de detalles **evento** del evento.
   b. En el campo **volúmenes afectados**, haga clic en el enlace del número de volúmenes del primer nodo.

      El rendimiento: Toda la vista de volúmenes se muestra con una lista filtrada de volúmenes en ese nodo.

   c. Haga clic en la columna **capacidad total** para ordenar los volúmenes por el espacio asignado más grande.

      Proporciona una lista de los volúmenes potenciales que se pueden mover.

   d. Escriba los nombres de los volúmenes que desea mover y los nombres de los agregados actuales en los que residen.
   e. Realice los pasos 4c y 4d para el segundo nodo que formaba parte de este evento para identificar los volúmenes posibles que desea mover también desde ese nodo.
5. Mueva los volúmenes a los agregados que ha identificado como con la mayor capacidad de rendimiento libre del nuevo nodo.

   Puede llevar a cabo la operación de transferencia con System Manager de ONTAP, OnCommand Workflow Automation, comandos de ONTAP o una combinación de estas herramientas.

Tras unos días, puede comprobar si está recibiendo el mismo tipo de eventos de este nodo o agregado.

Mover cargas de trabajo a otro nodo en un par de alta disponibilidad diferente

Puede usar Unified Manager para ayudar a identificar un agregado en un nodo en un par

de alta disponibilidad diferente que está menos ocupado que el par de alta disponibilidad en el que se están ejecutando las cargas de trabajo en ese momento. A continuación, puede mover los volúmenes seleccionados a agregados en la nueva pareja de ha. Mover cargas de trabajo de alto rendimiento a un agregado en un nodo menos ocupado permite que las cargas de trabajo de ambos nodos funcionen de forma más eficiente.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Su clúster debe constar de un mínimo de dos parejas de alta disponibilidad. No puede utilizar este proceso de corrección si solo tiene un par de alta disponibilidad en su clúster.
- Debe haber registrado los nombres de los dos nodos de la pareja de ha que están teniendo el problema de rendimiento.
- Debe haber registrado la fecha y la hora en que los nodos recibieron el evento de rendimiento.
- Unified Manager debe haber recopilado y analizado un mes o más de datos de rendimiento.

Estos pasos le ayudan a identificar los siguientes recursos para poder mover cargas de trabajo de alto rendimiento a un nodo más bajo utilizado en un par de alta disponibilidad diferente:

- Los nodos de una pareja de alta disponibilidad diferente en el mismo clúster que se usan menos
- Los agregados de los nuevos nodos que menos se utilizan
- Los volúmenes de mayor rendimiento en los nodos actuales

Pasos

1. Identifique los nodos que forman parte de una pareja de alta disponibilidad diferente en el mismo clúster:
   a. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **clústeres** y seleccione **rendimiento** > **todos los clústeres** en el menú Ver.

      Se muestra la vista Performance: All Clusters.

   b. Haga clic en el número del campo **recuento de nodos** del clúster actual.

      El rendimiento: Se muestra la vista todos los nodos.

   c. Escriba los nombres de los nodos que están en parejas de ha diferentes de la pareja de ha que tiene actualmente el problema de rendimiento.
2. Identifique un nodo del nuevo par de alta disponibilidad que sea lo menos utilizado:
   a. Haga clic en la columna **utilización** para ordenar los nodos por menos utilizados.

      También puede identificar aquellos nodos que tengan la capacidad libre * más grande. Proporciona una lista de nodos potenciales a los que se podría mover cargas de trabajo.

   b. Escriba el nombre del nodo al que desea mover las cargas de trabajo.
3. Identifique un agregado en el nuevo nodo que sea lo menos utilizado:
   a. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **agregados** y seleccione **rendimiento** > **todos los agregados** en el menú Ver.

      Se muestra la vista rendimiento: Todos los agregados.

b. Haga clic en **filtrado**, seleccione **nodo** en el menú desplegable de la izquierda, escriba el nombre del nodo en el campo de texto y, a continuación, haga clic en **aplicar filtro**.

   La vista rendimiento: Todos los agregados se vuelve a mostrar con la lista de agregados disponibles en este nodo.

c. Haga clic en la columna **utilización** para ordenar los agregados por menos utilizados.

   También puede identificar aquellos agregados que tengan la capacidad libre * más grande. De este modo, se proporciona una lista de agregados potenciales a los que se pueden mover cargas de trabajo.

d. Escriba el nombre del agregado al que desea mover las cargas de trabajo.

4. Identifique las cargas de trabajo de alto rendimiento desde los nodos que recibieron el evento:
   a. Vuelva a la página de detalles **evento** del evento.
   b. En el campo **volúmenes afectados**, haga clic en el enlace del número de volúmenes del primer nodo.

      El rendimiento: Toda la vista de volúmenes se muestra con una lista filtrada de volúmenes en ese nodo.

   c. Haga clic en la columna **capacidad total** para ordenar los volúmenes por el espacio asignado más grande.

      Proporciona una lista de los volúmenes potenciales que se pueden mover.

   d. Escriba los nombres de los volúmenes que desea mover y los nombres de los agregados actuales en los que residen.
   e. Realice los pasos 4c y 4d para el segundo nodo que formaba parte de este evento para identificar los volúmenes posibles que desea mover también desde ese nodo.
5. Mueva los volúmenes a los agregados que ha identificado como si tuviera una utilización baja en el nodo nuevo.

   Puede llevar a cabo la operación de transferencia con System Manager de ONTAP, OnCommand Workflow Automation, comandos de ONTAP o una combinación de estas herramientas.

Tras unos días, compruebe si está recibiendo el mismo tipo de eventos de este nodo o agregado.

Utilice la configuración de la política de calidad de servicio para priorizar el trabajo de este nodo

Es posible establecer un límite en un grupo de políticas de calidad de servicio para controlar las operaciones de I/o por segundo (IOPS) o el límite de rendimiento de Mbps para las cargas de trabajo en las que contenga. Si las cargas de trabajo se encuentran en un grupo de políticas sin un límite establecido, como el grupo de políticas predeterminado, o el límite establecido no cumple con sus necesidades, puede aumentar el límite establecido o mover las cargas de trabajo a un grupo de políticas nuevo o existente que tenga el límite deseado.

Si un evento de rendimiento de un nodo se debe a que las cargas de trabajo utilizan excesivamente los recursos de nodo, la descripción del evento de la página de detalles Event muestra un enlace a la lista de

volúmenes implicados. En la página Performance/Volumes, es posible ordenar los volúmenes afectados por IOPS y Mbps para ver qué cargas de trabajo tienen el uso más alto que podría haber contribuido al evento.

Al asignar los volúmenes que están utilizando en exceso los recursos del nodo a una configuración de grupo de políticas más restrictiva, el grupo de políticas limita las cargas de trabajo a restringir su actividad, lo que puede reducir el uso de los recursos en ese nodo.

Puede usar los comandos de ONTAP System Manager o ONTAP para gestionar los grupos de políticas, incluidas las siguientes tareas:

- Crear un grupo de políticas
- Agregar o eliminar cargas de trabajo en un grupo de políticas
- Mover una carga de trabajo entre grupos de políticas
- Cambiar el límite de rendimiento de un grupo de políticas

Quite los volúmenes y las LUN inactivos

Cuando el espacio libre del agregado se haya identificado como un problema, puede buscar volúmenes y LUN sin usar y eliminarlos del agregado. Esto puede ayudar a solucionar el problema del poco espacio en disco.

Si un evento de rendimiento en un agregado está provocado por un bajo espacio en disco, puede determinar qué volúmenes y LUN ya no se están utilizando.

Para identificar volúmenes no utilizados:

- En la página Detalles de eventos, el campo **recuento de objetos afectados** proporciona un vínculo que muestra la lista de volúmenes afectados.

  Haga clic en el enlace para mostrar los volúmenes en la vista rendimiento: Todos los volúmenes. Desde allí puede ordenar los volúmenes afectados por **IOPS** para ver qué volúmenes no han estado activos.

Para identificar las LUN no utilizadas:

1. En la página de detalles Event, escriba el nombre del agregado en el que se ha producido el evento.
2. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **LUN** y seleccione **rendimiento** > **todas las LUN** en el menú Ver.
3. Haga clic en **filtrado**, seleccione **agregado** en el menú desplegable de la izquierda, escriba el nombre del agregado en el campo de texto y, a continuación, haga clic en **aplicar filtro**.
4. Ordene la lista resultante de LUN afectadas por **IOPS** para ver las LUN que no están activas.

Después de identificar los volúmenes y las LUN no utilizados, puede usar System Manager de ONTAP o los comandos de la ONTAP para eliminar esos objetos.

Añada discos y realice la reconstrucción de distribución de agregados

Puede añadir discos a un agregado para aumentar la capacidad de almacenamiento y el rendimiento de dicho agregado. Después de añadir los discos, solo se observa una mejora en el rendimiento después de reconstruir el agregado.

Cuando recibe un evento de umbral definido por el sistema en la página de detalles Event, el texto de descripción del evento enumera el nombre del agregado que tiene el problema. Puede añadir discos y reconstruir datos en este agregado.

Los discos que agregue al agregado ya deben existir en el clúster. Si el clúster no tiene discos adicionales disponibles, puede que tenga que ponerse en contacto con su administrador o adquirir más discos. Puede usar System Manager o los comandos de la ONTAP de ONTAP para añadir discos a un agregado.

"Informe técnico 3838: Guía de configuración del subsistema de almacenamiento"

Configuración de una conexión entre un servidor Unified Manager y un proveedor de datos externo

Una conexión entre un servidor Unified Manager y un proveedor de datos externo permite enviar datos de rendimiento del clúster a un servidor externo para que los gestores de almacenamiento puedan definir las métricas de rendimiento mediante software de terceros.

Se establece una conexión entre un servidor de Unified Manager y un proveedor de datos externo a través de la opción de menú "'Proveedor de datos externos'" de la consola de mantenimiento.

Datos de rendimiento que se pueden enviar a un servidor externo

Unified Manager recopila diversos datos de rendimiento de todos los clústeres que supervisa. Puede enviar grupos específicos de datos a un servidor externo.

En función de los datos de rendimiento que desee asignar al gráfico, puede optar por enviar uno de los siguientes grupos de estadísticas:

Grupo de estadísticas	Datos incluidos	Detalles
Monitor de rendimiento	Estadísticas de rendimiento de alto nivel para los siguientes objetos: • LUN • Volúmenes	Este grupo proporciona IOPS o latencia total para todos los LUN y volúmenes de todos los clústeres supervisados. Este grupo proporciona la cantidad más pequeña de estadísticas.
Utilización de recursos	Estadísticas de utilización de recursos para los siguientes objetos: • Nodos • Agregados	Este grupo proporciona estadísticas de utilización para el nodo y agrega recursos físicos en todos los clústeres supervisados. También proporciona las estadísticas recogidas en el grupo Performance Monitor.

Grupo de estadísticas	Datos incluidos	Detalles
Acceda a la pantalla	Estadísticas de lectura/escritura de bajo nivel y por protocolo para todos los objetos con seguimiento: • Nodos • Agregados • LUN • Volúmenes • Discos • LIF • Puertos/NIC	Este grupo proporciona desgloses de lectura/escritura y por protocolo para los siete tipos de objeto con seguimiento en todos los clústeres supervisados. También proporciona las estadísticas recogidas en el grupo Performance Monitor y en el grupo Resource Utilization. Este grupo proporciona el mayor número de estadísticas.

Si se cambia el nombre de un clúster, u objeto de clúster, en el sistema de almacenamiento, tanto los objetos antiguos como los nuevos contendrán datos de rendimiento en el servidor externo (denominado «ruta_métrica»). Los dos objetos no están correlacionados con el mismo objeto. Por ejemplo, si cambia el nombre de un volumen de "'volume1_acct'" a "'acct_vol1'", verá los antiguos datos de rendimiento del volumen antiguo y los nuevos datos de rendimiento del nuevo volumen.

Consulte el artículo 30096 de Knowledge base para ver la lista de todos los contadores de rendimiento que se pueden enviar a un proveedor de datos externo.

"Los contadores de rendimiento de Unified Manager que se pueden exportar a un proveedor de datos externo"

Configurar Graphite para obtener datos de rendimiento de Unified Manager

Graphite es una herramienta de software abierta para recopilar y crear gráficos de datos de rendimiento de sistemas informáticos. Su servidor y software de Graphite deben configurarse correctamente para recibir datos estadísticos de Unified Manager.

NetApp no prueba ni verifica versiones específicas de Graphite u otras herramientas de terceros.

Después de instalar Graphite de acuerdo con las instrucciones de instalación, debe hacer los siguientes cambios para admitir la transferencia de datos estadísticos de Unified Manager:

- En la `/opt/graphite/conf/carbon.conf` Archivo, el número máximo de archivos que se pueden crear en el servidor Graphite por minuto debe configurarse en *200* (**`MAX_CREATES_PER_MINUTE = 200`**).

  Según la cantidad de clústeres de la configuración y los objetos de estadísticas que seleccionó para enviar, es posible que haya miles de archivos nuevos que deban crearse inicialmente. A 200 archivos por minuto, puede tardar 15 minutos o más antes de que se creen inicialmente todos los archivos de métricas. Una vez creados todos los archivos de métricas únicos, este parámetro ya no es relevante.

- Si está ejecutando Graphite en un servidor implementado con una dirección IPv6, el valor para LINE_RECEIVER_INTERFACE en `/opt/graphite/conf/carbon.conf` el archivo deberá cambiarse de «'0.0.0.0» a «»:». (**`LINE_RECEIVER_INTERFACE = ::`**)
- En la `/opt/graphite/conf/storage-schemas.conf` archivo, la `retentions` el parámetro se debe

utilizar para establecer la frecuencia en 5 minutos y el período de retención en la cantidad de días que son relevantes para su entorno.

El período de retención puede ser siempre que lo permita el entorno, pero el valor de frecuencia debe configurarse en 5 minutos para al menos una configuración de retención. En el ejemplo siguiente, se define una sección para Unified Manager mediante el `pattern` parámetro, y los valores establecen la frecuencia inicial en 5 minutos y el período de retención en 100 días: **`[OPM]`**

```
pattern = ^netapp-performance\..

retentions = 5m:100d
```

Si la etiqueta predeterminada del proveedor cambia de «'netapp-performance» a algo diferente, dicho cambio deberá reflejarse en la `pattern` también parámetros.

Si el servidor de Graphite no está disponible cuando el servidor de Unified Manager intenta enviar datos de rendimiento, los datos no se envían y habrá un hueco en los datos recopilados.

Configuración de una conexión desde un servidor de Unified Manager con un proveedor de datos externo

Unified Manager puede enviar datos de rendimiento de clúster a un servidor externo. Puede especificar el tipo de datos estadísticos que se envían y el intervalo en el que se envían los datos.

Lo que necesitará

- Debe tener un ID de usuario autorizado para iniciar sesión en la consola de mantenimiento del servidor de Unified Manager.
- Debe tener la siguiente información acerca del proveedor de datos externo:
  - Nombre o dirección IP del servidor (IPv4 o IPv6)
  - Puerto predeterminado del servidor (si no se utiliza el puerto predeterminado 2003)
- Debe haber configurado el servidor remoto y el software de terceros para que pueda recibir datos estadísticos del servidor de Unified Manager.
- Debe conocer el grupo de estadísticas que desea enviar:
  - PERFORMANCE_INDICATOR: Estadísticas del monitor de rendimiento
  - APROVECHAMIENTO_DE_RECURSOS: Estadísticas del monitor de rendimiento y utilización de recursos
  - DESGLOSE: Todas las estadísticas
- Se debe conocer el intervalo de tiempo en el que se desea transmitir estadísticas: 5, 10 o 15 minutos

  De forma predeterminada, Unified Manager recopila estadísticas a intervalos de 5 minutos. Si establece el intervalo de transmisión en 10 (o 15) minutos, la cantidad de datos que se envían durante cada transmisión es dos (o tres) veces mayor que cuando se utiliza el intervalo predeterminado de 5 minutos.

Si se cambia el intervalo de recogida de rendimiento de Unified Manager a 10 o 15 minutos, se debe cambiar el intervalo de transmisión de modo que sea igual o mayor que el intervalo de recogida de Unified Manager.

Es posible configurar una conexión entre un servidor de Unified Manager y un servidor de proveedor de datos externo.

Pasos

1. Inicie sesión como el usuario de mantenimiento en la consola de mantenimiento del servidor de Unified Manager.

   Se muestran los avisos de la consola de mantenimiento de Unified Manager.

2. En la consola de mantenimiento, escriba el número de la opción de menú **Proveedor de datos externos**.

   Aparece el menú Conexión del servidor externo.

3. Escriba el número de la opción de menú **Agregar/Modificar conexión de servidor**.

   Se muestra la información de conexión actual del servidor.

4. Cuando se le solicite, escriba `y` para continuar.
5. Cuando se le solicite, introduzca la dirección IP o el nombre del servidor de destino y la información del puerto del servidor (si es diferente del puerto predeterminado 2003).
6. Cuando se le solicite, escriba `y` para comprobar que la información introducida es correcta.
7. Pulse cualquier tecla para volver al menú Conexión del servidor externo.
8. Escriba el número de la opción de menú **Modificar configuración del servidor**.

   Se muestra la información de configuración actual del servidor.

9. Cuando se le solicite, escriba `y` para continuar.
10. Cuando se le solicite, escriba el tipo de estadísticas que se enviarán, el intervalo en el que se enviarán las estadísticas y si desea habilitar la transmisión de estadísticas ahora:

Para.	Introduzca…
ID del grupo de estadísticas	`0` - INDICADOR_RENDIMIENTO (predeterminado) `1` - RECURSO_UTILIZACIÓN `2` - DESGLOSE

Para.	Introduzca…
Etiqueta del proveedor	Nombre descriptivo de la carpeta donde se almacenarán las estadísticas en el servidor externo. «'netapp-rendimiento» es el nombre predeterminado, pero puede introducir otro valor. Mediante la notación de puntos puede definir una estructura de carpetas jerárquica. Por ejemplo, introduzca **`stats.performance.netapp`** las estadísticas se ubicarán en **stats** > **performance** > **netapp**.
Intervalo de transmisión	**`5`** (predeterminado), **`10`**, o. **`15`** minutos
Activar/desactivar	**`0`** - Desactivar **`1`** - Activar (predeterminado)

11. Cuando se le solicite, escriba **`y`** para comprobar que la información introducida es correcta.
12. Pulse cualquier tecla para volver al menú Conexión del servidor externo.
13. Tipo **`x`** para salir de la consola de mantenimiento.

Una vez configurada la conexión, los datos de rendimiento seleccionados se envían al servidor de destino en el intervalo de tiempo especificado. Tarda unos minutos en aparecer las métricas en la herramienta externa. Es posible que deba actualizar el explorador para ver las nuevas métricas en la jerarquía de métricas.

Supervise y gestione el estado del clúster

Introducción a la supervisión del estado de Active IQ Unified Manager

Active IQ Unified Manager (anteriormente Unified Manager de OnCommand) le ayuda a supervisar un gran número de sistemas que ejecutan el software ONTAP a través de una interfaz de usuario centralizada. La infraestructura de servidor de Unified Manager proporciona escalabilidad y compatibilidad, así como funcionalidades mejoradas de supervisión y notificación.

Las funciones clave de Unified Manager incluyen la supervisión, la alerta, la gestión de la disponibilidad y la capacidad de los clusters, la gestión de las capacidades de protección, y la agrupación de datos de diagnóstico y el envío de estos a soporte técnico.

Puede usar Unified Manager para supervisar los clústeres. Cuando se producen problemas en el clúster, Unified Manager notifica los detalles de estos problemas mediante eventos. Algunos eventos también le proporcionan una acción correctiva que puede tomar para resolver los problemas. Es posible configurar alertas para eventos que, cuando se produzcan problemas, se le notificarán por correo electrónico y capturas SNMP.

Puede utilizar Unified Manager para gestionar objetos de almacenamiento en el entorno asociándolos con anotaciones. Puede crear anotaciones personalizadas y asociar de forma dinámica clústeres, máquinas virtuales de almacenamiento (SVM) y volúmenes con las anotaciones mediante las reglas.

También puede planificar los requisitos de almacenamiento de los objetos de clúster mediante la información proporcionada en los gráficos de capacidad y estado del objeto de clúster correspondiente.

Capacidad física y lógica

Unified Manager utiliza los conceptos de espacio físico y lógico utilizados para objetos de almacenamiento de ONTAP.

- Capacidad física: El espacio físico se refiere a los bloques físicos del almacenamiento que se usa en el volumen. La «capacidad física utilizada» suele ser menor que la capacidad lógica utilizada debido a la reducción de datos de las funciones de eficiencia del almacenamiento (como la deduplicación y la compresión).
- Capacidad lógica: El espacio lógico se refiere al espacio utilizable (los bloques lógicos) de un volumen. El espacio lógico hace referencia a cómo se puede utilizar el espacio teórico, sin tener en cuenta los resultados de la deduplicación o la compresión. El “espacio lógico utilizado” es el espacio físico utilizado más el ahorro que se obtiene gracias a las funciones de eficiencia del almacenamiento (como la deduplicación y compresión) que se han configurado. Esta medición suele ser mayor que la capacidad física utilizada porque incluye copias Snapshot, clones y otros componentes, y no refleja la compresión de datos ni otras reducciones del espacio físico. Por lo tanto, la capacidad lógica total podría ser mayor que el espacio aprovisionado.

Unidades de medida de capacidad

Unified Manager calcula la capacidad de almacenamiento en función de unidades binarias de 1024 (2 10) bytes. En ONTAP 9.10.0 y anteriores, estas unidades se mostraban como KB, MB, GB, TB y PB. A partir de ONTAP 9.10.1, se muestran en Unified Manager como KiB, MIB, GIB, TIB y PIB.

Las unidades utilizadas para el rendimiento continúan siendo kilobytes por segundo (Kbps), megabytes por segundo (Mbps), gigabytes por segundo (Gbps) o terabytes por segundo (Tbps), etc., para todas las versiones de ONTAP.

La unidad de capacidad se muestra en Unified Manager para ONTAP 9.10.0 y versiones anteriores	La unidad de capacidad se muestra en Unified Manager para ONTAP 9.10.1	Cálculo	Valor en bytes
KB	KiB	1024	1024 bytes
MB	MIB	1024 * 1024	1,048,576 bytes
GB	GIB	1024 * 1024 * 1024	1,073,741,824 bytes
TB	TIB	1024 * 1024 * 1024 * 1024	1,099,511,627,776 bytes

Funciones de supervisión del estado de Unified Manager

Unified Manager se basa en una infraestructura de servidor que ofrece escalabilidad y compatibilidad, así como funciones mejoradas de supervisión y notificación. Unified Manager admite la supervisión de sistemas que ejecutan el software ONTAP.

Unified Manager incluye las siguientes funciones:

- Detección, supervisión y notificaciones de los sistemas instalados con el software ONTAP:
  - Objetos físicos: Nodos, discos, bandejas de discos, parejas SFO, puertos, Y Flash Cache
  - Objetos lógicos: Clústeres, máquinas virtuales de almacenamiento (SVM), agregados, volúmenes, LUN, espacios de nombres, Qtrees, LIF, copias Snapshot, rutas de unión, recursos compartidos NFS, Recursos compartidos de SMB, cuotas de usuarios y grupos, grupos de políticas de calidad de servicio e iGroups
  - Protocolos: CIFS, NFS, FC, iSCSI, NVMe, Y FCoE
  - Eficiencia del almacenamiento: Agregados de SSD, agregados de Flash Pool, agregados de FabricPool, deduplicación y compresión
  - Protección: Relaciones de SnapMirror (síncronas y asíncronas) y relaciones de SnapVault
- Ver el estado de la detección y supervisión del clúster
- Configuraciones de MetroCluster over FC e IP: Permite ver y supervisar la configuración, los problemas y el estado de conectividad de los componentes del clúster. Switches y puentes MetroCluster para configuraciones de MetroCluster sobre FC
- Alertas mejoradas, eventos e infraestructura de umbral
- LDAP, LDAPS, autenticación SAML y compatibilidad de usuario local
- RBAC (para un conjunto de roles predefinido)
- AutoSupport y el paquete de soporte

- Panel mejorado para mostrar el estado de la capacidad, la disponibilidad, la protección y el rendimiento del entorno
- Interoperabilidad con movimiento de volúmenes, historial de movimientos de volúmenes e historial de cambios de ruta de unión
- Alcance del área de impacto que muestra gráficamente los recursos que se ven afectados por eventos como algunos discos con errores, mirroring de agregado de MetroCluster degradado y discos de repuesto de MetroCluster abandonados
- Área posible EFFECT que muestra el efecto de los eventos de MetroCluster
- Área Suggested Corrective Actions que muestra las acciones que se pueden realizar para abordar eventos como algunos discos con errores, MetroCluster aggregate Mirroring degradado y MetroCluster Spare Disks Left Behind
- Los recursos que podrían verse afectados muestran los recursos que podrían verse afectados por eventos como el evento Volume offline, el evento Volume restricted y el evento Thin-Provisioning Volume at Risk
- Soporte para SVM con volúmenes FlexVol o FlexGroup
- Compatibilidad con la supervisión de volúmenes raíz de nodos
- Supervisión de copias snapshot mejorada, incluido el espacio informático reclamable y la eliminación de copias snapshot
- Anotaciones para objetos de almacenamiento
- Creación de informes y gestión de información de objetos de almacenamiento como capacidad física y lógica, utilización, ahorro de espacio, rendimiento y eventos relacionados
- Integración con OnCommand Workflow Automation para ejecutar flujos de trabajo

  El almacén de automatización del almacenamiento contiene paquetes de flujos de trabajo de almacenamiento automatizados y certificados de NetApp, desarrollados para su uso con OnCommand Workflow Automation (WFA). Puede descargar los paquetes e importarlos a WFA para ejecutarlos. Los flujos de trabajo automatizados están disponibles aquí:

  "Almacén de automatización del almacenamiento"

Las interfaces de Unified Manager que se utilizan para gestionar el estado del sistema de almacenamiento

Estas secciones contienen información acerca de las dos interfaces de usuario que Active IQ Unified Manager proporciona para la solución de problemas de capacidad de almacenamiento de datos, disponibilidad y protección. Las dos IU son la interfaz de usuario web de Unified Manager y la consola de mantenimiento.

Si desea utilizar las funciones de protección en Unified Manager, también debe instalar y configurar OnCommand Workflow Automation (WFA).

Interfaz de usuario web de Unified Manager

La interfaz de usuario web de Unified Manager permite a un administrador supervisar y solucionar los problemas de los clústeres relacionados con la capacidad de almacenamiento de datos, la disponibilidad y la protección.

Estas secciones describen algunos flujos de trabajo comunes que un administrador puede seguir para solucionar problemas de capacidad de almacenamiento, disponibilidad de datos o protección que se muestran

en la interfaz de usuario web de Unified Manager.

Consola de mantenimiento

La consola de mantenimiento de Unified Manager permite a un administrador supervisar, diagnosticar y solucionar problemas del sistema operativo, problemas de actualización de la versión, problemas de acceso del usuario y problemas de red relacionados con el propio servidor de Unified Manager. Si la interfaz de usuario web de Unified Manager no está disponible, la consola de mantenimiento es el único formato de acceso a Unified Manager.

Puede usar esta información para acceder a la consola de mantenimiento y utilizarla para resolver los problemas relacionados con el funcionamiento del servidor de Unified Manager.

Gestionar y supervisar clústeres y el estado de objetos del clúster

Unified Manager utiliza consultas de API periódicas y un motor de recogida de datos para recoger datos de los clústeres. Al añadir clústeres a la base de datos de Unified Manager, puede supervisar y gestionar estos clústeres para cualquier riesgo de disponibilidad y capacidad.

Supervisión del clúster

Puede añadir clústeres a la base de datos de Unified Manager para supervisar los clústeres en busca de disponibilidad, capacidad y otros detalles, como el uso de CPU, las estadísticas de la interfaz, el espacio en disco libre, el uso de qtrees y el entorno del chasis.

Los eventos se generan si el estado es anormal o cuando se incumple un umbral predefinido. Si se configura para hacerlo, Unified Manager envía una notificación a un destinatario especificado cuando un evento activa una alerta.

Volúmenes raíz de nodos

Puede supervisar el volumen raíz del nodo mediante Unified Manager. La práctica recomendada es que el volumen raíz del nodo debe tener capacidad suficiente para evitar que el nodo se apague.

Cuando la capacidad utilizada del volumen raíz del nodo supera el 80 % de la capacidad total del volumen raíz del nodo, se genera el evento Node Root Volume Space casi Full. Puede configurar una alerta para que el evento reciba una notificación. Puede tomar las acciones adecuadas para evitar que el nodo deje de funcionar mediante System Manager de ONTAP o la CLI de ONTAP.

Eventos y umbrales para agregados raíz de nodos

Puede supervisar el agregado raíz del nodo mediante Unified Manager. La práctica recomendada es aprovisionar considerablemente el volumen raíz en el agregado raíz para evitar que se detenga el nodo.

De manera predeterminada, no se generan eventos de capacidad ni rendimiento para los agregados raíz.

Además, los valores de umbral que utiliza Unified Manager no son aplicables a los agregados raíz del nodo. Solo un representante del soporte técnico puede modificar la configuración de estos eventos para que se generen. Cuando el representante de soporte técnico modifica la configuración, los valores del umbral de capacidad se aplican al agregado raíz del nodo.

Puede realizar acciones adecuadas para evitar que el nodo se detenga por medio de ONTAP System Manager o la CLI de ONTAP.

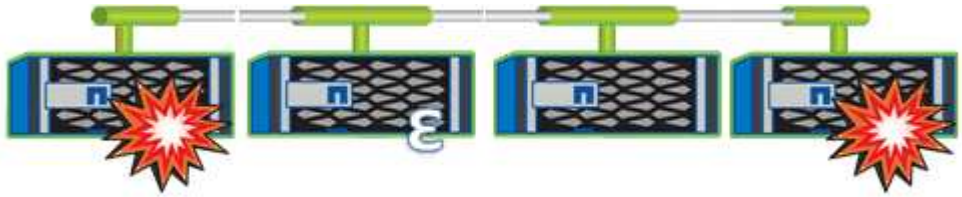
Comprensión del quórum y del épsilon

El quórum y el épsilon son medidas importantes para el estado y la función de los clusters, que, en su conjunto, indican cómo abordan los clusters los desafíos potenciales de comunicaciones y conectividad.

Quórum es una condición previa para un clúster en pleno funcionamiento. Cuando un clúster se encuentra en quórum, una mayoría simple de nodos está en buen estado y puede comunicarse entre sí. Cuando se pierde quorum, el clúster pierde la capacidad de realizar las operaciones normales del clúster. Sólo una colección de nodos puede tener quórum a la vez porque todos los nodos comparten colectivamente una única vista de los datos. Por lo tanto, si dos nodos sin comunicación tienen permiso para modificar los datos de maneras divergentes, ya no es posible reconciliar los datos en una única vista de datos.

Cada nodo del clúster participa en un protocolo de votación que selecciona un nodo principal frente a cada uno de los restantes, que será secundario. El nodo maestro es responsable de sincronizar la información en todo el clúster. Cuando se forma el quórum, se mantiene mediante una votación continua. Si el nodo maestro se desconecta y el clúster aún se mantiene quórum, los nodos que permanecen en línea eligen un nuevo maestro.

Dado que en un cluster existe la posibilidad de empate con un número par de nodos, uno de ellos tiene un peso adicional fraccionario al votar, llamado épsilon. Si falla la conectividad entre dos partes iguales de un clúster de gran tamaño, el grupo de nodos que contienen épsilon mantendrá el quórum, suponiendo que todos los nodos estén en buen estado. Por ejemplo, en la siguiente ilustración se muestra un clúster de cuatro nodos en el que dos de los nodos fallan. Sin embargo, dado que uno de los nodos supervivientes tiene épsilon, el cluster permanece en quórum aunque no hay una mayoría simple de nodos sanos.



Cuando se crea el clúster, se asigna automáticamente al primer nodo épsilon. Si el nodo que contiene épsilon se queda poco saludable, supera a su partner de alta disponibilidad o lo hace su partner de alta disponibilidad, se asignará el valor épsilon automáticamente a un nodo sano en una pareja de alta disponibilidad diferente.

Desconectar un nodo puede afectar a la capacidad del clúster para permanecer de quórum. Por lo tanto, ONTAP emite un mensaje de advertencia si se intenta una operación que impide que el clúster se quorum o si se elimina una interrupción del servicio de una pérdida de quórum. Puede deshabilitar los mensajes de advertencia de quórum mediante el comando cluster quorum-service options modify en el nivel de privilegio avanzado.

En general, suponiendo que haya una conectividad fiable entre los nodos del clúster, un clúster más grande es más estable que un clúster más pequeño. En un cluster de 24 nodos es más fácil mantener el requisito de quórum de la mayoría simple de la mitad de los nodos más con épsilon que en un cluster de dos nodos.

Un clúster de dos nodos presenta algunos retos únicos para mantener el quórum. Los clústeres de dos nodos utilizan Cluster ha, en los que ninguno de los dos nodos está configurado con épsilon; en su lugar, ambos nodos reciben un sondeo continuo para garantizar que si uno de ellos falla, el otro tiene acceso completo de lectura/escritura a los datos, así como acceso a interfaces lógicas y funciones de gestión.

Ver la lista del clúster y sus detalles

La vista Health: All Clusters se puede usar para ver el inventario de clústeres. La vista Capacity: All Clusters permite ver información resumida sobre la capacidad de almacenamiento y la utilización en todos los clústeres.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

También puede ver detalles de cada clúster, como el estado del clúster, la capacidad, la configuración, las LIF, los nodos, Y los discos en ese clúster mediante la página de detalles Cluster / Health.

Los detalles en la vista Health: All Clusters, Capacity: All Clusters y la página de detalles Cluster / Health le ayudan a planificar el almacenamiento. Por ejemplo, antes de aprovisionar un nuevo agregado, puede seleccionar un clúster específico de la vista Estado: Todos los clústeres y obtener detalles de capacidad para determinar si el clúster tiene el espacio requerido.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **clústeres**.
2. En el menú Ver, seleccione **Estado: Todos los clústeres** ver para ver información de salud, o **capacidad: Todos los clústeres** ver detalles sobre la capacidad de almacenamiento y la utilización en todos los clústeres.
3. Haga clic en el nombre de un clúster para ver los detalles completos del clúster en la página de detalles **Cluster / Health**.

Información relacionada

- "Página de detalles Cluster / Health"
- "Rendimiento: Vista All Clusters"
- "Supervisar las configuraciones de MetroCluster"
- "Visualización del estado de seguridad para clústeres y máquinas virtuales de almacenamiento"
- "Qué criterios de seguridad se están evaluando"

Comprobar el estado de los clústeres en una configuración de MetroCluster

Puede usar Active IQ Unified Manager (Unified Manager) para comprobar el estado operativo de los clústeres y sus componentes, en configuraciones de MetroCluster over FC e MetroCluster over IP. Si los clústeres estaban implicados en un evento de rendimiento detectado por Unified Manager, el estado puede ayudarle a determinar si un problema de hardware o software ha contribuido al evento.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Debe haber analizado un evento de rendimiento de una configuración de MetroCluster y obtener el nombre del clúster involucrado.
- Ambos clústeres de la configuración de MetroCluster mediante FC e IP deben supervisarse con la misma instancia de Unified Manager.

Determinar el estado del clúster en la configuración de MetroCluster over FC

Siga estos pasos para determinar el estado del clúster en una configuración de MetroCluster over FC.

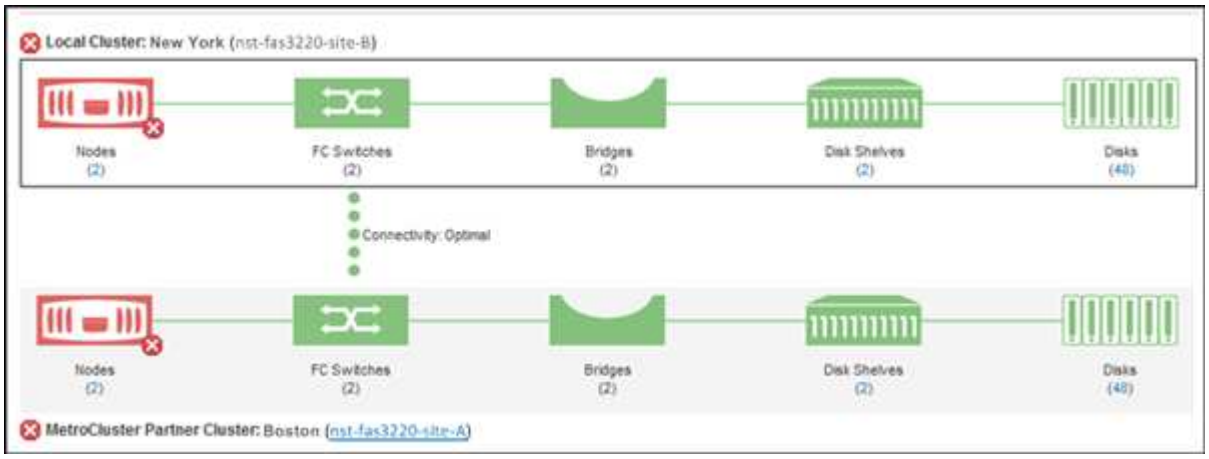
Pasos

1. En el panel de navegación izquierdo, haga clic en **Gestión de eventos** para mostrar la lista de eventos.
2. En el panel de filtros, seleccione todos los filtros MetroCluster en la categoría **Tipo de fuente**. Se ven todos los eventos levantados en su entorno para todas las configuraciones de MetroCluster.
3. Junto a un evento de MetroCluster, haga clic en el nombre del clúster.

   Si no se muestran eventos de MetroCluster, puede usar la barra de búsqueda para buscar el nombre del clúster involucrado en el evento relacionado con su configuración de MetroCluster over FC.

   La vista Estado: Todos los clústeres se muestra con información detallada sobre el evento.

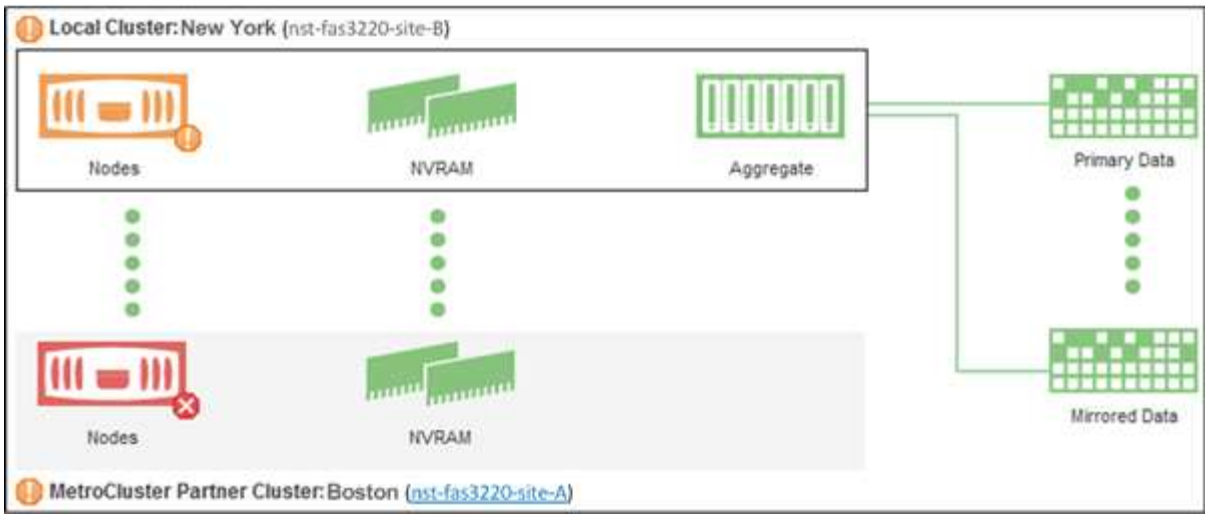
4. Seleccione la ficha **conectividad MetroCluster** para mostrar el estado de la conexión entre el clúster seleccionado y su clúster asociado.



   En este ejemplo, se muestran los nombres y los componentes del clúster local y su clúster asociado. Un icono amarillo o rojo indica un evento de estado para el componente resaltado. El icono de conectividad representa el enlace entre los clústeres. Puede colocar el cursor del ratón en un icono para mostrar la información del evento o hacer clic en el icono para mostrar los eventos. Es posible que un problema de estado en cualquiera de los clústeres haya contribuido al evento de rendimiento.

   Unified Manager supervisa el componente NVRAM del enlace entre los clústeres. Si el icono de switches FC en el clúster local o asociado o el icono de conectividad están en rojo, es posible que haya provocado un problema de estado del enlace el evento de rendimiento.

5. Seleccione la ficha **replicación de MetroCluster**.



En este ejemplo, si el icono NVRAM del clúster local o del partner es amarillo o rojo, un problema de estado de la NVRAM podría haber provocado el evento de rendimiento. Si no hay iconos de color rojo o amarillo en la página, es posible que un problema de rendimiento del clúster de partners haya provocado el evento de rendimiento.

Determinación del estado del clúster en la configuración de MetroCluster over IP

Siga estos pasos para determinar el estado del clúster en una configuración de MetroCluster over IP.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Gestión de eventos** para mostrar la lista de eventos.
2. En el panel de filtro, en la categoría **Tipo de fuente**, seleccione la `MetroCluster Relationship` filtro. Se ven todos los eventos levantados en su entorno para todas las configuraciones de MetroCluster.

   Si no puede ver los eventos de MetroCluster notificados, puede utilizar la barra de búsqueda para buscar según el nombre del clúster involucrado en el evento relacionado con la configuración de MetroCluster over IP.

3. Junto al evento de MetroCluster relevante, haga clic en el nombre del clúster. La página Clusters se muestra con los detalles de ese clúster. Para obtener información acerca de cómo determinar problemas de salud, consulte "Supervise los problemas de conectividad en la configuración de MetroCluster over IP".

Ver el estado y la capacidad de los clústeres de la cabina All SAN

Se pueden usar las páginas del inventario de clústeres para mostrar el estado y la capacidad de los clústeres de la cabina All SAN.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Se puede ver información general de todos los clústeres de cabina SAN en la vista Estado: Todos los clústeres y su capacidad: Todos los clústeres. Además, puede ver detalles en la página de detalles Cluster / Health.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **clústeres**.
2. Asegúrese de que la columna "'Personality'" se muestra en la vista **Salud: Todos los clusters**, o añádala utilizando el control **Mostrar / Ocultar**.

   Esta columna muestra «"cabina All SAN»» de los clústeres de la cabina All SAN.

3. Revise la información.
4. Para ver información sobre la capacidad de almacenamiento de esos clústeres, seleccione la vista Capacity: All Clusters.
5. Para ver información detallada sobre el estado y la capacidad de almacenamiento de esos clústeres, haga clic en el nombre de un clúster de cabina All SAN.

   Consulte los detalles en las pestañas Estado, capacidad y nodos en la página de detalles Cluster / Health

Ver la lista y los detalles del nodo

Puede usar la vista Health: All Nodes para ver la lista de nodos en los clústeres. Puede usar la página de detalles Cluster / Health para ver información detallada acerca de los nodos que forman parte del clúster que se supervisa.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Es posible ver detalles como el estado del nodo, el clúster que contiene el nodo, detalles de capacidad del agregado (usado y total) y detalles de capacidad bruta (utilizable, de reserva y total). También puede obtener información acerca de las parejas de alta disponibilidad, bandejas de discos y puertos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **nodos**.
2. En la vista **Estado: Todos los nodos**, haga clic en el nodo cuyos detalles desee ver.

   La información detallada del nodo seleccionado se muestra en la página de detalles Cluster / Health. En el panel izquierdo se muestra la lista de pares de alta disponibilidad. De forma predeterminada, ha Details está abierto, lo que muestra detalles de estado de alta disponibilidad y eventos relacionados con el par de alta disponibilidad seleccionado.

3. Para ver otros detalles sobre el nodo, realice la acción correspondiente:

Para ver…	Haga clic en…
Detalles acerca de las bandejas de discos	**Bandejas de discos**.
Información relacionada con el puerto	**Puertos**.

Para obtener más información, consulte:

- "Rendimiento: Vista de todos los nodos"
- "Ver los valores de IOPS disponibles de los nodos y los agregados"

- "Ver los valores de capacidad de rendimiento de los nodos y los agregados"

Generar un informe de inventario de hardware para la renovación de contrato

Es posible generar un informe que contenga una lista completa de información de clústeres y nodos; por ejemplo, números de modelo del hardware y números de serie, tipos y números de disco, licencias instaladas, etc. Este informe resulta útil para la renovación de contratos en sitios seguros (sitios "seguros") que no están conectados a la plataforma Active IQ de NetApp.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **nodos**.
2. Vaya a la vista **Estado: Todos los nodos** o **rendimiento: Todos los nodos**.
3. Seleccione **Informes** > *** >** Informe de inventario de hardware*.

   El informe de inventario de hardware se descarga como un archivo .csv con información completa a partir de la fecha actual.

4. Facilite esta información a su contacto de soporte de NetApp para la renovación de su contrato.

Consulte la lista y los detalles de la máquina virtual de almacenamiento

En la vista Health: All Storage VMs, puede supervisar el inventario de máquinas virtuales de almacenamiento (SVM). Puede usar la página de detalles Storage VM / Health para ver información detallada sobre las SVM que se supervisan.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Puede ver detalles de SVM, como la capacidad, la eficiencia y la configuración de una SVM. También se puede ver información sobre los dispositivos relacionados y las alertas relacionadas de esa SVM.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **Storage VMs**.
2. Elija una de las siguientes maneras de ver los detalles de SVM:
   - Para ver información sobre el estado de todas las SVM de todos los clústeres, en el menú Ver, seleccione Estado: All Storage VMs view.
   - Para ver los detalles completos, haga clic en el nombre de la máquina virtual de almacenamiento.

     También puede ver todos los detalles haciendo clic en **Ver detalles** en el cuadro de diálogo Detalles mínimos.

3. Vea los objetos relacionados con la SVM haciendo clic en **Ver relacionado** en el cuadro de diálogo Detalles mínimos.

Información relacionada

- "Storage VM: Página de detalles Health"
- "Rendimiento: Vista de todas las máquinas virtuales de almacenamiento"
- "Seguridad: Vista antiransomware"
- "Visualización del estado de seguridad para clústeres y máquinas virtuales de almacenamiento"
- "Relación: Vista todas las relaciones"

Consulte la lista de agregados y los detalles

En la vista Health: All Aggregates, puede supervisar su inventario de agregados. La vista capacidad: Todos los agregados le permite ver información sobre la capacidad y la utilización de los agregados en todos los clústeres.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Puede ver detalles como la capacidad y la configuración del agregado, y la información sobre el disco en la página de detalles Aggregate / Health. Puede utilizar estos detalles antes de configurar los ajustes del umbral si es necesario.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **agregados**.
2. Seleccione una de las siguientes formas de ver los detalles del agregado:
   - Para ver información sobre el estado de todos los agregados de todos los clústeres, en el menú Ver, seleccione Estado: Todos los agregados vista.
   - Para ver información sobre la capacidad y la utilización de todos los agregados en todos los clústeres, en el menú Ver, seleccione capacidad: All Aggregates View.
   - Para ver todos los detalles, haga clic en el nombre del agregado.

     También puede ver todos los detalles haciendo clic en **Ver detalles** en el cuadro de diálogo Detalles mínimos.
3. Para ver los objetos relacionados con el agregado, haga clic en **Ver relacionado** en el cuadro de diálogo Detalles mínimos.

Información relacionada

- "Página de detalles Aggregate / Health"
- "Rendimiento: Vista de todos los agregados"
- "Personalizar los informes de capacidad de agregados"

Visualización de información de capacidad de FabricPool

Es posible ver información sobre la capacidad de FabricPool de los clústeres, los agregados y los volúmenes en las páginas de detalles y el inventario de capacidad y rendimiento de estos objetos. Estas páginas también muestran información de

duplicación de FabricPool cuando se configuró un nivel de duplicación.

Estas páginas muestran información, como la capacidad disponible en el nivel de rendimiento local y en el nivel de nube, cuánta capacidad se utiliza en ambos niveles, qué agregados están conectados a un nivel de la nube, Y qué volúmenes están implementando las funciones de FabricPool moviendo cierta información al nivel de cloud.

Cuando un nivel de nube se duplica con otro proveedor de la nube (el «nivel de irritación»), ambos niveles de la nube se muestran en la página de detalles de agregado / Salud.

Pasos

1. Realice una de las siguientes acciones:

Para ver información de capacidad de…	Realice lo siguiente…
De clúster	a. En la vista Capacity: All Clusters, haga clic en un clúster. b. En la página de detalles Cluster / Health, haga clic en la ficha **Configuration**. La pantalla muestra los nombres de cualquier nivel de cloud a la que esté conectado el clúster.
Agregados	a. En la vista capacidad: Todos los agregados, haga clic en un agregado donde el campo Tipo indique «SD (FabricPool)» o «HDD (FabricPool)». b. En la página de detalles Agreate / Health, haga clic en la ficha **Capacity**. La pantalla muestra la capacidad total utilizada en el nivel de cloud. c. Haga clic en la ficha **Información de disco**. La pantalla muestra el nombre del nivel de cloud y la capacidad utilizada. d. Haga clic en la ficha **Configuración**. La pantalla muestra el nombre del nivel de cloud y otra información detallada acerca del nivel de cloud.

Para ver información de capacidad de…	Realice lo siguiente…
Volúmenes	a. En la vista Capacity: All Volumes, haga clic en un volumen donde aparece el nombre de una política en el campo «'Tiering Policy». b. En la página de detalles Volume / Health, haga clic en la ficha **Configuration**. La pantalla muestra el nombre de la política de organización en niveles de FabricPool asignada al volumen.

2. En la página **Análisis de carga de trabajo** puede seleccionar «'Vista de nivel de cloud» en el área **tendencias de capacidad** para ver la capacidad que se utiliza en el nivel de rendimiento local y en el nivel de cloud durante el mes anterior.

Para obtener más información sobre los agregados de FabricPool, consulte "Descripción general de discos y agregados".

Ver los detalles del pool de almacenamiento

Es posible ver los detalles del pool de almacenamiento para supervisar el estado del pool de almacenamiento, la caché total y disponible, y las asignaciones usadas y disponibles.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **agregados**.
2. Haga clic en el nombre de un agregado.

   Se muestran los detalles del agregado seleccionado.

3. Haga clic en la ficha **Información de disco**.

   Aparece información detallada sobre el disco.

   La tabla de caché solo se muestra cuando el agregado seleccionado utiliza un pool de almacenamiento.

4. En la tabla caché, mueva el puntero sobre el nombre del pool de almacenamiento requerido.

   Se muestran los detalles del pool de almacenamiento.

Ver la lista de volúmenes y los detalles

En la vista Health: Todos los volúmenes, es posible supervisar el inventario de volúmenes. La capacidad: Todos los volúmenes de la vista le permite ver información sobre la capacidad y la utilización de los volúmenes de un clúster.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

También se puede usar la página de detalles Volume / Health para ver información detallada sobre los volúmenes que se supervisan, incluida la capacidad, la eficiencia, la configuración y la protección de los volúmenes. También es posible ver información sobre los dispositivos relacionados y las alertas relacionadas para un volumen específico.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. Seleccione una de las siguientes maneras de ver los detalles del volumen:
   - Para ver información detallada sobre el estado de los volúmenes de un clúster, en el menú Ver, seleccione Estado: All Volumes view.
   - Para ver información detallada sobre la capacidad y la utilización de los volúmenes en un clúster, en el menú Ver, seleccione capacidad: All Volumes view.
   - Para ver los detalles completos, haga clic en el nombre del volumen.

     También puede ver todos los detalles haciendo clic en **Ver detalles** en el cuadro de diálogo Detalles mínimos.
3. **Opcional:** para ver los objetos relacionados con el volumen, haga clic en **Ver relacionados** en el cuadro de diálogo Detalles mínimos.

Información relacionada

- "Volumen: Página de detalles Health"
- "Rendimiento: Vista de todos los volúmenes"
- "Seguridad: Vista antiransomware"
- "Visualización de las relaciones de protección de volúmenes"
- "Creación de un informe para ver los gráficos de capacidad de los volúmenes disponibles"

Ver detalles acerca de los recursos compartidos de NFS

Es posible ver detalles sobre todos los recursos compartidos de NFS, como su estado, la ruta asociada con el volumen (volúmenes FlexGroup o volúmenes FlexVol), los niveles de acceso de los clientes a los recursos compartidos NFS y la política de exportación definida para los volúmenes que se exportan. Use la vista Health: All NFS Shares para ver todos los recursos compartidos de NFS de todos los clústeres supervisados, y use la página de detalles Storage VM / Health para ver todos los recursos compartidos de NFS en una máquina virtual de almacenamiento específica (SVM).

Lo que necesitará

- La licencia de NFS debe estar habilitada en el clúster.
- Se deben configurar las interfaces de red que sirven a los recursos compartidos de NFS.
- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Paso

1. En el panel de navegación de la izquierda, siga los siguientes pasos dependiendo de si desea ver todos los recursos compartidos NFS o solo los recursos compartidos NFS de una SVM concreta.

Para…	Siga estos pasos…
Ver todos los recursos compartidos de NFS	Haga clic en **almacenamiento** > **Recursos compartidos NFS**
Vea los recursos compartidos de NFS para un único SVM	a. Haga clic en **almacenamiento** > **Storage VMs** b. Haga clic en la SVM para la que desea ver los detalles de los recursos compartidos de NFS. c. En la página de detalles Storage VM / Health, haga clic en la ficha **NFS Shares**.

Para obtener más información, consulte "Aprovisionar los volúmenes compartidos de archivos" y.. "Aprovisionamiento de recursos compartidos de archivos CIFS y NFS mediante API".

Ver detalles sobre los recursos compartidos de SMB/CIFS

Puede ver detalles sobre todos los recursos compartidos SMB/CIFS, como el nombre del recurso compartido, la ruta de unión, que contiene objetos, la configuración de seguridad y las políticas de exportación definidas para el recurso compartido. Use la vista Health: Todos los recursos compartidos de SMB para ver todos los recursos compartidos de SMB en todos los clústeres supervisados y use la página de detalles Storage VM / Health para ver todos los recursos compartidos de SMB en una máquina virtual de almacenamiento (SVM) específica.

Lo que necesitará

- La licencia de CIFS debe estar habilitada en el clúster.
- Se deben configurar las interfaces de red que sirven a los recursos compartidos de SMB/CIFS.
- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

No se muestran los recursos compartidos de las carpetas.

Paso

1. En el panel de navegación de la izquierda, siga los siguientes pasos dependiendo de si desea ver todos los recursos compartidos de SMB/CIFS o solo los recursos compartidos de una SVM en particular.

Para…	Siga estos pasos…
Ver todos los recursos compartidos de SMB/CIFS	Haga clic en **almacenamiento** > **Recursos compartidos SMB**

Para…	Siga estos pasos…
Vea los recursos compartidos de SMB/CIFS para un único SVM	a. Haga clic en **almacenamiento** > **Storage VMs** b. Haga clic en la SVM para la que desea ver los detalles de los recursos compartidos de SMB/CIFS. c. En la página de detalles Storage VM / Health, haga clic en la ficha **Recursos compartidos SMB**.

Para obtener más información, consulte "Aprovisionamiento de recursos compartidos de archivos CIFS y NFS mediante API".

Ver la lista de copias Snapshot

Puede ver la lista de copias Snapshot de un volumen seleccionado. Puede usar la lista de copias Snapshot para calcular la cantidad de espacio en disco que puede recuperarse si se eliminan una o más copias Snapshot y puede eliminar las copias Snapshot si fuera necesario.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- El volumen que contiene las copias Snapshot debe estar en línea.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En la vista **Estado: Todos los volúmenes**, seleccione el volumen que contiene las copias Snapshot que desea ver.
3. En la página de detalles **Volume / Health**, haga clic en la ficha **Capacity**.
4. En el panel **Detalles** de la ficha **capacidad**, en la sección otros detalles, haga clic en el enlace que se encuentra junto a **copias Snapshot**.

   El número de copias de Snapshot es un enlace que muestra la lista de copias de Snapshot.

Información relacionada

"Página Health/Volumes"

Eliminar copias Snapshot

Puede eliminar una copia Snapshot para conservar espacio o a liberar espacio en disco, o bien puede eliminar la copia Snapshot si ya no se necesita.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

El volumen debe estar en línea.

Para eliminar una copia snapshot que está ocupada o bloqueada, debe haber liberado la copia snapshot de la aplicación que la estaba utilizando.

- No puede eliminar la copia snapshot básica de un volumen principal si un volumen FlexClone está utilizando esa copia snapshot.

  La copia Snapshot básica es la copia Snapshot que se utiliza para crear el volumen FlexClone y muestra el estado `Busy` Y Dependencia de aplicaciones como `Busy, Vclone` en el volumen principal.

- No se puede eliminar una copia snapshot bloqueada que se haya utilizado en una relación de SnapMirror.

  La copia snapshot está bloqueada y es necesaria para la siguiente actualización.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En la vista **Estado: Todos los volúmenes**, seleccione el volumen que contiene las copias Snapshot que desea ver.

   Se muestra la lista de copias Snapshot.

3. En la página de detalles **Volume / Health**, haga clic en la ficha **Capacity**.
4. En el panel **Detalles** de la ficha **capacidad**, en la sección otros detalles, haga clic en el enlace que se encuentra junto a **copias Snapshot**.

   El número de copias de Snapshot es un enlace que muestra la lista de copias de Snapshot.

5. En la vista **copias Snapshot**, seleccione las copias Snapshot que desee eliminar y, a continuación, haga clic en **Eliminar seleccionadas**.

Cálculo del espacio de la reclamación para las copias snapshot

Puede calcular la cantidad de espacio en disco que se puede recuperar si se eliminan una o más copias Snapshot.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- El volumen debe estar en línea.
- El volumen debe ser un volumen de FlexVol, pero esta funcionalidad no es compatible con FlexGroup Volumes.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En la vista **Estado: Todos los volúmenes**, seleccione el volumen que contiene las copias Snapshot que desea ver.

   Se muestra la lista de copias Snapshot.

3. En la página de detalles **Volume / Health**, haga clic en la ficha **Capacity**.

4. En el panel **Detalles** de la ficha **capacidad**, en la sección otros detalles, haga clic en el enlace que se encuentra junto a **copias Snapshot**.

   El número de copias de Snapshot es un enlace que muestra la lista de copias de Snapshot.

5. En la vista **copias Snapshot**, seleccione las copias Snapshot para las que desea calcular el espacio que se puede reclamar.
6. Haga clic en **calcular**.

   Se muestra el espacio reclamable (en porcentaje, KB, MB, GB, etc.) del volumen.

7. Para volver a calcular el espacio que se puede reclamar, seleccione las copias Snapshot necesarias y haga clic en **Recalcular**.

Descripción de las ventanas y cuadros de diálogo del objeto del clúster

Es posible ver todos los clústeres y los objetos del clúster desde la página de objetos de almacenamiento correspondiente. También puede ver los detalles desde la página de detalles del objeto de almacenamiento correspondiente. Ahora se puede iniciar la interfaz de usuario de System Manager desde las siguientes secciones de ALMACENAMIENTO Y PROTECCIÓN del INVENTARIO.

- Páginas Cluster Inventory, Cluster Health y Cluster Performance
- Páginas Aggregate Inventory, Aggregate Health y Aggregate Performance
- Páginas Volume Inventory, Volume Health y Volume Performance
- Páginas Node Inventory and Node Performance
- Páginas de inventario de StorageVM, estado de StorageVM y rendimiento de StorageVM
- Páginas de relaciones de protección

Flujos de trabajo y tareas comunes del estado de Unified Manager

Algunos flujos de trabajo administrativos y tareas comunes asociados con Unified Manager incluyen la selección de los clústeres de almacenamiento que se van a supervisar; el diagnóstico de condiciones que afectan negativamente a la disponibilidad de los datos, la capacidad y la protección; la restauración de datos perdidos; la configuración y la gestión de volúmenes; y la agrupación y el envío de datos de diagnóstico al soporte técnico (cuando sea necesario).

Unified Manager permite a los administradores de almacenamiento ver una consola, evaluar la capacidad general, la disponibilidad y el estado de protección de los clústeres de almacenamiento gestionados y, a continuación, identificar, localizar, diagnosticar y asignar rápidamente para solucionar cualquier problema específico que pueda surgir.

Los problemas más importantes relacionados con un clúster, una máquina virtual de almacenamiento (SVM), un volumen o un volumen FlexGroup que afectan a la capacidad de almacenamiento o la disponibilidad de datos de los objetos de almacenamiento gestionados se muestran en los gráficos de estado del sistema y los eventos en la página Dashboard. Cuando se identifican problemas críticos, esta página proporciona enlaces

para respaldar flujos de trabajo de solución de problemas adecuados.

Unified Manager también se puede incluir en los flujos de trabajo que incluyen herramientas de capacidad de gestión relacionadas, como OnCommand Workflow Automation (WFA), para dar soporte a la configuración directa de los recursos de almacenamiento.

En este documento se describen los flujos de trabajo comunes relacionados con las siguientes tareas administrativas:

- Diagnóstico y gestión de problemas de disponibilidad

  Si los problemas de fallo de hardware o de configuración de recursos de almacenamiento ocasionan la visualización de eventos de disponibilidad de datos en la página Consola, los administradores de almacenamiento pueden seguir los enlaces integrados para ver información de conectividad sobre el recurso de almacenamiento afectado, ver consejos para la solución de problemas y asignar solución de problemas a otros administradores.

- Configurar y supervisar incidentes de rendimiento

  El administrador puede supervisar y gestionar el rendimiento de los recursos del sistema de almacenamiento que se supervisan. Consulte "Introducción a la supervisión del rendimiento de Active IQ Unified Manager" si quiere más información.

- Diagnosticar y gestionar problemas de capacidad de volumen

  Si los problemas de capacidad de almacenamiento de volumen se muestran en la página Consola, los administradores de almacenamiento pueden seguir los enlaces integrados para ver las tendencias actuales e históricas relacionadas con la capacidad de almacenamiento del volumen afectado, ver asesoramiento sobre solución de problemas y asignar solución de problemas a otros administradores.

- Configuración, supervisión y diagnóstico de problemas en las relaciones de protección

  Después de crear y configurar relaciones de protección, los administradores de almacenamiento pueden ver los posibles problemas relacionados con las relaciones de protección, el estado actual de las relaciones de protección, la información de éxito actual e histórica de las relaciones afectadas y el asesoramiento sobre solución de problemas. Consulte "Creación, supervisión y solución de problemas de relaciones de protección" si quiere más información.

- Crear archivos de copia de seguridad y restaurar datos a partir de archivos de copia de seguridad.
- Asociación de objetos de almacenamiento con anotaciones

  Al asociar los objetos de almacenamiento con anotaciones, los administradores de almacenamiento pueden filtrar y ver los eventos relacionados con los objetos de almacenamiento, lo que permite a los administradores de almacenamiento priorizar y resolver los problemas asociados con los eventos.

- El uso de API REST para ayudar a gestionar los clústeres mediante la visualización de la información de estado, capacidad y rendimiento que captura Unified Manager. Consulte "Primeros pasos con API de REST de Active IQ Unified Manager" si quiere más información.
- Enviar un bundle de soporte al soporte técnico

  Los administradores de almacenamiento pueden recuperar y enviar un bundle de soporte al soporte técnico mediante la consola de mantenimiento. Los paquetes de soporte se deben enviar al soporte técnico cuando el problema requiera un diagnóstico y una solución de problemas más detallados de lo que proporcione un mensaje de AutoSupport.

Supervisión y solución de problemas de disponibilidad de datos

Unified Manager supervisa la fiabilidad con la que los usuarios autorizados pueden acceder a sus datos almacenados, alerta de condiciones que bloquean o impiden el acceso. Además, le permite diagnosticar estas condiciones, asignar y realizar un seguimiento de su resolución.

Los temas de flujo de trabajo de disponibilidad de esta sección describen ejemplos de cómo un administrador de almacenamiento puede usar la interfaz de usuario web de Unified Manager para detectar, diagnosticar y asignar para resolver las condiciones de hardware y software que afectan negativamente a la disponibilidad de datos.

Buscar y solucionar las condiciones de enlace inactivo de interconexión de conmutación por error de almacenamiento

Este flujo de trabajo proporciona un ejemplo de cómo puede analizar, evaluar y resolver las condiciones de los enlaces de interconexión de conmutación por error del almacenamiento desactivado. En esta situación, es un administrador que utiliza Unified Manager para analizar los riesgos de la conmutación por error del almacenamiento antes de iniciar una actualización de la versión de ONTAP en los nodos.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Si se producen errores en las interconexiones de conmutación por error del almacenamiento entre nodos de parejas de alta disponibilidad durante un intento de actualización no disruptivo, la actualización falla. Por lo tanto, una práctica común es que el administrador supervise y confirme la fiabilidad de la conmutación por error del almacenamiento en los nodos del clúster que desea actualizar antes del inicio de una actualización.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Gestión de eventos**.
2. En la página de inventario **Event Management**, seleccione **Eventos de disponibilidad activa**.
3. En la parte superior de la columna **Event Management** Inventory page **Name**, haga clic en e introduzca `*failover` en el cuadro de texto para limitar el evento para que se muestre a eventos relacionados con la conmutación por error de almacenamiento.

   Se muestran todos los eventos anteriores relacionados con las condiciones de conmutación por error del almacenamiento.

   En este escenario, Unified Manager muestra el evento «interconexión por conmutación por error del almacenamiento uno o más enlaces abajo» en su sección incidentes de disponibilidad.

4. Si se muestran uno o más eventos relacionados con la conmutación por error del almacenamiento en la página de inventario **Event Management**, realice los siguientes pasos:

   a. Haga clic en el enlace del título del evento para mostrar detalles de dicho evento.

      En este ejemplo, haga clic en el título del evento «interconexión de conmutación por error de almacenamiento uno o más enlaces hacia abajo».

   Se muestra la página de detalles Event para ese evento.

a. En la página Event Details, puede realizar una o varias de las siguientes tareas:
   - Revise el mensaje de error en el campo causa y evalúe el problema.
   - Asigne el evento a un administrador.
   - Reconozca el evento.

Información relacionada

"Página de detalles Event"

"Roles y funcionalidades de usuario de Unified Manager"

Realizar acciones correctivas para enlaces de interconexión de conmutación al nodo de respaldo de almacenamiento inactivos

Cuando se muestra la página de detalles Event de un evento de almacenamiento relacionado con conmutación al nodo de respaldo, puede revisar la información de resumen de la página para determinar la urgencia del evento, la posible causa del problema y la posible resolución del problema.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

En este ejemplo, el resumen de eventos que se proporciona en la página de detalles Event contiene la siguiente información sobre la condición de enlace inactivo de la interconexión de conmutación por error de almacenamiento:

```
Event: Storage Failover Interconnect One or More Links Down

Summary

Severity: Warning
State: New
Impact Level: Risk
Impact Area: Availability
Source: aardvark
Source Type: Node
Acknowledged By:
Resolved By:
Assigned To:
Cause: At least one storage failover interconnected link
       between the nodes aardvark and bonobo is down.
       RDMA interconnect is up (Link0 up, Link1 down)
```

La información de eventos de ejemplo indica que un enlace de interconexión de conmutación por error de almacenamiento, Link1, entre los nodos de par ha aardvark y bonobo está inactivo, pero que Link0 entre Apple y Boy está activo. Debido a que hay un enlace activo, el acceso remoto a la memoria dinámica (RDMA) sigue funcionando y una tarea de recuperación tras fallos del almacenamiento aún puede tener éxito.

Sin embargo, para asegurarse de que los enlaces que fallan y la protección de recuperación tras fallos de almacenamiento están totalmente deshabilitados, usted decide diagnosticar más lejos la razón de la caída de Link1.

Pasos

1. En la página de detalles **Event**, puede hacer clic en el enlace al evento especificado en el campo Source para obtener más detalles de otros eventos que podrían estar relacionados con la condición de enlace inactivo de interconexión de conmutación por error del almacenamiento.

   En este ejemplo, el origen del evento es el nodo llamado aardvark. Al hacer clic en el nombre de ese nodo se muestran los detalles de alta disponibilidad para la pareja de alta disponibilidad afectada, aardvark y bonobo, en la pestaña nodos de la página de detalles Cluster / Health y se muestran otros eventos que se produjeron recientemente en la pareja de alta disponibilidad afectada.

2. Consulte los detalles de **ha** para obtener más información relacionada con el evento.

   En este ejemplo, la información relevante se encuentra en la tabla Eventos. La tabla muestra el evento "Conexión de conmutación por error de almacenamiento uno o más vínculos abajo", la hora en que se generó el evento y, de nuevo, el nodo desde el que se originó este evento.

Mediante la información de ubicación del nodo en los detalles de alta disponibilidad, solicite o realice una inspección física y reparación del problema de la conmutación por error del almacenamiento en los nodos del par de alta disponibilidad afectados.

Información relacionada

"Página de detalles Event"

"Roles y funcionalidades de usuario de Unified Manager"

Resolver problemas de volumen sin conexión

Este flujo de trabajo proporciona un ejemplo de cómo se puede evaluar y resolver un evento de volumen sin conexión que Unified Manager podría mostrar en la página del inventario Event Management. En esta situación, es un administrador que utiliza Unified Manager para solucionar uno o varios eventos sin conexión de volúmenes.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Es posible que los volúmenes se informen sin conexión por varios motivos:

- El administrador de SVM desconectó el volumen de manera deliberada.
- El nodo de clúster host del volumen está inactivo y la conmutación por error del almacenamiento a su par de alta disponibilidad también ha fallado.
- La máquina virtual de almacenamiento (SVM) que aloja el volumen se detiene porque el nodo que aloja el volumen raíz de esa SVM está inactivo.
- El agregado de host del volumen está inactivo debido a una falla simultánea de dos discos RAID.

Puede usar la página del inventario Event Management y las páginas de detalles Cluster/Health, Storage VM/Health y Volume/Health para confirmar o eliminar una o varias de estas posibilidades.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Gestión de eventos**.
2. En la página de inventario **Event Management**, seleccione **Eventos de disponibilidad activa**.
3. Haga clic en el enlace de hipertexto que se muestra para el evento volumen sin conexión.

   Se muestra la página de detalles Event para la incidencia de disponibilidad.

4. En esa página, compruebe las notas para indicar que el administrador de SVM ha puesto el volumen en cuestión sin conexión.
5. En la página de detalles **evento**, puede consultar la información de una o más de las siguientes tareas:
   - Revise la información que se muestra en el campo causa para obtener una posible guía de diagnóstico.

     En este ejemplo, la información del campo causa solo informa que el volumen está sin conexión.

   - Consulte el área Notas y actualizaciones para ver si el administrador de SVM ha desactivado el volumen de forma deliberada.
   - Haga clic en el origen del evento, en este caso el volumen que se notifica sin conexión, para obtener más información sobre ese volumen.
   - Asigne el evento a un administrador.
   - Reconozca el evento o, si procede, márquelo como solucionado.

Realización de acciones de diagnóstico para condiciones de sin conexión de un volumen

Después de navegar a la página de detalles Volume/Health de un volumen al que se informa que está sin conexión, puede buscar información adicional útil para diagnosticar la condición de volumen sin conexión.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Si el volumen que se informa sin conexión no se desconecta deliberadamente, ese volumen puede estar sin conexión por varios motivos.

A partir de la página de detalles Volume / Health del volumen sin conexión, puede ir a otras páginas y paneles para confirmar o eliminar las posibles causas:

- Haga clic en **volumen / Página de detalles Health** para determinar si el volumen está desconectado debido a que su nodo host está inactivo y la conmutación por error de almacenamiento a su par ha asociado también ha fallado.

  Consulte "Determinar si una condición de volumen sin conexión es causada por un nodo inactivo".

- Haga clic en **volumen / Estado** página de detalles vínculos para determinar si el volumen está sin conexión y su máquina virtual de almacenamiento host (SVM) se detiene porque el nodo que aloja el volumen raíz de esa SVM está inactivo.

  Consulte "Determinar si un volumen está sin conexión y la SVM se ha detenido debido a que el nodo está inactivo".

- Haga clic en **volumen / Página de detalles Health** para determinar si el volumen está fuera de línea debido a discos rotos en su agregado de host.

  Consulte "Determinar si un volumen está sin conexión debido a discos dañados en un agregado".

Información relacionada

"Roles y funcionalidades de usuario de Unified Manager"

Determinar si un volumen está sin conexión debido a que su nodo de host está inactivo

Puede utilizar la interfaz de usuario web de Unified Manager para confirmar o eliminar la posibilidad de que un volumen esté sin conexión debido a que su nodo de host está inactivo y que la conmutación por error del almacenamiento a su partner de pareja de alta disponibilidad no se puede realizar correctamente.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Para determinar si la condición de volumen sin conexión se debe a un fallo en el nodo de host y a una conmutación por error del almacenamiento posterior a una conmutación por error, realice las siguientes acciones:

Pasos

1. Busque y haga clic en el enlace de hipertexto que aparece bajo SVM en el panel **dispositivos relacionados** de la página de detalles **volumen / Salud** del volumen sin conexión.

   La página de detalles Storage VM / Health muestra información sobre la máquina virtual de almacenamiento (SVM) que aloja el volumen sin conexión.

2. En el panel **dispositivos relacionados** de la página de detalles **Storage VM / Health**, busque y haga clic en el enlace de hipertexto que aparece bajo volúmenes.

   La vista Estado: Todos los volúmenes muestra una tabla con información sobre todos los volúmenes alojados en la SVM.

3. En el encabezado de la columna **Estado: Todos los volúmenes** Ver estado, haga clic en el símbolo de filtro Y, a continuación, seleccione la opción **sin conexión**.

   Solo se muestran los volúmenes SVM que están en estado sin conexión.

4. En la vista Estado: Todos los volúmenes, haga clic en el símbolo de cuadrícula Y, a continuación, seleccione la opción **nodos de clúster**.

   Es posible que tenga que desplazarse por el cuadro de selección de cuadrícula para localizar la opción **nodos de clúster**.

   La columna Cluster Nodes se añade al inventario de volúmenes y muestra el nombre del nodo que aloja cada volumen sin conexión.

5. En la vista **Estado: Todos los volúmenes**, busque la lista del volumen sin conexión y, en su columna nodo de clúster, haga clic en el nombre de su nodo host.

La pestaña Nodes de la página Cluster / Health muestra el estado de la pareja de ha de los nodos a los que pertenece el nodo de alojamiento. El estado del nodo de host y el éxito de cualquier operación de conmutación por error del clúster se indican en la pantalla.

Después de confirmar que existe la condición de estado sin conexión del volumen porque su nodo de host está inactivo y se ha producido un error en la conmutación por error del almacenamiento al par de alta disponibilidad, póngase en contacto con el administrador o operador apropiado para reiniciar manualmente el nodo inactivo y solucionar el problema de conmutación por error del almacenamiento.

Determinar si un volumen está sin conexión y su SVM se ha detenido debido a que el nodo está inactivo

Puede usar la interfaz de usuario web de Unified Manager para confirmar o eliminar la posibilidad de que un volumen esté sin conexión debido a que su máquina virtual de almacenamiento (SVM) de host se detiene debido a que el nodo que aloja el volumen raíz de esa SVM está inactivo.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Para determinar si la condición del volumen sin conexión fue causada por que la SVM de host se detuvo porque el nodo donde se aloja el volumen raíz de esa SVM está inactivo, debe realizar las siguientes acciones:

Pasos

1. Busque y haga clic en el enlace de hipertexto que aparece bajo la SVM en el panel **dispositivos relacionados** de la página de detalles **volumen / Salud** del volumen sin conexión.

   La página de detalles de Storage VM / Health muestra el estado «'running'» o «Mostrad» de la SVM de acogida. Si el estado de la SVM está en ejecución, la condición del volumen sin conexión no es causada por el nodo que aloja el volumen raíz de esa SVM que está inactivo.

2. Si el estado de la SVM es detenido, haga clic en **Ver SVM** para identificar aún más la causa de la SVM host que se detiene.
3. En el encabezado de columna * Health: All Storage VMs* view SVM, haga clic en el símbolo de filtro Y a continuación, escriba el nombre de la SVM detenida.

   La información para esa SVM se muestra en una tabla.

4. En la vista **Health: All Storage VMs**, haga clic en Y, a continuación, seleccione la opción **volumen raíz**.

   La columna Root Volume se añade al inventario de SVM y muestra el nombre del volumen raíz de la SVM detenida.

5. En la columna volumen raíz, haga clic en el nombre del volumen raíz para mostrar la página de detalles **Storage VM / Health** correspondiente a ese volumen.

   Si el estado del volumen raíz de SVM es (en línea), la condición del volumen original sin conexión no se debe porque el nodo que aloja el volumen raíz de esa SVM está inactivo.

6. Si el estado del volumen raíz de la SVM es (sin conexión), busque y haga clic en el enlace de hipertexto

que se muestra bajo agregado en el panel dispositivos relacionados de la página de detalles Volume / Health del volumen raíz de la SVM.

7. Busque y haga clic en el enlace de hipertexto que aparece bajo nodo en el panel **dispositivos relacionados** de la página de detalles **agregado / Salud** del agregado.

   En la pestaña Nodes de la página Cluster / Health se muestra el estado de la pareja de nodos a la que pertenece el nodo de alojamiento del volumen raíz de SVM. El estado del nodo se indica en la pantalla.

Una vez que confirma que la condición de sin conexión del volumen está provocada por la condición de SVM del host de ese volumen, que sí está provocada por el nodo que aloja el volumen raíz de esa SVM que está inactivo, póngase en contacto con el administrador o operador apropiado para reiniciar manualmente el nodo inactivo.

Determinar si un volumen está sin conexión debido a discos dañados en un agregado

Puede utilizar la interfaz de usuario web de Unified Manager para confirmar o eliminar la posibilidad de que un volumen esté sin conexión debido a que los problemas de disco RAID han desconectado su agregado de host.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Para determinar si la condición del volumen sin conexión está provocada por problemas de disco RAID que desconectan el agregado de alojamiento, realice las siguientes acciones:

Pasos

1. Busque y haga clic en el enlace de hipertexto que aparece bajo agregado en el panel **dispositivos relacionados** de la página de detalles **volumen / Salud**.

   La página de detalles Aggregate / Health muestra el estado en línea o sin conexión del agregado de host. Si el estado del agregado es en línea, los problemas del disco RAID no son la causa por la que el volumen se encuentra sin conexión.

2. Si el estado del agregado es sin conexión, haga clic en **Información del disco** y busque eventos de disco rotos en la lista **Eventos** de la ficha **Información del disco**.
3. Para identificar los discos rotos, haga clic en el enlace de hipertexto que aparece bajo nodo en el panel **dispositivos relacionados**.

   Se muestra la página de detalles Cluster / Health.

4. Haga clic en **discos** y, a continuación, seleccione **roto** en el panel **Filtros** para enumerar todos los discos en estado roto.

   Si los discos en estado roto causaron el estado sin conexión del agregado host, el nombre del agregado se muestra en la columna del agregado afectado.

Después de confirmar que la condición del volumen fuera de línea está provocada por discos RAID rotos y el agregado de host resultante fuera de línea, póngase en contacto con el administrador o operador apropiado para sustituir manualmente los discos rotos y volver a poner el agregado en línea.

Resolver problemas de capacidad

Este flujo de trabajo proporciona un ejemplo de cómo puede resolver un problema de capacidad. En esta situación, usted es administrador o operador y accede a la página Unified Manager Dashboard para ver si alguno de los objetos de almacenamiento supervisados tiene problemas de capacidad. Desea determinar la posible causa del problema y su resolución.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

En la página Panel, busque un evento de error "'espacio de volumen lleno'" en el panel capacidad de la lista desplegable eventos.

Pasos

1. En el panel **Capacity** de la página **Dashboard**, haga clic en el nombre del evento de error Volume Space Full.

   Se muestra la página de detalles Event para el error.

2. En la página de detalles **evento**, puede realizar una o más de las siguientes tareas:
   - Revise el mensaje de error en el campo causa y haga clic en las sugerencias en acciones correctivas sugeridas para revisar las descripciones de posibles soluciones.
   - Haga clic en el nombre del objeto, en este caso un volumen, en el campo Source para obtener detalles del objeto.
   - Busque las notas que se podrían haber añadido acerca de este evento.
   - Agregar una nota al evento.
   - Asigne el evento a otro usuario.
   - Reconozca el evento.
   - Marque el evento como solucionado.

Información relacionada

"Página de detalles Event"

Ejecución de acciones correctivas sugeridas para un volumen completo

Después de recibir un evento de error «'espacio de volumen completo'», revise las acciones correctivas sugeridas en la página de detalles del evento y decida realizar una de las acciones sugeridas.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Un usuario con cualquier rol puede realizar todas las tareas en este flujo de trabajo que utiliza Unified Manager.

En este ejemplo, ha visto un evento de error de espacio de volumen completo en la página del inventario de

Unified Manager Event Management y ha hecho clic en el nombre del evento.

Entre las posibles acciones para solucionarlos que se pueden llevar a cabo en un volumen completo se encuentran las siguientes:

- Habilitar el crecimiento automático, la deduplicación o la compresión en el volumen
- Cambiar el tamaño o mover el volumen
- Eliminar o mover datos del volumen

Si bien todas estas acciones deben realizarse desde ONTAP System Manager o desde la interfaz de línea de comandos de ONTAP, puede usar Unified Manager para buscar información que pueda ser necesario determinar qué acciones deben realizarse.

Pasos

1. En la página de detalles **evento**, haga clic en el nombre del volumen en el campo origen para ver detalles sobre el volumen afectado.
2. En la página de detalles **Volume / Health**, haga clic en **Configuration** y compruebe que la deduplicación y la compresión ya están activadas en el volumen.

   Decide cambiar el tamaño del volumen.

3. En el panel **dispositivos relacionados**, haga clic en el nombre del agregado de alojamiento para ver si el agregado puede acomodar un volumen mayor.
4. En la página de detalles **Aggregate / Health**, puede ver que el agregado que aloja el volumen completo tiene suficiente capacidad disponible, por lo que utiliza System Manager de ONTAP para cambiar el tamaño del volumen, por lo que aumenta la capacidad.

Información relacionada

"Página de detalles Event"

Gestión de umbrales de salud

Puede configurar valores de umbral de estado global para todos los agregados, volúmenes y qtrees a fin de realizar un seguimiento de cualquier incumplimiento de umbral de estado.

Los umbrales del estado de la capacidad del almacenamiento

Un umbral de estado de la capacidad de almacenamiento es el punto en el que Unified Manager Server genera eventos para informar de cualquier problema de capacidad con los objetos de almacenamiento. Es posible configurar alertas para que envíen notificaciones cuando se produzcan dichos eventos.

Los umbrales de estado de la capacidad de almacenamiento para todos los agregados, volúmenes y qtrees se establecen con los valores predeterminados. Puede cambiar la configuración según sea necesario para un objeto o un grupo de objetos.

Configuración de los valores del umbral de estado global

Puede configurar las condiciones de umbral de estado global para la capacidad, el

crecimiento, la reserva de Snapshot, las cuotas y los inodos para supervisar de manera eficaz el agregado, el volumen y el tamaño de qtree. También se puede editar la configuración para generar eventos que superen los umbrales de desfase.

La configuración de umbral de estado global se aplica a todos los objetos con los que están asociados, como agregados, volúmenes, etc. Cuando se sobrepasan los umbrales, se genera un evento y, si se configuran alertas, se envía una notificación de alerta. Los valores predeterminados de umbral se establecen en valores recomendados, pero se pueden modificar para generar eventos a intervalos que satisfagan sus necesidades específicas. Cuando se cambian los umbrales, los eventos se generan o se vuelven obsoletos en el próximo ciclo de supervisión.

Se puede acceder a los ajustes del umbral de estado global desde la sección umbrales de sucesos del menú de navegación izquierdo. También puede modificar la configuración del umbral para objetos individuales, desde la página de inventario o la página de detalles de ese objeto.

- Para obtener más información, consulte "Configuración de los valores de umbral de estado globales del agregado".

  Puede configurar la configuración del umbral de estado para la capacidad, el crecimiento y las copias Snapshot de todos los agregados para realizar un seguimiento de cualquier incumplimiento del umbral.

- Para obtener más información, consulte "Configurar los valores de umbral de estado de volúmenes globales".

  Puede editar la configuración del umbral de estado para la capacidad, las copias de Snapshot, las cuotas de qtree, el crecimiento del volumen, el espacio de reserva de sobrescritura, e inodos, para todos los volúmenes, para realizar un seguimiento de cualquier incumplimiento de umbral.

- Para obtener más información, consulte "Configuración de los valores de umbral de estado globales para qtrees".

  Puede editar la configuración del umbral de estado de la capacidad de todos los qtrees para realizar un seguimiento de cualquier incumplimiento del umbral.

- Para obtener más información, consulte "Edición de la configuración del umbral de mantenimiento de posposición para relaciones de protección no administradas".

  Puede aumentar o reducir el porcentaje de tiempo de retraso de advertencia o error para que los eventos se generen a intervalos más adecuados a sus necesidades.

Configuración de los valores de umbral de estado globales del agregado

Puede configurar valores de umbral de estado global para todos los agregados para realizar un seguimiento de cualquier incumplimiento de umbral. Se generan los eventos adecuados para incumplimiento de umbrales y puede tomar medidas preventivas basadas en estos eventos. Puede configurar los valores globales basándose en la configuración de prácticas recomendadas para los umbrales que se aplican a todos los agregados supervisados.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Al configurar las opciones globalmente, se modifican los valores predeterminados de los objetos. Sin embargo, si los valores predeterminados se han cambiado a nivel de objeto, los valores globales no se modifican.

Las opciones de umbral tienen valores predeterminados para una mejor supervisión, sin embargo, puede cambiar los valores para adaptarlos a los requisitos de su entorno.

Cuando se habilita la opción Autofila en los volúmenes que residen en el agregado, los umbrales de capacidad del agregado se consideran sin infracción en función del tamaño máximo del volumen establecido por el crecimiento automático, no según el tamaño del volumen original.

Los valores de umbral de estado no se aplican al agregado raíz del nodo.

Pasos

1. En el panel de navegación izquierdo, haga clic en **umbrales de evento** > **agregado**.
2. Configure los valores de umbral adecuados para la capacidad, el crecimiento y las copias Snapshot.
3. Haga clic en **Guardar**.

Información relacionada

"Adición de usuarios"

Configurar los valores de umbral de estado de volúmenes globales

Puede configurar los valores de umbral de estado global para todos los volúmenes para realizar un seguimiento de cualquier incumplimiento de umbral. Se generan eventos apropiados para las infracciones de los umbrales de salud y puede tomar medidas preventivas basadas en estos eventos. Puede configurar los valores globales a partir de la configuración de prácticas recomendadas para los umbrales que se aplican a todos los volúmenes supervisados.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

La mayoría de las opciones de umbral tienen valores predeterminados para una mejor supervisión. Sin embargo, puede cambiar los valores para adaptarlos a los requisitos de su entorno.

Tenga en cuenta que cuando se habilita la opción Autofila en un volumen, se consideran límites de capacidad según el tamaño máximo de volumen establecido por crecimiento automático, no según el tamaño del volumen original.

El valor predeterminado de 1000 copias de Snapshot se aplica solo a los volúmenes FlexVol cuando la versión de ONTAP es 9.4 o posterior, y a los volúmenes FlexGroup cuando la versión de ONTAP es 9.8 y posterior. En los clústeres instalados con versiones anteriores del software ONTAP, el número máximo es de 250 copias snapshot por volumen. En estas versiones anteriores, Unified Manager interpreta este número 1000 (y cualquier número entre 1000 y 250) como 250; lo que significa que continuará recibiendo eventos cuando el número de copias Snapshot llegue a 250. Si desea establecer este umbral en menos de 250 para estas versiones anteriores, debe establecer el umbral en 250 o inferior aquí, en la vista Estado: Todos los volúmenes o en la página de detalles volumen / Estado.

Pasos

1. En el panel de navegación izquierdo, haga clic en **umbrales de evento** > **volumen**.
2. Configurar los valores de umbral adecuados para la capacidad, las copias Snapshot, las cuotas de qtree, el crecimiento de volumen y los inodos.
3. Haga clic en **Guardar**.

Información relacionada

"Adición de usuarios"

Configuración de los valores de umbral de estado globales para qtrees

Puede configurar los valores de umbral de estado global de todos los qtrees para realizar un seguimiento de cualquier incumplimiento de umbral. Se generan eventos apropiados para las infracciones de los umbrales de salud y puede tomar medidas preventivas basadas en estos eventos. Puede configurar los valores globales basándose en la configuración de mejores prácticas para los umbrales que se aplican a todos los qtrees supervisados.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Las opciones de umbral tienen valores predeterminados para una mejor supervisión, sin embargo, puede cambiar los valores para adaptarlos a los requisitos de su entorno.

Los eventos se generan para un qtree solo cuando se ha establecido una cuota de Qtree o una cuota predeterminada en él. Los eventos no se generan si el espacio definido en una cuota de usuario o cuota de grupo ha superado el umbral.

Pasos

1. En el panel de navegación izquierdo, haga clic en **umbrales de evento** > **Qtree**.
2. Configure los valores de umbral de capacidad adecuados.
3. Haga clic en **Guardar**.

Configuración de la configuración del umbral de desfase para relaciones de protección no administradas

Puede editar la configuración global predeterminada de umbral de advertencia de desfase y de estado de error para relaciones de protección no administradas, de modo que los eventos se generen a intervalos apropiados para sus necesidades.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

El tiempo de desfase no debe superar el intervalo de programación de transferencia definido. Por ejemplo, si la programación de transferencia es por hora, el intervalo de demora no debe ser superior a una hora. El umbral de desfase especifica un porcentaje que no debe superar el tiempo de desfase. Con el ejemplo de una hora, si el umbral de desfase se define como 150%, recibirá un evento cuando el tiempo de retraso sea superior a 1.5 horas.

La configuración descrita en esta tarea se aplica globalmente a todas las relaciones de protección no administradas. La configuración no se puede especificar y aplicar exclusivamente a una relación de protección no administrada.

Pasos

1. En el panel de navegación izquierdo, haga clic en **umbrales de evento** > **relación**.
2. Aumente o disminuya el porcentaje de tiempo de demora de error o advertencia global predeterminado según sea necesario.
3. Para desactivar la activación de un evento de advertencia o error desde cualquier cantidad de umbral de desfase, desactive la casilla situada junto a **habilitado**.
4. Haga clic en **Guardar**.

Información relacionada

"Adición de usuarios"

Editar la configuración de umbral de estado de cada agregado

Puede editar la configuración del umbral de estado para la capacidad del agregado, el crecimiento y las copias Snapshot de uno o más agregados. Cuando se supera un umbral, se generan alertas y se reciben notificaciones. Estas notificaciones le ayudan a tomar medidas preventivas basadas en el evento generado.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Basándose en los cambios de los valores de umbral, los eventos se generan o se vuelven obsoletos en el siguiente ciclo de supervisión.

Cuando se habilita la opción Autofila en los volúmenes que residen en el agregado, los umbrales de capacidad del agregado se consideran sin infracción en función del tamaño máximo del volumen establecido por el crecimiento automático, no según el tamaño del volumen original.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **agregados**.
2. En la vista **Estado: Todos los agregados**, seleccione uno o más agregados y, a continuación, haga clic en **Editar umbrales**.
3. En el cuadro de diálogo **Editar umbrales agregados**, edite la configuración de umbral de una de las siguientes opciones: Capacidad, crecimiento o copias Snapshot seleccionando la casilla de verificación apropiada y modificando la configuración.
4. Haga clic en **Guardar**.

Información relacionada

"Adición de usuarios"

Editar la configuración de umbral de estado de cada volumen

Es posible editar la configuración del umbral de estado para la capacidad de volumen, el

crecimiento, la cuota y la reserva de espacio de uno o más volúmenes. Cuando se supera un umbral, se generan alertas y se reciben notificaciones. Estas notificaciones le ayudan a tomar medidas preventivas basadas en el evento generado.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Basándose en los cambios de los valores de umbral, los eventos se generan o se vuelven obsoletos en el siguiente ciclo de supervisión.

Tenga en cuenta que cuando se habilita la opción Autofila en un volumen, se consideran límites de capacidad según el tamaño máximo de volumen establecido por crecimiento automático, no según el tamaño del volumen original.

> El valor predeterminado de 1000 copias de Snapshot se aplica solo a los volúmenes FlexVol cuando la versión de ONTAP es 9.4 o posterior, y a los volúmenes FlexGroup cuando la versión de ONTAP es 9.8 y posterior. En los clústeres instalados con versiones anteriores del software ONTAP, el número máximo es de 250 copias snapshot por volumen. En estas versiones anteriores, Unified Manager interpreta este número 1000 (y cualquier número entre 1000 y 250) como 250; lo que significa que continuará recibiendo eventos cuando el número de copias Snapshot llegue a 250. Si desea establecer este umbral en menos de 250 para estas versiones anteriores, debe establecer el umbral en 250 o inferior aquí, en la vista Estado: Todos los volúmenes o en la página de detalles volumen / Estado.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En la vista **Estado: Todos los volúmenes**, seleccione uno o más volúmenes y, a continuación, haga clic en **Editar umbrales**.
3. En el cuadro de diálogo **Editar umbrales de volumen**, edite la configuración de umbral de una de las siguientes opciones: Capacidad, copias Snapshot, cuota de qtree, crecimiento o inodos. Para ello, active la casilla de verificación correspondiente y, a continuación, modifique la configuración.
4. Haga clic en **Guardar**.

Información relacionada

"Adición de usuarios"

Editar la configuración de umbral de estado de qtree individual

Es posible editar la configuración del umbral de estado para la capacidad de qtrees de uno o varios qtrees. Cuando se supera un umbral, se generan alertas y se reciben notificaciones. Estas notificaciones le ayudan a tomar medidas preventivas basadas en el evento generado.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Basándose en los cambios de los valores de umbral, los eventos se generan o se vuelven obsoletos en el siguiente ciclo de supervisión.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **Qtrees**.
2. En la vista **capacidad: All Qtrees**, seleccione uno o más qtrees y, a continuación, haga clic en **Editar umbrales**.
3. En el cuadro de diálogo **Edit Qtree Thresholds**, cambie los umbrales de capacidad para el qtree o qtrees seleccionados y haga clic en **Save**.

> También puede establecer umbrales de qtree individuales en la pestaña Qtrees en la página de detalles Storage VM / Health.

Gestión de los objetivos de seguridad del clúster

Unified Manager proporciona un panel que identifica la seguridad de los clústeres, las máquinas virtuales de almacenamiento (SVM) y los volúmenes de ONTAP según las recomendaciones definidas en la *Guía de fortalecimiento de seguridad de NetApp para ONTAP 9*.

El objetivo de la consola de seguridad es mostrar las áreas en las que los clústeres de ONTAP no estén alineados con las directrices recomendadas por NetApp para poder resolver estos problemas potenciales. En la mayoría de los casos, se solucionarán los problemas con ONTAP System Manager o la CLI de ONTAP. Es posible que su organización no siga todas las recomendaciones, por lo que en algunos casos no necesitará hacer ningún cambio.

Consulte el "Guía de fortalecimiento de la seguridad de NetApp para ONTAP 9" (TR-4569) para obtener recomendaciones y soluciones detalladas.

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

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

Qué criterios de seguridad se están evaluando

En general, los criterios de seguridad de los clústeres, las máquinas virtuales de almacenamiento (SVM) y los volúmenes de ONTAP se evalúan con arreglo a las recomendaciones definidas en la *Guía de seguridad reforzada de NetApp para ONTAP 9*.

Algunas de las comprobaciones de seguridad incluyen:

- Si un clúster utiliza un método de autenticación segura, como SAML
- si los clústeres con una relación entre iguales tienen cifrado de comunicación
- Si un equipo virtual de almacenamiento tiene habilitado el registro de auditoría
- si sus volúmenes tienen activado el cifrado de software o hardware

Consulte los temas sobre categorías de cumplimiento y la "Guía de fortalecimiento de la seguridad de NetApp para ONTAP 9" para obtener información detallada.

Los eventos de actualización notificados desde la plataforma Active IQ también se consideran eventos de seguridad. Estos eventos identifican problemas en los que la resolución requiere actualizar el software ONTAP, el firmware del nodo o el software del sistema operativo (para avisos de seguridad). Estos eventos no se muestran en el panel Seguridad, pero están disponibles en la página de inventario de Event Management.

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

Categorías de cumplimiento de clusters

En esta tabla se describen los parámetros de cumplimiento de normativas de seguridad del clúster que Unified Manager evalúa, la recomendación de NetApp y si el parámetro afecta a la determinación general del clúster que se está quejando o no.

El hecho de que haya SVM no compatibles en un clúster afectará al valor de cumplimiento de normativas para el clúster. Por lo tanto, en algunos casos puede que necesite solucionar problemas de seguridad con una SVM antes de que la seguridad del clúster se vea como compatible.

Tenga en cuenta que no todos los parámetros enumerados a continuación aparecen para todas las instalaciones. Por ejemplo, si no tiene clústeres con una relación entre iguales o si ha deshabilitado AutoSupport en un clúster, no verá los elementos de transporte HTTPS de Cluster peering o AutoSupport en la página de interfaz de usuario.

Parámetro	Descripción	Recomendación	Afecta a Cluster Compliance
FIPS global	Indica si el modo de cumplimiento de normativas Global FIPS (estándar de procesamiento de información federal) 140-2 está habilitado o deshabilitado. Cuando FIPS está habilitada, TLSv1 y SSLv3 están desactivados y sólo se permiten TLSv1.1 y TLSv1.2.	Activado	Sí
Telnet	Indica si el acceso Telnet al sistema está activado o desactivado. NetApp recomienda Secure Shell (SSH) para el acceso remoto seguro.	Deshabilitado	Sí
Configuración SSH no segura	Indica si SSH utiliza cifrados no seguros, por ejemplo, cifrados que empiecen por *cbc.	No	Sí

Parámetro	Descripción	Recomendación	Afecta a Cluster Compliance
Banner de inicio de sesión	Indica si el banner de inicio de sesión está habilitado o deshabilitado para los usuarios que acceden al sistema.	Activado	Sí
Conexión de clústeres entre iguales	Indica si la comunicación entre clústeres con una relación entre iguales está cifrada o no cifrada. El cifrado debe configurarse en los clústeres de origen y destino para que este parámetro se considere compatible.	Cifrado	Sí
Protocolo de hora de red	Indica si el clúster tiene uno o más servidores NTP configurados. Para redundancia y mejor servicio, NetApp recomienda asociar al menos tres servidores NTP al clúster.	Configurado	Sí
OCSP	Indica si hay aplicaciones en ONTAP que no están configuradas con OCSP (protocolo de estado de certificado en línea) y, por lo tanto, las comunicaciones no están cifradas. Se enumeran las aplicaciones no conformes.	Activado	No
Registro de auditoría remota	Indica si el reenvío de registros (Syslog) está cifrado o no cifrado.	Cifrado	Sí
Transporte HTTPS AutoSupport	Indica si se utiliza HTTPS como el protocolo de transporte predeterminado para enviar mensajes de AutoSupport al soporte de NetApp.	Activado	Sí

Parámetro	Descripción	Recomendación	Afecta a Cluster Compliance
Usuario administrador predeterminado	Indica si el usuario administrador predeterminado (integrado) está activado o desactivado. NetApp recomienda bloquear (deshabilitar) cualquier cuenta integrada que no sea innecesaria.	Deshabilitado	Sí
Usuarios de SAML	Indica si SAML está configurado. SAML permite configurar la autenticación multifactor (MFA) como método de inicio de sesión para el inicio de sesión único.	No	No
Usuarios de Active Directory	Indica si está configurado Active Directory. Active Directory y LDAP son los mecanismos de autenticación preferidos para los usuarios que acceden a clústeres.	No	No
Usuarios LDAP	Indica si LDAP está configurado. Active Directory y LDAP son los mecanismos de autenticación preferidos para los usuarios que gestionan clústeres a través de usuarios locales.	No	No
Usuarios certificados	Indica si se configuró un usuario de certificado para iniciar sesión en el clúster.	No	No
Usuarios locales	Indica si se han configurado usuarios locales para iniciar sesión en el clúster.	No	No

Parámetro	Descripción	Recomendación	Afecta a Cluster Compliance
Shell remoto	Indica si RSH está activado. Por motivos de seguridad, se debe desactivar RSH. Se recomienda Secure Shell (SSH) para acceso remoto seguro.	Deshabilitado	Sí
MD5 en uso	Indica si las cuentas de usuario de ONTAP utilizan la función Hash MD5 menos segura. Se prefiere la migración de cuentas de usuario hash MD5 a la función hash criptográfica más segura como SHA-512.	No	Sí
Tipo de emisor de certificados	Indica el tipo de certificado digital utilizado.	Firmado por CA	No

Categorías de cumplimiento de normativas para máquinas virtuales de almacenamiento

En esta tabla se describen los criterios de cumplimiento de la seguridad de la máquina virtual de almacenamiento (SVM) que evalúa Unified Manager, la recomendación de NetApp y si el parámetro afecta a la determinación general de la SVM que se está quejando o no.

Parámetro	Descripción	Recomendación	Afecta a SVM Compliance
Registro de auditoría	Indica si el registro de auditoría está activado o desactivado.	Activado	Sí
Configuración SSH no segura	Indica si SSH utiliza cifrados no seguros, por ejemplo, cifrados que empiecen por `cbc*`.	No	Sí
Banner de inicio de sesión	Indica si el banner de inicio de sesión está habilitado o deshabilitado para los usuarios que acceden a las SVM del sistema.	Activado	Sí

Parámetro	Descripción	Recomendación	Afecta a SVM Compliance
Cifrado LDAP	Indica si el cifrado LDAP está activado o desactivado.	Activado	No
Autenticación NTLM	Indica si la autenticación NTLM está activada o desactivada.	Activado	No
Firma de carga útil LDAP	Indica si la firma de carga útil LDAP está activada o desactivada.	Activado	No
Configuración DE CHAP	Indica si CHAP está habilitado o deshabilitado.	Activado	No
Kerberos V5	Indica si la autenticación Kerberos V5 está activada o desactivada.	Activado	No
Autenticación NIS	Indica si se ha configurado el uso de la autenticación NIS.	Deshabilitado	No
Estado de FPolicy activo	Indica si se ha creado o no FPolicy.	Sí	No
Cifrado SMB habilitado	Indica si la firma y el sellado SMB no están habilitados.	Sí	No
Firma SMB habilitada	Indica si la firma SMB no está habilitada.	Sí	No

Categorías de cumplimiento de volúmenes

En esta tabla, se describen los parámetros de cifrado de volúmenes que Unified Manager evalúa para determinar si los datos de los volúmenes están protegidos de forma adecuada para que usuarios no autorizados puedan acceder a ellos.

Tenga en cuenta que los parámetros de cifrado de volúmenes no afectan a si el clúster o el equipo virtual de almacenamiento se consideran conformes.

Parámetro	Descripción
Cifrado por software	Muestra el número de volúmenes protegidos con las soluciones de cifrado de software de cifrado de volúmenes de NetApp (NVE) o cifrado de agregados de NetApp (NAE).
Cifrado por hardware	Muestra la cantidad de volúmenes protegidos con cifrado de hardware de cifrado de almacenamiento de NetApp (NSE).
Cifrado de software y hardware	Muestra el número de volúmenes protegidos por cifrado de software y hardware.
No cifrado	Muestra el número de volúmenes que no están cifrados.

Qué significa no cumplir con las normativas

Los clústeres y las máquinas virtuales de almacenamiento (SVM) no se consideran conformes cuando no se cumple ninguno de los criterios de seguridad evaluados con respecto a las recomendaciones definidas en la *Guía de seguridad reforzada de NetApp para ONTAP 9*. Además, se considera que un clúster no es compatible cuando se Marca ninguna SVM como no compatible.

Los iconos de estado de las tarjetas de seguridad tienen los siguientes significados en relación con su cumplimiento:

- - El parámetro está configurado como se recomienda.
- - El parámetro no está configurado como se recomienda.
- - O bien la funcionalidad no está habilitada en el clúster, o bien el parámetro no está configurado como recomendado, pero este parámetro no contribuye al cumplimiento del objeto.

Tenga en cuenta que el estado del cifrado de volúmenes no contribuye a si el clúster o SVM se consideran conformes.

Visualización del estado de seguridad para clústeres y máquinas virtuales de almacenamiento

Active IQ Unified Manager le permite ver el estado de seguridad de los objetos de almacenamiento en su entorno desde diferentes puntos de la interfaz. Puede recopilar y analizar información e informes a partir de parámetros definidos, y detectar comportamientos sospechosos o cambios del sistema no autorizados en los clústeres supervisados y las máquinas virtuales de almacenamiento.

Para conocer las recomendaciones de seguridad, consulte "Guía de fortalecimiento de la seguridad de NetApp para ONTAP 9"

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

Como administrador del sistema, puede utilizar la página **Seguridad** para obtener visibilidad sobre la seguridad de los clústeres de ONTAP y los equipos virtuales de almacenamiento en los centros de datos y los sitios. Los objetos admitidos son clúster, máquinas virtuales de almacenamiento y volúmenes. Siga estos pasos:

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Panel**.
2. En función de si desea ver el estado de seguridad de todos los clústeres supervisados o de un único clúster, seleccione **todos los clústeres** o seleccione un único clúster en el menú desplegable.
3. Haga clic en la flecha derecha del panel **Seguridad**. Aparece la página Seguridad.

Haga clic en los gráficos de barras, cuenta y `View Reports` Los enlaces le llevan a la página volúmenes, clústeres o máquinas virtuales de almacenamiento para ver los detalles correspondientes o generar informes, según sea necesario.

La página Seguridad muestra los siguientes paneles:

- **Cluster Compliance**: El estado de seguridad (número de clústeres que cumplen o no son compatibles) de todos los clústeres de un centro de datos
- **Storage VM Compliance**: Estado de seguridad (número de equipos virtuales de almacenamiento que cumplen o no cumplen con las normativas) para todos los equipos virtuales de almacenamiento de su centro de datos
- **Cifrado de volumen**: El estado de cifrado de volumen (número de volúmenes cifrados o no cifrados) de todos los volúmenes de su entorno
- **Volume Anti-ransomware Status**: El estado de seguridad (número de volúmenes con antiransomware activado o desactivado) de todos los volúmenes del entorno
- **Autenticación de clúster y certificados**: Número de clústeres que usan cada tipo de método de autenticación, como SAML, Active Directory o mediante certificados y autenticación local. El panel también muestra el número de clústeres cuyos certificados han caducado o están a punto de expirar en 60 días.

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

La página de detalles **Clusters / Security** le permite ver el estado de cumplimiento de seguridad a nivel de clúster.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **almacenamiento > Clusters**.
2. Seleccione **Ver > Seguridad > todos los clústeres**.

Parámetros de seguridad predeterminados, como FIPS global, Telnet, configuración de SSH insegura, banner de inicio de sesión, protocolo de hora de red, Se muestran los servicios de transporte HTTPS de AutoSupport, así como el estado de caducidad del certificado del clúster.

Haga clic en el ⋮ Más opciones y elija ver los detalles de seguridad en la página **Seguridad** de Unified Manager o en System Manager. Debe tener credenciales válidas para ver los detalles en System Manager.

> ⓘ Si un clúster tiene un certificado caducado, puede hacer clic en `expired` En **validez del certificado de clúster**, y renuévelo desde System Manager (9.10.1 y posterior). No puede hacer clic en `expired` Si la instancia de System Manager tiene una versión anterior a 9.10.1.

Consulte los detalles de seguridad de todos los clústeres desde la página de máquinas virtuales de almacenamiento

La página de detalles **Storage VMs / Security** le permite ver el estado de cumplimiento de la seguridad a nivel de VM de almacenamiento.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **almacenamiento > Storage VMs**.
2. Seleccione **Ver > Seguridad > todas las VM de almacenamiento**. Se muestra una lista de los clústeres con los parámetros de seguridad.

Es posible tener una vista predeterminada del cumplimiento de seguridad de las máquinas virtuales de almacenamiento comprobando los parámetros de seguridad, como las máquinas virtuales de almacenamiento, el clúster, el banner de inicio de sesión, el registro de auditoría y la configuración de SSH no segura.

Haga clic en el ⋮ Más opciones y elija ver los detalles de seguridad en la página **Seguridad** de Unified Manager o en System Manager. Debe tener credenciales válidas para ver los detalles en System Manager.

Para obtener detalles de seguridad antiransomware para volúmenes y máquinas virtuales de almacenamiento, consulte "Ver el estado antiransomware de todos los volúmenes y las máquinas virtuales de almacenamiento".

Ver eventos de seguridad que pueden requerir actualizaciones de software o firmware

Hay determinados eventos de seguridad que tienen un área de impacto de "'Upgrade'". Estos eventos se notifican en la plataforma Active IQ e identifican problemas en los que la solución requiere actualizar el software ONTAP, el firmware del nodo o el software del sistema operativo (para avisos de seguridad).

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Quizás desee realizar una acción correctiva inmediata para algunos de estos problemas, mientras que otros pueden esperar hasta el siguiente mantenimiento programado. Puede ver todos estos eventos y asignarlos a los usuarios que puedan resolver los problemas. Además, si hay determinados eventos de actualización de seguridad sobre los que no desea recibir notificaciones, esta lista puede ayudarle a identificar esos eventos para que pueda deshabilitarlos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Gestión de eventos**.

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

2. En el menú Ver, seleccione **Eventos de actualización**.

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

Ver cómo se gestiona la autenticación de usuario en todos los clústeres

En la página Seguridad, se muestran los tipos de autenticación que se usan para autenticar usuarios en cada clúster y el número de usuarios que acceden al clúster

mediante cada tipo. Esto permite verificar que la autenticación de usuarios se está realizando de forma segura según lo definido por la organización.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Panel**.
2. En la parte superior del panel, seleccione **todos los clústeres** en el menú desplegable.
3. Haga clic en la flecha derecha del panel **Seguridad** y aparecerá la página **Seguridad**.
4. Consulte la tarjeta **autenticación de clúster** para ver el número de usuarios que acceden al sistema utilizando cada tipo de autenticación.
5. Consulte la tarjeta **Seguridad del clúster** para ver los mecanismos de autenticación que se utilizan para autenticar usuarios en cada clúster.

Si hay algunos usuarios que acceden al sistema mediante un método no seguro o utilizan un método que no recomienda NetApp, puede deshabilitar el método.

Ver el estado de cifrado de todos los volúmenes

Puede ver una lista de todos los volúmenes y su estado de cifrado actual para poder determinar si los datos de los volúmenes están protegidos correctamente para que otros usuarios no autorizados puedan acceder a ellos.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

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

- Software: Volúmenes protegidos con las soluciones de cifrado por software de cifrado de volúmenes de NetApp (NVE) o cifrado de agregados de NetApp (NAE).
- Hardware: Volúmenes protegidos con cifrado de hardware de cifrado del almacenamiento de NetApp (NSE).
- Software y hardware: Volúmenes protegidos por cifrado de software y hardware.
- None: Volúmenes que no están cifrados.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En el menú Ver, seleccione **Estado** > **cifrado de volúmenes**
3. En la vista **Estado: Cifrado de volúmenes**, ordene el campo **Tipo de cifrado** o utilice el filtro para mostrar los volúmenes que tienen un tipo de cifrado específico, o que no están cifrados (Tipo de cifrado ""Ninguno"").

Ver el estado antiransomware de todos los volúmenes y máquinas virtuales de almacenamiento

Puede ver una lista de todos los volúmenes y máquinas virtuales de almacenamiento (SVM) y su estado actual antiransomware para poder determinar si los datos de sus volúmenes y SVM están protegidos adecuadamente de ataques de ransomware.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Para obtener más información sobre los diferentes Estados del antiransomware, consulte "ONTAP: Habilite el antiransomware".

Consulte detalles de seguridad de todos los volúmenes con detección antiransomware

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En el menú Ver, seleccione **Salud** > **Seguridad** > **Antiransomware**
3. En la vista * Security: Anti-ransomware*, puede ordenar por los distintos campos o usar el filtro.

> No se admite el ransomware para volúmenes sin conexión, volúmenes restringidos, volúmenes SnapLock, volúmenes FlexGroup, volúmenes FlexCache, Volúmenes solo SAN, volúmenes de máquinas virtuales de almacenamiento detenidas, volúmenes raíz de las máquinas virtuales de almacenamiento o volúmenes de protección de datos.

Consulte detalles de seguridad de todas las máquinas virtuales de almacenamiento con detección antiransomware

Pasos

1. En el panel de navegación de la izquierda, haga clic en **almacenamiento > Storage VMs**.
2. Seleccione **Ver > Seguridad > Anti-ransomware**. Se muestra una lista de las SVM con el estado antiransomware.

> La supervisión antiransomware no es compatible con máquinas virtuales de almacenamiento que no tienen el protocolo NAS habilitado.

Ver todos los eventos de seguridad activos

Puede ver todos los eventos de seguridad activos y, a continuación, asignar cada uno de ellos a un usuario que pueda resolver el problema. Además, si hay determinados eventos de seguridad que no desea recibir, esta lista puede ayudarle a identificar los eventos que desea deshabilitar.

Lo que necesitará

Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Gestión de eventos**.

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

2. En el menú Ver, seleccione **Eventos de seguridad activos**.

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

Agregar alertas para eventos de seguridad

Es posible configurar alertas para eventos de seguridad individuales, como cualquier otro evento recibido por Unified Manager. Además, si desea tratar todos los eventos de seguridad por igual y enviar correo electrónico a la misma persona, puede crear una única alerta para notificarle cuando se desencadenen eventos de seguridad.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

En el siguiente ejemplo se muestra cómo crear una alerta para el evento de seguridad "'Protocolo Telnet habilitado'". Esto enviará una alerta si el acceso Telnet está configurado para el acceso administrativo remoto al clúster. Puede utilizar esta misma metodología para crear alertas para todos los eventos de seguridad.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de alertas**.
2. En la página **Configuración de alertas**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar alerta**, haga clic en **Nombre** e introduzca un nombre y una descripción para la alerta.
4. Haga clic en **Recursos** y seleccione el clúster o clúster en el que desea activar esta alerta.
5. Haga clic en **Eventos** y realice las siguientes acciones:
   a. En la lista gravedad del evento, seleccione **Advertencia**.
   b. En la lista Eventos coincidentes, seleccione **Protocolo Telnet activado**.
6. Haga clic en **acciones** y, a continuación, seleccione el nombre del usuario que recibirá el correo electrónico de alerta en el campo **Alerta a estos usuarios**.
7. Configure cualquier otra opción de esta página para la frecuencia de notificación, la emisión de toques SNMP y la ejecución de un script.
8. Haga clic en **Guardar**.

Desactivación de eventos de seguridad específicos

Todos los eventos están habilitados de forma predeterminada. Puede deshabilitar eventos específicos para evitar la generación de notificaciones para los eventos que no son importantes en el entorno. Puede habilitar eventos deshabilitados si desea reanudar la recepción de notificaciones.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Si deshabilita eventos, los eventos generados previamente en el sistema se marcan como obsoletos, y no se activan las alertas configuradas para estos eventos. Cuando se habilitan eventos que están deshabilitados, las notificaciones para estos eventos se generan a partir del próximo ciclo de supervisión.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de eventos**.

2. En la página **Event** Setup (Configuración de evento*), desactive o habilite los eventos seleccionando una de las siguientes opciones:

Si desea…	Realice lo siguiente…
Deshabilite eventos	a. Haga clic en **Desactivar**. b. En el cuadro de diálogo Deshabilitar eventos, seleccione la gravedad **Advertencia**. Esta es la categoría para todos los eventos de seguridad. c. En la columna Eventos coincidentes, seleccione los eventos de seguridad que desea deshabilitar y, a continuación, haga clic en la flecha derecha para mover dichos eventos a la columna Deshabilitar eventos. d. Haga clic en **Guardar y cerrar**. e. Compruebe que los eventos que ha deshabilitado se muestran en la vista de lista de la página Event Setup.
Habilite eventos	a. En la lista de eventos deshabilitados, seleccione la casilla de comprobación del evento o los eventos que desea volver a habilitar. b. Haga clic en **Activar**.

Eventos de seguridad

Los eventos de seguridad le proporcionan información sobre el estado de seguridad de los clústeres de ONTAP, las máquinas virtuales de almacenamiento (SVM) y los volúmenes en función de los parámetros definidos en la *Guía de seguridad reforzada de NetApp para ONTAP 9*. Estos eventos le notifican de posibles problemas para que pueda evaluar su gravedad y corregir el problema, si es necesario.

Los eventos de seguridad se agrupan por tipo de origen e incluyen el nombre de evento y captura, nivel de impacto y gravedad. Estos eventos aparecen en las categorías de eventos de clústeres y máquinas virtuales de almacenamiento.

Gestión de operaciones de backup y restauración

Es posible crear backups de Active IQ Unified Manager y usar la función de restauración para restaurar el backup en el mismo sistema (local) o un nuevo sistema (remoto) en caso de un fallo del sistema o pérdida de datos.

Existen tres métodos de backup y restauración según el sistema operativo en el que haya instalado Unified Manager y según el número de clústeres y nodos que se gestionan:

Sistema operativo	Tamaño de la puesta en marcha	Método de copia de seguridad recomendado
VSphere de VMware	Cualquiera	Copia Snapshot de VMware del dispositivo virtual de Unified Manager
Red Hat Enterprise Linux o CentOS de Linux	Pequeño	Volcado de base de datos MySQL de Unified Manager
	Grande	Snapshot de NetApp de la base de datos de Unified Manager
Microsoft Windows	Pequeño	Volcado de base de datos MySQL de Unified Manager
	Grande	Snapshot de NetApp de la base de datos de Unified Manager con protocolo iSCSI

Estos diferentes métodos se describen en las secciones siguientes.

Backup y restauración para Unified Manager en dispositivo virtual

El modelo de backup y restauración de Unified Manager cuando se instala en un dispositivo virtual es capturar y restaurar una imagen de toda la aplicación virtual.

Las siguientes tareas permiten completar un backup del dispositivo virtual:

1. Apague la máquina virtual y tome una copia Snapshot de VMware del dispositivo virtual de Unified Manager.
2. Haga una copia Snapshot de NetApp en el almacén de datos para capturar la snapshot de VMware.

   Si el almacén de datos no está alojado en un sistema que ejecuta el software ONTAP, siga las directrices del proveedor de almacenamiento para crear un backup de la snapshot de VMware.
3. Replicar la copia Snapshot de NetApp, o el equivalente del snapshot, en un almacenamiento alternativo.
4. Elimine la snapshot de VMware.

Debe implementar una programación de backup mediante estas tareas para garantizar que el dispositivo virtual de Unified Manager esté protegido si surge algún problema.

Para restaurar la máquina virtual, se puede usar la snapshot de VMware que se creó para restaurar la máquina virtual en el estado de un momento específico del backup.

Realizar backups y restauraciones con un volcado de base de datos de MySQL

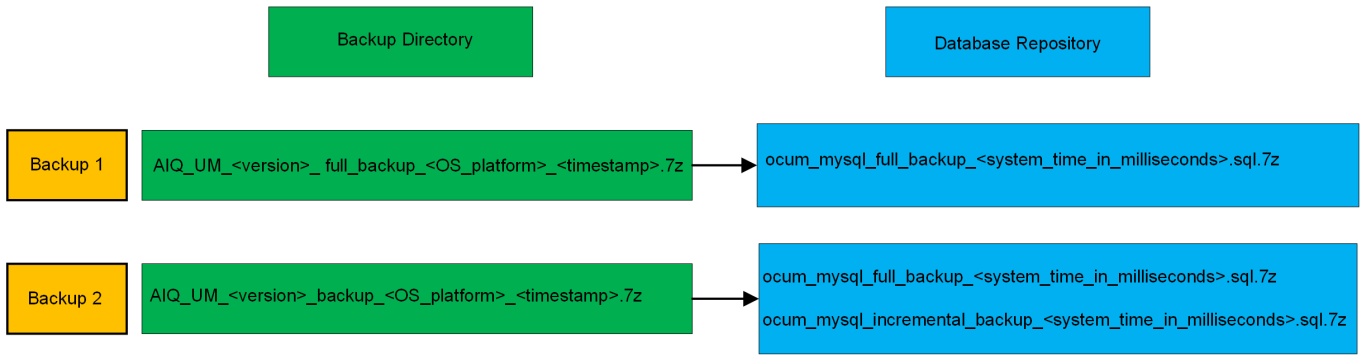
Un backup de volcado de base de datos de MySQL es una copia de la base de datos de Active IQ Unified Manager y los archivos de configuración que puede utilizar en caso de fallo del sistema o pérdida de datos. Se puede programar la escritura de una copia de

seguridad en un destino local o en un destino remoto. Es muy recomendable definir una ubicación remota externa al sistema host Active IQ Unified Manager.

El volcado de bases de datos de MySQL es el mecanismo de backup predeterminado cuando Unified Manager se instala en un servidor Linux y Windows. Sin embargo, si Unified Manager está gestionando una gran cantidad de clústeres y nodos, o si sus backups de MySQL tardan muchas horas en completarse, puede realizar el backup con copias de Snapshot. Esta funcionalidad está disponible en Red Hat Enterprise Linux, sistemas CentOS Linux y Windows.

Una copia de seguridad de volcado de la base de datos consta de un solo archivo en el directorio de copia de seguridad y uno o varios archivos en el directorio de repositorio de la base de datos. El archivo del directorio de copia de seguridad es muy pequeño porque sólo contiene un puntero a los archivos ubicados en el directorio de repositorio de la base de datos que se necesitan para volver a crear la copia de seguridad.

La primera vez que se genera una copia de seguridad de la base de datos se crea un solo archivo en el directorio de copia de seguridad y se crea un archivo de copia de seguridad completa en el directorio de repositorio de la base de datos. La próxima vez que genere una copia de seguridad, se creará un solo archivo en el directorio de copia de seguridad y se creará un archivo de copia de seguridad incremental en el directorio del repositorio de la base de datos que contenga las diferencias con respecto al archivo de copia de seguridad completa. Este proceso continúa mientras se crean backups adicionales, hasta la configuración de retención máxima, como se muestra en la siguiente figura.



No cambie el nombre ni elimine ninguno de los archivos de copia de seguridad de estos dos directorios o se producirá un error en ninguna operación de restauración posterior.

Si escribe los archivos de copia de seguridad en el sistema local, debe iniciar un proceso para copiar los archivos de copia de seguridad en una ubicación remota para que estén disponibles en caso de que tenga un problema con el sistema que requiera una restauración completa.

Antes de iniciar una operación de backup, Active IQ Unified Manager realiza una comprobación de integridad para verificar que existen y pueden escribirse todos los archivos de backup y directorios de backup necesarios. También comprueba que hay suficiente espacio en el sistema para crear el archivo de copia de seguridad.

Configurar el destino y la programación para backups de volcado de base de datos

Es posible configurar los ajustes de backup de volcado de la base de datos de Unified Manager para configurar la ruta de backup, el número de retención y la programación de backups. Se pueden habilitar backups programados diarios o semanales. De forma predeterminada, las copias de seguridad programadas están deshabilitadas, pero debe configurar una programación de copia de seguridad.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Debe tener un mínimo de 150 GB de espacio disponible en la ubicación que defina como ruta de backup.

  Se recomienda que utilice una ubicación remota externa al sistema host de Unified Manager.

- Cuando Unified Manager se instala en un sistema Linux y se utiliza el backup de MySQL, asegúrese de que se han establecido los siguientes permisos y propiedades en el directorio de backup.

  Permisos: 0750, propiedad: jboss:mantenimiento

- Cuando Unified Manager se instala en un sistema Windows y utiliza un backup de MySQL, asegúrese de que solo el administrador tenga acceso al directorio de backup.

Se requiere más tiempo la primera vez que se realiza un backup que para backups posteriores, ya que el primer backup es un backup completo. Un backup completo puede tener más de 1 GB y puede tardar entre tres y cuatro horas. Los backups posteriores son incrementales y requieren menos tiempo.

- Si encuentra que el número de archivos de copia de seguridad incremental es demasiado grande para el espacio que ha asignado para las copias de seguridad, puede tomar una copia de seguridad completa periódicamente para reemplazar la copia de seguridad antigua y sus archivos incrementales. Como otra opción, puede tomar un backup utilizando las copias Snapshot.
- El backup realizado durante los 15 días iniciales de un nuevo clúster añadido puede no ser lo suficientemente preciso para obtener los datos de rendimiento históricos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **copia de seguridad de la base de datos**.
2. En la página **copia de seguridad de la base de datos**, haga clic en **Configuración de copia de seguridad**.
3. Configure los valores adecuados para una ruta de backup, un recuento de retención y una programación.

   El valor predeterminado para el número de retención es 10; se puede usar 0 para crear copias de seguridad ilimitadas.

4. Seleccione el botón **Diario programado** o **Semanal programado** y, a continuación, especifique los detalles del programa.
5. Haga clic en **aplicar**.

Los archivos de backup de volcado de bases de datos se crean según la programación. Puede ver los archivos de copia de seguridad disponibles en la página copia de seguridad de la base de datos.

Qué es una restauración de base de datos

Una restauración de base de datos de MySQL es el proceso de restaurar un archivo de backup de Unified Manager existente en el mismo servidor de Unified Manager o en uno diferente. La operación de restauración se realiza desde la consola de mantenimiento de Unified Manager.

Si va a realizar una operación de restauración en el mismo sistema (local) y los archivos de backup se

almacenan localmente, puede ejecutar la opción de restauración con la ubicación predeterminada. Si va a realizar una operación de restauración en un sistema de Unified Manager diferente (un sistema remoto), debe copiar el archivo de backup o los archivos, desde el almacenamiento secundario al disco local antes de ejecutar la opción de restauración.

Durante el proceso de restauración, se cerró la sesión en Unified Manager. Se puede iniciar sesión en el sistema una vez completado el proceso de restauración.

Si va a restaurar la imagen de backup en un servidor nuevo, una vez que finalice la operación de restauración, debe generar un nuevo certificado de seguridad HTTPS y reiniciar el servidor de Unified Manager. También deberá volver a configurar la configuración de autenticación SAML, si es necesario, al restaurar la imagen de backup en un nuevo servidor.

No es posible usar los archivos de backup antiguos para restaurar una imagen después de que Unified Manager se haya actualizado a una versión más reciente de software. Para ahorrar espacio, se eliminan automáticamente todos los archivos de backup antiguos, excepto el archivo más reciente, al actualizar Unified Manager.

Información relacionada

"Generar un certificado de seguridad HTTPS"

"Habilitación de la autenticación SAML"

"Autenticación con Active Directory u OpenLDAP"

Restaurar un backup de base de datos de MySQL en un sistema Linux

Si se produce la pérdida de datos o daños en los datos, es posible restaurar Unified Manager al estado estable anterior con la pérdida mínima de datos. Puede restaurar la base de datos de Unified Manager a un sistema Red Hat Enterprise Linux o CentOS local o remoto mediante la consola de mantenimiento de Unified Manager.

Lo que necesitará

- Debe tener las credenciales de usuario raíz del host Linux en el que está instalado Unified Manager.
- Debe tener un ID de usuario y una contraseña autorizados para iniciar sesión en la consola de mantenimiento del servidor de Unified Manager.
- Debe haber copiado el archivo de backup de Unified Manager y el contenido del directorio de repositorio de la base de datos en el sistema donde se ejecutará la operación de restauración.

  Se recomienda copiar el archivo de copia de seguridad en el directorio predeterminado `/data/ocum-backup`. Los archivos de repositorio de base de datos deben copiarse a `/database-dumps-repo` subdirectorio bajo el `/ocum-backup` directorio.

- Los archivos de copia de seguridad deben ser de `.7z` tipo.

La función de restauración es específica de la plataforma y de cada versión. Puede restaurar un backup de Unified Manager solo en la misma versión de Unified Manager. Puede restaurar un archivo de copia de seguridad de Linux o un archivo de copia de seguridad de dispositivo virtual en un sistema Red Hat Enterprise Linux o CentOS.

Si el nombre de la carpeta de copia de seguridad contiene un espacio, debe incluir la ruta absoluta o la ruta relativa entre comillas dobles.

Pasos

1. Si va a realizar una restauración en un servidor nuevo, después de instalar Unified Manager no inicia la interfaz de usuario ni configura ninguna configuración de clústeres, usuarios o autenticación cuando se haya completado la instalación. El archivo de backup rellena esta información durante el proceso de restauración.
2. Mediante Secure Shell, conéctese a la dirección IP o al nombre de dominio completo del sistema Unified Manager.
3. Inicie sesión en el sistema con el nombre y la contraseña del usuario de mantenimiento (umadmin).
4. Introduzca el comando `maintenance_console` Y pulse Intro.
5. En la consola de mantenimiento **Menú principal**, introduzca el número de la opción **Restauración de copia de seguridad**.
6. Introduzca el número para **Restaurar copia de seguridad MySQL**.
7. Cuando se le solicite, introduzca la ruta absoluta del archivo de copia de seguridad.

   ```
   Bundle to restore from: /data/ocum-
   backup/UM_9.8.N151113.1348_backup_rhel_02-20-2020-04-45.7z
   ```

   Una vez finalizada la operación de restauración, puede iniciar sesión en Unified Manager.

Después de restaurar el backup, si el servidor OnCommand Workflow Automation no funciona, realice los siguientes pasos:

1. En el servidor de Workflow Automation, cambie la dirección IP del servidor de Unified Manager para que apunte a la máquina más reciente.
2. En el servidor de Unified Manager, restablezca la contraseña de la base de datos si se produce un error en la adquisición en el paso 1.

Restaurar un backup de base de datos de MySQL en Windows

En caso de pérdida de datos o corrupción de datos, es posible usar la función de restauración para restaurar Unified Manager al estado estable anterior con una pérdida mínima. Puede restaurar la base de datos de MySQL de Unified Manager a un sistema Windows local o a un sistema Windows remoto mediante la consola de mantenimiento de Unified Manager.

Lo que necesitará

- Debe tener privilegios de administrador de Windows.
- Debe haber copiado el archivo de backup de Unified Manager y el contenido del directorio de repositorio de la base de datos en el sistema donde se ejecutará la operación de restauración.

  Se recomienda copiar el archivo de copia de seguridad en el directorio predeterminado `\ProgramData\NetApp\OnCommandAppData\ocum\backup`. Los archivos de repositorio de base de

datos deben copiarse a `\database_dumps_repo` subdirectorio bajo el `\backup` directorio.

- Los archivos de copia de seguridad deben ser de `.7z` tipo.

La función de restauración es específica de la plataforma y de cada versión. Puede restaurar un backup de MySQL de Unified Manager solo en la misma versión de Unified Manager y un backup de Windows solo se puede restaurar en una plataforma Windows.

Si los nombres de carpeta contienen un espacio, debe incluir la ruta absoluta o la ruta relativa del archivo de copia de seguridad entre comillas dobles.

Pasos

1. Si va a realizar una restauración en un servidor nuevo, después de instalar Unified Manager no inicia la interfaz de usuario ni configura ninguna configuración de clústeres, usuarios o autenticación cuando se haya completado la instalación. El archivo de backup rellena esta información durante el proceso de restauración.
2. Inicie sesión en el sistema Unified Manager con credenciales de administrador.
3. Inicie PowerShell o el símbolo del sistema como administrador de Windows.
4. Introduzca el comando `maintenance_console` Y pulse Intro.
5. En la consola de mantenimiento **Menú principal**, introduzca el número de la opción **Restauración de copia de seguridad**.
6. Introduzca el número para **Restaurar copia de seguridad MySQL**.
7. Cuando se le solicite, introduzca la ruta absoluta del archivo de copia de seguridad.

```
Bundle to restore from:
\ProgramData\NetApp\OnCommandAppData\ocum\backup\UM_9.8.N151118.2300_bac
kup_windows_02-20-2020-02-51.7z
```

   Una vez finalizada la operación de restauración, puede iniciar sesión en Unified Manager.

Después de restaurar el backup, si el servidor OnCommand Workflow Automation no funciona, realice los siguientes pasos:

1. En el servidor de Workflow Automation, cambie la dirección IP del servidor de Unified Manager para que apunte a la máquina más reciente.
2. En el servidor de Unified Manager, restablezca la contraseña de la base de datos si se produce un error en la adquisición en el paso 1.

Backups y restauraciones con Snapshot de NetApp

Una copia de Snapshot de NetApp crea una imagen de un momento específico de los archivos de configuración y base de datos de Unified Manager que se pueden utilizar para restaurar en caso de un fallo del sistema o pérdida de datos. Programa que una copia Snapshot se escriba en un volumen en uno de los clústeres de ONTAP periódicamente para que siempre tenga una copia actual.

Esta funcionalidad no está disponible para Active IQ Unified Manager instalado en un dispositivo virtual.

Configuración de backup en Linux

Si su Active IQ Unified Manager está instalado en un equipo Linux, puede decidir configurar su backup y restaurar mediante los Snapshots de NetApp.

Las copias Snapshot ocupan muy poco tiempo, por lo general, sólo unos minutos. La base de datos de Unified Manager se bloquea durante un período muy breve, por lo que la instalación apenas se ve afectada. La imagen consume un espacio de almacenamiento mínimo y tiene una sobrecarga del rendimiento mínima, ya que solo registra los cambios que se han realizado en los ficheros desde que se realizó la última copia Snapshot. Dado que la copia Snapshot se crea en un clúster de ONTAP, puede aprovechar otras funciones de NetApp, como SnapMirror, para crear una protección secundaria, si es necesario.

Antes de iniciar una operación de backup, Unified Manager realiza una comprobación de integridad para verificar que el sistema de destino está disponible.

- Puede restaurar una copia Snapshot solo en la misma versión de Active IQ Unified Manager.

  Por ejemplo, si creó un backup en Unified Manager 9.12, el backup solo se puede restaurar en sistemas Unified Manager 9.12.

- Si hay algún cambio en la configuración de Snapshot, puede que la snapshot no sea válida.

Configurar la ubicación de la copia Snapshot

Puede configurar el volumen donde se almacenarán las copias Snapshot en uno de los clústeres de ONTAP mediante System Manager de ONTAP o mediante la interfaz de línea de comandos de ONTAP.

Lo que necesitará

El clúster, la máquina virtual de almacenamiento y el volumen deben cumplir los siguientes requisitos:

- Requisitos del clúster:
  - Se debe instalar ONTAP 9.3 o superior
  - Debe estar geográficamente cerca del servidor de Unified Manager
  - Unified Manager se puede supervisar, pero no es obligatorio
- Requisitos de Storage VM:
  - El modificador de nombre y la asignación de nombres deben configurarse para que utilicen "'files'".
  - Los usuarios locales creados para corresponder con los usuarios del cliente
  - Asegúrese de que está seleccionado todo el acceso de lectura/escritura
  - Asegúrese de que Superuser Access esté definido en «'any'» en la política de exportación
  - NFS para Snapshot de NetApp para Linux
  - NFSv4 deben estar habilitados en el servidor NFS y el dominio de ID de NFSv4 especificado en las máquinas virtuales de almacenamiento y cliente

- El volumen debe ser al menos el doble del tamaño del directorio Unified Manager/opt/netapp/data

  Utilice el comando du -sh /opt/netapp/data/ para comprobar el tamaño actual.

- Requisitos del volumen:
  - El volumen debe tener al menos el doble de tamaño del directorio Unified Manager /opt/netapp/data
  - El estilo de seguridad se debe establecer en UNIX
  - Debe deshabilitarse la política de Snapshot local
  - Se debe habilitar autosize para el volumen
  - El nivel de servicio de rendimiento debe definirse en una política con una tasa elevada de IOPS y una baja latencia, como «'Extreme»

Para obtener los pasos detallados para crear el volumen NFS, consulte "Cómo configurar NFSv4 en ONTAP 9" y la "Guía exprés de configuración de NFS de ONTAP 9".

Especificar la ubicación de destino para las copias de Snapshot

Debe configurar la ubicación de destino para las copias Snapshot de Active IQ Unified Manager en un volumen que ya se haya configurado en uno de los clústeres de ONTAP. Debe utilizar la consola de mantenimiento para definir la ubicación.

- Debe tener las credenciales de usuario raíz del host Linux en el que está instalado Active IQ Unified Manager.
- Debe tener un ID de usuario y una contraseña autorizados para iniciar sesión en la consola de mantenimiento del servidor de Unified Manager.
- Debe tener la dirección IP de gestión del clúster, el nombre de la máquina virtual de almacenamiento, el nombre del volumen, y el nombre de usuario y la contraseña del sistema de almacenamiento.
- Debe haber montado el volumen en el host Active IQ Unified Manager y la ruta de montaje debe ser.

Pasos

1. Utilice Secure Shell para conectarse a la dirección IP o FQDN del sistema Active IQ Unified Manager.
2. Inicie sesión en el sistema con el nombre y la contraseña del usuario de mantenimiento (umadmin).
3. Introduzca el comando `maintenance_console` Y pulse Intro.
4. En la consola de mantenimiento **Menú principal**, introduzca el número de la opción **Restauración de copia de seguridad**.
5. Introduzca el número para **Configurar Snapshot Backup de NetApp**.
6. Introduzca el número para configurar NFS.
7. Revise la información que necesitará proporcionar y, a continuación, introduzca el número para **introducir detalles de configuración de copia de seguridad**.
8. Para identificar el volumen donde se escribirá la snapshot, introduzca la dirección IP de la interfaz de gestión del clúster, el nombre de la máquina virtual de almacenamiento, el nombre del volumen, el nombre de LUN, el nombre de usuario y la contraseña del sistema de almacenamiento y la ruta de montaje.
9. Compruebe esta información e introduzca `y`.

   El sistema ejecuta las siguientes tareas:

- Establece la conexión con el clúster
- Detiene todos los servicios
- Crea un nuevo directorio en el volumen y copia los archivos de configuración de la base de datos Active IQ Unified Manager
- Elimina los archivos de Active IQ Unified Manager y crea un enlace simbólico al nuevo directorio de la base de datos
- Reinicia todos los servicios

10. Salga de la consola de mantenimiento e inicie la interfaz de Active IQ Unified Manager para crear una programación para la copia Snapshot si no lo ha hecho todavía.

Configuración de la copia de seguridad en Windows

Active IQ Unified Manager admite backup y restauración usando snapshots de NetApp en el sistema operativo Windows con la ayuda de LUN con el protocolo iSCSI.

Se puede realizar un backup basado en Snapshot mientras todos los servicios de Unified Manager están en ejecución. Como parte de la Snapshot, se captura un estado coherente de la base de datos a medida que el backup coloca un bloqueo de lectura global en toda la base de datos que evita las escrituras simultáneas. En el caso de que el sistema Unified Manager esté instalado en el sistema operativo Windows para realizar backups y restauraciones con Snapshot de NetApp, primero debe configurar Unified Manager backup en Snapshot mediante la consola de mantenimiento.

Antes de configurar Unified Manager para crear copias Snapshot, debe realizar las siguientes tareas de configuración.

- Configure el clúster ONTAP
- Configurar el equipo host de Windows

Configuración de la ubicación de la copia de seguridad para Windows

Debe configurar el volumen para almacenar copias de Snapshot después de realizar un backup de Unified Manager en Windows.

Lo que necesitará

El clúster, la máquina virtual de almacenamiento y el volumen deben cumplir los siguientes requisitos:

- Requisitos del clúster:
  - Se debe instalar ONTAP 9.3 o superior
  - Debe estar geográficamente cerca del servidor de Unified Manager
  - Se supervisa mediante Unified Manager
- Requisitos de Storage VM:
  - Conectividad iSCSI en clúster de ONTAP
  - El protocolo iSCSI debe estar habilitado para el equipo configurado
  - Debe tener un volumen y LUN dedicados para la configuración de backup. El volumen seleccionado solo debe contener un LUN y nada más.
  - El tamaño de la LUN debe ser al menos el doble del tamaño de datos que se espera que se maneja en

la Active IQ Unified Manager de 9.9.

Esto establece también el mismo requisito de tamaño en el volumen.

- Asegúrese de que está seleccionado todo el acceso de lectura/escritura
- Asegúrese de que Superuser Access esté definido en «'any'» en la política de exportación

- Requisitos del volumen y LUN:
  - El volumen debe tener al menos el doble del tamaño del directorio de datos MySQL de Unified Manager.
  - El estilo de seguridad se debe establecer en Windows
  - Debe deshabilitarse la política de Snapshot local
  - Se debe habilitar autosize para el volumen
  - El nivel de servicio de rendimiento debe definirse en una política con una tasa elevada de IOPS y una baja latencia, como «'Extreme»

Configurando clúster de ONTAP

Es necesario realizar algunos pasos de configuración previa en clústeres de ONTAP para poder realizar un backup y restaurar Active IQ Unified Manager mediante la copia de Snapshot en sistemas Windows.

Es posible configurar el clúster de ONTAP mediante el símbolo del sistema o la interfaz de usuario de System Manager. La configuración del clúster de ONTAP implica la configuración de LIF de datos para que estén disponibles como LIF iSCSI para el equipo virtual de almacenamiento. El paso siguiente consiste en configurar un equipo virtual de almacenamiento habilitado para iSCSI mediante la interfaz de usuario de System Manager. Tendrá que configurar una ruta de red estática para esta máquina virtual de almacenamiento a fin de controlar cómo utilizan las LIF la red para el tráfico saliente.

Debe tener un volumen dedicado y un LUN para la configuración de backup. El volumen seleccionado solo debe incluir un LUN. El tamaño de la LUN debe ser al menos el doble del tamaño de datos que se espera que gestione Active IQ Unified Manager.

Debe realizar la siguiente configuración:

Pasos

1. Configurar una máquina virtual de almacenamiento habilitada para iSCSI o utilizar una máquina virtual de almacenamiento existente con la misma configuración.
2. Configure una ruta de red para el equipo virtual de almacenamiento configurado.
3. Configure un volumen de la capacidad adecuada y una única LUN dentro para garantizar que el volumen se dedica únicamente a esta LUN.

   En una situación en la que se crea la LUN en System Manager, es posible que la desasignación de la LUN elimine el igroup y que se produzca un error en la restauración. Para evitar esta situación, asegúrese de que al crear una LUN, se crea explícitamente y no se elimina cuando se anula la asignación de la LUN.

4. Configure un iGroup en la máquina virtual de almacenamiento.
5. Configurar un conjunto de puertos.

6. Integre el igroup con el conjunto de puertos.
7. Asigne la LUN al igroup.

Configuración de máquina host de Windows

Es necesario configurar el equipo host de Windows antes de poder usar Snapshot de NetApp para realizar backup y restaurar Active IQ Unified Manager. Para iniciar el iniciador iSCSI de Microsoft en un equipo host de Windows, escriba "'iscsi'" en la barra de búsqueda y haga clic en **Iniciador iSCSI**.

Lo que necesitará

Debe limpiar cualquier configuración anterior en el equipo host.

Si está intentando iniciar el iniciador iSCSI en una instalación nueva de Windows, se le pedirá confirmación y, en su confirmación, se muestra el cuadro de diálogo Propiedades de iSCSI. Si se trata de una instalación de Windows existente, el cuadro de diálogo Propiedades de iSCSI aparece con un destino que está inactivo o intentando conectarse. Por lo tanto, deberá asegurarse de que se hayan eliminado todas las configuraciones anteriores del host de Windows.

Pasos

1. Limpie cualquier configuración anterior en el equipo host.
2. Descubra el portal de destino.
3. Conéctese al portal de destino.
4. Conéctese mediante multivía al portal de destino.
5. Descubra ambos LIF.
6. Detecte el LUN configurado en el equipo Windows como dispositivo.
7. Configure el LUN detectado como una unidad de volumen nueva en Windows.

Especificar la ubicación de destino para las copias de Snapshot en Windows

Debe configurar la ubicación de destino para las copias Snapshot de Active IQ Unified Manager en un volumen que ya se haya configurado en uno de los clústeres de ONTAP. Debe utilizar la consola de mantenimiento para definir la ubicación.

- Debe tener el privilegio de administrador para el host de Windows en el que está instalado Active IQ Unified Manager.
- Debe tener un ID de usuario y una contraseña autorizados para iniciar sesión en la consola de mantenimiento del servidor de Unified Manager.
- Debe tener la dirección IP de gestión del clúster, el nombre de la máquina virtual de almacenamiento, el nombre del volumen, el nombre de LUN y el nombre de usuario y la contraseña del sistema de almacenamiento.
- Debe haber montado el volumen como unidad de red en el host Active IQ Unified Manager y debe tener la unidad de montaje.

Pasos

1. Con el Shell de alimentación, conéctese a la dirección IP o al nombre de dominio completo del sistema Active IQ Unified Manager.

2. Inicie sesión en el sistema con el nombre y la contraseña del usuario de mantenimiento (umadmin).
3. Introduzca el comando `maintenance_console` Y pulse Intro.
4. En la consola de mantenimiento **Menú principal**, introduzca el número de la opción **Restauración de copia de seguridad**.
5. Introduzca el número para **Configurar Snapshot Backup de NetApp**.
6. Introduzca el número para configurar iSCSI.
7. Revise la información que necesitará proporcionar y, a continuación, introduzca el número para **introducir detalles de configuración de copia de seguridad**.
8. Para identificar el volumen donde se escribirá la snapshot, introduzca la dirección IP de la interfaz de gestión del clúster, el nombre de la máquina virtual de almacenamiento, el nombre del volumen, el nombre de LUN, el nombre de usuario y la contraseña del sistema de almacenamiento y la unidad de montaje.
9. Compruebe esta información e introduzca `y`.

   El sistema ejecuta las siguientes tareas:

   - El equipo virtual de almacenamiento se valida
   - Se valida el volumen
   - El estado y la unidad de montaje se validan
   - Estado y existencia de LUN
   - Existencia de unidades de red
   - Se valida la existencia de espacio recomendado (más de dos veces del directorio de datos mysql) en el volumen montado
   - Ruta de LUN correspondiente al LUN dedicado del volumen
   - nombre del igroup
   - GUID del volumen en el que está montada la unidad de red
   - Iniciador de iSCSI que se utiliza para comunicarse con ONTAP
10. Salga de la consola de mantenimiento e inicie la interfaz de Active IQ Unified Manager para crear una programación para las copias de Snapshot.

Configurar el backup por copia Snapshot desde la consola de mantenimiento

Para realizar un backup de Active IQ Unified Manager con copia Snapshot, debe realizar unos cuantos pasos de configuración desde la consola de mantenimiento.

Lo que necesitará

Debe tener los siguientes detalles de su sistema:

- Dirección IP del clúster
- Nombre de la máquina virtual de almacenamiento
- Nombre del volumen
- Nombre de LUN
- Ruta de montaje
- Credenciales del sistema de almacenamiento

Pasos

1. Acceda a la consola de mantenimiento de Unified Manager.
2. Introduzca 4 para seleccionar **Restauración de copia de seguridad**.
3. Introduzca 2 para seleccionar **Backup and Restore Using NetApp Snapshot**.

> Si desea cambiar la configuración de backup, introduzca 3 para seleccionar **Actualizar la configuración de backup de snapshot de NetApp**. Sólo puede actualizar la contraseña.

4. En el menú, introduzca 1 para seleccionar **Configurar Snapshot Backup de NetApp**.
5. Introduzca 1 para proporcionar la información necesaria.
6. Proporcione el nombre de usuario y la contraseña de la consola de mantenimiento y, a continuación, proporcione la confirmación de que la LUN está montada en el host.

   A continuación, el proceso verifica que el directorio de datos, la ruta de LUN, el equipo virtual de almacenamiento, los volúmenes, la disponibilidad de espacio, la unidad, etc. proporcionada por usted es correcta. Las operaciones que se realizan en segundo plano son:

   - Los servicios se han detenido
   - El directorio de la base de datos se mueve al almacenamiento montado
   - El directorio de la base de datos se elimina y se establecen enlaces simbólicos
   - Los servicios se reinician una vez que la configuración finaliza en la interfaz de Active IQ Unified Manager, el tipo de backup se modifica para incluir en las copias Snapshot de NetApp y se refleja en la interfaz de usuario como Backup de bases de datos (basado en Snapshot).

Antes de iniciar una operación de backup, debe comprobar si hay algún cambio en la configuración de Snapshot porque podría provocar que la copia de Snapshot no sea válida. Supongamos que ha configurado el backup en la unidad G y en la instantánea tomada. Más tarde reconfiguró la copia de seguridad en la unidad E y los datos se guardan en la unidad E según la nueva configuración. Si intenta restaurar Snapshot tomadas mientras estaba en la unidad G, se produce un error y la unidad G no existe.

Definición de una programación de backup para Linux y Windows

Puede configurar la programación en la que se crean las copias de Snapshot de Unified Manager mediante la interfaz de usuario de Unified Manager.

Lo que necesitará

- Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
- Configuró los ajustes para crear copias Snapshot desde la consola de mantenimiento para identificar el destino donde se crearán las snapshots.

Las copias Snapshot se crean en solo unos minutos y la base de datos de Unified Manager se bloquea solo durante unos pocos segundos.

> El backup realizado durante los 15 días iniciales de un nuevo clúster añadido puede no ser lo suficientemente preciso para obtener los datos de rendimiento históricos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **copia de seguridad de la base de datos**.

2. En la página **copia de seguridad de la base de datos**, haga clic en **Configuración de copia de seguridad**.
3. Introduzca el número máximo de copias Snapshot que desea retener en el campo **recuento de retención**.

   El valor predeterminado para el número de retención es 10. El número máximo de copias Snapshot viene determinado por la versión del software ONTAP del clúster. Puede dejar este campo en blanco para implementar el valor máximo independientemente de la versión de ONTAP.

4. Seleccione el botón **Diario programado** o **Semanal programado** y, a continuación, especifique los detalles del programa.
5. Haga clic en **aplicar**.

Las copias Snapshot se crean según la programación. Puede ver los archivos de copia de seguridad disponibles en la página copia de seguridad de la base de datos.

Debido a la importancia de este volumen y de las copias de Snapshot, puede crear una o dos alertas para este volumen, de modo que reciba una notificación cuando:

- El espacio del volumen está lleno al 90%. Utilice el evento **espacio de volumen lleno** para configurar la alerta.

  Es posible añadir capacidad al volumen con ONTAP System Manager o la interfaz de línea de comandos de ONTAP para que la base de datos de Unified Manager no se quede sin espacio.

- El número de instantáneas está cerca de alcanzar el número máximo. Utilice el evento **demasiadas copias Snapshot** para configurar la alerta.

  Puede eliminar copias de Snapshot más antiguas con System Manager de ONTAP o la interfaz de línea de comandos de ONTAP para que siempre haya espacio para las copias de Snapshot nuevas.

Las alertas se configuran en la página Alert Setup.

Restaurar Unified Manager con copias de Snapshot

Si se produce la pérdida de datos o daños en los datos, es posible restaurar Unified Manager al estado estable anterior con la pérdida mínima de datos. Puede restaurar la base de datos de Snapshot de Unified Manager a un sistema operativo local o remoto mediante la consola de mantenimiento de Unified Manager.

Lo que necesitará

- Debe tener las credenciales de usuario raíz para el host Linux y los privilegios administrativos para la máquina host de Windows en la que está instalado Unified Manager.
- Debe tener un ID de usuario y una contraseña autorizados para iniciar sesión en la consola de mantenimiento del servidor de Unified Manager.

La función de restauración es específica de la plataforma y de cada versión. Puede restaurar un backup de Unified Manager solo en la misma versión de Unified Manager.

Pasos

1. Conéctese a la dirección IP o el nombre de dominio completo del sistema Unified Manager.
   - Linux: Secure Shell

◦ Windows: Shell de energía

2. Inicie sesión en el sistema con las credenciales de usuario raíz.
3. Introduzca el comando `maintenance_console` Y pulse Intro.
4. En la consola de mantenimiento **Menú principal**, introduzca 4 para la opción **Restauración de copia de seguridad**.
5. Introduzca 2 para seleccionar **copia de seguridad y restauración con NetApp Snapshot**.

   Si va a realizar una restauración en un servidor nuevo, después de instalar Unified Manager no inicia la interfaz de usuario ni configura ninguna configuración de clústeres, usuarios o autenticación cuando se haya completado la instalación. Introduzca 1 para seleccionar **Configurar Snapshot Backup de NetApp** y configure los ajustes para las copias Snapshot tal y como están en el sistema original.

6. Introduzca 3 para seleccionar **Restaurar con Snapshot de NetApp**.
7. Seleccione la copia Snapshot a partir de la que desea restaurar Unified Manager. Pulse **Intro**.
8. Una vez completado el proceso de restauración, inicie sesión en la interfaz de usuario de Unified Manager.

Después de restaurar el backup, si el servidor de Workflow Automation no funciona, realice los siguientes pasos:

1. En el servidor de Workflow Automation, cambie la dirección IP del servidor de Unified Manager para que apunte a la máquina más reciente.
2. En el servidor de Unified Manager, restablezca la contraseña de la base de datos si se produce un error en la adquisición en el paso 1.

Modificación del tipo de backup

Si desea cambiar el tipo de backup del sistema Active IQ Unified Manager, puede usar las opciones de la consola de mantenimiento. La opción **Desactivar copia de seguridad Snapshot** de NetApp le permite recuperar el backup basado en MySQL.

Lo que necesitará

Debe tener un ID de usuario y una contraseña autorizados para iniciar sesión en la consola de mantenimiento del servidor de Unified Manager.

Pasos

1. Acceda a la consola de mantenimiento.
2. Seleccione 4 en el **Menú principal** para copia de seguridad y restauración.
3. Seleccione 2 en el **Menú copia de seguridad y restauración**.
4. Seleccione 4 para **desconfigurar Snapshot Backup de NetApp**.

   Se muestran las acciones que se realizan, que son, detener los servicios, interrumpir el enlace simbólico, mover los datos del almacenamiento al directorio y, a continuación, volver a iniciar los servicios.

   Después de modificar el método de backup, el mecanismo de backup cambia de la copia Snapshot al backup MySQL predeterminado. Este cambio aparece en la sección copia de seguridad de la base de datos de la configuración General.

Backup bajo demanda para Unified Manager

Puede utilizar la interfaz de usuario de Active IQ Unified Manager para generar backup bajo demanda cuando lo necesite. El backup bajo demanda permite crear de forma instantánea un backup con el método de backup existente. El backup bajo demanda no distingue entre MySQL o backup basado en Snapshot de NetApp.

Puede realizar una copia de seguridad bajo demanda con el botón **copia de seguridad ahora** de la página copia de seguridad de la base de datos. El backup bajo demanda no depende de las programaciones configuradas para Active IQ Unified Manager.

Migración de un dispositivo virtual de Unified Manager a un sistema Linux

Puede restaurar un backup de volcado de base de datos de MySQL de Unified Manager desde un dispositivo virtual a un sistema Red Hat Enterprise Linux o CentOS Linux si desea cambiar el sistema operativo del host en el que se ejecuta Unified Manager.

Lo que necesitará

- En el dispositivo virtual:
  - Debe tener el rol de operador, administrador de aplicaciones o administrador de almacenamiento.
  - Debe conocer el nombre del usuario de mantenimiento de Unified Manager para la operación de restauración.
- En el sistema Linux:
  - Debe haber instalado Unified Manager en un servidor Linux según las instrucciones descritas en "Instalación de Unified Manager en sistemas Linux".
  - La versión de Unified Manager en este servidor debe ser la misma que la versión del dispositivo virtual desde el que se utiliza el archivo de backup.
  - No inicie la interfaz de usuario ni configure ningún clúster, usuario ni configuración de autenticación en el sistema Linux después de la instalación. El archivo de backup rellena esta información durante el proceso de restauración.
  - Debe tener las credenciales de usuario raíz para el host Linux.

Estos pasos describen cómo crear un archivo de copia de seguridad en el dispositivo virtual, copiar los archivos de copia de seguridad en el sistema Red Hat Enterprise Linux o CentOS y, a continuación, restaurar la copia de seguridad de la base de datos en el nuevo sistema.

Pasos

1. En el dispositivo virtual, haga clic en **Administración** > **copia de seguridad de la base de datos**.
2. En la página **copia de seguridad de la base de datos**, haga clic en **Configuración de copia de seguridad**.
3. Cambie la ruta de backup a /jail/support.
4. En la sección Programación, seleccione **Diario programado** e introduzca una hora unos minutos después de la hora actual para que la copia de seguridad se cree en breve.
5. Haga clic en **aplicar**.
6. Espere unas horas para que se genere el backup.

   Un backup completo puede tener más de 1 GB y puede tardar entre tres y cuatro horas en completarse.

7. Inicie sesión como usuario raíz en el host Linux en el que está instalado Unified Manager y copie los archivos de backup desde /support en el dispositivo virtual con SCP.`root@<rhel_server>:/# scp -r admin@<vapp_server_ip_address>:/support/* .`

   ```
   root@ocum_rhel-21:/# scp -r admin@10.10.10.10:/support/* .
   ```

   Asegúrese de haber copiado el archivo de backup .7z y todos los archivos de repositorio .7z en el subdirectorio /database-vuels-repo.

8. En el símbolo del sistema, restaure el backup: `um backup restore -f /<backup_file_path>/<backup_file_name>`

   ```
   um backup restore -f /UM_9.7.N151113.1348_backup_unix_02-12-2019-04-16.7z
   ```

9. Una vez que finaliza la operación de restauración, inicie sesión en la interfaz de usuario web de Unified Manager.

Debe realizar las siguientes tareas:

- Genere un nuevo certificado de seguridad HTTPS y reinicie Unified Manager Server.
- Cambie la ruta de copia de seguridad al valor predeterminado del sistema Linux (/data/ocum-backup) o a una nueva ruta de acceso de su elección, porque no hay ninguna ruta de /cárcel/soporte en el sistema Linux.
- Vuelva a configurar ambas partes de su conexión de Workflow Automation si se está utilizando WFA.
- Vuelva a configurar la configuración de autenticación SAML si utiliza SAML.

Después de verificar que todo se está ejecutando como se espera en el sistema Linux, puede apagar y quitar el dispositivo virtual de Unified Manager.

Administrar scripts

Es posible usar scripts para modificar o actualizar automáticamente varios objetos de almacenamiento en Unified Manager. El script está asociado a una alerta. Cuando un evento activa una alerta, se ejecuta el script. Puede cargar scripts personalizados y probar su ejecución cuando se genera una alerta.

La capacidad de cargar scripts en Unified Manager y ejecutarlas está habilitada de forma predeterminada. Si su organización no desea permitir esta funcionalidad debido a razones de seguridad, puede desactivar esta funcionalidad desde **Storage Management** > **Configuración de funciones**.

Cómo funcionan los scripts con alertas

Es posible asociar una alerta a la secuencia de comandos para que se ejecute el script cuando se genera una alerta para un evento en Unified Manager. Puede usar los scripts para resolver problemas con objetos de almacenamiento o identificar qué objetos de almacenamiento generan los eventos.

Cuando se genera una alerta para un evento en Unified Manager, se envía un correo electrónico de alerta a los destinatarios especificados. Si asoció una alerta a un script, se ejecuta el script. Puede obtener los detalles de los argumentos pasados al script desde el correo electrónico de alerta.

Si ha creado una secuencia de comandos personalizada y la ha asociado con una alerta para un tipo de evento específico, las acciones se realizan en función de su secuencia de comandos personalizada para ese tipo de evento y las acciones **Fix it** no están disponibles de forma predeterminada en la página acciones de administración o en el panel de Unified Manager.

El script utiliza los siguientes argumentos para su ejecución:

- `-eventID`
- `-eventName`
- `-eventSeverity`
- `-eventSourceID`
- `-eventSourceName`
- `-eventSourceType`
- `-eventState`
- `-eventArgs`

Puede utilizar los argumentos de las secuencias de comandos y recopilar información de eventos relacionada o modificar objetos de almacenamiento.

Ejemplo para obtener argumentos de scripts

```
print "$ARGV[0] : $ARGV[1]\n"
print "$ARGV[7] : $ARGV[8]\n"
```

Cuando se genera una alerta, se ejecuta este script y se muestra el siguiente resultado:

```
-eventID : 290
-eventSourceID : 4138
```

Añadiendo scripts

Puede añadir scripts en Unified Manager y asociarlos con alertas. Estos scripts se ejecutan automáticamente cuando se genera una alerta, y le permiten obtener información sobre los objetos de almacenamiento para los que se genera el evento.

Lo que necesitará

- Debe haber creado y guardado los scripts que desea añadir al servidor de Unified Manager.
- Los formatos de archivo compatibles con scripts son Perl, Shell, PowerShell, Python y. `.bat` archivos.

Plataforma en la que se ha instalado Unified Manager	Idiomas compatibles
VMware	Scripts Perl y Shell
Linux	Scripts Perl, Python y Shell
Windows	PowerShell, Perl, Python y scripts .bat

  - Para los scripts Perl, se debe instalar Perl en el servidor Unified Manager. Para instalaciones de VMware, se instala Perl 5 de forma predeterminada y los scripts solo admiten lo que admite Perl 5. Si se instaló Perl después de Unified Manager, debe reiniciar el servidor de Unified Manager.
  - Para los scripts de PowerShell, se debe establecer la directiva de ejecución de PowerShell correspondiente en el servidor Windows para poder ejecutar los scripts.

> Si el script crea archivos de registro para realizar un seguimiento del progreso del script de alertas, debe asegurarse de que no se creen los archivos de registro en ningún lugar de la carpeta de instalación de Unified Manager.

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Puede cargar scripts personalizados y recopilar detalles de eventos acerca de la alerta.

> Si no ve esta capacidad disponible en la interfaz de usuario, se debe a que el administrador ha desactivado la funcionalidad. Si es necesario, puede activar esta funcionalidad desde **Storage Management** > **Configuración de funciones**.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Storage Management** > **Scripts**.
2. En la página **Scripts**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar script**, haga clic en **examinar** para seleccionar el archivo de secuencia de comandos.
4. Introduzca una descripción para la secuencia de comandos que seleccione.
5. Haga clic en **Agregar**.

Eliminar scripts

Es posible eliminar un script de Unified Manager cuando el script ya no se requiere o no es válido.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- El script no debe estar asociado a una alerta.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Storage Management** > **Scripts**.
2. En la página **Scripts**, seleccione la secuencia de comandos que desea eliminar y, a continuación, haga

clic en **Eliminar**.

3. En el cuadro de diálogo **Advertencia**, confirme la eliminación haciendo clic en **Sí**.

Prueba de la ejecución de scripts

Puede verificar que el script se ejecute correctamente cuando se genera una alerta para un objeto de almacenamiento.

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber cargado un script en el formato de archivo compatible a Unified Manager.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Storage Management** > **Scripts**.
2. En la página Scripts, agregue el script de prueba.
3. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Configuración de alertas**.
4. En la página **Configuración de alertas**, realice una de las siguientes acciones:

Para…	Realice lo siguiente…
Añadir una alerta	a. Haga clic en **Agregar**. b. En la sección acciones, asocie la alerta al script de prueba.
Editar una alerta	a. Seleccione una alerta y, a continuación, haga clic en **Editar**. b. En la sección acciones, asocie la alerta al script de prueba.

5. Haga clic en **Guardar**.
6. En la página **Configuración de alertas**, seleccione la alerta que ha agregado o modificado y, a continuación, haga clic en **Prueba**.

   El script se ejecuta con el argumento «»-test» y se envía una alerta de notificación a las direcciones de correo electrónico especificadas al crear la alerta.

Gestión y supervisión de grupos

Es posible crear grupos en Unified Manager para gestionar objetos de almacenamiento.

Comprender los grupos

Es posible crear grupos en Unified Manager para gestionar objetos de almacenamiento. Comprender los conceptos sobre los grupos y la forma en que las reglas de grupo permiten añadir objetos de almacenamiento a un grupo le ayudará a gestionar los objetos de almacenamiento del entorno.

Qué es un grupo

Un grupo es una colección dinámica de objetos de almacenamiento heterogéneos (clústeres, SVM o volúmenes). Es posible crear grupos en Unified Manager para gestionar de forma sencilla un conjunto de objetos de almacenamiento. Los miembros de un grupo pueden cambiar, según los objetos de almacenamiento supervisados por Unified Manager en un momento específico.

- Cada grupo tiene un nombre único.
- Debe configurar un mínimo de una regla de grupo para cada grupo.
- Puede asociar un grupo con más de una regla de grupo.
- Cada grupo puede incluir varios tipos de objetos de almacenamiento, como clústeres, SVM o volúmenes.
- Los objetos de almacenamiento se añaden de forma dinámica a un grupo en función de cuándo se crea una regla de grupo o cuando Unified Manager completa un ciclo de supervisión.
- Es posible aplicar acciones simultáneamente en todos los objetos de almacenamiento de un grupo, como configurar umbrales para los volúmenes.

Cómo funcionan las reglas de grupo para los grupos

Una regla de grupo es un criterio que se define para habilitar los objetos de almacenamiento (volúmenes, clústeres o SVM) que se incluirán en un grupo específico. Puede utilizar grupos de condiciones o condiciones para definir reglas de grupo para un grupo.

- Debe asociar una regla de grupo a un grupo.
- Debe asociar un tipo de objeto para una regla de grupo; sólo hay un tipo de objeto asociado a una regla de grupo.
- Los objetos de almacenamiento se agregan o eliminan del grupo después de cada ciclo de supervisión o cuando se crea, edita o elimina una regla.
- Una regla de grupo puede tener uno o más grupos de condiciones y cada grupo de condiciones puede tener una o más condiciones.
- Los objetos de almacenamiento pueden pertenecer a varios grupos según las reglas de grupo que cree.

Condiciones

Puede crear varios grupos de condiciones y cada grupo de condiciones puede tener una o más condiciones. Puede aplicar todos los grupos de condiciones definidos en una regla de grupo para los grupos con el fin de especificar qué objetos de almacenamiento se incluyen en el grupo.

Las condiciones dentro de un grupo de condiciones se ejecutan utilizando lógica Y. Deben cumplirse todas las condiciones de un grupo de condiciones. Al crear o modificar una regla de grupo, se crea una condición que aplica, selecciona y agrupa sólo los objetos de almacenamiento que cumplen todas las condiciones del grupo de condiciones. Puede utilizar varias condiciones dentro de un grupo de condiciones cuando desee limitar el ámbito de los objetos de almacenamiento que se incluirán en un grupo.

Puede crear condiciones con objetos de almacenamiento mediante las operaciones y el operador siguientes y especificando el valor requerido.

Tipo de objeto de almacenamiento	Operandos aplicables
Volumen	• Nombre del objeto • Propietario del nombre del clúster • Nombre de SVM propietario • Anotaciones
SVM	• Nombre del objeto • Propietario del nombre del clúster • Anotaciones
Clúster	• Nombre del objeto • Anotaciones

Cuando se selecciona anotación como operando para cualquier objeto de almacenamiento, el operador "'is'" está disponible. Para el resto de operandos, puede seleccionar "'is'" o "'contains'" como operador.

- Operando

  La lista de operandos en Unified Manager cambia según el tipo de objeto seleccionado. La lista incluye el nombre del objeto, el nombre del clúster propietario, el nombre de SVM propietario y las anotaciones que defina en Unified Manager.

- Operador

  La lista de operadores cambia según el operando seleccionado para una condición. Los operadores admitidos en Unified Manager son «'is'» y «'contains».

  Cuando se selecciona el operador "'is'", la condición se evalúa para la coincidencia exacta del valor de operando con el valor proporcionado para el operando seleccionado.

  Al seleccionar el operador "'contains'", la condición se evalúa para cumplir uno de los siguientes criterios:

  - El valor de operando es una coincidencia exacta con el valor proporcionado para el operando seleccionado
  - El valor de operando contiene el valor proporcionado para el operando seleccionado

- Valor

  El campo valor cambia según el operando seleccionado.

Ejemplo de una regla de grupo con condiciones

Considere un grupo de condiciones para un volumen con las dos condiciones siguientes:

- El nombre contiene «'vol'»
- El nombre de SVM es «data_svm».

Este grupo de condiciones selecciona todos los volúmenes que incluyen «'vol'» en sus nombres y que están alojados en las SVM con el nombre «dATA_svm».

Grupos de condiciones

Los grupos de condiciones se ejecutan mediante lógico O y, a continuación, se aplican a los objetos de almacenamiento. Los objetos de almacenamiento deben satisfacer uno de los grupos de condición que se incluirán en un grupo. Se combinan los objetos de almacenamiento de todos los grupos de condiciones. Puede utilizar grupos de condiciones para aumentar el alcance de los objetos de almacenamiento que se incluirán en un grupo.

Ejemplo de una regla de grupo con grupos de condiciones

Debe tener en cuenta dos grupos de condiciones para un volumen, con cada grupo que contiene las dos condiciones siguientes:

- Grupo de condición 1
  - El nombre contiene «'vol'»
  - El nombre de SVM es «data_svm» el grupo de condiciones 1 selecciona todos los volúmenes que incluyen «'vol» en sus nombres y que están alojados en las SVM con el nombre «data_svm».
- Grupo de condiciones 2
  - El nombre contiene «'vol'»
  - El valor de anotación de la prioridad de datos es el grupo de condiciones «'crítico'» 2 selecciona todos los volúmenes que incluyen «'vol'» en sus nombres y que se anotan con el valor de anotación de prioridad de datos como «'crítico'».

Cuando se aplica una regla de grupo que contiene estos dos grupos de condiciones a los objetos de almacenamiento, se agregan los siguientes objetos de almacenamiento a un grupo seleccionado:

- Todos los volúmenes que incluyan «'vol» en sus nombres y que estén alojados en la SVM con el nombre «data_svm».
- Todos los volúmenes que incluyan «'vol'» en sus nombres y que estén anotados con el valor de anotación de prioridad de datos «'crítico'».

Cómo funcionan las acciones de grupo en los objetos de almacenamiento

Una acción de grupo es una operación que se realiza en todos los objetos de almacenamiento de un grupo. Por ejemplo, es posible configurar la acción del grupo de umbrales de volúmenes para cambiar simultáneamente los valores de umbral de volumen de todos los volúmenes de un grupo.

Los grupos admiten tipos de acciones de grupo únicos. Es posible tener un grupo con un solo tipo de acción de grupo de umbral de estado de volumen. Sin embargo, puede configurar un tipo diferente de acción de grupo, si está disponible, para el mismo grupo. El rango de una acción de grupo determina el orden en el que se aplica la acción a los objetos de almacenamiento. La página de detalles de un objeto de almacenamiento proporciona información sobre la acción de grupo que se aplica en el objeto de almacenamiento.

Ejemplo de acciones de grupo únicas

Considere un volumen A que pertenece a los grupos G1 y G2, y las siguientes acciones de grupo de umbral de estado de volumen están configuradas para estos grupos:

- `Change_capacity_threshold` acción de grupo con rango 1, para configurar la capacidad del volumen

- `Change_snapshot_copies` Acción del grupo con el rango 2, para configurar las copias Snapshot del volumen

La `Change_capacity_threshold` la acción de grupo siempre tiene prioridad sobre la `Change_snapshot_copies` La acción del grupo y se aplica al volumen A. Cuando Unified Manager completa un ciclo de supervisión, los eventos relacionados con el umbral de estado del volumen A se vuelven a evaluar según la `Change_capacity_threshold` acción de grupo. No puede configurar otro tipo de umbral de volumen de acción de grupo para los grupos G1 o G2.

Agregar grupos

Puede crear grupos para combinar clústeres, volúmenes y máquinas virtuales de almacenamiento (SVM) con el fin de simplificar la gestión.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Puede definir reglas de grupo para agregar o quitar miembros del grupo y modificar acciones de grupo para el grupo.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **grupos**.
2. En la ficha **grupos**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar grupo**, escriba un nombre y una descripción para el grupo.
4. Haga clic en **Agregar**.

Edición de grupos

Puede editar el nombre y la descripción de un grupo creado en Unified Manager.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Cuando edite un grupo para actualizar el nombre, debe especificar un nombre único; no puede utilizar un nombre de grupo existente.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **grupos**.
2. En la ficha **grupos**, seleccione el grupo que desea editar y, a continuación, haga clic en **Editar**.
3. En el cuadro de diálogo **Editar grupo**, cambie el nombre, la descripción o ambos para el grupo.
4. Haga clic en **Guardar**.

Eliminación de grupos

Un grupo se puede eliminar de Unified Manager cuando ya no se necesita el grupo.

Lo que necesitará

- Ninguno de los objetos de almacenamiento (clústeres, SVM o volúmenes) debe estar asociado con cualquier regla de grupo asociada con el grupo que desea eliminar.
- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **grupos**.
2. En la ficha **grupos**, seleccione el grupo que desea eliminar y, a continuación, haga clic en **Eliminar**.
3. En el cuadro de diálogo **Advertencia**, confirme la eliminación haciendo clic en **Sí**.

   Al eliminar un grupo no se eliminan las acciones de grupo asociadas al grupo. Sin embargo, estas acciones de grupo se desasignarán una vez eliminado el grupo.

Agregando reglas de grupo

Puede crear reglas de grupo para que un grupo añada objetos de almacenamiento de forma dinámica, como volúmenes, clústeres o máquinas virtuales de almacenamiento (SVM) al grupo. Debe configurar al menos un grupo de condiciones con al menos una condición para crear una regla de grupo.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Los objetos de almacenamiento que se supervisan actualmente se agregan tan pronto como se crea la regla de grupo. Los nuevos objetos sólo se agregan una vez completado el ciclo de supervisión.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **grupos**.
2. En la ficha **Reglas de grupo**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar regla de grupo**, especifique un nombre para la regla de grupo.
4. En el campo **Tipo de objeto de destino**, seleccione el tipo de objeto de almacenamiento que desea agrupar.
5. En el campo **Grupo**, seleccione el grupo requerido para el que desea crear reglas de grupo.
6. En la sección **Condiciones**, realice los siguientes pasos para crear una condición, un grupo de condiciones o ambos:

Para crear	Realice lo siguiente…
Una condición	a. Seleccione un operando de la lista de operandos. b. Seleccione **contiene** o **es** como operador. c. Introduzca un valor o seleccione un valor de la lista disponible.

Para crear	Realice lo siguiente…
Un grupo de condiciones	a. Haga clic en **Agregar grupo de condiciones** b. Seleccione un operando de la lista de operandos. c. Seleccione **contiene** o **es** como operador. d. Introduzca un valor o seleccione un valor de la lista disponible. e. Haga clic en **Agregar condición** para crear más condiciones si es necesario y repita los pasos de la a a la d para cada condición.

7. Haga clic en **Agregar**.

Ejemplo para crear una regla de grupo

Realice los siguientes pasos en el cuadro de diálogo Agregar regla de grupo para crear una regla de grupo, incluida la configuración de una condición y la adición de un grupo de condiciones:

Pasos

1. Especifique un nombre para la regla de grupo.
2. Seleccione el tipo de objeto como máquina virtual de almacenamiento (SVM).
3. Seleccione un grupo de la lista de grupos.
4. En la sección Condiciones, seleccione **Nombre de objeto** como operando.
5. Seleccione **contiene** como operador.
6. Introduzca el valor como `svm_data`.
7. Haga clic en **Agregar grupo de condiciones**.
8. Seleccione **Nombre de objeto** como operando.
9. Seleccione **contiene** como operador.
10. Introduzca el valor como `vol`.
11. Haga clic en **Agregar condición**.
12. Repita los pasos del 8 al 10 seleccionando **prioridad de datos** como operando en el paso 8, **is** como operador en el paso 9 y **crítico** como valor en el paso 10.
13. Haga clic en **Agregar** para crear la condición para la regla de grupo.

Editar reglas de grupo

Puede editar las reglas de grupo para modificar los grupos de condiciones y las condiciones de un grupo de condiciones para agregar o quitar objetos de almacenamiento a un grupo específico o desde él.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **grupos**.
2. En la ficha **Reglas de grupo**, seleccione la regla de grupo que desea editar y, a continuación, haga clic en **Editar**.
3. En el cuadro de diálogo **Editar regla de grupo**, cambie el nombre de la regla de grupo, el nombre del grupo asociado, los grupos de condición y las condiciones según sea necesario.

   No puede cambiar el tipo de objeto de destino para una regla de grupo.

4. Haga clic en **Guardar**.

Eliminando reglas de grupo

Puede eliminar una regla de grupo de Active IQ Unified Manager cuando la regla de grupo ya no sea necesaria.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Cuando se elimina una regla de grupo, los objetos de almacenamiento asociados se eliminarán del grupo.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **grupos**.
2. En la ficha **Reglas de grupo**, seleccione la regla de grupo que desea eliminar y, a continuación, haga clic en **Eliminar**.
3. En el cuadro de diálogo **Advertencia**, confirme la eliminación haciendo clic en **Sí**.

Agregando acciones de grupo

Puede configurar las acciones de grupo que desee aplicar a los objetos de almacenamiento de un grupo. La configuración de acciones para un grupo permite ahorrar tiempo, ya que no es necesario agregar estas acciones a cada objeto de forma individual.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **grupos**.
2. En la ficha **acciones de grupo**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar acción de grupo**, escriba un nombre y una descripción para la acción.
4. En el menú **Grupo**, seleccione el grupo para el que desea configurar la acción.
5. En el menú **Tipo de acción**, seleccione un tipo de acción.

   El cuadro de diálogo se expande, lo que permite configurar el tipo de acción seleccionado con los parámetros necesarios.

6. Introduzca los valores adecuados para los parámetros necesarios para configurar una acción de grupo.
7. Haga clic en **Agregar**.

Editar acciones de grupo

Puede editar los parámetros de acción del grupo que configuró en Unified Manager, como el nombre de la acción del grupo, la descripción, el nombre del grupo asociado y los parámetros del tipo de acción.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **grupos**.
2. En la ficha **acciones de grupo**, seleccione la acción de grupo que desea editar y, a continuación, haga clic en **Editar**.
3. En el cuadro de diálogo **Editar acción de grupo**, cambie el nombre de la acción de grupo, la descripción, el nombre del grupo asociado y los parámetros del tipo de acción, según sea necesario.
4. Haga clic en **Guardar**.

Configurar los umbrales de estado de volúmenes para grupos

Puede configurar umbrales de estado del volumen a nivel de grupo para la capacidad, las copias Snapshot, las cuotas de qtree, el crecimiento y los inodos.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

El tipo de umbral de estado del volumen de la acción del grupo se aplica solo a los volúmenes de un grupo.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **grupos**.
2. En la ficha **acciones de grupo**, haga clic en **Agregar**.
3. Introduzca un nombre y una descripción para la acción de grupo.
4. En el cuadro desplegable **Grupo**, seleccione el grupo para el que desea configurar la acción de grupo.
5. Seleccione **Tipo de acción** como el umbral de estado del volumen.
6. Seleccione la categoría para la que desea establecer el umbral.
7. Introduzca los valores necesarios para el umbral de estado.
8. Haga clic en **Agregar**.

Eliminar acciones de grupo

Es posible eliminar una acción de grupo de Unified Manager cuando ya no se necesita la acción de grupo.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Cuando se elimina la acción de grupo para el umbral de estado del volumen, se aplican umbrales globales a los objetos de almacenamiento de ese grupo. Cualquier umbral de estado a nivel de objeto que se establezca en el objeto de almacenamiento no se ve afectado.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **grupos**.
2. En la ficha **acciones de grupo**, seleccione la acción de grupo que desea eliminar y, a continuación, haga clic en **Eliminar**.
3. En el cuadro de diálogo **Advertencia**, confirme la eliminación haciendo clic en **Sí**.

Reordenación de acciones de grupo

Puede cambiar el orden de las acciones de grupo que se aplicarán a los objetos de almacenamiento de un grupo. Las acciones de grupo se aplican secuencialmente a objetos de almacenamiento en función de su rango. La clasificación más baja se asigna a la acción de grupo que configuró en último lugar. Puede cambiar el rango de la acción de grupo en función de sus necesidades.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Puede seleccionar una sola fila o varias filas y, a continuación, realizar varias operaciones de arrastrar y soltar para cambiar la clasificación de las acciones del grupo. Sin embargo, debe guardar los cambios para que la repriorización se refleje en la cuadrícula de acciones de grupo.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **grupos**.
2. En la ficha **acciones de grupo**, haga clic en **Reordenar**.
3. En el cuadro de diálogo **Reordenar acciones de grupo**, arrastre y suelte las filas para reorganizar la secuencia de acciones de grupo según sea necesario.
4. Haga clic en **Guardar**.

Priorizando eventos de objetos de almacenamiento mediante anotaciones

Puede crear y aplicar reglas de anotación a los objetos de almacenamiento para poder identificar y filtrar esos objetos en función del tipo de anotación aplicada y su prioridad.

Comprensión más acerca de las anotaciones

Comprender los conceptos sobre las anotaciones permite gestionar los eventos relacionados con los objetos de almacenamiento del entorno.

Qué son las anotaciones

Una anotación es una cadena de texto (el nombre) que se asigna a otra cadena de texto (el valor). Cada par nombre-valor de anotación puede asociarse dinámicamente con

objetos de almacenamiento mediante reglas de anotación. Cuando asocia objetos de almacenamiento con anotaciones predefinidas, puede filtrar y ver los eventos relacionados con ellos. Puede aplicar anotaciones a clústeres, volúmenes y máquinas virtuales de almacenamiento (SVM).

Cada nombre de anotación puede tener varios valores; cada par nombre-valor puede asociarse con un objeto de almacenamiento mediante reglas.

Por ejemplo, se puede crear una anotación denominada «centro de datos» con los valores «'Boston» y «'Canadá». A continuación, puede aplicar la anotación "centro-ATA" con el valor "'Boston'" al volumen v1. Cuando se genera una alerta para cualquier evento en un volumen v1 anotado con "deata-Center", el correo electrónico generado indica la ubicación del volumen "'Boston'", lo que permite priorizar y resolver el problema.

Cómo funcionan las reglas de anotación en Unified Manager

Una regla de anotación es un criterio que se define para anotar los objetos de almacenamiento (volúmenes, clústeres o máquinas virtuales de almacenamiento (SVM). Puede utilizar grupos de condiciones o condiciones para definir reglas de anotación.

- Debe asociar una regla de anotación a una anotación.
- Debe asociar un tipo de objeto para una regla de anotación; sólo se puede asociar un tipo de objeto para una regla de anotación.
- Unified Manager añade o elimina anotaciones de los objetos de almacenamiento después de cada ciclo de supervisión o cuando se crea, se edita, se elimina o se reordena una regla.
- Una regla de anotación puede tener uno o más grupos de condiciones y cada grupo de condiciones puede tener una o más condiciones.
- Los objetos de almacenamiento pueden tener varias anotaciones. Una regla de anotación para una anotación determinada también puede utilizar anotaciones diferentes en las condiciones de regla para agregar otra anotación a objetos ya anotados.

Condiciones

Puede crear varios grupos de condiciones y cada grupo de condiciones puede tener una o más condiciones. Puede aplicar todos los grupos de condiciones definidos en una regla de anotación de una anotación para anotar los objetos de almacenamiento.

Las condiciones dentro de un grupo de condiciones se ejecutan utilizando lógica Y. Deben cumplirse todas las condiciones de un grupo de condiciones. Al crear o modificar una regla de anotación, se crea una condición que aplica, selecciona y anota sólo aquellos objetos de almacenamiento que cumplen todas las condiciones del grupo de condiciones. Puede utilizar varias condiciones dentro de un grupo de condiciones cuando desee limitar el alcance de los objetos de almacenamiento que desea anotar.

Puede crear condiciones con objetos de almacenamiento mediante las operaciones y el operador siguientes y especificando el valor requerido.

Tipo de objeto de almacenamiento	Operandos aplicables
Volumen	• Nombre del objeto • Propietario del nombre del clúster • Nombre de SVM propietario • Anotaciones
SVM	• Nombre del objeto • Propietario del nombre del clúster • Anotaciones
Clúster	• Nombre del objeto • Anotaciones

Cuando se selecciona anotación como operando para cualquier objeto de almacenamiento, el operador "'is'" está disponible. Para el resto de operandos, puede seleccionar "'is'" o "'contains'" como operador. Cuando se selecciona el operador "'is'", la condición se evalúa para una coincidencia exacta del valor de operando con el valor proporcionado para el operando seleccionado. Al seleccionar el operador "'contains'", la condición se evalúa para cumplir uno de los siguientes criterios:

- El valor de operando es una coincidencia exacta con el valor del operando seleccionado.
- El valor de operando contiene el valor proporcionado para el operando seleccionado.

Ejemplo de regla de anotación con condiciones

Considere una regla de anotación con un grupo de condiciones para un volumen con las dos condiciones siguientes:

- El nombre contiene «'vol'»
- El nombre de SVM es «data_svm».

Esta regla de anotación anota todos los volúmenes que incluyen «'vol» en sus nombres y que se alojan en los SVM con el nombre «deata_svm» con la anotación seleccionada y el tipo de anotación.

Grupos de condiciones

Los grupos de condiciones se ejecutan mediante lógico O y, a continuación, se aplican a los objetos de almacenamiento. Los objetos de almacenamiento deben cumplir los requisitos de uno de los grupos de condiciones que se van a anotar. Se anotan los objetos de almacenamiento que cumplen las condiciones de todos los grupos de condiciones. Puede utilizar grupos de condiciones para aumentar el alcance de los objetos de almacenamiento que desea anotar.

Ejemplo de regla de anotación con grupos de condiciones

Considere una regla de anotación con dos grupos de condiciones para un volumen; cada grupo contiene las dos condiciones siguientes:

- Grupo de condición 1

    - El nombre contiene «'vol'»
    - El nombre de SVM es «data_svm». Este grupo de condiciones anota todos los volúmenes que incluyen «'vol» en sus nombres y que están alojados en las SVM con el nombre «data_svm».
- Grupo de condiciones 2
    - El nombre contiene «'vol'»
    - El valor de anotación de la prioridad de datos es «'crítico'» este grupo de condiciones anota todos los volúmenes que incluyen «'vol'» en sus nombres y que se anotan con el valor de anotación de prioridad de datos como «'crítico'».

Cuando se aplica una regla de anotación que contiene estos dos grupos de condiciones a los objetos de almacenamiento, se anotan los siguientes objetos de almacenamiento:

- Todos los volúmenes que incluyan «'vol» en sus nombres y que estén alojados en SVM con el nombre «data_svm».
- Todos los volúmenes que incluyan «'vol'» en sus nombres y que estén anotados con el valor de anotación de prioridad de datos como «'crítico'».

Descripción de los valores de anotación predefinidos

Prioridad de datos es una anotación predefinida que tiene los valores Misión crítica, Alta y Baja. Estos valores permiten anotar los objetos de almacenamiento en función de la prioridad de los datos que contienen. No se pueden editar ni eliminar los valores de anotación predefinidos.

- **Prioridad de datos:Misión crítica**

  Esta anotación se aplica a objetos de almacenamiento que contienen datos críticos. Por ejemplo, los objetos que contienen aplicaciones de producción pueden considerarse críticos para el negocio.

- **Prioridad de datos:Alta**

  Esta anotación se aplica a objetos de almacenamiento que contienen datos de alta prioridad. Por ejemplo, los objetos que alojan aplicaciones de negocio pueden considerarse de alta prioridad.

- **Prioridad de datos:Baja**

  Esta anotación se aplica a objetos de almacenamiento que contienen datos de baja prioridad. Por ejemplo, los objetos que están en almacenamiento secundario, como los destinos de backup y reflejo, pueden ser de baja prioridad.

Adición dinámica de anotaciones

Cuando se crean anotaciones personalizadas, Unified Manager asocia de forma dinámica clústeres, máquinas virtuales de almacenamiento (SVM) y volúmenes con las anotaciones usando reglas. Estas reglas asignan automáticamente las anotaciones a objetos de almacenamiento.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Anotaciones**.
2. En la página **Anotaciones**, haga clic en **Agregar anotación**.
3. En el cuadro de diálogo **Agregar anotación**, escriba un nombre y una descripción para la anotación.
4. Opcional: En la sección **valores de anotación**, haga clic en **Agregar** para agregar valores a la anotación.
5. Haga clic en **Guardar**.

Adición de valores a anotaciones

Puede agregar valores a anotaciones y, a continuación, asociar objetos de almacenamiento a un par de nombre y valor de anotación concreto. Añadir valores a anotaciones le ayuda a gestionar los objetos de almacenamiento de forma más eficaz.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

No se pueden agregar valores a anotaciones predefinidas.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Anotaciones**.
2. En la página **Anotaciones**, seleccione la anotación a la que desea agregar un valor y, a continuación, haga clic en **Agregar** en la sección **valores**.
3. En el cuadro de diálogo **Agregar valor de anotación**, especifique un valor para la anotación.

   El valor especificado debe ser único para la anotación seleccionada.

4. Haga clic en **Agregar**.

Eliminar anotaciones

Puede eliminar anotaciones personalizadas y sus valores cuando ya no sean necesarias.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Los valores de anotación no deben utilizarse en otras anotaciones ni en otras reglas de grupo.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Anotaciones**.
2. En la ficha **Anotaciones**, seleccione la anotación que desea eliminar.

   Se muestran los detalles de la anotación seleccionada.

3. Haga clic en **acciones** > **Eliminar** para eliminar la anotación seleccionada y su valor.
4. En el cuadro de diálogo de advertencia, haga clic en **Sí** para confirmar la eliminación.

Ver la lista de anotaciones y los detalles

Puede ver la lista de anotaciones que están asociadas dinámicamente a clústeres, volúmenes y máquinas virtuales de almacenamiento (SVM). También puede ver detalles como la descripción, creada por, fecha de creación, valores, reglas, y los objetos asociados a la anotación.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Anotaciones**.
2. En la ficha **Anotaciones**, haga clic en el nombre de la anotación para ver los detalles asociados.

Eliminar valores de anotaciones

Puede eliminar valores asociados con anotaciones personalizadas cuando ese valor ya no se aplica a la anotación.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- El valor de anotación no debe estar asociado a ninguna regla de anotación o reglas de grupo.

No se pueden eliminar valores de anotaciones predefinidas.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Anotaciones**.
2. En la lista de anotaciones de la ficha **Anotaciones**, seleccione la anotación desde la que desea eliminar un valor.
3. En el área **valores** de la ficha **Anotaciones**, seleccione el valor que desea eliminar y haga clic en **Eliminar**.
4. En el cuadro de diálogo **Advertencia**, haga clic en **Sí**.

   El valor se elimina y ya no se muestra en la lista de valores para la anotación seleccionada.

Creación de reglas de anotación

Puede crear reglas de anotación que Unified Manager utilice para anotar dinámicamente objetos de almacenamiento, como volúmenes, clústeres o máquinas virtuales de almacenamiento (SVM).

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Los objetos de almacenamiento que se supervisan actualmente se anotan tan pronto como se crea la regla de anotación. Los objetos nuevos se anotan sólo una vez completado el ciclo de supervisión.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Anotaciones**.
2. En la ficha **Reglas de anotación**, haga clic en **Agregar**.

3. En el cuadro de diálogo **Agregar regla de anotación**, especifique un nombre para la regla de anotación.
4. En el campo **Tipo de objeto de destino**, seleccione el tipo de objeto de almacenamiento que desea anotar.
5. En los campos **aplicar anotación**, seleccione el valor de anotación y anotación que desea utilizar.
6. En la sección Condiciones, realice la acción adecuada para crear una condición, un grupo de condiciones o ambos:

Para crear…	Realice lo siguiente…
Una condición	a. Seleccione un operando de la lista de operandos. b. Seleccione **contiene** o **es** como operador. c. Introduzca un valor o seleccione un valor de la lista disponible.
Un grupo de condiciones	a. Haga clic en **Agregar grupo de condiciones**. b. Seleccione un operando de la lista de operandos. c. Seleccione **contiene** o **es** como operador. d. Introduzca un valor o seleccione un valor de la lista disponible. e. Haga clic en **Agregar condición** para crear más condiciones si es necesario y repita los pasos de la a a la d para cada condición.

7. Haga clic en **Agregar**.

Ejemplo de creación de una regla de anotación

Realice los siguientes pasos en el cuadro de diálogo Agregar regla de anotación para crear una regla de anotación, incluida la configuración de una condición y la adición de un grupo de condiciones:

Pasos

1. Especifique un nombre para la regla de anotación.
2. Seleccione el tipo de objeto de destino como máquina virtual de almacenamiento (SVM).
3. Seleccione una anotación de la lista de anotaciones y especifique un valor.
4. En la sección Condiciones, seleccione **Nombre de objeto** como operando.
5. Seleccione **contiene** como operador.
6. Introduzca el valor como `svm_data`.
7. Haga clic en **Agregar grupo de condiciones**.
8. Seleccione **Nombre de objeto** como operando.
9. Seleccione **contiene** como operador.
10. Introduzca el valor como `vol`.
11. Haga clic en **Agregar condición**.

12. Repita los pasos del 8 al 10 seleccionando **prioridad de datos** como operando en el paso 8, **is** como operador en el paso 9, y **misión crítica** como valor en el paso 10.
13. Haga clic en **Agregar**.

Añadir anotaciones manualmente a objetos de almacenamiento individuales

Puede anotar manualmente volúmenes, clústeres y SVM seleccionados sin usar reglas de anotación. Puede anotar un único objeto de almacenamiento o varios objetos de almacenamiento y especificar la combinación de par nombre-valor necesaria para la anotación.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. Desplácese hasta los objetos de almacenamiento que desea anotar:

Para agregar anotaciones a…	Realice lo siguiente…
De clúster	a. Haga clic en **almacenamiento** > **Clusters**. b. Seleccione uno o varios clústeres.
Volúmenes	a. Haga clic en **almacenamiento** > **volúmenes**. b. Seleccione uno o varios volúmenes.
SVM	a. Haga clic en **almacenamiento** > **SVM**. b. Seleccione una o varias SVM.

2. Haga clic en **anotar** y seleccione un par nombre-valor.
3. Haga clic en **aplicar**.

Edición de reglas de anotación

Puede editar las reglas de anotación para modificar los grupos de condiciones y las condiciones del grupo de condiciones para agregar anotaciones o eliminar anotaciones de los objetos de almacenamiento.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Las anotaciones se disocian de los objetos de almacenamiento al editar las reglas de anotación asociadas.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Anotaciones**.
2. En la ficha **Reglas de anotación**, seleccione la regla de anotación que desea editar y, a continuación, haga clic en **acciones** > **Editar**.

3. En el cuadro de diálogo **Editar regla de anotación**, cambie el nombre de la regla, el nombre y el valor de la anotación, los grupos de condición y las condiciones según sea necesario.

   No se puede cambiar el tipo de objeto de destino para una regla de anotación.

4. Haga clic en **Guardar**.

Configuración de condiciones para reglas de anotación

Puede configurar una o más condiciones para crear reglas de anotación que Unified Manager aplica en los objetos de almacenamiento. Los objetos de almacenamiento que cumplen la regla de anotación se anotan con el valor especificado en la regla.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Anotaciones**.
2. En la ficha **Reglas de anotación**, haga clic en **Agregar**.
3. En el cuadro de diálogo **Agregar regla de anotación**, escriba un nombre para la regla.
4. Seleccione un tipo de objeto de la lista Tipo de objeto de destino y, a continuación, seleccione un nombre de anotación y un valor de la lista.
5. En la sección **Condiciones** del cuadro de diálogo, seleccione un operando y un operador de la lista e introduzca un valor de condición, o haga clic en **Agregar condición** para crear una nueva condición.
6. Haga clic en **Guardar y Agregar**.

Ejemplo de configuración de una condición para una regla de anotación

Considere una condición para el tipo de objeto SVM, donde el nombre del objeto contiene «mvm_data».

Realice los siguientes pasos en el cuadro de diálogo Agregar regla de anotación para configurar la condición:

Pasos

1. Escriba un nombre para la regla de anotación.
2. Seleccione el tipo de objeto objetivo como SVM.
3. Seleccione una anotación de la lista de anotaciones y un valor.
4. En el campo **Condiciones**, seleccione **Nombre de objeto** como operando.
5. Seleccione **contiene** como operador.
6. Introduzca el valor como `svm_data`.
7. Haga clic en **Agregar**.

Eliminación de reglas de anotación

Puede eliminar reglas de anotación de Active IQ Unified Manager cuando las reglas ya no sean necesarias.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Al eliminar una regla de anotación, la anotación se desasocia y se elimina de los objetos de almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Anotaciones**.
2. En la ficha **Reglas de anotación**, seleccione la regla de anotación que desea eliminar y haga clic en **Eliminar**.
3. En el cuadro de diálogo **Advertencia**, haga clic en **Sí** para confirmar la eliminación.

Reordenación de las reglas de anotación

Es posible cambiar el orden en que Unified Manager aplica reglas de anotación a los objetos de almacenamiento. Las reglas de anotación se aplican secuencialmente a los objetos de almacenamiento en función de su rango. Al configurar una regla de anotación, la clasificación es mínima. Pero puede cambiar la clasificación de la regla de anotación en función de sus requisitos.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Puede seleccionar una sola fila o varias filas y realizar muchas operaciones de arrastrar y colocar para cambiar el rango de las reglas de anotación. Sin embargo, debe guardar los cambios para que la repriorización se muestre en la pestaña Reglas de anotación.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **Anotaciones**.
2. En la ficha **Reglas de anotación**, haga clic en **reordenar**.
3. En el cuadro de diálogo **Regla de anotación de reordenación**, arrastre y suelte filas únicas o múltiples para reorganizar la secuencia de las reglas de anotación.
4. Haga clic en **Guardar**.

   Debe guardar los cambios para que se muestre la reordenación.

Enviar un paquete de soporte a través de la interfaz de usuario web y la consola de mantenimiento

Debe enviar un bundle de soporte cuando el problema requiere un diagnóstico y una solución de problemas más detallados de los que proporciona un mensaje AutoSupport. Puede enviar un paquete de soporte al soporte técnico mediante la consola de mantenimiento y la interfaz de usuario web de Unified Manager.

Unified Manager almacena un máximo de dos paquetes de soporte completo y tres paquetes de soporte ligeros de una vez.

Información relacionada

"Roles y funcionalidades de usuario de Unified Manager"

Enviar mensajes de AutoSupport y paquetes de soporte al soporte técnico

La página AutoSupport permite enviar mensajes de AutoSupport predefinidos y bajo demanda al equipo de soporte técnico para garantizar el funcionamiento correcto del entorno y ayudarle a mantener la integridad del entorno. AutoSupport está habilitado de forma predeterminada y no debe deshabilitarse, lo que le permite recibir los beneficios de Active IQ de NetApp.

Puede enviar información del sistema de diagnóstico y datos detallados sobre el servidor de Unified Manager en un mensaje tal y como sea necesario, programar un mensaje para que se envíe periódicamente o incluso generar y enviar paquetes de soporte al equipo de soporte técnico.

> Un usuario con el rol de administrador de almacenamiento puede generar y enviar mensajes de AutoSupport bajo demanda y paquetes de soporte al soporte técnico. Sin embargo, sólo un administrador o usuario de mantenimiento puede habilitar o deshabilitar AutoSupport periódico y configurar los ajustes HTTP como se describe en la sección Configuración del servidor proxy HTTP. En un entorno que tiene que usar un servidor proxy HTTP, la configuración debe completarse antes de que el administrador de almacenamiento pueda enviar mensajes de AutoSupport bajo demanda y paquetes de soporte al soporte técnico.

Envío de mensajes de AutoSupport bajo demanda

Puede generar y enviar un mensaje bajo demanda al soporte técnico, a un destinatario de correo electrónico especificado o a ambos.

Pasos

1. Navegue hasta **General** > **AutoSupport** y realice una o ambas de las siguientes acciones:
2. Si desea enviar el mensaje AutoSupport al soporte técnico, active la casilla de verificación **Enviar al soporte técnico**.
3. Si desea enviar el mensaje AutoSupport a un destinatario de correo electrónico específico, active la casilla de verificación **Enviar a destinatario de correo electrónico** e introduzca la dirección de correo electrónico del destinatario.
4. Haga clic en **Guardar**.
5. Haga clic en **generar y enviar AutoSupport**.

Habilitar AutoSupport periódica

Puede enviar mensajes específicos y predefinidos al soporte técnico para el diagnóstico y la resolución periódica de los problemas. Esta funcionalidad está habilitada de forma predeterminada. Si está desactivada, un administrador o un usuario de mantenimiento pueden activar la configuración.

Pasos

1. Navegue hasta **General** > **AutoSupport**.
2. En la sección AutoSupport periódico, active la casilla de verificación **Activar envío periódico de datos AutoSupport a Active IQ** .
3. Si es necesario, defina el nombre, el puerto y la información de autenticación del servidor proxy HTTP como se describe en la sección Configuración del servidor proxy HTTP.
4. Haga clic en **Guardar**.

Carga del bundle de soporte bajo demanda

Es posible generar y enviar un bundle de soporte al soporte técnico en función de los requisitos para la solución de problemas. Unified Manager almacena solo los dos paquetes de soporte generados más recientemente. Los paquetes de soporte más antiguos se eliminan del sistema.

Como algunos tipos de datos de soporte pueden usar una gran cantidad de recursos del clúster o demorar mucho para completarse, cuando selecciona el paquete de soporte completo, puede incluir o excluir tipos de datos específicos para reducir el tamaño del paquete de soporte. También tiene la opción de crear un paquete de soporte ligero que contenga sólo 30 días de registros y registros de la base de datos de configuración, lo que excluye datos de rendimiento, archivos de grabación de adquisición y volcado de pila del servidor.

Pasos

1. Navegue hasta **General** > **AutoSupport**.
2. En la sección paquete de soporte bajo demanda, haga clic en **generar y enviar paquete de soporte**.
3. Para enviar un paquete de soporte ligero al soporte técnico, en la ventana emergente generar y enviar paquete de soporte, seleccione la casilla de comprobación**Generate Light Support Bundle**.
4. Como alternativa, para enviar un paquete de soporte completo, active la casilla de verificación **generar paquete de soporte completo**. Seleccione los tipos de datos específicos que se incluirán o excluyan en el bundle de soporte.

   Aunque no seleccione ningún tipo de datos, el bundle de soporte sigue generado con otros datos de Unified Manager.

5. Active la casilla de verificación **Enviar el paquete al soporte técnico** para generar y enviar el paquete al soporte técnico. Si no selecciona esta casilla de comprobación, el paquete se genera y se almacena localmente en Unified Manager Server. El paquete de soporte generado está disponible para su uso posterior en el directorio /support de los sistemas VMware, en `/opt/netapp/data/support/` En sistemas Linux y en `ProgramData\NetApp\OnCommandAppData\ocum\support` En sistemas Windows.
6. Haga clic en **Enviar**.

Configuración del servidor proxy HTTP

Puede designar un proxy para proporcionar el acceso a Internet a fin de enviar contenido AutoSupport a soporte si su entorno no proporciona acceso directo desde el servidor de Unified Manager. Esta sección sólo está disponible para usuarios de administrador y mantenimiento.

- **Usar proxy HTTP**

  Marque esta casilla para identificar el servidor que se está utilizando como proxy HTTP.

  Introduzca el nombre de host o la dirección IP del servidor proxy y el número de puerto utilizado para conectarse al servidor.

- **Usar autenticación**

  Marque esta casilla si necesita proporcionar información de autenticación para acceder al servidor que se está utilizando como proxy HTTP.

  Introduzca el nombre de usuario y la contraseña necesarias para la autenticación con el proxy HTTP.

Los proxies HTTP que sólo proporcionan autenticación básica no son compatibles.

Acceso a la consola de mantenimiento

Si la interfaz de usuario de Unified Manager no está en funcionamiento o si necesita ejecutar funciones que no están disponibles en la interfaz de usuario, puede acceder a la consola de mantenimiento para gestionar el sistema de Unified Manager.

Lo que necesitará

Debe haber instalado y configurado Unified Manager.

Tras 15 minutos de inactividad, la consola de mantenimiento cierra la sesión.

Cuando se instala en VMware, si ya ha iniciado sesión como usuario de mantenimiento a través de la consola VMware, no podrá iniciar sesión simultáneamente con Secure Shell.

Paso

1. Siga estos pasos para acceder a la consola de mantenimiento:

En este sistema operativo…	Siga estos pasos…
VMware	a. Mediante Secure Shell, conéctese a la dirección IP o al nombre de dominio completo del dispositivo virtual de Unified Manager. b. Inicie sesión en la consola de mantenimiento con su nombre de usuario y contraseña de mantenimiento.
Linux	a. Mediante Secure Shell, conéctese a la dirección IP o al nombre de dominio completo del sistema Unified Manager. b. Inicie sesión en el sistema con el nombre y la contraseña del usuario de mantenimiento (umadmin). c. Introduzca el comando `maintenance_console` Y pulse Intro.
Windows	a. Inicie sesión en el sistema Unified Manager con credenciales de administrador. b. Inicie PowerShell como administrador de Windows. c. Introduzca el comando `maintenance_console` Y pulse Intro.

Se muestra el menú de la consola de mantenimiento de Unified Manager.

Generar y cargar un bundle de soporte

Es posible generar un bundle de soporte, que contiene información de diagnóstico, de modo que se pueda enviar al soporte técnico para la ayuda de solución de problemas.

A partir de Unified Manager 9.8, si el servidor de Unified Manager está conectado a Internet, también puede cargar el paquete de soporte a NetApp desde la consola de mantenimiento.

Lo que necesitará

Debe tener acceso a la consola de mantenimiento como usuario de mantenimiento.

Como algunos tipos de datos de soporte pueden usar una gran cantidad de recursos del clúster o demorar mucho tiempo para completarse, cuando selecciona el paquete de soporte completo puede especificar los tipos de datos que se incluirán o excluir para reducir el tamaño del paquete de soporte. También tiene la opción de crear un paquete de soporte ligero que contenga sólo 30 días de registros y registros de la base de datos de configuración, lo que excluye datos de rendimiento, archivos de grabación de adquisición y volcado de pila del servidor.

Unified Manager almacena solo los dos paquetes de soporte generados más recientemente. Los paquetes de soporte más antiguos se eliminan del sistema.

Pasos

1. En la consola de mantenimiento **Menú principal**, seleccione **Soporte/Diagnóstico**.
2. Seleccione **generar paquete de soporte ligero** o **generar paquete de soporte** dependiendo del nivel de detalles que desee tener en el paquete de soporte.
3. Si elige el paquete de soporte completo, seleccione o anule la selección de los siguientes tipos de datos para incluir o excluir en el paquete de soporte:

   - **volcado de base de datos**

     Un volcado de la base de datos de MySQL Server.

   - **volcado de pila**

     Una copia Snapshot del estado de los procesos principales del servidor de Unified Manager. Esta opción está deshabilitada de forma predeterminada y solo se debe seleccionar cuando el servicio de soporte al cliente lo solicite.

   - **grabaciones de adquisición**

     Un registro de todas las comunicaciones entre Unified Manager y los clústeres supervisados.

   Si anule la selección de todos los tipos de datos, el bundle de soporte se sigue generando con otros datos de Unified Manager.

4. Tipo `g`Y, a continuación, presione Intro para generar el paquete de soporte.

   Dado que la generación de un bundle de soporte es una operación que utiliza bastante memoria, se le solicita que verifique que desea generar el bundle de soporte en este momento.

5. Tipo `y`Y, a continuación, presione Intro para generar el paquete de soporte.

   Si no desea generar el bundle de soporte en este momento, escriba `n`Y, a continuación, pulse Intro.

6. Si incluyó archivos de volcado de base de datos en el bundle de soporte completo, se le solicitará que especifique el periodo de tiempo durante el cual se incluirán las estadísticas de rendimiento. Las estadísticas de rendimiento pueden requerir mucho tiempo y espacio, por lo que también puede volcar la base de datos sin incluir las estadísticas de rendimiento:

   a. Introduzca la fecha de inicio con el formato AAAAMMDD.

      Por ejemplo, introduzca `20210101` Para el 1 de enero de 2021. Introduzca `n` si no desea incluir las estadísticas de rendimiento.

   b. Introduzca la cantidad de días de estadísticas que se incluirán; a partir de las 12:00 en la fecha de inicio especificada.

      Puede introducir un número del 1 al 10.

   Si se incluyen las estadísticas de rendimiento, el sistema muestra el periodo de tiempo durante el cual se recogerán las estadísticas de rendimiento.

7. Una vez creado el paquete de soporte, se le solicitará si desea cargarlo a NetApp. Tipo `y`Y, a continuación, pulse Intro.

   Se le pedirá que introduzca el número de caso de soporte.

8. Si ya dispone de un número de caso, introduzca el número y pulse Intro. En caso contrario, pulse Intro.

   El bundle de soporte se carga a NetApp.

Si el servidor de Unified Manager no está conectado a Internet o si no puede cargar el bundle de soporte por cualquier otro motivo, puede recuperarlo y enviarlo manualmente. Puede recuperarlo con un cliente SFTP o con comandos de la CLI de UNIX o Linux. En instalaciones de Windows puede utilizar Remote Desktop (RDP) para recuperar el paquete de soporte.

El paquete de soporte generado reside en el directorio /Support de los sistemas VMware, en /opt/netapp/data/support/ en sistemas Linux y en ProgramData\NetApp\dAppData\ocum\support en sistemas Windows.

Información relacionada

"Roles y funcionalidades de usuario de Unified Manager"

La recuperación del paquete de soporte con un cliente Windows

Si es un usuario de Windows, puede descargar e instalar una herramienta para recuperar el paquete de soporte desde el servidor de Unified Manager. Es posible enviar el bundle de soporte al soporte técnico para un diagnóstico más detallado de un problema. FileZilla o WinSCP son ejemplos de herramientas que puede utilizar.

Lo que necesitará

Debe ser el usuario de mantenimiento para realizar esta tarea.

Debe usar una herramienta que admita SCP o SFTP.

Pasos

1. Descargue e instale una herramienta para recuperar el paquete de soporte.
2. Abra la herramienta.
3. Conecte con el servidor de gestión de Unified Manager mediante SFTP.

   La herramienta muestra el contenido del directorio /support y se pueden ver todos los paquetes de soporte existentes.

4. Seleccione el directorio de destino del bundle de soporte que desea copiar.
5. Seleccione el paquete de soporte que desea copiar y utilice la herramienta para copiar el archivo del servidor de Unified Manager en el sistema local.

La recuperación del paquete de soporte con un cliente UNIX o Linux

Si es usuario de UNIX o Linux, puede recuperar el bundle de soporte desde el vApp a través de la interfaz de línea de comandos (CLI) en el servidor cliente Linux. Puede usar SCP o SFTP para recuperar el paquete de soporte.

Lo que necesitará

Debe ser el usuario de mantenimiento para realizar esta tarea.

Debe haber generado un bundle de soporte con la consola de mantenimiento y tener disponible el nombre del bundle de soporte.

Pasos

1. Acceda a la CLI a través de Telnet o de la consola, utilizando el servidor cliente Linux.
2. Acceda a /`support` directorio.
3. Recupere el bundle de soporte y cópielo en el directorio local mediante el siguiente comando:

Si está usando…	Después, use el siguiente comando…
SCP	`scp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory>`
SFTP	`sftp <maintenance-user>@<vApp-name-or-ip>:/support/support_bundle_file_name.7z <destination-directory>`

   El nombre del paquete de soporte se proporciona al generarlo mediante la consola de mantenimiento.

4. Introduzca la contraseña del usuario de mantenimiento.

Ejemplos

En el ejemplo siguiente se utiliza SCP para recuperar el paquete de soporte:

```
        `$ scp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `<maintenance_user_password>`
support_bundle_20160216_145359.7z   100%  119MB  11.9MB/s   00:10
```

En el siguiente ejemplo, se usa SFTP para recuperar el paquete de soporte:

```
        `$ sftp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `<maintenance_user_password>`
Connected to 10.228.212.69.
Fetching /support/support_bundle_20130216_145359.7z to
./support_bundle_20130216_145359.7z
/support/support_bundle_20160216_145359.7z
```

Enviar un bundle de soporte al soporte técnico

Cuando un problema requiere un diagnóstico más detallado y una información de solución de problemas que los que ofrece un mensaje AutoSupport, es posible enviar un bundle de soporte al soporte técnico.

Lo que necesitará

Debe tener acceso al bundle de soporte para enviarlo al soporte técnico.

Debe tener un número de caso generado a través del sitio web de soporte técnico.

Pasos

1. Inicie sesión en el sitio de soporte de NetApp.
2. Cargue el archivo.

   "Cómo cargar un archivo en NetApp"

Tareas e información relacionada con varios flujos de trabajo

Algunas tareas y textos de referencia que pueden ayudarle a comprender y completar un flujo de trabajo son comunes a muchos de los flujos de trabajo de Unified Manager, como añadir y revisar notas sobre un evento, asignar un evento, reconocer y resolver eventos, así como detalles sobre volúmenes, máquinas virtuales de almacenamiento (SVM), agregados, y así sucesivamente.

Los componentes del clúster y el motivo por los que pueden estar en contención

Puede identificar los problemas de rendimiento del clúster cuando un componente del clúster entra en disputa. El rendimiento de las cargas de trabajo que utilizan el

componente disminuye y aumenta su tiempo de respuesta (latencia) para las solicitudes de clientes, lo que activa un evento en Unified Manager.

Un componente que está en disputa no puede ejecutarse en un nivel óptimo. Su rendimiento ha disminuido, y el rendimiento de otros componentes del clúster y las cargas de trabajo, llamado *Victimas*, puede haber aumentado la latencia. Para eliminar un componente de la contención, debe reducir su carga de trabajo o aumentar su capacidad para gestionar más trabajo, de modo que el rendimiento pueda volver a los niveles normales. Dado que Unified Manager recopila y analiza el rendimiento de la carga de trabajo en intervalos de cinco minutos, solo detecta cuando un componente de clúster se utiliza de forma coherente en exceso. No se detectan picos transitorios de sobreutilización que duran solo una corta duración dentro del intervalo de cinco minutos.

Por ejemplo, un agregado de almacenamiento puede ser objeto de disputa porque una o más cargas de trabajo en él están compitiendo por sus solicitudes de I/O. Otras cargas de trabajo del agregado pueden verse afectadas, lo que provoca una disminución del rendimiento. Para reducir la cantidad de actividad del agregado, hay diferentes pasos que se pueden realizar, como mover una o varias cargas de trabajo a agregados o nodos menos ocupados para reducir la demanda general de la carga de trabajo en el agregado actual. En el caso de un grupo de políticas de calidad de servicio, puede ajustar el límite de rendimiento o mover cargas de trabajo a otro grupo de políticas, de modo que las cargas de trabajo ya no se aceleren.

Unified Manager supervisa los siguientes componentes del clúster para alertarle cuando los hay en disputa:

- **Red**

  Representa el tiempo de espera de las solicitudes de I/o de los protocolos de red externos del clúster. El tiempo de espera transcurrido para que las transacciones «'están listas para la transferencia» finalicen antes de que el clúster pueda responder a una solicitud de I/O. Si el componente de red es objeto de disputa, significa que un tiempo de espera elevado en la capa de protocolo está afectando a la latencia de una o más cargas de trabajo.

- **Procesamiento de red**

  Representa el componente de software del clúster involucrado en el procesamiento de I/o entre la capa de protocolo y el clúster. Es posible que el nodo que gestiona el procesamiento de red haya cambiado desde que se detectó el evento. Si el componente de red es objeto de disputa, significa que un uso elevado en el nodo de procesamiento de red está afectando a la latencia de una o más cargas de trabajo.

  Cuando se utiliza un clúster de cabina All SAN en una configuración activo-activo, el valor de latencia de procesamiento de red se muestra en ambos nodos para poder verificar que los nodos comparten la carga igualmente.

- **Límite de QoS máx.**

  Representa la configuración máxima de rendimiento (pico) del grupo de políticas de calidad de servicio del almacenamiento asignado a la carga de trabajo. Si el componente del grupo de políticas es objeto de disputa, significa que el límite de rendimiento establecido está acelerando todas las cargas de trabajo del grupo de políticas, lo que afecta a la latencia de una o más cargas de trabajo.

- **Límite de QoS mín.**

  Representa la latencia de una carga de trabajo causada por la configuración de rendimiento mínimo de calidad de servicio (esperado) asignada a otras cargas de trabajo. Si el valor mínimo de calidad de servicio establecido en ciertas cargas de trabajo utiliza la mayoría del ancho de banda para garantizar el rendimiento prometido, se aceleran otras cargas de trabajo y muestran más latencia.

- **Interconexión en cluster**

  Representa los cables y los adaptadores que conectan de forma física los nodos en clúster. Si el componente de interconexión del clúster es objeto de disputa, significa que un tiempo de espera elevado para las solicitudes de I/o en la interconexión del clúster está afectando a la latencia de una o más cargas de trabajo.

- **Procesamiento de datos**

  Representa el componente de software del clúster involucrado en el procesamiento de I/o entre el clúster y el agregado de almacenamiento que contiene la carga de trabajo. Es posible que el nodo que gestiona el procesamiento de datos haya cambiado desde que se detectó el evento. Si el componente de procesamiento de datos es objeto de disputa, significa que un uso elevado en el nodo de procesamiento de datos está afectando a la latencia de una o más cargas de trabajo.

- **Activación de volumen**

  Representa el proceso que realiza un seguimiento del uso de todos los volúmenes activos. En entornos de gran tamaño en los que hay más de 1000 volúmenes activos, este proceso realiza un seguimiento de la cantidad de volúmenes críticos que se necesitan para acceder a los recursos a través del nodo al mismo tiempo. Cuando el número de volúmenes activos simultáneos supera el umbral máximo recomendado, algunos de los volúmenes no críticos experimentan latencia según se identifica aquí.

- **Recursos de MetroCluster**

  Representa los recursos de MetroCluster, incluidos NVRAM y los vínculos interswitch (ISL), que se usan para reflejar datos entre los clústeres de una configuración de MetroCluster. Si el componente MetroCluster es objeto de disputa, significa que el alto rendimiento de escritura de las cargas de trabajo del clúster local o un problema de estado del enlace afectan a la latencia de una o más cargas de trabajo del clúster local. Si el clúster no está en una configuración MetroCluster, este icono no se muestra.

- **Operaciones globales o agregados de SSD**

  Representa el agregado de almacenamiento en el que se ejecutan las cargas de trabajo. Si el componente de agregado es objeto de disputa, significa que un uso elevado en el agregado está afectando a la latencia de una o más cargas de trabajo. Un agregado está formado por todos los HDD, o una combinación de HDD y SSD (un agregado de Flash Pool), o una combinación de HDD y un nivel de cloud (un agregado de FabricPool). Un «agregado SD» está compuesto por todos los SSD (un agregado all-flash) o una combinación de SSD y un nivel de cloud (un agregado de FabricPool).

- **Latencia de cloud**

  Representa el componente de software del clúster involucrado en el procesamiento de I/o entre el clúster y el nivel de cloud en el que se almacenan los datos del usuario. Si el componente de latencia del cloud es objeto de disputa, significa que una gran cantidad de lecturas de volúmenes que están alojados en el nivel de cloud están afectando a la latencia de una o más cargas de trabajo.

- **SnapMirror** sincronizado

  Representa el componente de software del clúster involucrado en la replicación de datos de usuario del volumen primario al secundario en una relación de SnapMirror Synchronous. Si el componente Sync SnapMirror es objeto de disputa, significa que la actividad de las operaciones de SnapMirror Synchronous está afectando a la latencia de una o más cargas de trabajo.

Página de detalles Volume / Health

Puede usar la página de detalles Volume / Health para ver información detallada sobre un volumen seleccionado, como la capacidad, la eficiencia del almacenamiento, la configuración, la protección, anotaciones y eventos generados. También es posible ver información sobre los objetos relacionados y las alertas relacionadas para ese volumen.

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Botones de comando

Los botones de comando permiten realizar las siguientes tareas para el volumen seleccionado:

- **Cambiar a la Vista de rendimiento**

  Permite desplazarse a la página de detalles Volume / Performance.

- **Acciones**
  - Añadir alerta

    Permite añadir una alerta al volumen seleccionado.

  - Editar umbrales

    Permite modificar la configuración de umbral para el volumen seleccionado.

  - Anotar

    Permite anotar el volumen seleccionado.

  - Proteger

    Permite crear relaciones de SnapMirror o SnapVault para el volumen seleccionado.

  - Relación

    Permite ejecutar las siguientes operaciones de relación de protección:

    - Editar

      Abre el cuadro de diálogo Edit Relationship, que permite cambiar las políticas, las programaciones y las tasas de transferencia máximas de SnapMirror existentes para una relación de protección existente.

    - Anular

      Cancela las transferencias que están en curso para una relación seleccionada. De forma opcional, le permite quitar el punto de control de reinicio para transferencias distintas de la transferencia de línea base. No puede quitar el punto de comprobación para una transferencia de línea base.

    - Modo de inactividad

      Deshabilita temporalmente las actualizaciones programadas de una relación seleccionada. Las transferencias que ya están en curso deben completarse antes de que la relación se detiene.

- Interrumpir

  Rompe la relación entre los volúmenes de origen y de destino y cambia el destino a un volumen de lectura/escritura.

- Quitar

  Elimina permanentemente la relación entre el origen y el destino seleccionados. Los volúmenes no se destruyen y las copias Snapshot de los volúmenes no se eliminan. Esta operación no se puede deshacer.

- Reanudar

  Habilita las transferencias programadas para establecer una relación en modo inactivo. En el siguiente intervalo de transferencia programada, se utiliza un punto de control de reinicio, si existe alguno.

- Resincronizar

  Permite volver a sincronizar una relación rota previamente.

- Inicializar/Actualizar

  Le permite realizar una primera transferencia de línea de base en una nueva relación de protección, o realizar una actualización manual si la relación ya se ha inicializado.

- Resincronización inversa

  Permite restablecer una relación de protección previamente rota, invirtiendo la función del origen y el destino haciendo de la fuente una copia del destino original. El contenido del origen se sobrescribe con el contenido del destino y los datos más recientes que los datos de la copia Snapshot común se eliminan.

◦ Restaurar

Permite restaurar datos de un volumen a otro. Para obtener más información, consulte "Restaurar datos mediante la página de detalles Volume / Health".

> El botón Restore y los botones de operación de relación no están disponibles para los volúmenes que se encuentran en relaciones de protección síncrona.

- **Ver volúmenes**

  Permite navegar hasta la vista Estado: Todos los volúmenes.

Pestaña Capacity

En la pestaña capacidad, se muestran detalles sobre el volumen seleccionado, como la capacidad física, la capacidad lógica, la configuración de umbral, la capacidad de cuota y información sobre cualquier operación de movimiento de volúmenes:

- **Capacidad física**

  Detalla la capacidad física del volumen:

- Desbordamiento de instantánea

  Muestra el espacio de datos que consumen las copias Snapshot.

- Utilizado

  Muestra el espacio utilizado por los datos del volumen.

- Advertencia

  Indica que el espacio del volumen está casi lleno. Si se supera este umbral, se genera el evento Space casi Full.

- Error

  Indica que el espacio del volumen está lleno. Si se supera este umbral, se genera el evento Space Full.

- Inutilizable

  Indica que el evento de riesgo de espacio de volumen con aprovisionamiento fino se genera y que el espacio en el volumen con aprovisionamiento fino está en riesgo debido a problemas de capacidad del agregado. La capacidad inutilizable se muestra solo para los volúmenes aprovisionados con thin provisioning.

- Gráfico de datos

  Muestra la capacidad total de datos y la capacidad de datos utilizada del volumen.

  Si el crecimiento automático está habilitado, el gráfico de datos también muestra el espacio disponible en el agregado. En el gráfico de datos, se muestra el espacio de almacenamiento efectivo que pueden utilizar los datos del volumen, que puede ser uno de los siguientes:

  - Capacidad de datos real del volumen en las siguientes condiciones:
    - El crecimiento automático está deshabilitado.
    - El volumen con la función de crecimiento automático habilitada se alcanzó el tamaño máximo.
    - El volumen con un crecimiento excesivo habilitado para el crecimiento automático no puede crecer aún más.
  - Capacidad de datos del volumen después de considerar el tamaño máximo de volumen (para volúmenes con Thin Provisioning y para volúmenes con aprovisionamiento grueso cuando el agregado tiene espacio para que el volumen alcance el tamaño máximo)
  - Capacidad de datos del volumen después de considerar el siguiente tamaño de crecimiento automático posible (para volúmenes con un aprovisionamiento grueso que tienen un umbral de crecimiento automático)

- Gráfico de copias Snapshot

  Este gráfico solo se muestra cuando la capacidad de Snapshot utilizada o la reserva de Snapshot no es cero.

Ambos gráficos muestran la capacidad por la cual la capacidad de Snapshot supera la reserva de Snapshot si la capacidad de Snapshot utilizada supera la reserva de Snapshot.

- **Capacidad lógica**

  Muestra las características de espacio lógico del volumen. El espacio lógico indica el tamaño real de los datos que se almacenan en disco sin aplicar el ahorro derivado de las tecnologías de eficiencia del almacenamiento de ONTAP.

  - Informes de espacio lógico

    Muestra si el volumen tiene configurada la generación de informes de espacio lógico. El valor puede ser Enabled, Disabled o Not aplica. Se muestra «"no aplicable"» para volúmenes de versiones anteriores de ONTAP o en volúmenes que no admiten informes de espacio lógico.

  - Utilizado

    Muestra la cantidad de espacio lógico que utilizan los datos del volumen y el porcentaje de espacio lógico utilizado según la capacidad de datos total.

  - Cumplimiento del espacio lógico

    Muestra si la aplicación del espacio lógico está configurada para volúmenes con Thin Provisioning. Cuando se configura en Enabled, el tamaño lógico utilizado del volumen no puede ser mayor que el tamaño actual del volumen físico establecido.

- **Auto-fila**

  Muestra si el volumen crece automáticamente cuando está sin espacio.

- **Garantía Espacial**

  Muestra el control de configuración de volumen FlexVol cuando un volumen quita los bloques libres de un agregado. A continuación, se garantiza que estos bloques estén disponibles para la escritura en archivos del volumen. La garantía de espacio se puede establecer en una de las siguientes opciones:

  - Ninguno

    No hay ninguna garantía de espacio configurada para el volumen.

  - Archivo

    Se garantiza el tamaño completo de los archivos escritos con escasa densidad (por ejemplo, LUN).

  - Volumen

    El tamaño completo del volumen está garantizado.

  - Parcial

    El volumen FlexCache reserva espacio según su tamaño. Si el tamaño del volumen FlexCache es de 100 MB o más, la garantía de espacio mínimo se establece de forma predeterminada en 100 MB. Si el tamaño del volumen de FlexCache es inferior a 100 MB, la garantía de espacio mínimo se establece en el tamaño del volumen de FlexCache. Si el tamaño del volumen de FlexCache se crece más adelante, la garantía de espacio mínimo no aumenta.

    La garantía de espacio es parcial cuando el volumen es de tipo Data-Cache.

- **Detalles (físicos)**

  Muestra las características físicas del volumen.

- **Capacidad total**

  Muestra la capacidad física total en el volumen.

- **Capacidad de datos**

  Muestra la cantidad de espacio físico utilizado por el volumen (capacidad utilizada) y la cantidad de espacio físico que sigue disponible (capacidad libre) en el volumen. Estos valores también se muestran como un porcentaje de la capacidad física total.

  Cuando el evento de espacio de volumen con aprovisionamiento fino en riesgo se genera para volúmenes con aprovisionamiento fino, se muestra la cantidad de espacio utilizada por el volumen (capacidad utilizada) y la cantidad de espacio disponible en el volumen, pero no se puede utilizar (capacidad inutilizable) debido a problemas de capacidad del agregado.

- **Reserva Snapshot**

  Muestra la cantidad de espacio utilizada por las copias de Snapshot (capacidad utilizada) y la cantidad de espacio disponible para las copias de Snapshot (capacidad libre) del volumen. Estos valores también se muestran como un porcentaje de la reserva total de Snapshot.

  Cuando el evento de espacio de volumen con aprovisionamiento fino en riesgo se genera para volúmenes con aprovisionamiento fino, la cantidad de espacio usado por las copias Snapshot (capacidad utilizada) y la cantidad de espacio disponible en el volumen, pero no se puede utilizar para hacer copias Snapshot (capacidad inutilizable) debido a problemas de capacidad del agregado, se muestra.

- **Umbrales de volumen**

  Muestra los siguientes umbrales de capacidad del volumen:

  - Umbral casi completo

    Especifica el porcentaje en el que un volumen está casi completo.

  - Umbral completo

    Especifica el porcentaje al que se llena un volumen.

- **Otros detalles**

  - Tamaño máximo del crecimiento automático

    Muestra el tamaño máximo hasta el que el volumen puede crecer automáticamente. El valor predeterminado es el 120% del tamaño del volumen cuando se crea. Este campo solo se muestra cuando se habilita el crecimiento automático para el volumen.

  - Capacidad comprometida de la cuota qtree

    Muestra el espacio reservado en las cuotas.

  - La cuota qtree superó la capacidad comprometida

Muestra la cantidad de espacio que se puede utilizar antes de que el sistema genere el evento de exceso de cuota de Volume Qtree.

- Reserva fraccionaria

  Controla el tamaño de la reserva de sobrescritura. De forma predeterminada, la reserva fraccionaria se establece en 100, lo que indica que se reserva el 100% del espacio reservado necesario para que los objetos estén completamente protegidos para sobrescrituras. Si la reserva fraccionaria es inferior al 100 %, el espacio reservado de todos los archivos de espacio reservado en ese volumen se reducirá al porcentaje de reserva fraccionaria.

- Tasa de crecimiento diario de instantáneas

  Muestra el cambio (en porcentaje, o en KB, MB, GB, etc.) que se produce cada 24 horas en las copias Snapshot del volumen seleccionado.

- Snapshot días a completo

  Muestra el número estimado de días que queda antes de que el espacio reservado para las copias de Snapshot en el volumen alcance el umbral especificado.

  El campo Snapshot Days to Full muestra un valor no aplicable cuando la tasa de crecimiento de las copias Snapshot en el volumen es cero o negativa, o cuando no hay datos suficientes para calcular la tasa de crecimiento.

- Eliminación automática de instantáneas

  Especifica si se eliminan automáticamente las copias Snapshot para liberar espacio cuando falla una escritura en un volumen debido a la falta de espacio en el agregado.

- Copias Snapshot

  Muestra información sobre las copias Snapshot del volumen.

  El número de copias Snapshot del volumen se muestra como un enlace. Al hacer clic en el enlace se abre el cuadro de diálogo Snapshot Copies on a Volume, el cual muestra los detalles de las copias Snapshot.

El número de copias de Snapshot se actualiza aproximadamente cada hora; sin embargo, la lista de copias Snapshot se actualiza en el momento en que hace clic en el icono. Esto puede generar una diferencia entre el número de copias de Snapshot que se muestra en la topología y el número de copias de Snapshot que se enumeran cuando hace clic en el icono.

- **Movimiento de volumen**

  Muestra el estado de la operación actual o de la última de movimiento de volumen que se ejecutó en el volumen y otros detalles, como la fase actual de la operación de movimiento de volúmenes que está en curso, agregado de origen, agregado de destino, hora de inicio, hora de finalización y tiempo de finalización estimado.

  También muestra la cantidad de operaciones de movimiento de volúmenes que se realizan en el volumen seleccionado. Para ver más información acerca de las operaciones de movimiento de volúmenes, haga clic en el enlace **Historial de movimiento de volúmenes**.

Pestaña Configuration

En la pestaña Configuration, se muestran detalles sobre el volumen seleccionado, como la política de exportación, el tipo de RAID, la capacidad y las funciones relacionadas con la eficiencia del almacenamiento del volumen:

- **Descripción general**
  - Nombre completo

    Muestra el nombre completo del volumen.
  - Agregados

    Muestra el nombre del agregado en el que reside el volumen o el número de agregados en los que reside el volumen FlexGroup.
  - Política de organización en niveles

    Muestra el conjunto de políticas de organización en niveles del volumen; si el volumen se ha implementado en un agregado habilitado para FabricPool. La política puede ser None, Snapshot only, Backup, Auto o All.
  - Máquina virtual de almacenamiento

    Muestra el nombre de la SVM que contiene el volumen.
  - Ruta de unión

    Muestra el estado de la ruta, que puede ser activa o inactiva. También se muestra la ruta de la SVM a la que se monta el volumen. Puede hacer clic en el enlace **Historial** para ver los cinco cambios más recientes en la ruta de unión.
  - Política de exportación

    Muestra el nombre de la política de exportación que se creó para el volumen. Puede hacer clic en el enlace para ver detalles sobre las políticas de exportación, los protocolos de autenticación y el acceso habilitados en los volúmenes que pertenecen a la SVM.
  - Estilo

    Muestra el estilo de volumen. El estilo del volumen puede ser FlexVol o FlexGroup.
  - Tipo

    Muestra el tipo de volumen seleccionado. El tipo de volumen puede ser de lectura y escritura, uso compartido de carga, protección de datos, caché de datos o temporal.
  - Tipo de RAID

    Muestra el tipo de RAID del volumen seleccionado. El tipo de RAID puede ser RAID0, RAID4, RAID-DP o RAID-TEC.

    Pueden aparecer varios tipos de RAID en los volúmenes de FlexGroup, ya que los volúmenes constituyentes de FlexGroups pueden estar en agregados de diferentes tipos.

- Tipo de SnapLock

  Muestra el tipo de SnapLock del agregado que contiene el volumen.

- Caducidad de SnapLock

  Muestra la fecha de caducidad del volumen SnapLock.

- **Capacidad**
  - Aprovisionamiento ligero

    Muestra si está configurado thin provisioning para el volumen.

  - Crecimiento automático

    Muestra si el volumen flexible crece automáticamente dentro de un agregado.

  - Eliminación automática de instantáneas

    Especifica si se eliminan automáticamente las copias Snapshot para liberar espacio cuando falla una escritura en un volumen debido a la falta de espacio en el agregado.

  - Cuotas

    Especifica si las cuotas están habilitadas para el volumen.

- **Eficiencia**
  - Compresión

    Especifica si la compresión está habilitada o deshabilitada.

  - Deduplicación

    Especifica si la deduplicación está habilitada o deshabilitada.

  - Modo de deduplicación

    Especifica si la operación de deduplicación habilitada en un volumen es una operación manual, programada o basada en políticas. Si el modo se establece en Scheduled, se muestra la programación de las operaciones y, si el modo está configurado en una política, se muestra el nombre de la política.

  - Tipo de deduplicación

    Especifica el tipo de operación de deduplicación que se está ejecutando en el volumen. Si el volumen está en una relación de SnapVault, el tipo que se muestra es SnapVault. Para cualquier otro volumen, el tipo se muestra como normal.

  - Política de eficiencia de almacenamiento

    Especifica el nombre de la política de eficiencia del almacenamiento que se asignó a través de Unified Manager a este volumen. Esta normativa puede controlar la configuración de compresión y deduplicación.

- **Protección**

- Copias Snapshot

  Especifica si las copias Snapshot automáticas están habilitadas o deshabilitadas.

Ficha Protección

En la pestaña Protection, se muestran detalles de protección sobre el volumen seleccionado, como información de desfase, tipo de relación y topología de la relación.

- **Resumen**

  Muestra las propiedades de las relaciones de protección (recuperación ante desastres de SnapMirror, SnapVault o máquina virtual de almacenamiento) de un volumen seleccionado. Para cualquier otro tipo de relación, sólo se muestra la propiedad Tipo de relación. Si se selecciona un volumen primario, solo se muestran la política de copia de Snapshot local y gestionada. Las propiedades mostradas para las relaciones de SnapMirror y SnapVault incluyen las siguientes:

  - Volumen de origen

    Muestra el nombre del origen del volumen seleccionado si el volumen seleccionado es un destino.

  - Estado de desfase

    Muestra el estado de actualización o de desfase de transferencia para una relación de protección. El estado puede ser error, Advertencia o crítico.

    El estado de desfase no se aplica a relaciones síncronas.

  - Duración de desfase

    Muestra la hora a la que los datos del reflejo se retrasan con respecto al origen.

  - Última actualización correcta

    Muestra la fecha y la hora de la actualización de protección más reciente.

    La última actualización realizada correctamente no es aplicable a las relaciones síncronas.

  - Miembro del servicio de almacenamiento

    Muestra Sí o no para indicar si el volumen pertenece o no y está gestionado por un servicio de almacenamiento.

  - Replicación flexible con la versión

    Muestra las opciones Sí, Sí con copia de seguridad o Ninguno. Sí indica que la replicación de SnapMirror es posible aunque los volúmenes de origen y destino ejecuten distintas versiones del software ONTAP. Sí, con la opción de backup indica la implementación de la protección de SnapMirror con la capacidad de conservar varias versiones de copias de backup en el destino. None indica que la replicación flexible de versiones no está activada.

  - Capacidad de relación

    Indica las funcionalidades de ONTAP disponibles para la relación de protección.

- Servicio de protección

  Muestra el nombre del servicio de protección si la relación está gestionada por una aplicación asociada de protección.

- Tipo de relación

  Muestra cualquier tipo de relación, incluidos Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StrictSync, Y sinc.

- Estado de relación

  Muestra el estado de la relación de SnapMirror o SnapVault. El estado puede ser sin inicializar, con SnapMirror o con Broken-Off. Si se selecciona un volumen de origen, no se aplica el estado de relación y no se muestra.

- Estado de transferencia

  Muestra el estado de transferencia de la relación de protección. El estado de la transferencia puede ser uno de los siguientes:

  - Anulando

    Las transferencias de SnapMirror están habilitadas; no obstante, hay una operación de anulación de transferencia que puede incluir la eliminación del punto de comprobación en curso.

  - Comprobando

    El volumen de destino está sometido a una comprobación de diagnóstico y no hay transferencia en curso.

  - Finalizando

    Las transferencias de SnapMirror están habilitadas. El volumen se encuentra actualmente en la fase de postransferencia para las transferencias incrementales de la SnapVault.

  - Inactivo

    Las transferencias están habilitadas y no hay transferencia en curso.

  - Sinc

    Los datos de los dos volúmenes en la relación síncrona están sincronizados.

  - Fuera de sincronización

    Los datos del volumen de destino no están sincronizados con el volumen de origen.

  - Preparando

    Las transferencias de SnapMirror están habilitadas. El volumen se encuentra actualmente en la fase de transferencia previa a las transferencias de SnapVault incrementales.

  - En cola

    Las transferencias de SnapMirror están habilitadas. No hay transferencias en curso.

- En modo inactivo

  Las transferencias de SnapMirror están deshabilitadas. No hay transferencia en curso.

- Ralentización

  Hay una transferencia de SnapMirror en curso. Las transferencias adicionales están deshabilitadas.

- Transfiriendo

  Las transferencias de SnapMirror están habilitadas y hay una transferencia en curso.

- En transición

  Se completó la transferencia asíncrona de datos del volumen de origen al volumen de destino y se inició la transición hacia la operación síncrona.

- Esperando

  Se ha iniciado una transferencia de SnapMirror, pero algunas tareas asociadas están a la espera de que se pongan en cola.

◦ Velocidad máxima de transferencia

Muestra la tasa de transferencia máxima para la relación. La velocidad máxima de transferencia puede ser un valor numérico en kilobytes por segundo (Kbps), megabytes por segundo (Mbps), gigabytes por segundo (Gbps) o terabytes por segundo (Tbps). Si no se muestra ningún límite, la transferencia de línea de base entre relaciones es ilimitada.

◦ Política de SnapMirror

Muestra la política de protección del volumen. DPDefault indica la política de protección de reflejos asíncronos predeterminada, XDPDefault indica la política de almacén asíncrono predeterminada y DPSyncDefault indica la política predeterminada de MirrorVault asíncrono. StrictSync indica la política de protección estricta síncrona predeterminada y Sync indica la política síncrona predeterminada. Puede hacer clic en el nombre de la política para ver los detalles asociados con esa política, incluida la siguiente información:

- Prioridad de transferencia
- Ignorar la configuración de tiempo de acceso
- Intenta limitar
- Comentarios
- Etiquetas de SnapMirror
- Configuración de retención
- Copias Snapshot reales
- Conserve copias Snapshot
- Umbral de advertencia de retención
- Copias Snapshot sin configuración de retención en una relación SnapVault en cascada donde el origen es un volumen de protección de datos (DP); solo se aplica la regla "m_creado".

- Actualizar programa

  Muestra la programación de SnapMirror asignada a la relación. Al colocar el cursor sobre el icono de información se muestran los detalles de la programación.

- Política de Snapshot local

  Muestra la política de copias Snapshot del volumen. La directiva es predeterminada, Ninguno o cualquier nombre otorgado a una directiva personalizada.

- Protegido por

  Muestra el tipo de protección utilizada para el volumen seleccionado. Por ejemplo, si un volumen está protegido por relaciones de volumen de SnapMirror y grupo de coherencia, este campo muestra SnapMirror y el grupo de coherencia. Este campo también proporciona un enlace que le redirige a la página de relaciones para ver el estado de la relación unificada. El vínculo sólo se aplica a las relaciones constituyentes.

- Grupo de consistencia

  Si el volumen está protegido por relaciones de continuidad de negocio de SnapMirror (SM-BC), esta columna muestra el grupo de coherencia del volumen.

- **Vistas**

Muestra la topología de protección del volumen seleccionado. La topología incluye representaciones gráficas de todos los volúmenes relacionados con el volumen seleccionado. El volumen seleccionado se indica con un borde gris oscuro y las líneas entre volúmenes de la topología indican el tipo de relación de protección. La dirección de las relaciones en la topología se muestra de izquierda a derecha, con el origen de cada relación a la izquierda y el destino a la derecha.

Las líneas de doble negrita especifican una relación de duplicación asíncrona, una única línea en negrita especifica una relación de almacén asíncrono, dos líneas individuales especifican una relación de MirrorVault asíncrona y una línea en negrita y una línea en negrita especifica una relación de síncrona. La siguiente tabla indica si la relación síncrona es StrictSync o Sync.

Al hacer clic con el botón derecho en un volumen, se muestra un menú desde el cual se puede elegir entre proteger el volumen o restaurar los datos. Al hacer clic con el botón derecho del ratón en una relación se muestra un menú en el que puede elegir editar, cancelar, desactivar, desactivar, o reanudar una relación.

Los menús no se mostrarán en las siguientes instancias:

- Si la configuración de RBAC no permite esta acción, por ejemplo, si solo tiene privilegios de operador
- Si el volumen está en una relación de protección síncrona
- Si se desconoce el ID de volumen, por ejemplo, cuando todavía no se detectó una relación de interconexión de clústeres y el clúster de destino hace clic en otro volumen de la topología. Se selecciona y se muestra información sobre ese volumen. Un signo de interrogación ( ) en la esquina superior izquierda de un volumen indica que falta el volumen o que aún no se ha detectado. También podría indicar que no se encuentra la información de capacidad. Al colocar el cursor sobre el signo de interrogación, se muestra información adicional, incluidas sugerencias para las acciones correctivas.

La topología muestra información sobre la capacidad de los volúmenes, las copias Snapshot y la última transferencia de datos realizada correctamente si cumple con una de las diferentes plantillas de topología comunes. Si una topología no cumple una de estas plantillas, se muestra información acerca de retraso de volumen y transferencia de datos realizada correctamente en una tabla de relaciones en la topología. En

ese caso, la fila resaltada de la tabla indica el volumen seleccionado y, en la vista de topología, las líneas en negrita con un punto azul indican la relación entre el volumen seleccionado y su volumen de origen.

Las vistas de topología incluyen la siguiente información:

- Capacidad

  Muestra la cantidad total de capacidad utilizada por el volumen. Al colocar el cursor sobre un volumen en la topología, se muestran los ajustes actuales del umbral crítico y de advertencia de ese volumen en el cuadro de diálogo Configuración de umbral actual. También puede editar la configuración de umbral haciendo clic en el enlace **Editar umbrales** del cuadro de diálogo Configuración de umbral actual. Al desactivar la casilla de comprobación **capacidad** se oculta toda la información de capacidad de todos los volúmenes de la topología.

- Desfase

  Muestra la duración de la demora y el estado de la demora de las relaciones de protección entrantes. Al desactivar la casilla de verificación **Lag** se oculta toda la información de Lag de todos los volúmenes de la topología. Cuando la casilla de verificación **Lag** está atenuada, la información de demora del volumen seleccionado se muestra en la tabla de relaciones situada debajo de la topología, así como la información de posposición de todos los volúmenes relacionados.

- Snapshot

  Muestra el número de copias Snapshot disponibles para un volumen. Al desactivar la casilla de verificación **Snapshot**, se oculta toda la información de copias snapshot de todos los volúmenes de la topología. Hacer clic en el icono de una copia Snapshot ( ) Muestra la lista de copias Snapshot de un volumen. El número de copias Snapshot mostrado junto al icono se actualiza aproximadamente cada hora; no obstante, la lista de copias Snapshot se actualiza en el momento en que hace clic en el icono. Esto puede generar una diferencia entre el número de copias de Snapshot que se muestra en la topología y el número de copias de Snapshot que se enumeran cuando hace clic en el icono.

- Última transferencia realizada correctamente

  Muestra la cantidad, la duración, la hora y la fecha de la última transferencia de datos realizada correctamente. Cuando la casilla de verificación **última transferencia satisfactoria** está atenuada, la información de transferencia correcta para el volumen seleccionado se muestra en la tabla de relaciones debajo de la topología, así como la información de la última transferencia correcta para todos los volúmenes relacionados.

    - * Historia*

      Muestra en un gráfico el historial de relaciones de protección de SnapVault y SnapMirror entrantes para el volumen seleccionado. Hay tres gráficos de historial disponibles: Duración del retraso de la relación entrante, duración de la transferencia de la relación entrante y tamaño de transferencia de la relación entrante. La información del historial se muestra solo cuando se selecciona un volumen de destino. Si selecciona un volumen primario, los gráficos están vacíos y se muestra el mensaje no se encontraron datos. Si los volúmenes están protegidos por relaciones síncronas de grupos de coherencia y SnapMirror, no se muestra la información acerca de la duración de transferencia de la relación y el tamaño de transferencia de la relación.

  Puede seleccionar un tipo de gráfico en la lista desplegable situada en la parte superior del panel Historial. También puede ver los detalles de un período de tiempo específico seleccionando 1 semana, 1 mes o 1 año. Los gráficos del historial pueden ayudarle a identificar tendencias: Por ejemplo, si se transfieren

grandes cantidades de datos a la misma hora del día o de la semana, o si se produce una infracción constante en el umbral de aviso de desfase o de error de desfase, puede tomar las medidas adecuadas. Además, puede hacer clic en el botón **Exportar** para crear un informe en formato CSV para el gráfico que está viendo.

Los gráficos del historial de protección muestran la siguiente información:

- **Duración del retraso de la relación**

  Muestra segundos, minutos u horas en el eje vertical (y) y muestra días, meses o años en el eje horizontal (x), dependiendo del período de duración seleccionado. El valor superior del eje y indica la duración máxima de la demora alcanzada en el período de duración indicado en el eje x. La línea naranja horizontal del gráfico muestra el umbral de error de desfase, y la línea amarilla horizontal muestra el umbral de advertencia de desfase. Al colocar el cursor sobre estas líneas se muestra el valor del umbral. La línea azul horizontal muestra la duración del desfase. Para ver los detalles de puntos específicos del gráfico, coloque el cursor sobre un área de interés.

- **Duración de transferencia de relaciones**

  Muestra segundos, minutos u horas en el eje vertical (y) y muestra días, meses o años en el eje horizontal (x), dependiendo del período de duración seleccionado. El valor superior del eje y indica la duración máxima de transferencia alcanzada en el período de duración indicado en el eje x. Para ver los detalles de puntos específicos del gráfico, coloque el cursor sobre el área de interés.

  > Este gráfico no está disponible para los volúmenes que tienen relaciones de protección síncronas.

- **Tamaño transferido de la relación**

  Muestra bytes, kilobytes, megabytes, etc., en el eje vertical (y) según el tamaño de la transferencia y muestra días, meses o años en el eje horizontal (x) dependiendo del período de tiempo seleccionado. El valor superior del eje y indica el tamaño máximo de transferencia alcanzado en el período de duración indicado en el eje x. Para ver los detalles de puntos específicos del gráfico, coloque el cursor sobre un área de interés.

  > Este gráfico no está disponible para los volúmenes que tienen relaciones de protección síncronas.

Historial

En el área Historial, se muestran gráficos que ofrecen información sobre las reservas de capacidad y espacio del volumen seleccionado. Además, puede hacer clic en el botón **Exportar** para crear un informe en formato CSV para el gráfico que está viendo.

Los gráficos pueden estar vacíos y el mensaje no se encontraron datos cuando los datos o el estado del volumen permanecen sin cambios durante un periodo de tiempo.

Puede seleccionar un tipo de gráfico en la lista desplegable situada en la parte superior del panel Historial. También puede ver los detalles de un período de tiempo específico seleccionando 1 semana, 1 mes o 1 año. Los gráficos de historial pueden ayudarle a identificar tendencias, por ejemplo, si el uso de volumen está violando constantemente el umbral casi completo, puede tomar la acción adecuada.

Los gráficos del historial muestran la siguiente información:

- **Capacidad de volumen utilizada**

  Muestra la capacidad utilizada en el volumen y la tendencia en el uso de la capacidad de volumen en función del historial de uso, como gráficos de líneas en bytes, kilobytes, megabytes, etc., en el eje vertical (y). El período de tiempo se muestra en el eje horizontal (x). Puede seleccionar un período de tiempo de una semana, un mes o un año. Puede ver los detalles de puntos específicos del gráfico situando el cursor sobre un área determinada. Puede ocultar o mostrar un gráfico de líneas haciendo clic en la leyenda correspondiente. Por ejemplo, cuando hace clic en la leyenda volumen capacidad utilizada, la línea del gráfico volumen capacidad utilizada está oculta.

- **Capacidad de volumen utilizada frente a total**

  Muestra la tendencia de cómo se utiliza la capacidad de volumen en función del historial de uso, así como la capacidad utilizada, la capacidad total y los detalles del ahorro de espacio obtenido con la deduplicación y la compresión, como gráficos de líneas, en bytes, kilobytes, megabytes, y así sucesivamente, en el eje vertical (y). El período de tiempo se muestra en el eje horizontal (x). Puede seleccionar un período de tiempo de una semana, un mes o un año. Puede ver los detalles de puntos específicos del gráfico situando el cursor sobre un área determinada. Puede ocultar o mostrar un gráfico de líneas haciendo clic en la leyenda correspondiente. Por ejemplo, al hacer clic en la leyenda capacidad de tendencias utilizada, la línea gráfica capacidad de tendencias utilizada está oculta.

- **Capacidad de volumen utilizada (%)**

  Muestra la capacidad utilizada en el volumen y la tendencia en el uso de la capacidad de volumen en función del historial de uso, como gráficos de líneas, en porcentaje, en el eje vertical (y). El período de tiempo se muestra en el eje horizontal (x). Puede seleccionar un período de tiempo de una semana, un mes o un año. Puede ver los detalles de puntos específicos del gráfico situando el cursor sobre un área determinada. Puede ocultar o mostrar un gráfico de líneas haciendo clic en la leyenda correspondiente. Por ejemplo, cuando hace clic en la leyenda volumen capacidad utilizada, la línea del gráfico volumen capacidad utilizada está oculta.

- **Capacidad de instantánea utilizada (%)**

  Muestra el umbral de advertencia de Snapshot y de reserva como gráficos de líneas, y la capacidad utilizada por las copias Snapshot como un gráfico de área, en porcentaje, en el eje vertical (y). El desbordamiento de instantánea se representa con diferentes colores. El período de tiempo se muestra en el eje horizontal (x). Puede seleccionar un período de tiempo de una semana, un mes o un año. Puede ver los detalles de puntos específicos del gráfico situando el cursor sobre un área determinada. Puede ocultar o mostrar un gráfico de líneas haciendo clic en la leyenda correspondiente. Por ejemplo, al hacer clic en la leyenda Reserva de instantáneas, la línea del gráfico Reserva de instantáneas está oculta.

Lista Events

En la lista Eventos se muestran detalles sobre eventos nuevos y reconocidos:

- **Gravedad**

  Muestra la gravedad del evento.

- **Evento**

  Muestra el nombre del evento.

- **Tiempo activado**

Muestra el tiempo transcurrido desde que se generó el evento. Si el tiempo transcurrido supera una semana, se muestra la Marca de tiempo cuando se generó el evento.

Panel Anotaciones relacionadas

El panel Anotaciones relacionadas permite ver detalles de anotaciones asociadas al volumen seleccionado. Los detalles incluyen el nombre de la anotación y los valores de anotación que se aplican al volumen. También puede eliminar anotaciones manuales del panel Anotaciones relacionadas.

Panel Related Devices

El panel Related Devices permite ver y desplazarse a las SVM, los agregados, los qtrees, las LUN y las copias Snapshot relacionadas con el volumen:

- **Máquina virtual de almacenamiento**

  Muestra la capacidad y el estado de la SVM que contiene el volumen seleccionado.

- **Agregado**

  Muestra la capacidad y el estado del agregado que contiene el volumen seleccionado. Para los volúmenes de FlexGroup, se muestra la cantidad de agregados que componen la FlexGroup.

- **Volúmenes en el agregado**

  Muestra la cantidad y la capacidad de todos los volúmenes que pertenecen al agregado principal del volumen seleccionado. El estado de los volúmenes también se muestra, según el nivel de gravedad más alto. Por ejemplo, si un agregado contiene diez volúmenes, cinco de los cuales muestran el estado Advertencia y los cinco restantes muestran el estado crítico, el estado mostrado es crítico. Este componente no se muestra en los volúmenes FlexGroup.

- **Qtrees**

  Muestra la cantidad de qtrees que contiene el volumen seleccionado y la capacidad de qtrees con la cuota que contiene el volumen seleccionado. La capacidad de los qtrees con cuota se muestra en relación con la capacidad de datos del volumen. También se muestra el estado de los qtrees, según el nivel de gravedad más alto. Por ejemplo, si un volumen tiene diez qtrees, cinco con estado Warning y los cinco restantes con estado crítico, el estado mostrado es crucial.

- **Recursos compartidos NFS**

  Muestra el número y el estado de los recursos compartidos de NFS asociados con el volumen.

- **Recursos compartidos SMB**

  Muestra el número y el estado de los recursos compartidos SMB/CIFS.

- **LUN**

  Muestra el número y el tamaño total de todas las LUN del volumen seleccionado. También se muestra el estado de las LUN, en función del nivel de gravedad más alto.

- **Cuotas de usuarios y grupos**

  Muestra el número y el estado de las cuotas de usuario y grupo de usuarios asociadas con el volumen y

sus qtrees.

- **Volúmenes FlexClone**

  Muestra la cantidad y la capacidad de todos los volúmenes clonados del volumen seleccionado. El número y la capacidad solo se muestran si el volumen seleccionado contiene algún volumen clonado.

- **Volumen principal**

  Muestra el nombre y la capacidad del volumen principal de un volumen FlexClone seleccionado. El volumen principal solo se muestra si el volumen seleccionado es un volumen FlexClone.

Panel Related Groups

El panel Related Groups permite ver la lista de grupos asociados con el volumen seleccionado.

Panel Related Alerts

El panel Related Alerts permite ver la lista de alertas creadas para el volumen seleccionado. También es posible añadir una alerta si se hace clic en el enlace Add Alert o editar una alerta existente haciendo clic en el nombre de la alerta.

Página de detalles Storage VM / Health

Puede utilizar la página de detalles Storage VM / Health para ver información detallada acerca de la máquina virtual de almacenamiento seleccionada, como su estado, capacidad, configuración, políticas de datos, interfaces lógicas (LIF), LUN, qtrees, usuarios, cuotas de grupos de usuarios y detalles de protección . También es posible ver información sobre los objetos relacionados y las alertas relacionadas para la máquina virtual de almacenamiento.

Solo puede supervisar máquinas virtuales de almacenamiento de datos.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas para la máquina virtual de almacenamiento seleccionada:

- **Cambiar a la Vista de rendimiento**

  Permite navegar a la página de detalles Storage VM / Performance.

- **Acciones**
  - Añadir alerta

    Permite añadir una alerta a la máquina virtual de almacenamiento seleccionada.

  - Anotar

    Permite anotar la máquina virtual de almacenamiento seleccionada.

- **Ver VM de almacenamiento**

Permite desplazarse a la vista Estado: Todas las máquinas virtuales de almacenamiento.

Estado

La pestaña Estado muestra información detallada sobre los problemas de disponibilidad de datos, capacidad de datos y protección de diversos objetos, como volúmenes, agregados, LIF NAS, LIF SAN, LUN, Protocolos, servicios, recursos compartidos NFS y recursos compartidos CIFS.

Puede hacer clic en el gráfico de un objeto para ver la lista filtrada de objetos. Por ejemplo, puede hacer clic en el gráfico de capacidad del volumen que muestra advertencias para ver la lista de volúmenes que tienen problemas de capacidad con gravedad como advertencia.

- **Problemas de disponibilidad**

  Muestra, como gráfico, el número total de objetos, incluidos los objetos que tienen problemas de disponibilidad y objetos que no tienen problemas relacionados con la disponibilidad. Los colores del gráfico representan los diferentes niveles de gravedad de los problemas. La siguiente información del gráfico proporciona detalles sobre problemas de disponibilidad que pueden afectar o ya han afectado a la disponibilidad de los datos en el equipo virtual de almacenamiento. Por ejemplo, se muestra información acerca de las LIF NAS y las LIF SAN que están inactivas y los volúmenes que están sin conexión.

  También puede ver información acerca de los protocolos y servicios relacionados que se están ejecutando en ese momento, así como del número y el estado de los recursos compartidos NFS y CIFS.

- **Problemas de capacidad**

  Muestra, como gráfico, la cantidad total de objetos, incluidos los objetos que tienen problemas de capacidad y objetos que no tienen problemas relacionados con la capacidad. Los colores del gráfico representan los diferentes niveles de gravedad de los problemas. La siguiente información del gráfico proporciona detalles sobre problemas de capacidad que pueden afectar o ya han afectado a la capacidad de los datos del equipo virtual de almacenamiento. Por ejemplo, se muestra información sobre los agregados que probablemente no cumplan los valores de umbral establecidos.

- **Cuestiones de protección**

  Proporciona una descripción rápida del estado relacionado con la protección de las máquinas virtuales de almacenamiento mostrando, como cuadro de diálogo de campo, el número total de relaciones, incluidas las relaciones que tienen problemas de protección y relaciones que no tienen problemas relacionados con la protección. También se puede ver el estado de la relación de recuperación ante desastres de la máquina virtual de almacenamiento seleccionada. Los eventos de relaciones de recuperación ante desastres de las máquinas virtuales de almacenamiento se muestran aquí y, al hacer clic en ellos, se abre la página de detalles del evento. Cuando existen volúmenes sin proteger, al hacer clic en el enlace se le lleva al estado: Todos los volúmenes, en la vista donde se puede ver una lista filtrada de los volúmenes no protegidos en la máquina virtual de almacenamiento. Los colores del gráfico representan los diferentes niveles de gravedad de los problemas. Al hacer clic en un gráfico, se le lleva a la relación: Todas las relaciones, donde se puede ver una lista filtrada de detalles de relaciones de protección. La siguiente información del gráfico proporciona detalles sobre problemas de protección que pueden afectar o ya han afectado a la protección de datos del equipo virtual de almacenamiento. Por ejemplo, se muestra información acerca de los volúmenes que tienen una reserva de copia Snapshot casi completa o acerca de los problemas con retrasos en la relación con SnapMirror.

Pestaña Capacity

La pestaña capacidad muestra información detallada sobre la capacidad de datos de la SVM seleccionada.

Se muestra la siguiente información para una máquina virtual de almacenamiento con un volumen de FlexVol o FlexGroup:

- **Capacidad**

  El área de capacidad muestra detalles sobre la capacidad asignada y disponible en todos los volúmenes:

  - Capacidad total

    Muestra la capacidad total de la máquina virtual de almacenamiento.

  - Utilizado

    Muestra el espacio utilizado por los datos de los volúmenes que pertenecen a la máquina virtual de almacenamiento.

  - Garantizado disponible

    Muestra el espacio disponible garantizado para datos disponibles para volúmenes en la máquina virtual de almacenamiento.

  - No garantizado

    Muestra el espacio disponible restante para los datos asignados a volúmenes con Thin Provisioning en el equipo virtual de almacenamiento.

- **Volúmenes con problemas de capacidad**

  La lista de volúmenes con problemas de capacidad muestra, en una tabla de resultados, detalles sobre los volúmenes que tienen problemas de capacidad:

  - Estado

    Indica que el volumen tiene un problema relacionado con la capacidad de una gravedad indicada.

    Es posible mover el puntero sobre el estado para ver más información sobre el evento o los eventos relacionados con la capacidad que se generan para el volumen.

    Si el estado del volumen viene determinado por un solo evento, puede ver información como el nombre del evento, la hora y la fecha en que se activó el evento, el nombre del administrador al que se asigna el evento y la causa del evento. Puede utilizar el botón **Ver detalles** para ver más información sobre el evento.

    Si el estado del volumen está determinado por varios eventos de la misma gravedad, los tres eventos principales se muestran con información como el nombre del evento, la hora y la fecha en que se activaron los eventos y el nombre del administrador al que se asignó el evento. Si desea ver más detalles de cada uno de estos eventos, haga clic en el nombre del evento. También puede hacer clic en el enlace **Ver todos los eventos** para ver la lista de eventos generados.

    > Un volumen puede tener varios eventos de la misma gravedad o de diferentes gravedad. Sin embargo, solo se muestra la gravedad más alta. Por ejemplo, si un volumen tiene dos eventos con gravedades de error y advertencia, solo se muestra la gravedad del error.

  - Volumen

Muestra el nombre del volumen.

- Capacidad de datos utilizada

  Muestra, como gráfico, información sobre el uso de la capacidad del volumen (en porcentaje).

- Días a lleno

  Muestra la cantidad estimada de días que quedan antes de que el volumen alcance la capacidad completa.

- Con Thin Provisioning

  Muestra si se ha establecido la garantía de espacio para el volumen seleccionado. Los valores válidos son Yes y no

- Agregados

  Para FlexVol Volumes, se muestra el nombre del agregado que contiene el volumen. Para los volúmenes de FlexGroup, se muestra la cantidad de agregados que se usan en FlexGroup.

Pestaña Configuration

En la pestaña Configuration, se muestran detalles de configuración sobre la máquina virtual de almacenamiento seleccionada, como el clúster, el volumen raíz, el tipo de volúmenes que contiene (volúmenes FlexVol), las políticas y la protección creada en la máquina virtual de almacenamiento:

- **Descripción general**
  - Clúster

    Muestra el nombre del clúster al que pertenece la máquina virtual de almacenamiento.

  - Tipo de volumen permitido

    Muestra el tipo de volúmenes que se pueden crear en la máquina virtual de almacenamiento. El tipo puede ser FlexVol o FlexVol/FlexGroup.

  - Volumen raíz

    Muestra el nombre del volumen raíz de la máquina virtual de almacenamiento.

  - Protocolos permitidos

    Muestra el tipo de protocolos que se pueden configurar en el equipo virtual de almacenamiento. Además, indica si un protocolo está activo (), abajo (), o no está configurado ().

- **Interfaces de red de datos**
  - NAS

    Muestra el número de interfaces NAS asociadas con la máquina virtual de almacenamiento. Además, indica si las interfaces están up () o abajo ().

  - SAN

    Muestra el número de interfaces DE SAN asociadas con la máquina virtual de almacenamiento.

Además, indica si las interfaces están up (🟢) o abajo (🟠).

- FC-NVMe

  Muestra el número de interfaces de FC-NVMe asociadas con la máquina virtual de almacenamiento. Además, indica si las interfaces están up (🟢) o abajo (🟠).

- **Interfaces de red de gestión**
  - Disponibilidad

    Muestra el número de interfaces de gestión asociadas con la máquina virtual de almacenamiento. Además, indica si las interfaces de administración están abiertas (🟢) o abajo (🟠).

- **Políticas**
  - Snapshot

    Muestra el nombre de la política de Snapshot que se crea en la máquina virtual de almacenamiento.

  - Políticas de exportación

    Muestra el nombre de la política de exportación si se crea una sola política o el número de políticas de exportación en caso de que se creen varias.

- **Protección**
  - Recuperación ante desastres de máquinas virtuales de almacenamiento

    Muestra si la máquina virtual de almacenamiento seleccionada está protegida, de destino o desprotegida, y el nombre del destino en el que está protegida la máquina virtual de almacenamiento. Si la máquina virtual de almacenamiento seleccionada es un destino, se muestran los detalles de la máquina virtual de almacenamiento de origen. En caso de dispersión, este campo muestra el número de equipos virtuales de almacenamiento de destino totales en los que está protegida la máquina virtual de almacenamiento. El enlace de recuento lo lleva a la cuadrícula de relaciones de la máquina virtual de almacenamiento filtrada en una máquina virtual de almacenamiento de origen.

  - Volúmenes protegidos

    Muestra el número de volúmenes protegidos en la máquina virtual de almacenamiento seleccionada fuera del total de los volúmenes. Si ve una máquina virtual de almacenamiento de destino, el enlace Number es para los volúmenes de destino de la máquina virtual de almacenamiento seleccionada.

  - Volúmenes sin protección

    Muestra la cantidad de volúmenes sin proteger en la máquina virtual de almacenamiento seleccionada.

- **Servicios**
  - Tipo

    Muestra el tipo de servicio que está configurado en el equipo virtual de almacenamiento. El tipo puede ser sistema de nombres de dominio (DNS) o Servicio de información de red (NIS).

  - Estado

    Muestra el estado del servicio, que puede ser activo (🟢), abajo (🟠), o no configurado (⚪).

- Nombre de dominio

  Muestra los nombres de dominio completos (FQDN) del servidor DNS para los servicios DNS o el servidor NIS para los servicios NIS. Cuando el servidor NIS está activado, se muestra el FQDN activo del servidor NIS. Cuando el servidor NIS está deshabilitado, se muestra la lista de todas las FQDN.

- Dirección IP

  Muestra las direcciones IP del servidor DNS o NIS. Cuando el servidor NIS está activado, se muestra la dirección IP activa del servidor NIS. Cuando el servidor NIS está desactivado, se muestra la lista de todas las direcciones IP.

Pestaña Network interfaces

La pestaña Network interfaces muestra detalles sobre las interfaces de red de datos (LIF) creadas en la máquina virtual de almacenamiento seleccionada:

- **Interfaz de red**

  Muestra el nombre de la interfaz que se crea en la máquina virtual de almacenamiento seleccionada.

- **Estado operativo**

  Muestra el estado operativo de la interfaz, que puede ser Up ( ), abajo ( ), o Desconocido ( ). El estado operativo de una interfaz viene determinado por el estado de sus puertos físicos.

- **Estado administrativo**

  Muestra el estado administrativo de la interfaz, que puede ser activo ( ), abajo ( ), o Desconocido ( ). El administrador de almacenamiento controla el estado administrativo de una interfaz para realizar cambios en la configuración o con fines de mantenimiento. El estado administrativo puede ser diferente del estado operativo. Sin embargo, si el estado administrativo de una interfaz es inactivo, el estado operativo es inactivo de forma predeterminada.

- **Dirección IP / WWPN**

  Muestra la dirección IP de las interfaces Ethernet y el nombre de puerto WWPN de las LIF FC.

- **Protocolos**

  Muestra la lista de protocolos de datos que se especifican para la interfaz, como CIFS, NFS, iSCSI, FC/FCoE, FC-NVMe y FlexCache.

- **Rol**

  Muestra el rol de la interfaz. Los roles pueden ser datos o gestión.

- **Puerto de la casa**

  Muestra el puerto físico al que estaba asociada originalmente la interfaz.

- **Puerto actual**

  Muestra el puerto físico al que está asociada la interfaz actualmente. Si se migra la interfaz, el puerto actual puede ser diferente del puerto de inicio.

- **Conjunto de puertos**

  Muestra el conjunto de puertos al que se asigna la interfaz.

- **Política de relevo**

  Muestra la política de conmutación por error configurada para la interfaz. Para las interfaces NFS, CIFS y FlexCache, la política de recuperación tras fallos predeterminada es Siguiente disponible. La política de conmutación por error no es aplicable a las interfaces de FC e iSCSI.

- **Grupos de enrutamiento**

  Muestra el nombre del grupo de enrutamiento. Puede ver más información sobre las rutas y la puerta de enlace de destino haciendo clic en el nombre del grupo de enrutamiento.

  Los grupos de enrutamiento no son compatibles con ONTAP 8.3 o una versión posterior y, por lo tanto, se muestra una columna vacía para estos clústeres.

- **Grupo de recuperación tras fallos**

  Muestra el nombre del grupo de conmutación por error.

Pestaña Qtrees

La pestaña Qtrees muestra detalles sobre qtrees y sus cuotas. Puede hacer clic en el botón **Editar umbrales** si desea editar la configuración del umbral de estado de la capacidad de qtree para uno o más qtrees.

Utilice el botón **Exportar** para crear un archivo de valores separados por comas (.csv) que contenga los detalles de todos los qtrees supervisados. Cuando se exporta a un archivo CSV, puede optar por crear un informe de qtrees para la máquina virtual de almacenamiento actual, para todas las máquinas virtuales de almacenamiento del clúster actual o para todas las máquinas virtuales de almacenamiento de todos los clústeres del centro de datos. Algunos campos de qtrees adicionales aparecen en el archivo CSV exportado.

- **Estado**

  Muestra el estado actual del qtree. El estado puede ser crítico (), error (), Advertencia (), o normal ().

  Es posible mover el puntero sobre el icono de estado para ver más información acerca del evento o los eventos que se generan para el qtree.

  Si el estado del qtree se determina en función de un único evento, puede ver información como el nombre del evento, la hora y la fecha en que se activó el evento, el nombre del administrador al que se asigna el evento y la causa del evento. Puede utilizar **Ver detalles** para ver más información sobre el evento.

  Si el estado del qtree se determina por varios eventos de la misma gravedad, los tres eventos principales se muestran con información como el nombre del evento, la hora y la fecha en que se desencadenaron los eventos y el nombre del administrador al que se asigna el evento. Si desea ver más detalles de cada uno de estos eventos, haga clic en el nombre del evento. También puede utilizar **Ver todos los eventos** para ver la lista de eventos generados.

  > Un qtree puede tener varios eventos de la misma gravedad o de diferentes niveles. Sin embargo, solo se muestra la gravedad más alta. Por ejemplo, si un qtree tiene dos eventos con gravedades de error y advertencia, solo se muestra la gravedad de error.

- **Qtree**

  Muestra el nombre del qtree.

- **Cluster**

  Muestra el nombre del clúster que contiene el qtree. Sólo aparece en el archivo CSV exportado.

- **Máquina virtual de almacenamiento**

  Muestra el nombre de la máquina virtual de almacenamiento (SVM) que contiene el qtree. Sólo aparece en el archivo CSV exportado.

- **Volumen**

  Muestra el nombre del volumen que contiene el qtree.

  Es posible mover el puntero sobre el nombre del volumen para ver más información sobre él.

- **Conjunto de cuotas**

  Indica si se habilita o se deshabilita una cuota en el qtree.

- **Tipo de cuota**

  Especifica si la cuota es para un usuario, un grupo de usuarios o un qtree. Sólo aparece en el archivo CSV exportado.

- **Usuario o Grupo**

  Muestra el nombre del usuario o del grupo de usuarios. Habrá varias filas para cada usuario y grupo de usuarios. Cuando el tipo de cuota es Qtree o si no se establece la cuota, la columna está vacía. Sólo aparece en el archivo CSV exportado.

- **Disco utilizado %**

  Muestra el porcentaje de espacio en disco utilizado. Si se establece un límite de disco duro, este valor se basa en el límite de disco duro. Si la cuota se establece sin un límite duro de disco, el valor se basa en el espacio de datos de volumen. Si no se establece la cuota o si las cuotas están desactivadas en el volumen al que pertenece el qtree, aparece "'no aplicable'" en la página de la cuadrícula y el campo está vacío en los datos de exportación de CSV.

- **Límite de disco duro**

  Muestra la cantidad máxima de espacio en disco asignado al qtree. Unified Manager genera un evento crítico cuando se alcanza este límite y no se permiten más escrituras de disco. El valor se muestra como "'Unlimited'" en las siguientes condiciones: Si la cuota se establece sin un límite de disco duro, si no se establece la cuota o si las cuotas están desactivadas en el volumen al que pertenece el qtree.

- **Límite de software de disco**

  Muestra la cantidad de espacio en disco asignado al qtree antes de que se genere un evento de advertencia. El valor se muestra como "'Unlimited'" en las siguientes condiciones: Si la cuota se establece sin un límite de software de disco, si no se establece la cuota o si las cuotas están desactivadas en el volumen al que pertenece el qtree. De forma predeterminada, esta columna está oculta.

- **Umbral de disco**

  Muestra el valor de umbral definido en el espacio en disco. El valor se muestra como "'Unlimited'" en las siguientes condiciones: Si la cuota se establece sin un límite de umbral de disco, si no se establece la cuota o si las cuotas están desactivadas en el volumen al que pertenece el qtree. De forma predeterminada, esta columna está oculta.

- **Archivos usados %**

  Muestra el porcentaje de archivos usados en el qtree. Si se establece el límite duro del archivo, este valor se basa en el límite duro del archivo. No se muestra ningún valor si la cuota se establece sin un límite duro de archivo. Si no se establece la cuota o si las cuotas están desactivadas en el volumen al que pertenece el qtree, aparece "'no aplicable'" en la página de la cuadrícula y el campo está vacío en los datos de exportación de CSV.

- **Límite duro de archivos**

  Muestra el límite rígido para el número de archivos permitidos en los qtrees. El valor se muestra como "'Unlimited'" en las siguientes condiciones: Si la cuota se establece sin un límite mínimo de archivo, si no se establece la cuota o si las cuotas están desactivadas en el volumen al que pertenece el qtree.

- **Límite de software de archivo**

  Muestra el límite soft del número de archivos permitidos en los qtrees. El valor se muestra como "'Unlimited'" en las siguientes condiciones: Si la cuota se establece sin un límite de software de archivo, si no se establece la cuota o si las cuotas están desactivadas en el volumen al que pertenece el qtree. De forma predeterminada, esta columna está oculta.

Pestaña User and Group Quotas

Muestra detalles sobre las cuotas de usuario y grupo de usuarios para la máquina virtual de almacenamiento seleccionada. Puede ver información como el estado de la cuota, el nombre del usuario o del grupo de usuarios, los límites de software y de disco duro establecidos en los discos y archivos, la cantidad de espacio en disco y el número de archivos utilizados y el valor de umbral del disco. También puede cambiar la dirección de correo electrónico asociada a un usuario o grupo de usuarios.

- **Botón de comando Editar dirección de correo electrónico**

  Abre el cuadro de diálogo Editar dirección de correo electrónico, que muestra la dirección de correo electrónico actual del usuario o grupo de usuarios seleccionado. Puede modificar la dirección de correo electrónico. Si el campo **Editar dirección de correo electrónico** está en blanco, la regla predeterminada se utiliza para generar una dirección de correo electrónico para el usuario o grupo de usuarios seleccionado.

  Si más de un usuario tiene la misma cuota, los nombres de los usuarios se muestran como valores separados por comas. Además, la regla predeterminada no se utiliza para generar la dirección de correo electrónico; por lo tanto, debe proporcionar la dirección de correo electrónico necesaria para enviar las notificaciones.

- **Botón de comando Configurar reglas de correo electrónico**

  Permite crear o modificar reglas para generar una dirección de correo electrónico para las cuotas de usuario o grupos de usuarios que se han configurado en la máquina virtual de almacenamiento. Se envía una notificación a la dirección de correo electrónico especificada cuando hay una infracción de cuota.

- **Estado**

  Muestra el estado actual de la cuota. El estado puede ser crítico (), Advertencia (), o normal ().

  Es posible mover el puntero por el icono de estado para ver más información sobre el evento o los eventos que se generan para la cuota.

  Si el estado de la cuota está determinado por un solo evento, puede ver información como el nombre del evento, la hora y la fecha en que se activó el evento, el nombre del administrador al que se asigna el evento y la causa del evento. Puede utilizar **Ver detalles** para ver más información sobre el evento.

  Si el estado de la cuota está determinado por varios eventos de la misma gravedad, los tres eventos principales se muestran con información como el nombre del evento, la hora y la fecha en que se desencadenaron los eventos y el nombre del administrador al que se asigna el evento. Si desea ver más detalles de cada uno de estos eventos, haga clic en el nombre del evento. También puede utilizar **Ver todos los eventos** para ver la lista de eventos generados.

  > Una cuota puede tener varios eventos de la misma gravedad o de distintas gravedades. Sin embargo, solo se muestra la gravedad más alta. Por ejemplo, si una cuota tiene dos eventos con gravedades de error y advertencia, sólo se muestra la gravedad del error.

- **Usuario o Grupo**

  Muestra el nombre del usuario o del grupo de usuarios. Si más de un usuario tiene la misma cuota, los nombres de los usuarios se muestran como valores separados por comas.

  El valor se muestra como "'Desconocido'" cuando ONTAP no proporciona un nombre de usuario válido debido a errores de SECD.

- **Tipo**

  Especifica si la cuota es para un usuario o un grupo de usuarios.

- **Volumen o qtree**

  Muestra el nombre del volumen o qtree en el que se ha especificado la cuota de usuario o grupo de usuarios.

  Puede mover el puntero sobre el nombre del volumen o qtree para ver más información acerca del volumen o el qtree.

- **Disco utilizado %**

  Muestra el porcentaje de espacio en disco utilizado. El valor se muestra como "'no aplicable'" si la cuota se establece sin un límite de disco duro.

- **Límite de disco duro**

  Muestra la cantidad máxima de espacio en disco asignado a la cuota. Unified Manager genera un evento crítico cuando se alcanza este límite y no se permiten más escrituras de disco. El valor se muestra como "'Unlimited'" si la cuota se establece sin un límite de disco duro.

- **Límite de software de disco**

  Muestra la cantidad de espacio en disco asignado a la cuota antes de que se genere un evento de

advertencia. El valor se muestra como "'Unlimited'" si la cuota se establece sin un límite de software de disco. De forma predeterminada, esta columna está oculta.

- **Umbral de disco**

  Muestra el valor de umbral definido en el espacio en disco. El valor se muestra como "'Unlimited'" si la cuota se establece sin un límite de umbral de disco. De forma predeterminada, esta columna está oculta.

- **Archivos usados %**

  Muestra el porcentaje de archivos usados en el qtree. El valor se muestra como "'no aplicable'" si la cuota se establece sin un límite mínimo de archivo.

- **Límite duro de archivos**

  Muestra el límite duro para el número de archivos permitidos en la cuota. El valor se muestra como "'Unlimited'" si la cuota se establece sin un límite mínimo de archivo.

- **Límite de software de archivo**

  Muestra el límite de software para el número de archivos permitidos en la cuota. El valor se muestra como "'Unlimited'" si la cuota se establece sin un límite de software de archivo. De forma predeterminada, esta columna está oculta.

- **Dirección de correo electrónico**

  Muestra la dirección de correo electrónico del usuario o grupo de usuarios al que se envían las notificaciones cuando hay una infracción en las cuotas.

Pestaña NFS Shares

En la pestaña NFS Shares, se muestra información sobre los recursos compartidos de NFS, como su estado, la ruta asociada con el volumen (volúmenes de FlexGroup o volúmenes de FlexVol), los niveles de acceso de los clientes a los recursos compartidos de NFS y la política de exportación definida para los volúmenes que se exportan. Los recursos compartidos de NFS no se mostrarán en las siguientes condiciones: Si el volumen no está montado o si los protocolos asociados con la política de exportación del volumen no contienen recursos compartidos NFS.

- **Estado**

  Muestra el estado actual de los recursos compartidos de NFS. El estado puede ser error ( ) O normal ().

- **Ruta del cruce**

  Muestra la ruta en la que se monta el volumen. Si se aplica una política explícita de exportaciones NFS a un qtree, la columna muestra la ruta del volumen a través del cual se puede acceder al qtree.

- **Ruta de unión activa**

  Muestra si la ruta para acceder al volumen montado está activa o inactiva.

- **Volumen o qtree**

  Muestra el nombre del volumen o qtree al que se aplica la política de exportación de NFS. Si se aplica una

política de exportación NFS a un qtree del volumen, la columna muestra los nombres del volumen y del qtree.

Puede hacer clic en el vínculo para ver los detalles del objeto en la página de detalles correspondiente. Si el objeto es un qtree, se muestran enlaces tanto para el qtree como para el volumen.

- **Estado del volumen**

  Muestra el estado del volumen que se está exportando. El estado puede ser sin conexión, en línea, restringida o mixta.

  - Sin conexión

    No se permite el acceso de lectura o escritura al volumen.

  - En línea

    Se permite el acceso de lectura y escritura al volumen.

  - Restringida

    Se permiten operaciones limitadas, como la reconstrucción de paridad, pero no se permite el acceso a los datos.

  - Mixto

    No todos los componentes de un volumen FlexGroup están en el mismo estado.

- **Estilo de seguridad**

  Muestra el permiso de acceso de los volúmenes exportados. El estilo de seguridad puede ser UNIX, Unified, NTFS o mixto.

  - UNIX (clientes NFS)

    Los archivos y los directorios del volumen tienen permisos UNIX.

  - Unificado

    Los archivos y directorios del volumen tienen un estilo de seguridad unificado.

  - NTFS (clientes CIFS)

    Los archivos y directorios del volumen tienen permisos NTFS de Windows.

  - Mixto

    Los archivos y directorios del volumen pueden tener permisos UNIX o NTFS de Windows.

- **Permiso de UNIX**

  Muestra los bits de permiso UNIX en un formato de cadena octal, que se establece para los volúmenes que se exportan. Es similar a los bits de permiso de estilo UNIX.

- **Política de exportación**

Muestra las reglas que definen el permiso de acceso para los volúmenes que se exportan. Puede hacer clic en el enlace para ver detalles sobre las reglas asociadas con la política de exportación, como los protocolos de autenticación y el permiso de acceso.

Pestaña SMB Shares

Muestra información sobre los recursos compartidos de SMB en la máquina virtual de almacenamiento seleccionada. Puede ver información como el estado del recurso compartido de SMB, el nombre del recurso compartido, la ruta asociada con la máquina virtual de almacenamiento, el estado de la ruta de unión del recurso compartido, que contiene el objeto, el estado del volumen que contiene, los datos de seguridad del recurso compartido y las políticas de exportación definidas para el recurso compartido. También puede determinar si existe una ruta NFS equivalente para el recurso compartido de SMB.

Los recursos compartidos de las carpetas no se muestran en la pestaña SMB Shares.

- **Botón de comando Ver asignación de usuarios**

  Abre el cuadro de diálogo asignación de usuarios.

  Es posible ver los detalles de la asignación de usuario de la máquina virtual de almacenamiento.

- **Mostrar botón de comando ACL**

  Abre el cuadro de diálogo Control de acceso del recurso compartido.

  Puede ver detalles de usuarios y permisos del recurso compartido seleccionado.

- **Estado**

  Muestra el estado actual del recurso compartido. El estado puede ser normal ( ) O error ( ).

- **Nombre del recurso compartido**

  Muestra el nombre del recurso compartido de SMB.

- **Ruta**

  Muestra la ruta de unión en la que se ha creado el recurso compartido.

- **Ruta de unión activa**

  Muestra si la ruta de acceso al recurso compartido está activa o inactiva.

- **Objeto que contiene**

  Muestra el nombre del objeto que contiene al que pertenece el recurso compartido. El objeto que contiene puede ser un volumen o un qtree.

  Al hacer clic en el enlace, puede ver los detalles del objeto que contiene en la página Detalles correspondiente. Si el objeto que contiene es un qtree, se muestran enlaces tanto para qtree como para el volumen.

- **Estado del volumen**

  Muestra el estado del volumen que se está exportando. El estado puede ser sin conexión, en línea,

restringida o mixta.

- Sin conexión

  No se permite el acceso de lectura o escritura al volumen.

- En línea

  Se permite el acceso de lectura y escritura al volumen.

- Restringida

  Se permiten operaciones limitadas, como la reconstrucción de paridad, pero no se permite el acceso a los datos.

- Mixto

  No todos los componentes de un volumen FlexGroup están en el mismo estado.

- **Seguridad**

  Muestra el permiso de acceso de los volúmenes exportados. El estilo de seguridad puede ser UNIX, Unified, NTFS o mixto.

  - UNIX (clientes NFS)

    Los archivos y los directorios del volumen tienen permisos UNIX.

  - Unificado

    Los archivos y directorios del volumen tienen un estilo de seguridad unificado.

  - NTFS (clientes CIFS)

    Los archivos y directorios del volumen tienen permisos NTFS de Windows.

  - Mixto

    Los archivos y directorios del volumen pueden tener permisos UNIX o NTFS de Windows.

- **Política de exportación**

  Muestra el nombre de la política de exportación aplicable al recurso compartido. Si no se especifica una política de exportación para la máquina virtual de almacenamiento, el valor se muestra como no habilitado.

  Puede hacer clic en el enlace para ver detalles sobre las reglas asociadas con la política de exportación, como los protocolos de acceso y los permisos. El enlace se deshabilita si la política de exportación se deshabilita para la máquina virtual de almacenamiento seleccionada.

- **Equivalente de NFS**

  Especifica si hay un equivalente de NFS para el recurso compartido.

Pestaña SAN

Muestra detalles sobre las LUN, los iGroups y los iniciadores de la máquina virtual de almacenamiento seleccionada. De forma predeterminada, se muestra la vista de LUN. Puede ver detalles sobre los iGroups en la pestaña iGroups y detalles sobre los iniciadores en la pestaña iniciadores.

- **Ficha LUN**

  Muestra detalles sobre las LUN que pertenecen a la máquina virtual de almacenamiento seleccionada. Puede ver información como el nombre de la LUN, el estado de LUN (en línea o sin conexión), el nombre del sistema de archivos (volumen o qtree) que contiene el LUN, el tipo de sistema operativo del host, la capacidad de datos total y el número de serie de la LUN. La columna LUN Performance proporciona un enlace a la página de detalles LUN/rendimiento.

  También puede ver información si thin provisioning está habilitado en la LUN y si la LUN está asignada a un iGroup. Si la está asignada a un iniciador, puede ver los iGroups y los iniciadores que están asignados a la LUN seleccionada.

- **Ficha iGroups**

  Muestra detalles sobre los iGroups. Puede ver detalles como el nombre del iGroup, el estado de acceso, el tipo de sistema operativo del host que utilizan todos los iniciadores del grupo y el protocolo compatible. Al hacer clic en el enlace de la columna de estado de acceso, puede ver el estado de acceso actual del iGroup.

  - **Normal**

    El iGroup está conectado a varias rutas de acceso.

  - **Ruta única**

    El iGroup está conectado a una sola ruta de acceso.

  - **Sin trayectos**

    No hay una ruta de acceso conectada al iGroup.

    Puede ver si los iGroups están asignados a todas las interfaces o a interfaces específicas a través de un conjunto de puertos. Al hacer clic en el enlace de recuento de la columna interfaces asignadas, se muestran todas las interfaces o las interfaces específicas de un conjunto de puertos. Las interfaces asignadas a través del portal de destino no se muestran. Se muestra el número total de iniciadores y LUN asignados a un iGroup.

  También puede ver las LUN y los iniciadores asignados al iGroup seleccionado.

- **Ficha iniciadores**

  Muestra el nombre y el tipo del iniciador y la cantidad total de iGroups asignados a este iniciador para la máquina virtual de almacenamiento seleccionada.

```
initiator groups that are mapped to the selected initiator group.
```

Panel Anotaciones relacionadas

El panel Anotaciones relacionadas permite ver los detalles de anotaciones asociadas a la VM de almacenamiento seleccionada. Los detalles incluyen el nombre de anotación y los valores de anotación que se aplican a la VM de almacenamiento. También puede eliminar anotaciones manuales del panel Anotaciones relacionadas.

Panel Related Devices

El panel Related Devices permite ver el clúster, los agregados y los volúmenes relacionados con la máquina virtual de almacenamiento:

- **Cluster**

  Muestra el estado del clúster al que pertenece la máquina virtual de almacenamiento.

- **Agregados**

  Muestra la cantidad de agregados que pertenecen a la máquina virtual de almacenamiento seleccionada. También se muestra el estado de los agregados, en función del nivel de gravedad más alto. Por ejemplo, si una máquina virtual de almacenamiento contiene diez agregados, cinco de los cuales muestran el estado de advertencia y los cinco restantes muestran el estado crítico, el estado mostrado es crítico.

- **Agregados asignados**

  Muestra la cantidad de agregados asignados a una máquina virtual de almacenamiento. También se muestra el estado de los agregados, en función del nivel de gravedad más alto.

- **Volúmenes**

  Muestra la cantidad y la capacidad de los volúmenes que pertenecen a la máquina virtual de almacenamiento seleccionada. El estado de los volúmenes también se muestra, según el nivel de gravedad más alto. Si hay volúmenes FlexGroup en la máquina virtual de almacenamiento, la cuenta también incluye FlexGroups, pero no incluye los componentes FlexGroup.

Panel Related Groups

El panel Related Groups le permite ver la lista de grupos asociados a la máquina virtual de almacenamiento seleccionada.

Panel Related Alerts

El panel Related Alerts permite ver la lista de alertas creadas para la máquina virtual de almacenamiento seleccionada. También puede agregar una alerta haciendo clic en el enlace **Agregar alerta** o editar una alerta existente haciendo clic en el nombre de la alerta.

Página de detalles Cluster / Health

La página de detalles Cluster / Health proporciona información detallada sobre un clúster seleccionado, como detalles del estado, la capacidad y la configuración. También puede ver información acerca de las interfaces de red (LIF), los nodos, los discos, los dispositivos relacionados y las alertas relacionadas para el clúster.

El estado junto al nombre del clúster, por ejemplo (bueno), representa el estado de comunicación; si Unified

Manager puede comunicarse con el clúster. No representa el estado de conmutación por error o el estado general del clúster.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas para el clúster seleccionado:

- **Cambiar a la Vista de rendimiento**

  Permite desplazarse a la página de detalles Cluster / Performance.

- **Acciones**

  - Añadir alerta: Se abre el cuadro de diálogo Añadir alerta, que permite añadir una alerta al clúster seleccionado.
  - Volver a detectar: Inicia una actualización manual del clúster, lo que permite a Unified Manager detectar cambios recientes en el clúster.

    Si Unified Manager se empareja con OnCommand Workflow Automation, la operación de nueva detección también vuelve a adquirir datos almacenados en caché de WFA, si los hay.

  Una vez iniciada la operación de redetección, se muestra un enlace a los detalles del trabajo asociado para permitir el seguimiento del estado del trabajo.

  - Annotate: Permite anotar el clúster seleccionado.
- **Ver clusters**

  Permite ir a la vista Estado: Todos los clústeres.

Estado

Muestra información detallada sobre los problemas de disponibilidad de datos y capacidad de datos de diversos objetos del clúster, como nodos, SVM y agregados. Los problemas de disponibilidad están relacionados con la capacidad de servicio de datos de los objetos del clúster. Los problemas de capacidad están relacionados con la funcionalidad de almacenamiento de datos de los objetos del clúster.

Puede hacer clic en el gráfico de un objeto para ver una lista filtrada de los objetos. Por ejemplo, puede hacer clic en el gráfico de capacidad de SVM que muestra advertencias para ver una lista filtrada de SVM. La lista contiene las SVM que tienen volúmenes o qtrees que tienen problemas de capacidad con un nivel de gravedad de advertencia. También puede hacer clic en el gráfico de disponibilidad de las SVM que muestra advertencias para ver la lista de las SVM que tienen problemas de disponibilidad con un nivel de gravedad de advertencia.

Problemas de disponibilidad

Muestra gráficamente el número total de objetos, incluidos los que tienen problemas de disponibilidad y los objetos que no tienen problemas relacionados con la disponibilidad. Los colores del gráfico representan los diferentes niveles de gravedad de los problemas. La información que se muestra a continuación del gráfico proporciona detalles sobre problemas de disponibilidad que pueden afectar o ya han afectado a la disponibilidad de los datos del clúster. Por ejemplo, se muestra información acerca de las bandejas de discos inactivas y los agregados que están sin conexión.

Los datos que se muestran para el gráfico de barra SFO se basan en el estado de alta disponibilidad de los nodos. Los datos que se muestran para el resto de gráficos de barras se calculan en función de los eventos generados.

Problemas de capacidad

Muestra gráficamente la cantidad total de objetos, incluidos los objetos que tienen problemas de capacidad y objetos que no tienen problemas relacionados con la capacidad. Los colores del gráfico representan los diferentes niveles de gravedad de los problemas. La información que se muestra a continuación del gráfico proporciona detalles sobre problemas de capacidad que pueden afectar o ya han afectado a la capacidad de los datos del clúster. Por ejemplo, se muestra información sobre los agregados que probablemente no cumplan los valores de umbral establecidos.

Pestaña Capacity

Muestra información detallada sobre la capacidad del clúster seleccionado.

Capacidad

Muestra el gráfico de capacidad de datos sobre la capacidad utilizada y la capacidad disponible de todos los agregados asignados:

- Espacio lógico utilizado

  El tamaño real de los datos que se almacenan en todos los agregados de este clúster sin aplicar el ahorro derivado del uso de las tecnologías de eficiencia del almacenamiento de ONTAP.

- Utilizado

  La capacidad física que utilizan los datos en todos los agregados. Esto no incluye la capacidad que se utiliza para la paridad, el dimensionamiento correcto y la reserva.

- Disponible

  Muestra la capacidad disponible para los datos.

- Repuestos

  Muestra la capacidad de almacenamiento posible disponible en todos los discos de repuesto.

- Aprovisionado

  Muestra la capacidad que se aprovisiona para todos los volúmenes subyacentes.

Detalles

Muestra información detallada sobre la capacidad utilizada y disponible. El cálculo excluye los datos agregados raíz.

- Capacidad total

  Muestra la capacidad total del clúster. Esto no incluye la capacidad asignada para la paridad.

- Utilizado

Muestra la capacidad que usan los datos. Esto no incluye la capacidad que se utiliza para la paridad, el dimensionamiento correcto y la reserva.

- Disponible

  Muestra la capacidad disponible para los datos.

- Aprovisionado

  Muestra la capacidad que se aprovisiona para todos los volúmenes subyacentes.

- Repuestos

  Muestra la capacidad de almacenamiento posible disponible en todos los discos de repuesto.

Nivel de cloud

Muestra la capacidad total utilizada de los niveles de cloud y la capacidad utilizada para cada nivel de cloud conectado para agregados que admiten FabricPool en el clúster. Un FabricPool puede tener licencia o no tener licencia.

Interrupción de la capacidad física por tipo de disco

El área Physical Capacity Breakout by Disk Type muestra información detallada acerca de la capacidad de disco de los distintos tipos de discos del clúster. Al hacer clic en el tipo de disco, puede ver más información acerca del tipo de disco en la pestaña Disks.

- Capacidad útil total

  Muestra la capacidad disponible y la capacidad de reserva de los discos de datos.

- HDD

  Muestra gráficamente la capacidad utilizada y la capacidad disponible de todos los discos de datos de HDD en el clúster. La línea de puntos representa la capacidad de reserva de los discos de datos del HDD.

- Flash
  - Datos de SSD

    Muestra gráficamente la capacidad utilizada y la capacidad disponible de los discos de datos de unidades de estado sólido en el clúster.

  - Caché SSD

    Muestra gráficamente la capacidad de almacenamiento de los discos de caché SSD en el clúster.

  - Pieza de repuesto de SSD

    Muestra gráficamente la capacidad de reserva de los discos SSD, datos y discos de caché en el clúster.

- Discos sin asignar

  Muestra el número de discos sin asignar en el clúster.

Agregados con lista de problemas de capacidad

Muestra detalles en formato tabular sobre la capacidad utilizada y la capacidad disponible de los agregados que tienen problemas de riesgo de capacidad.

- Estado

  Indica que el agregado tiene un problema relacionado con la capacidad de una cierta gravedad.

  Es posible mover el puntero sobre el estado para ver más información sobre el evento o los eventos que se generan para el agregado.

  Si el estado del agregado está determinado por un solo evento, puede ver información como el nombre del evento, la hora y la fecha en que se activó el evento, el nombre del administrador al que se asigna el evento y la causa del evento. Puede hacer clic en el botón **Ver detalles** para ver más información sobre el evento.

  Si el estado del agregado está determinado por varios eventos de la misma gravedad, los tres eventos principales se muestran con información como el nombre del evento, la hora y la fecha en que se activan los eventos y el nombre del administrador al que se asigna el evento. Si desea ver más detalles de cada uno de estos eventos, haga clic en el nombre del evento. También puede hacer clic en el enlace **Ver todos los eventos** para ver la lista de eventos generados.

  > Un agregado puede tener varios eventos relacionados con la capacidad de la misma gravedad o de diferentes gravedad. Sin embargo, solo se muestra la gravedad más alta. Por ejemplo, si un agregado tiene dos eventos con niveles de gravedad de error y crítico, solo se muestra la gravedad Critical.

- Agregado

  Muestra el nombre del agregado.

- Capacidad de datos utilizada

  Muestra gráficamente la información sobre el uso de la capacidad del agregado (en porcentaje).

- Días a lleno

  Muestra la cantidad estimada de días que quedan antes de que el agregado alcance la capacidad completa.

Pestaña Configuration

Muestra los detalles sobre el clúster seleccionado, como la dirección IP, el contacto y la ubicación:

Descripción general de clúster

- Interfaz de gestión

  Muestra la LIF de gestión del clúster que Unified Manager utiliza para conectarse al clúster. También se muestra el estado operativo de la interfaz.

- Nombre del host o dirección IP

  Muestra el FQDN, el nombre corto o la dirección IP de la LIF de gestión de clústeres que utiliza Unified

Manager para conectarse con el clúster.

- FQDN

  Muestra el nombre de dominio completo (FQDN) del clúster.

- Versión del SO

  Muestra la versión de ONTAP que ejecuta el clúster. Si los nodos del clúster ejecutan versiones diferentes de ONTAP, se muestra la primera versión de ONTAP.

- Contacto

  Muestra detalles sobre el administrador con el que debe ponerse en contacto en caso de problemas con el clúster.

- Ubicación

  Muestra la ubicación del clúster.

- Personalidad

  Identifica si se trata de un clúster configurado de una cabina All SAN.

Información general sobre el clúster remoto

Proporciona detalles sobre el clúster remoto en una configuración de MetroCluster. Esta información solo se muestra para configuraciones MetroCluster.

- Clúster

  Muestra el nombre del clúster remoto. Puede hacer clic en el nombre del clúster para acceder a la página de detalles del clúster.

- Nombre de host o dirección IP

  Muestra el FQDN, el nombre abreviado o la dirección IP del clúster remoto.

- Ubicación

  Muestra la ubicación del clúster remoto.

Información general de MetroCluster

Proporciona detalles sobre el clúster local en una configuración de MetroCluster over FC o MetroCluster over IP. Esta información solo se muestra para configuraciones de MetroCluster over FC o IP.

- Tipo

  Muestra si el tipo de MetroCluster es de dos o cuatro nodos. Para MetroCluster sobre IP, solo se admiten cuatro nodos.

- Configuración

  Muestra la configuración de MetroCluster por FC e IP, que puede tener los siguientes valores:

Para FC

- Configuración de ampliación con cables SAS
- Configuración de ampliación con puente FC-SAS
- Configuración de estructura con switches FC

> Para un MetroCluster de cuatro nodos, solo se admite la configuración estructural con switches FC.

Para IP

- Configuración IP con switches Ethernet (L2 o L3, en función de cómo esté configurado el clúster)
  - Conmutación automática no planificada (NO PLANIFICADA)

    Muestra si la conmutación no planificada automatizada está habilitada para el clúster local. De forma predeterminada, AUSO se encuentra habilitada para todos los clústeres de una configuración de MetroCluster de dos nodos en Unified Manager. Puede utilizar la interfaz de línea de comandos para cambiar la configuración DE AUSO. Solo es compatible con MetroCluster over FC.

  - Modo de conmutación

    Muestra el modo de conmutación para la configuración de MetroCluster over IP. Los valores disponibles son: `Active`, `Negotiated Switchover`, y. `Automatic Unplanned Switchover`.

Nodos

- Disponibilidad

  Muestra el número de nodos que están activos (🟢) o abajo (🟠) en el clúster.

- Versiones de SO

  Muestra las versiones de ONTAP que se están ejecutando los nodos y el número de nodos que ejecutan una versión de ONTAP en particular. Por ejemplo, 9.6 (2), 9.3 (1) especifica que dos nodos ejecutan ONTAP 9.6 y un nodo ejecuta ONTAP 9.3.

Máquinas virtuales de almacenamiento

- Disponibilidad

  Muestra el número de SVM que están up (🟢) o abajo (🟠) en el clúster.

Interfaces de red

- Disponibilidad

  Muestra el número de LIF no data que están up (🟢) o abajo (🟠) en el clúster.

- Interfaces de gestión del clúster

  Muestra el número de LIF de administración de clústeres.

- Interfaces de gestión de nodos

  Muestra el número de LIF de gestión de nodos.

- Interfaces de clúster

  Muestra el número de LIF del clúster.

- Interfaces de interconexión de clústeres

  Muestra el número de LIF de interconexión de clústeres.

Protocolos

- Protocolos de datos

  Muestra la lista de protocolos de datos con licencia que están habilitados para el clúster. Los protocolos de datos incluyen iSCSI, CIFS, NFS, NVMe y FC/FCoE.

Protección

- Mediadores

  Muestra si el clúster admite mediadores y el estado de conectividad del mediador. Indica si el mediador está configurado y, si está configurado, muestra el estado de los mediadores.

  - No aplicable

    Se muestra cuando el clúster no admite mediadores.

  - No configurado

    Se muestra cuando el clúster admite mediadores, pero el mediador no está configurado.

  - Dirección IP

    Se muestra cuando el clúster admite mediadores y el mediador está configurado. El estado del mediador se indica por color. El color verde indica que el estado del mediador es accesible. El color rojo indica que el estado del mediador es inalcanzable.

Niveles de cloud

Enumera los nombres de los niveles de cloud a los que está conectado el clúster. También incluye el tipo (Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage, Google Cloud Storage, Alibaba Cloud Object Storage o StorageGRID) y los estados de los niveles cloud (disponibles o no disponibles).

Pestaña conectividad MetroCluster

Muestra los problemas y el estado de conectividad de los componentes del clúster en la configuración de MetroCluster over FC. Un clúster se muestra en un cuadro rojo cuando el partner de recuperación de desastres del clúster tiene problemas.

La pestaña conectividad de MetroCluster solo se muestra para los clústeres que están en una configuración de MetroCluster over FC.

Puede desplazarse a la página de detalles de un clúster remoto haciendo clic en el nombre del clúster remoto. También puede ver los detalles de los componentes haciendo clic en el enlace contar de un componente. Por ejemplo, al hacer clic en el enlace count del nodo en el clúster se muestra la pestaña Node en la página de detalles del clúster. Al hacer clic en el enlace count de discos en el clúster remoto se muestra la pestaña Disk en la página de detalles del clúster remoto.

Al gestionar una configuración MetroCluster de ocho nodos, al hacer clic en el enlace de recuento del componente bandejas de discos se muestran solo las bandejas locales del par de alta disponibilidad predeterminado. Además, no hay forma de mostrar las bandejas locales en el otro par de alta disponibilidad.

Es posible mover el puntero por los componentes para ver los detalles y el estado de conectividad de los clústeres por si cualquier problema y ver más información sobre el evento o los eventos generados para el problema.

Si el estado del problema de conectividad entre componentes está determinado por un solo evento, puede ver información como el nombre del evento, la hora y la fecha en que se activó el evento, el nombre del administrador al que se asigna el evento y la causa del evento. El botón View Details proporciona más información sobre el evento.

Si el estado del problema de conectividad entre componentes está determinado por varios eventos de la misma gravedad, los tres eventos principales se muestran con información como el nombre del evento, la hora y la fecha en que se activan los eventos y el nombre del administrador al que se asigna el evento. Si desea ver más detalles de cada uno de estos eventos, haga clic en el nombre del evento. También puede hacer clic en el enlace **Ver todos los eventos** para ver la lista de eventos generados.

Pestaña MetroCluster Replication

Muestra el estado de los datos que se están replicando en una configuración de MetroCluster over FC. Puede usar la pestaña replicación de MetroCluster para garantizar la protección de datos mediante el mirroring sincrónico de los datos con clústeres que ya tienen una relación entre iguales. Un clúster se muestra en un cuadro rojo cuando el partner de recuperación de desastres del clúster tiene problemas.

La pestaña MetroCluster Replication solo se muestra para los clústeres que están en una configuración de MetroCluster over FC.

En un entorno de MetroCluster, puede utilizar esta pestaña para comprobar las conexiones lógicas y la relación entre iguales del clúster local con el clúster remoto. Puede ver la representación objetiva de los componentes del clúster con sus conexiones lógicas. Esto ayuda a identificar los problemas que se pueden producir durante el mirroring de metadatos y datos.

En la pestaña replicación de MetroCluster, el clúster local proporciona la representación gráfica detallada del clúster seleccionado y el partner de MetroCluster hace referencia al clúster remoto.

Pestaña Network interfaces

Muestra detalles acerca de todas las LIF sin datos que se crean en el clúster seleccionado.

Interfaz de red

Muestra el nombre de la LIF que se crea en el clúster seleccionado.

Estado operativo

Muestra el estado operativo de la interfaz, que puede ser Up ( ), abajo ( ), o Desconocido ( ). El estado operativo de una interfaz de red está determinado por el estado de sus puertos físicos.

Estado administrativo

Muestra el estado administrativo de la interfaz, que puede ser activo ( ), abajo ( ), o Desconocido ( ). Puede controlar el estado administrativo de una interfaz cuando realice cambios en la configuración o durante el mantenimiento. El estado administrativo puede ser diferente del estado operativo. Sin embargo, si el estado administrativo de una LIF es inactivo, el estado operativo es inactivo de forma predeterminada.

Dirección IP

Muestra la dirección IP de la interfaz.

Función

Muestra el rol de la interfaz. Los roles posibles son las LIF Cluster-Management, las LIF Node-Management, las LIF en clúster y las LIF de interconexión de clústeres.

Puerto de inicio

Muestra el puerto físico al que estaba asociada originalmente la interfaz.

Puerto actual

Muestra el puerto físico al que está asociada la interfaz actualmente. Tras la migración LIF, el puerto actual puede ser diferente del puerto de inicio.

Política de conmutación por error

Muestra la política de conmutación por error configurada para la interfaz.

Grupos de enrutamiento

Muestra el nombre del grupo de enrutamiento. Puede ver más información sobre las rutas y la puerta de enlace de destino haciendo clic en el nombre del grupo de enrutamiento.

Los grupos de enrutamiento no son compatibles con ONTAP 8.3 o una versión posterior y, por lo tanto, se muestra una columna vacía para estos clústeres.

Grupo de recuperación tras fallos

Muestra el nombre del grupo de conmutación por error.

Pestaña Nodes

Muestra información sobre los nodos del clúster seleccionado. Puede ver información detallada acerca de las parejas de alta disponibilidad, las bandejas de discos y los puertos:

Pestaña HA Details

Proporciona una representación gráfica del estado ha y el estado de salud de los nodos del par ha. El estado del nodo se indica con los siguientes colores:

- **Verde**

  El nodo está en una condición de funcionamiento.

- **Amarillo**

  El nodo ha tomado el control del partner o el nodo se enfrenta a algunos problemas de entorno.

- **Rojo**

  El nodo está inactivo.

Puede ver información acerca de la disponibilidad del par de alta disponibilidad y emprender las acciones necesarias para evitar riesgos. Por ejemplo, si existe una posible operación de toma de control, se muestra el siguiente mensaje: Es posible la recuperación tras fallos del almacenamiento.

Puede ver una lista de eventos relacionados con la pareja de ha y su entorno, como ventiladores, suministros de alimentación, batería NVRAM, tarjetas flash, procesador de servicio y conectividad de las bandejas de discos. También puede ver la hora a la que se activaron los eventos.

Puede ver otra información relacionada con los nodos, como el número de modelo.

Si hay clústeres de un solo nodo, también puede ver detalles sobre los nodos.

Bandejas de discos

Muestra información acerca de las bandejas de discos de la pareja de ha.

También es posible ver los eventos generados para las bandejas de discos y los componentes del entorno, así como la hora en que se activaron los eventos.

- **ID de la bandeja**

  Muestra el ID de la bandeja donde está ubicado el disco.

- **Estado de componentes**

  Muestra detalles del entorno de las bandejas de discos, como suministros de alimentación, ventiladores, sensores de temperatura, sensores actuales, conectividad del disco, y sensores de tensión. Los detalles del entorno se muestran como iconos en los siguientes colores:

  - **Verde**

    Los componentes medioambientales funcionan correctamente.

  - **Gris**

    No hay datos disponibles para los componentes medioambientales.

  - **Rojo**

Algunos de los componentes medioambientales están inactivos.

- **Estado**

  Muestra el estado de la bandeja de discos. Los estados posibles son sin conexión, en línea, sin estado, inicialización necesaria, ausente, Y desconocidos.

- **Modelo**

  Muestra el número de modelo de la bandeja de discos.

- **Bandeja de discos locales**

  Indica si la bandeja de discos se encuentra en el clúster local o el clúster remoto. Esta columna solo se muestra para los clústeres de una configuración de MetroCluster.

- **ID exclusivo**

  Muestra el identificador único de la bandeja de discos.

- **Versión del firmware**

  Muestra la versión del firmware de la bandeja de discos.

Puertos

Muestra información sobre los puertos FC, FCoE y Ethernet asociados. Puede ver detalles acerca de los puertos y las LIF asociadas haciendo clic en los iconos del puerto.

También es posible ver los eventos generados para los puertos.

Puede ver los siguientes detalles del puerto:

- Identificador del puerto

  Muestra el nombre del puerto. Por ejemplo, los nombres de puerto pueden ser e0M, e0a y e0b.

- Función

  Muestra la función del puerto. Los roles posibles son Cluster, Data, Intercluster, Node-Management y Undefined.

- Tipo

  Muestra el protocolo de capa física utilizado para el puerto. Los tipos posibles son Ethernet, Fibre Channel y FCoE.

- WWPN

  Muestra el nombre de puerto WWPN del puerto.

- Rev. Firmware

  Muestra la revisión del firmware del puerto FC/FCoE.

- Estado

  Muestra el estado actual del puerto. Los estados posibles son Arriba, abajo, Vincular no conectado o Desconocido ( ).

  Es posible ver los eventos relacionados con el puerto en la lista Events. También puede ver los detalles de la LIF asociada, como el nombre de la LIF, el estado operativo, la dirección IP o WWPN, los protocolos, el nombre de la SVM asociada con la LIF, el puerto actual, la política de conmutación por error y el grupo de conmutación por error.

Pestaña Disks

Muestra detalles sobre los discos del clúster seleccionado. Es posible ver información relacionada con discos, como el número de discos usados, discos de repuesto, discos rotos y discos sin asignar. También es posible ver otros detalles, como el nombre del disco, el tipo de disco y el nodo de propietario del disco.

Resumen de pool de discos

Muestra el número de discos clasificados por tipos efectivos (FCAL, SAS, SATA, MSATA, SSD, NVMe SSD, SSD CAP, Array LUN y VMDISK) y el estado de los discos. También puede ver otros detalles, como el número de agregados, discos compartidos, discos de repuesto, discos rotos, discos sin asignar. y discos no compatibles. Si hace clic en el enlace recuento del tipo de disco efectivo, se muestran los discos del estado seleccionado y el tipo efectivo. Por ejemplo, si hace clic en el enlace count para el estado de disco roto y del tipo efectivo SAS, se muestran todos los discos con el estado de disco roto y el tipo efectivo SAS.

Disco

Muestra el nombre del disco.

Grupos de RAID

Muestra el nombre del grupo RAID.

Nodo del propietario

Muestra el nombre del nodo al que pertenece el disco. Si el disco no está asignado, en esta columna no se muestra ningún valor.

Estado

Muestra el estado del disco: Agregado, compartido, repuesto, roto, sin asignar, No compatibles o Desconocido. De forma predeterminada, esta columna se ordena para mostrar los estados en el siguiente orden: Roto, sin asignar, no admitido, repuesto, agregado, Y compartidas.

Disco local

Muestra Sí o no para indicar si el disco se encuentra en el clúster local o en el clúster remoto. Esta columna solo se muestra para los clústeres de una configuración de MetroCluster.

Posición

Muestra la posición del disco en función del tipo de contenedor: Por ejemplo, copia, datos o paridad. De forma predeterminada, esta columna está oculta.

Agregados afectados

Muestra la cantidad de agregados afectados debido al error de disco. Puede mover el puntero por el enlace de recuento para ver los agregados afectados y, a continuación, hacer clic en el nombre del agregado para ver detalles del agregado. También puede hacer clic en el número de agregados para ver la lista de los agregados afectados en la vista Estado: Todos los agregados.

En esta columna no se muestra ningún valor para los casos siguientes:

- Para discos rotos cuando un clúster que contiene dichos discos se añade a Unified Manager
- Cuando no hay discos con errores

Pool de almacenamiento

Muestra el nombre del pool de almacenamiento al que pertenece el SSD. Es posible mover el puntero por el nombre del pool de almacenamiento para ver detalles del pool de almacenamiento.

Capacidad de almacenamiento posible

Muestra la capacidad del disco disponible para su uso.

Capacidad bruta

Muestra la capacidad del disco sin formato antes del ajuste de tamaño correcto y la configuración RAID. De forma predeterminada, esta columna está oculta.

Tipo

Muestra los tipos de discos: Por ejemplo, ATA, SATA, FCAL o VMDISK.

Tipo efectivo

Muestra el tipo de disco asignado por ONTAP.

Algunos tipos de discos ONTAP se consideran equivalentes para crear y añadir agregados, así como para la gestión de reserva. ONTAP asigna un tipo de disco efectivo para cada tipo de disco.

% De los bloques de reserva consumidos

Muestra en porcentaje los bloques de reserva que se consumen en el disco SSD. Esta columna está vacía para discos distintos de los discos SSD.

% De vida útil estimada utilizada

Muestra en porcentaje una estimación de la vida útil de las unidades SSD utilizadas, según el uso real de las unidades SSD y la predicción del fabricante de la vida útil de las unidades SSD. Un valor mayor de 99 indica que se ha consumido la resistencia estimada, pero no puede indicar un fallo de SSD. Si el valor es desconocido, se omite el disco.

Firmware

Muestra la versión del firmware del disco.

RPM

Muestra las revoluciones por minuto (RPM) del disco. De forma predeterminada, esta columna está oculta.

Modelo

Muestra el número de modelo del disco. De forma predeterminada, esta columna está oculta.

Proveedor

Muestra el nombre del proveedor de discos. De forma predeterminada, esta columna está oculta.

ID de bandeja

Muestra el ID de la bandeja donde está ubicado el disco.

Bahía

Muestra el ID de la bahía donde se encuentra el disco.

Panel Anotaciones relacionadas

Permite ver los detalles de la anotación asociados con el clúster seleccionado. Los detalles incluyen el nombre de la anotación y los valores de anotación que se aplican al clúster. También puede eliminar anotaciones manuales del panel Anotaciones relacionadas.

Panel Related Devices

Permite ver los detalles del dispositivo asociados al clúster seleccionado.

Los detalles incluyen propiedades del dispositivo conectado al clúster, como el tipo de dispositivo, el tamaño, el número y el estado. Puede hacer clic en el enlace de recuento para realizar más análisis en ese dispositivo concreto.

Puede utilizar el panel de partners de MetroCluster para obtener el recuento y los detalles sobre el partner de MetroCluster remoto junto con los componentes de clúster asociados, como nodos, agregados y SVM. El panel MetroCluster Partner solo se muestra para los clústeres de una configuración de MetroCluster.

El panel Related Devices permite ver los nodos, las SVM y los agregados relacionados con el clúster, así como desplazarse hacia los:

Partner de MetroCluster

Muestra el estado del asociado de MetroCluster. El enlace de recuento permite navegar más allá y obtener información acerca del estado y la capacidad de los componentes del clúster.

Nodos

Muestra el número, la capacidad y el estado de los nodos que pertenecen al clúster seleccionado. La capacidad indica la capacidad utilizable total sobre la capacidad disponible.

Máquinas virtuales de almacenamiento

Muestra el número de SVM que pertenecen al clúster seleccionado.

Agregados

Muestra la cantidad, la capacidad y el estado de los agregados que pertenecen al clúster seleccionado.

Panel Related Groups

Le permite ver la lista de grupos que incluyen el clúster seleccionado.

Panel Related Alerts

El panel Related Alerts permite ver la lista de alertas del clúster seleccionado. También es posible añadir una alerta si se hace clic en el enlace Add Alert o editar una alerta existente haciendo clic en el nombre de la alerta.

Información relacionada

"Página Volumes"
"Ver la lista del clúster y sus detalles"

Página de detalles Aggregate / Health

Puede usar la página de detalles Aggregate / Health para ver información detallada sobre el agregado seleccionado, como la capacidad, la información de disco, los detalles de configuración y los eventos generados. También puede ver información sobre los objetos relacionados y las alertas relacionadas de ese agregado.

Botones de comando

> Al supervisar un agregado habilitado para FabricPool, los valores comprometidos y sobrecomprometidos de esta página solo serán relevantes para la capacidad local o el nivel de rendimiento. La cantidad de espacio disponible en el nivel de cloud no se refleja en los valores sobrecomprometidos. Del mismo modo, los valores de umbral agregados sólo son relevantes para el nivel de rendimiento local.

Los botones de comando permiten realizar las siguientes tareas para el agregado seleccionado:

- **Cambiar a la Vista de rendimiento**

  Permite desplazarse a la página de detalles Aggregate / Performance.

- **Acciones**
  - Añadir alerta

    Permite añadir una alerta al agregado seleccionado.

  - Editar umbrales

    Permite modificar la configuración de umbral para el agregado seleccionado.

- **Ver agregados**

  Le permite ir a la vista Estado: Todos los agregados.

Pestaña Capacity

En la pestaña capacidad, se muestra información detallada sobre el agregado seleccionado, como la capacidad, los umbrales y la tasa de crecimiento diario.

De manera predeterminada, no se generan eventos de capacidad para los agregados raíz. Además, los valores de umbral que utiliza Unified Manager no se aplican a los agregados raíz del nodo. Solo un representante del soporte técnico puede modificar la configuración de estos eventos para que se generen. Cuando un representante de soporte técnico modifica la configuración, los valores del umbral se aplican al agregado raíz del nodo.

- **Capacidad**

  Muestra el gráfico de capacidad de datos y el gráfico de copias Snapshot, que muestra detalles de capacidad sobre el agregado:

  - Espacio lógico utilizado

    El tamaño real de los datos que se almacenan en el agregado sin aplicar los ahorros obtenidos con las tecnologías de eficiencia del almacenamiento de ONTAP.

  - Utilizado

    La capacidad física utilizada por los datos en el agregado.

  - Sobrecomprometidos

    Cuando el espacio del agregado está sobrecargado, el gráfico muestra un indicador con la cantidad sobrecomprometida.

  - Advertencia

    Muestra una línea punteada en la ubicación donde se establece el umbral de advertencia; es decir, el espacio del agregado está casi lleno. Si se supera este umbral, se genera el evento Space casi Full.

  - Error

    Muestra una línea sólida en la ubicación en la que se ha definido el umbral de error; es decir, se ha lleno espacio en el agregado. Si se supera este umbral, se genera el evento Space Full.

  - Gráfico de copias Snapshot

    Este gráfico solo se muestra cuando la capacidad de Snapshot utilizada o la reserva de Snapshot no es cero.

  Ambos gráficos muestran la capacidad por la cual la capacidad de Snapshot supera la reserva de Snapshot si la capacidad de Snapshot utilizada supera la reserva de Snapshot.

- **Nivel de cloud**

  Muestra el espacio utilizado por los datos en el nivel de cloud para los agregados habilitados para FabricPool. Un FabricPool puede tener licencia o no tener licencia.

  Cuando el nivel de cloud se refleja en otro proveedor de cloud (el «nivel de irritación»), ambos niveles de cloud se muestran aquí.

- **Detalles**

  Muestra información detallada sobre la capacidad.

  - Capacidad total

    Muestra la capacidad total del agregado.

  - Capacidad de datos

    Muestra la cantidad de espacio utilizada por el agregado (capacidad utilizada) y la cantidad de espacio disponible en el agregado (capacidad libre).

  - Reserva Snapshot

    Muestra la capacidad de la snapshot utilizada y libre del agregado.

  - Capacidad excesiva

    Muestra el exceso de compromiso del agregado. El exceso de compromiso de los agregados le permite proporcionar más almacenamiento del que realmente está disponible en un agregado determinado, siempre que no se utilice todo ese almacenamiento en ese momento. Cuando se utiliza thin provisioning, el tamaño total de volúmenes del agregado puede superar la capacidad total del agregado.

    Si ha comprometido un exceso de espacio en el agregado, debe supervisar con cuidado el espacio disponible y añadir almacenamiento según sea necesario para evitar errores de escritura debido a la falta de espacio.

  - Nivel de cloud

    Muestra el espacio utilizado por los datos en el nivel de cloud para los agregados habilitados para FabricPool. Un FabricPool puede tener licencia o no tener licencia. Cuando el nivel de cloud se refleja en otro proveedor de cloud (el nivel de reflejo), aquí se muestran ambos niveles de cloud

  - Espacio total en caché

    Muestra el espacio total de las unidades de estado sólido (SSD) o las unidades de asignación agregadas a un agregado de Flash Pool. Si habilitó Flash Pool para un agregado, pero no añadió ningún SSD, el espacio de la caché se mostrará como 0 KB.

    Este campo se oculta si Flash Pool está deshabilitado para un agregado.

  - Umbrales del agregado

    Muestra los siguientes umbrales de capacidad del agregado:

    - Umbral casi completo

      Especifica el porcentaje en el que un agregado está casi lleno.

    - Umbral completo

      Especifica el porcentaje en el que está lleno un agregado.

        - Umbral casi sobrecargado

          Especifica el porcentaje en el que un agregado está casi sobrecargado.

        - Umbral sobrecomprometido

          Especifica el porcentaje en el que un agregado está sobrecargado.

    - Otros detalles: Tasa de crecimiento diario

      Muestra el espacio en disco utilizado en el agregado si la tasa de cambio entre las dos últimas muestras continúa durante 24 horas.

      Por ejemplo, si un agregado utiliza 10 GB de espacio en disco a 2 pm y 12 GB a 6 pm, la tasa de crecimiento diario (GB) para este agregado es de 2 GB.

    - Movimiento de volúmenes

      Muestra la cantidad de operaciones de movimiento de volúmenes que actualmente están en curso:

        - Volúmenes

          Muestra la cantidad y la capacidad de los volúmenes que se están moviendo fuera del agregado.

      Puede hacer clic en el enlace para ver más detalles, como el nombre del volumen, el agregado al que se mueve el volumen, el estado de la operación de movimiento de volúmenes y la hora de finalización estimada.

        - Volúmenes de

          Muestra el número y la capacidad restante de los volúmenes que se van a mover al agregado.

    Puede hacer clic en el enlace para ver más detalles, como el nombre del volumen, el agregado desde el cual se mueve el volumen, el estado de la operación de movimiento de volúmenes y la hora de finalización estimada.

    - Capacidad utilizada estimada tras mover un volumen

      Muestra la cantidad estimada de espacio usado (como un porcentaje, y en KB, MB, GB, etc.) en el agregado después de que completen las operaciones de movimiento de volúmenes.

- **Descripción general de la capacidad - volúmenes**

  Muestra gráficos que proporcionan información sobre la capacidad de los volúmenes que contiene el agregado. Se muestra la cantidad de espacio usado por el volumen (capacidad utilizada) y la cantidad de espacio disponible (capacidad libre) del volumen. Cuando el evento de espacio de volumen con aprovisionamiento fino en riesgo se genera para volúmenes con aprovisionamiento fino, se muestra la cantidad de espacio utilizada por el volumen (capacidad utilizada) y la cantidad de espacio disponible en el volumen, pero no se puede utilizar (capacidad inutilizable) debido a problemas de capacidad del agregado.

  Puede seleccionar el gráfico que desea ver en las listas desplegables. Puede ordenar los datos que se muestran en el gráfico para mostrar detalles como el tamaño usado, el tamaño aprovisionado, la capacidad disponible, la tasa de crecimiento diaria más rápida y la tasa de crecimiento más lenta. Puede filtrar los datos en función de las máquinas virtuales de almacenamiento (SVM) que contengan los volúmenes del agregado. También es posible ver detalles de los volúmenes aprovisionados con thin

provisioning. Para ver los detalles de puntos específicos del gráfico, coloque el cursor sobre el área de interés. De forma predeterminada, el gráfico muestra los 30 volúmenes filtrados más importantes en el agregado.

Pestaña Disk Information

Muestra información detallada sobre los discos del agregado seleccionado, incluido el tipo y el tamaño de RAID y el tipo de discos utilizados en el agregado. La ficha también muestra gráficamente los grupos RAID y los tipos de discos utilizados (como SAS, ATA, FCAL, SSD o VMDISK). Es posible ver más información, como la bahía de disco, la bandeja y la velocidad de rotación, colocando el cursor sobre los discos de paridad y los discos de datos.

- **Datos**

  Muestra gráficamente los detalles sobre discos de datos dedicados, discos de datos compartidos o ambos. Cuando los discos de datos contienen discos compartidos, se muestran detalles gráficos de los discos compartidos. Cuando los discos de datos contienen discos dedicados y discos compartidos, se muestran detalles gráficos de los discos de datos dedicados y los discos de datos compartidos.

  - **Detalles de RAID**

    Los detalles de RAID se muestran solo para los discos dedicados.

    - Tipo

      Muestra el tipo de RAID (RAID0, RAID4, RAID-DP o RAID-TEC).

    - Tamaño del grupo

      Muestra el número máximo de discos permitidos en el grupo RAID.

    - Grupos

      Muestra el número de grupos RAID en el agregado.

  - **Discos utilizados**
    - Tipo efectivo

      Muestra los tipos de discos de datos (por ejemplo, ATA, SATA, FCAL, SSD, O VMDISK) en el agregado.

    - Discos de datos

      Muestra la cantidad y la capacidad de los discos de datos que están asignados a un agregado. Los detalles de los discos de datos no se muestran cuando el agregado solo contiene discos compartidos.

    - Discos de paridad

      Muestra el número y la capacidad de los discos de paridad que se asignan a un agregado. Los detalles del disco de paridad no se muestran cuando el agregado solo contiene discos compartidos.

    - Discos compartidos

Muestra la cantidad y la capacidad de los discos de datos compartidos que se asignan a un agregado. Los detalles de los discos compartidos solo se muestran cuando el agregado contiene discos compartidos.

- **Discos de repuesto**

  Muestra el tipo, el número y la capacidad efectivos de los discos de datos de repuesto que están disponibles para el nodo en el agregado seleccionado.

  Cuando un agregado se cambia al nodo del partner, Unified Manager no muestra todos los discos de repuesto que sean compatibles con el agregado.

- **Caché SSD**

  Proporciona detalles sobre discos SSD de caché dedicados y discos SSD de caché compartida.

  Se muestran los siguientes detalles de los discos SSD de caché dedicada:

  - **Detalles de RAID**
    - Tipo

      Muestra el tipo de RAID (RAID0, RAID4, RAID-DP o RAID-TEC).

    - Tamaño del grupo

      Muestra el número máximo de discos permitidos en el grupo RAID.

    - Grupos

      Muestra el número de grupos RAID en el agregado.

  - **Discos utilizados**
    - Tipo efectivo

      Indica que los discos utilizados para la caché del agregado son del tipo SSD.

    - Discos de datos

      Muestra la cantidad y la capacidad de los discos de datos que se asignan a un agregado para la caché.

    - Discos de paridad

      Muestra el número y la capacidad de los discos de paridad que se asignan a un agregado para la caché.

  - **Discos de repuesto**

    Muestra el tipo, número y capacidad efectivos de los discos de repuesto que están disponibles para el nodo en el agregado seleccionado para la caché.

    Cuando un agregado se cambia al nodo del partner, Unified Manager no muestra todos los discos de repuesto que sean compatibles con el agregado.

Proporciona los siguientes detalles de la caché compartida:

- **Piscina de almacenamiento**

  Muestra el nombre del pool de almacenamiento. Es posible mover el puntero por el nombre del pool de almacenamiento para ver los siguientes detalles:

  - Estado

    Muestra el estado del pool de almacenamiento, que puede ser en buen estado o incorrecto.

  - Asignaciones totales

    Muestra las unidades de asignación totales y el tamaño de la agrupación de almacenamiento.

  - Tamaño de unidad de asignación

    Muestra la cantidad mínima de espacio del pool de almacenamiento que se puede asignar a un agregado.

  - Discos

    Muestra el número de discos utilizados para crear el pool de almacenamiento. Si el número de discos en la columna del pool de almacenamiento y el número de discos que se muestran en la pestaña Información de disco de ese pool de almacenamiento no coinciden, indica que uno o varios discos se encuentran dañados y el pool de almacenamiento es incorrecto.

  - Asignación utilizada

    Muestra el número y el tamaño de las unidades de asignación utilizadas por los agregados. Puede hacer clic en el nombre del agregado para ver los detalles del agregado.

  - Asignación disponible

    Muestra el número y el tamaño de las unidades de asignación disponibles para los nodos. Puede hacer clic en el nombre del nodo para ver los detalles del agregado.

- **Caché asignada**

  Muestra el tamaño de las unidades de asignación utilizadas por el agregado.

- **Unidades de asignación**

  Muestra el número de unidades de asignación utilizadas por el agregado.

- **Discos**

  Muestra la cantidad de discos contenidos en el pool de almacenamiento.

- **Detalles**
  - Pool de almacenamiento

    Muestra el número de pools de almacenamiento.

  - Tamaño total

Muestra el tamaño total de los pools de almacenamiento.

- **Nivel de cloud**

  Muestra el nombre del nivel de cloud, si ha configurado un agregado habilitado para FabricPool y muestra el espacio total utilizado. Cuando el nivel de cloud se refleja en otro proveedor de cloud (el nivel de reflejo), aquí se muestran los detalles de ambos niveles de cloud

Pestaña Configuration

En la pestaña Configuration, se muestran detalles sobre el agregado seleccionado, como el nodo del clúster, el tipo de bloque, el tipo de RAID, el tamaño de RAID y el número de grupos RAID:

- **Descripción general**
  - Nodo

    Muestra el nombre del nodo que contiene el agregado seleccionado.

  - Tipo de bloque

    Muestra el formato de bloque del agregado: De 32 bits o de 64 bits.

  - Tipo de RAID

    Muestra el tipo de RAID (RAID0, RAID4, RAID-DP, RAID-TEC o RAID mixto).

  - Tamaño de RAID

    Muestra el tamaño del grupo RAID.

  - Grupos de RAID

    Muestra el número de grupos RAID en el agregado.

  - Tipo de SnapLock

    Muestra el tipo de SnapLock del agregado.

- **Nivel de cloud**

  Si este es un agregado habilitado para FabricPool, se muestran los detalles del nivel de cloud. Algunos campos varían según el proveedor de almacenamiento. Cuando el nivel de cloud se refleja en otro proveedor de cloud (el «nivel de irritación»), ambos niveles de cloud se muestran aquí.

  - Proveedor

    Muestra el nombre del proveedor de almacenamiento, por ejemplo, StorageGRID, Amazon S3, IBM Cloud Object Storage, Microsoft Azure Cloud, Google Cloud Storage o Alibaba Cloud Object Storage.

  - Nombre

    Muestra el nombre del nivel de cloud cuando lo creó ONTAP.

  - Servidor

Muestra el FQDN del nivel de cloud.

- Puerto

  El puerto que se utiliza para comunicarse con el proveedor de cloud.

- Clave de acceso o cuenta

  Muestra la clave de acceso o cuenta del nivel de cloud.

- Nombre del contenedor

  Muestra el nombre de bloque o contenedor del nivel de cloud.

- SSL

  Muestra si el cifrado SSL está activado para el nivel de nube.

Historial

El área History muestra gráficos que proporcionan información sobre la capacidad del agregado seleccionado. Además, puede hacer clic en el botón **Exportar** para crear un informe en formato CSV para el gráfico que está viendo.

Puede seleccionar un tipo de gráfico en la lista desplegable situada en la parte superior del panel Historial. También puede ver los detalles de un período de tiempo específico seleccionando 1 semana, 1 mes o 1 año. Los gráficos del historial pueden ayudarle a identificar tendencias: Por ejemplo, si el uso del agregado está violando constantemente el umbral casi completo, puede tomar la acción adecuada.

Los gráficos del historial muestran la siguiente información:

- **Capacidad agregada utilizada (%)**

  Muestra la capacidad utilizada en el agregado y la tendencia en el uso de la capacidad agregada en función del historial de uso como gráficos de líneas, en porcentaje, en el eje vertical (y). El período de tiempo se muestra en el eje horizontal (x). Puede seleccionar un período de tiempo de una semana, un mes o un año. Puede ver los detalles de puntos específicos del gráfico situando el cursor sobre un área determinada. Puede ocultar o mostrar un gráfico de líneas haciendo clic en la leyenda correspondiente. Por ejemplo, al hacer clic en la leyenda de capacidad utilizada, la línea del gráfico de capacidad utilizada queda oculta.

- **Capacidad agregada utilizada frente a capacidad total**

  Muestra la tendencia en la forma en que se utiliza la capacidad agregada en función del historial de uso, así como la capacidad utilizada y la capacidad total, como gráficos de líneas, en bytes, megabytes, kilobytes, y así sucesivamente, en el eje vertical (y). El período de tiempo se muestra en el eje horizontal (x). Puede seleccionar un período de tiempo de una semana, un mes o un año. Puede ver los detalles de puntos específicos del gráfico situando el cursor sobre un área determinada. Puede ocultar o mostrar un gráfico de líneas haciendo clic en la leyenda correspondiente. Por ejemplo, al hacer clic en la leyenda capacidad de tendencias utilizada, la línea gráfica capacidad de tendencias utilizada está oculta.

- **Capacidad agregada utilizada (%) frente a comprometida (%)**

  Muestra la tendencia en la forma en que se utiliza la capacidad agregada en función del historial de uso, así como el espacio comprometido como gráficos de líneas, como porcentaje, en el eje vertical (y). El

período de tiempo se muestra en el eje horizontal (x). Puede seleccionar un período de tiempo de una semana, un mes o un año. Puede ver los detalles de puntos específicos del gráfico situando el cursor sobre un área determinada. Puede ocultar o mostrar un gráfico de líneas haciendo clic en la leyenda correspondiente. Por ejemplo, al hacer clic en la leyenda espacio asignado, la línea del gráfico espacio comprometido está oculta.

Lista Events

En la lista Eventos se muestran detalles sobre eventos nuevos y reconocidos:

- **Gravedad**

  Muestra la gravedad del evento.

- **Evento**

  Muestra el nombre del evento.

- **Tiempo activado**

  Muestra el tiempo transcurrido desde que se generó el evento. Si el tiempo transcurrido supera una semana, se muestra la Marca de tiempo para el momento en que se generó el evento.

Panel Related Devices

El panel Related Devices permite ver el nodo del clúster, los volúmenes y los discos relacionados con el agregado:

- **Nodo**

  Muestra la capacidad y el estado del nodo que contiene el agregado. La capacidad indica la capacidad utilizable total sobre la capacidad disponible.

- **Agregados en el nodo**

  Muestra la cantidad y la capacidad de todos los agregados del nodo del clúster que contiene el agregado seleccionado. También se muestra el estado de los agregados, en función del nivel de gravedad más alto. Por ejemplo, si un nodo de clúster contiene diez agregados, cinco de los cuales muestran el estado Warning y los cinco restantes, que muestran el estado Critical, el estado mostrado es crucial.

- **Volúmenes**

  Muestra el número y la capacidad de los volúmenes FlexVol y FlexGroup en el agregado; el número no incluye los componentes FlexGroup. El estado de los volúmenes también se muestra, según el nivel de gravedad más alto.

- **Piscina de recursos**

  Muestra los pools de recursos relacionados con el agregado.

- **Discos**

  Muestra el número de discos del agregado seleccionado.

Panel Related Alerts

El panel Related Alerts permite ver la lista de alertas creadas para el agregado seleccionado. También es posible añadir una alerta si se hace clic en el enlace Add Alert o editar una alerta existente haciendo clic en el nombre de la alerta.

Información relacionada

"Ver los detalles del pool de almacenamiento"

Proteja y restaure sus datos

Creación, supervisión y solución de problemas de relaciones de protección

Unified Manager permite crear relaciones de protección, supervisar y solucionar problemas de protección de reflejos y protección de almacén de backup de los datos almacenados en clústeres gestionados, así como restaurar datos cuando se sobrescriben o se pierden.

Tipos de protección SnapMirror

Según la puesta en marcha de la topología de almacenamiento de datos, Unified Manager permite configurar varios tipos de relaciones de protección de SnapMirror. Todas las variaciones de la protección de SnapMirror ofrecen protección de recuperación tras fallos, pero ofrecen distintas funcionalidades en cuanto a rendimiento, flexibilidad de versiones y protección de backups múltiples.

Relaciones de protección asíncrona de SnapMirror tradicionales

La protección asíncrona de SnapMirror tradicional proporciona protección con mirroring de replicación en bloques entre los volúmenes de origen y de destino.

En las relaciones de SnapMirror tradicionales, las operaciones de mirroring se ejecutan más rápido de lo que tendrían en relaciones de SnapMirror alternativas, ya que la operación de mirroring se basa en la replicación por bloques. Sin embargo, la protección SnapMirror tradicional requiere que el volumen de destino se ejecute con la misma versión secundaria o posterior del software ONTAP que el volumen de origen en la misma versión principal (por ejemplo, la versión 8.x a la 8.x o de 9.x a 9.x). No se admite la replicación de un origen 9.1 a un destino 9.0 porque el destino ejecuta una versión principal anterior.

Protección asíncrona de SnapMirror con replicación de versión flexible

La protección asíncrona de SnapMirror con la replicación flexible de versiones proporciona protección de reflejos de replicación lógica entre volúmenes de origen y de destino, incluso si dichos volúmenes se ejecutan en versiones diferentes de ONTAP 8.3 o posteriores (por ejemplo, de la versión 8.3 a la 8.3.1, o de 8.3 a 9.1, o de 9.2.2 a 9.2).

En las relaciones de SnapMirror con una replicación de versión flexible, las operaciones de mirroring no se ejecutan con la misma rapidez que en las relaciones tradicionales de SnapMirror.

Debido a una ejecución más lenta, SnapMirror con protección de replicación flexible de versión no es adecuado de ninguna de las siguientes circunstancias:

- El objeto de origen contiene más de 10 millones de archivos que proteger.
- El objetivo de punto de recuperación de los datos protegidos es de dos horas o menos. (Es decir, el destino siempre debe contener datos duplicados y recuperables, que tengan una antigüedad superior a dos horas respecto a los datos de origen).

En una de las circunstancias indicadas, se requiere la ejecución más rápida basada en replicación por bloques de la protección SnapMirror predeterminada.

Protección asíncrona de SnapMirror con la replicación con versión flexible y la opción de backup

La protección asíncrona de SnapMirror con la opción de backup y replicación flexible con versión proporciona protección mediante mirroring entre volúmenes de origen y de destino, y la posibilidad de almacenar varias copias de los datos reflejados en el destino.

El administrador de almacenamiento puede especificar qué copias Snapshot se reflejan de un origen a un destino y también puede especificar el tiempo que debe retener esas copias en el destino, incluso si se eliminan en el origen.

En las relaciones de SnapMirror con una opción de backup y replicación de versión flexible, las operaciones de mirroring no se ejecutan con la misma rapidez que en las relaciones tradicionales de SnapMirror.

Replicación unificada de SnapMirror (mirroring y almacén)

La replicación unificada de SnapMirror le permite configurar la recuperación ante desastres y el archivado en el mismo volumen de destino. Al igual que sucede con SnapMirror, la protección de datos unificada realiza una transferencia de referencia la primera vez que se invoca. Una transferencia básica con la política de protección de datos unificada predeterminada «MirrorAndVault» hace una copia Snapshot del volumen de origen y, a continuación, transfiere dicha copia y los bloques de datos a los que hace referencia al volumen de destino. Al igual que SnapVault, la protección de datos unificada no incluye copias Snapshot anteriores en la referencia.

Protección de SnapMirror Synchronous con una sincronización estricta

La protección SnapMirror Synchronous con sincronización «esencial» garantiza que los volúmenes primario y secundario siempre sean una copia real del otro. Si se produce un fallo de replicación al intentar escribir datos en el volumen secundario, las operaciones de I/o del cliente en el volumen primario se interrumpen.

Protección de SnapMirror Synchronous con sincronización normal

La protección de SnapMirror Synchronous con sincronización «relativamente» no requiere que el volumen primario y el secundario siempre sean una copia real del otro, lo que garantiza la disponibilidad del volumen primario. Si se produce un fallo de replicación al intentar escribir datos en el volumen secundario, los volúmenes primario y secundario quedan sin sincronizar y la I/o del cliente continuará en el volumen primario.

El botón Restaurar y los botones de operación de relación no están disponibles al supervisar las relaciones de protección síncrona en la vista Estado: Todos los volúmenes o la página de detalles volumen / Estado.

Continuidad del negocio de SnapMirror Synchronous

La función de continuidad del negocio de SnapMirror (SM-BC) está disponible con ONTAP 9.8 y versiones posteriores, y puede usarla para proteger las aplicaciones con LUN, lo que permite que las aplicaciones se conmute de forma transparente y garantiza la continuidad del negocio en caso de desastre.

Permite detectar y supervisar las relaciones síncronas de SnapMirror para los grupos de consistencia (CG) disponibles en los clústeres y las máquinas virtuales de almacenamiento de Unified Manager. SM-BC es compatible en clústeres AFF o clústeres de cabina All SAN (ASA), donde los clústeres principal y secundario pueden ser AFF o ASA. SM-BC protege las aplicaciones con LUN iSCSI o FCP.

Cuando se ven los volúmenes y las LUN protegidos por la relación SM-BC, puede obtener una vista unificada de las relaciones de protección, los grupos de coherencia en el inventario de volúmenes, ver la topología de la protección para las relaciones de grupos de coherencia, ver datos históricos de las relaciones de grupos de

coherencia de hasta un año. También puede descargar el informe. También se puede ver el resumen de las relaciones del grupo de coherencia, buscar el soporte de las relaciones del grupo de coherencia y obtener información sobre los volúmenes que está protegido por el grupo de coherencia.

En la página Relationships, también se puede ordenar, filtrar y extender la protección en los objetos de almacenamiento de origen y destino, y su relación que está protegida por el grupo de coherencia.

Si quiere más información sobre la continuidad del negocio de SnapMirror síncrono, consulte "Documentación de ONTAP 9 para SM-BC".

Configuración de las relaciones de protección en Unified Manager

Hay varios pasos que debe realizar para usar Unified Manager y OnCommand Workflow Automation a fin de configurar las relaciones de SnapMirror y SnapVault para proteger sus datos.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber establecido relaciones entre iguales entre dos clústeres o dos máquinas virtuales de almacenamiento (SVM).
- OnCommand Workflow Automation debe integrarse con Unified Manager:
  - "Configure OnCommand Workflow Automation".
  - "Verificación del almacenamiento en caché de origen de datos de Unified Manager en Workflow Automation".

Pasos

1. Según el tipo de relación de protección que desee crear, realice una de las siguientes acciones:
   - "Cree una relación de protección de SnapMirror".
   - "Cree una relación de protección SnapVault".
2. Si desea crear una directiva para la relación, en función del tipo de relación que esté creando, realice una de las siguientes acciones:
   - "Cree una política de SnapVault".
   - "Cree una política de SnapMirror".
3. "Cree una programación de SnapMirror o SnapVault".

Configuración de una conexión entre Workflow Automation y Unified Manager

Puede configurar una conexión segura entre OnCommand Workflow Automation (WFA) y Unified Manager. La conexión a Workflow Automation le permite usar funciones de protección como flujos de trabajo de configuración de SnapMirror y SnapVault, así como comandos para gestionar las relaciones de SnapMirror.

Lo que necesitará

- La versión instalada de Workflow Automation debe ser 5.1 o superior.

El «paquete WFA para gestionar Clustered Data ONTAP» se incluye en WFA 5.1, por lo que no es necesario descargar este paquete del almacén de automatización del almacenamiento de NetApp e instalarlo por separado en su servidor WFA, tal y como se requería en el pasado. "PAQUETE WFA para gestionar ONTAP"

- Debe tener el nombre del usuario de la base de datos que ha creado en Unified Manager para admitir conexiones de WFA y Unified Manager.

  Este usuario de la base de datos debe haber sido asignado el rol de usuario del Esquema de integración.

- Debe tener asignado la función de administrador o de arquitecto en Workflow Automation.
- Debe tener la dirección de host, el número de puerto 443, el nombre de usuario y la contraseña para la configuración de Workflow Automation.
- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Workflow Automation**.
2. En el área **Usuario de base de datos** de la página **Automatización de flujos de trabajo**, seleccione el nombre e introduzca la contraseña del usuario de base de datos que creó para admitir conexiones de Unified Manager y Workflow Automation.
3. En el área **Workflow Automation Credentials** de la página, introduzca el nombre de host o la dirección IP (IPv4 o IPv6) y el nombre de usuario y la contraseña para la configuración de Workflow Automation.

   Debe usar el puerto del servidor de Unified Manager (puerto 443).

4. Haga clic en **Guardar**.
5. Si utiliza un certificado autofirmado, haga clic en **Sí** para autorizar el certificado de seguridad.

   Se mostrará la página Workflow Automation.

6. Haga clic en **Sí** para volver a cargar la interfaz de usuario web y agregar las funciones de Workflow Automation.

Información relacionada

"Documentación de NetApp: OnCommand Workflow Automation (versiones actuales)"

Verificación del almacenamiento en caché de origen de datos de Unified Manager en Workflow Automation

Puede determinar si el almacenamiento en caché de origen de datos de Unified Manager funciona correctamente comprobando si la adquisición del origen de datos se ha realizado correctamente en Workflow Automation. Puede hacerlo cuando se integre Workflow Automation con Unified Manager para garantizar que la funcionalidad Workflow Automation esté disponible después de la integración.

Lo que necesitará

Para realizar esta tarea, debe tener asignado la función Administrador o la función Arquitecto de Workflow Automation.

Pasos

1. En la interfaz de usuario de Workflow Automation, seleccione **ejecución** > **orígenes de datos**.
2. Haga clic con el botón derecho del ratón en el nombre del origen de datos de Unified Manager y, a continuación, seleccione **adquirir ahora**.
3. Compruebe que la adquisición se realiza correctamente sin errores.

   Para que la integración de Workflow Automation en Unified Manager se tenga éxito, es necesario resolver los errores de adquisición.

Qué ocurre cuando se vuelve a instalar o actualizar OnCommand Workflow Automation

Antes de reinstalar o actualizar OnCommand Workflow Automation, primero debe quitar la conexión entre OnCommand Workflow Automation y Unified Manager y asegurarse de que se hayan detenido todos los trabajos programados o en ejecución actualmente de OnCommand Workflow Automation.

También debe eliminar manualmente Unified Manager de OnCommand Workflow Automation.

Después de reinstalar o actualizar OnCommand Workflow Automation, debe configurar de nuevo la conexión con Unified Manager.

Se elimina la configuración de OnCommand Workflow Automation de Unified Manager

Puede eliminar la configuración de OnCommand Workflow Automation de Unified Manager cuando ya no desee usar Workflow Automation.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **General** > **Workflow Automation** en el menú de configuración izquierdo.
2. En la página **Workflow Automation**, haga clic en **Eliminar configuración**.

Recuperación tras fallos y recuperación de una relación de protección

Cuando se deshabilita un volumen de origen en la relación de protección debido a un error de hardware o un desastre, se pueden usar las funciones de relaciones de protección en Unified Manager para que el destino de la protección sea accesible de lectura/escritura y se pueda conmutar por error a ese volumen hasta que el origen vuelva a estar en línea; a continuación, puede volver a la fuente original cuando esté disponible para servir datos.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado OnCommand Workflow Automation para realizar esta operación.

Pasos

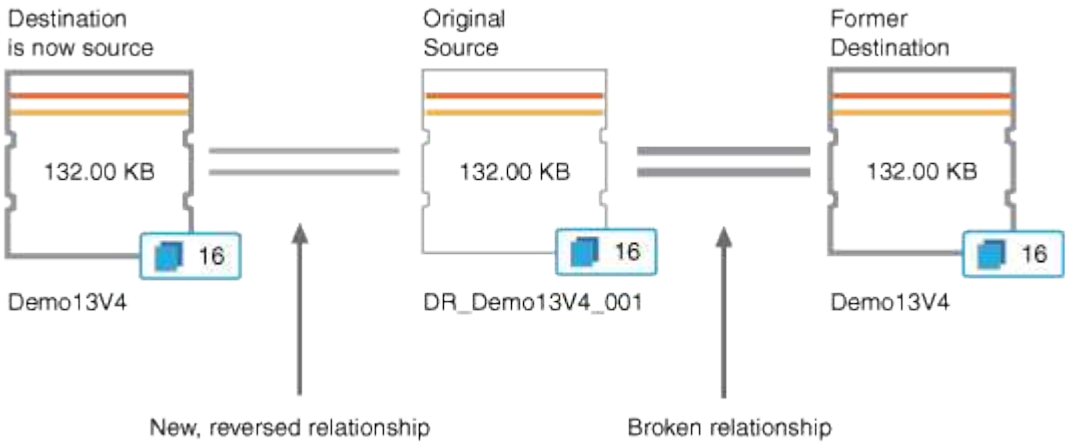
1. "Rompa la relación de SnapMirror".

   Se debe romper la relación antes de convertir el destino de un volumen de protección de datos a un volumen de lectura/escritura, y antes de poder revertir la relación.

2. "Invierta la relación de protección".

   Cuando el volumen de origen original vuelva a estar disponible, se puede decidir restablecer la relación de protección original mediante la restauración del volumen de origen. Para poder restaurar el origen, debe sincronizarlo con los datos escritos en el destino anterior. Utiliza la operación de resincronización inversa para crear una nueva relación de protección mediante la reversión de los roles de la relación original y la sincronización del volumen de origen con el destino anterior. Se crea una nueva copia Snapshot de referencia para la nueva relación.

   La relación inversa tiene un aspecto similar a una relación en cascada:



3. "Rompa la relación de SnapMirror invertida".

   Cuando se resincronizaba el volumen de origen original y se pueden volver a servir datos, use la operación de interrupción para romper la relación inversa.

4. "Eliminar la relación".

   Cuando la relación inversa ya no sea necesaria, debe eliminar dicha relación antes de volver a establecer la relación original.

5. "Resincronice la relación".

   Utilice la operación Resynchronize para sincronizar los datos del origen con el destino y restablecer la relación original.

Romper una relación de SnapMirror en la página de detalles Volume/Health

Es posible interrumpir una relación de protección en la página de detalles Volume/Health y detener las transferencias de datos entre un volumen de origen y un volumen de destino en una relación de SnapMirror. Puede romper una relación cuando desea migrar datos, para la recuperación ante desastres o para la prueba de aplicaciones. El volumen de destino se cambia a un volumen de lectura/escritura. No es posible interrumpir una

relación de SnapVault.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

Pasos

1. En la pestaña **Protección** de la página de detalles **volumen / Salud**, seleccione en la topología la relación de SnapMirror que desea romper.
2. Haga clic con el botón derecho del ratón en el destino y seleccione **romper** en el menú.

   Se muestra el cuadro de diálogo romper relación.

3. Haga clic en **continuar** para romper la relación.
4. En la topología, compruebe que la relación está rota.

Inversión de las relaciones de protección desde la página de detalles volumen / Estado

Cuando un desastre deshabilita el volumen de origen en la relación de protección, es posible usar el volumen de destino para suministrar datos mediante la conversión a lectura/escritura mientras se repara o se reemplaza el origen. Cuando el origen vuelve a estar disponible para recibir datos, puede utilizar la operación de resincronización inversa para establecer la relación en la dirección inversa y sincronizar los datos del origen con los datos en el destino de lectura/escritura.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.
- La relación no debe ser una relación de SnapVault.
- Debe haber una relación de protección.
- La relación de protección debe romperse.
- El origen y el destino deben estar en línea.
- El origen no debe ser el destino de otro volumen de protección de datos.
- Cuando realiza esta tarea, se eliminan los datos en el origen más nuevos que los de la copia Snapshot común.
- Las políticas y las programaciones creadas en la relación de resincronización inversa son las mismas que en la relación de protección original.

  Si no existen las políticas y las programaciones, se crean.

Pasos

1. En la ficha **Protección** de la página de detalles **volumen / Salud**, busque en la topología la relación de SnapMirror en la que desea invertir el origen y el destino y haga clic con el botón derecho del ratón en él.
2. Seleccione **Reverse Resync** en el menú.

Se muestra el cuadro de diálogo Reverse Resync.

3. Compruebe que la relación mostrada en el cuadro de diálogo **Resync. Inversa** es la que desea realizar la operación de resincronización inversa y, a continuación, haga clic en **Enviar**.

   Se cierra el cuadro de diálogo Reverse Resync y se muestra un enlace del trabajo en la parte superior de la página de detalles Volume/Health.

4. **Opcional:** haga clic en **Ver trabajos** en la página de detalles **volumen / Salud** para realizar un seguimiento del estado de cada trabajo de resincronización inversa.

   Se muestra una lista filtrada de trabajos.

5. **Opcional:** haga clic en la flecha **Atrás** de su navegador para volver a la página de detalles **volumen / Salud**.

   La operación de resincronización inversa se finaliza cuando todas las tareas de trabajo se completaron correctamente.

Eliminación de una relación de protección de la página de detalles Volume / Health

Puede quitar una relación de protección para eliminar de forma permanente una relación existente entre el origen y el destino seleccionados: Por ejemplo, cuando desea crear una relación con otro destino. Esta operación elimina todos los metadatos y no puede deshacerse.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

Pasos

1. En la ficha **Protección** de la página de detalles **volumen / Estado**, seleccione en la topología la relación de SnapMirror que desee eliminar.
2. Haga clic con el botón derecho del ratón en el nombre del destino y seleccione **Quitar** en el menú.

   Se muestra el cuadro de diálogo Eliminar relación.

3. Haga clic en **continuar** para eliminar la relación.

   La relación se elimina de la página de detalles Volume/Health.

Resincronizando las relaciones de protección desde la página de detalles Volume / Health

Puede volver a sincronizar los datos de una relación de SnapMirror o SnapVault que se rompió y, a continuación, el destino se hizo de lectura/escritura para que los datos del origen coincidan con los del destino. También es posible resincronizar cuando se elimina una copia Snapshot común requerida en el volumen de origen, y esto provoca errores en las actualizaciones de SnapMirror o SnapVault.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado OnCommand Workflow Automation.

Pasos

1. En la ficha **Protección** de la página de detalles **volumen / Salud**, busque en la topología la relación de protección que desea volver a sincronizar y haga clic con el botón derecho del ratón en ella.
2. Seleccione **Resynchronize** en el menú.

   Como alternativa, en el menú **acciones**, seleccione **relación** > **Resincronizar** para volver a sincronizar la relación para la que está viendo los detalles.

   Aparecerá el cuadro de diálogo Resynchronize.

3. En la pestaña **Opciones de resincronización**, seleccione una prioridad de transferencia y la tasa de transferencia máxima.
4. Haga clic en **copias Snapshot de origen**; a continuación, en la columna **copia Snapshot**, haga clic en **predeterminado**.

   Se muestra el cuadro de diálogo Seleccionar copia Snapshot de origen.

5. Si desea especificar una copia Snapshot existente en lugar de transferir la copia Snapshot predeterminada, haga clic en **copia Snapshot existente** y seleccione una copia Snapshot de la lista.
6. Haga clic en **Enviar**.

   Volverá al cuadro de diálogo Resynchronize.

7. Si ha seleccionado más de un origen para volver a sincronizar, haga clic en **predeterminado** para el siguiente origen para el que desea especificar una copia Snapshot existente.
8. Haga clic en **Enviar** para iniciar el trabajo de resincronización.

   El trabajo de resincronización se inició, regresará a la página de detalles Volume / Health y se mostrará un enlace de trabajos en la parte superior de la página.

9. **Opcional:** haga clic en **Ver trabajos** en la página **volumen / Detalles de la salud** para realizar un seguimiento del estado de cada trabajo de resincronización.

   Se muestra una lista filtrada de trabajos.

10. **Opcional:** haga clic en la flecha **Atrás** de su navegador para volver a la página de detalles **volumen / Salud**.

    El trabajo de resincronización finaliza cuando se completan correctamente todas las tareas de trabajo.

Solucionar un error de un trabajo de protección

Este flujo de trabajo proporciona un ejemplo de cómo se puede identificar y resolver un error de trabajo de protección en la consola de Unified Manager.

Lo que necesitará

Debido a que algunas tareas de este flujo de trabajo requieren que inicie sesión utilizando la función Administrador, debe estar familiarizado con las funciones necesarias para utilizar varias funciones.

En este caso, debe acceder a la página Dashboard para ver si hay algún problema con los trabajos de protección. En el área incidente de protección, se observa que hay un incidente de trabajo terminado, mostrando un error de trabajo de protección en un volumen. Investiga este error para determinar la causa posible y la resolución potencial.

Pasos

1. En el panel Protection Incidents del área Dashboard Unresolved Incidents and Risks, haga clic en el evento **Protection job failed**.

   El texto vinculado para el evento se escribe en el formulario `object_name:/object_name - Error Name`, por ejemplo `cluster2_src_svm:/cluster2_src_vol2 - Protection Job Failed`.

   Se muestra la página de detalles Event del trabajo de protección con errores.

2. Revise el mensaje de error en el campo causa del área **Resumen** para determinar el problema y evaluar las posibles acciones correctivas.

   Consulte "Identificar el problema y realizar acciones correctivas para un trabajo de protección con errores".

Identificar el problema y realizar acciones correctivas para un trabajo de protección con errores

Revisa el mensaje de error de error de trabajo en el campo CAUSE de la página de detalles Event y determina que el trabajo ha fallado debido a un error de copia de Snapshot. Luego continúa a la página de detalles Volume / Health para recopilar más información.

Lo que necesitará

Debe tener la función Administrador de aplicaciones.

El mensaje de error proporcionado en el campo causa de la página de detalles Event contiene el siguiente texto sobre el trabajo con errores:

```
Protection Job Failed. Reason: (Transfer operation for
relationship 'cluster2_src_svm:cluster2_src_vol2->cluster3_dst_svm:
managed_svc2_vol3' ended unsuccessfully. Last error reported by
Data ONTAP: Failed to create Snapshot copy 0426cluster2_src_vol2snap
on volume cluster2_src_svm:cluster2_src_vol2. (CSM: An operation
failed due to an ONC RPC failure.)
Job Details
```

Este mensaje proporciona la siguiente información:

- Un trabajo de backup o reflejo no se completó correctamente.

  El trabajo implicaba una relación de protección entre el volumen de origen `cluster2_src_vol2` en el servidor virtual `cluster2_src_svm` y el volumen de destino `managed_svc2_vol3` en el servidor virtual llamado `cluster3_dst_svm`.

- Error de un trabajo de copia Snapshot para `0426cluster2_src_vol2snap` en el volumen de origen `cluster2_src_svm:/cluster2_src_vol2`.

En este caso, puede identificar la causa y las posibles acciones correctivas del error del trabajo. Sin embargo, para resolver el fallo es necesario acceder a la interfaz de usuario web de System Manager o a los comandos de la CLI de ONTAP.

Pasos

1. Revisa el mensaje de error y determina que ha producido un error en un trabajo de copia Snapshot en el volumen de origen, lo que indica que probablemente haya un problema con el volumen de origen.

   Si lo desea, puede hacer clic en el enlace **Detalles del trabajo** al final del mensaje de error, pero a efectos de este escenario, elige no hacerlo.

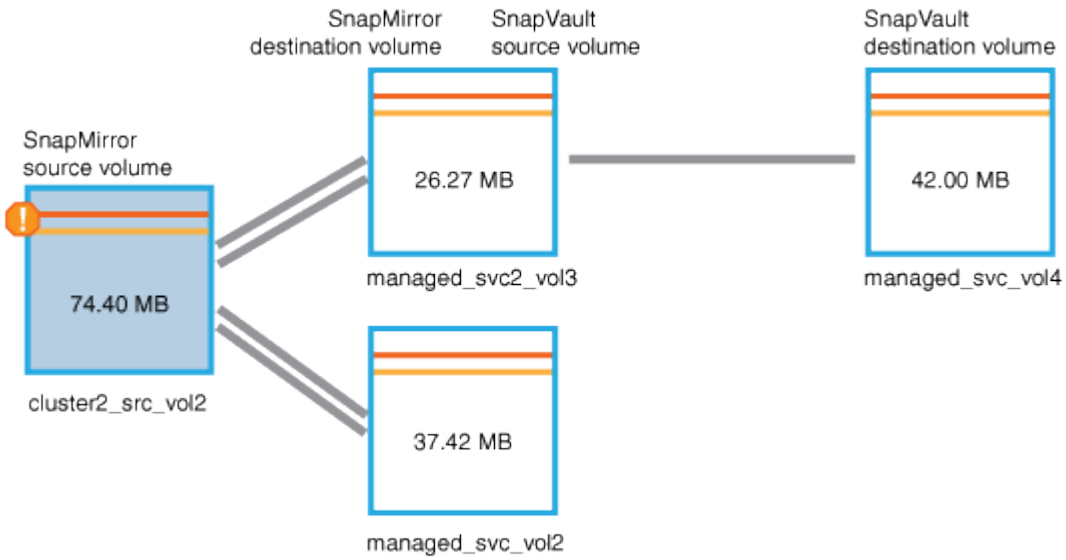
2. Decide que desea intentar resolver el evento, de modo que haga lo siguiente:
   a. Haga clic en el botón **asignar a** y seleccione **Me** en el menú.
   b. Haga clic en el botón **Confirmar** para que no siga recibiendo notificaciones de alerta de repetición, si se han configurado alertas para el evento.
   c. Opcionalmente, también puede agregar notas sobre el evento.
3. Haga clic en el campo **Fuente** del panel **Resumen** para ver detalles sobre el volumen de origen.

   El campo **origen** contiene el nombre del objeto de origen: En este caso, el volumen en el que se programó el trabajo de copia Snapshot.

   Se muestra la página de detalles volumen / Estado para `cluster2_src_vol2`, Que muestra el contenido de la ficha Protección .

4. Al ver el gráfico de topología de protección, se muestra un icono de error asociado con el primer volumen de la topología, que es el volumen de origen de la relación de SnapMirror.

   También puede ver las barras horizontales en el icono de volumen de origen, que indican los umbrales de advertencia y error definidos para ese volumen.



5. Coloque el cursor sobre el icono de error para ver el cuadro de diálogo emergente que muestra la configuración del umbral y ver que el volumen ha superado el umbral de error, lo que indica un problema

de capacidad.

6. Haga clic en la ficha **capacidad**.

   Información de capacidad acerca de volumen `cluster2_src_vol2` pantallas.

7. En el panel **capacidad**, verá que hay un icono de error en el gráfico de barras, indicando de nuevo que la capacidad del volumen ha superado el nivel de umbral establecido para el volumen.
8. Debajo del gráfico de capacidad, puede ver que se deshabilitó el crecimiento automático del volumen y que se estableció una garantía de espacio de volumen.

   Se puede decidir habilitar el crecimiento automático, pero para los fines de este escenario, se decide investigar más antes de tomar una decisión sobre cómo resolver el problema de capacidad.

9. Desplácese hacia abajo hasta la lista **Eventos** y vea que se generaron eventos error de trabajo de protección, volumen días hasta lleno y espacio de volumen lleno.
10. En la lista **Eventos**, usted hace clic en el evento **espacio de volumen lleno** para obtener más información, habiendo decidido que este evento parece más relevante para su problema de capacidad.

    La página de detalles Event muestra el evento Volume Space Full para el volumen de origen.

11. En el área **Resumen**, lee el campo causa del evento: `The full threshold set at 90% is breached. 45.38 MB (95.54%) of 47.50 MB is used.`
12. Debajo del área Resumen, verá acciones correctivas sugeridas.

    Las acciones correctivas sugeridas se muestran solo para algunos eventos, de modo que no se ve esta área para todos los tipos de eventos.

    Haga clic en la lista de acciones sugeridas que puede realizar para resolver el evento Volume Space Full:

    - Habilite el crecimiento automático en este volumen.
    - Cambie el tamaño del volumen.
    - Habilite y ejecute la deduplicación en este volumen.
    - Habilite y ejecute la compresión en este volumen.

13. Decida habilitar el crecimiento automático en el volumen, pero para hacerlo, debe determinar el espacio libre disponible en el agregado principal y la tasa de crecimiento del volumen actual:
    a. Observe el agregado principal, `cluster2_src_aggr1`, En el panel **dispositivos relacionados**.

       Puede hacer clic en el nombre del agregado para obtener más detalles sobre él.

       Se determina que el agregado tiene espacio suficiente para habilitar el crecimiento automático del volumen.

    b. En la parte superior de la página, observe el icono que indica una incidencia crítica y revise el texto debajo del icono.

       Usted determina que "días a lleno: Menos de un día | tasa de crecimiento diario: 5.4%".

14. Vaya a System Manager o acceda a la CLI de ONTAP para habilitar el `volume autogrow` opción.

Anote los nombres del volumen y del agregado para que estén disponibles al habilitar el crecimiento automático.

15. Después de resolver el problema de capacidad, vuelva a la página de detalles de Unified Manager **evento** y marque el evento como solucionado.

Resolución de problemas de desfase

Este flujo de trabajo proporciona un ejemplo de cómo puede resolver un problema de desfase. En esta situación, usted es administrador o operador que accede a la página Unified Manager Dashboard para ver si hay algún problema en las relaciones de protección y, si existen, para buscar soluciones.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

En la página Dashboard, se puede ver el área Unresolved Incidents and Risks y se muestra un error de desfase de SnapMirror en el panel Protection Risks.

Pasos

1. En el panel **Protection** de la página **Dashboard**, localice el error de retraso de la relación de SnapMirror y haga clic en él.

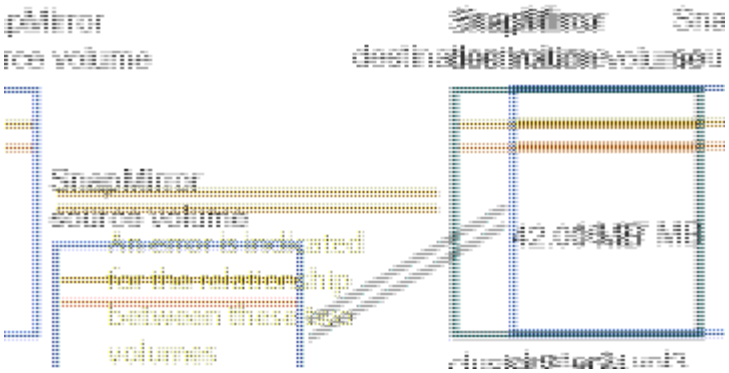
   Se muestra la página de detalles Event para el evento de error de desfase.

2. En la página de detalles **evento** puede realizar una o más de las siguientes tareas:
   - Revise el mensaje de error en el campo causa del área Resumen para determinar si hay alguna acción correctiva sugerida.
   - Haga clic en el nombre del objeto, en este caso, un volumen, en el campo Source del área Summary para obtener detalles sobre el volumen.
   - Busque las notas que se podrían haber añadido acerca de este evento.
   - Agregar una nota al evento.
   - Asignar el evento a un usuario específico.
   - Reconozca o resuelva el evento.
3. En este escenario, haga clic en el nombre del objeto (en este caso, un volumen) en el campo origen del área **Resumen** para obtener detalles sobre el volumen.

   Se muestra la pestaña Protection de la página de detalles Volume / Health.

4. En la ficha **Protección**, verá el diagrama de topología.

   Ha observado que el volumen con el error de desfase es el último volumen en una cascada de SnapMirror de tres volúmenes. El volumen seleccionado se resume en gris oscuro y una línea naranja doble del volumen de origen indica un error de relación de SnapMirror.



5. Haga clic en cada uno de los volúmenes en la cascada de SnapMirror.

   Al seleccionar cada volumen, la información de protección en Summary, Topology, History, Events, Related Devices, Y las áreas Alertas relacionadas cambian para mostrar detalles relevantes para el volumen seleccionado.

6. Verá el área **Resumen** y coloque el cursor sobre el icono de información en el campo **Actualizar programa** de cada volumen.

   En este caso, debe tener en cuenta que la política de SnapMirror es DPDefault, y la programación de SnapMirror se actualiza cada hora a los cinco minutos. Usted sabe que todos los volúmenes de la relación están intentando completar una transferencia de SnapMirror al mismo tiempo.

7. Para resolver el problema de desfase, se modifican los horarios de dos de los volúmenes en cascada de modo que cada destino inicie una transferencia de SnapMirror una vez que su origen haya completado una transferencia.

Gestión y supervisión de relaciones de protección

Active IQ Unified Manager permite crear relaciones de protección, supervisar y solucionar problemas de relaciones de SnapMirror y SnapVault en clústeres gestionados, y restaurar datos cuando se sobrescriben o se pierden.

Para las operaciones de SnapMirror, existen dos tipos de replicación:

- Asíncrona

  La replicación del volumen primario al secundario se determina mediante una programación.

- Síncrona

  La replicación se realiza de forma simultánea en el volumen primario y secundario.

Se pueden ejecutar hasta 10 tareas de protección simultáneamente sin que el rendimiento se vea afectado. Es posible que experimente algún impacto en el rendimiento cuando se ejecutan entre 11 y 30 trabajos al mismo tiempo. No se recomienda ejecutar más de 30 trabajos simultáneamente.

Ver el estado de protección de volumen

La página Data Protection presenta una vista holística de los detalles de la protección de datos de todos los volúmenes protegidos en un único clúster, o todos los clústeres de un

centro de datos.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **Panel**.
2. En función de si desea ver el estado de protección de datos de todos los clústeres supervisados o de un solo clúster, seleccione **todos los clústeres** o seleccione un único clúster en el menú desplegable.
3. Haga clic en la flecha derecha de la parte superior del panel Data Protection. Aparece la página **Data Protection**.

Según si seleccionó una única o todos los clústeres del centro de datos, esta página muestra el estado de protección de datos de los volúmenes protegidos por copias de Snapshot o políticas de SnapMirror, y también muestra el número de volúmenes sin proteger.

Al seleccionar un clúster de la lista **Individual Cluster** se muestra el estado de la protección Snapshot y la relación SnapMirror de los volúmenes protegidos en ese clúster.

Al hacer clic en los eventos de esta página, se abre la página de detalles Event. Puede hacer clic en el enlace **Ver todo** para ver todos los eventos de protección activos en la página de inventario de Event Management. Puede pasar el ratón sobre el mismo para ver los recuentos y leyendas correspondientes. Puede hacer clic en:

- Los gráficos de barras de volúmenes no protegidos y volúmenes protegidos por copias Snapshot para ir a la página Volumes y ver los detalles.
- Los gráficos de barras de todas las relaciones se van a la página Relaciones, donde el clúster de origen filtra los detalles.

Consulte el estado de protección de volúmenes protegidos por copias de Snapshot

Descripción general de las copias Snapshot: Descripción general de los volúmenes protegidos por copias Snapshot, como:

- La cantidad total de volúmenes protegidos y sin protección mediante copias Snapshot.
- El número total de volúmenes que utilizan o superan el espacio de reserva para las copias Snapshot.

Análisis de copias Snapshot detalla la siguiente información:

- Eventos individuales para copias Snapshot, incluidos los eventos realizados en las últimas 24 horas.
- Gráfico detallado para volúmenes protegidos y no protegidos por copias Snapshot
- Volúmenes que utilizan, no utilizan y abrevian la capacidad reservada de la copia Snapshot.
- La división del volumen en términos del número de sus copias Snapshot.

Puntos que tener en cuenta para las copias Snapshot

- Para el recuento de los volúmenes protegidos por copias Snapshot, se consideran los volúmenes de origen y destino.
- El número de copias Snapshot que se devuelven solo es para los volúmenes en línea y disponibles.
- El intervalo de gráficos del número de copias Snapshot es dinámico. Se genera en función del número de snapshots presentes en el clúster seleccionado.
- Para considerar un volumen como protegido, se debe habilitar la programación para la copia Snapshot del volumen.

- El valor del espacio de reserva para las copias Snapshot es importante para ver la cantidad de espacio en disco utilizado o para calcular el espacio que puede reclamarse si una o más copias de Snapshot se han eliminado.

Consulte el estado de protección de las relaciones de SnapMirror

Descripción general de SnapMirror: Descripción general de los volúmenes protegidos por políticas de SnapMirror, como:

- El número de volúmenes protegidos por las respectivas políticas de SnapMirror, como las relaciones de SnapMirror para volúmenes, la recuperación ante desastres de las máquinas virtuales de almacenamiento (SVM-DR) y sus combinaciones.
- El número total de relaciones de SnapMirror que experimentan un desfase de objetivo de punto de recuperación (RPO) se basa en el estado de desfase.

Análisis de SnapMirror detalla la siguiente información:

- Eventos individuales planteados para las relaciones de SnapMirror, incluidos los eventos de las últimas 24 horas
- El número de volúmenes protegidos por cada tipo de política de SnapMirror.
- La cantidad de relaciones protegidas por los tipos de relación de SnapMirror, como Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StricxtSync, SnapMirror Business Continuity (SMBC) y Sync.
- El número de relaciones saludables y poco saludables.
- Desglose del número de relaciones de volumen. Puede cambiar los gráficos por el estado y el tiempo de retraso de RPO.
- Umbrales de desfase para una relación no gestionada. Puede hacer clic en el icono de configuración ( ) para configurar los ajustes del umbral de demora. Para obtener más información, consulte "Configuración de la configuración del umbral de desfase para relaciones de protección no administradas".

Puntos que tener en cuenta sobre las relaciones de SnapMirror

- Para tener en cuenta las relaciones de SnapMirror, se cuentan los volúmenes de origen, que están habilitados para lectura y escritura. Los volúmenes de destino y raíz no se consideran.
- Para la relación de SnapMirror, los eventos se muestran para el clúster de origen.
- El número de relaciones de SnapMirror incluye la cantidad de volúmenes con orígenes y destinos en los mismos clústeres o diferentes.
- La duración de la demora en el objetivo de punto de recuperación en la replicación de datos se basa en la relación con SnapMirror. El estado se clasifica como `ok`, `warning`, o. `error`, basado en el conjunto de umbrales de relación. Puede consultar el estado para determinar si los parámetros funcionan según lo esperado o si debe solucionar algún problema.
- Si un volumen tiene varias relaciones de SnapMirror, cada tipo de relación se cuenta para el desfase de RPO.
- Las relaciones de volúmenes se consideran poco saludables si hay problemas en la replicación de datos entre el origen y el destino, por ejemplo, cuando la relación está rota.

Ver clústeres protegidos por la configuración de MetroCluster

El panel **Protección MetroCluster** de la página **Protección de datos** muestra el número de clústeres protegidos o no protegidos por la configuración de MetroCluster sobre FC o IP en su sitio. Al hacer clic en los gráficos de barras de este panel, se desplaza a la página Clusters donde los detalles del clúster se filtran en función de los clústeres protegidos o no protegidos. Para obtener información acerca de cómo supervisar la configuración de MetroCluster, consulte "Supervisar las configuraciones de MetroCluster".

Visualización de las relaciones de protección de volúmenes

En la vista Relationship: All Relationships y, en la página Volume Relationships, puede ver el estado de las relaciones de SnapMirror y SnapVault para volúmenes existentes. También puede examinar detalles sobre las relaciones de protección, como el estado de transferencia y desfase, los detalles de origen y destino, la información sobre la programación y las políticas, etc.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

También puede iniciar los comandos de relaciones desde esta página.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En el menú Ver, seleccione **relación** > **todas las relaciones**.

   Se muestra la vista relación: Todas las relaciones.
3. Seleccione una de las siguientes maneras de ver los detalles de protección de volumen:
   - Para ver la información actual acerca de todas las relaciones de volumen, permanezca en la página predeterminada **todas las relaciones**.
   - Para ver información detallada acerca de las tendencias de transferencia de volúmenes durante un periodo de tiempo, en el menú Ver, seleccione relación: Vista Estado de transferencia de último 1 mes.
   - Para ver información detallada sobre la actividad de transferencia de volumen día a día, en el menú Ver, seleccione relación: Vista de tarifa de transferencia de último 1 mes.

   Las vistas de transferencia de volúmenes muestran información solo sobre los volúmenes en relaciones asíncronas: No se muestran los volúmenes de las relaciones síncronas.

Supervisar las LUN en una relación de grupo de consistencia

Si su entorno ONTAP admite la continuidad empresarial de SnapMirror (SM-BC) para proteger las aplicaciones con LUN, puede consultar y supervisar dichas LUN en Active IQ Unified Manager.

SM-BC garantiza un objetivo de tiempo de recuperación cero durante la conmutación por error en entornos SAN. En una implementación típica compatible con SM-BC, las LUN de los volúmenes están protegidas por relaciones de grupos de consistencia.

Estas LUN principales y secundarias son LUN compuestas, o una pareja de LUN de réplica con el mismo

UUID y número de serie. Las operaciones de E/S (tanto de lectura como de escritura) se multiplexan a través de los sitios de origen y destino en estas LUN compuestas, lo que garantiza la transparencia.

Para ver las LUN compuestas, se deben añadir y detectar en Unified Manager los clústeres primario y secundario con las LUN que forman parte de la relación del grupo de consistencia. Solo se admiten LUN iSCSI y FCP.

Para obtener información sobre SM-BC, consulte "Documentación de ONTAP 9 para SM-BC".

Para ver las LUN compuestas en su entorno, siga estos pasos:

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **LUN**.
2. En el menú Ver, seleccione **relación** > **todas las LUN**.

   La relación: Se muestra toda la vista de LUN.

Puede ver los detalles del LUN, como el nombre del LUN, el volumen, la máquina virtual de almacenamiento que aloja el LUN, el clúster, el grupo de consistencia y el LUN del partner. Puede hacer clic en cada uno de estos componentes para profundizar en una vista detallada. Al hacer clic en el grupo de consistencia se abre la página Relaciones.

Al hacer clic en el LUN de partners puede ver sus detalles de configuración en la pestaña SAN de la página Storage VM Details de la máquina virtual de almacenamiento donde está alojado la LUN de partner. Se muestra información como los iniciadores y los iGroups y otros aspectos de la LUN del partner.

Puede realizar las funciones estándar de nivel de grid para ordenar, filtrar, generar y cargar informes para las LUN protegidas en el entorno.

Crear una relación de protección SnapVault desde la vista Estado: Todos los volúmenes

Puede usar la vista Estado: Todos los volúmenes para crear relaciones de SnapVault para uno o más volúmenes en la misma máquina virtual de almacenamiento a fin de habilitar backups de datos para fines de protección.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

El menú **Protect** no aparece en los siguientes casos:

- Si la configuración de RBAC no permite esta acción: Por ejemplo, si solo tiene privilegios de operador
- Cuando se desconoce el ID de volumen: Por ejemplo, cuando se mantiene una relación de interconexión de clústeres y el clúster de destino aún no se detectó

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En la vista **Estado: Todos los volúmenes**, seleccione el volumen que desea proteger y haga clic en **proteger**.

Como alternativa, para crear varias relaciones de protección en la misma máquina virtual de almacenamiento (SVM), seleccione uno o más volúmenes en la vista Estado: Todos los volúmenes y haga clic en **proteger** en la barra de herramientas.

3. Seleccione **SnapVault** en el menú.

   Se abre el cuadro de diálogo Configure Protection.

4. Haga clic en **SnapVault** para ver la ficha **SnapVault** y configurar la información del volumen secundario.
5. Haga clic en **Avanzado** para establecer la deduplicación, compresión, crecimiento automático y garantía de espacio según sea necesario y, a continuación, haga clic en **aplicar**.
6. Complete el área **Información de destino** y el área **Configuración de relación** de la ficha **SnapVault**.
7. Haga clic en **aplicar**.

   Se devuelve a la vista Health: Todos los volúmenes.

8. Haga clic en el enlace del trabajo de configuración de protección situado en la parte superior de la vista **Estado: Todos los volúmenes**.

   Si solo se crea una relación de protección, se muestra la página de detalles Job; sin embargo, si se crea más de una relación de protección, se muestra una lista filtrada de todos los trabajos asociados con la operación de protección.

9. Debe realizar una de las siguientes acciones:
   - Si sólo tiene un trabajo, haga clic en **Actualizar** para actualizar la lista de tareas y los detalles de tareas asociados con el trabajo de configuración de protección y para determinar cuándo se ha completado el trabajo.
   - Si tiene más de un trabajo:
     i. Haga clic en un trabajo de la lista trabajos.
     ii. Haga clic en **Actualizar** para actualizar la lista de tareas y los detalles de tareas asociados con el trabajo de configuración de protección y para determinar cuándo se ha completado el trabajo.
     iii. Utilice el botón **Atrás** para volver a la lista filtrada y ver otro trabajo.

Crear una relación de protección SnapVault desde la página de detalles Volume/Health

Puede crear una relación de SnapVault mediante la página de detalles Volume/Health para que los backups de datos estén habilitados para la protección en los volúmenes.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation para que lleve a cabo esta tarea.

El menú **Protect** no aparece en los siguientes casos:

- Si la configuración de RBAC no permite esta acción: Por ejemplo, si solo tiene privilegios de operador
- Cuando se desconoce el ID de volumen: Por ejemplo, cuando se mantiene una relación de interconexión de clústeres y el clúster de destino aún no se detectó

Pasos

1. En la ficha **Protección** de la página de detalles **volumen / Salud**, haga clic con el botón derecho del ratón en un volumen de la vista de topología que desee proteger.
2. Seleccione **proteger** > **SnapVault** en el menú.

   Se abre el cuadro de diálogo Configure Protection.

3. Haga clic en **SnapVault** para ver la ficha **SnapVault** y configurar la información del recurso secundario.
4. Haga clic en **Avanzado** para establecer la deduplicación, compresión, crecimiento automático y garantía de espacio según sea necesario y, a continuación, haga clic en **aplicar**.
5. Complete el área **Información de destino** y el área **Configuración de relación** del cuadro de diálogo **Configurar protección**.
6. Haga clic en **aplicar**.

   Volverá a la página de detalles Volume / Health.

7. Haga clic en el enlace del trabajo de configuración de protección situado en la parte superior de la página de detalles **volumen / Estado**.

   Aparece la página de detalles Job.

8. Haga clic en **Actualizar** para actualizar la lista de tareas y los detalles de tareas asociados con el trabajo de configuración de protección y para determinar cuándo se ha completado el trabajo.

   Cuando se completan las tareas de trabajos, las nuevas relaciones se muestran en la vista de topología de la página de detalles Volume/Health.

Crear una relación de protección de SnapMirror desde la vista Estado: Todos los volúmenes

Con la vista Estado: Todos los volúmenes, es posible crear varias relaciones de protección de SnapMirror a la vez. Para ello, se seleccionan más de un volumen en la misma máquina virtual de almacenamiento.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

El menú **Protect** no aparece en los siguientes casos:

- Si la configuración de RBAC no permite esta acción: Por ejemplo, si solo tiene privilegios de operador
- Cuando se desconoce el ID de volumen: Por ejemplo, cuando se mantiene una relación de interconexión de clústeres y el clúster de destino aún no se detectó

Pasos

1. En la vista **Estado: Todos los volúmenes**, seleccione el volumen que desea proteger.

   Como alternativa, para crear varias relaciones de protección en el mismo SVM, seleccione uno o más volúmenes en la vista Estado: Todos los volúmenes y haga clic en **proteger** > **SnapMirror** en la barra de herramientas.

Se muestra el cuadro de diálogo Configurar protección.

2. Haga clic en **SnapMirror** para ver la ficha **SnapMirror** y configurar la información de destino.
3. Haga clic en **Avanzado** para establecer la garantía de espacio según sea necesario y, a continuación, haga clic en **aplicar**.
4. Complete el área **Información de destino** y el área **Configuración de relación** de la ficha **SnapMirror**.
5. Haga clic en **aplicar**.

   Se devuelve a la vista Health: Todos los volúmenes.

6. Haga clic en el enlace del trabajo de configuración de protección en la parte superior de la vista * Estado: Todos los volúmenes*.

   Si solo se crea una relación de protección, se muestra la página de detalles Job; sin embargo, si se crea más de una relación de protección, se muestra una lista de todos los trabajos asociados con la operación de protección.

7. Debe realizar una de las siguientes acciones:
   - Si sólo tiene un trabajo, haga clic en **Actualizar** para actualizar la lista de tareas y los detalles de tareas asociados con el trabajo de configuración de protección y para determinar cuándo se ha completado el trabajo.
   - Si tiene más de un trabajo:
     i. Haga clic en un trabajo de la lista trabajos.
     ii. Haga clic en **Actualizar** para actualizar la lista de tareas y los detalles de tareas asociados con el trabajo de configuración de protección y para determinar cuándo se ha completado el trabajo.
     iii. Utilice el botón **Atrás** para volver a la lista filtrada y ver otro trabajo.

En función de la SVM de destino especificada durante la configuración o de las opciones habilitadas en su configuración avanzada, la relación de SnapMirror resultante puede ser una de varias variaciones posibles:

- Si especificó una SVM de destino que se ejecuta con la misma versión o una posterior de ONTAP en comparación con la del volumen de origen, el resultado predeterminado será una relación de SnapMirror basada en replicación de bloques.
- Si especificó una SVM de destino que se ejecuta con una misma versión o una más reciente de ONTAP en comparación con la del volumen de origen, pero habilitó la replicación de versión flexible en la configuración avanzada, se obtiene una relación de SnapMirror con la replicación de versión flexible.
- Si especificó una SVM de destino que se ejecuta con una versión de ONTAP anterior a la del volumen de origen y la versión anterior admite la replicación de versión flexible, el resultado es una relación de SnapMirror con la replicación de versión flexible.

Crear una relación de protección SnapMirror desde la página de detalles Volume/Health

Puede usar la página de detalles Volume / Health para crear una relación de SnapMirror de modo que la replicación de datos esté habilitada para fines de protección. La replicación de SnapMirror permite restaurar datos del volumen de destino en caso de que se pierdan datos en el origen.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

El menú **Protect** no aparece en los siguientes casos:

- Si la configuración de RBAC no permite esta acción: Por ejemplo, si solo tiene privilegios de operador
- Cuando se desconoce el ID de volumen: Por ejemplo, cuando se mantiene una relación de interconexión de clústeres y el clúster de destino aún no se detectó

Se pueden ejecutar hasta 10 tareas de protección simultáneamente sin que el rendimiento se vea afectado. Es posible que experimente algún impacto en el rendimiento cuando se ejecutan entre 11 y 30 trabajos al mismo tiempo. No se recomienda ejecutar más de 30 trabajos simultáneamente.

Pasos

1. En la pestaña **Protección** de la página de detalles **volumen / Salud**, haga clic con el botón derecho del ratón en la vista de topología el nombre de un volumen que desea proteger.
2. Seleccione **proteger** > **SnapMirror** en el menú.

   Se muestra el cuadro de diálogo Configurar protección.

3. Haga clic en **SnapMirror** para ver la ficha **SnapMirror** y configurar la información de destino.
4. Haga clic en **Avanzado** para establecer la garantía de espacio según sea necesario y, a continuación, haga clic en **aplicar**.
5. Complete el área **Información de destino** y el área **Configuración de relación** del cuadro de diálogo **Configurar protección**.
6. Haga clic en **aplicar**.

   Volverá a la página de detalles Volume / Health.

7. Haga clic en el enlace del trabajo de configuración de protección situado en la parte superior de la página de detalles **volumen / Estado**.

   Las tareas y detalles del trabajo se muestran en la página de detalles Job.

8. En la página de detalles **Trabajo**, haga clic en **Actualizar** para actualizar la lista de tareas y los detalles de tareas asociados con el trabajo de configuración de protección y determinar cuándo se ha completado el trabajo.
9. Una vez completadas las tareas de trabajo, haga clic en **Atrás** en el explorador para volver a la página de detalles **volumen / Salud**.

   La nueva relación se muestra en la vista de topología de la página de detalles Volume/Health.

En función de la SVM de destino especificada durante la configuración o de las opciones habilitadas en su configuración avanzada, la relación de SnapMirror resultante puede ser una de varias variaciones posibles:

- Si especificó una SVM de destino que se ejecuta con la misma versión o una posterior de ONTAP en comparación con la del volumen de origen, el resultado predeterminado será una relación de SnapMirror basada en replicación de bloques.
- Si especificó una SVM de destino que se ejecuta con una misma versión o una más reciente de ONTAP en comparación con la del volumen de origen, pero habilitó la replicación de versión flexible en la configuración avanzada, se obtiene una relación de SnapMirror con la replicación de versión flexible.

- Si especificó una SVM de destino que se ejecuta en una versión anterior de ONTAP o una versión superior a la del volumen de origen y la versión anterior admite la replicación de versión flexible, el resultado es una relación de SnapMirror con la replicación de versión flexible.

Crear una relación de SnapMirror con una replicación de versión flexible

Puede crear una relación de SnapMirror con una replicación de versión flexible. La replicación con flexibilidad de versiones le permite implementar la protección de SnapMirror, incluso si los volúmenes de origen y destino se ejecutan en distintas versiones de ONTAP.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.
- Las SVM de origen y destino deben tener habilitada una licencia de SnapMirror.
- Las SVM de origen y destino deben ejecutarse en una versión del software ONTAP que admita la replicación con flexibilidad de versión.

SnapMirror con la replicación flexible de versiones le permite implementar la protección de SnapMirror incluso en entornos de almacenamiento heterogéneos en los que no todo el almacenamiento se ejecute en una versión de ONTAP; sin embargo, las operaciones de mirroring realizadas en SnapMirror con la replicación flexible de versión no se ejecutan con la misma rapidez que con SnapMirror de replicación tradicional por bloques.

Pasos

1. Abra el cuadro de diálogo **Configurar protección** para el volumen que desea proteger.
   - Si está viendo la ficha Protection de la página de detalles Volume / Health, haga clic con el botón derecho del ratón en la vista de topología que tiene el nombre de un volumen que desea proteger y seleccione **Protect** > **SnapMirror** en el menú.
   - Si está viendo la vista Estado: Todos los volúmenes, busque un volumen que desee proteger y haga clic con el botón derecho del ratón en él; a continuación, seleccione **proteger** > **SnapMirror** en el menú. Se muestra el cuadro de diálogo Configurar protección.
2. Haga clic en **SnapMirror** para ver la ficha **SnapMirror**.
3. Complete el área **Información de destino** y el área **Configuración de relación** del cuadro de diálogo **Configurar protección**.

   Si se especifica una SVM de destino que se ejecuta en una versión anterior de ONTAP que el volumen de origen que se está protegiendo y, si esa versión anterior admite la replicación con flexibilidad de versión, esta tarea configura automáticamente SnapMirror con replicación de versión flexible.

4. Si especifica una SVM de destino que se ejecuta con la misma versión de ONTAP que la del volumen de origen, pero desea configurar SnapMirror con replicación de versión flexible, haga clic en **Avanzado** para activar la replicación de versión flexible y, a continuación, haga clic en **aplicar**.
5. Haga clic en **aplicar**.

   Volverá a la página de detalles Volume / Health.

6. Haga clic en el enlace del trabajo de configuración de protección situado en la parte superior de la página de detalles **volumen / Estado**.

Las tareas y los detalles de los trabajos se muestran en la página de detalles Job.

7. En la página de detalles **Trabajo**, haga clic en **Actualizar** para actualizar la lista de tareas y los detalles de tareas asociados con el trabajo de configuración de protección y determinar cuándo se ha completado el trabajo.
8. Una vez completadas las tareas de trabajo, haga clic en **Atrás** en el explorador para volver a la página de detalles **volumen / Salud**.

   La nueva relación se muestra en la vista de topología de la página de detalles Volume/Health.

Crear relaciones SnapMirror con una replicación de versión flexible con la opción de backup

Puede crear una relación de SnapMirror con la funcionalidad de opción de replicación y backup con versión flexible. La funcionalidad de opción de backup le permite implementar la protección de SnapMirror y también conservar varias versiones de copias de backup en la ubicación de destino.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.
- Las SVM de origen y destino deben tener habilitada una licencia de SnapMirror.
- Las SVM de origen y destino deben tener habilitada una licencia de SnapVault.
- Las SVM de origen y destino deben ejecutarse en una versión del software ONTAP que admita la replicación con flexibilidad de versión.

La configuración de SnapMirror con la funcionalidad de opción de backup permite proteger los datos con las funcionalidades de recuperación ante desastres de SnapMirror, como la posibilidad de recuperación tras fallos en volúmenes, y al mismo tiempo proporcionar funcionalidades SnapVault, como la protección de varias copias de backup.

Pasos

1. Abra el cuadro de diálogo **Configurar protección** para el volumen que desea proteger.
   - Si está viendo la ficha Protection de la página de detalles Volume / Health, haga clic con el botón derecho del ratón en la vista de topología en el nombre de un volumen que desea proteger y seleccione **Protect** > **SnapMirror** en el menú.
   - Si está viendo la vista Estado: Todos los volúmenes, busque un volumen que desee proteger y haga clic con el botón derecho del ratón en él; a continuación, seleccione **proteger** > **SnapMirror** en el menú. Se muestra el cuadro de diálogo Configurar protección.
2. Haga clic en **SnapMirror** para ver la ficha **SnapMirror**.
3. Complete el área **Información de destino** y el área **Configuración de relación** del cuadro de diálogo **Configurar protección**.
4. Haga clic en **Avanzado** para que aparezca el cuadro de diálogo **Configuración avanzada de destino**.
5. Si la casilla de verificación **Version-flexible Replication** no está activada, selecciónela ahora.
6. Active la casilla de verificación **con opción de copia de seguridad** para activar la función de opción de copia de seguridad; a continuación, haga clic en **aplicar**.

7. Haga clic en **aplicar**.

   Volverá a la página de detalles Volume / Health.

8. Haga clic en el enlace del trabajo de configuración de protección situado en la parte superior de la página de detalles **volumen / Estado**.

   Las tareas y los detalles de los trabajos se muestran en la página de detalles Job.

9. En la página de detalles **Trabajo**, haga clic en **Actualizar** para actualizar la lista de tareas y los detalles de tareas asociados con el trabajo de configuración de protección y determinar cuándo se ha completado el trabajo.
10. Una vez completadas las tareas de trabajo, haga clic en **Atrás** en el explorador para volver a la página de detalles **volumen / Salud**.

    La nueva relación se muestra en la vista de topología de la página de detalles Volume/Health.

Configurar los ajustes de eficiencia de destino

Puede configurar opciones de eficiencia de destino como la deduplicación, la compresión, el crecimiento automático y la garantía de espacio en un destino de protección con el cuadro de diálogo Advanced Destination Settings. Esta configuración se usa cuando se desea maximizar el uso de espacio en un volumen de destino o secundario.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

De forma predeterminada, la configuración de eficiencia coincide con la del volumen de origen, excepto la configuración de compresión de una relación SnapVault, que se deshabilita de forma predeterminada.

Pasos

1. Haga clic en la ficha **SnapMirror** o en la ficha **SnapVault** del cuadro de diálogo **Configurar protección**, según el tipo de relación que esté configurando.
2. Haga clic en **Avanzado** en el área **Información de destino**.

   Se abre el cuadro de diálogo Advanced Destination Settings.

3. Habilitar o deshabilitar la configuración de eficiencia para la deduplicación, la compresión, el crecimiento automático y la garantía de espacio, según sea necesario.
4. Haga clic en **aplicar** para guardar las selecciones y volver al cuadro de diálogo **Configurar protección**.

Crear programaciones de SnapMirror y SnapVault

Puede crear programaciones básicas o avanzadas de SnapMirror y SnapVault para habilitar las transferencias automáticas de protección de datos en un volumen primario o de origen, de modo que las transferencias se realicen con mayor frecuencia o menos frecuencia, según la frecuencia de los cambios de datos en los volúmenes.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Ya debe completar el área Destination Information en el cuadro de diálogo Configure Protection.
- Debe haber configurado Workflow Automation para que lleve a cabo esta tarea.

Pasos

1. En la ficha **SnapMirror** o en la ficha **SnapVault** del cuadro de diálogo **Configurar protección**, haga clic en el vínculo **Crear programación** del área **Configuración de relación**.

   Se mostrará el cuadro de diálogo Crear programación.

2. En el campo **Nombre de horario**, escriba el nombre que desea asignar a la programación.
3. Seleccione una de las siguientes opciones:
   - **Básico**

     Seleccione si desea crear una programación básica de tipo intervalo.

   - **Avanzado**

     Seleccione si desea crear una programación de tareas con Cron.

4. Haga clic en **Crear**.

   La nueva programación se muestra en la lista desplegable SnapMirror Schedule o SnapVault Schedule.

Crear relaciones en cascada o con ventilador para ampliar la protección a partir de una relación de protección existente

Puede ampliar la protección a partir de una relación existente creando fanout a partir del volumen de origen o una cascada a partir del volumen de destino de una relación existente. Puede hacerlo cuando necesite copiar datos de un sitio a muchos sitios o para proporcionar protección adicional mediante la creación de más backups.

Es posible ampliar la protección a los volúmenes mediante el grupo de coherencia, que es un contenedor donde se contienen varios volúmenes para que se puedan gestionar todos los volúmenes como una entidad. Puede ver el grupo de coherencia de continuidad del negocio de SnapMirror (SM-BC) y la relación de grupo de coherencia síncrono en la página Relationships de Unified Manager.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

Pasos

1. Haga clic en **Protección** > **Relaciones**. Como alternativa, puede ver las relaciones en la página de detalles Volume.
2. En la página **Relaciones de volumen**, seleccione la relación de SnapMirror desde la que desea ampliar la protección.
3. En la barra de acciones, haga clic en **extender protección**.

4. En el menú, seleccione **desde origen** o **desde destino**, dependiendo de si está creando una relación de fanout desde la fuente o una relación de cascada desde el destino.
5. Seleccione **con SnapMirror** o **con SnapVault** según el tipo de relación de protección que esté creando.

   Aparece el cuadro de diálogo **Configurar protección**.

   Esto se puede lograr a partir de la página de detalles Unified Relationship / Volume Relationship y Volume / Health.

6. Complete la información como se indica en el cuadro de diálogo **Configurar protección**.

Editar las relaciones de protección en la página Volume Relationships

Las relaciones de protección existentes se pueden editar para cambiar la tasa de transferencia máxima, la política de protección o la programación de protección. Se puede editar una relación para reducir el ancho de banda que se usa para las transferencias o aumentar la frecuencia de las transferencias programadas, ya que los datos cambian con frecuencia.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Los volúmenes seleccionados deben ser destinos de relaciones de protección. No puede editar las relaciones cuando se seleccionan los volúmenes de origen, los volúmenes compartidos de carga o los volúmenes que no son el destino de una relación de SnapMirror o SnapVault.

Pasos

1. En la página **Relaciones de volumen**, seleccione en la lista de volúmenes uno o más volúmenes en la misma SVM para la que desea editar la configuración de relaciones y, a continuación, seleccione **Editar** en la barra de herramientas.

   Se muestra el cuadro de diálogo Editar relación.

2. En el cuadro de diálogo **Editar relación**, edite la tasa de transferencia máxima, la política de protección o el programa de protección según sea necesario.
3. Haga clic en **aplicar**.

   Los cambios se aplican a las relaciones seleccionadas.

Editar las relaciones de protección desde la página de detalles volumen / Estado

Es posible editar las relaciones de protección existentes para cambiar la tasa de transferencia máxima actual, la política de protección o la programación de protección. Se puede editar una relación para reducir el ancho de banda que se usa para las transferencias o aumentar la frecuencia de las transferencias programadas, ya que los datos cambian con frecuencia.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber instalado y configurado Workflow Automation.

Los volúmenes seleccionados deben ser destinos de relaciones de protección. No puede editar las relaciones cuando se seleccionan los volúmenes de origen, los volúmenes compartidos de carga o los volúmenes que no son el destino de una relación de SnapMirror o SnapVault.

Pasos

1. En la pestaña **Protección** de la página de detalles **volumen / Salud**, busque en la topología la relación de protección que desea editar y haga clic con el botón derecho del ratón en ella.
2. Seleccione **Editar** en el menú.

   Como alternativa, en el menú **acciones**, seleccione **relación** > **Edición** para editar la relación para la que está viendo los detalles.

   Aparece el cuadro de diálogo **Editar relación**.
3. En el cuadro de diálogo Edit Relationship, edite la tasa de transferencia máxima, la política de protección o la programación de protección según sea necesario.
4. Haga clic en **aplicar**.

   Los cambios se aplican a las relaciones seleccionadas.

Creación de una política de SnapMirror para maximizar la eficiencia de transferencia

Puede crear una política de SnapMirror para especificar la prioridad de transferencia de SnapMirror para las relaciones de protección. Las políticas de SnapMirror permiten maximizar la eficiencia de transferencia del origen al destino asignando las prioridades para que las transferencias de menor prioridad se programen después de las transferencias de prioridad normal.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.
- En esta tarea se supone que ya ha completado el área Información de destino del cuadro de diálogo Configurar protección.

Pasos

1. En la ficha **SnapMirror** del cuadro de diálogo **Configurar protección**, haga clic en el enlace **Crear directiva** del área **Configuración de relación**.

   Se mostrará el cuadro de diálogo Create SnapMirror Policy.
2. En el campo **Nombre de directiva**, escriba el nombre que desea asignar a la directiva.
3. En el campo **prioridad de transferencia**, seleccione la prioridad de transferencia que desea asignar a la directiva.
4. En el campo **Comentario**, introduzca un comentario opcional para la directiva.

5. Haga clic en **Crear**.

   La nueva política se muestra en la lista desplegable SnapMirror Policy.

Creación de una política de SnapVault para maximizar la eficiencia de transferencia

Puede crear una nueva política de SnapVault para configurar la prioridad para una transferencia de SnapVault. Las políticas se usan para maximizar la eficiencia de las transferencias del almacenamiento primario al secundario en una relación de protección.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.
- Ya debe haber completado el área Destination Information en el cuadro de diálogo Configure Protection.

Pasos

1. En la ficha **SnapVault** del cuadro de diálogo **Configurar protección**, haga clic en el enlace **Crear directiva** del área **Configuración de relación**.

   Aparece la pestaña SnapVault.

2. En el campo **Nombre de directiva**, escriba el nombre que desea asignar a la directiva.
3. En el campo **prioridad de transferencia**, seleccione la prioridad de transferencia que desea asignar a la directiva.
4. **Opcional:** en el campo **Comentario**, introduzca un comentario para la directiva.
5. En el área **etiqueta de replicación**, agregue o edite una etiqueta de replicación, según sea necesario.
6. Haga clic en **Crear**.

   La nueva directiva se muestra en la lista desplegable Crear directiva.

Cancelar una transferencia de protección de datos activa desde la página Relaciones de volumen

Puede anular una transferencia de protección de datos activa cuando desee detener una replicación de SnapMirror en curso. También puede borrar el punto de comprobación de reinicio para las transferencias posteriores a la transferencia de línea de base. Puede cancelar una transferencia cuando entra en conflicto con otra operación, como un movimiento de volumen.

No se pueden cancelar relaciones de volúmenes protegidas por el grupo de coherencia.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

La acción Anular no se muestra en las siguientes instancias:

- Si la configuración de RBAC no permite esta acción: Por ejemplo, si solo tiene privilegios de operador
- Cuando se desconoce el ID de volumen: Por ejemplo, cuando se mantiene una relación de interconexión de clústeres y el clúster de destino aún no se detectó

No puede borrar el punto de comprobación de reinicio para una transferencia de línea de base.

Pasos

1. Para cancelar las transferencias de una o más relaciones de protección, en la página **Relaciones de volumen**, seleccione uno o más volúmenes y, en la barra de herramientas, haga clic en **Anular**.

   Aparecerá el cuadro de diálogo Anular transferencia .

2. Si desea borrar el punto de comprobación de reinicio para una transferencia que no sea una transferencia de línea de base, seleccione **Borrar puntos de control**.
3. Haga clic en **continuar**.

   El cuadro de diálogo Anular transferencia se cierra y el estado del trabajo de interrupción se muestra en la parte superior de la página Relaciones de volumen junto con un vínculo a los detalles del trabajo.

4. **Opcional:** haga clic en el enlace **Ver detalles** para ir a la página de detalles **Trabajo** para obtener más detalles y ver el progreso del trabajo.

Cancelación de una transferencia de protección de datos activa desde la página de detalles volumen / Salud

Puede anular una transferencia de protección de datos activa cuando desee detener una replicación de SnapMirror en curso. También puede borrar el punto de control de reinicio para una transferencia si no es una transferencia de línea base. Puede cancelar una transferencia cuando entra en conflicto con otra operación, como un movimiento de volumen.

No se pueden cancelar relaciones de volúmenes protegidas por el grupo de coherencia.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

La acción Anular no se muestra en las siguientes instancias:

- Si la configuración de RBAC no permite esta acción: Por ejemplo, si solo tiene privilegios de operador
- Cuando se desconoce el ID de volumen: Por ejemplo, cuando se mantiene una relación de interconexión de clústeres y el clúster de destino aún no se detectó

No puede borrar el punto de comprobación de reinicio para una transferencia de línea de base.

Pasos

1. En la pestaña **Protección** de la página de detalles **volumen / Salud**, haga clic con el botón derecho del ratón en la relación en la vista de topología para la transferencia de datos que desea cancelar y seleccione **Anular**.

Aparecerá el cuadro de diálogo Anular transferencia .

2. Si desea borrar el punto de comprobación de reinicio para una transferencia que no sea una transferencia de línea de base, seleccione **Borrar puntos de control**.
3. Haga clic en **continuar**.

   El cuadro de diálogo Anular transferencia se cierra y el estado de la operación de anulación se muestra en la parte superior de la página de detalles volumen/Estado junto con un enlace a los detalles del trabajo.

4. **Opcional:** haga clic en el enlace **Ver detalles** para ir a la página de detalles **Trabajo** para obtener más detalles y ver el progreso del trabajo.
5. Haga clic en cada tarea de trabajo para ver sus detalles.
6. Haga clic en la flecha Atrás de su navegador para volver a la página de detalles **volumen / Salud**.

   La operación de anulación finaliza cuando todas las tareas de trabajo se completan correctamente.

Desactivación de una relación de protección en la página Relaciones de volumen

En la página Volume Relationships, es posible desactivar una relación de protección para evitar temporalmente las transferencias de datos. Puede desactivar una relación cuando desea crear una copia Snapshot de un volumen de destino de SnapMirror que contiene una base de datos, y desea garantizar que su contenido sea estable durante la operación de copia de Snapshot.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

La acción de inactividad no se muestra en las siguientes instancias:

- Si la configuración de RBAC no permite esta acción; por ejemplo, si solo tiene privilegios de operador
- Cuando se desconoce el ID de volumen; por ejemplo, cuando se establece una relación de interconexión de clústeres y el clúster de destino aún no se detectó
- Cuando no esté emparejado Workflow Automation y Unified Manager

Pasos

1. Para desactivar las transferencias para una o más relaciones de protección, en la página **Relaciones de volumen**, seleccione uno o más volúmenes y, en la barra de herramientas, haga clic en **Quiesce**.

   Aparecerá el cuadro de diálogo Quiesce.

2. Haga clic en **continuar**.

   El estado del trabajo de inactividad se muestra en la parte superior de la página de detalles Volume / Health, junto con un enlace a los detalles del trabajo.

3. Haga clic en el enlace **Ver detalles** para ir a la página de detalles **Trabajo** para obtener detalles adicionales y el progreso del trabajo.
4. **Opcional:** haga clic en la flecha **Atrás** de su navegador para volver a la página **Relaciones de volumen**.

El trabajo de inactividad finaliza cuando todas las tareas de trabajo se completan correctamente.

Desactivación de una relación de protección desde la página de detalles volumen / Salud

Es posible poner en modo inactivo una relación de protección para evitar temporalmente las transferencias de datos. Puede desactivar una relación cuando desea crear una copia Snapshot de un volumen de destino de SnapMirror que contiene una base de datos, y desea garantizar que su contenido sea estable durante la copia Snapshot.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

La acción de inactividad no se muestra en las siguientes instancias:

- Si la configuración de RBAC no permite esta acción, por ejemplo, si solo tiene privilegios de operador
- Si se desconoce el ID de volumen, por ejemplo, cuando se mantiene una relación de interconexión de clústeres y el clúster de destino aún no se detectó
- Cuando no esté emparejado Workflow Automation y Unified Manager

Pasos

1. En la pestaña **Protección** de la página de detalles **volumen / Salud**, haga clic con el botón derecho del ratón en la relación en la vista de topología para la relación de protección que desea desactivar.
2. Seleccione **Quiesce** en el menú.
3. Haga clic en **Sí** para continuar.

   El estado del trabajo de inactividad se muestra en la parte superior de la página de detalles Volume / Health, junto con un enlace a los detalles del trabajo.

4. Haga clic en el enlace **Ver detalles** para ir a la página de detalles **Trabajo** para obtener detalles adicionales y el progreso del trabajo.
5. **Opcional:** haga clic en la flecha Atrás de su navegador para volver a la página de detalles **volumen / Salud**.

   El trabajo de inactividad finaliza cuando todas las tareas de trabajo se completan correctamente.

Interrumpir una relación de SnapMirror en la página Volume Relationships

Puede romper una relación de protección para detener las transferencias de datos entre un volumen de origen y un volumen de destino en una relación de SnapMirror. Puede romper una relación cuando desea migrar datos, para la recuperación ante desastres o para la prueba de aplicaciones. El volumen de destino cambia a un volumen de lectura/escritura. No es posible interrumpir una relación de SnapVault.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

Pasos

1. En la página **Relaciones de volumen**, seleccione uno o más volúmenes con relaciones de protección para los que desea detener las transferencias de datos y, en la barra de herramientas, haga clic en **Pausa**.

   Se muestra el cuadro de diálogo romper relación.

2. Haga clic en **continuar** para romper la relación.
3. En la página **Relaciones de volumen**, compruebe en la columna **Estado de relación** que la relación está rota.

   La columna Estado de la relación está oculta de forma predeterminada, por lo que es posible que tenga que seleccionarla en la lista Mostrar u ocultar columnas .

Quitar una relación de protección en la página Volume Relationships

En la página Volume Relationships, puede quitar una relación de protección para eliminar de forma permanente una relación existente entre el origen y el destino seleccionados: Por ejemplo, cuando desea crear una relación con otro destino. Esta operación elimina todos los metadatos y no puede deshacerse.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

Pasos

1. En la página **Relaciones de volumen**, seleccione uno o más volúmenes con relaciones de protección que desee quitar y, en la barra de herramientas, haga clic en **Quitar**.

   Se muestra el cuadro de diálogo Eliminar relación.

2. Haga clic en **continuar** para eliminar la relación.

   La relación se eliminará de la página Relaciones de volumen.

Reanude las transferencias programadas en una relación de modo inactivo en la página Relaciones de volumen

Después de poner en modo inactivo una relación para detener las transferencias programadas, puede usar **Reanudar** para volver a habilitar las transferencias programadas de modo que se protejan los datos del volumen de origen o primario. Las transferencias se reanudan desde un punto de comprobación, si existe alguno, en el siguiente intervalo de transferencia programada.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

Puede seleccionar no más de 10 relaciones en modo inactivo en las que reanudar las transferencias.

Pasos

1. En la página volumen **Relaciones**, seleccione uno o más volúmenes con relaciones en modo inactivo y, en la barra de herramientas, haga clic en **Reanudar**.
2. En el cuadro de diálogo **Reanudar**, haga clic en **continuar**.

   Volverá a la página Volume Relationships.
3. Para ver las tareas de trabajo relacionadas y realizar un seguimiento de su progreso, haga clic en el vínculo de trabajo que aparece en la parte superior de la página **Relaciones de volumen**.
4. Debe realizar una de las siguientes acciones:
   - Si sólo se muestra un trabajo, en la página de detalles del trabajo, haga clic en **Actualizar** para actualizar la lista de tareas y los detalles de las tareas asociados con el trabajo de configuración de protección y para determinar cuándo se ha completado el trabajo.
   - Si se muestra más de un trabajo,
     i. En la página Jobs, haga clic en el trabajo para el que desea ver los detalles.
     ii. En la página de detalles del trabajo, haga clic en **Actualizar** para actualizar la lista de tareas y los detalles de las tareas asociadas con el trabajo de configuración de protección y para determinar cuándo se ha completado el trabajo. Cuando los trabajos finalizan, las transferencias de datos se reanudan en el siguiente intervalo de transferencia programado.

Reanude las transferencias programadas en una relación en modo inactivo en la página de detalles Volume/Health

Después de poner en modo inactivo una relación para detener las transferencias programadas, puede usar **Reanudar** en la página de detalles volumen / Estado para volver a habilitar las transferencias programadas de modo que los datos en el volumen de origen o primario estén protegidos. Las transferencias se reanudan desde un punto de comprobación, si existe alguno, en el siguiente intervalo de transferencia programada.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

Pasos

1. En la pestaña **Protección** de la página de detalles **volumen / Salud**, haga clic con el botón derecho del ratón en la vista de topología en una relación en modo inactivo que desea reanudar.

   Como alternativa, seleccione **Reanudar** en el menú **acciones** > **relación**.
2. En el cuadro de diálogo **Reanudar**, haga clic en **continuar**.

   Volverá a la página de detalles Volume / Health.

3. Para ver las tareas de trabajo relacionadas y realizar un seguimiento de su progreso, haga clic en el enlace de trabajo que aparece en la parte superior de la página de detalles **volumen / Salud**.
4. En la página de detalles **Trabajo**, haga clic en **Actualizar** para actualizar la lista de tareas y los detalles de tareas asociados con el trabajo de configuración de protección y determinar cuándo se ha completado el trabajo.

   Una vez finalizados los trabajos, las transferencias de datos se reanudan en el siguiente intervalo de transferencia programada.

Inicializando o actualizando relaciones de protección en la página Volume Relationships

Desde la página Volume Relationships, puede realizar una primera transferencia inicial de referencia en una nueva relación de protección o actualizar una relación si ya se ha inicializado y desea realizar una actualización incremental manual no programada para transferir de inmediato.

No se pueden inicializar o actualizar volúmenes protegidos por grupos de coherencia.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado OnCommand Workflow Automation.

Pasos

1. En la página **Relaciones de volumen**, haga clic con el botón secundario del ratón en un volumen y seleccione uno o más volúmenes con relaciones que desee actualizar o inicializar y, a continuación, haga clic en **inicializar/Actualizar** en la barra de herramientas.

   Aparece el cuadro de diálogo **inicializar/actualizar**.

2. En la ficha **Opciones de transferencia**, seleccione una prioridad de transferencia y la velocidad máxima de transferencia.
3. Haga clic en **copias Snapshot de origen**; a continuación, en la columna **copia Snapshot**, haga clic en **predeterminado**.

   Se muestra el cuadro de diálogo Seleccionar copia Snapshot de origen.

4. Si desea especificar una copia Snapshot existente en lugar de transferir la copia Snapshot predeterminada, haga clic en **copia Snapshot existente** y seleccione una copia Snapshot de la lista.
5. Haga clic en **Enviar**.

   Volverá al cuadro de diálogo **inicializar/actualizar**.

6. Si ha seleccionado más de un origen para inicializar o actualizar, haga clic en **predeterminado** para el siguiente origen para el que desea especificar una copia Snapshot existente.
7. Haga clic en **Enviar** para iniciar el trabajo de inicialización o actualización.

   El trabajo de inicialización o actualización se inicia, vuelve a la página Volume Relationships y se muestra un enlace Jobs en la parte superior de la página.

8. **Opcional:** haga clic en **Ver trabajos** en la vista **Estado: Todos los volúmenes** para realizar un seguimiento del estado de cada trabajo de inicialización o actualización.

   Se muestra una lista filtrada de trabajos.

9. **Opcional:** haga clic en cada trabajo para ver sus detalles.
10. **Opcional:** haga clic en la flecha **Atrás** de su navegador para volver a la página **Relaciones de volumen**.

    La operación de inicialización o actualización finaliza cuando todas las tareas finalizan correctamente.

Inicializar o actualizar las relaciones de protección en la página de detalles Volume / Health

Puede realizar una primera transferencia de referencia en una nueva relación de protección o actualizar una relación si ya está inicializada y desea realizar una actualización incremental manual no programada para transferir datos de inmediato.

NOTA: No puede inicializar ni actualizar volúmenes protegidos por grupos de consistencia.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado OnCommand Workflow Automation.

Pasos

1. En la ficha **Protección** de la página de detalles **volumen / Salud**, busque en la topología la relación de protección que desea inicializar o actualizar y haga clic con el botón secundario del ratón en ella.
2. Seleccione **inicializar/actualizar** en el menú.

   Como alternativa, en el menú **acciones**, seleccione **relación** > **inicializar/actualizar** para inicializar o actualizar la relación para la que está viendo los detalles.

   Aparece el cuadro de diálogo inicializar/actualizar.

3. En la ficha **Opciones de transferencia**, seleccione una prioridad de transferencia y la velocidad máxima de transferencia.
4. Haga clic en **copias Snapshot de origen**; a continuación, en la columna **copia Snapshot**, haga clic en **predeterminado**.

   Se muestra el cuadro de diálogo Seleccionar copia Snapshot de origen.

5. Si desea especificar una copia Snapshot existente en lugar de transferir la copia Snapshot predeterminada, haga clic en **copia Snapshot existente** y seleccione una copia Snapshot de la lista.
6. Haga clic en **Enviar**.

   Volverá al cuadro de diálogo inicializar/actualizar.

7. Si ha seleccionado más de un origen para inicializar o actualizar, haga clic en **predeterminado** para el siguiente origen de lectura/escritura para el que desea especificar una copia Snapshot existente.

   No puede seleccionar una copia Snapshot diferente para los volúmenes de protección de datos.

8. Haga clic en **Enviar** para iniciar el trabajo de inicialización o actualización.

   El trabajo de inicialización o actualización se inicia, vuelve a la página de detalles Volume / Health y se muestra un enlace Jobs en la parte superior de la página.

9. **Opcional:** haga clic en **Ver trabajos** en la página de detalles **volumen / Salud** para realizar un seguimiento del estado de cada trabajo de inicialización o actualización.

   Se muestra una lista filtrada de trabajos.

10. **Opcional:** haga clic en cada trabajo para ver sus detalles.
11. **Opcional:** haga clic en la flecha Atrás de su navegador para volver a la página de detalles **volumen / Salud**.

    La operación de inicialización o actualización finaliza cuando todas las tareas de trabajo se completan correctamente.

Resincronizando las relaciones de protección desde la página Volume Relationships

En la página Volume Relationships, es posible volver a sincronizar una relación para recuperarse de un evento que deshabilitó el volumen de origen o cuando desea cambiar el origen actual a otro volumen.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.

Pasos

1. En la página **Relaciones de volumen**, seleccione uno o más volúmenes con relaciones en modo inactivo y, en la barra de herramientas, haga clic en **Resincronizar**.

   Aparecerá el cuadro de diálogo Resynchronize.

2. En la pestaña **Opciones de resincronización**, seleccione una prioridad de transferencia y la tasa de transferencia máxima.
3. Haga clic en **copias Snapshot de origen**; a continuación, en la columna **copia Snapshot**, haga clic en **predeterminado**.

   Se muestra el cuadro de diálogo Seleccionar copia Snapshot de origen.

4. Si desea especificar una copia Snapshot existente en lugar de transferir la copia Snapshot predeterminada, haga clic en **copia Snapshot existente** y seleccione una copia Snapshot de la lista.
5. Haga clic en **Enviar**.

   Volverá al cuadro de diálogo Resynchronize.

6. Si ha seleccionado más de un origen para volver a sincronizar, haga clic en **predeterminado** para el siguiente origen para el que desea especificar una copia Snapshot existente.
7. Haga clic en **Enviar** para iniciar el trabajo de resincronización.

El trabajo de resincronización se inició, regresará a la página Volume Relationships y se mostrará un enlace de trabajos en la parte superior de la página.

8. **Opcional:** haga clic en **Ver trabajos** en la página **Relaciones de volumen** para realizar un seguimiento del estado de cada trabajo de resincronización.

   Se muestra una lista filtrada de trabajos.

9. **Opcional:** haga clic en la flecha **Atrás** de su navegador para volver a la página **Relaciones de volumen**.

   La operación de resincronización finaliza cuando todas las tareas de trabajo se finalizan correctamente.

Inversión de las relaciones de protección en la página Volume Relationships

Cuando un desastre deshabilita el volumen de origen en la relación de protección, es posible utilizar el volumen de destino para suministrar datos mediante la conversión a un volumen de lectura/escritura mientras se repara o sustituye el origen. Cuando el origen vuelve a estar disponible para recibir datos, puede utilizar la operación de resincronización inversa para establecer la relación en la dirección inversa y sincronizar los datos del origen con los datos en el destino de lectura/escritura.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado Workflow Automation.
- La relación no debe ser una relación de SnapVault.
- Debe haber una relación de protección.
- La relación de protección debe romperse.
- El origen y el destino deben estar en línea.
- El origen no debe ser el destino de otro volumen de protección de datos.
- Cuando realiza esta tarea, se eliminan los datos en el origen más nuevos que los de la copia Snapshot común.
- Las políticas y las programaciones creadas en relaciones de resincronización inversa son las mismas que en la relación de protección original.

  Si no existen las políticas y las programaciones, se crean.

Pasos

1. En la página **Relaciones de volumen**, seleccione uno o más volúmenes con relaciones que desee invertir y, en la barra de herramientas, haga clic en **Resync inversa**.

   Se muestra el cuadro de diálogo Reverse Resync.

2. Compruebe que las relaciones que aparecen en el cuadro de diálogo **Resync inversa** son las que desea realizar la operación de resincronización inversa y, a continuación, haga clic en **Enviar**.

   Se inicia la operación de resincronización inversa, vuelve a la página Relaciones de volumen y se muestra un enlace de trabajos en la parte superior de la página.

3. **Opcional:** haga clic en **Ver trabajos** en la página **Relaciones de volumen** para realizar un seguimiento del estado de cada trabajo de resincronización inversa.

   Se muestra una lista filtrada de trabajos relacionados con esta operación.

4. **Opcional:** haga clic en la flecha **Atrás** de su navegador para volver a la página **Relaciones de volumen**.

   La operación de resincronización inversa se completa cuando todas las tareas de trabajo se completan correctamente.

Restaurar datos mediante las páginas de detalles Volume y Volume/Health

Es posible restaurar archivos, directorios o un volumen entero sobrescritos o eliminados de una copia Snapshot con la función de restauración en las páginas de detalles Volume and Volume/Health.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Tenga en cuenta lo siguiente:

- No puede restaurar flujos de archivos NTFS.
- La opción de restauración no está disponible si:
  - El ID de volumen es desconocido: Por ejemplo, cuando se mantiene una relación de interconexión de clústeres y el clúster de destino todavía no se detectó.
  - El volumen está configurado para la replicación síncrona de SnapMirror.

Pasos

1. Desde el panel de navegación izquierdo, vaya a **almacenamiento > volúmenes**.
2. Seleccione el volumen y haga clic en el botón **Restaurar**. Como alternativa, haga clic en el volumen para ir a **Detalles del volumen / Salud > acciones > Restaurar**. Aparece el cuadro de diálogo Restaurar. Para obtener información sobre esta página, consulte "Restaurar".
3. Seleccione el volumen y la copia Snapshot de los que desea restaurar datos si es diferente de la predeterminada.
4. Seleccione los elementos que desea restaurar, por ejemplo, la LUN de origen.

   Es posible restaurar todo el volumen, o bien especificar carpetas y archivos que se desean restaurar.

5. Seleccione la ubicación a la que desea restaurar los elementos seleccionados: **Ubicación original** o **ubicación alternativa existente**.
6. Si selecciona una ubicación existente alternativa, realice una de las siguientes acciones:
   - En el campo de texto Restaurar ruta, escriba la ruta de acceso de la ubicación en la que desea restaurar los datos y, a continuación, haga clic en **Seleccionar directorio**.
   - Haga clic en **examinar** para abrir el cuadro de diálogo examinar directorios y siga los pasos siguientes:
     i. Seleccione el clúster de destino, la máquina virtual de almacenamiento (SVM) y el volumen donde desee restaurar.

ii. En la tabla Name, seleccione un nombre de directorio que debe restaurarse.

iii. Haga clic en **Seleccionar directorio**.

7. Haga clic en **Restaurar**.

   Se inicia el proceso de restauración. Se crea un trabajo en el back-end para completar el proceso de restauración.

8. Si desea ver el progreso del trabajo, en el panel de navegación izquierdo, vaya a **Protección > trabajos** para ver el estado del trabajo de restauración desde la lista de trabajos.

> Si una operación de restauración falla entre clústeres de Cloud Volumes ONTAP HA con un error NDMP, es posible que deba agregar una ruta de AWS explícita en el clúster de destino para que este pueda comunicarse con el LIF de administración del clúster del sistema de origen. Este paso de configuración se realiza mediante la consola de NetApp .

Qué pools de recursos son

Los pools de recursos son grupos de agregados creados por un administrador de almacenamiento mediante Unified Manager con el fin de proporcionar el aprovisionamiento a aplicaciones de partner para la gestión de backup.

Puede agrupar sus recursos en función de atributos como el rendimiento, el costo, la ubicación física o la disponibilidad. Mediante la agrupación de recursos relacionados en un pool, puede tratar el pool como una única unidad para la supervisión y el aprovisionamiento. Esto simplifica la gestión de estos recursos y permite un uso más flexible y eficiente del almacenamiento.

Durante el aprovisionamiento de almacenamiento secundario, Unified Manager determina el agregado más adecuado del pool de recursos para su protección usando los siguientes criterios:

- El agregado es un agregado de datos (no un agregado raíz) y se ENCUENTRA EN LÍNEA.
- El agregado se encuentra en un nodo de clúster de destino cuya versión de ONTAP sea la misma o superior a la versión principal del clúster de origen.
- El agregado tiene el mayor espacio disponible de todos los agregados del pool de recursos.
- Tras aprovisionar el volumen de destino, el espacio de la agrupación se encuentra dentro del umbral casi completo y casi comprometido definido para el agregado (umbral global o local, lo que corresponda).
- El número de volúmenes de FlexVol en el nodo de destino no debe superar el límite de plataforma.

Creación de pools de recursos

Puede utilizar el cuadro de diálogo Crear pool de recursos para agrupar agregados con fines de aprovisionamiento.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

Los pools de recursos pueden contener agregados de clústeres de diferentes, pero el mismo agregado no puede pertenecer a pools de recursos diferentes.

1. En el panel de navegación izquierdo, haga clic en **Protección** > **agrupaciones de recursos**.
2. En la página **Pools de recursos**, haga clic en **Crear**.
3. Siga las instrucciones del cuadro de diálogo **Crear grupo de recursos** para proporcionar un nombre y una descripción y agregar agregados como miembros al pool de recursos que desea crear.

Editar pools de recursos

Puede editar un pool de recursos existente cuando desee cambiar el nombre del pool de recursos y la descripción.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

El botón **Editar** sólo se activa cuando se selecciona un pool de recursos. Si se selecciona más de un pool de recursos, el botón **Editar** está desactivado.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Protección** > **agrupaciones de recursos**.
2. Seleccione un pool de recursos de la lista.
3. Haga clic en **Editar**.

   Aparecerá la ventana Editar pool de recursos.

4. Edite el nombre del pool de recursos y la descripción según sea necesario.
5. Haga clic en **Guardar**.

   El nuevo nombre y la descripción se muestran en la lista del pool de recursos.

Ver el inventario de pools de recursos

Es posible usar la página Resource Pools para ver el inventario del pool de recursos y supervisar la capacidad restante de cada pool de recursos.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Paso

1. En el panel de navegación izquierdo, haga clic en **Protección** > **agrupaciones de recursos**.

   Se mostrará el inventario del pool de recursos.

Agregar miembros del pool de recursos

Un pool de recursos consta de un número de agregados miembros. Puede añadir agregados a pools de recursos existentes para aumentar la cantidad de espacio disponible para el aprovisionamiento de volúmenes secundarios.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

No puede añadir más de 200 agregados a un pool de recursos a la vez. Los agregados que se muestran en el cuadro de diálogo agregados no pertenecen a ningún otro pool de recursos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Protección** > **agrupaciones de recursos**.
2. Seleccione un pool de recursos de la lista **Pools de recursos**.

   Los miembros del pool de recursos se muestran en el área situada debajo de la lista del pool de recursos.

3. En el área miembro del pool de recursos, haga clic en **Agregar**.

   Aparecerá el cuadro de diálogo Aggregates.

4. Seleccione uno o varios agregados.
5. Haga clic en **Agregar**.

   El cuadro de diálogo se cierra y los agregados se muestran en la lista de miembros del conjunto de recursos seleccionado.

Eliminación de agregados de pools de recursos

Es posible quitar agregados de un pool de recursos existente: Por ejemplo, cuando se desea usar un agregado con otro fin.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Los miembros del pool de recursos solo se muestran cuando se selecciona un pool de recursos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Protección** > **agrupaciones de recursos**.
2. Seleccione el pool de recursos del que desea quitar agregados miembros.

   La lista de agregados de miembros se muestra en el panel Miembros.

3. Seleccione uno o varios agregados.

   El botón **Quitar** está activado.

4. Haga clic en **Quitar.**

   Aparecerá un cuadro de diálogo de advertencia.

5. Haga clic en **Sí** para continuar.

   Los agregados seleccionados se eliminan del panel Miembros.

Eliminación de pools de recursos

Es posible eliminar pools de recursos cuando ya no son necesarios. Por ejemplo, es posible que desee redistribuir los agregados miembros de un pool de recursos a otros grupos de recursos, de modo que el pool de recursos original quede obsoleto.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

El botón **Eliminar** sólo está habilitado cuando se selecciona al menos un conjunto de recursos.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Protección** > **agrupaciones de recursos**.
2. Seleccione el pool de recursos que desea eliminar.
3. Haga clic en **Eliminar**.

   El pool de recursos se elimina de la lista del pool de recursos y sus agregados se quitan de la lista de miembros.

Supervisar las relaciones de protección de recuperación ante desastres de las máquinas virtuales de almacenamiento

Active IQ Unified Manager admite la supervisión de las relaciones de recuperación ante desastres de máquinas virtuales de almacenamiento, lo que proporciona recuperación ante desastres a la granularidad de un nivel de equipo virtual de almacenamiento. La recuperación ante desastres del equipo virtual de almacenamiento permite la recuperación de los datos presentes en los volúmenes constituyentes del equipo virtual de almacenamiento y la recuperación de la configuración del equipo virtual de almacenamiento.

Se crea una relación de recuperación ante desastres de una máquina virtual de almacenamiento a partir de la máquina virtual de almacenamiento de origen, hasta la máquina virtual de almacenamiento de destino, con el fin de proporcionar una recuperación ante desastres asíncrona. Puede seleccionar si desea replicar toda la configuración del equipo virtual de almacenamiento o un subconjunto de ella (excepto la configuración de la red y del protocolo) junto con los volúmenes de datos en función de la configuración del clúster.

Una vez configurada la relación de recuperación ante desastres de la máquina virtual de almacenamiento de origen, cuando la máquina virtual de almacenamiento de origen deja de estar disponible debido a un error de hardware o a un desastre en el entorno, se inicia la máquina virtual de almacenamiento de destino, lo que proporciona acceso a los datos con la menor interrupción. Del mismo modo, cuando la máquina virtual de almacenamiento de origen está disponible, se resincronizaba con la máquina virtual de almacenamiento de destino y, a continuación, el origen se reinicia para proporcionar los datos. Puede usar comandos de SnapMirror para configurar y gestionar las relaciones de recuperación ante desastres de máquinas virtuales de almacenamiento.

Supervisión de máquinas virtuales de almacenamiento mediante la página Relaciones

Las relaciones de recuperación ante desastres de las máquinas virtuales de almacenamiento se pueden supervisar desde la página Relationships de la sección

PROTECTION del INVENTARIO. De forma predeterminada, la página Relaciones muestra sólo las relaciones de nivel superior a medida que se aplica el filtro de relaciones constituyentes.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Puede utilizar filtros para ver las relaciones de recuperación ante desastres de las máquinas virtuales de almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **PROTECTION** > **Relationships**.

   La página muestra todo el tipo de relaciones: Volumen, grupo de coherencia y relaciones de máquina virtual de almacenamiento.

2. Haga clic en **filtro** y seleccione **Tipo de objeto de relación** y **Storage VM** para ver sólo las relaciones de recuperación ante desastres de Storage VM.
3. Haga clic en **aplicar filtro**.

   Debe borrar el filtro de relaciones constituyentes para ver todas las relaciones de protección.

   La página muestra solo las relaciones de recuperación ante desastres de la máquina virtual de almacenamiento.

Ver las relaciones de protección en la página Storage VMs

Mediante la página Storage VMs, puede ver el estado de las relaciones de recuperación ante desastres de los equipos virtuales de almacenamiento existentes.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

También puede examinar los detalles de las relaciones de protección, incluidos el estado de transferencia y desfase, los detalles de origen y destino. Puede programar informes o descargar informes existentes en el formato que necesite. El botón **Mostrar/Ocultar** permite agregar las columnas necesarias a los informes, ya que no se muestran de forma predeterminada.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **STORAGE** > **Storage VMs**.
2. En el menú **VER**, seleccione **relación** > **todas las relaciones**.

   La relación: Se muestra una vista de todas las relaciones con todas las máquinas virtuales de almacenamiento configuradas.

Ver las máquinas virtuales de almacenamiento en función del estado de protección

Puede usar la página Storage VMs del inventario para ver todas las máquinas virtuales

de almacenamiento en Active IQ Unified Manager y filtrar las máquinas virtuales de almacenamiento en función de su estado de protección.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Se añade un nuevo rol de protección de columnas a la vista de máquinas virtuales de almacenamiento que proporciona información sobre si la máquina virtual de almacenamiento está protegida o sin protección.

Si un clúster de origen no se añade a Active IQ Unified Manager, en los grids toda la información relacionada con ese clúster no estará disponible.

Pasos

1. En el panel de navegación de la izquierda, haga clic en **STORAGE** > **Storage VMs**.
2. En el menú **VIEW**, seleccione **Health** > **All Storage VMs**.

   Se muestra el estado: Todas las máquinas virtuales de almacenamiento.

3. Haga clic en **filtro** para ver uno de los siguientes equipos virtuales de almacenamiento.

Para ver	Valor de filtro
VMs de almacenamiento protegido	**La función de protección** está **protegida**
VMs de almacenamiento sin protección	**La función de protección** está **desprotegida**

   No se pueden ver las máquinas virtuales de almacenamiento protegidas y sin protección al mismo tiempo. Deberá borrar el filtro existente para volver a aplicar una nueva opción de filtro.

4. Haga clic en **aplicar filtro**.

   La vista sin guardar muestra todas las máquinas virtuales de almacenamiento protegidas o desprotegidas por la recuperación ante desastres de las máquinas virtuales de almacenamiento en función de las selecciones de filtro.

Asociaciones de máquinas virtuales de almacenamiento

Las asociaciones de máquinas virtuales de almacenamiento (máquinas virtuales de almacenamiento) son asignaciones de una máquina virtual de almacenamiento de origen a una máquina virtual de almacenamiento de destino que utilizan las aplicaciones asociadas para la selección de recursos y el aprovisionamiento de volúmenes secundarios.

Las asociaciones se crean entre una máquina virtual de almacenamiento de origen y una máquina virtual de almacenamiento de destino, independientemente de si la máquina virtual de almacenamiento de destino es un destino secundario o un destino terciario. No se puede usar una máquina virtual de almacenamiento de destino secundario como origen para crear una asociación con una máquina virtual de almacenamiento de destino terciario.

Como administrador de aplicaciones o administrador de almacenamiento, puede ver las asociaciones de VM de almacenamiento en su entorno en la página **Protección** > **Asociaciones de VM de almacenamiento**.

Puede asociar SVM de tres maneras:

- **Asociar cualquier VM de almacenamiento**: Puede crear una asociación entre cualquier VM de almacenamiento de origen primario y una o más SVM de destino. Esto significa que todas las SVM existentes que actualmente requieren protección, así como las SVM que se creen en el futuro, están asociadas con las SVM de destino especificadas. Por ejemplo, puede que desee que se realice el backup de aplicaciones de varios orígenes distintos en ubicaciones en una o varias SVM de destino en una misma ubicación.
- **Asociar una VM de almacenamiento particular**: Puede crear una asociación entre una VM de almacenamiento de origen específica y una o más SVM de destino específicas. Por ejemplo, si proporciona servicios de almacenamiento a muchos clientes cuyos datos deben estar separados entre sí, puede elegir esta opción para asociar una máquina virtual de almacenamiento de origen específica a una máquina virtual de almacenamiento de destino específica que esté asignada únicamente a ese cliente.
- **Asociar con una VM de almacenamiento externo**: Puede crear una asociación entre una VM de almacenamiento de origen y un volumen flexible externo de una VM de almacenamiento de destino.

Crear asociaciones de máquinas virtuales de almacenamiento

El asistente Create Storage Virtual Machine Associations permite que las aplicaciones de protección de partners asocien una máquina virtual de almacenamiento de origen con una máquina virtual de almacenamiento de destino para usarla con las relaciones de SnapMirror y SnapVault. Las aplicaciones de partners utilizan estas asociaciones en el momento del aprovisionamiento inicial de volúmenes de destino para determinar los recursos que se deben seleccionar.dd

Lo que necesitará

- La máquina virtual de almacenamiento que está asociando ya debe existir.
- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Para cualquier tipo de relación y máquina virtual de almacenamiento de origen, solo se puede seleccionar una máquina virtual de almacenamiento de destino en cada clúster de destino.

Cambiar asociaciones utilizando las funciones DELETE y CREATE sólo afecta a las operaciones de aprovisionamiento futuras. No mueve volúmenes de destino existentes.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Protección** > **Storage VM Associations**.
2. En la página **Storage VM Associations**, haga clic en **Crear**.

   Se inicia el asistente **Crear asociaciones de máquinas virtuales de almacenamiento**.

3. Seleccione una de las siguientes fuentes:
   - **Cualquiera**

     Seleccione esta opción si desea crear una asociación entre cualquier origen de máquina virtual de almacenamiento primario a una o varias máquinas virtuales de almacenamiento de destino. Esto significa que todos los equipos virtuales de almacenamiento existentes que actualmente requieren protección, así como todos los equipos virtuales de almacenamiento que se creen en el futuro, están asociados con el equipo virtual de almacenamiento de destino especificado. Por ejemplo, puede ser

conveniente que se lanzaran backups de aplicaciones de varios orígenes distintos en ubicaciones en una o varias máquinas virtuales de almacenamiento de destino en una misma ubicación.

- **Individual**

  Elija esta opción si desea seleccionar una máquina virtual de almacenamiento de origen específica asociada con una o varias máquina virtual de almacenamiento de destino. Por ejemplo, si proporciona servicios de almacenamiento a muchos clientes cuyos datos deben estar separados entre sí, elija esta opción para asociar un origen específico de las máquinas virtuales de almacenamiento a un destino específico de máquinas virtuales de almacenamiento que se asigne solo a ese cliente.

- **Ninguna (externa)**

  Seleccione esta opción si desea crear una asociación entre una máquina virtual de almacenamiento de origen y un volumen flexible externo de una máquina virtual de almacenamiento de destino.

4. Seleccione el tipo de relación de protección que desea crear o los dos:
   - **SnapMirror**
   - **SnapVault**
5. Haga clic en **Siguiente**.
6. Seleccione uno o varios destinos de protección para máquinas virtuales de almacenamiento.
7. Haga clic en **Finalizar**.

Eliminar asociaciones de máquinas virtuales de almacenamiento

Es posible eliminar las asociaciones de máquinas virtuales de almacenamiento para aplicaciones asociadas a fin de eliminar la relación de aprovisionamiento secundaria entre la máquina virtual de almacenamiento de origen y de destino; por ejemplo, puede hacerlo cuando la máquina virtual de almacenamiento de destino esté llena y desea crear una nueva asociación de protección de máquinas virtuales de almacenamiento.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

El botón **Eliminar** se desactiva hasta que se selecciona al menos una asociación de VM de almacenamiento. Cambiar las asociaciones que utilizan las funciones de eliminación y creación afecta solo a las operaciones de aprovisionamiento futuras; no mueve los volúmenes de destino existentes.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Protección** > **Storage VM Associations**.
2. Seleccione al menos una asociación de máquina virtual de almacenamiento.

   El botón **Eliminar** está activado.

3. Haga clic en **Eliminar.**

   Aparecerá un cuadro de diálogo de advertencia.

4. Haga clic en **Sí** para continuar.

   La asociación de máquina virtual de almacenamiento seleccionada se elimina de la lista.

Requisitos de SVM y pool de recursos para dar soporte a servicios de almacenamiento

Puede garantizar mejor que se cumplan las aplicaciones asociadas si observa algunos requisitos de asociación SVM y de pool de recursos específicos de los servicios de almacenamiento: Por ejemplo, cuando asocia una SVM y crea pools de recursos en Unified Manager para admitir una topología de protección en un servicio de almacenamiento proporcionado por una aplicación de partner.

Algunas aplicaciones se asocian con el servidor de Unified Manager para proporcionar servicios que configuran y ejecutan automáticamente la protección de backup de SnapMirror o SnapVault entre los volúmenes de origen y los volúmenes de protección en ubicaciones secundarias o terciarias. Para admitir estos servicios de almacenamiento de protección, debe utilizar Unified Manager para configurar las asociaciones de SVM y los pools de recursos necesarios.

Para admitir la protección de un único salto de servicio de almacenamiento o en cascada, incluida la replicación desde un volumen primario de SnapMirror de origen o SnapVault a volúmenes de backup de destino SnapMirror o a SnapVault que residen en ubicaciones secundarias o terciarias, siga los siguientes requisitos:

- Las asociaciones de SVM deben configurarse entre la SVM que contiene el volumen primario de SnapMirror o SnapVault y cualquier SVM en la que resida un volumen secundario o un volumen terciario.
  - Por ejemplo, para admitir una topología de protección en la que el volumen de origen reside Vol_A en SVM_1, y el volumen de destino secundario de SnapMirror reside Vol_B en SVM_2, Y el volumen de backup terciario de SnapVault Vol_ C reside en SVM_3, debe usar la interfaz de usuario web de Unified Manager para configurar una asociación de SnapMirror entre SVM_1 y SVM_2, y una asociación de backup de SnapVault entre SVM_1 y SVM_3.

    En este ejemplo, no es necesaria ninguna asociación de SnapMirror o asociación de backup de SnapVault entre SVM_2 y SVM_3, y no se utiliza.

  - Para admitir una topología de protección en la que residen el volumen de origen Vol_A y el volumen de destino de SnapMirror Vol_B en SVM_1, debe configurar una asociación de SnapMirror entre SVM_1 y SVM_1.
- Los pools de recursos deben incluir recursos del agregado del clúster disponibles para las SVM asociadas.

  Puede configurar los pools de recursos mediante la interfaz de usuario web de Unified Manager y, posteriormente, asignar mediante la aplicación para partners los nodos de destino secundario y de destino terciario del servicio de almacenamiento.

Qué trabajos son

Un trabajo es una serie de tareas que se pueden supervisar con Unified Manager. La visualización de trabajos y sus tareas asociadas permite determinar si los trabajos se completaron correctamente.

Los trabajos se inician cuando se crean relaciones de SnapMirror y SnapVault, al realizar cualquier operación de relación (break, editar, poner en modo inactivo, eliminar, reanudar, resincronizar y resincronización inversa), cuando realiza tareas de restauración de datos, cuando inicia sesión en un clúster, etc.

Al iniciar un trabajo, es posible usar la página Jobs y la página de detalles Job para supervisar el trabajo y el progreso de las tareas asociadas.

Supervisar trabajos de

Puede utilizar la página Jobs para supervisar el estado del trabajo y ver propiedades del trabajo, como el tipo de servicio de almacenamiento, el estado, la hora de envío y la hora de finalización, a fin de determinar si un trabajo se ha completado correctamente o no.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Protección** > **trabajos**.

   Aparece la página Jobs.

2. Consulte la columna **Estado** para determinar el estado de los trabajos que se están ejecutando actualmente.
3. Haga clic en un nombre de trabajo para ver los detalles de ese trabajo en particular.

   Aparece la página de detalles Job.

Ver los detalles del trabajo

Después de iniciar un trabajo, puede realizar un seguimiento de su progreso desde la página de detalles Job y supervisar las tareas asociadas para detectar posibles errores.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Protección** > **trabajos**.
2. En la página Jobs, haga clic en un nombre de trabajo en la columna **Name** para mostrar la lista de tareas asociadas al trabajo.
3. Haga clic en una tarea para mostrar información adicional en el panel **Detalles de la tarea** y en el panel **mensajes de la tarea** situado a la derecha de la lista de tareas.

Anulación de trabajos

Puede utilizar la página trabajos para cancelar un trabajo si tarda demasiado en finalizarlo, si encuentra demasiados errores o si ya no es necesario. Sólo puede cancelar un trabajo si su estado y el tipo permitir. Puede anular cualquier trabajo en ejecución.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Protección** > **trabajos**.
2. En la lista de trabajos, seleccione un trabajo y, a continuación, haga clic en **Anular**.
3. En el mensaje de confirmación, haga clic en **Sí** para anular el trabajo seleccionado.

Volver a intentar un trabajo de protección con errores

Después de haber tomado medidas para corregir un trabajo de protección fallido, puede utilizar **Reintentar** para volver a ejecutar el trabajo. Al volver a intentar un trabajo, se crea un trabajo nuevo con el ID de trabajo original.

Lo que necesitará

Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Solo se puede volver a intentar un trabajo fallido a la vez. Al seleccionar más de un trabajo, se desactiva el botón **Reintentar**. Solo se pueden volver a intentar los trabajos del tipo Configuración de protección y operación de relación de protección.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Protección** > **trabajos**.
2. En la lista de trabajos, seleccione un solo trabajo de tipo Configuración de protección o operación de relación de protección que no se han podido completar.

   El botón **Reintentar** está activado.

3. Haga clic en **Reintentar**.

   Se reinicia el trabajo.

Descripción de las ventanas y cuadros de diálogo de relaciones de protección

Es posible ver y gestionar detalles relacionados con la protección, como pools de recursos, asociaciones de SVM y trabajos de protección. Puede usar la página umbrales de estado adecuados para configurar valores de umbral de estado global para agregados, volúmenes y relaciones.

Página Resource Pools

La página Resource Pools muestra los pools de recursos existentes y sus miembros, y permite crear, supervisar y gestionar pools de recursos para fines de aprovisionamiento.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Crear**

  Abre el cuadro de diálogo Crear pool de recursos, que se puede utilizar para crear pools de recursos.

- **Edición**

  Permite editar el nombre y la descripción de los pools de recursos que se crean.

- **Eliminar**

  Permite eliminar uno o varios pools de recursos.

Lista de pools de recursos

La lista Pools de recursos muestra (en formato de tabla) las propiedades de los pools de recursos existentes.

- **Piscina de recursos**

  Muestra el nombre del conjunto de recursos.

- **Descripción**

  Describe el pool de recursos.

- **Tipo de SnapLock**

  Muestra el tipo de SnapLock que utilizan los agregados del pool de recursos. Los valores válidos para el tipo de SnapLock son Compliance, Enterprise y Non-SnapLock. Un pool de recursos solo puede contener agregados de un tipo SnapLock.

- **Capacidad total**

  Muestra la capacidad total (en MB, GB, etc.) del pool de recursos.

- **Capacidad usada**

  Muestra la cantidad de espacio (en MB, GB, etc.) que se utiliza en el pool de recursos.

- **Capacidad disponible**

  Muestra la cantidad de espacio (en MB, GB, etc.) disponible en el pool de recursos.

- **% Utilizado**

  Muestra el porcentaje de espacio que se utiliza en el pool de recursos.

Botones de comando de lista de miembros

Los botones de comando de la lista Miembros le permiten realizar las siguientes tareas:

- **Agregar**

  Permite añadir miembros al pool de recursos.

- **Eliminar**

  Permite eliminar uno o varios miembros del conjunto de recursos.

Lista de miembros

La lista Miembros muestra (en formato tabular) los miembros del pool de recursos y sus propiedades cuando se selecciona un pool de recursos.

- **Estado**

  Muestra el estado actual del agregado miembro. El estado puede ser crítico ( ), error ( ), Advertencia ( ), o normal ( ).

- **Nombre agregado**

  Muestra el nombre del agregado miembro.

- **Estado**

  Muestra el estado actual del agregado, que puede ser uno de los siguientes:

  - Sin conexión

    No se permite el acceso de lectura ni escritura.

  - En línea

    Se permite el acceso de lectura y escritura a los volúmenes alojados en este agregado.

  - Restringida

    Se permiten operaciones limitadas (como la reconstrucción de paridad), pero no se permite el acceso a los datos.

  - Creando

    Se está creando el agregado.

  - Destruyendo

    El agregado se está destruyendo.

  - Error

    El agregado no se puede conectar.

  - Congelado

    El agregado no está sirviendo solicitudes (temporalmente).

  - Incoherente

    El agregado se ha marcado como dañado, por lo que debe ponerse en contacto con el soporte técnico.

  - Plancha restringida

    No se pueden ejecutar herramientas de diagnóstico en el agregado.

- Montaje

  El agregado está en proceso de montaje.

- Parcial

  Se encontró al menos un disco para el agregado, pero faltan dos o más discos.

- Ralentización

  El agregado se está poniendo en modo inactivo.

- En modo inactivo

  El agregado se detiene.

- Revertido

  Se ha completado la reversión de un agregado.

- Desmontada

  El agregado se ha desmontado.

- Desmontaje

  El agregado se está desconectando.

- Desconocido

  Se detecta el agregado, pero el servidor de Unified Manager aún no ha recuperado la información de agregado.

De forma predeterminada, esta columna está oculta.

- **Cluster**

  Muestra el nombre del clúster al que pertenece el agregado.

- **Nodo**

  Muestra el nombre del nodo en el que reside el agregado.

- **Capacidad total**

  Muestra la capacidad total (en MB, GB, etc.) del agregado.

- **Capacidad usada**

  Muestra la cantidad de espacio (en MB, GB, etc.) que se usa en el agregado.

- **Capacidad disponible**

  Muestra la cantidad de espacio (en MB, GB, etc.) disponible en el agregado.

- **% Utilizado**

Muestra el porcentaje de espacio que se usa en el agregado.

- **Tipo de disco**

  Muestra el tipo de configuración de RAID, que puede ser uno de los siguientes:

  - RAID0: Todos los grupos RAID son de tipo RAID0.
  - RAID4: Todos los grupos RAID son del tipo RAID4.
  - RAID-DP: Todos los grupos RAID son del tipo RAID-DP.
  - RAID-TEC: Todos los grupos RAID son del tipo RAID-TEC.
  - RAID mixto: El agregado contiene grupos RAID de distintos tipos de RAID (RAID0, RAID4, RAID-DP y RAID-TEC). De forma predeterminada, esta columna está oculta.

Cuadro de diálogo Create Resource Pool

Puede usar el cuadro de diálogo Crear pool de recursos para asignar un nombre y describir un nuevo pool de recursos, así como para añadir y eliminar agregados de ese pool de recursos.

Nombre del pool de recursos

Los cuadros de texto permiten agregar la siguiente información para crear un conjunto de recursos:

Permite especificar un nombre de pool de recursos.

Descripción

Permite describir un conjunto de recursos.

Miembros

Muestra los miembros del conjunto de recursos. También puede agregar y eliminar miembros.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Agregar**

  Abre el cuadro de diálogo agregados para que pueda añadir agregados desde un clúster específico al pool de recursos. Es posible añadir agregados desde clústeres de diferentes, pero no es posible añadir los mismos agregados a más de un pool de recursos.

- **Eliminar**

  Permite quitar agregados seleccionados del pool de recursos.

- **Crear**

  Crea el pool de recursos. Este botón no está habilitado hasta que se haya introducido información en los campos Nombre del grupo de recursos o Descripción.

- **Cancelar**

Descarta los cambios y cierra el cuadro de diálogo Crear grupo de recursos.

Cuadro de diálogo Edit Resource Pool

Puede utilizar el cuadro de diálogo Editar pool de recursos para cambiar el nombre y la descripción de un pool de recursos existente. Por ejemplo, si el nombre y la descripción originales no son precisos o son incorrectos, puede cambiarlos para que sean más precisos.

Cuadros de texto

Los cuadros de texto permiten cambiar la siguiente información para el conjunto de recursos seleccionado:

- **Nombre del grupo de recursos**

  Permite introducir un nombre nuevo.

- **Descripción**

  Permite introducir una nueva descripción.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Guardar**

  Guarda los cambios en el nombre y la descripción del pool de recursos.

- **Cancelar**

  Descarta los cambios y cierra el cuadro de diálogo Editar grupo de recursos.

Cuadro de diálogo Aggregates

Puede utilizar el cuadro de diálogo Aggregates para seleccionar los agregados que desea agregar al pool de recursos.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Agregar**

  Añade los agregados seleccionados al pool de recursos. El botón Agregar no está activado hasta que se seleccione al menos un agregado.

- **Cancelar**

  Descarta los cambios y cierra el cuadro de diálogo agregados.

Lista Aggregates

La lista Aggregates muestra (en formato de tabla) los nombres y las propiedades de los agregados supervisados.

- **Estado**

  Muestra el estado actual de un volumen. El estado puede ser crítico ( ), error ( ), Advertencia ( ), o normal ( ).

  Es posible mover el puntero sobre el estado para ver más información sobre el evento o los eventos que se generan para el volumen.

- **Nombre agregado**

  Muestra el nombre del agregado.

- **Estado**

  Muestra el estado actual del agregado, que puede ser uno de los siguientes:

  - Sin conexión

    No se permite el acceso de lectura ni escritura.

  - Restringida

    Se permiten operaciones limitadas (como la reconstrucción de paridad), pero no se permite el acceso a los datos.

  - En línea

    Se permite el acceso de lectura y escritura a los volúmenes alojados en este agregado.

  - Creando

    Se está creando el agregado.

  - Destruyendo

    El agregado se está destruyendo.

  - Error

    El agregado no se puede conectar.

  - Congelado

    El agregado no está sirviendo solicitudes (temporalmente).

  - Incoherente

    El agregado se ha marcado como dañado, por lo que debe ponerse en contacto con el soporte técnico.

  - Plancha restringida

No se pueden ejecutar herramientas de diagnóstico en el agregado.

- Montaje

  El agregado está en proceso de montaje.

- Parcial

  Se encontró al menos un disco para el agregado, pero faltan dos o más discos.

- Ralentización

  El agregado se está poniendo en modo inactivo.

- En modo inactivo

  El agregado se detiene.

- Revertido

  Se ha completado la reversión de un agregado.

- Desmontada

  El agregado está sin conexión.

- Desmontaje

  El agregado se está desconectando.

- Desconocido

  Se detecta el agregado, pero el servidor de Unified Manager aún no ha recuperado la información de agregado.

- **Cluster**

  Muestra el nombre del clúster en el que reside el agregado.

- **Nodo**

  Muestra el nombre de la controladora de almacenamiento que contiene el agregado.

- **Capacidad total**

  Muestra el tamaño total de datos (en MB, GB, etc.) del agregado. De forma predeterminada, esta columna está oculta.

- **Capacidad comprometida**

  Muestra el espacio total (en MB, GB, etc.) asignado a todos los volúmenes del agregado. De forma predeterminada, esta columna está oculta.

- **Capacidad usada**

  Muestra la cantidad de espacio (en MB, GB, etc.) que se usa en el agregado.

- **Capacidad disponible**

  Muestra la cantidad de espacio (en MB, GB, etc.) disponible para los datos del agregado. De forma predeterminada, esta columna está oculta.

- **Disponible %**

  Muestra el porcentaje de espacio disponible para los datos del agregado. De forma predeterminada, esta columna está oculta.

- **% Utilizado**

  Muestra el porcentaje de espacio que utilizan los datos en el agregado.

- **Tipo RAID**

  Muestra el tipo de RAID del volumen seleccionado. El tipo de RAID puede ser RAID0, RAID4, RAID-DP, RAID-TEC o RAID mixto.

Trabajos

La página Jobs permite ver el estado actual y otra información acerca de todos los trabajos de protección de aplicaciones asociadas que se están ejecutando en ese momento, así como los trabajos que se completaron. Puede utilizar esta información para ver qué trabajos aún se están ejecutando y si un trabajo se ha realizado correctamente o ha fallado.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Abort**

  Anula el trabajo seleccionado. Esta opción sólo está disponible si el trabajo seleccionado se está ejecutando.

- **Reintentar**

  Reinicia un trabajo fallido de tipo Configuración de protección o operación de relación de protección. Solo se puede volver a intentar un trabajo fallido a la vez. Si se selecciona más de un trabajo fallido, el botón **Reintentar** está desactivado. No se pueden volver a intentar los trabajos de servicio de almacenamiento con errores.

- **Actualizar**

  Actualiza la lista de trabajos y la información asociada a ellos.

Lista trabajos

La lista trabajos muestra, en una tabla de resultados, una lista de los trabajos en curso. De forma predeterminada, la lista muestra sólo los trabajos generados durante la semana pasada. Puede utilizar la ordenación y el filtrado de columnas para personalizar qué trabajos se muestran.

- **Estado**

  Muestra el estado actual de un trabajo. El estado puede ser error (⚠️) O normal (✅).

- **ID de trabajo**

  Muestra el número de identificación del trabajo. De forma predeterminada, esta columna está oculta.

  El número de identificación del trabajo es único y el servidor lo asigna cuando inicia el trabajo. Puede buscar un trabajo concreto introduciendo el número de identificación del trabajo en el cuadro de texto proporcionado por el filtro de columna.

- **Nombre**

  Muestra el nombre del trabajo.

- **Tipo**

  Muestra el tipo de trabajo. Los tipos de trabajo son los siguientes:

  - **Adquisición de Cluster**

    Una tarea de Workflow Automation se está redetectando un clúster.

  - **Configuración de protección**

    Una tarea de protección está iniciando flujos de trabajo de Workflow Automation, como programaciones de cron, creación de políticas de SnapMirror, etc.

  - **Operación de relación de protección**

    Un trabajo de protección ejecuta operaciones de SnapMirror.

  - **Cadena de flujo de trabajo de protección**

    Una tarea de Workflow Automation está ejecutando varios flujos de trabajo.

  - **Restaurar**

    Hay un trabajo de restauración en ejecución.

  - **Limpieza**

    El trabajo está limpiando los artefactos del miembro del servicio de almacenamiento que ya no son necesarios para fines de restauración.

  - **Conforme**

    El trabajo consiste en comprobar la configuración de los miembros del servicio de almacenamiento para garantizar que cumplen sus necesidades.

  - **Destruir**

    El trabajo está destruyendo un servicio de almacenamiento.

  - **Importar**

El trabajo está importando objetos de almacenamiento no gestionados a un servicio de almacenamiento existente.

- **Modificar**

  El trabajo está modificando los atributos de un servicio de almacenamiento existente.

- **Suscribirse**

  El trabajo está suscribiendo miembros a un servicio de almacenamiento.

- **Darse de baja**

  El trabajo está anulando la suscripción a los miembros de un servicio de almacenamiento.

- **Actualizar**

  Se está ejecutando un trabajo de actualización de protección.

- **Configuración de WFA**

  Un trabajo de Workflow Automation está presionando las credenciales del clúster y sincronizando las cachés de la base de datos.

- **Estado**

  Muestra el estado en ejecución del trabajo. Las opciones de estado son las siguientes:

  - **Anulado**

    El trabajo se ha anulado.

  - **Aborto**

    El trabajo está en proceso de anulación.

  - **Completado**

    El trabajo ha finalizado.

  - **En funcionamiento**

    El trabajo se está ejecutando.

- **Tiempo de envío**

  Muestra la hora a la que se envió el trabajo.

- **Duración**

  Muestra la cantidad de tiempo que el trabajo ha tardado en completarse. Esta columna se muestra de forma predeterminada.

- **Tiempo de finalización**

  Muestra la hora a la que finalizó el trabajo. De forma predeterminada, esta columna está oculta.

Página de detalles Job

La página de detalles Job permite ver el estado y otra información sobre tareas de trabajos de protección específicas en ejecución, que se encuentran en cola o que han finalizado. Es posible usar esta información para supervisar el progreso del trabajo de protección y solucionar problemas de fallos de trabajos.

Resumen de tareas

El resumen de trabajos muestra la siguiente información:

- ID de trabajo
- Tipo
- Estado
- Hora de envío
- Tiempo de finalización
- Duración

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Actualizar**

  Actualiza la lista de tareas y las propiedades asociadas a cada tarea.

- **Ver trabajos**

  Regresa a la página Jobs.

Lista de tareas de trabajo

La lista tareas de trabajo muestra en una tabla todas las tareas asociadas a un trabajo específico y las propiedades relacionadas con cada tarea.

- **Tiempo de inicio**

  Muestra el día y la hora en que se inició la tarea. De forma predeterminada, las tareas más recientes se muestran en la parte superior de la columna y las tareas más antiguas se muestran en la parte inferior.

- **Tipo**

  Muestra el tipo de tarea.

- **Estado**

  El estado de una tarea en particular:

  - **Completado**

    La tarea ha finalizado.

- **En cola**

  La tarea está a punto de ejecutarse.

- **En funcionamiento**

  La tarea está en ejecución.

- **Esperando**

  Se ha enviado un trabajo y algunas tareas asociadas están esperando a que se pongan en cola y se ejecuten.

- **Estado**

  Muestra el estado de la tarea:

  - **Error ( )**

    Error de tarea.

  - **Normal ( )**

    La tarea se ha realizado correctamente.

  - **Omitida ( )**

    Error en una tarea, por lo que se omitirán tareas posteriores.

- **Duración**

  Muestra el tiempo transcurrido desde que comenzó la tarea.

- **Tiempo de finalización**

  Muestra el tiempo que ha finalizado la tarea. De forma predeterminada, esta columna está oculta.

- **ID de tarea**

  Muestra el GUID que identifica una tarea individual para un trabajo. La columna se puede ordenar y filtrar. De forma predeterminada, esta columna está oculta.

- **Orden de dependencia**

  Muestra un entero que representa la secuencia de tareas de un gráfico, con cero asignado a la primera tarea. De forma predeterminada, esta columna está oculta.

- **Panel de detalles de tareas**

  Muestra información adicional acerca de cada tarea de trabajo, incluido el nombre de la tarea, la descripción de la tarea y, si la tarea no se realizó correctamente, un motivo del error.

- **Panel de mensajes de tarea**

  Muestra mensajes específicos de la tarea seleccionada. Los mensajes pueden incluir un motivo para el error y sugerencias para resolverlo. No todas las tareas muestran mensajes de tareas.

Cuadro de diálogo Advanced Secondary Settings

Puede utilizar el cuadro de diálogo Advanced Secondary Settings para habilitar la replicación con flexibilidad de versiones, backup de varias copias y configuración relacionada con el espacio en un volumen secundario. Puede usar el cuadro de diálogo Configuración secundaria avanzada si desea cambiar la opción Habilitar o deshabilitar la configuración actual.

La configuración relacionada con el espacio maximiza la cantidad de datos que se están almacenando, lo que incluye lo siguiente: Deduplicación, compresión de datos, crecimiento automático y garantía de espacio.

El cuadro de diálogo incluye los siguientes campos:

- **Activar la replicación de versión flexible**

  Permite utilizar SnapMirror con una replicación de versión flexible. La replicación flexible con la versión permite la protección de SnapMirror de un volumen de origen aunque el volumen de destino se ejecute con una versión anterior de ONTAP que el del volumen de origen.

  - Habilite Backup

    Si la replicación de versión flexible está activada, también permite transferir y conservar varias copias snapshot de los datos de origen de SnapMirror en el destino de SnapMirror.

- **Activar deduplicación**

  Permite la deduplicación en el volumen secundario en una relación con SnapVault, de modo que se eliminan los bloques de datos duplicados para obtener ahorros de espacio. Puede utilizar la deduplicación cuando el ahorro de espacio sea del 10 % como mínimo y cuando la tasa de sobrescritura de datos no sea rápida. La deduplicación se utiliza a menudo para entornos virtualizados, recursos compartidos de archivos y datos de backup. Esta configuración está deshabilitada de forma predeterminada. Cuando se habilita esta opción, se inicia esta operación después de cada transferencia.

  - Habilite la compresión

    Permite una compresión de datos transparente. Puede utilizar la compresión cuando el ahorro de espacio sea del 10 % como mínimo, cuando la sobrecarga potencial sea aceptable y cuando haya suficientes recursos del sistema para que la compresión se complete durante las horas en las que no son pico. En una relación de SnapVault, esta configuración está deshabilitada de manera predeterminada. La compresión solo está disponible cuando se selecciona la deduplicación.

  - Comprima en línea

    Permite un ahorro de espacio inmediato al comprimir los datos antes de escribirlos en el disco. Puede utilizar la compresión en línea cuando su sistema no tenga un uso superior al 50 % durante las horas de máximo actividad y cuando el sistema pueda acomodar nuevas escrituras y CPU adicional durante las horas de mayor actividad. Este ajuste sólo está disponible si se selecciona "'Habilitar compresión'".

- **Activar auto-fila**

  Permite aumentar automáticamente el volumen de destino cuando el porcentaje de espacio libre está por debajo del umbral especificado, siempre que haya espacio disponible en el agregado asociado.

- **Tamaño máximo**

Establece el porcentaje máximo al que puede crecer un volumen. El valor predeterminado es un 20 % mayor que el tamaño del volumen de origen. Un volumen no crece automáticamente si el tamaño actual es mayor o igual que el porcentaje de crecimiento automático máximo. Este campo solo se habilita cuando se habilita la configuración de crecimiento automático.

- **Tamaño de incremento**

  Especifica el incremento de porcentaje según el cual el volumen crece automáticamente antes de alcanzar el porcentaje máximo del volumen de origen.

- **Garantía Espacial**

  Garantiza que se asigne espacio suficiente en el volumen secundario para que las transferencias de datos siempre tengan éxito. El ajuste de garantía de espacio puede ser uno de los siguientes:

  - Archivo
  - Volumen
  - Ninguno + por ejemplo, es posible que tenga un volumen de 200 GB que contenga archivos de un total de 50 GB; sin embargo, esos archivos contienen sólo 10 GB de datos. La garantía de volumen asigna 200 GB al volumen de destino, independientemente del contenido del origen. La garantía de archivo asigna 50 GB para asegurarse de que se reserva suficiente espacio para los archivos del origen; al seleccionar Ninguno en este escenario, sólo se asignan 10 GB en el destino para el espacio real utilizado por los datos de archivo en el origen.

  De manera predeterminada, la garantía de espacio se establece en volumen.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Aplicar**

  Guarda la configuración de eficiencia seleccionada y la aplica al hacer clic en **aplicar** en el cuadro de diálogo Configurar protección.

- **Cancelar**

  Descarta las selecciones y cierra el cuadro de diálogo Configuración avanzada de destino.

Cuadro de diálogo Advanced Destination Settings

Puede usar el cuadro de diálogo Advanced Destination Settings para habilitar la configuración de garantía de espacio en un volumen de destino. Puede seleccionar la configuración avanzada cuando la garantía de espacio está desactivada en el origen, pero desea que esté activada en el destino. La configuración de deduplicación, compresión y crecimiento automático en una relación de SnapMirror se hereda del volumen de origen y no se puede cambiar.

Garantía de espacio

Garantiza que se asigne espacio suficiente en el volumen de destino para que las transferencias de datos siempre tengan éxito. El ajuste de garantía de espacio puede ser uno de los siguientes:

- Archivo
- Volumen
- Ninguno

Por ejemplo, es posible que tenga un volumen de 200 GB que contenga archivos de un total de 50 GB; sin embargo, esos archivos contienen sólo 10 GB de datos. La garantía de volumen asigna 200 GB al volumen de destino, independientemente del contenido del origen. La garantía de archivo asigna 50 GB para asegurarse de que se reserva suficiente espacio para los archivos de origen en el destino; al seleccionar **Ninguno** en este escenario se asigna sólo 10 GB en el destino para el espacio real utilizado por los datos de archivo en el origen.

De manera predeterminada, la garantía de espacio se establece en volumen.

Restaurar

Puede utilizar el cuadro de diálogo Restore para restaurar datos a un volumen a partir de una copia Snapshot específica.

Restaurar desde

El área Restore from permite especificar el lugar donde desea restaurar datos.

- **Volumen**

  Especifica el volumen desde el cual desea restaurar datos. De forma predeterminada, se selecciona el volumen en el que inició la acción de restauración. Es posible seleccionar un volumen diferente de la lista desplegable que contiene todos los volúmenes con relaciones de protección al volumen en el que se inició la acción de restauración.

- **Copia snapshot**

  Especifica la copia Snapshot que desea usar para restaurar los datos. De forma predeterminada, se selecciona la copia de Snapshot más reciente. También puede seleccionar una copia Snapshot diferente de la lista desplegable. La lista de copias Snapshot cambia según qué volumen se selecciona.

- **Lista un máximo de 995 ficheros y directorios**

  De forma predeterminada, se muestra un máximo de 995 objetos en la lista. Puede anular la selección de esta casilla de comprobación si desea ver todos los objetos del volumen seleccionado. Esta operación puede tardar algún tiempo si el número de artículos es muy grande.

Seleccione los elementos que desea restaurar

El área Seleccionar elementos para restaurar permite seleccionar el volumen completo o los archivos y carpetas específicos que desea restaurar. Puede seleccionar un máximo de 10 archivos, carpetas o una combinación de ambos. Cuando se selecciona el número máximo de elementos, se desactivan las casillas de verificación selección de elementos.

- **Campo Ruta**

  Muestra la ruta a los datos que desea restaurar. Es posible desplazarse a la carpeta y los archivos que desea restaurar o escribir la ruta. Este campo está vacío hasta que seleccione o escriba una ruta. Haga clic en una vez que haya elegido una ruta de acceso, sube un nivel en la estructura de directorios.

- **Lista de carpetas y archivos**

  Muestra el contenido de la ruta introducida. De forma predeterminada, se muestra inicialmente la carpeta raíz. Al hacer clic en un nombre de carpeta se muestra el contenido de la carpeta.

Puede seleccionar elementos para restaurar de la siguiente manera:

- Cuando se introduce la ruta de acceso con un nombre de archivo determinado especificado en el campo de ruta, el archivo especificado se muestra en carpetas y archivos.
- Cuando se introduce una ruta de acceso sin especificar un archivo concreto, el contenido de la carpeta se muestra en la lista carpetas y archivos, y se pueden seleccionar hasta 10 archivos, carpetas o una combinación de ambos para restaurar.

  Si una carpeta contiene más de 995 elementos, aparece un mensaje para indicar que hay demasiados elementos que mostrar y si continúa con la operación se restauran todos los elementos de la carpeta especificada. Puede anular la selección de la casilla de verificación "'Listar máximo de 995 archivos y directorios'" si desea ver todos los objetos del volumen seleccionado.

No puede restaurar flujos de archivos NTFS.

Restaurar a.

El área Restore to permite especificar dónde desea restaurar los datos.

- **Ubicación original en Volume_Name**

  Restaura los datos seleccionados en el directorio del origen desde el que se realizó una copia de seguridad original de los datos.

- **Ubicación alternativa**

  Restaura los datos seleccionados en una ubicación nueva:

  - Ruta de restauración

    Especifica una ruta alternativa para restaurar los datos seleccionados. La ruta de acceso ya debe existir. Puede utilizar el botón **Browse** para desplazarse hasta la ubicación en la que desea restaurar los datos o puede introducir la ruta manualmente mediante el clúster de formato://svm/volume/path.

  - Conservar jerarquía de directorios

    Cuando esta opción está activada, conserva la estructura del archivo o directorio original. Por ejemplo, si el origen es /A/B/C/myfile.txt y el destino es /X/y/Z, Unified Manager restaura los datos mediante la siguiente estructura de directorio en el destino: /X/y/Z/A/B/C/myfile.txt.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Cancelar**

  Descarta las selecciones y cierra el cuadro de diálogo Restaurar.

- **Restaurar**

  Aplica las selecciones e inicia el proceso de restauración.

Cuadro de diálogo Browse Directories

Puede utilizar el cuadro de diálogo Browse Directories si desea restaurar los datos en un directorio de un clúster y una SVM que sea diferente del origen original. El clúster y el volumen de origen originales se seleccionan de forma predeterminada.

El cuadro de diálogo Browse Directories permite seleccionar el clúster, la SVM, el volumen y la ruta de directorio en la que se desean restaurar los datos.

- **Cluster**

  Enumera los destinos de clúster disponibles en los que puede restaurar. De forma predeterminada, se selecciona el clúster del volumen de origen original.

- **Lista desplegable de SVM**

  Muestra la SVM disponible para el clúster seleccionado. De forma predeterminada, se selecciona la SVM del volumen de origen original.

- **Volumen**

  Enumera todos los volúmenes de lectura/escritura en una SVM seleccionada. Es posible filtrar los volúmenes por nombre y por espacio disponible. El volumen con mayor espacio se enumera primero, y así sucesivamente, en orden descendente. De forma predeterminada, se selecciona el volumen de origen original.

- **Cuadro de texto Ruta de archivo**

  Permite escribir la ruta del archivo en el que desea restaurar los datos. La ruta introducida ya debe existir.

- **Nombre**

  Muestra los nombres de las carpetas disponibles para el volumen seleccionado. Al hacer clic en una carpeta de la lista Nombre se muestran las subcarpetas, si existen. Los archivos contenidos en las carpetas no se muestran. Haga clic en después de seleccionar una carpeta, sube un nivel en la estructura de directorios.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Seleccione Directorio**

  Aplica las selecciones y cierra el cuadro de diálogo Browse Directories. Si no hay ningún directorio seleccionado, este botón está desactivado.

- **Cancelar**

  Descarta las selecciones y cierra el cuadro de diálogo examinar directorios.

Cuadro de diálogo Configure Protection

Puede utilizar el cuadro de diálogo Configurar protección para crear relaciones de SnapMirror y SnapVault para todos los volúmenes de protección de datos de lectura, escritura y escritura en los clústeres a fin de garantizar que se repliquen los datos en un volumen de origen o un volumen primario.

Pestaña Source

- **Vista de topología**

  Muestra una representación visual de la relación que está creando. El origen de la topología se resalta de forma predeterminada.

- **Información de la fuente**

  Muestra detalles sobre los volúmenes de origen seleccionados, incluida la siguiente información:

  - Nombre del clúster de origen
  - Nombre de la SVM de origen
  - Tamaño total del volumen acumulativo

    Muestra el tamaño total de todos los volúmenes de origen seleccionados.

  - Tamaño acumulativo del volumen utilizado

    Muestra el tamaño acumulativo del volumen utilizado para todos los volúmenes de origen seleccionados.

  - Volumen de origen

    Muestra la siguiente información de una tabla:

    - Volumen de origen

      Muestra los nombres de los volúmenes de origen seleccionados.

    - Tipo

      Muestra el tipo de volumen.

    - Tipo de SnapLock

      Muestra el tipo de SnapLock del volumen. Las opciones son Compliance, Enterprise y Non-SnapLock.

    - Copia snapshot

      Muestra la copia Snapshot que se usa para la transferencia básica. Si el volumen de origen es de lectura/escritura, el valor predeterminado en la columna copia Snapshot indica que se crea una nueva copia Snapshot de forma predeterminada, y se usa para la transferencia básica. Si el volumen de origen es un volumen de protección de datos, el valor predeterminado en la columna copia Snapshot indica que no se crea ninguna copia Snapshot nueva y todas las copias Snapshot existentes se transfieren al destino. Al hacer clic en el valor de la copia Snapshot se muestra una

lista de copias Snapshot desde las que puede seleccionar una copia Snapshot existente para utilizarla en la transferencia básica. No se puede seleccionar una copia Snapshot predeterminada diferente si el tipo de origen es protección de datos.

Pestaña SnapMirror

Permite especificar un clúster de destino, una máquina virtual de almacenamiento (SVM) y un agregado para una relación de protección, así como una convención de nomenclatura para los destinos a la vez que se crea una relación de SnapMirror. También puede especificar una política y una programación de SnapMirror.

- **Vista de topología**

  Muestra una representación visual de la relación que está creando. El recurso de destino de SnapMirror en la topología se destaca de forma predeterminada.

- **Información de destino**

  Permite seleccionar los recursos de destino para una relación de protección:

  - Vínculo avanzado

    Inicia el cuadro de diálogo Advanced Destination Settings cuando se crea una relación de SnapMirror.

  - Clúster

    Enumera los clústeres que están disponibles como hosts de destino de protección. El campo es obligatorio

  - Máquina virtual de almacenamiento (SVM)

    Enumera las SVM que están disponibles en el clúster seleccionado. Debe seleccionar un clúster antes de completar la lista de SVM. El campo es obligatorio

  - Agregado

    Enumera los agregados que están disponibles en la SVM seleccionada. Debe seleccionarse un clúster antes de rellenar la lista de agregados. El campo es obligatorio En la lista de agregados se muestra la siguiente información:

    - Clasificación

      Cuando varios agregados satisfacen todos los requisitos de un destino, la clasificación indica la prioridad en la que se indica el agregado, según las siguientes condiciones:

      A. Se prefiere un agregado ubicado en un nodo diferente al nodo del volumen de origen para habilitar la separación de dominios de fallo.
      B. Se prefiere un agregado en un nodo con menos volúmenes para habilitar el equilibrio de carga entre nodos de un clúster.
      C. Se prefiere un agregado que tenga más espacio libre que otros agregados para habilitar el equilibrio de capacidad. Un rango de 1 significa que el agregado es el más preferido según los tres criterios.

    - Nombre del agregado

      Nombre del agregado

- Capacidad disponible
- Cantidad de espacio disponible en el agregado para los datos
- Conjunto de recursos

  Nombre del pool de recursos al que pertenece el agregado

◦ Convención de nomenclatura

Especifica la convención de nomenclatura predeterminada que se aplica al volumen de destino. Puede aceptar la convención de nomenclatura proporcionada o crear una personalizada. La convención de nomenclatura puede tener los siguientes atributos: %C, %M, %V y %N, donde %C es el nombre del clúster, %M es el nombre de SVM, %V es el volumen de origen y %N es el nombre del nodo de destino de topología.

El campo de convención de nomenclatura se resalta en rojo si la entrada no es válida. Al hacer clic en el vínculo «'Nombre de vista previa'», se muestra una vista previa de la convención de nomenclatura introducida y el texto de vista previa se actualiza dinámicamente a medida que se escribe una convención de nomenclatura en el campo de texto. Se agrega un sufijo entre 001 y 999 al nombre de destino cuando se crea la relación, reemplazando la nnn que aparece en el texto de vista previa, con 001 asignado primero, 002 en segundo asignado, etc.

- **Ajustes de relación**

Permite especificar la tasa de transferencia máxima, la política de SnapMirror y la programación que utiliza la relación de protección:

◦ Velocidad máxima de transferencia

Especifica la tasa máxima a la que se transfieren los datos entre los clústeres a través de la red. Si decide no utilizar una tasa de transferencia máxima, la transferencia de línea de base entre relaciones es ilimitada.

◦ Política de SnapMirror

Especifica la política de SnapMirror de ONTAP para la relación. El valor predeterminado es DPDefault.

◦ Crear política

Inicia el cuadro de diálogo Create SnapMirror Policy, que permite crear y utilizar una nueva política de SnapMirror.

◦ Programación de SnapMirror

Especifica la política de SnapMirror de ONTAP para la relación. Las programaciones disponibles incluyen ninguna, 5min, 8horas, diaria, por hora, y semanal. El valor predeterminado es None, lo que indica que no hay ningún programa asociado a la relación. Las relaciones sin programaciones no tienen valores de estado de desfase, a menos que pertenezcan a un servicio de almacenamiento.

◦ Crear programación

Abre el cuadro de diálogo Create Schedule, que permite crear una nueva programación de SnapMirror.

Pestaña SnapVault

Permite especificar un clúster secundario, una SVM y un agregado para una relación de protección, así como una convención de nomenclatura para los volúmenes secundarios al crear una relación de SnapVault. También puede especificar una política y una programación de SnapVault.

- **Vista de topología**

  Muestra una representación visual de la relación que está creando. El recurso secundario SnapVault de la topología se destaca de forma predeterminada.

- **Información secundaria**

  Permite seleccionar los recursos secundarios para una relación de protección:

  - Vínculo avanzado

    Inicia el cuadro de diálogo Configuración secundaria avanzada.

  - Clúster

    Enumera los clústeres que están disponibles como hosts de protección secundarios. El campo es obligatorio

  - Máquina virtual de almacenamiento (SVM)

    Enumera las SVM que están disponibles en el clúster seleccionado. Debe seleccionar un clúster antes de completar la lista de SVM. El campo es obligatorio

  - Agregado

    Enumera los agregados que están disponibles en la SVM seleccionada. Debe seleccionarse un clúster antes de rellenar la lista de agregados. El campo es obligatorio En la lista de agregados se muestra la siguiente información:

    - Clasificación

      Cuando varios agregados satisfacen todos los requisitos de un destino, la clasificación indica la prioridad en la que se indica el agregado, según las siguientes condiciones:

      A. Se recomienda un agregado ubicado en un nodo diferente al nodo de volumen primario para habilitar la separación de dominios de fallo.
      B. Se prefiere un agregado en un nodo con menos volúmenes para habilitar el equilibrio de carga entre nodos de un clúster.
      C. Se prefiere un agregado que tenga más espacio libre que otros agregados para habilitar el equilibrio de capacidad. Un rango de 1 significa que el agregado es el más preferido según los tres criterios.

    - Nombre del agregado

      Nombre del agregado

    - Capacidad disponible
    - Cantidad de espacio disponible en el agregado para los datos

        - Conjunto de recursos

          Nombre del pool de recursos al que pertenece el agregado

    - Convención de nomenclatura

      Especifica la convención de nomenclatura predeterminada que se aplica al volumen secundario. Puede aceptar la convención de nomenclatura proporcionada o crear una personalizada. La convención de nomenclatura puede tener los siguientes atributos: %C, %M, %V y %N, donde %C es el nombre del clúster, %M es el nombre de SVM, %V es el volumen de origen y %N es el nombre del nodo secundario de topología.

  El campo de convención de nomenclatura se resalta en rojo si la entrada no es válida. Al hacer clic en el vínculo «'Nombre de vista previa'», se muestra una vista previa de la convención de nomenclatura introducida y el texto de vista previa se actualiza dinámicamente a medida que se escribe una convención de nomenclatura en el campo de texto. Si escribe un valor no válido, la información no válida se muestra como signos de interrogación rojos en el área de vista previa. Se agrega un sufijo entre 001 y 999 al nombre secundario cuando se crea la relación, reemplazando la nnn que aparece en el texto de vista previa, con 001 asignado primero, 002 segundos asignados, etc.

- **Ajustes de relación**

  Permite especificar la tasa de transferencia máxima, la política SnapVault y la programación SnapVault que utiliza la relación de protección:

  - Velocidad máxima de transferencia

    Especifica la tasa máxima a la que se transfieren los datos entre los clústeres a través de la red. Si decide no utilizar una tasa de transferencia máxima, la transferencia de línea de base entre relaciones es ilimitada.

  - Política de SnapVault

    Especifica la política de ONTAP SnapVault para la relación. El valor predeterminado es XDPDefault.

  - Crear política

    Inicia el cuadro de diálogo Crear política de SnapVault, que permite crear y utilizar una nueva política de SnapVault.

  - Programación de SnapVault

    Especifica la programación de ONTAP SnapVault para la relación. Las programaciones disponibles incluyen ninguna, 5min, 8horas, diaria, por hora, y semanal. El valor predeterminado es None, lo que indica que no hay ningún programa asociado a la relación. Las relaciones sin programaciones no tienen valores de estado de desfase, a menos que pertenezcan a un servicio de almacenamiento.

  - Crear programación

    Abre el cuadro de diálogo Crear programación, que permite crear una programación SnapVault.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Cancelar**

  Descarta las selecciones y cierra el cuadro de diálogo Configurar protección.

- **Aplicar**

  Aplica las selecciones e inicia el proceso de protección.

Cuadro de diálogo Create Schedule

El cuadro de diálogo Create Schedule permite crear un programa de protección básico o avanzado para las transferencias de relaciones de SnapMirror y SnapVault. Es posible crear una nueva programación para aumentar la frecuencia de las transferencias de datos debido a actualizaciones de datos frecuentes, o bien crear una programación menos frecuente cuando cambian los datos con poca frecuencia.

Las programaciones no se pueden configurar para las relaciones de SnapMirror síncrono.

- **Cluster de destino**

  El nombre del clúster seleccionado en la pestaña SnapVault o la pestaña SnapMirror del cuadro de diálogo Configure Protection.

- **Nombre del programa**

  El nombre que se proporciona para la programación. Los nombres de horarios pueden consistir de los caracteres De La A a la Z, de la a a la z, del 0 al 9, así como cualquiera de los siguientes caracteres especiales: ! @ # $ % ^ & * ( ) _ -. Los nombres de las programaciones no pueden incluir los siguientes caracteres: < >.

- **Básico o Avanzado**

  El modo de programación que desea utilizar.

  El modo básico incluye los siguientes elementos:

  - Repetición

    La frecuencia con la que se produce una transferencia programada. Las opciones incluyen horarios, diarios y semanales.

  - Día

    Cuando se selecciona una repetición semanal, se produce el día de la semana en que se realiza una transferencia.

  - Tiempo

    Cuando se selecciona Diario o Semanal, se produce la hora del día en que se realiza una transferencia.

    El modo avanzado incluye los siguientes elementos:

  - Meses

Lista numérica separada por comas que representa los meses del año. Los valores válidos son de 0 a 11, con cero que representa enero, etc. Este elemento es opcional. Si deja el campo en blanco, las transferencias se producen cada mes.

- Días

  Lista numérica separada por comas que representa el día del mes. Los valores válidos son de 1 a 31. Este elemento es opcional. Dejar el campo en blanco implica que se produce una transferencia todos los días del mes.

- Días laborables

  Lista numérica separada por comas que representa los días de la semana. Los valores válidos son de 0 a 6, con 0 que representa domingo, etc. Este elemento es opcional. Dejar el campo en blanco implica que se produce una transferencia todos los días de la semana. Si se especifica un día de la semana pero no se especifica un día del mes, la transferencia se produce sólo en el día especificado de la semana y no todos los días.

- Horas

  Lista numérica separada por comas que representa el número de horas de un día. Los valores válidos son de 0 a 23, mientras que 0 representa la medianoche. Este elemento es opcional.

- Minutos

  Lista numérica separada por comas que representa los minutos en una hora. Los valores válidos abarcan de 0 a 59. Este elemento es obligatorio.

Cuadro de diálogo Create SnapMirror Policy

El cuadro de diálogo Create SnapMirror Policy permite crear una política para establecer la prioridad para las transferencias de SnapMirror. Las políticas se usan para maximizar la eficiencia de las transferencias del origen al destino.

- **Cluster de destino**

  El nombre del clúster seleccionado en la pestaña SnapMirror del cuadro de diálogo Configure Protection.

- **SVM de destino**

  El nombre de la SVM seleccionada en la pestaña SnapMirror del cuadro de diálogo Configure Protection.

- **Nombre de la política**

  Nombre que se proporcionará para la nueva política. Los nombres de políticas pueden consistir de los caracteres De La A a la Z, de la a a la z, del 0 al 9, punto (.), guión (-), y guión bajo (_).

- **Prioridad de transferencia**

  La prioridad en la que se ejecuta una transferencia para operaciones asíncronas. Puede seleccionar normal o Baja. Relaciones de transferencia con políticas que especifican una prioridad de transferencia normal ejecutada antes de aquellas con políticas que especifican una prioridad de transferencia baja.

- **Comentario**

Campo opcional en el que puede agregar comentarios acerca de la política.

- **Reiniciar transferencia**

  Indica qué acción de reinicio se debe realizar cuando una transferencia se interrumpe por una operación de interrupción o cualquier tipo de fallo, como una interrupción de la red. Puede seleccionar una de las siguientes opciones:

  ◦ Siempre

  Especifica que se crea una nueva copia Snapshot antes de reiniciar una transferencia y, si existe alguna, se reinicia la transferencia desde un punto de comprobación, seguido de una transferencia incremental desde la copia Snapshot recién creada.

  ◦ Nunca

  Especifica que las transferencias interrumpidas nunca se reinician.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Cancelar**

  Descarta las selecciones y cierra el cuadro de diálogo Configurar protección.

- **Aplicar**

  Aplica las selecciones e inicia el proceso de protección.

Cuadro de diálogo Create SnapVault Policy

El cuadro de diálogo Crear política de SnapVault permite crear una política para establecer la prioridad para las transferencias de SnapVault. Se usan políticas para maximizar la eficiencia de las transferencias del volumen primario al secundario.

- **Cluster de destino**

  El nombre del clúster seleccionado en la pestaña SnapVault del cuadro de diálogo Configurar protección.

- **SVM de destino**

  El nombre de la SVM seleccionada en la pestaña SnapVault del cuadro de diálogo Configure Protection.

- **Nombre de la política**

  Nombre que se proporcionará para la nueva política. Los nombres de políticas pueden consistir de los caracteres De La A a la Z, de la a a la z, del 0 al 9, punto (.), guión (-), y guión bajo (_).

- **Prioridad de transferencia**

  Prioridad a la que se ejecuta la transferencia. Puede seleccionar normal o Baja. Relaciones de transferencia con políticas que especifican una prioridad de transferencia normal ejecutada antes de aquellas con políticas que especifican una prioridad de transferencia baja. El valor predeterminado es

normal.

- **Comentario**

  Un campo opcional en el que puede añadir un comentario de hasta 255 caracteres acerca de la política de SnapVault.

- **Ignorar tiempo de acceso**

  Especifica si se omiten las transferencias incrementales para los archivos que sólo tienen cambiado el tiempo de acceso.

- **Etiqueta de replicación**

  Enumera en una tabla las reglas asociadas con las copias de Snapshot seleccionadas por ONTAP que tienen una etiqueta de replicación específica en una política. También está disponible la siguiente información y acciones:

  - Botones de comando

    Los botones de comando le permiten realizar las siguientes acciones:

    - Agregar

      Permite crear una etiqueta de copia Snapshot y un recuento de retenciones.

    - Editar recuento de retenciones

      Permite cambiar el número de retención de una etiqueta de copia Snapshot existente. El número de retención debe ser un número entre 1 y 251. La suma de todos los recuentos de retención para todas las reglas no puede ser mayor que 251.

    - Eliminar

      Permite eliminar una etiqueta de copia Snapshot existente.

  - Etiqueta de copia snapshot

    Muestra la etiqueta de la copia Snapshot. Si selecciona uno o varios volúmenes con la misma política de copia de Snapshot local, se muestra una entrada para cada etiqueta de la política. Si selecciona varios volúmenes con dos o más políticas de copia de Snapshot locales, la tabla muestra todas las etiquetas de todas las políticas

  - Programación

    Muestra la programación asociada con cada etiqueta de copia Snapshot. Si una etiqueta tiene más de una programación asociada, las programaciones de esa etiqueta se muestran en una lista separada por comas. Si selecciona varios volúmenes con la misma etiqueta pero con horarios diferentes, la programación mostrará "'varios'" para indicar que hay más de un programa asociado a los volúmenes seleccionados.

  - Recuento de retenciones de destino

    Muestra el número de copias de Snapshot con la etiqueta especificada que se conservan en el volumen secundario de SnapVault. El recuento de retenciones de etiquetas con varias programaciones muestra la suma de los recuentos de retención de cada etiqueta y pareja de programaciones. Si

selecciona varios volúmenes con dos o más políticas de copia de Snapshot locales, el número de retención estará vacío.

Cuadro de diálogo Edit Relationship

Es posible editar una relación de protección existente para cambiar la tasa de transferencia máxima, la política de protección o la programación de protección.

Información de destino

- **Cluster de destino**

  El nombre del clúster de destino seleccionado.

- **SVM de destino**

  El nombre de la SVM seleccionada

- **Ajustes de relación**

  Permite especificar la tasa de transferencia máxima, la política de SnapMirror y la programación que utiliza la relación de protección:

  - Velocidad máxima de transferencia

    Especifica la tasa máxima a la que se transfieren los datos de base entre los clústeres a través de la red. Cuando se selecciona, el ancho de banda de red está limitado al valor especificado. Puede introducir un valor numérico y, a continuación, seleccionar kilobytes por segundo (kbps), megabytes por segundo (Mbps), gigabytes por segundo (Gbps) o terabytes por segundo (Tbps). La velocidad de transferencia máxima que especifique debe ser superior a 1 kbps e inferior a 4 Tbps. Si decide no utilizar una tasa de transferencia máxima, la transferencia de línea de base entre relaciones es ilimitada. Si el clúster principal y el secundario son iguales, esta configuración se deshabilita.

  - Política de SnapMirror

    Especifica la política de SnapMirror de ONTAP para la relación. El valor predeterminado es DPDefault.

  - Crear política

    Inicia el cuadro de diálogo Create SnapMirror Policy, que permite crear y utilizar una nueva política de SnapMirror.

  - Programación de SnapMirror

    Especifica la política de SnapMirror de ONTAP para la relación. Las programaciones disponibles incluyen ninguna, 5min, 8horas, diaria, por hora, y semanal. El valor predeterminado es None, lo que indica que no hay ningún programa asociado a la relación. Las relaciones sin programaciones no tienen valores de estado de desfase, a menos que pertenezcan a un servicio de almacenamiento.

  - Crear programación

    Abre el cuadro de diálogo Create Schedule, que permite crear una nueva programación de SnapMirror.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Cancelar**

  Descarta las selecciones y cierra el cuadro de diálogo Configurar protección.

- **Enviar**

  Aplica las selecciones y cierra el cuadro de diálogo Editar relación.

Cuadro de diálogo Initialize/Update

El cuadro de diálogo inicializar/actualizar le permite realizar una primera transferencia de referencia en una nueva relación de protección o actualizar una relación si ya está inicializada y desea realizar una actualización manual, no programada e incremental.

Pestaña Transfer Options

La ficha Opciones de transferencia permite cambiar la prioridad de inicialización de una transferencia y cambiar el ancho de banda utilizado durante las transferencias.

- **Prioridad de transferencia**

  Prioridad a la que se ejecuta la transferencia. Puede seleccionar normal o Baja. Relaciones con políticas que especifican una prioridad de transferencia normal ejecutada antes de las que especifican una prioridad de transferencia baja. Normal está seleccionado de forma predeterminada.

- **Velocidad máxima de transferencia**

  Especifica la tasa máxima a la que se transfieren los datos entre los clústeres a través de la red. Si decide no utilizar una tasa de transferencia máxima, la transferencia de línea de base entre relaciones es ilimitada. Si selecciona más de una relación con diferentes tasas de transferencia máximas, puede especificar una de las siguientes opciones de velocidad de transferencia máxima:

  - Utilice los valores especificados durante la configuración o edición de una relación individual

    Cuando se selecciona, las operaciones de inicialización y actualización utilizan la tasa de transferencia máxima especificada en el momento de la creación o edición de cada relación. Este campo sólo está disponible cuando se inicializan o actualizan varias relaciones con diferentes tasas de transferencia.

  - Ilimitada

    Indica que no hay limitación del ancho de banda en las transferencias entre relaciones. Este campo sólo está disponible cuando se inicializan o actualizan varias relaciones con diferentes tasas de transferencia.

  - Limite el ancho de banda a.

    Cuando se selecciona, el ancho de banda de red está limitado al valor especificado. Puede introducir un valor numérico y, a continuación, seleccionar kilobytes por segundo (kbps), megabytes por segundo (Mbps), gigabytes por segundo (Gbps) o terabytes por segundo (Tbps). La velocidad de transferencia máxima que especifique debe ser superior a 1 kbps e inferior a 4 Tbps.

Pestaña Source Snapshot Copies

La pestaña Source Snapshot Copies muestra la siguiente información sobre la copia Snapshot de origen que se utiliza para la transferencia básica:

- **Volumen de origen**

  Muestra los nombres de los volúmenes de origen correspondientes.

- **Volumen de destino**

  Muestra los nombres de los volúmenes de destino seleccionados.

- **Tipo de fuente**

  Muestra el tipo de volumen. El tipo puede ser de lectura/escritura o protección de datos.

- **Copia snapshot**

  Muestra la copia Snapshot que se usa para la transferencia de datos. Al hacer clic en el valor de la copia Snapshot se muestra el cuadro de diálogo Select Source Snapshot Copy, en el que puede seleccionar una copia Snapshot específica para la transferencia, según el tipo de relación de protección que tenga y la operación que esté realizando. La opción para especificar una copia Snapshot diferente no está disponible para los orígenes de tipo de protección de datos.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Cancelar**

  Descarta las selecciones y cierra el cuadro de diálogo inicializar/actualizar.

- **Enviar**

  Guarda las selecciones e inicia el trabajo de inicialización o actualización.

Cuadro de diálogo Resynchronize

El cuadro de diálogo Resynchronize permite volver a sincronizar los datos de una relación de SnapMirror o SnapVault que se han roto previamente y, a continuación, el destino se ha creado un volumen de lectura/escritura. También es posible resincronizar cuando se elimina una copia Snapshot común requerida en el volumen de origen, y esto provoca errores en las actualizaciones de SnapMirror o SnapVault.

Pestaña Resynchronization Options

La pestaña Opciones de resincronización permite configurar la prioridad de transferencia y la tasa de transferencia máxima para la relación de protección que se está resincronizando.

- **Prioridad de transferencia**

  Prioridad a la que se ejecuta la transferencia. Puede seleccionar normal o Baja. Las relaciones con las directivas que especifican una prioridad de transferencia normal se ejecutan antes de las que tienen

directivas que especifican una prioridad de transferencia baja.

- **Velocidad máxima de transferencia**

  Especifica la tasa máxima a la que se transfieren los datos entre los clústeres a través de la red. Cuando se selecciona, el ancho de banda de red está limitado al valor especificado. Puede introducir un valor numérico y, a continuación, seleccionar kilobytes por segundo (kbps), megabytes por segundo (Mbps), gigabytes por segundo (Gbps) o Tbps. Si decide no utilizar una tasa de transferencia máxima, la transferencia de línea de base entre relaciones es ilimitada.

Pestaña Source Snapshot Copies

La pestaña Source Snapshot Copies muestra la siguiente información sobre la copia Snapshot de origen que se utiliza para la transferencia básica:

- **Volumen de origen**

  Muestra los nombres de los volúmenes de origen correspondientes.

- **Volumen de destino**

  Muestra los nombres de los volúmenes de destino seleccionados.

- **Tipo de fuente**

  Muestra el tipo de volumen: Lectura/escritura o protección de datos.

- **Copia snapshot**

  Muestra la copia Snapshot que se usa para la transferencia de datos. Al hacer clic en el valor de la copia de Snapshot se muestra el cuadro de diálogo Select Source Snapshot Copy, en el que puede seleccionar una copia de Snapshot específica para la transferencia, según el tipo de relación de protección que tenga y la operación que esté realizando.

Botones de comando

- **Enviar**

  Inicia el proceso de resincronización y cierra el cuadro de diálogo Resincronizar.

- **Cancelar**

  Cancela las selecciones y cierra el cuadro de diálogo Resynchronize.

Cuadro de diálogo Select Source Snapshot Copy

Utilice el cuadro de diálogo Seleccionar copia Snapshot de origen para seleccionar una copia Snapshot específica para transferir datos entre relaciones de protección, o bien seleccione el comportamiento predeterminado, que varía en función de si está inicializando, actualizando o resincronizando una relación y si la relación es SnapMirror o SnapVault.

Predeterminado

Permite seleccionar el comportamiento predeterminado para determinar qué copia Snapshot se utiliza para inicializar, actualizar y resincronizar transferencias para relaciones de SnapVault y SnapMirror.

Si realiza una transferencia de SnapVault, el comportamiento predeterminado de cada operación es el siguiente:

Funcionamiento	Comportamiento SnapVault predeterminado cuando el origen es de lectura/escritura	Comportamiento de SnapVault predeterminado cuando el origen es Protección de datos (DP)
Inicializar	Crea una nueva copia Snapshot y la transfiere.	Transfiere la última copia snapshot exportada.
Actualizar	Transfiere solo las copias Snapshot etiquetadas, como se especifica en la política.	Transfiere la última copia snapshot exportada.
Resincronizar	Transfiere todas las copias Snapshot etiquetadas creadas después de la copia Snapshot común más reciente.	Transfiere la copia Snapshot más reciente etiquetada.

Si realiza una transferencia de SnapMirror, el comportamiento predeterminado de cada operación es el siguiente:

Funcionamiento	Comportamiento de SnapMirror predeterminado	Comportamiento predeterminado de SnapMirror cuando la relación es un segundo salto en una cascada de SnapMirror a SnapMirror
Inicializar	Crea una nueva copia Snapshot y la transfiere, y todas las copias Snapshot creadas antes de la nueva copia Snapshot.	Transfiere todas las copias Snapshot del origen.
Actualizar	Crea una nueva copia Snapshot y la transfiere, y todas las copias Snapshot creadas antes de la nueva copia Snapshot.	Transfiere todas las copias Snapshot.
Resincronizar	Crea una nueva copia Snapshot y, a continuación, transfiere todas las copias Snapshot del origen.	Transfiere todas las copias Snapshot del volumen secundario al volumen terciario y elimina los datos que agregue tras la creación de la copia de Snapshot común más reciente.

Copia Snapshot existente

Permite seleccionar una copia de Snapshot existente de la lista si se permite la selección de una copia de Snapshot para esa operación.

- **Copia snapshot**

  Muestra las copias Snapshot existentes desde las que puede seleccionar para una transferencia.

- **Fecha de creación**

  Muestra la fecha y la hora en que se creó la copia Snapshot. Las copias snapshot se enumeran de las más recientes a las menos recientes, con la más reciente en la parte superior de la lista.

Si va a realizar una transferencia de SnapVault y desea seleccionar una copia Snapshot existente para transferir de un origen a un destino, el comportamiento de cada operación es el siguiente:

Funcionamiento	Comportamiento de SnapVault al especificar una copia Snapshot	Comportamiento de SnapVault al especificar una copia Snapshot en una cascada
Inicializar	Transfiere la copia Snapshot especificada.	No se admite la selección de copias Snapshot de origen para los volúmenes de protección de datos.
Actualizar	Transfiere la copia Snapshot especificada.	No se admite la selección de copias Snapshot de origen para los volúmenes de protección de datos.
Resincronizar	Transfiere la copia Snapshot seleccionada.	No se admite la selección de copias Snapshot de origen para los volúmenes de protección de datos.

Si va a realizar una transferencia de SnapMirror y desea seleccionar una copia de Snapshot existente para transferir de un origen a un destino, el comportamiento de cada operación es el siguiente:

Funcionamiento	Comportamiento de SnapMirror al especificar una copia Snapshot	Comportamiento de SnapMirror al especificar una copia Snapshot en una cascada
Inicializar	Transfiere todas las copias Snapshot del origen, hasta la copia Snapshot especificada.	No se admite la selección de copias Snapshot de origen para los volúmenes de protección de datos.
Actualizar	Transfiere todas las copias Snapshot del origen, hasta la copia Snapshot especificada.	No se admite la selección de copias Snapshot de origen para los volúmenes de protección de datos.

Funcionamiento	Comportamiento de SnapMirror al especificar una copia Snapshot	Comportamiento de SnapMirror al especificar una copia Snapshot en una cascada
Resincronizar	Transfiere todas las copias Snapshot del origen, hasta la copia Snapshot seleccionada y, a continuación, elimina los datos que se hayan añadido después de crear la copia Snapshot común más reciente.	No se admite la selección de copias Snapshot de origen para los volúmenes de protección de datos.

Botones de comando

Los botones de comando le permiten realizar las siguientes tareas:

- **Enviar**

  Envía las selecciones y cierra el cuadro de diálogo Seleccionar copia Snapshot de origen.

- **Cancelar**

  Descarta las selecciones y cierra el cuadro de diálogo Seleccionar copia Snapshot de origen.

Cuadro de diálogo Reverse Resync

Cuando tiene una relación de protección rota debido a que el volumen de origen está deshabilitado y el destino se hace un volumen de lectura/escritura, la resincronización inversa permite invertir la dirección de la relación de modo que el destino se convierta en el nuevo origen y el origen se convierta en el nuevo destino.

Cuando un desastre deshabilita el volumen de origen en la relación de protección, se puede usar el volumen de destino para suministrar datos mediante la conversión a lectura/escritura, mientras se repara o sustituye el origen, se actualiza el origen y se establece la relación. Cuando realiza una operación de resincronización inversa, se eliminan los datos del origen más nuevos que los de la copia común de Snapshot.

Antes de realizar una resincronización inversa

Muestra el origen y el destino de una relación antes de una operación de resincronización inversa.

- **Volumen de origen**

  El nombre y la ubicación del volumen de origen antes de una operación de resincronización inversa.

- **Volumen de destino**

  El nombre y la ubicación del volumen de destino antes de una operación de resincronización inversa.

Tras realizar una resincronización inversa

Muestra el origen y el destino de una relación después de una operación de resincronización de reserva.

- **Volumen de origen**

  El nombre y la ubicación del volumen de origen después de una operación de resincronización inversa.

- **Volumen de destino**

  El nombre y la ubicación del volumen de destino después de una operación de resincronización inversa.

Botones de comando

Los botones de comando le permiten realizar las siguientes acciones:

- **Enviar**

  Inicia el proceso de resincronización inversa.

- **Cancelar**

  Cierra el cuadro de diálogo Reverse Resync sin iniciar una operación de resincronización inversa.

Relación: Vista todas las relaciones

La relación: La vista todas las relaciones muestra información sobre las relaciones de protección en el sistema de almacenamiento.

De forma predeterminada, cuando accede a la página Relationships, el informe que se muestra incluye las relaciones de protección de nivel superior tanto para volúmenes como para máquinas virtuales de almacenamiento. Los controles situados en la parte superior de la página permiten seleccionar una vista concreta, realizar búsquedas para localizar objetos específicos, crear y aplicar filtros para restringir la lista de datos mostrados, añadir/eliminar/reordenar columnas en la página y exportar los datos de la página a .csv, .pdf, o archivo .xlsx. Después de personalizar la página, puede guardar los resultados como una vista personalizada y, a continuación, programar un informe de estos datos para que se genere y se envíe por correo electrónico regularmente. De forma predeterminada, al seleccionar el menú **Relaciones**, el informe que se muestra incluye relaciones de protección tanto para volúmenes como para equipos virtuales de almacenamiento en el centro de datos. Puede utilizar la opción **filtro** para ver sólo los sistemas de almacenamiento seleccionados como sólo los volúmenes o sólo los equipos virtuales de almacenamiento. El mismo informe se muestra en la página almacenamiento y solo para la entidad de almacenamiento seleccionada. Si desea ver las relaciones de VM de volumen o almacenamiento, puede acceder a la página **almacenamiento** > **volúmenes** > **relación: Todas las relaciones** o a **Protección** > **Relaciones** > **relación: Todas las relaciones**, y utilice la opción **Tipo de objeto de relación** de **filtro** para filtrar sólo volúmenes o datos de equipos virtuales de almacenamiento.

La página Relaciones que enumera todas las relaciones de protección tiene el vínculo **Ver en System Manager** para el clúster de destino que permite ver los mismos objetos en el Administrador del sistema de ONTAP.

- **Estado**

  Muestra el estado actual de la relación de protección.

  El estado puede ser uno de los errores (), Advertencia () O bien OK ().

- **VM de almacenamiento de origen**

Muestra el nombre de la SVM de origen. Para ver más detalles sobre la SVM de origen, se debe hacer clic en el nombre de la SVM.

Cuando hay una SVM en el clúster, pero aún no se ha añadido al inventario de Unified Manager o cuando la SVM se creó después de la última actualización del clúster, este campo estará vacío. Debe asegurarse de que exista la SVM o realizar una nueva detección en el clúster para actualizar la lista de recursos.

- **Fuente**

  Muestra el volumen de origen o la máquina virtual de almacenamiento de origen que se está protegiendo según lo seleccionado. Si desea ver más detalles sobre el volumen de origen o la máquina virtual de almacenamiento, haga clic en el nombre del volumen o de la máquina virtual de almacenamiento.

  Si el mensaje `Resource-key not discovered` Si se muestra, esto puede indicar que el volumen existe en el clúster pero que aún no se ha añadido al inventario de Unified Manager o que el volumen se creó después de la última actualización del clúster. Debe asegurarse de que el volumen exista o realizar una nueva detección en el clúster para actualizar la lista de recursos.

- **Almacenamiento de destino VM**

  Muestra el nombre de la SVM de destino. Para ver más detalles sobre la SVM de destino, se debe hacer clic en el nombre de la SVM.

- **Destino**

  Muestra el nombre del volumen de destino o de la máquina virtual de almacenamiento según la selección. Puede ver más detalles sobre el volumen de destino o la máquina virtual de almacenamiento haciendo clic en el nombre del objeto correspondiente.

- **Tipo de objeto de relación**

  Muestra el tipo de objeto usado en la relación, como la máquina virtual de almacenamiento, el volumen y el grupo de consistencia. Para los objetos de una relación de consistencia, el origen de las relaciones y los destinos muestran el grupo de consistencia, y al hacer clic en ellos le lleva a la página de LUN para ver la relación.

- **Política**

  Muestra el nombre de la política de protección para la relación de SnapMirror. Puede hacer clic en el nombre de la política para ver los detalles asociados con esa política, incluida la siguiente información:

  - Prioridad de transferencia

    Especifica la prioridad en la que se ejecuta una transferencia para operaciones asíncronas. La prioridad de transferencia es normal o Baja. Las transferencias de prioridad normal se programan antes de que se realicen transferencias de baja prioridad. El valor predeterminado es normal.

  - Ignorar tiempo de acceso

    Se aplica solo a las relaciones de SnapVault. Esto especifica si las transferencias incrementales ignoran archivos que sólo cambian su tiempo de acceso. Los valores son True o False. El valor predeterminado es False.

  - Cuando la relación no está sincronizada

    Especifica la acción que ONTAP realiza cuando no se puede sincronizar una relación síncrona. Las

relaciones de StrictSync restringirán el acceso al volumen primario si no se ha podido sincronizar con el volumen secundario. Las relaciones de sincronización no restringen el acceso al primario si no se sincroniza con el secundario.

- Intenta el límite

  Especifica la cantidad máxima de veces que se debe intentar cada transferencia manual o programada para una relación de SnapMirror. El valor predeterminado es 8.

- Comentarios

  Proporciona un campo de texto para comentarios específicos de la directiva seleccionada.

- Etiqueta de SnapMirror

  Especifica la etiqueta de SnapMirror para la primera programación asociada a la política de copia de Snapshot. El subsistema SnapVault utiliza la etiqueta de SnapMirror al realizar un backup de copias de Snapshot en un destino de SnapVault.

- Configuración de retención

  Especifica cuánto tiempo se conservarán los backups, en función del tiempo o de la cantidad de backups.

- Copias Snapshot reales

  Especifica la cantidad de copias de Snapshot en este volumen que coinciden con la etiqueta especificada.

- Conserve copias Snapshot

  Especifica el número de copias de Snapshot de SnapVault que no se eliminan automáticamente aunque se alcance el límite máximo de la política. Los valores son True o False. El valor predeterminado es False.

- Umbral de advertencia de retención

  Especifica el límite de copias de Snapshot en el que se envía una advertencia para indicar que el límite de retención máximo está casi alcanzado.

- **Duración de retraso**

  Muestra la cantidad de tiempo que los datos del reflejo se retrasan con respecto al origen.

  La duración de la demora debe ser cercana o igual a 0 segundos para las relaciones de StrictSync.

- **Estado de retraso**

  Muestra el estado de posposición de las relaciones administradas y de las relaciones no administradas que tienen una programación asociada a dicha relación. El estado de desfase puede ser:

  - Error

    La duración de la demora es mayor o igual que el umbral de error de desfase.

  - Advertencia

La duración de la demora es mayor o igual que el umbral de aviso de desfase.

- DE ACUERDO

  La duración de la demora se encuentra dentro de los límites normales.

- No aplicable

  El estado de desfase no es aplicable a las relaciones síncronas porque no es posible configurar una programación.

- **Última actualización realizada correctamente**

  Muestra la hora a la que se realizó la última operación correcta de SnapMirror o SnapVault.

  La última actualización realizada correctamente no es aplicable a las relaciones síncronas.

- **Relaciones Constitutivas**

  Muestra si hay volúmenes en el objeto seleccionado.

- **Tipo de relación**

  Muestra el tipo de relación utilizado para replicar un volumen. Los tipos de relaciones incluyen:

  - Reflejo asíncrono
  - Vault asíncrono
  - Reflejo asíncrono de Vault
  - StrictSync
  - Sincr

- **Estado de transferencia**

  Muestra el estado de transferencia de la relación de protección. El estado de la transferencia puede ser uno de los siguientes:

  - Anulando

    Las transferencias de SnapMirror están habilitadas; no obstante, hay una operación de anulación de transferencia que puede incluir la eliminación del punto de comprobación en curso.

  - Comprobando

    El volumen de destino está sometido a una comprobación de diagnóstico y no hay transferencia en curso.

  - Finalizando

    Las transferencias de SnapMirror están habilitadas. El volumen se encuentra actualmente en la fase de postransferencia para las transferencias incrementales de la SnapVault.

  - Inactivo

    Las transferencias están habilitadas y no hay transferencia en curso.

- Sinc

  Los datos de los dos volúmenes en la relación síncrona están sincronizados.

- Fuera de sincronización

  Los datos del volumen de destino no están sincronizados con el volumen de origen.

- Preparando

  Las transferencias de SnapMirror están habilitadas. El volumen se encuentra actualmente en la fase de transferencia previa a las transferencias de SnapVault incrementales.

- En cola

  Las transferencias de SnapMirror están habilitadas. No hay transferencias en curso.

- En modo inactivo

  Las transferencias de SnapMirror están deshabilitadas. No hay transferencia en curso.

- Ralentización

  Hay una transferencia de SnapMirror en curso. Las transferencias adicionales están deshabilitadas.

- Transfiriendo

  Las transferencias de SnapMirror están habilitadas y hay una transferencia en curso.

- En transición

  Se completó la transferencia asíncrona de datos del volumen de origen al volumen de destino y se inició la transición hacia la operación síncrona.

- Esperando

  Se ha iniciado una transferencia de SnapMirror, pero algunas tareas asociadas están a la espera de que se pongan en cola.

- **Duración de la última transferencia**

  Muestra el tiempo que se tarda en finalizar la última transferencia de datos.

  La duración de la transferencia no es aplicable a las relaciones de StrictSync porque la transferencia debe ser simultánea.

- **Tamaño de la última transferencia**

  Muestra el tamaño, en bytes, de la última transferencia de datos.

  El tamaño de transferencia no es aplicable a las relaciones StrictSync.

- * Mediadores*

  Muestra el estado del mediador.

- No aplicable

  Si el clúster no es compatible con la continuidad empresarial de SnapMirror.

- No configurado

  Si no está configurado, o si está configurado pero solo se añade el clúster de destino y el clúster de origen no se añade en Unified Manager.

- Dirección IP del mediador

  Si está configurado, y los clústeres de origen y destino se añaden en Unified Manager.

- **Estado**

  Muestra el estado de la relación de SnapMirror o SnapVault. El estado puede ser sin inicializar, con SnapMirror o con Broken-Off. Si se selecciona un volumen de origen, no se aplica el estado de relación y no se muestra.

- **Salud de la relación**

  Muestra el estado de la relación del clúster.

- **Razón insalubre**

  La razón por la que la relación está en un estado poco saludable.

- **Prioridad de transferencia**

  Muestra la prioridad en la que se ejecuta una transferencia. La prioridad de transferencia es normal o Baja. Las transferencias de prioridad normal se programan antes de que se realicen transferencias de baja prioridad.

  La prioridad de transferencia no es aplicable a las relaciones síncronas porque todas las transferencias se tratan con la misma prioridad.

- **Horario**

  Muestra el nombre de la programación de protección asignada a la relación.

  La programación no se aplica para relaciones síncronas.

- **Replicación flexible de versiones**

  Muestra las opciones Sí, Sí con copia de seguridad o Ninguno.

- **Cluster de origen**

  Muestra el FQDN, el nombre abreviado o la dirección IP del clúster de origen para la relación de SnapMirror.

- **Cluster de origen FQDN**

  Muestra el nombre del clúster de origen de la relación SnapMirror.

- **Nodo de origen**

Muestra el nombre del enlace de nombre del nodo de origen de la relación de SnapMirror de un volumen y muestra el enlace de recuento de nodos de relación de SnapMirror cuando el objeto es una máquina virtual de almacenamiento o un grupo de consistencia.

En la vista personalizada, al hacer clic en el enlace del nombre del nodo, puede ver y extender la protección de objetos de almacenamiento en los que los volúmenes de esos grupos de coherencia pertenecen a una relación SM-BC.

Cuando hace clic en el enlace del recuento de nodos, llega a la página del nodo con los respectivos nodos asociados a dicha relación. Cuando el número de nodos es 0, no se muestra ningún valor, ya que no hay nodos asociados con la relación.

- **Nodo de destino**

  Muestra el nombre del enlace de nombre de nodo de destino de la relación de SnapMirror de un volumen y muestra el enlace de recuento de nodos de relación de SnapMirror cuando el objeto es una máquina virtual de almacenamiento o un grupo de consistencia.

  Cuando hace clic en el enlace del recuento de nodos, llega a la página del nodo con los respectivos nodos asociados a dicha relación. Cuando el número de nodos es 0, no se muestra ningún valor, ya que no hay nodos asociados con la relación.

- **Cluster de destino**

  Muestra el nombre del clúster de destino de la relación SnapMirror.

- **FQDN del clúster de destino**

  Muestra el FQDN, el nombre abreviado o la dirección IP del clúster de destino para la relación de SnapMirror.

- * Protegido por*

  Muestra las diferentes relaciones. En esta columna, puede ver relaciones de volúmenes y grupos de coherencia para los clústeres y el orden de las máquinas virtuales de almacenamiento, como:

  - SnapMirror
  - Recuperación ante desastres de máquinas virtuales de almacenamiento
  - SnapMirror y recuperación ante desastres de máquinas virtuales de almacenamiento
  - Grupo de consistencia
  - SnapMirror, grupo de consistencia.

Información relacionada

- Para obtener información acerca de **relación: Vista MetroCluster**, consulte "Supervisar las configuraciones de MetroCluster".
- Para obtener información acerca de **relación: Vista Estado de transferencia de último 1 mes**, consulte "Relación: Vista Estado de transferencia de último 1 mes".
- Para obtener información acerca de la vista **relación: Todas las relaciones**, consulte "Relación: Última vista de tarifa de transferencia de 1 mes".

Relación: Vista Estado de transferencia de último 1 mes

La vista relación: El estado de transferencia de último 1 mes permite analizar las tendencias de transferencia durante un periodo de tiempo para volúmenes y máquinas virtuales de almacenamiento en relaciones asíncronas. En esta página también se muestra si la transferencia ha sido satisfactoria o no.

Los controles situados en la parte superior de la página permiten realizar búsquedas para localizar objetos específicos, crear y aplicar filtros para restringir la lista de datos mostrados, añadir/eliminar/reordenar columnas en la página y exportar los datos de la página a un `.csv`, `.pdf`, o. `.xlsx` archivo. Después de personalizar la página, puede guardar los resultados como una vista personalizada y, a continuación, programar un informe de estos datos para que se genere y se envíe por correo electrónico regularmente. Puede utilizar la opción **filtro** para ver sólo los sistemas de almacenamiento seleccionados como sólo los volúmenes o sólo las máquinas virtuales de almacenamiento. El mismo informe se muestra en la página almacenamiento y solo para la entidad de almacenamiento seleccionada. Por ejemplo, si desea ver las relaciones de volumen, puede acceder a la relación: Último informe de estado de transferencia de 1 mes para los equipos virtuales de almacenamiento desde el menú **almacenamiento** > **Storage VMs** > **relación: Último 1 mes Estado de transferencia** o desde **Protección** > **Relaciones** > **relación: Último menú Estado de transferencia de 1 mes** y utilice el **filtro** para ver sólo los datos de los volúmenes.

- **Volumen de origen**

  Muestra el nombre del volumen de origen.

- **Volumen de destino**

  Muestra el nombre del volumen de destino.

- **Tipo de operación**

  Muestra el tipo de transferencia de volumen.

- **Resultado de funcionamiento**

  Muestra si la transferencia de volumen se realizó correctamente.

- **Hora de inicio de la transferencia**

  Muestra la hora de inicio de la transferencia del volumen.

- **Tiempo de finalización de transferencia**

  Muestra la hora de finalización de la transferencia del volumen.

- **Duración de transferencia**

  Muestra el tiempo necesario (en horas) para completar la transferencia de volumen.

- **Tamaño de transferencia**

  Muestra el tamaño (en MB) del volumen transferido.

- **Fuente SVM**

  Muestra el nombre de la máquina virtual de almacenamiento (SVM).

- **Cluster de origen**

  Muestra el nombre del clúster de origen.

- **SVM de destino**

  Muestra el nombre de la SVM de destino.

- **Cluster de destino**

  Muestra el nombre del clúster de destino.

Información relacionada

- Para obtener información acerca de la vista **relación: Todas las relaciones**, consulte "Relación: Vista todas las relaciones".
- Para obtener información acerca de la vista **relación:MetroCluster**, consulte "Supervisar las configuraciones de MetroCluster".
- Para obtener información acerca de la vista **relación: Todas las relaciones**, consulte "Relación: Última vista de tarifa de transferencia de 1 mes".

Relación: Última vista de tarifa de transferencia de 1 mes

La vista relación: La vista tasa de transferencia de 1 mes pasado permite analizar la cantidad de volumen de datos que se transfiere el día a día para los volúmenes en relaciones asíncronas. En esta página, también se ofrecen detalles sobre las transferencias diarias y el tiempo necesario para completar la operación de transferencia de volúmenes y máquinas virtuales de almacenamiento.

Los controles en la parte superior de la página le permiten realizar búsquedas para localizar objetos específicos, crear y aplicar filtros para restringir la lista de datos mostrados, añadir/eliminar/reordenar columnas en la página y exportar los datos de la página a un archivo .csv, .pdf o .xlsx. Después de personalizar la página, puede guardar los resultados como una vista personalizada y, a continuación, programar un informe de estos datos para que se genere y se envíe por correo electrónico regularmente. Por ejemplo, si desea ver las relaciones de volumen, puede acceder al menú **almacenamiento** > **volúmenes** > **relación: Último 1 mes velocidad de transferencia** o acceder al menú **Protección** > **Relaciones** > **Relaciones:último 1 mes velocidad de transferencia** y utilizar el menú **filtro** para ver sólo los datos de los volúmenes.

- **Tamaño total de transferencia**

  Muestra el tamaño total de la transferencia de volumen en gigabytes.

- **Día**

  Muestra el día en el que se inició la transferencia de volumen.

- **Hora final**

  Muestra la hora de finalización de la transferencia de volumen con la fecha.

Información relacionada

- Para obtener información acerca de la vista **relación:MetroCluster**, consulte "Supervisar las configuraciones de MetroCluster".
- Para obtener información acerca de **relación: Vista Estado de transferencia de último 1 mes**, consulte "Relación: Vista Estado de transferencia de último 1 mes".
- Para obtener información acerca de la vista **relación: Todas las relaciones**, consulte "Relación: Última vista de tarifa de transferencia de 1 mes"

Generar informes personalizados

Informes de Unified Manager

Active IQ Unified Manager (anteriormente Unified Manager de OnCommand) ofrece la capacidad de ver, personalizar, descargar y programar informes para sus sistemas de almacenamiento de ONTAP. Los informes pueden proporcionar detalles sobre la capacidad, el estado, el rendimiento, la seguridad y las relaciones de protección del sistema de almacenamiento.

La nueva funcionalidad de programación y generación de informes de Unified Manager incluida en Active IQ Unified Manager 9.6 sustituye al motor de informes anterior que se retiró en Unified Manager versión 9.5.

Los informes proporcionan diferentes puntos de vista de la red, ofreciendo información práctica sobre capacidad, estado, rendimiento, seguridad y datos de protección. Puede personalizar las vistas mostrando, ocultando y reorganizando columnas, filtrando datos, ordenando datos, y buscando los resultados. Puede guardar vistas personalizadas para volver a utilizarlas, descargarlas como informes y programarlas como informes periódicos para distribuirlas por correo electrónico.

Puede descargar vistas en formato Microsoft® Excel y personalizarlas. Puede utilizar características avanzadas de Excel, como ordenaciones complejas, filtros con capas, tablas dinámicas y gráficos. Cuando esté satisfecho con el informe de Excel resultante, puede cargar el archivo de Excel para utilizarlo cada vez que se programe y comparta el informe.

Además de generar informes desde la interfaz de usuario, puede extraer datos de estado, seguridad y rendimiento de Unified Manager mediante estos métodos adicionales:

- Utilizar las herramientas ODBC (Open Database Connectivity) y ODBC para acceder directamente a la base de datos para obtener información del clúster
- Ejecutar las API DE REST de Unified Manager para obtener la información que desea revisar

A partir de esta versión de Active IQ Unified Manager se han realizado las siguientes mejoras en los informes:

- Se envía un correo electrónico para un informe según la programación configurada. Incluso cuando genere un informe bajo demanda, recibirá un correo electrónico.
- El nombre de archivo del informe y los metadatos del informe incluyen el nombre de host desde donde se generó el informe. Incluso si alguien cambia el nombre de archivo, todavía puede identificar el nombre de host desde donde se generó el informe debido a esta mejora.

Puntos de acceso para generar informes

Puede recopilar información en Unified Manager sobre los clústeres para crear informes desde la interfaz de usuario, consultas de base de datos de MySQL y API DE REST.

Estas secciones describen los informes de Unified Manager y la programación a través de la interfaz de usuario de.

Existen tres formas de acceder a las funcionalidades de generación de informes que proporciona Unified Manager:

- Extrayendo datos directamente de las páginas de inventario de la interfaz de usuario.

- Utilizar las herramientas ODBC (Open Database Connectivity) y ODBC para tener acceso a todos los objetos disponibles.
- Ejecute las API DE REST de Unified Manager para obtener la información que desea revisar.

Estas secciones describen los informes de Unified Manager y la programación a través de la interfaz de usuario de.

Bases de datos de Unified Manager accesibles para la generación de informes personalizados

Unified Manager utiliza una base de datos de MySQL para almacenar datos de los clústeres que se están supervisando. Los datos se mantienen en varios esquemas en la base de datos de MySQL.

Todos los datos de las tablas de las siguientes bases de datos están disponibles:

Base de datos	Descripción
modelo_netapp	Datos acerca de los objetos en controladoras ONTAP.
vista_modelo_netapp	Datos acerca de los objetos en controladoras ONTAP, adecuados para consumo de herramientas de informes.
rendimiento_netapp	Contadores de rendimiento específicos del clúster.
ocum	Datos e información de aplicaciones de Unified Manager para admitir el filtrado, la ordenación y el cálculo de algunos campos derivados de la interfaz de usuario.
ocum_report	Datos para obtener información relacionada con la capacidad y la configuración de inventario.
ocum_report_birt	Vistas para la configuración de inventario y los datos relacionados con la capacidad, adecuados para el consumo de la herramienta de informes.
opm	Información del umbral y de la configuración del rendimiento.
escalemador	Datos sobre los problemas de estado y rendimiento de las aplicaciones de Unified Manager.
modelo_vmware	Datos de objetos de VMware para almacenes de datos alojados en almacenamiento de NetApp.

Base de datos	Descripción
vista_modelo_vmware	Vistas de los datos de objetos de VMware para almacenes de datos alojados en el almacenamiento de NetApp, adecuado para el consumo de la herramienta de informes.
rendimiento_de_vmware	Datos de contadores de rendimiento de VMware para almacenes de datos alojados en almacenamiento de NetApp.

Un usuario de informes — un usuario de base de datos con el rol de esquema de informes — puede tener acceso a los datos de estas tablas. Este usuario tiene acceso de solo lectura a las vistas de informes y otras bases de datos directamente desde la base de datos de Unified Manager. Tenga en cuenta que este usuario no tiene permiso para acceder a ninguna tabla que contenga datos de usuario o información de credenciales de clúster.

Las API DE REST de Unified Manager que se pueden usar para crear informes

Puede usar API REST para ayudar a gestionar los clústeres mediante la visualización de la información de estado, capacidad, rendimiento y seguridad capturada por Unified Manager.

Las API DE REST se exponen a través de la página web de Swagger. Es posible acceder a la página web de Swagger para ver la documentación de la API DE REST de Unified Manager, y también para emitir manualmente una llamada API. En la interfaz de usuario web de Unified Manager, en la barra de menús, haga clic en el botón **Ayuda** y seleccione **Documentación de API**. Para obtener información sobre las API DE REST de Unified Manager, consulte "Primeros pasos con API de REST de Active IQ Unified Manager".

Debe tener el rol de operador, administrador de almacenamiento o administrador de aplicaciones para acceder a las API DE REST.

Informes

Los informes muestran información detallada sobre el almacenamiento, la red, la calidad del servicio y las relaciones de protección, lo que ayuda a identificar y solucionar los problemas potenciales antes de que se produzcan.

Al personalizar una vista, puede guardarla con un nombre único para utilizarla en el futuro. Puede programar un informe basado en esa vista para que se ejecute con regularidad y lo comparta con otras personas. También puede descargar la vista en Excel para personalizarla mediante características avanzadas de Excel y, a continuación, volver a cargarla en Unified Manager . Si programa un informe con esa vista, utilizará el archivo de Excel que ha cargado para crear informes sólidos que pueda compartir.

Es posible gestionar todos los informes programados desde la página Report Schedules.

Para administrar informes, debe tener la función Administrador de aplicaciones o Administrador de almacenamiento.

Puede descargar informes como archivos de valores separados por comas (CSV), Excel o PDF.

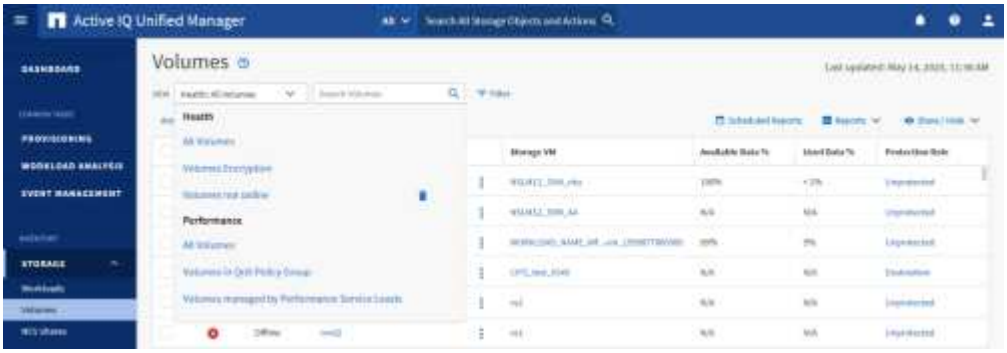
Comprensión de la relación de vista e informe

Las vistas y las páginas de inventario se convierten en informes cuando las descarga o las programa.

Se pueden personalizar y guardar vistas y páginas de inventario para volver a utilizarlas. Casi todo lo que se puede ver en Unified Manager se puede guardar, reutilizar, personalizar, programar y compartir como un informe.

En el menú desplegable de la vista, los elementos con el icono de eliminación son vistas personalizadas existentes que usted u otro usuario han creado. Los elementos sin un icono son las vistas predeterminadas que se proporcionan con Unified Manager. Las vistas predeterminadas no se pueden modificar ni eliminar.

- Si elimina una vista personalizada de la lista, también elimina los archivos de Excel o los informes programados que utilicen esa vista.
- Si cambia una vista personalizada, los informes que utilizan esa vista reflejarán el cambio la próxima vez que se genere el informe y se envíe por correo electrónico de acuerdo con la programación del informe. Al cambiar las vistas, asegúrese de que los cambios funcionan con las personalizaciones de Excel asociadas que se utilizan para los informes. Si es necesario, puede actualizar el archivo de Excel descargándolo, realizando los cambios necesarios y cargándolo como una nueva personalización de Excel para la vista.



Sólo los usuarios con la función Administrador de aplicaciones o Administrador de almacenamiento pueden ver el icono de eliminar, cambiar o eliminar una vista, o cambiar o eliminar un informe programado.

Tipos de informes

Esta tabla proporciona una lista completa de las vistas y páginas de inventario que están disponibles como informes que se pueden personalizar, descargar y programar.

Informes de Active IQ Unified Manager

Tipo	Objeto de almacenamiento o red
Capacidad	De clúster Agregados Volúmenes Qtrees

Tipo	Objeto de almacenamiento o red
Salud	De clúster Nodos Agregados Máquinas virtuales de almacenamiento Volúmenes Recursos compartidos SMB/CIFS Recursos compartidos de NFS
Rendimiento	De clúster Nodos Agregados Máquinas virtuales de almacenamiento Volúmenes LUN Espacios de nombres de NVMe Interfaces de red (LIF) Puertos
Calidad de servicio	Grupos de políticas de calidad de servicio tradicionales Grupos de políticas de calidad de servicio adaptativos Grupos de políticas de nivel de servicio de rendimiento
Relaciones de protección de volúmenes (disponibles en la página volúmenes)	Todas las relaciones Estado de transferencia de último 1 mes Tarifa de transferencia de 1 mes
Seguridad	Máquinas virtuales de almacenamiento De clúster

Limitaciones en la generación de informes

Existen algunas limitaciones con la nueva funcionalidad de generación de informes de Active IQ Unified Manager que debe tener en cuenta.

Informes existentes de versiones anteriores de Unified Manager

Solo es posible editar la programación y los destinatarios de los informes existentes que se hayan creado e importado (como archivos .rptdesign) en Unified Manager 9.5 y versiones anteriores. Si ha personalizado alguno de los informes estándar proporcionados en Unified Manager 9.5 o una versión anterior, estos informes personalizados no se importan en la nueva herramienta de generación de informes.

Si necesita editar informes existentes importados de archivos .rptdesign, realice una de las acciones siguientes y elimine el informe importado:

- crear una nueva vista y programar un informe desde esa vista (preferido)
- Pase el ratón sobre el informe, copie el SQL y extraiga los datos con una herramienta externa

Las vistas predeterminadas se pueden generar como informes sin necesidad de ninguna personalización. Puede usar la nueva solución de generación de informes para volver a crear los informes personalizados.

Relación de programación e informes

Puede crear muchas programaciones diferentes con cualquier combinación de destinatarios para cada informe guardado. Sin embargo, no puede reutilizar la programación para varios informes.

Protección de informes

Cualquier usuario con los permisos adecuados puede editar o eliminar informes. No hay forma de impedir que otros usuarios eliminen o realicen cambios en las vistas o horarios guardados.

Informes de eventos

Aunque puede personalizar la vista de eventos y descargar el informe resultante en formato CSV, no puede programar informes de eventos recurrentes para generación y distribución.

Archivos adjuntos de informes

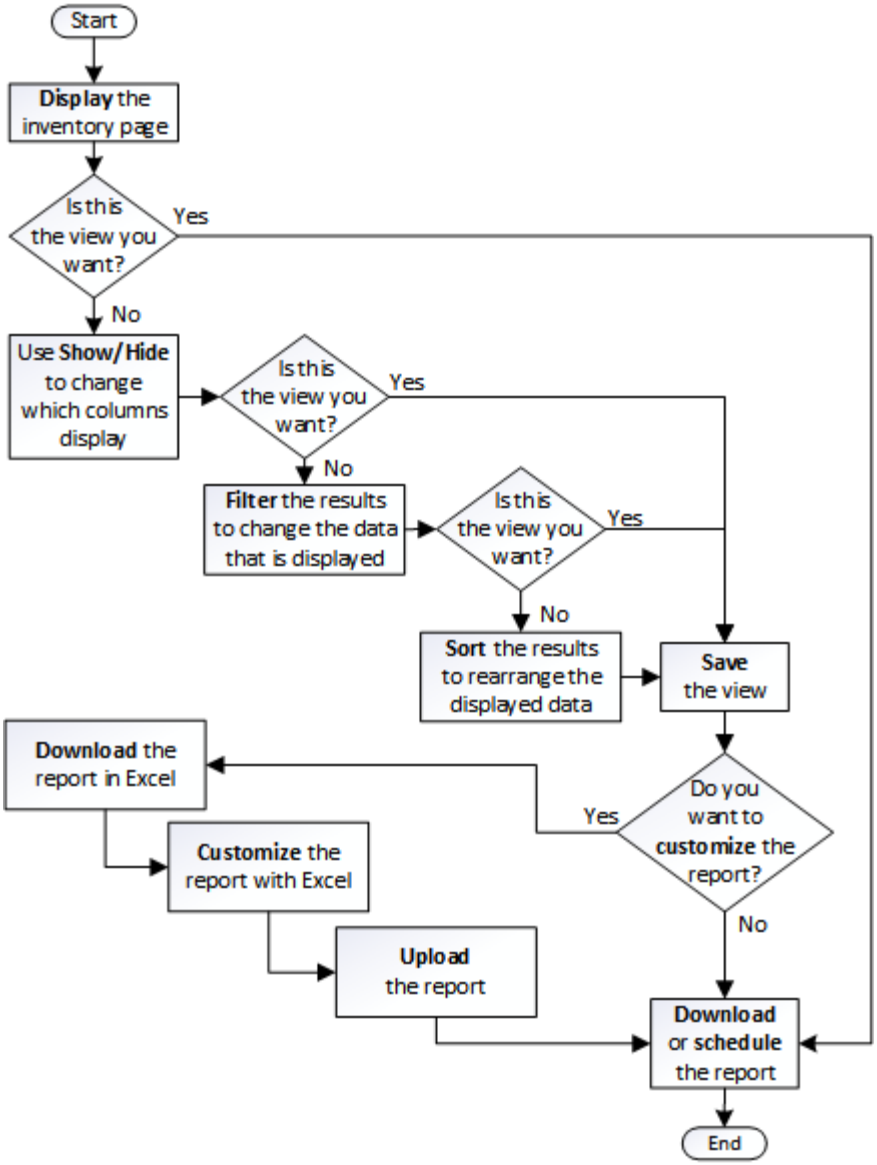
Los informes no se pueden enviar en el cuerpo de un correo electrónico. En su lugar, los informes sólo se envían como archivos PDF, Excel o CSV.

Trabajar con informes

Aprenda a buscar y personalizar las vistas de páginas de inventario en informes programados compartibles.

Flujo de trabajo de informes

Árbol de decisiones que describe el flujo de trabajo del informe.



Inicio rápido de informes

Cree un informe personalizado de ejemplo para disfrutar de la exploración de vistas e informes de programación. Este informe de inicio rápido encuentra una lista de volúmenes que es posible que desee mover al nivel de cloud porque hay una cantidad justa de datos inactivos (fríos). Se abrirá la vista rendimiento: Todos los volúmenes, se personalizará la vista con filtros y columnas, se guardará la vista personalizada como informe y se programará el informe para que se comparta una vez por semana.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado agregados de FabricPool y tener volúmenes en esos agregados.

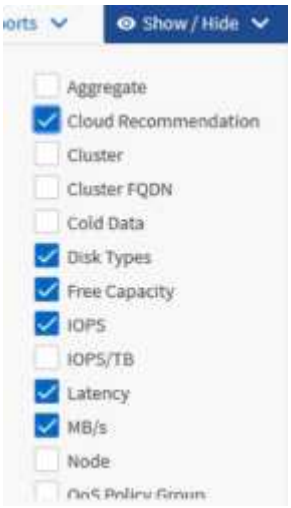
Siga estos pasos para:

- Abra la vista predeterminada

- Personalice las columnas filtrando y ordenando los datos
- Guarde la vista
- Programar un informe que se va a generar para la vista personalizada

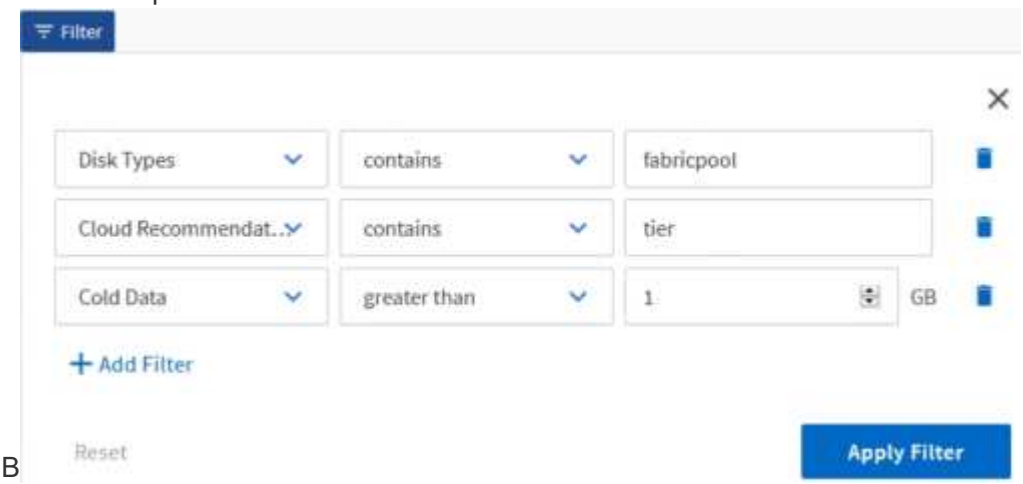
Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En el menú Ver, seleccione **rendimiento** > **todos los volúmenes**.
3. Haga clic en **Mostrar/Ocultar** para asegurarse de que la columna "tipos de disco" aparece en la vista.



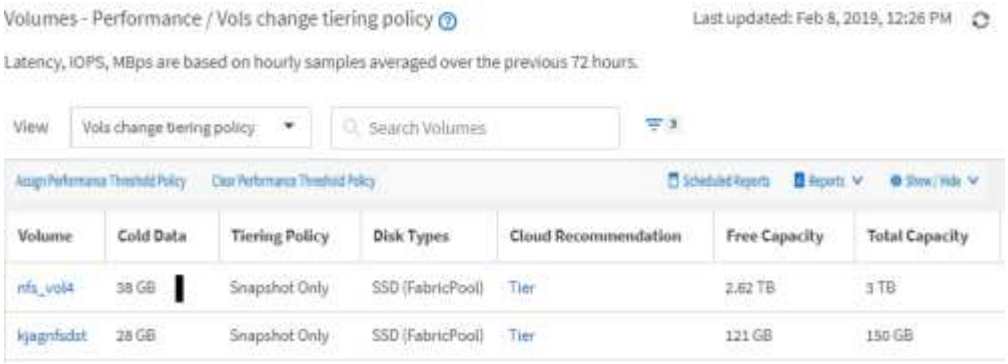
Agregue o elimine otras columnas para crear una vista que contenga los campos que son importantes para el informe.

4. Arrastre la columna "tipos de disco" situada junto a la columna "Recomendación sobre la nube".
5. Haga clic en el icono de filtro para agregar los tres filtros siguientes y, a continuación, haga clic en **aplicar filtro**:
   - Los tipos de disco contienen FabricPool
   - Las recomendaciones de cloud contienen nivel
   - Datos fríos superiores a 10 GB



Tenga en cuenta que cada filtro está Unido a un valor lógico Y que todos los volúmenes devueltos deben cumplir todos los criterios. Puede agregar un máximo de cinco filtros.

6. Haga clic en la parte superior de la columna datos fríos para ordenar los resultados de modo que los volúmenes con datos más fríos aparezcan en la parte superior de la vista.
7. Cuando la vista está personalizada, el nombre de la vista es Vista no guardada. Nombre la vista para reflejar lo que muestra la vista, por ejemplo «'Vols change Tiering policy»». Cuando haya terminado, haga clic en la Marca de verificación o pulse **Intro** para guardar la vista con el nuevo nombre.



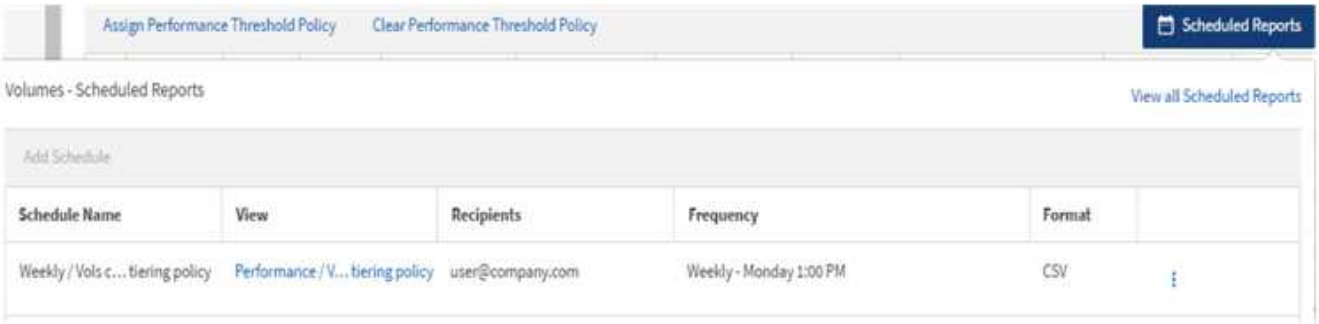
8. Descargue el informe como un archivo **CSV**, **Excel** o **PDF** para ver el resultado antes de programarlo o compartirlo.

   Abra el archivo con una aplicación instalada, como Microsoft Excel (CSV o Excel) o Adobe Acrobat (PDF), o guarde el archivo.

   > Puede personalizar aún más el informe utilizando filtros, ordenaciones, tablas dinámicas o gráficos complejos descargando la vista como un archivo de Excel. Después de abrir el archivo en Excel, utilice las funciones avanzadas para personalizar el informe. Cuando esté satisfecho, cargue el archivo de Excel. Este archivo, con sus personalizaciones, se aplica a la vista cuando se ejecuta el informe.

   Para obtener más información acerca de cómo personalizar informes con Excel, vea *Sample Microsoft Excel Reports*.

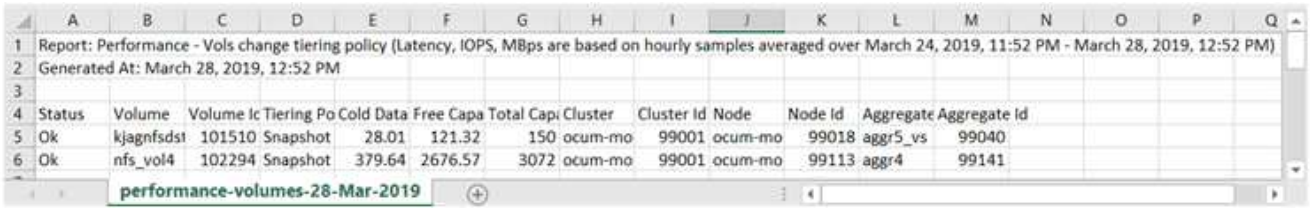
9. Haga clic en el botón **Informes programados** de la página de inventario. Todos los informes programados relacionados con el objeto, en este caso volúmenes, aparecen en la lista.



10. Haga clic en **Agregar programación** para agregar una nueva fila a la página programas de informes de modo que pueda definir las características de programación para el nuevo informe.
11. Introduzca un nombre para el informe y complete los demás campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

    El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

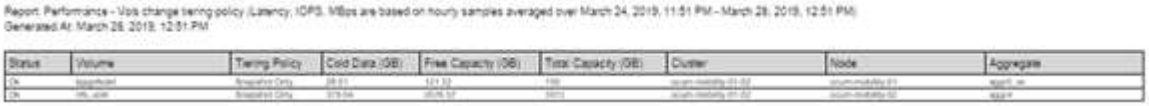
El siguiente informe de ejemplo tiene el formato CSV:



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:52 PM - March 28, 2019, 12:52 PM)																
2	Generated At: March 28, 2019, 12:52 PM																
3																	
4	Status	Volume	Volume Ic	Tiering Po	Cold Data	Free Capa	Total Capi	Cluster	Cluster Id	Node	Node Id	Aggregate	Aggregate Id				
5	Ok	kjagnfsdst	101510	Snapshot	28.01	121.32	150	ocum-mo	99001	ocum-mo	99018	aggr5_vs	99040				
6	Ok	nfs_vol4	102294	Snapshot	379.64	2676.57	3072	ocum-mo	99001	ocum-mo	99113	aggr4	99141				

performance-volumes-28-Mar-2019

El siguiente informe de ejemplo está en formato PDF:



Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:51 PM - March 28, 2019, 12:51 PM)
Generated At: March 28, 2019, 12:51 PM

Status	Volume	Tiering Policy	Cold Data (GB)	Free Capacity (GB)	Total Capacity (GB)	Cluster	Node	Aggregate
Ok								
Ok								

En función de los resultados mostrados en el informe, puede que desee utilizar System Manager de ONTAP o la interfaz de línea de comandos de ONTAP para cambiar la política de organización en niveles a «'auto» o «'all'» en determinados volúmenes para descargar más datos inactivos al nivel cloud.

Buscando un informe programado

Puede buscar informes programados por nombre, nombre de vista, tipo de objeto o destinatarios.

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **programas de informes**.
2. Utilice el campo de texto **Buscar informes programados**.

Para encontrar informes por …	Pruebe …
Nombre del programa	Escriba parte del nombre del programa del informe.
Nombre de la vista	Escriba parte del nombre de la vista de informe. Las vistas predeterminadas y las vistas personalizadas aparecen en la lista de vistas.
Destinatario	Escriba parte de la dirección de correo electrónico.
Tipo de archivo	Escriba "PDF", "CSV" o "XLSX".

3. Puede hacer clic en un encabezado de columna para ordenar los informes en orden ascendente o descendente por esa columna, como el nombre de la programación o el formato.

Personalización de informes

Existen muchas maneras de personalizar las vistas para que se pueda crear un informe que contenga toda la información necesaria para gestionar los clústeres de ONTAP.

Empiece por una página de inventario predeterminada o una vista personalizada y, a continuación, personalízala agregando o quitando columnas, cambiando el orden de las columnas, filtrando los datos o ordenando una columna específica en orden ascendente o descendente.

A partir de Unified Manager 9.8, también se puede descargar la vista en Excel para personalizarla mediante funciones avanzadas. Cuando termine, cargue el archivo de Excel personalizado. Si programa un informe con esa vista, utilizará el archivo de Excel personalizado para crear informes sólidos que pueda compartir.

Para obtener más información acerca de cómo personalizar informes con Excel, vea *Sample Microsoft Excel Reports*.

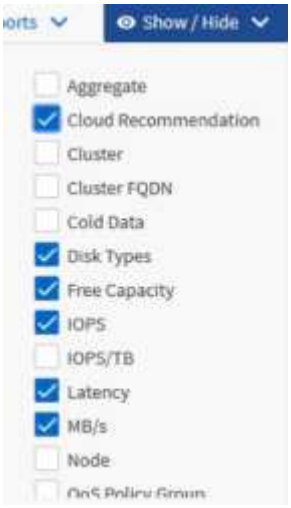
Para administrar informes, debe tener la función Administrador de aplicaciones o Administrador de almacenamiento.

Personalizar columnas

Utilice **Mostrar/Ocultar** para seleccionar las columnas que desea utilizar en el informe. Arrastre las columnas de la página de inventario para reorganizarlas.

Pasos

1. Haga clic en **Mostrar/Ocultar** para añadir o eliminar columnas.



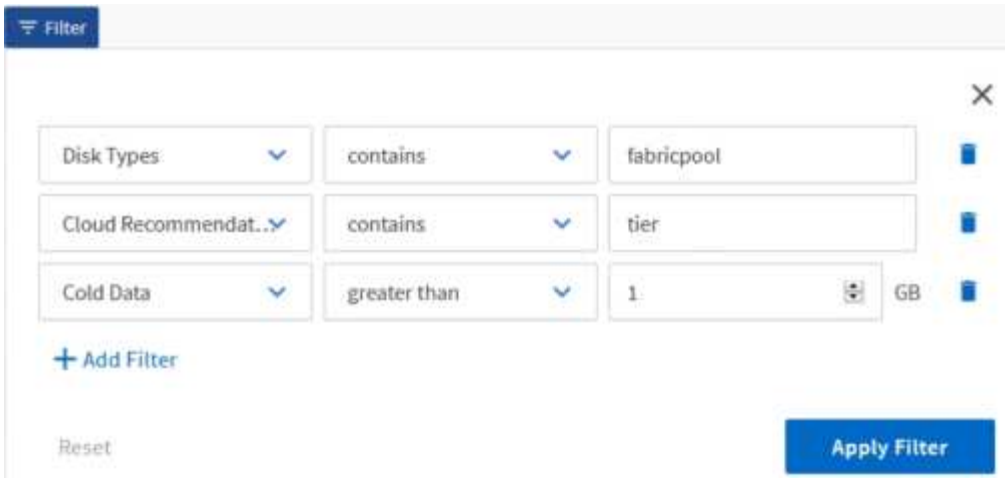
2. En la página de inventario, arrastre columnas para reorganizarlas en el orden que desee del informe.
3. Asigne un nombre a la vista sin guardar para guardar los cambios.

Filtrado de datos

Filtre los datos para asegurarse de que los resultados coinciden con los requisitos del informe. El filtrado le permite mostrar únicamente los datos que le interesen.

Pasos

1. Haga clic en el icono de filtro para agregar filtros para enfocar los resultados que desea ver y, a continuación, haga clic en **aplicar filtro**.



2. Asigne un nombre a la vista sin guardar para guardar los cambios.

Ordenar datos

Para ordenar los resultados, haga clic en una columna e indique el orden ascendente o descendente. Ordenar los datos da prioridad a la información que necesita para elaborar el informe.

Pasos

1. Haga clic en la parte superior de una columna para ordenar los resultados de modo que la información más importante aparezca en la parte superior de la vista.
2. Asigne un nombre a la vista sin guardar para guardar los cambios.

Uso de la búsqueda para afinar la vista

Una vez que tenga la vista deseada, puede afinar los resultados con el campo Buscar para centrarse en los resultados que desea incluir en el informe.

Pasos

1. Abra la vista personalizada o predeterminada que desea utilizar como base del informe.
2. Escriba el campo Buscar para afinar los datos que aparecen en la vista. Puede introducir datos parciales en cualquiera de las columnas mostradas. Por ejemplo, si desea buscar nodos que incluyan "US_East" en el nombre, puede afinar la lista completa de nodos.

   Los resultados de la búsqueda se guardan en la vista personalizada y se utilizan en el informe programado resultante.

3. Asigne un nombre a la vista sin guardar para guardar los cambios.

Uso de Excel para personalizar el informe

Una vez guardada la vista, puede descargarla en formato de libro de Excel (.xlsx). Al abrir el archivo de Excel, puede utilizar características avanzadas de Excel para personalizar el informe.

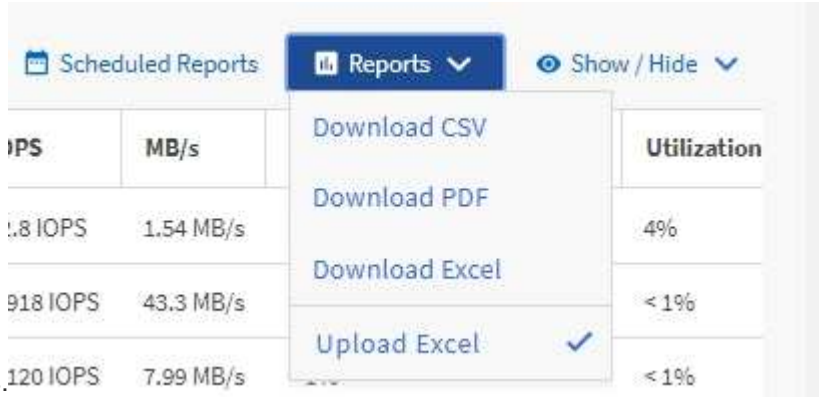
Lo que necesitará

Solo puede cargar un archivo de libro de Excel con la extensión .xlsx.

Por ejemplo, algunas de las características avanzadas de Excel que puede utilizar en el informe incluyen:

- Ordenación multicolumna
- Filtrado complejo
- Tablas dinámicas
- Gráficos

- El archivo de Excel descargado utiliza el nombre de archivo predeterminado para la vista, no el nombre guardado.
  - El formato es `<View Area>-<Day>-<Month>-<Year>-<Hour>-<Minute>-<Second>.xlsx`.
  - Por ejemplo, una vista guardada personalizada denominada `Volumes-not online` tiene un nombre de archivo de `health-volumes-05-May-2020-19-18-00.xlsx` si se guardan en ese día y hora.
- Puede agregar hojas al archivo de Excel, pero no cambiar las existentes.
  - No cambie las hojas, datos e información existentes. En su lugar, copie los datos en una página nueva que cree.
  - Una excepción a la regla anterior es que usted puede crear fórmulas en la página "data". Utilice las fórmulas de las páginas de datos para crear gráficos en páginas nuevas.
  - No asigne un nombre a una nueva hoja de datos o información.
- Si existe un archivo de Excel personalizado, hay una Marca de verificación junto al elemento de menú **Informes** > **cargar Excel**. Al descargar el archivo de Excel, se utiliza la versión con las



personalizaciones.

Pasos

1. Abra la vista predeterminada, personalizada o guardada que desee utilizar como base para el informe.
2. Seleccione **Informes** > **Descargar Excel**.
3. Guarde el archivo. El archivo se guarda en la carpeta de descargas.
4. Abra el archivo guardado en Excel. No mueva el archivo a una nueva ubicación o si realiza el trabajo en otra ubicación, vuelva a guardarlo en la ubicación original utilizando el nombre del archivo original antes de cargarlo.
5. Personalice el archivo utilizando características de Excel, como ordenaciones complejas, filtros con capas, tablas dinámicas o gráficos. Para obtener más información, consulte la documentación de Microsoft®

Excel.

6. Seleccione **Informes** > **cargar Excel** y seleccione el archivo que ha modificado. El archivo descargado más recientemente se carga desde la misma ubicación de archivo.
7. Envíe un informe de prueba utilizando la función **Informes programados**.

Descargando informes

Puede descargar informes y guardar los datos en una unidad local o de red como un archivo de valores separados por comas (CSV), un archivo de Microsoft Excel (.XLSX) o un archivo PDF. Puede abrir archivos CSV y XLSX con aplicaciones de hoja de cálculo, como Microsoft Excel, y archivos PDF con lectores como Adobe Acrobat.

Pasos

1. Haga clic en el botón **Informes** para descargar el informe como una de las siguientes opciones:

Seleccione	Para…
Descargue CSV	Guarde el informe como un archivo de valores separados por comas (CSV).
Descargar PDF	Guarde el informe como un archivo .pdf.
Descargue Excel	Guarde el informe como un archivo de Microsoft Excel (XLSX).

Programación de informes

Una vez que tenga la vista que desea reutilizar y compartir como un informe, puede programarla mediante Active IQ Unified Manager. Puede gestionar informes programados, cambiando los destinatarios y la frecuencia de distribución de cada programación de informes.

Es posible programar la mayoría de las vistas o páginas de inventario en Unified Manager. Las excepciones son eventos, que son informes que puede descargar como archivos CSV, pero no puede programar eventos para regeneración y uso compartido. Tampoco puede descargar ni programar los paneles, los favoritos ni las páginas de configuración.

A partir de Active IQ Unified Manager 9.8, puede descargar vistas en formato Microsoft® Excel y personalizarlas. Puede utilizar características avanzadas de Excel como ordenaciones complejas, filtros con capas, tablas dinámicas y gráficos. Cuando esté satisfecho con el informe de Excel resultante, puede cargar el archivo de Excel para utilizarlo cada vez que se programe y comparta el informe.

Puede programar las vistas incorporadas que desee personalizar. Puede elegir el tipo de archivo que desea enviar, ya sea CSV, PDF o XSLX. Cuando programe un informe por primera vez, puede descargarlo y asignarlo como el único destinatario para verlo como lo verán sus destinatarios.

Programar un informe

Después de tener una vista o un archivo de Excel que desee programar para la generación y distribución regulares, puede programar el informe.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado la configuración del servidor SMTP en la página **General** > **Notificaciones** para que el motor de informes pueda enviar informes como adjuntos de correo electrónico a la lista de destinatarios desde el servidor de Unified Manager.
- El servidor de correo electrónico debe configurarse para permitir el envío de archivos adjuntos con los correos electrónicos generados.

Utilice los pasos siguientes para probar y programar un informe que se generará para una vista. Seleccione o personalice la vista que desee usar. El procedimiento siguiente utiliza una vista de red que muestra el rendimiento de las interfaces de red, pero puede utilizar cualquier vista que desee.

Pasos

1. Abra la vista. En este ejemplo, se utiliza la vista de red predeterminada que muestra el rendimiento de la LIF. En el panel de navegación izquierdo, haga clic en **Red > interfaces de red**.
2. Personalice la vista según sea necesario con las funciones integradas de Unified Manager.
3. Después de personalizar la vista, puede proporcionar un nombre único en el campo **Ver** y hacer clic en la Marca de verificación para guardarla.

4. Puede utilizar las características avanzadas de Microsoft® Excel para personalizar el informe. Para obtener más información, consulte "Uso de Excel para personalizar el informe".
5. Para ver el resultado antes de programarlo o compartirlo:

Opción	Descripción
Si ha utilizado Excel para personalizar el informe	Ver el archivo de Excel descargado existente.
Si no ha utilizado Excel para personalizar el informe	Descargue el informe como un archivo **CSV**, **PDF** o **XLSX**.

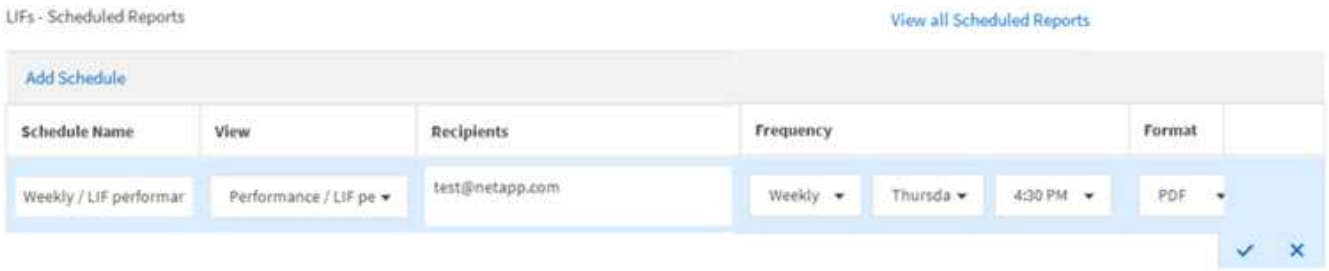
   Abra el archivo con una aplicación instalada, como Microsoft Excel (CSV/XSLX) o Adobe Acrobat (PDF).

6. Si está satisfecho con el informe, haga clic en **Informes programados**.
7. En la página programas de informes, haga clic en **Agregar programación**.
8. Acepte el nombre predeterminado, que es una combinación del nombre de la vista y la frecuencia, o personalice el **nombre de la programación**.
9. Para probar el informe programado por primera vez, agregue sólo como **destinatario**. Cuando esté satisfecho, agregue las direcciones de correo electrónico para todos los destinatarios del informe.

10. Especifique con qué frecuencia se generará y enviará el informe a los destinatarios. Puede elegir **Diario**, **Semanal** o **Mensual**.
11. Seleccione el formato **PDF**, **CSV** o **XSLX**.

    Para los informes en los que utilizó Excel para personalizar el contenido, seleccione siempre **XSLX**.

12. Haga clic en la Marca de verificación (✓) para guardar la programación del informe.



El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia programada.

Programar informes .rptdesign importados

Es posible programar los informes existentes que se crearon e importaron en una versión anterior de Unified Manager.

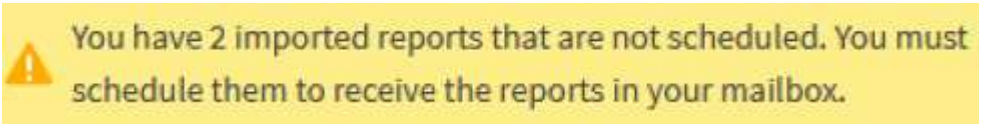
La programación de informes importados requiere lo siguiente:

- Se importaron informes de archivos .rptdesign diseñados por BIRT en una versión anterior de Unified Manager
- Esto se aplica cuando se actualiza a Unified Manager 9.6 GA o posterior

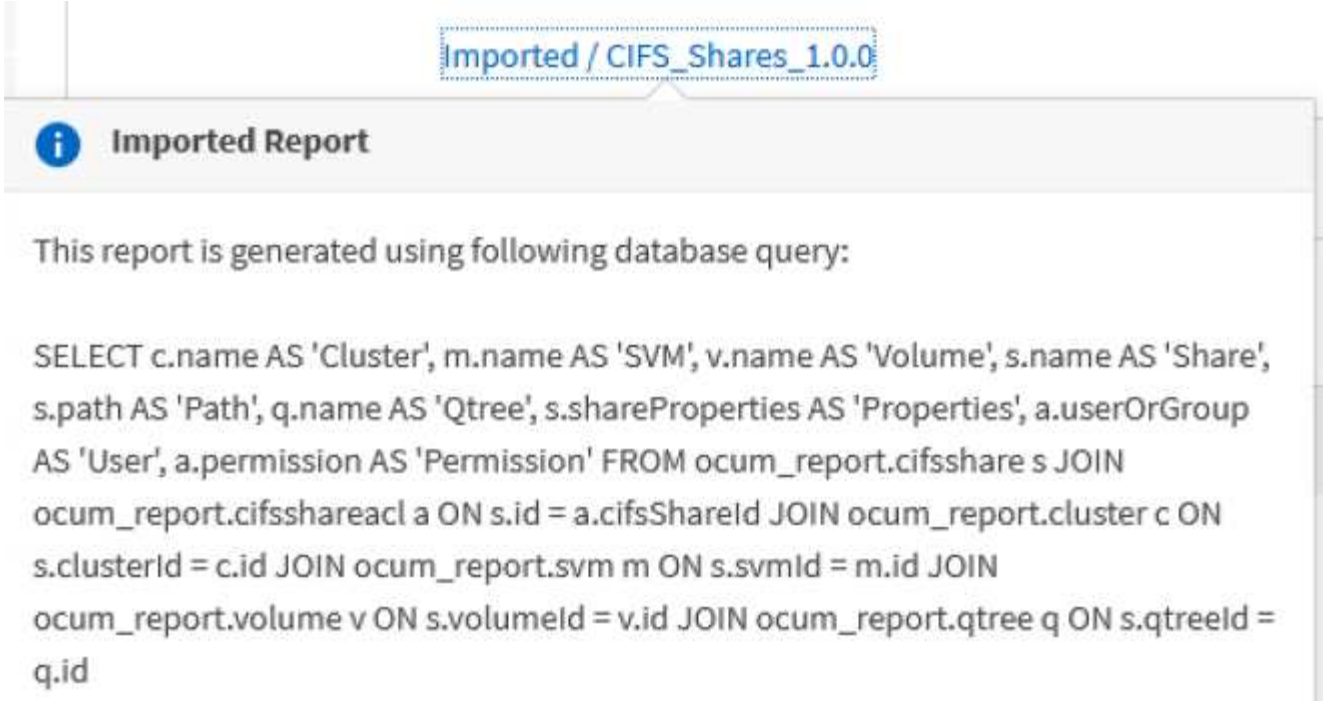
Después de actualizar a Unified Manager 9.6 GA o una versión posterior, la página Report Schedules enumera los informes importados. Puede editar la programación de estos informes para especificar las direcciones de correo electrónico, la frecuencia y el formato de los destinatarios (PDF o CSV). De lo contrario, estos informes no se pueden editar ni ver en la interfaz de usuario de Unified Manager.

Pasos

1. Abra la página programas de informes. Si ha importado informes, aparece un mensaje.



2. Haga clic en el nombre **View** para mostrar la consulta SQL que se utiliza para generar el informe.



3. Haga clic en el icono más ⋮, Haga clic en **Editar**, defina los detalles de la programación del informe y guarde el informe.

   También puede eliminar los informes no deseados del icono más ⋮.

Gestión de programas de informes

Las programaciones de informes se pueden gestionar desde la página Report Schedules. Es posible ver, modificar o eliminar programaciones existentes.

Lo que necesitará

No es posible programar nuevos informes desde la página Report Schedules. Sólo puede agregar informes programados desde las páginas de inventario de objetos.

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **programas de informes**.
2. En la página Report Schedules:

Si desea…	Realice lo siguiente…
Ver una programación existente	Desplácese por la lista de informes existentes con las barras de desplazamiento y los controles de página.

Si desea…	Realice lo siguiente…
Editar una programación existente	a. Haga clic en el icono más ⋮ para la programación que desea usar. b. Haga clic en **Editar**. c. Realice los cambios necesarios. d. Haga clic en la Marca de verificación para guardar los cambios.
Eliminar una programación existente	a. Haga clic en el icono más ⋮ para la programación que desea usar. b. Haga clic en **Eliminar**. c. Confirme su decisión.

Edición de informes programados

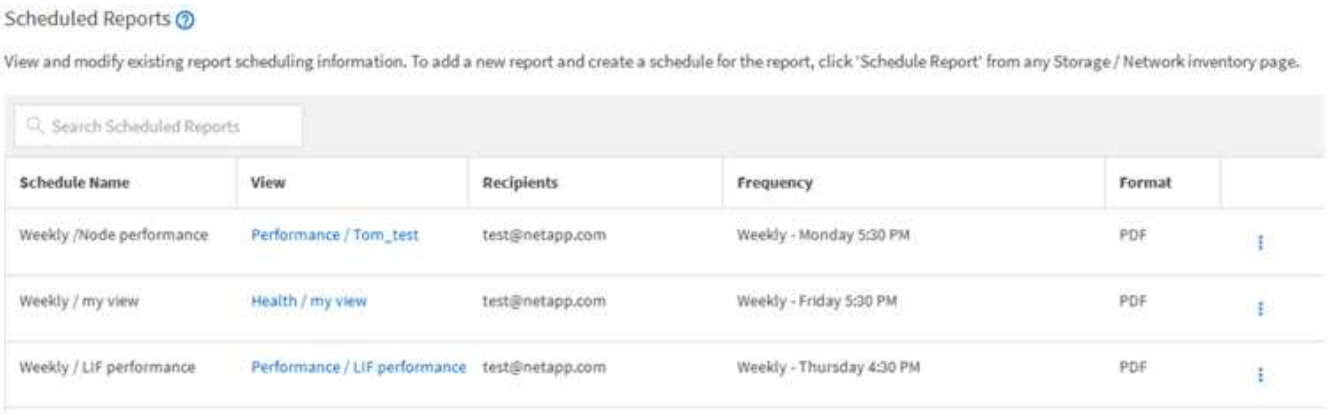
Después de programar los informes, puede editarlos en la página programas de informes.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **programas de informes**.



Si dispone de los permisos adecuados, puede modificar cualquier informe y su programación en el sistema.

2. Haga clic en el icono más ⋮ para la programación que desea cambiar.
3. Haga clic en **Editar**.
4. Puede cambiar la lista **Nombre de programa**, **destinatario**, **frecuencia** y **Formato** para el programa de informes.

5. Cuando haya terminado, haga clic en la Marca de verificación para guardar los cambios.

Eliminar informes programados

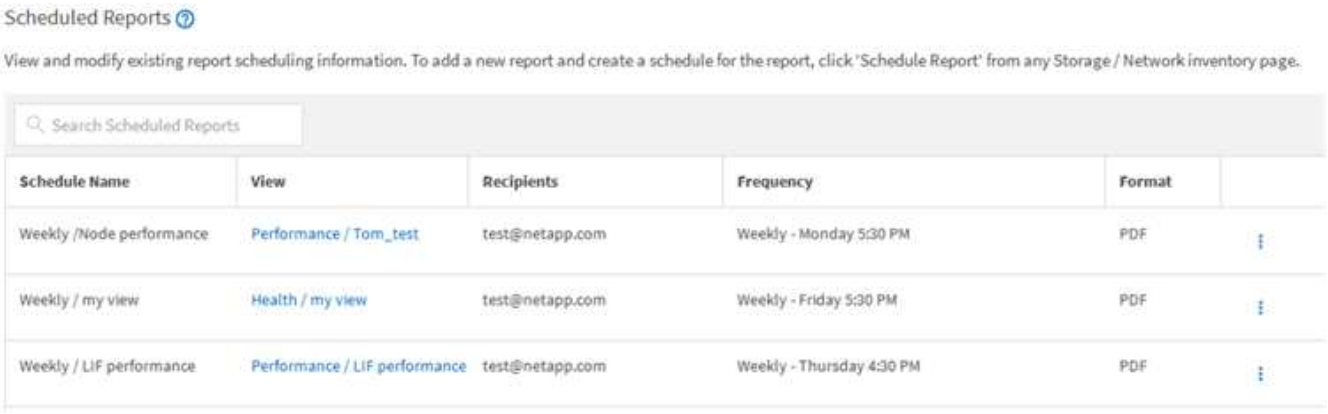
Una vez programados los informes, puede eliminarlos de la página programas de informes.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Pasos

1. En el panel de navegación izquierdo, haga clic en **Administración de almacenamiento** > **programas de informes**.



Si dispone de los permisos adecuados, puede eliminar cualquier informe y su programación en el sistema.

2. Haga clic en el icono más ⋮ para la programación que desea eliminar.
3. Haga clic en **Eliminar**.
4. Confirme su decisión.

   El informe programado se elimina de la lista y ya no se generará ni distribuirá en el programa establecido.

Si elimina una vista personalizada de la página de inventario, también se eliminarán los archivos de Excel personalizados o los informes programados que utilicen esa vista.

Informes personalizados de muestra

Estos informes personalizados de ejemplo se utilizan normalmente para ayudar a identificar problemas potenciales y responder a problemas potenciales antes de que se produzcan problemas.

La lista de informes de esta sección no es exhaustiva y aumentará con el tiempo. Puede sugerir informes personalizados para añadir a esta sección mediante comentarios en la documentación.

Para administrar informes, debe tener la función Administrador de aplicaciones o Administrador de almacenamiento.

Personalizar informes de almacenamiento de clúster

Los informes de almacenamiento de clúster de ejemplo de esta sección son solo muestras que le ayudan a comprender la forma de crear informes sobre la capacidad de los clústeres para ayudarle a supervisar los recursos del sistema de almacenamiento.

Creación de un informe para ver la capacidad por modelo de clúster

Puede crear un informe para analizar la capacidad de almacenamiento y la utilización de los clústeres según el modelo del sistema de almacenamiento.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Use los siguientes pasos para crear una vista personalizada que muestra la capacidad según el modelo de clúster y, a continuación, programar un informe que se generará para esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **clústeres**.
2. En el menú Ver, seleccione **capacidad** > **todos los clústeres**.
3. Seleccione **Mostrar/Ocultar** para eliminar cualquier columna, como "'Cluster FQDN'" y "'Versión del SO'", que no desee en el informe.
4. Arrastre la «capacidad bruta total», «Model/Familia» y las tres columnas agregadas cerca de la columna «Cluster».
5. Haga clic en la parte superior de la columna "Model/Familia" para ordenar los resultados por tipo de cluster.
6. Guarde la vista con un nombre específico que refleje lo que muestra la vista, por ejemplo, «'capacidad por modelo de clúster'».
7. Haga clic en el botón **Informes programados** de la página de inventario.
8. Haga clic en **Agregar programación** para agregar una nueva fila a la página **programas de informes** de modo que pueda definir las características de programación para el nuevo informe.
9. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

   El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Según los resultados mostrados en el informe, quizás desee añadir más capacidad a determinados clústeres o actualizar modelos de clústeres anteriores.

Cree un informe para identificar los clústeres con la capacidad de LUN más sin asignar

Puede crear un informe para encontrar los clústeres con la capacidad LUN más sin asignar, mayor de 0,5 TB, para ayudar a identificar dónde puede añadir cargas de trabajo

adicionales.

Lo que necesitará * debe tener la función Administrador de aplicaciones o Administrador de almacenamiento.

Utilice los siguientes pasos para crear una vista personalizada que muestra los clústeres con la capacidad de LUN más sin asignar y, a continuación, programe un informe que se genere para esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **clústeres**.
2. En el menú Ver, seleccione **capacidad** > **todos los clústeres**.
3. Seleccione **Mostrar/Ocultar** para eliminar las columnas que no desee del informe.
4. Arrastre la columna «'capacidad LUN no asignada'» cerca de la columna «'par ha'».
5. Haga clic en el icono de filtro, agregue el siguiente filtro y, a continuación, haga clic en **aplicar filtro**:
   - Capacidad de LUN sin asignar mayor a 0.5 TB
6. Haga clic en la parte superior de la columna «'capacidad de LUN no asignada'» para ordenar los resultados según la mayor cantidad de capacidad de LUN sin asignar.
7. Guarde la vista con un nombre específico que refleje lo que se muestra en la vista, por ejemplo, «más capacidad de LUN sin asignar» y haga clic en la Marca de verificación (✓).
8. Haga clic en el botón **Informes programados** de la página de inventario.
9. Haga clic en **Agregar programación** para agregar una nueva fila a la página programas de informes de modo que pueda definir las características de programación para el nuevo informe.
10. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

    El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Según los resultados que se muestran en el informe, podría utilizar la capacidad LUN sin asignar del clúster.

Crear un informe para ver los pares de alta disponibilidad con la capacidad más disponible

Puede crear un informe para encontrar los pares de alta disponibilidad con la mayor capacidad para aprovisionar nuevos volúmenes y LUN.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Utilice los siguientes pasos para crear una vista personalizada que muestre parejas de alta disponibilidad ordenadas por la capacidad más disponible para aprovisionar volúmenes y LUN nuevos y, a continuación, programar un informe para que se genere para esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **clústeres**.
2. En el menú Ver, seleccione **capacidad** > **todos los clústeres**.
3. Seleccione **Mostrar/Ocultar** para eliminar las columnas que no desee del informe.
4. Arrastre la columna «'capacidad no utilizada agregada'» cerca de la columna «'par ha'».

5. Haga clic en el icono de filtro, agregue el siguiente filtro y, a continuación, haga clic en **aplicar filtro**:
   - Capacidad no utilizada del agregado superior a 0.5 TB
6. Haga clic en la parte superior de la columna «"capacidad no utilizada agregada"» para ordenar los resultados por la mayor cantidad de capacidad agregada no utilizada.
7. Guarde la vista con un nombre específico que refleje lo que se muestra en la vista, por ejemplo, «"capacidad agregada mínima utilizada»» y haga clic en la Marca de verificación (✓).
8. Haga clic en el botón **Informes programados** de la página de inventario.
9. Haga clic en **Agregar programación** para agregar una nueva fila a la página programas de informes de modo que pueda definir las características de programación para el nuevo informe.
10. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

    El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

En función de los resultados mostrados en el informe, tal vez le interese equilibrar los pares de alta disponibilidad en función de la capacidad de los agregados.

Crear un informe para ver los nodos que ejecutan versiones anteriores de ONTAP

Puede crear un informe para mostrar la versión del software ONTAP que está instalada en todos los nodos del clúster de modo que pueda ver qué nodos debe actualizar.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Use los siguientes pasos para crear una vista personalizada que muestre los nodos que ejecutan versiones anteriores de ONTAP y, a continuación, programar un informe para que se genere en esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **nodos**.
2. Seleccione **Mostrar/Ocultar** para quitar las columnas que no desee del informe.
3. Arrastre la columna «'OS Version'» cerca de la columna «'Node'».
4. Haga clic en la parte superior de la columna "'Versión del SO'" para ordenar los resultados por la versión más antigua de ONTAP.
5. Guarde la vista con un nombre específico que refleje lo que muestra la vista, por ejemplo, «'Nodes by ONTAP version'».
6. Haga clic en el botón **Informes programados** de la página de inventario.
7. Haga clic en **Agregar programación** para agregar una nueva fila a la página programas de informes de modo que pueda definir las características de programación para el nuevo informe.
8. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

   El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Según los resultados que se muestran en el informe, quizás desee actualizar nodos que ejecutan versiones anteriores de ONTAP.

Personalizar los informes de capacidad de agregados

Estos informes personalizados de muestra se utilizan para ayudarle a identificar y responder a problemas potenciales relacionados con la capacidad de almacenamiento agregada.

Los informes de esta sección son solo muestras que le ayudarán a comprender la forma de crear informes sobre la capacidad de agregado con el fin de ayudarle a supervisar los recursos del sistema de almacenamiento.

Creación de un informe para ver los agregados que alcanzan la capacidad completa

Puede crear un informe para encontrar los agregados que están alcanzando toda su capacidad, de tal modo que pueda añadir más capacidad o mover cargas de trabajo a otros agregados.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Utilice los siguientes pasos para crear una vista personalizada donde se muestren los agregados que alcanzan su capacidad completa y, a continuación, programar un informe que se generará para esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **agregados**.
2. En el menú Ver, seleccione **capacidad** > **todos los agregados**.
3. Seleccione **Mostrar/Ocultar** para eliminar las columnas que no desee del informe.
4. Haga clic en el icono de filtro, agregue el siguiente filtro y, a continuación, haga clic en **aplicar filtro**:
   - Días a completo menos de 45 días
5. Haga clic en la parte superior de la columna "Days to Full" para ordenar los resultados por el número mínimo de días restantes para alcanzar la capacidad completa.
6. Guarde la vista con un nombre específico que refleje lo que se muestra en la vista, por ejemplo, "días a capacidad agregada completa" y haga clic en la Marca de verificación (✓).
7. Haga clic en el botón **Informes programados** de la página de inventario.
8. Haga clic en **Agregar programación** para agregar una nueva fila a la página **programas de informes** de modo que pueda definir las características de programación para el nuevo informe.
9. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

   El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

De acuerdo con los resultados que se muestran en el informe, quizás desee aumentar el almacenamiento de agregados que alcanzan su capacidad completa. Además, es posible que desee aumentar los días hasta que el umbral de capacidad completa supere los 7 días predeterminados para recibir eventos que proporcionen

más tiempo para reaccionar ante el espacio que llega a reducir en los agregados.

Creación de un informe para ver agregados del 80 % o más completos

Puede crear un informe para resaltar los agregados que estén un 80 % o más completos.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Siga estos pasos para crear una vista personalizada que muestre agregados del 80 % o más completos y, a continuación, programe un informe para su generación.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **agregados**.
2. En el menú Ver, seleccione **capacidad** > **todos los agregados**.
3. Seleccione **Mostrar/Ocultar** para eliminar las columnas que no desee del informe.
4. Arrastre las columnas «'% de datos disponibles'» y « % de datos usados» cerca de la columna «'agregado'».
5. Haga clic en el icono de filtro, agregue los siguientes filtros y, a continuación, haga clic en **aplicar filtro**:
   - % De datos usados es mayor que 80 %
6. Haga clic en la parte superior de la columna "'datos usados %'" para ordenar los resultados por porcentaje de capacidad.
7. Guarde la vista con un nombre específico que refleje lo que se muestra en la vista, por ejemplo, "'agregados casi completos'" y haga clic en la Marca de verificación (✓) .
8. Haga clic en el botón **Informes programados** de la página de inventario.
9. Haga clic en **Agregar programación** para agregar una nueva fila a la página programas de informes de modo que pueda definir las características de programación para el nuevo informe.
10. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

    El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Basándose en los resultados mostrados en el informe, quizás desee mover algunos datos de ciertos agregados.

Creación de un informe para ver los agregados que están sobrecomprometidos

Puede crear un informe para analizar la capacidad de almacenamiento y el uso de los agregados, así como para ver los agregados comprometidos en exceso.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Utilice los pasos siguientes para crear una vista personalizada que muestre los agregados que superan el umbral de exceso de compromiso y, a continuación, programe un informe que se genere para esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **agregados**.
2. En el menú Ver, seleccione **capacidad** > **todos los agregados**.
3. Seleccione **Mostrar/Ocultar** para quitar las columnas que no desee del informe.
4. Arrastre la columna «'% de capacidad sobrecomprometida'» cerca de la columna «'agregado'».
5. Haga clic en el icono de filtro, agregue los siguientes filtros y, a continuación, haga clic en **aplicar filtro**:
   - El % de capacidad sobrecomprometida es superior al 100 %
6. Haga clic en la parte superior de la columna «'% de capacidad sobrecomprometida'» para ordenar los resultados por porcentaje de capacidad.
7. Guarde la vista con un nombre específico que refleje lo que se muestra en la vista, por ejemplo, "'agregados comprometidos'" y haga clic en la Marca de verificación (✓).
8. Haga clic en el botón **Informes programados** de la página de inventario.
9. Haga clic en **Agregar programación** para agregar una nueva fila a la página programas de informes de modo que pueda definir las características de programación para el nuevo informe.
10. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

    El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

En función de los resultados que se muestran en el informe, puede que desee añadir más capacidad a agregados o mover algunos datos de ciertos agregados.

Personalización de los informes de capacidad de volúmenes

Estos informes personalizados de muestra se utilizan para ayudar a identificar y responder a problemas potenciales relacionados con la capacidad de volumen y el rendimiento.

Creación de un informe para identificar volúmenes que están casi por completo y que tienen desactivada la eliminación automática de Snapshot

Puede crear un informe que contenga la lista de volúmenes que se esté acercando a su capacidad completa con la función Snapshot Autodelete deshabilitada. Los resultados pueden ayudar a identificar volúmenes en los que se podría configurar la eliminación automática de instantánea.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Siga los pasos que se indican a continuación para crear una vista personalizada que muestre las columnas necesarias en el orden correcto y, a continuación, programe un informe que se genere para esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En el menú Ver, seleccione **capacidad** > **todos los volúmenes**.

3. Seleccione **Mostrar/Ocultar** para eliminar las columnas que no desee del informe.
4. Arrastre y suelte las columnas "Snapshot Autodelete" y "Days to Full" cerca de la columna "'Available Data Capacity".
5. Haga clic en el icono de filtro, agregue los dos filtros siguientes y, a continuación, haga clic en **aplicar filtro**:
   - Días a completo menos de 30 días
   - La eliminación automática de instantáneas está deshabilitada
6. Haga clic en la parte superior de la columna **días a Full** para que los volúmenes con menos días restantes aparezcan en la parte superior de la lista.
7. Guarde la vista con un nombre específico que refleje lo que muestra la vista, por ejemplo «'Vols near Capacity»».
8. Haga clic en el botón **Informes programados** de la página de inventario.
9. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

   El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

En función de los resultados mostrados en el informe, quizás desee habilitar la eliminación automática de instantánea en los volúmenes o buscar una forma de aumentar el espacio disponible.

Creación de un informe para identificar el espacio utilizado por los volúmenes con thin provisioning deshabilitado

Cuando no hay thin provisioning, un volumen ocupa toda la cantidad de espacio en el disco, tal y como se define cuando se creó el volumen. La identificación de volúmenes con thin provisioning deshabilitado ayuda a decidir si se desea habilitar el aprovisionamiento ligero en ciertos volúmenes.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Siga los pasos que se indican a continuación para crear una vista personalizada que muestre las columnas necesarias en el orden correcto y, a continuación, programe un informe que se genere para esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En el menú Ver, seleccione **capacidad** > **todos los volúmenes**.
3. Seleccione **Mostrar/Ocultar** para eliminar las columnas que no desee del informe.
4. Arrastre y suelte las columnas «% de datos usados» y «Thin Provisioned» cerca de la columna «capacidad de datos disponible».
5. Haga clic en el icono de filtro, agregue el siguiente filtro, **Thin Provisioned** es **no** y, a continuación, haga clic en **aplicar filtro**.
6. Haga clic en la parte superior de la columna "'datos usados %'" para ordenar los resultados de modo que los volúmenes con el porcentaje más alto aparezcan en la parte superior de la lista.

7. Guarde la vista con un nombre para reflejar lo que muestra la vista, por ejemplo «'Vols no thin provisioning»».
8. Haga clic en el botón **Informes programados** de la página de inventario.
9. Haga clic en **Agregar programación** para agregar una nueva fila a la página **programas de informes** para poder definir las características de programación para el nuevo informe.
10. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

    El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Según los resultados mostrados en el informe, quizás desee habilitar thin provisioning en ciertos volúmenes.

Creación de un informe para identificar volúmenes en agregados de FabricPool que deben mover datos al nivel de cloud

Puede crear un informe que contenga la lista de volúmenes que residen actualmente en agregados de FabricPool, que tienen una recomendación de nivel cloud y que tienen una gran cantidad de datos inactivos. Este informe puede ayudarle a decidir si debería cambiar la política de organización en niveles de determinados volúmenes a «auto» o «all» para descargar más datos inactivos (inactivos) al nivel cloud.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.
- Debe haber configurado agregados de FabricPool y tener volúmenes en esos agregados.

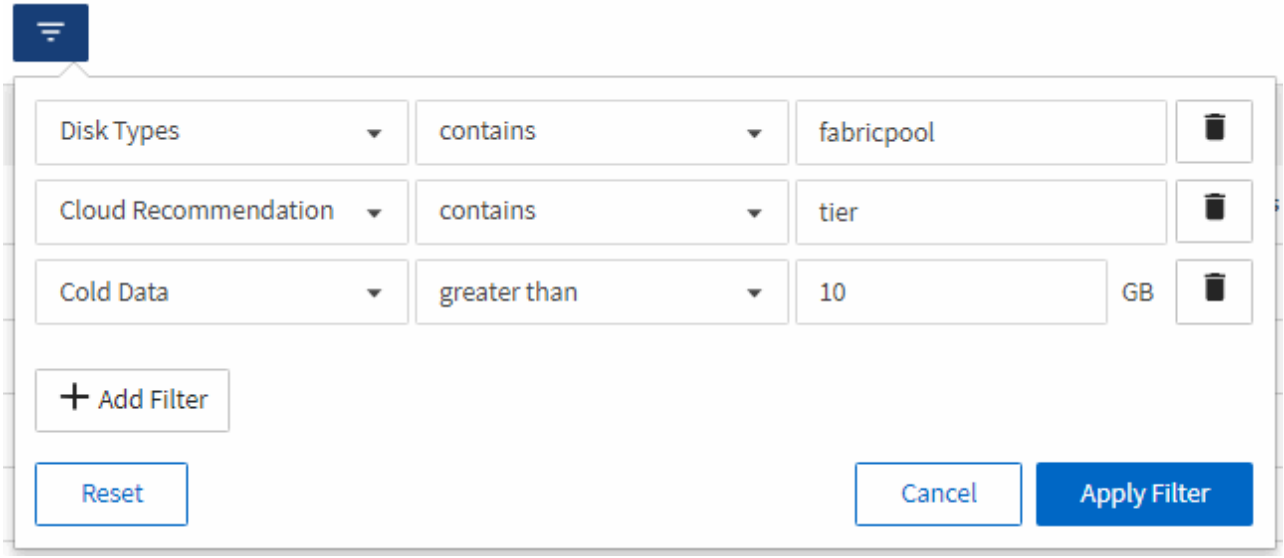
Siga los pasos que se indican a continuación para crear una vista personalizada que muestre las columnas necesarias en el orden correcto y, a continuación, programe un informe que se genere para esa vista.

Pasos

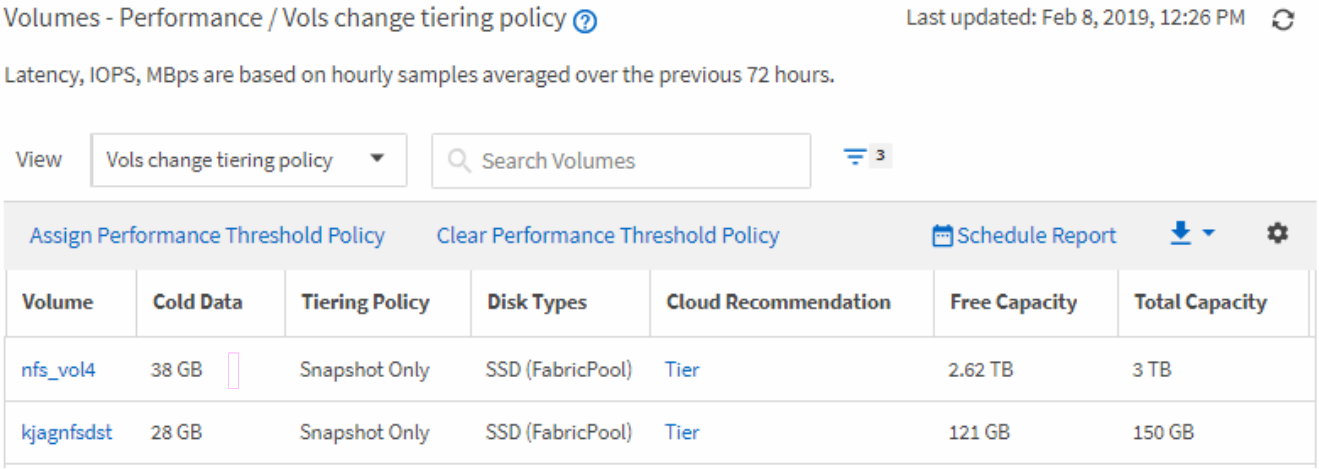
1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En el menú Ver, seleccione **rendimiento** > **todos los volúmenes**.
3. En el selector de columnas, asegúrese de que la columna "Tipo disco" aparece en la vista.

   Agregue o elimine otras columnas para crear una vista que sea importante para el informe.

4. Arrastre y suelte la columna "Tipo de disco" situada cerca de la columna "Recomendación de nube".
5. Haga clic en el icono de filtro, agregue los tres filtros siguientes y, a continuación, haga clic en **aplicar filtro**:
   - El tipo de disco contiene FabricPool
   - Las recomendaciones de cloud contienen nivel
   - Datos fríos superiores a 10 GB



6. Haga clic en la parte superior de la columna datos fríos para que los volúmenes con más datos fríos aparezcan en la parte superior de la vista.
7. Guarde la vista con un nombre para reflejar lo que muestra la vista, por ejemplo «'Política de cambio de Vols».



8. Haga clic en el botón **Informes programados** de la página de inventario.
9. Haga clic en **Agregar programación** para agregar una nueva fila a la página programas de informes de modo que pueda definir las características de programación para el nuevo informe.
10. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

    El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

En función de los resultados mostrados en el informe, puede que desee utilizar System Manager o la interfaz de línea de comandos de ONTAP para cambiar la política de organización en niveles a «'auto» o «'all'» en determinados volúmenes para descargar más datos inactivos al nivel cloud.

Personalizar los informes de capacidad de Qtree

Estos informes personalizados de ejemplo se utilizan para ayudarle a identificar y responder a los posibles problemas relacionados con la capacidad de Qtree.

Creación de un informe para ver qtrees que están casi llenos

Puede crear un informe para analizar la capacidad de almacenamiento y el uso de qtrees, y ver qtrees que están casi llenos.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Siga los pasos siguientes para crear una vista personalizada que muestre qtrees que están casi llenos y, a continuación, programar un informe que se generará para esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **Qtrees**.
2. Seleccione **Mostrar/Ocultar** para eliminar las columnas que no desee del informe.
3. Arrastre la columna "% utilizado" cerca de la columna "Qtrees".
4. Haga clic en el icono de filtro, agregue los siguientes filtros y, a continuación, haga clic en **aplicar filtro**:
   - El % del disco utilizado es superior al 75 %
5. Haga clic en la parte superior de la columna "disco utilizado %" para ordenar los resultados por porcentaje de capacidad.
6. Guarde la vista con un nombre específico que refleje lo que se muestra en la vista, por ejemplo, "'Qtrees está casi lleno'" y haga clic en la Marca de verificación (✓).
7. Haga clic en el botón **Informes programados** de la página de inventario.
8. Haga clic en **Agregar programación** para agregar una nueva fila a la página **programas de informes** para poder definir las características de programación para el nuevo informe.
9. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

   El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

En función de los resultados mostrados en el informe, es posible que desee ajustar los límites estrictos y flexibles del disco (si se ha establecido) o equilibrar los datos en los qtrees.

Personalización de informes de recursos compartidos de NFS

Puede personalizar los informes de recursos compartidos de NFS para analizar información sobre las reglas y políticas de exportación de NFS para volúmenes en sus sistemas de almacenamiento. Por ejemplo, se pueden personalizar los informes para que se muestren volúmenes con rutas de montaje no accesibles y volúmenes con la política de exportación predeterminada.

Creación de un informe para ver los volúmenes con una ruta de montaje inaccesible

Es posible crear un informe para encontrar volúmenes con una ruta de montaje inaccesible.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Use los siguientes pasos para crear una vista personalizada para volúmenes que tienen una ruta de montaje inaccesible y luego programar un informe para generar ese informe.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **recursos compartidos NFS**.
2. Seleccione **Mostrar/Ocultar** para quitar las columnas que no desee del informe.
3. Haga clic en el icono de filtro, agregue el siguiente filtro y, a continuación, haga clic en **aplicar filtro**:
   - La ruta de montaje activa no es
4. Guarde la vista con un nombre específico que refleje lo que se muestra en la vista, por ejemplo "'volúmenes con una ruta de montaje inaccesible'" y haga clic en la Marca de verificación (✓).
5. Haga clic en el botón **Informes programados** de la página de inventario.
6. Haga clic en **Agregar programación** para agregar una nueva fila a la página programas de informes de modo que pueda definir las características de programación para el nuevo informe.
7. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

   El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Según los resultados que se muestran en el informe, es posible que desee corregir las rutas de montaje inaccesibles.

Creación de un informe para ver los volúmenes que utilizan la política de exportación predeterminada

Puede crear un informe para buscar volúmenes con la política de exportación predeterminada.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Use los siguientes pasos para crear una vista personalizada para los volúmenes que utilizan la política de exportación predeterminada y, a continuación, programar un informe que se generará para esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **recursos compartidos NFS**.
2. Seleccione **Mostrar/Ocultar** para quitar las columnas que no desee del informe.
3. Arrastre la columna «'Política de exportación» situada cerca de la columna «'volumen»».
4. Haga clic en el icono de filtro, agregue el siguiente filtro y, a continuación, haga clic en **aplicar filtro**:
   - La directiva de exportación contiene el valor predeterminado
5. Guarde la vista con un nombre específico que refleje lo que se muestra en la vista, por ejemplo «'volúmenes con una política de exportación predeterminada'» y haga clic en la Marca de verificación (✓).
6. Haga clic en el botón **Informes programados** de la página de inventario.
7. Haga clic en **Agregar programación** para agregar una nueva fila a la página programas de informes de modo que pueda definir las características de programación para el nuevo informe.

8. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

   El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Basándose en los resultados mostrados en el informe, se recomienda configurar una política de exportación personalizada.

Personalizar los informes de VM de almacenamiento

Puede crear informes de equipos virtuales de almacenamiento para analizar información del volumen y ver el estado y la disponibilidad generales del almacenamiento. Por ejemplo, puede crear informes para mostrar las SVM que han alcanzado el número máximo de volúmenes y analizar las SVM detenidas.

Creación de un informe para ver las máquinas virtuales de almacenamiento que alcanzan el límite máximo de volumen

Puede crear un informe para encontrar las SVM que alcanzan el límite máximo de volumen.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Siga los siguientes pasos para crear una vista personalizada que muestre las máquinas virtuales de almacenamiento que alcanzan el límite máximo de volúmenes y, a continuación, programar un informe para que se genere en esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **Storage VMs**.
2. Seleccione **Mostrar/Ocultar** para eliminar las columnas que no desee del informe.
3. Arrastre las columnas «'número de volumen» y «máximo volumen permitido» cerca de la columna «máquina virtual de almacenamiento».
4. Haga clic en la parte superior de la columna "volumen máximo permitido" para ordenar los resultados por el número más alto de volúmenes.
5. Guarde la vista con un nombre específico que refleje lo que se muestra en la vista, por ejemplo, «MVMs Reaching max volumes»» y haga clic en la Marca de verificación (✓).
6. Haga clic en el botón **Informes programados** de la página de inventario.
7. Haga clic en **Agregar programación** para agregar una nueva fila a la página **programas de informes** de modo que pueda definir las características de programación para el nuevo informe.
8. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

   El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Según los resultados mostrados en el informe, quizás desee equilibrar los volúmenes asignados a equipos

virtuales de almacenamiento o, si es posible, usar System Manager de ONTAP para cambiar el número máximo permitido de volúmenes.

Crear un informe para ver las máquinas virtuales de almacenamiento detenidas

Puede crear un informe para mostrar una lista de todas las SVM detenidas.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Use los siguientes pasos para crear una vista personalizada que muestre las máquinas virtuales de almacenamiento detenidas y luego programar un informe que se generará para esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **Storage VMs**.
2. En el menú Ver, seleccione **Estado** > **todas las VM de almacenamiento**.
3. Seleccione **Mostrar/Ocultar** para quitar las columnas que no desee del informe.
4. Arrastre la columna «Estado» cerca de la columna «máquina virtual de almacenamiento».
5. Haga clic en el icono de filtro, agregue el siguiente filtro y, a continuación, haga clic en **aplicar filtro**:
   - El estado se ha detenido
6. Guarde la vista con un nombre específico que refleje lo que se muestra en la vista, por ejemplo, "SVM con encabezado" y haga clic en la Marca de verificación (✓).
7. Haga clic en el botón **Informes programados** de la página de inventario.
8. Haga clic en **Agregar programación** para agregar una nueva fila a la página **programas de informes** de modo que pueda definir las características de programación para el nuevo informe.
9. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

   El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Según los resultados mostrados en el informe, quizás desee investigar por qué se ha detenido la SVM para que vea si debe reiniciar las SVM detenidas.

Personalización de los informes de relaciones de volumen

El informe Volume Relationships Inventory permite analizar los detalles del inventario de almacenamiento en un clúster, conocer el grado de protección necesario para los volúmenes y filtrar los detalles del volumen en función del origen del error, el patrón y las programaciones.

Creación de un informe para agrupar relaciones de volumen por origen de error

Es posible crear un informe que agrupa volúmenes por el motivo que la relación está en estado incorrecto.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Use los siguientes pasos para crear una vista personalizada que agrupa volúmenes por origen de un error y, a continuación, programa la generación de un informe para esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En el menú Ver, seleccione **relación** > **todas las relaciones**.
3. Seleccione **Mostrar/Ocultar** para asegurarse de que las columnas «'Salud de la relación'» y «'razón no saludable'» aparecen en la vista.

   Agregue o elimine otras columnas para crear una vista que sea importante para el informe.
4. Arrastre las columnas «Salud de la relación» y «razón no saludable» cerca de la columna «Estado».
5. Haga clic en el icono de filtro, agregue el siguiente filtro y, a continuación, haga clic en **aplicar filtro**:
   - La salud de la relación es mala
6. Haga clic en la parte superior de la columna "'razón no saludable'" para agrupar las relaciones de volumen por origen del fallo.
7. Guarde la vista con un nombre específico que refleje lo que muestra la vista, por ejemplo, "'Relaciones vol por fallo'".
8. Haga clic en el botón **Informes programados** de la página de inventario.
9. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

   El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Basándose en los resultados mostrados en el informe, puede investigar la fuente y el impacto de cada tipo de fallo.

Creación de un informe para agrupar relaciones de volumen por problema

Es posible crear un informe que agrupa las relaciones de volumen por problema.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Utilice los siguientes pasos para crear una vista personalizada que agrupa las relaciones de volumen por problema y, a continuación, programa que se generará un informe para esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En el menú Ver, seleccione **relación** > **todas las relaciones**.
3. Seleccione **Mostrar/Ocultar** para eliminar las columnas que no desee del informe.
4. Arrastre la columna "'razón no saludable'" cerca de la columna "Estado".
5. Haga clic en la parte superior de la columna "'razón no saludable'" para agrupar los volúmenes por emisión.

6. Guarde la vista con un nombre específico que refleje lo que muestra la vista, por ejemplo, "'Relaciones de vol por problema'".
7. Haga clic en el botón **Informes programados** de la página de inventario.
8. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

   El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Basándose en los resultados mostrados en el informe, puede investigar la fuente y el impacto de cada tipo de problema.

Creación de un informe para ver las tendencias de transferencia de volumen en intervalos de tiempo específicos

Se puede crear un informe que muestre las tendencias de transferencia de volumen en intervalos de tiempo específicos.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Use los siguientes pasos para crear una vista personalizada de los volúmenes en intervalos de tiempo específicos y luego programar la generación de un informe para esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En el menú Ver, seleccione **relación** > **Estado de transferencia de último 1 mes**.
3. Seleccione **Mostrar/Ocultar** para eliminar las columnas que no desee del informe.
4. Arrastre la columna duración de la transferencia cerca de la columna "'Resultado operativo'".
5. Haga clic en el icono de filtro, agregue el siguiente filtro y, a continuación, haga clic en **aplicar filtro**:
   - Hora de finalización de la transferencia en los últimos 7 días
6. Haga clic en la parte superior de la columna "'duración de la transferencia'" para ordenar los volúmenes por intervalo de tiempo.
7. Guarde la vista con un nombre específico que refleje lo que se muestra en la vista, por ejemplo «'volúmenes por duración'».
8. Haga clic en el botón **Informes programados** de la página de inventario.
9. Introduzca un nombre para el programa de informes, establezca la frecuencia como **Semanal** y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

   El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Basándose en los resultados mostrados en el informe, puede investigar los intervalos de tiempo de transferencia.

Creación de un informe para ver una transferencia de volumen con errores o correctamente

Es posible crear un informe que muestre el estado de las transferencias de volúmenes. En este informe se pueden ver tanto las transferencias de volúmenes con errores como las correctas.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Utilice los pasos siguientes para crear una vista personalizada para mostrar qué transferencias han fallado y cuáles se han realizado correctamente y, a continuación, programe un informe que se generará para esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En el menú Ver, seleccione **relación** > **Estado de transferencia de último 1 mes**.
3. Seleccione **Mostrar/Ocultar** para quitar las columnas que no desee del informe.
4. Arrastre la columna "'Resultado de la operación'" cerca de la columna "Estado".
5. Haga clic en la parte superior de la columna "'Resultado de la operación'" para ordenar los volúmenes por el estado.
6. Guarde la vista con un nombre específico que refleje lo que se muestra en la vista, por ejemplo «'volúmenes por estado de transferencia'».
7. Haga clic en el botón **Informes programados** de la página de inventario.
8. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

   El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

En función de los resultados mostrados en el informe, puede investigar el estado de la transferencia.

Creación de un informe para ver las transferencias de volumen en función del tamaño de la transferencia

Es posible crear un informe para ver las transferencias de volumen en función del tamaño de la transferencia.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Utilice los siguientes pasos para crear una vista personalizada para las transferencias de volúmenes en función del tamaño de transferencia y, a continuación, programar un informe para que se genere en esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En el menú Ver, seleccione **relación** > **velocidad de transferencia de último 1 mes**.
3. Haga clic en la parte superior de la columna "'Tamaño total de transferencia'" para ordenar las transferencias de volumen por tamaño.

4. Guarde la vista con un nombre específico que refleje lo que se muestra en la vista, por ejemplo «'volúmenes por tamaño de transferencia'».
5. Haga clic en el botón **Informes programados** de la página de inventario.
6. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

   El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Según los resultados mostrados en el informe, puede investigar las relaciones de volumen por tamaño de transferencia.

Creación de un informe para ver las transferencias de volumen agrupadas por día

Es posible crear un informe para ver las transferencias de volúmenes agrupadas por día.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Use los siguientes pasos para crear una vista personalizada para las transferencias de volúmenes agrupadas por día y, a continuación, programar que se genere un informe para esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En el menú Ver, seleccione **relación** > **velocidad de transferencia de último 1 mes**.
3. Haga clic en la parte superior de la columna "Day" para ordenar las transferencias de volumen por día.
4. Guarde la vista con un nombre específico que refleje lo que se muestra en la vista, por ejemplo «'transferencias por volumen por día'».
5. Haga clic en el botón **Informes programados** de la página de inventario.
6. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

   El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Según los resultados mostrados en el informe, puede investigar las transferencias de volúmenes por día.

Personalización de los informes de rendimiento de volúmenes

Estos informes personalizados de muestra se utilizan para ayudarle a identificar y responder a problemas potenciales relacionados con el rendimiento de los volúmenes.

Crear un informe para ver volúmenes con una gran cantidad de datos fríos en un agregado que no está habilitado para FabricPool

Puede crear un informe para mostrar volúmenes con una gran cantidad de datos fríos en un agregado que no pertenece a FabricPool. Esto puede ayudarle a identificar los volúmenes que se deben mover a un agregado de FabricPool.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Use los siguientes pasos para crear una vista personalizada de volúmenes con una gran cantidad de datos inactivos en un agregado que no tiene habilitada la función FabricPool y, a continuación, programar un informe para que se genere para esa vista.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. En el menú Ver, seleccione **rendimiento** > **todos los volúmenes**.
3. Seleccione **Mostrar/Ocultar** para asegurarse de que la columna "Tipo disco" aparece en la vista.

   Agregue o elimine otras columnas para crear una vista que sea importante para el informe.

4. Arrastre la columna "Tipo disco" cerca de la columna "'datos fríos".
5. Haga clic en el icono de filtro, agregue el siguiente filtro y, a continuación, haga clic en **aplicar filtro**:
   - Datos fríos superiores a 100 GB
   - El tipo de disco contiene SSD
6. Haga clic en la parte superior de la columna "Tipo de disco" para ordenar los volúmenes por tipo de disco de forma que el tipo de disco SSD (FabricPool) esté en la parte inferior.
7. Guarde la vista con un nombre específico que refleje lo que muestra la vista, por ejemplo «'volos de datos fríos no FabricPool».
8. Haga clic en el botón **Informes programados** de la página de inventario.
9. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

   El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Según los resultados mostrados en el informe, puede encontrar volúmenes que sean candidatos válidos para moverlos a agregados de FabricPool.

Informes de ejemplo de Microsoft Excel

Estos informes de ejemplo de Microsoft Excel tienen como objetivo introducir opciones de generación de informes disponibles mediante las características avanzadas de Excel.

La funcionalidad avanzada de Excel puede crear una amplia gama de informes específicos a sus necesidades. Para obtener información completa sobre cómo utilizar Excel, consulte la documentación del producto.

Para administrar informes, debe tener la función Administrador de aplicaciones o Administrador de almacenamiento.

Creación de un informe para mostrar un gráfico y una tabla de capacidad agregada

Puede crear un informe para analizar la capacidad de un archivo de Excel utilizando

totales sumados y el formato de gráfico de columnas agrupadas.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Siga estos pasos para abrir una vista Estado: Todos los agregados, descargar la vista en Excel, crear un gráfico de capacidad disponible, cargar el archivo de Excel personalizado y programar el informe final.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **agregados**.
2. Seleccione **Informes** > **Descargar Excel**.

   Según el explorador, es posible que tenga que hacer clic en **Aceptar** para guardar el archivo.

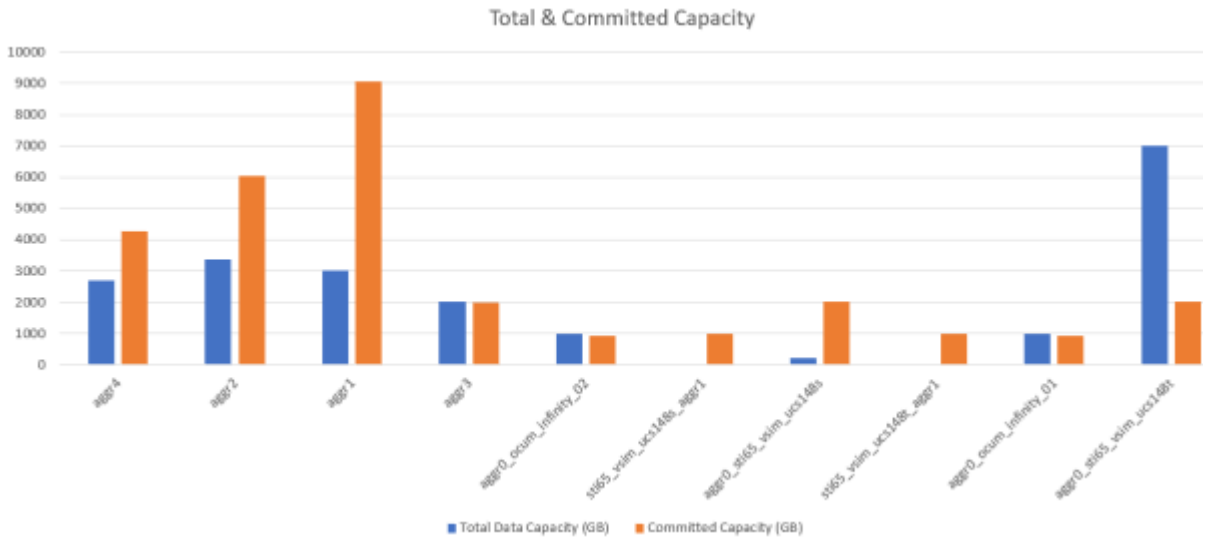
3. Si es necesario, haga clic en **Activar edición**.
4. En Excel, abra el archivo descargado.
5. Crear una nueva hoja (⊕) después del `data` Sheet y nombra **capacidad total de datos**.
6. Agregue las siguientes columnas en la nueva hoja capacidad total de datos:
   a. Capacidad de datos total (GB)
   b. Capacidad proporcionada (GB)
   c. Capacidad de datos utilizada (GB)
   d. Capacidad de datos disponible (GB)
7. En la primera fila de cada columna, introduzca la siguiente fórmula, asegurándose de que hace referencia a la hoja de datos (¡datos!) y hace referencia a los especificadores de fila y columna correctos para los datos capturados (capacidad total de datos obtiene datos de la columna E, filas 2 a 20).

   a. =SUMA(datos!E$2:datos!E$20)
   b. =SUMA(datos!F$2:datos!F$50)
   c. =SUMA(datos!G$2:datos!G$50)
   d. =SUMA(datos!H$2:datos!H$50)

   La fórmula suma cada columna en función de los datos actuales.

Total Data Capacity (GB)	Committed Capacity (GB)	Used Data Capacity (GB)	Available Data Capacity (GB)
5380.31	6892.47	11764.27	3911.03

1. En la hoja de datos, seleccione las columnas **capacidad total de datos (GB)** y **capacidad comprometida (GB)**.
2. Seleccione **Cartas recomendadas** en el menú **Insertar** y seleccione el gráfico **columna en clúster**.
3. Haga clic con el botón derecho del ratón en el gráfico y seleccione **mover gráfico** para mover el gráfico `Total Data Capacity` hoja.
4. Mediante los menús **Diseño** y **Formato**, que están disponibles cuando se selecciona el gráfico, puede personalizar el aspecto del gráfico.
5. Cuando esté satisfecho, guarde el archivo con los cambios. No cambie el nombre ni la ubicación del archivo.

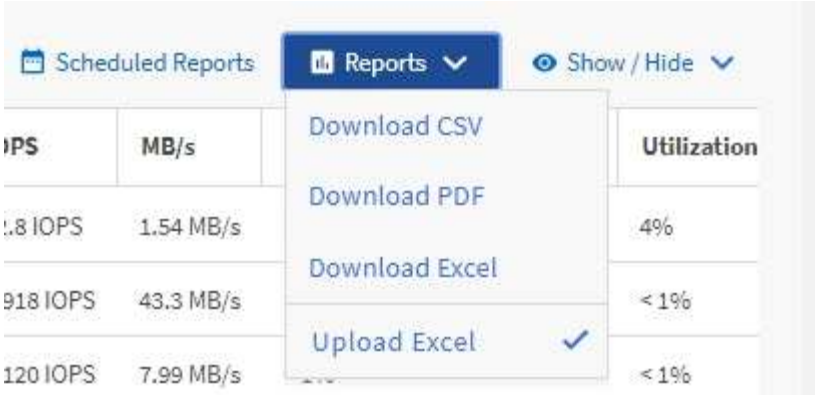


6. En Unified Manager, seleccione **Informes** > **cargar Excel**.

   Asegúrese de que se encuentra en la misma vista en la que descargó el archivo de Excel.

7. Seleccione el archivo de Excel que ha modificado.
8. Haga clic en **Abrir**.
9. Haga clic en **Enviar**.

   Aparece una Marca de verificación junto al elemento de menú **Informes** > **cargar Excel**.



10. Haga clic en **Informes programados**.
11. Haga clic en **Agregar programación** para agregar una nueva fila a la página programas de informes de modo que pueda definir las características de programación para el nuevo informe.

    Seleccione el formato **XLSX** para el informe.

12. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

    El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Basándose en los resultados mostrados en el informe, quizás desee investigar cómo utilizar de mejor forma la capacidad disponible en toda la red.

Creación de un informe para mostrar los gráficos de capacidad total agregado frente a los disponibles

Puede crear un informe para analizar el total de almacenamiento y la capacidad comprometida en un formato de gráfico de Excel.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

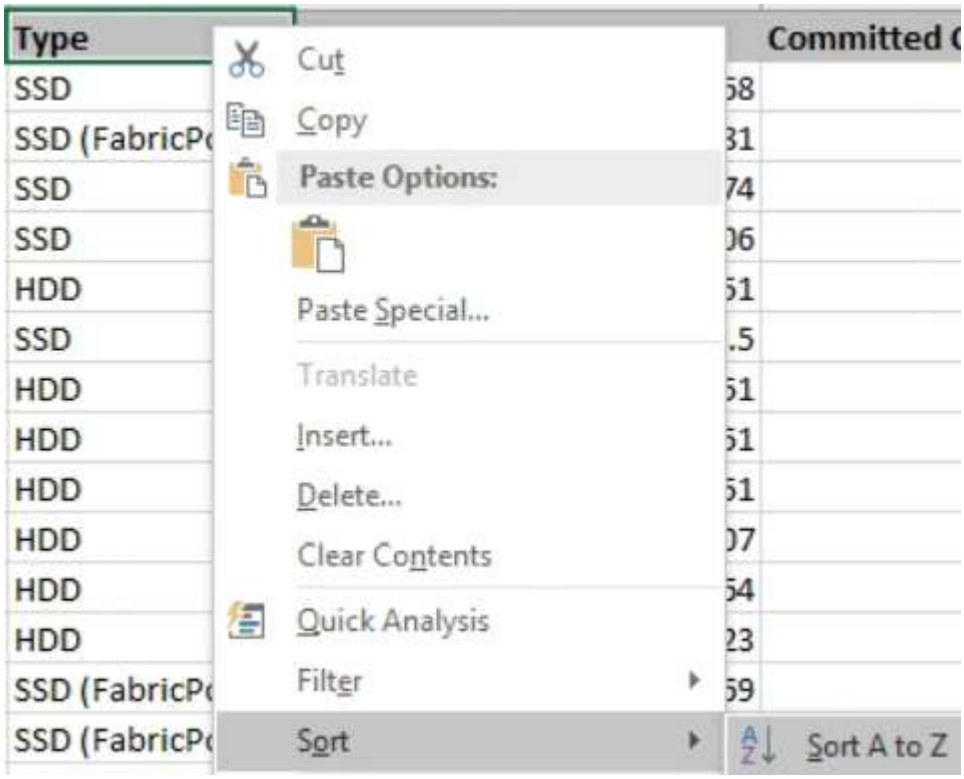
Siga estos pasos para abrir una vista Estado: Todos los agregados, descargar la vista en Excel, crear un gráfico de capacidad total y comprometida, cargar el archivo de Excel personalizado y programar el informe final.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **agregados**.
2. Seleccione **Informes** > **Descargar Excel**.

Según el explorador, es posible que tenga que hacer clic en **Aceptar** para guardar el archivo.

3. En Excel, abra el archivo descargado.
4. Si es necesario, haga clic en **Activar edición**.
5. En la hoja de datos, haga clic con el botón derecho del ratón en la columna Tipo y seleccione **Ordenar** > **Ordenar De La A a la Z**.



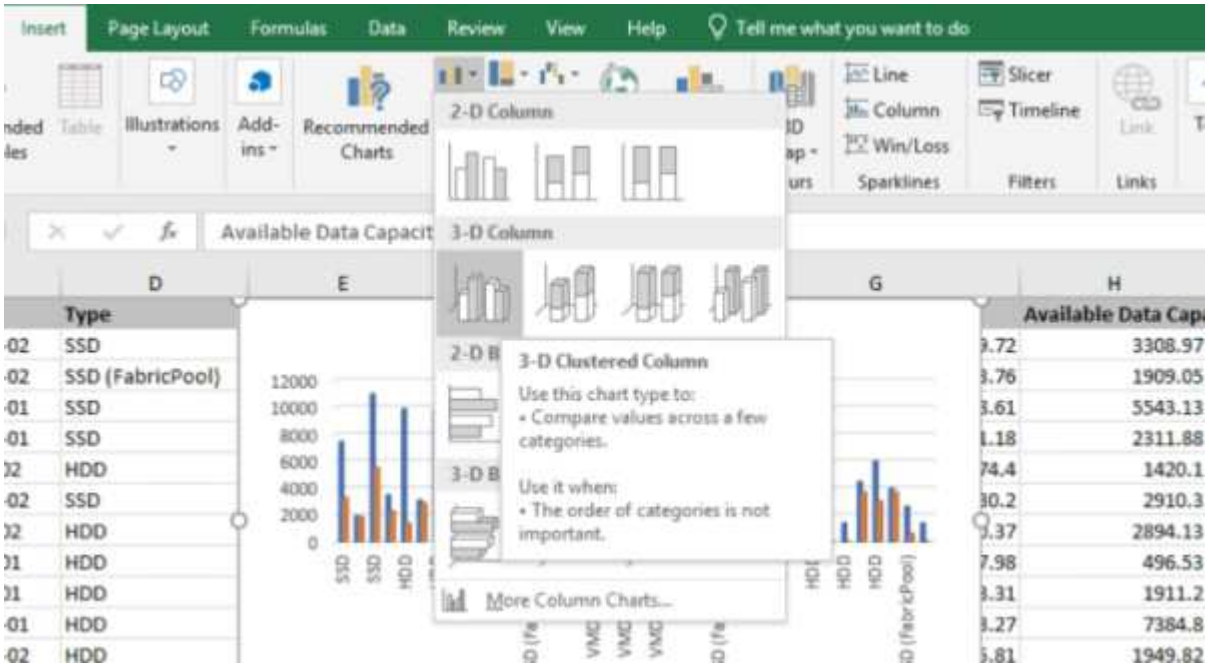
Esto organizará sus datos por tipo de almacenamiento, como:

- HDD
- Híbrido
- SSD
- SSD (FabricPool)

6. Seleccione la `Type, Total Data Capacity,` y.. `Available Data Capacity` columnas.

7. En el menú **Insertar**, seleccione un `3-D column` carta.

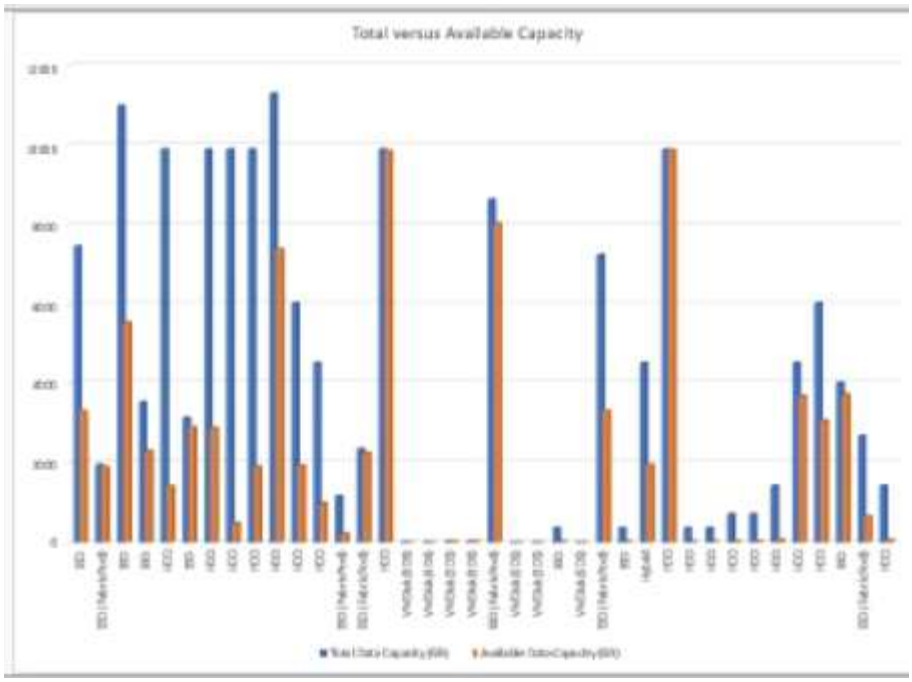
   El gráfico aparece en la hoja de datos.



8. Haga clic con el botón derecho del ratón en el gráfico y seleccione **mover gráfico**.
9. Seleccione **Nueva hoja** y asigne un nombre a la hoja **total Storage Charts**.

   Asegúrese de que la nueva hoja aparece después de las hojas de información y datos.

10. Nombre el título del gráfico **total frente a la capacidad disponible**.
11. Con los menús **Diseño** y **Formato**, disponibles cuando se selecciona el gráfico, puede personalizar el aspecto del gráfico.
12. Cuando esté satisfecho, guarde el archivo con los cambios. No cambie el nombre ni la ubicación del archivo.

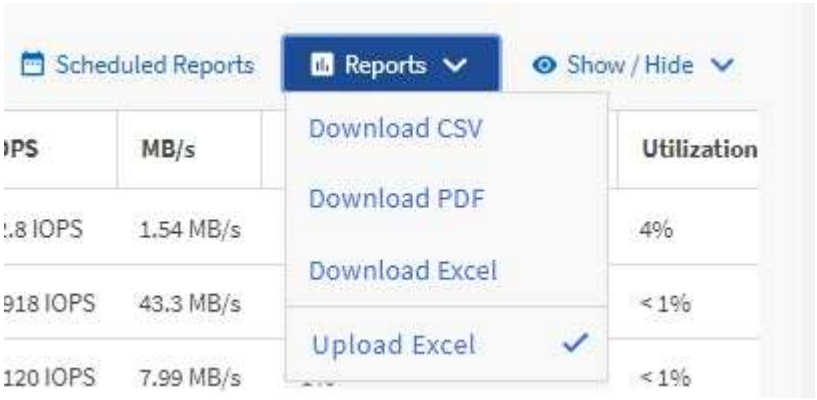


13. En Unified Manager, seleccione **Informes** > **cargar Excel**.

    Asegúrese de que se encuentra en la misma vista en la que descargó el archivo de Excel.

14. Seleccione el archivo de Excel que ha modificado.
15. Haga clic en **Abrir**.
16. Haga clic en **Enviar**.

    Aparece una Marca de verificación junto al elemento de menú **Informes** > **cargar Excel**.



17. Haga clic en **Informes programados**.
18. Haga clic en **Agregar programación** para agregar una nueva fila a la página **programas de informes** de modo que pueda definir las características de programación para el nuevo informe.

    Seleccione el formato **XLSX** para el informe.

19. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Según los resultados mostrados en el informe, quizás desee equilibrar la carga en los agregados.

Creación de un informe para ver los gráficos de capacidad de los volúmenes disponibles

Puede crear un informe para analizar la capacidad de volumen disponible en un gráfico de Excel.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Utilice los pasos siguientes para abrir una vista Estado: Todos los volúmenes, descargar la vista en Excel, crear un gráfico de capacidad disponible, cargar el archivo de Excel personalizado y programar el informe final.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **volúmenes**.
2. Seleccione **Informes** > **Descargar Excel**.

   Según el explorador, es posible que tenga que hacer clic en **Aceptar** para guardar el archivo.

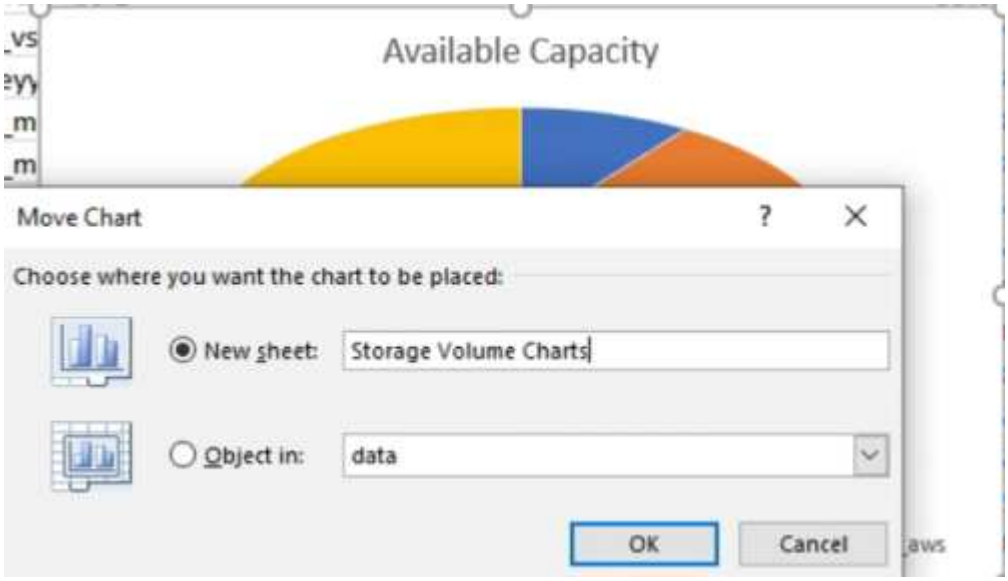
3. Si es necesario, haga clic en **Activar edición**.
4. En Excel, abra el archivo descargado.
5. En la `data` hoja, seleccione los datos que desea utilizar en `Volume` y.. `Available Data` % columnas.
6. En el menú **Insertar**, seleccione un `3-D piechart`.

   El gráfico muestra qué volúmenes tienen el mayor espacio disponible. El gráfico aparece en la hoja de datos.

En función de la configuración de red, la selección de columnas completas o de demasiadas filas de datos puede hacer que el gráfico circular no sea legible. Este ejemplo utiliza el gráfico circular 3-D, pero puede utilizar cualquier tipo de gráfico. Utilice el gráfico que mejor muestra los datos que desea capturar.

7. Nombre el título del gráfico **capacidad disponible**.
8. Haga clic con el botón derecho del ratón en el gráfico y seleccione **mover gráfico**.
9. Seleccione **Nueva hoja** y asigne un nombre a la hoja **gráficos de volumen de almacenamiento**.

   Asegúrese de que la nueva hoja aparece después de las hojas de información y datos.

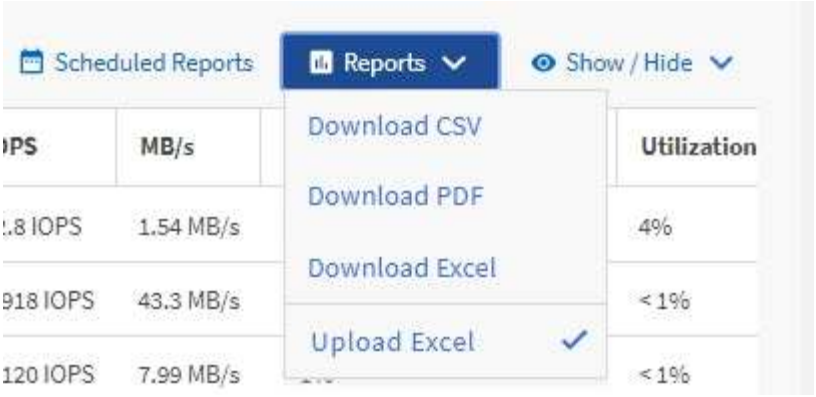


10. Con los menús **Diseño** y **Formato**, disponibles cuando se selecciona el gráfico, puede personalizar el aspecto del gráfico.
11. Cuando esté satisfecho, guarde el archivo con los cambios.
12. En Unified Manager, seleccione **Informes** > **cargar Excel**.

    Asegúrese de que se encuentra en la misma vista en la que descargó el archivo de Excel.

13. Seleccione el archivo de Excel que ha modificado.
14. Haga clic en **Abrir**.
15. Haga clic en **Enviar**.

    Aparece una Marca de verificación junto al elemento de menú **Informes** > **cargar Excel**.



16. Haga clic en **Informes programados**.
17. Haga clic en **Agregar programación** para agregar una nueva fila a la página **programas de informes** de modo que pueda definir las características de programación para el nuevo informe.
18. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

    Seleccione el formato **XLSX** para el informe.

    El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Según los resultados mostrados en el informe, se recomienda equilibrar la carga en los volúmenes.

Crear un informe para ver los agregados con la tasa de IOPS más disponible

Este informe muestra los agregados con la tasa de IOPS más disponible por tipo de agregado en los que se pueden aprovisionar nuevas cargas de trabajo.

Lo que necesitará

- Debe tener el rol de administrador de aplicaciones o de administrador del almacenamiento.

Utilice los pasos siguientes para abrir una vista Estado: Todos los volúmenes, descargar la vista en Excel, crear un gráfico de capacidad disponible, cargar el archivo de Excel personalizado y programar el informe final.

Pasos

1. En el panel de navegación izquierdo, haga clic en **almacenamiento** > **agregados**.
2. Seleccione **rendimiento: Todos los agregados** en el menú desplegable **Ver**.
3. Seleccione **Mostrar/Ocultar** para mostrar la `Available IOPS` y oculte la `Cluster FQDN, Inactive Data Reporting,` y.. `Threshold Policy` columnas.
4. Arrastre y suelte el `Available IOPS` y.. `Free Capacity` columnas junto a `Type` columna.
5. Asigne un nombre a la vista personalizada y guárdela `Available IOPS Per Aggr.`
6. Seleccione **Informes** > **Descargar Excel**.

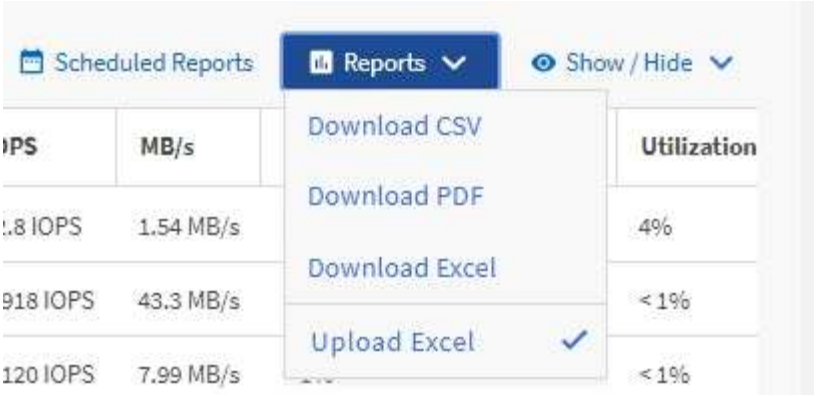
Según el explorador, es posible que tenga que hacer clic en **Aceptar** para guardar el archivo.

7. Si es necesario, haga clic en **Activar edición**.
8. En Excel, abra el archivo descargado.
9. En la hoja de datos, haga clic en el pequeño triángulo situado en la parte superior izquierda de la hoja para seleccionar toda la hoja.
10. En la cinta **Data**, seleccione **Sort** en `Sort & Filter area`.
11. Establezca los siguientes niveles de ordenación:
    a. Especifique **Ordenar por** como `Available IOPS` (IOPS), el **Ordenar en** como `Cell Values`, Y la **Orden** como `Largest to Smallest`.
    b. Haga clic en **Agregar nivel**.
    c. Especifique **Ordenar por** como `Type`, El **Ordenar en** como `Cell Values`, Y la **Orden** como `Z to A`.
    d. Haga clic en **Agregar nivel**.
    e. Especifique **Ordenar por** como `Free Capacity (GB)`, El **Ordenar en** como `Cell Values`, Y la **Orden** como `Largest to Smallest`.
    f. Haga clic en **Aceptar**.
12. Guarde y cierre el archivo de Excel.
13. En Unified Manager, seleccione **Informes** > **cargar Excel**.

    Asegúrese de que se encuentra en la misma vista en la que descargó el archivo de Excel.

14. Seleccione el archivo de Excel que ha modificado, en este caso `performance-aggregates-<date>.xlsx`.
15. Haga clic en **Abrir**.
16. Haga clic en **Enviar**.

Aparece una Marca de verificación junto al elemento de menú **Informes** > **cargar Excel**.



17. Haga clic en **Informes programados**.
18. Haga clic en **Agregar programación** para agregar una nueva fila a la página programas de informes de modo que pueda definir las características de programación para el nuevo informe.
19. Introduzca un nombre para el programa de informes y complete los otros campos de informe y, a continuación, haga clic en la Marca de verificación (✓) al final de la fila.

    Seleccione el formato **XLSX** para el informe.

    El informe se envía inmediatamente como prueba. Después de esto, el informe genera y se envía por correo electrónico a los destinatarios enumerados utilizando la frecuencia especificada.

Según los resultados mostrados en el informe, es posible que desee aprovisionar nuevas cargas de trabajo en los agregados con la mayor cantidad de IOPS disponible.

Gestión del almacenamiento usando API de REST

Primeros pasos con API de REST de Active IQ Unified Manager

Active IQ Unified Manager proporciona un conjunto de API para gestionar sus recursos de almacenamiento en los sistemas de almacenamiento compatibles mediante una interfaz de servicio web RESTful para cualquier integración de terceros.

En estos temas, encontrará información sobre las API de Unified Manager, flujos de trabajo de muestra para resolver problemas específicos y algunos códigos de muestra. Mediante esta información, puede crear clientes RESTful de soluciones de software de gestión de NetApp para gestionar sistemas NetApp. Las API se basan en el estilo arquitectónico de transferencia de estado representacional (REST). Se admiten las cuatro operaciones REST Create, Read, Update y Delete (también llamadas CRUD).

Destinatarios para este contenido

Estos temas están dirigidos a desarrolladores que crean aplicaciones que interactúan con el software de Active IQ Unified Manager a través de API DE REST.

Los administradores y arquitectos de sistemas de almacenamiento pueden consultar esta información para comprender cómo se pueden utilizar las API DE REST de Unified Manager para crear aplicaciones cliente con el fin de gestionar y supervisar sistemas de almacenamiento de NetApp.

Debe usar esta información si desea usar el proveedor de almacenamiento, el clúster de ONTAP y las API de administración de gestión para gestionar el almacenamiento.

> Debe tener una de las siguientes funciones: Operador, Administrador de almacenamiento o Administrador de aplicaciones. Debe conocer la dirección IP o el nombre de dominio completo del servidor de Unified Manager donde desea ejecutar las API DE REST.

Categorías y acceso API de Active IQ Unified Manager

Las API de Active IQ Unified Manager le permiten gestionar y aprovisionar objetos de almacenamiento en su entorno. También puede acceder a la interfaz de usuario web de Unified Manager para realizar algunas de estas funciones.

Creación de una URL para acceder directamente a las API de REST

Puede acceder a las API DE REST directamente a través de un lenguaje de programación, como Python, C#, C++, JavaScript, y así sucesivamente. Introduzca el nombre de host o la dirección IP y la URL para acceder a las API de REST en formato

https://<hostname>/api

> El puerto predeterminado es 443. Puede configurar el puerto según lo requiera su entorno.

Acceder a la página de documentación de API en línea

Puede acceder a la página de contenido de referencia *API Documentation* que se incluye junto con el producto para mostrar la documentación de la API, y también para emitir manualmente una llamada de API (en la interfaz, por ejemplo, Swagger). Puede acceder a esta documentación haciendo clic en **barra de menús** > **botón de ayuda** > **Documentación de API**

Como alternativa, introduzca el nombre o la dirección IP de host y la URL para acceder a la página API DE REST en formato

https://<hostname>/docs/api/

Categorías

Las llamadas API se organizan en función de las áreas o categorías. Para buscar una API específica, haga clic en la categoría API correspondiente.

Las API REST que proporciona Unified Manager ayudan a realizar funciones administrativas, de supervisión y de aprovisionamiento. Las API se agrupan en las siguientes categorías.

- **centro de datos**

  Esta categoría contiene las API que le ayudan en la gestión del almacenamiento del centro de datos y los análisis con herramientas como Work Flow Automation y Ansible. Las API DE REST en esta categoría proporcionan información sobre los clústeres, los nodos, los agregados, los volúmenes, las LUN, recursos compartidos de archivos, espacios de nombres y otros elementos del centro de datos.

- **servidor-administración**

  Las API bajo la categoría **Management-Server** contienen `jobs, system,` y.. `events` API. Los trabajos son operaciones que se programan para la ejecución asíncrona relacionadas con la gestión de objetos de almacenamiento o cargas de trabajo en Unified Manager. La `events` La API muestra eventos del centro de datos y del `system` La API muestra los detalles de la instancia de Unified Manager.

- **proveedor de almacenamiento**

  Esta categoría contiene todas las API de aprovisionamiento necesarias para gestionar y aprovisionar recursos compartidos de archivos, LUN, niveles de servicio de rendimiento y políticas de eficiencia del almacenamiento. Las API también permiten configurar extremos de acceso, directorios activos, así como asignar niveles de servicio de rendimiento y políticas de eficiencia del almacenamiento en cargas de trabajo de almacenamiento.

- **administración**

  Esta categoría contiene las API utilizadas para ejecutar tareas administrativas, como mantener la configuración de backup, ver certificados del almacén de confianza para los orígenes de datos de Unified Manager y gestionar clústeres de ONTAP como fuentes de datos para Unified Manager.

- **puerta de enlace**

  Unified Manager le permite invocar API DE REST de ONTAP a través de las API bajo la categoría de pasarela y gestionar los objetos de almacenamiento del centro de datos.

- **seguridad**

Esta categoría contiene API para gestionar usuarios de Unified Manager.

Servicios DE REST ofrecidos en Active IQ Unified Manager

Debe conocer los servicios DE REST y las operaciones ofrecidas, antes de empezar a usar las API Active IQ Unified Manager.

Las API de aprovisionamiento y administración que se usan para configurar el servidor API admiten las operaciones de lectura (GET) o escritura (POST, REVISIÓN, ELIMINACIÓN). A continuación se muestran algunos ejemplos de las operaciones GET, PATCH, POST y DELETE compatibles con las API:

- Ejemplo de OBTENER: `GET /datacenter/cluster/clusters` recupera los datos del clúster en el centro de datos. El número máximo de registros que devuelve el `GET` la operación es 1000.

  Las API permiten filtrar, ordenar y ordenar los registros por atributos admitidos.

- Ejemplo de PUBLICACIÓN: `POST /datacenter/svm/svms` Crea una máquina virtual de almacenamiento (SVM) personalizada.
- Ejemplo de PARCHE: `PATCH /datacenter/svm/svms/{key}` Modifica las propiedades de una SVM mediante su clave única.
- Ejemplo de ELIMINACIÓN: `DELETE /storage-provider/access-endpoints/{key}` Elimina un extremo de acceso de un LUN, una SVM o un recurso compartido de archivos mediante su clave única.

Las operaciones DE REST que se pueden realizar usando las API dependen de la función del usuario operador, administrador de almacenamiento o administrador de aplicaciones.

Rol de usuario	Método REST compatible
Operador	Acceso de solo lectura a los datos. Los usuarios con este rol pueden ejecutar todas las solicitudes GET.
Administrador de almacenamiento	Acceso de lectura a todos los datos. Los usuarios con este rol pueden ejecutar todas las solicitudes GET. Además, cuentan con acceso de escritura (para ejecutar solicitudes DE REVISIONES, TAREAS DE PUBLICACIÓN y ELIMINACIÓN) para realizar actividades específicas, como gestionar, objetos de servicio de almacenamiento y opciones de gestión del almacenamiento.
Administrador de aplicaciones	Acceso de lectura y escritura a todos los datos. Los usuarios con esta función pueden ejecutar solicitudes GET, PATCH, POST y DELETE para todas las funciones.

Para obtener más información sobre todas las operaciones DE REST, consulte la *Online API Documentage*.

Versión de API en Active IQ Unified Manager

Los URI de API REST en Active IQ Unified Manager especifican un número de versión. Por ejemplo: `/v2/datacenter/svm/svms`. El número de versión `v2` pulg `/v2/datacenter/svm/svms` Indica la versión de API utilizada en una versión específica. El número de versión minimiza el impacto de los cambios de API en el software cliente al enviar una respuesta que el cliente puede procesar.

La parte numérica de este número de versión es incremental con respecto a las versiones. Los URI con un número de versión proporcionan una interfaz coherente que mantiene la compatibilidad con versiones anteriores en versiones futuras. También puede encontrar las mismas API sin una versión, por ejemplo `/datacenter/svm/svms`, Que indican las API básicas sin una versión. Las API básicas siempre son la versión más reciente de las API.

> En la esquina superior derecha de la interfaz de Swagger, puede seleccionar la versión de la API que desea utilizar. La versión más alta está seleccionada de forma predeterminada. Se recomienda que utilice la versión más alta de una API determinada (con respecto al número entero incremental) disponible en la instancia de Unified Manager.

Para todas las solicitudes, debe solicitar explícitamente la versión de API que desea utilizar. Cuando se especifica el número de versión, el servicio no devuelve elementos de respuesta que la aplicación no está diseñada para manejar. En solicitudes DE REST, debe incluir el parámetro version. Después de algunas versiones, las versiones anteriores de las API quedaron obsoletas. En esta versión, la `v1` La versión de las API queda obsoleta.

Recursos de almacenamiento en ONTAP

Los recursos de almacenamiento de ONTAP pueden clasificarse en términos generales en recursos de almacenamiento físicos_ y recursos de almacenamiento lógico._ para gestionar de forma eficaz los sistemas de ONTAP mediante las API proporcionadas en Active IQ Unified Manager, deberá conocer el modelo de recursos de almacenamiento y la relación entre los distintos recursos de almacenamiento.

- **Recursos de almacenamiento físico**

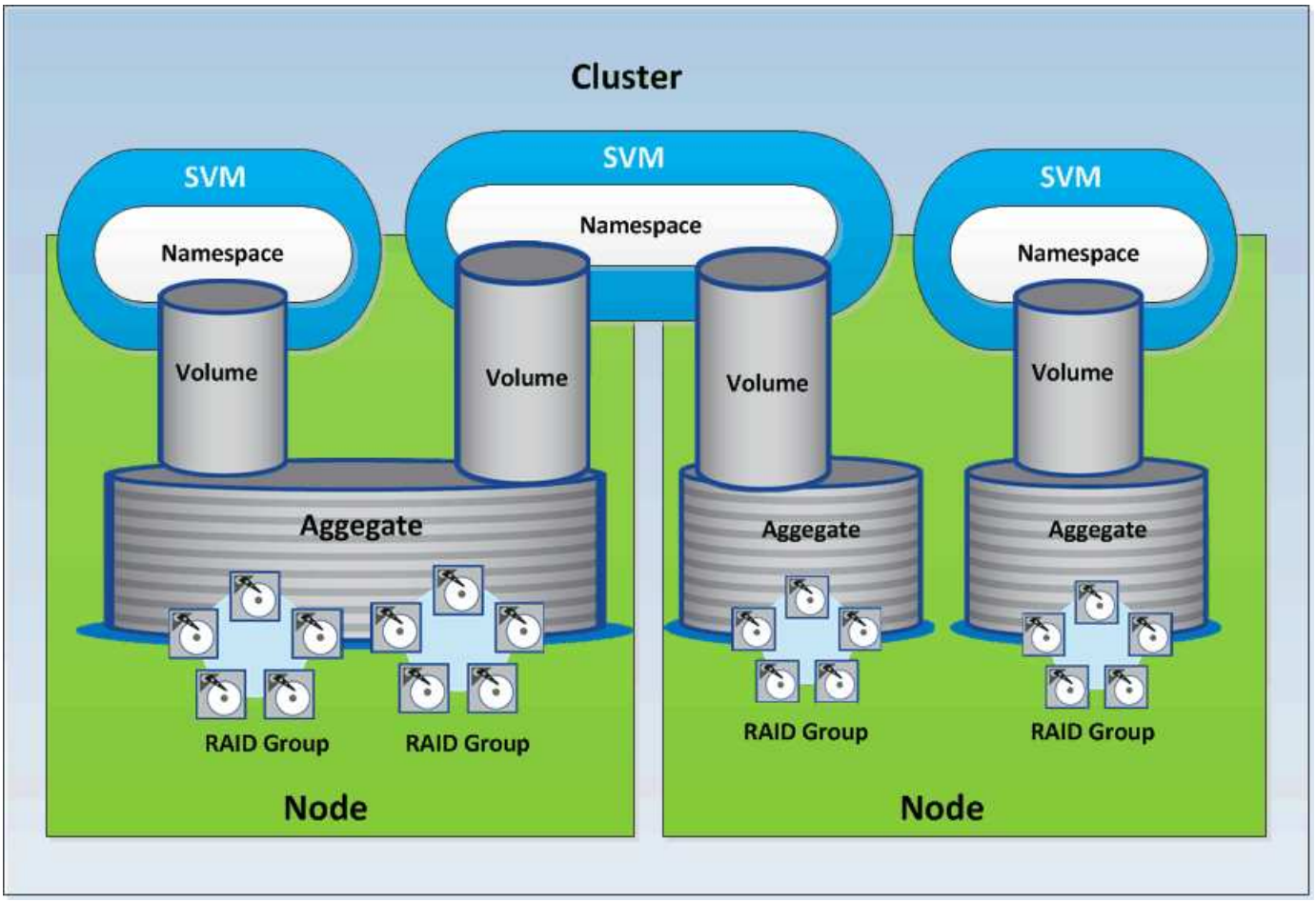
  Hace referencia a los objetos de almacenamiento físico que proporciona ONTAP. Los recursos de almacenamiento físico incluyen discos, clústeres, controladoras de almacenamiento, nodos y agregados.

- **Recursos de almacenamiento lógicos**

  Hace referencia a los recursos de almacenamiento que proporciona ONTAP que no están ligados a un recurso físico. Estos recursos están asociados a una máquina virtual de almacenamiento (SVM, antes denominada Vserver) y existen de forma independiente a cualquier recurso de almacenamiento físico específico como un disco, una LUN de cabina o un agregado.

  Los recursos de almacenamiento lógico incluyen volúmenes de todos los tipos y qtrees, así como las funcionalidades y configuraciones que puede utilizar con estos recursos, como copias de Snapshot, deduplicación, compresión y cuotas.

En la siguiente ilustración, se muestran los recursos de almacenamiento en un clúster de 2 nodos:



Acceso y autenticación de API DE REST en Active IQ Unified Manager

La API de REST de Active IQ Unified Manager es accesible mediante cualquier cliente REST o plataforma de programación que pueda emitir solicitudes HTTP con un mecanismo de autenticación HTTP básico.

Una solicitud y respuesta de muestra:

- **Solicitud**

```
GET
https://<IP
address/hostname>:<port_number>/api/v2/datacenter/cluster/clusters
```

- **Respuesta**

```
{
  "records": [
    {
      "key": "4c6bf721-2e3f-11e9-a3e2-
```

```
00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
      "name": "fas8040-206-21",
      "uuid": "4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
      "contact": null,
      "location": null,
      "version": {
        "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17 10:28:33
UTC 2019",
        "generation": 9,
        "major": 5,
        "minor": 0
      },
      "isSanOptimized": false,
      "management_ip": "10.226.207.25",
      "nodes": [
        {
          "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb",
          "uuid": "12cf06cc-2e3a-11e9-b9b4-00a0985badbb",
          "name": "fas8040-206-21-01",
          "_links": {
            "self": {
              "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb"
            }
          },
          "location": null,
          "version": {
            "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17
10:28:33 UTC 2019",
            "generation": 9,
            "major": 5,
            "minor": 0
          },
          "model": "FAS8040",
          "uptime": 13924095,
          "serial_number": "701424000157"
        },
        {
          "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-
00a0985bb9b7",
          "uuid": "1ed606ed-2e3a-11e9-a270-00a0985bb9b7",
          "name": "fas8040-206-21-02",
```

```
          "_links": {
            "self": {
              "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-
00a0985bb9b7"
            }
          },
          "location": null,
          "version": {
            "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17
10:28:33 UTC 2019",
            "generation": 9,
            "major": 5,
            "minor": 0
          },
          "model": "FAS8040",
          "uptime": 14012386,
          "serial_number": "701424000564"
        }
      ],
      "_links": {
        "self": {
          "href": "/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-
00a0985badbb"
        }
      }
    },
```

- *IP address/hostname* Es la dirección IP o el nombre de dominio completo (FQDN) del servidor API.
- Puerto 443

  443 es el puerto HTTPS predeterminado. Puede personalizar el puerto HTTPS, si fuera necesario.

Para emitir solicitudes HTTP desde un explorador web, tiene que utilizar los complementos de explorador de API DE REST. También podrá acceder a la API DE REST usando plataformas de scripting, como curl y Perl.

Autenticación

Unified Manager admite el esquema de autenticación HTTP básico para las API. Para obtener un flujo de información seguro (solicitud y respuesta), se puede acceder a las API DE REST solo a través de HTTPS. El servidor API proporciona un certificado SSL autofirmado a todos los clientes para la verificación del servidor. Este certificado puede sustituirse por un certificado personalizado (o certificado de CA).

Debe configurar el acceso de usuario al servidor API para invocar las API DE REST. Los usuarios pueden ser usuarios locales (perfiles de usuario almacenados en la base de datos local) o usuarios LDAP (si ha

configurado el servidor API para autenticarse en LDAP). Para gestionar el acceso de los usuarios, inicie sesión en la interfaz de usuario de Unified Manager Administration Console.

códigos de estado HTTP utilizados en Active IQ Unified Manager

Al ejecutar las API o solucionar problemas, debe tener en cuenta los distintos códigos de estado HTTP y códigos de error que utilizan las API de Active IQ Unified Manager.

En la siguiente tabla se enumeran los códigos de error relacionados con la autenticación:

Código de estado HTTP	Título del código de estado	Descripción
200	DE ACUERDO	Se devolvió al ejecutar correctamente las llamadas API síncronas.
201	Creado	Creación de recursos nuevos mediante llamadas síncronas, como la configuración de Active Directory.
202	Aceptado	Devuelto cuando la ejecución correcta de llamadas asíncronas para funciones de aprovisionamiento, como la creación de LUN y recursos compartidos de archivos.
400	Solicitud no válida	Indica fallo de validación de entrada. El usuario tiene que corregir las entradas, por ejemplo, las claves válidas de un cuerpo de solicitud.
401	Solicitud no autorizada	No está autorizado a ver el recurso o no autorizado.
403	Solicitud prohibida	Está prohibido acceder al recurso que estaba intentando alcanzar.
404	No se encuentra el recurso	No se encuentra el recurso al que estaba intentando acceder.
405	Método no permitido	Método no permitido.
429	Demasiadas solicitudes	Devuelto cuando el usuario envía demasiadas solicitudes dentro de un periodo de tiempo específico.

Código de estado HTTP	Título del código de estado	Descripción
500	Error interno del servidor	Error interno del servidor. Error al obtener la respuesta del servidor. Este error interno del servidor puede ser permanente o no. Por ejemplo, si ejecuta un `GET` o. `GET ALL` operación y recibir este error, se recomienda repetir esta operación por un mínimo de cinco reintentos. Si se trata de un error permanente, el código de estado devuelto sigue siendo 500. Si la operación se realiza correctamente, el código de estado devuelto es 200.

Recomendaciones para el uso de las API para Active IQ Unified Manager

Al usar las API en Active IQ Unified Manager, debe seguir ciertas prácticas recomendadas.

- Todos los tipos de contenido de la respuesta deben tener el siguiente formato para una ejecución válida:

```
application/json
```

- El número de versión de la API no está relacionado con el número de versión del producto. Debe utilizar la versión más reciente de la API disponible para la instancia de Unified Manager. Si quiere más información acerca de las versiones de la API de Unified Manager, consulte la sección «ARTÍCULO «Artículo DE la creación de versiones de la API en Active IQ Unified Manager».
- Al actualizar los valores de cabinas mediante una API de Unified Manager, debe actualizar toda la cadena de valores. No se pueden agregar valores a una matriz. Solo es posible reemplazar una cabina existente.
- Puede utilizar operadores de filtro, como pipe (|) y comodines (*) para todos los parámetros de consulta, excepto para valores dobles, por ejemplo, IOPS y rendimiento en las API de métricas.
- Evite consultar objetos mediante una combinación de la comoda (*) y la tubería (|) del operador de filtro. Es posible que recupere una cantidad incorrecta de objetos.
- Cuando utilice valores para el filtro, asegúrese de que el valor no contiene ninguno `?` carácter. Esto es para mitigar los riesgos de la inyección SQL.
- Observe que el `GET` (All) la solicitud de cualquier API devuelve un máximo de 1000 registros. Incluso si ejecuta la consulta estableciendo la `max_records` parámetro a un valor superior a 1000, sólo se devuelven 1000 registros.
- Para realizar funciones administrativas, se recomienda usar la interfaz de usuario de Unified Manager.

Registros para solución de problemas

Los registros del sistema le permiten analizar las causas de los errores y solucionar los problemas que pueden surgir al ejecutar las API.

Recupere los registros de la siguiente ubicación para solucionar problemas relacionados con las llamadas API.

Ubicación del registro	Uso
`/var/log/ocie/access_log.log`	Contiene todos los detalles de llamada de la API, como el nombre de usuario del usuario que invoca la API, la hora de inicio, la hora de ejecución, el estado y la URL. Puede usar este archivo de registro para comprobar las API que se usan con frecuencia o solucionar los problemas de cualquier flujo de trabajo de la interfaz gráfica de usuario. También se puede utilizar para ampliar el análisis en función del tiempo de ejecución.
`/var/log/ocum/ocumserver.log`	Contiene todos los registros de ejecución de la API. Es posible usar este archivo de registro para solucionar problemas y depurar las llamadas API.
`/var/log/ocie/server.log`	Contiene todas las implementaciones de servidores Wildfly y registros relacionados con el servicio de inicio y parada. Puede utilizar este archivo de registro para encontrar la causa raíz de cualquier problema que se produzca durante el inicio, la detención o la implementación del servidor Wildfly.
`/var/log/ocie/au.log`	Contiene registros relacionados con la unidad de adquisición. Puede utilizar este archivo de registro cuando ha creado, modificado o eliminado cualquier objeto de la ONTAP, pero no se reflejan para las API de REST de Active IQ Unified Manager.

Procesos asincrónicos de objetos de trabajo

Active IQ Unified Manager proporciona la `jobs` API que recupera información sobre los trabajos realizados mientras ejecuta otras API. Debe saber cómo funciona el procesamiento asíncrono mediante el objeto Job.

Algunas de las llamadas API, especialmente las que se utilizan para agregar o modificar recursos, pueden tardar más tiempo en completarse que otras llamadas. Unified Manager procesa estas solicitudes de ejecución prolongada de forma asíncrona.

Solicitudes asincrónicas descritas mediante el objeto Job

Después de realizar una llamada API que se ejecuta de forma asíncrona, el código de respuesta HTTP 202 indica que la solicitud se ha validado y aceptado correctamente, pero que aún no se ha completado. La

solicitud se procesa como una tarea en segundo plano que continúa ejecutándose después de la respuesta HTTP inicial al cliente. La respuesta incluye el objeto Job anclando la solicitud, incluyendo su identificador único.

Consulta del objeto Job asociado a una solicitud API

El objeto Job devuelto en la respuesta HTTP contiene varias propiedades. Puede consultar la propiedad state para determinar si la solicitud se completó correctamente. Un objeto Job puede estar en uno de los siguientes estados:

- `NORMAL`
- `WARNING`
- `PARTIAL_FAILURES`
- `ERROR`

Existen dos técnicas que se pueden utilizar al sondear un objeto Job para detectar un estado de terminal para la tarea, ya sea con éxito o con un error:

- Solicitud de sondeo estándar: El estado del trabajo actual se devuelve inmediatamente.
- Solicitud de sondeo largo: Cuando el estado del trabajo pasa a. `NORMAL, ERROR,` o. `PARTIAL_FAILURES.`

Pasos en una solicitud asíncrona

Puede utilizar el siguiente procedimiento de alto nivel para completar una llamada API asíncrona:

1. Emita la llamada de API asíncrona.
2. Reciba una respuesta HTTP 202 que indique la aceptación correcta de la solicitud.
3. Extraiga el identificador del objeto Job del cuerpo de respuesta.
4. Dentro de un bucle, espere a que el objeto Job alcance el estado de terminal `NORMAL, ERROR,` o. `PARTIAL_FAILURES.`
5. Compruebe el estado del terminal del trabajo y recupere el resultado del trabajo.

Hola servidor API

El *Hello API Server* es un programa de muestra que muestra cómo invocar una API REST en Active IQ Unified Manager mediante un simple cliente REST. El programa de ejemplo proporciona detalles básicos sobre el servidor API en formato JSON (el servidor solo admite) `application/json` formato).

El URI utilizado es: `https://<hostname>/api/datacenter/svm/svms`. Este código de ejemplo toma los siguientes parámetros de entrada:

- La dirección IP o el FQDN del servidor API
- Opcional: Número de puerto (predeterminado: 443)
- Nombre de usuario
- Contraseña

- Formato de respuesta (`application/json`)

Para invocar API REST, también puede utilizar otras secuencias de comandos, como Jersey y RESTeasy, para escribir un cliente Java REST para Active IQ Unified Manager. Debe tener en cuenta las siguientes consideraciones sobre el código de ejemplo:

- Utiliza una conexión HTTPS con Active IQ Unified Manager para invocar el URI DE REST especificado
- Ignora el certificado proporcionado por Active IQ Unified Manager
- Omite la verificación del nombre del host durante el apretón de manos
- Utiliza `javax.net.ssl.HttpsURLConnection` Para una conexión URI
- Utiliza una biblioteca de terceros (`org.apache.commons.codec.binary.Base64`) Para construir la cadena codificada Base64 utilizada en la autenticación básica HTTP

Para compilar y ejecutar el código de ejemplo, debe utilizar el compilador Java 1.8 o posterior.

```
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.net.URL;
import java.security.SecureRandom;
import java.security.cert.X509Certificate;
import javax.net.ssl.HostnameVerifier;
import javax.net.ssl.HttpsURLConnection;
import javax.net.ssl.SSLContext;
import javax.net.ssl.SSLSession;
import javax.net.ssl.TrustManager;
import javax.net.ssl.X509TrustManager;
import org.apache.commons.codec.binary.Base64;

public class HelloApiServer {

    private static String server;
    private static String user;
    private static String password;
    private static String response_format = "json";
    private static String server_url;
    private static String port = null;

    /*
     * * The main method which takes user inputs and performs the *
necessary steps
     * to invoke the REST URI and show the response
     */ public static void main(String[] args) {
        if (args.length < 2 || args.length > 3) {
            printUsage();
            System.exit(1);
        }
```

```
        setUserArguments(args);
        String serverBaseUrl = "https://" + server;
        if (null != port) {
            serverBaseUrl = serverBaseUrl + ":" + port;
        }
        server_url = serverBaseUrl + "/api/datacenter/svm/svms";
        try {
            HttpsURLConnection connection =
getAllTrustingHttpsUrlConnection();
            if (connection == null) {
                System.err.println("FATAL: Failed to create HTTPS
connection to URL: " + server_url);
                System.exit(1);
            }
            System.out.println("Invoking API: " + server_url);
            connection.setRequestMethod("GET");
            connection.setRequestProperty("Accept", "application/" +
response_format);
            String authString = getAuthorizationString();
            connection.setRequestProperty("Authorization", "Basic " +
authString);
            if (connection.getResponseCode() != 200) {
                System.err.println("API Invocation Failed : HTTP error
code : " + connection.getResponseCode() + " : "
                        + connection.getResponseMessage());
                System.exit(1);
            }
            BufferedReader br = new BufferedReader(new
InputStreamReader((connection.getInputStream())));
            String response;
            System.out.println("Response:");
            while ((response = br.readLine()) != null) {
                System.out.println(response);
            }
            connection.disconnect();
        } catch (Exception e) {
            e.printStackTrace();
        }
    }

    /* Print the usage of this sample code */ private static void
printUsage() {
        System.out.println("\nUsage:\n\tHelloApiServer <hostname> <user>
<password>\n");
        System.out.println("\nExamples:\n\tHelloApiServer localhost admin
mypassword");
```

```
        System.out.println("\tHelloApiServer 10.22.12.34:8320 admin
password");
        System.out.println("\tHelloApiServer 10.22.12.34 admin password
");
        System.out.println("\tHelloApiServer 10.22.12.34:8212 admin
password \n");
        System.out.println("\nNote:\n\t(1) When port number is not
provided, 443 is chosen by default.");
    }

    /* * Set the server, port, username and password * based on user
inputs. */ private static void setUserArguments(
            String[] args) {
        server = args[0];
        user = args[1];
        password = args[2];
        if (server.contains(":")) {
            String[] parts = server.split(":");
            server = parts[0];
            port = parts[1];
        }
    }

    /*
     * * Create a trust manager which accepts all certificates and * use
this trust
     * manager to initialize the SSL Context. * Create a
HttpsURLConnection for this
     * SSL Context and skip * server hostname verification during SSL
handshake. * *
     * Note: Trusting all certificates or skipping hostname verification *
is not
     * required for API Services to work. These are done here to * keep
this sample
     * REST Client code as simple as possible.
     */ private static HttpsURLConnection
getAllTrustingHttpsUrlConnection()    {        HttpsURLConnection conn =
null;        try {            /* Creating a trust manager that does not
validate certificate chains */            TrustManager[]
trustAllCertificatesManager = new                    TrustManager[]{new
X509TrustManager(){
     public X509Certificate[] getAcceptedIssuers(){return  null;}
     public void checkClientTrusted(X509Certificate[]
certs, String authType){}
     public void checkServerTrusted(X509Certificate[]
certs, String authType){}            }};            /* Initialize the
```

```
SSLContext with the all-trusting trust manager */
     SSLContext sslContext = SSLContext.getInstance("TLS");
sslContext.init(null, trustAllCertificatesManager, new
SecureRandom());
HttpsURLConnection.setDefaultSSLSocketFactory(sslContext.getSocketFactory(
));            URL url = new URL(server_url);            conn =
(HttpsURLConnection) url.openConnection();            /* Do not perform an
actual hostname verification during SSL Handshake.            Let all
hostname pass through as verified.*/
conn.setHostnameVerifier(new HostnameVerifier() {               public
boolean verify(String host, SSLSession                        session) {
return true;                }            });        } catch (Exception e)
{            e.printStackTrace();        }        return conn;    }

    /*
     * * This forms the Base64 encoded string using the username and
password *
     * provided by the user. This is required for HTTP Basic
Authentication.
     */ private static String getAuthorizationString() {
        String userPassword = user + ":" + password;
        byte[] authEncodedBytes =
Base64.encodeBase64(userPassword.getBytes());
        String authString = new String(authEncodedBytes);
        return authString;
    }

}
```

API de REST de Unified Manager

Las API DE REST para Active IQ Unified Manager se enumeran en esta sección, según sus categorías.

Es posible ver la página de documentación en línea desde la instancia de Unified Manager que incluye los detalles de cada llamada de API DE REST. Este documento no repite los detalles de la documentación en línea. Cada llamada de API que se enumera o se describe en este documento incluye solo la información que necesita para localizar la llamada en la página de documentación. Después de localizar una llamada API específica, puede revisar los detalles completos de esa llamada, incluidos los parámetros de entrada, formatos de salida, códigos de estado HTTP y tipo de procesamiento de solicitudes.

Se incluye la siguiente información para cada llamada de API dentro de un flujo de trabajo para ayudar a localizar la llamada en la página de documentación:

- Categoría

  Las llamadas API se organizan en la página de documentación en áreas o categorías relacionadas con la función. Para ubicar una llamada a API específica, desplácese hacia abajo hasta la parte inferior de la

página y, a continuación, haga clic en la categoría API correspondiente.

- Verbo HTTP (llamada)

  El verbo HTTP identifica la acción realizada en un recurso. Cada llamada API se ejecuta a través de un único verbo HTTP.

- Ruta

  La ruta determina el recurso específico que la acción utiliza como parte de la realización de una llamada. La cadena de ruta de acceso se anexa a la URL de núcleo para formar la URL completa que identifica el recurso.

Gestionar objetos de almacenamiento en un centro de datos mediante API

Las API DE REST debajo de `datacenter` La categoría le permite gestionar los objetos de almacenamiento en el centro de datos, como clústeres, nodos, agregados, máquinas virtuales de almacenamiento, Volúmenes, LUN, recursos compartidos de archivos y espacios de nombres. Estas API están disponibles para consultar la configuración de los objetos, mientras que algunas de ellas permiten realizar las operaciones de adición, eliminación o modificación de estos objetos.

La mayoría de estas API son LLAMADAS QUE proporcionan agregación entre clústeres con compatibilidad con filtrado, clasificación y paginación. Al ejecutar estas API, devuelven datos de la base de datos. Por lo tanto, los objetos recién creados deben ser descubiertos en el próximo ciclo de adquisición para que aparezcan en la respuesta.

Si desea consultar los detalles de un objeto específico, debe introducir el ID único de ese objeto para ver sus detalles. Por ejemplo, para obtener información de métricas y análisis de los objetos de almacenamiento, consulte "Ver las métricas de rendimiento".

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters/4c6bf721-
2e3f-11e9-a3e2-00a0985badbb" -H "accept: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>"
```

Los comandos CURL, ejemplos, solicitudes y respuestas a las API están disponibles en la interfaz de API de Swagger. Puede filtrar y ordenar los resultados por parámetros específicos según lo que se indica en Swagger. Estas API le permiten filtrar los resultados de objetos de almacenamiento específicos, como el clúster, el volumen o el equipo virtual de almacenamiento.

API para los objetos de almacenamiento en el centro de datos

Verbo HTTP	Ruta	Descripción
GET	/datacenter/cluster/clusters /datacenter/cluster/clusters/{key}	Puede usar este método para ver los detalles de los clústeres ONTAP en todo el centro de datos. La API muestra información, como la dirección IPv4 o IPv6 del clúster, información sobre el nodo, como el estado de los nodos, la capacidad de rendimiento y el par de alta disponibilidad (ha), e indica si el clúster es una cabina All SAN.
GET	/datacenter/cluster/licensing/licenses /datacenter/cluster/licensing/licenses/{key}	Muestra los detalles de las licencias instaladas en los clústeres del centro de datos. Puede filtrar los resultados en función de los criterios requeridos. Se devuelve información, como la clave de licencia, la clave de clúster, la fecha de caducidad y el alcance de la licencia. Puede introducir una clave de licencia para recuperar los detalles de una licencia específica.
GET	/datacenter/cluster/nodes /datacenter/cluster/nodes/{key}	Puede usar este método para ver los detalles de los nodos en el centro de datos. Se puede ver información sobre el clúster, el estado de los nodos, la capacidad de rendimiento y la pareja de alta disponibilidad (ha) del nodo.
GET	/datacenter/protocols/cifs/shares /datacenter/protocols/cifs/shares/{key}	Puede utilizar este método para ver los detalles de los recursos compartidos CIFS en el centro de datos. Además de los detalles del clúster, la SVM y los volúmenes, también se devuelve información sobre Access Control List (ACL).

Verbo HTTP	Ruta	Descripción
GET	/datacenter/protocols/nfs/export-policies /datacenter/protocols/nfs/export-policies/{key}	Puede utilizar este método para ver los detalles de las políticas de exportación de los servicios NFS admitidos. Puede consultar las políticas de exportación de una máquina virtual de almacenamiento o clúster y reutilizar la clave de política de exportación para aprovisionar los recursos compartidos de archivos NFS. Para obtener más información acerca de la asignación y reutilización de políticas de exportación en cargas de trabajo, consulte «'aprovisionamiento de recursos compartidos de archivos CIFS y NFS».
GET	/datacenter/storage/aggregates /datacenter/storage/aggregates/{key}	Puede usar este método para ver la recogida de agregados en el centro de datos o un agregado específico para aprovisionar cargas de trabajo en ellos o supervisar. Se obtiene información, como detalles del clúster y de los nodos, la capacidad de rendimiento utilizada, el espacio disponible y el uso, y la eficiencia del almacenamiento.
GET	/datacenter/storage/luns /datacenter/storage/luns/{key}	Puede utilizar este método para ver la colección de LUN en todo el centro de datos. Es posible ver información sobre el LUN, como detalles de clústeres y SVM, políticas de calidad de servicio y iGroups.
GET	/datacenter/storage/qos/policies /datacenter/storage/qos/policies/{key}	Puede utilizar este método para ver los detalles de todas las políticas de calidad de servicio aplicables a los objetos de almacenamiento del centro de datos. Se obtiene información, como los detalles del clúster y la SVM, los detalles de la política fija o adaptativa, y el número de objetos que se aplican a esa política.

Verbo HTTP	Ruta	Descripción
GET	/datacenter/storage/qtrees /datacenter/storage/qtrees/{key}	Puede usar este método para ver los detalles de qtree en el centro de datos de todos los volúmenes de FlexVol o de FlexGroup. Se devuelve información, como los detalles del clúster y la SVM, el volumen FlexVol y la política de exportación.
GET	/datacenter/storage/volumes /datacenter/storage/volumes/{key}	Puede usar este método para ver la recogida de volúmenes en el centro de datos. Se obtiene información sobre los volúmenes, como SVM y los detalles de los clústeres, las políticas de calidad de servicio y exportación, si el volumen es del tipo de lectura/escritura, la protección de datos o el uso compartido de carga. Para los volúmenes FlexVol y FlexClone, puede ver la información de los agregados correspondientes. En el caso de un volumen FlexGroup, la consulta devuelve la lista de agregados constituyentes.

Verbo HTTP	Ruta	Descripción

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/protocols/san/igroups`
	
	`/datacenter/protocols/san/igroups/{key}`
		Puede asignar grupos de iniciadores (iGroups) autorizados para acceder a destinos de LUN específicos. Si hay un igroup existente, puede asignarlo. También puede crear iGroups y asignarles a las LUN.
		
		Puede utilizar estos métodos para consultar, crear, eliminar y modificar iGroups respectivamente.
		
		Puntos que tener en cuenta:
		
		• `POST`: Al crear un igroup, es posible designar el equipo virtual de almacenamiento en el que desea asignar acceso.
		• `DELETE`: Debe proporcionar la clave de igroup como parámetro de entrada para eliminar un igroup determinado. Si ya ha asignado un igroup a una LUN, no puede eliminar ese igroup.
		• `PATCH`: Debe proporcionar la clave de igroup como parámetro de entrada para modificar un igroup determinado. También debe introducir la propiedad que desea actualizar junto con su valor.

Verbo HTTP	Ruta	Descripción

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/svm/svms`
	
	`/datacenter/svm/svms/{key}`
		Es posible usar estos métodos para ver, crear, eliminar y modificar máquinas virtuales de almacenamiento (máquinas virtuales de almacenamiento).
		
		• `POST`: Debe introducir el objeto de la máquina virtual de almacenamiento que desea crear como parámetro de entrada. Es posible crear una máquina virtual de almacenamiento personalizado y, a continuación, asignar las propiedades requeridas.
		• `DELETE`: Debe proporcionar la clave de máquina virtual de almacenamiento para eliminar una máquina virtual de almacenamiento particular.
		• `PATCH`: Debe proporcionar la clave de la máquina virtual de almacenamiento para modificar una máquina virtual de almacenamiento particular. También debe introducir las propiedades que desea actualizar, junto con sus valores.

Puntos que tener en cuenta:

Si ha habilitado el aprovisionamiento de cargas de trabajo basado en SLO en su entorno, al tiempo que crea el equipo virtual de almacenamiento, asegúrese de que admite todos los protocolos necesarios para aprovisionar las LUN y los recursos compartidos de archivos, por ejemplo, CIFS o SMB, NFS, FCP, E iSCSI. Es posible que se produzca un error en los flujos de trabajo de aprovisionamiento si la máquina virtual de almacenamiento no admite los servicios necesarios. Se recomienda habilitar también los servicios para los respectivos tipos de cargas de trabajo en el equipo virtual de almacenamiento.

Si ha habilitado el aprovisionamiento de carga de trabajo basado en SLO en su entorno, no puede eliminar esa máquina virtual de almacenamiento en la que se han aprovisionado las cargas de trabajo de almacenamiento. Cuando se elimina una máquina virtual de almacenamiento en la que se ha configurado un servidor CIFS o SMB, esta API también elimina el servidor CIFS o SMB, junto con la configuración de Active Directory local. Sin embargo, el nombre del servidor CIFS o SMB sigue estando en la configuración de Active Directory que debe eliminar manualmente del servidor de Active Directory.

API para los elementos de red en su centro de datos

Las siguientes API de la categoría de centro de datos recuperan información acerca de los puertos y las interfaces de red del entorno, específicamente los puertos FC, las interfaces FC, los puertos ethernet y las

interfaces IP.

Verbo HTTP	Ruta	Descripción
GET	/datacenter/network/ethernet/ports /datacenter/network/ethernet/ports/{key}	Recupera información sobre todos los puertos ethernet del entorno del centro de datos. Con una clave de puerto como parámetro de entrada, puede ver la información de ese puerto específico. Información, como los detalles del clúster, el dominio de retransmisión, los detalles del puerto, como estado, la velocidad, y escriba, y si el puerto está habilitado, se recupera.
GET	/datacenter/network/fc/interfaces /datacenter/network/fc/interfaces/{key}	Puede utilizar este método para ver los detalles de las interfaces FC en su entorno de centro de datos. Con una clave de interfaz como parámetro de entrada, puede ver la información de esa interfaz específica. Se recupera información, como los detalles del clúster, los detalles de los nodos de inicio y los detalles del puerto principal.
GET	/datacenter/network/fc/ports /datacenter/network/fc/ports/{key}	Recupera información sobre todos los puertos FC utilizados en los nodos del entorno de centro de datos. Con una clave de puerto como parámetro de entrada, puede ver la información de ese puerto específico. Se recupera información, como los detalles del clúster, la descripción del puerto, el protocolo compatible y el estado del puerto.
GET	/datacenter/network/ip/interfaces /datacenter/network/ip/interfaces/{key}	Puede utilizar este método para ver los detalles de las interfaces IP en el entorno del centro de datos. Con una clave de interfaz como parámetro de entrada, puede ver la información de esa interfaz específica. Se recupera información, como detalles del clúster, detalles del espacio IP, detalles del nodo principal, si la conmutación por error está habilitada.

Acceso a API de ONTAP a través de acceso de proxy

Las API de puerta de enlace le ofrecen la ventaja de usar las credenciales de Active IQ Unified Manager para ejecutar API DE REST de ONTAP y gestionar objetos de almacenamiento. Estas API están disponibles cuando se habilita la función API Gateway en la interfaz de usuario web de Unified Manager.

Las API DE REST de Unified Manager solo admiten un conjunto determinado de acciones que se realizarán en los orígenes de datos de Unified Manager, es decir, clústeres de ONTAP. Puede utilizar otras funciones con las API de ONTAP. Las API de puerta de enlace permiten a Unified Manager ser una interfaz de paso a través donde se encapsulan todas las solicitudes de API que se realizan en clústeres de ONTAP que gestiona, sin necesidad de iniciar sesión en cada clúster de centro de datos de forma individual. Realiza como un único punto de gestión para ejecutar las API en los clústeres de ONTAP gestionados por su instancia de Unified Manager. La función de puerta de enlace de API permite a Unified Manager ser un único plano de control desde el cual puede gestionar varios clústeres de ONTAP sin iniciar sesión de forma individual. Las API de puerta de enlace permiten seguir registrando en Unified Manager y gestionar los clústeres de ONTAP ejecutando operaciones de API de REST de ONTAP.

Todos los usuarios pueden ejecutar una consulta utilizando LA operación GET. Los administradores de aplicaciones pueden ejecutar todas las operaciones de REST de ONTAP.

La puerta de enlace actúa como proxy para tunear las solicitudes de API manteniendo las solicitudes de encabezado y cuerpo en el mismo formato que en las API de ONTAP. Puede usar las credenciales de Unified Manager y ejecutar las operaciones específicas para acceder a los clústeres de ONTAP y gestionarlos sin aprobar las credenciales de un clúster individual. Continúa gestionando la autenticación del clúster y la gestión del clúster, pero redirige las solicitudes de API para que se ejecuten directamente en el clúster específico. La respuesta que devuelven las API es la misma que la respuesta que devuelven las respectivas API DE REST de ONTAP ejecutadas directamente desde ONTAP.

Verbo HTTP	Ruta (URL)	Descripción
`GET`	`/gateways`	Este método GET recupera la lista de todos los clústeres gestionados por Unified Manager compatibles con las llamadas DE REST de ONTAP. Puede verificar los detalles del clúster y elegir ejecutar otros métodos basados en el UUID de clúster o en el identificador único universal (UUID). Las API de puerta de enlace solo recuperan los clústeres compatibles con ONTAP 9.5 o posterior, y se añaden a Unified Manager con HTTPS.

Verbo HTTP	Ruta (URL)	Descripción

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
 	
`OPTIONS` (No disponible en Swagger)
 	
`HEAD` (No disponible en Swagger)
	`/gateways/{uuid}/{path}`
	
	El valor de {UUID} debe sustituirse por el UUID de clúster en el que se va a realizar la operación REST. Además, asegúrese de que el UUID sea del clúster compatible con ONTAP 9.5 o una versión posterior, y de que se agregue a Unified Manager mediante HTTPS. La URL DE REST de ONTAP debe sustituir {path}. Debe quitar `/api/` Desde la URL.
		Se trata de una API de proxy de punto único que admite OPERACIONES POSTERIORES, DE ELIMINACIÓN y REVISIÓN, y QUE se APLICA a todas las API DE REST de ONTAP. No se aplican restricciones en ninguna de las API siempre que sean compatibles con ONTAP. La función de túnel o proxy no se puede desactivar.
		
		La `OPTIONS` Método devuelve todas las operaciones admitidas por una API DE REST de ONTAP. Por ejemplo, si una API de ONTAP solo admite el `GET` funcionamiento, ejecute el `OPTIONS` Método al usar esta API de puerta de enlace se devuelve `GET` como respuesta. Este método no es compatible con Swagger, pero se puede realizar en otras herramientas API.
		
		La `OPTIONS` método determina si un recurso está disponible. Esta operación se puede utilizar para ver los metadatos sobre un recurso en los encabezados de respuesta HTTP. Este método no es compatible con Swagger, pero se puede realizar en otras herramientas API.

Descripción del túnel de puerta de enlace API

Las API de puerta de enlace le permiten gestionar objetos ONTAP mediante Unified Manager. Unified Manager gestiona los clústeres y los detalles de autenticación, y redirige las solicitudes al extremo DE REST de ONTAP. La API de la puerta de enlace transforma la URL e Hypermedia como el Motor de Estado de aplicación (HATEOAS) enlaces en el encabezado y el cuerpo de respuesta con la URL base de la puerta de enlace API. La API de puerta de enlace actúa como la URL base del proxy a la cual se anexa la URL DE REST de ONTAP y se ejecuta el extremo de REST de ONTAP requerido.

Para que una API de ONTAP se ejecute correctamente a través de una pasarela API, la API debe ser compatible con esa versión del clúster ONTAP en el que se está ejecutando. La ejecución de una API que no es compatible con el clúster de ONTAP no devuelve ningún resultado.

En este ejemplo, la API de la puerta de enlace (URL base de proxy) es: `/gateways/{uuid}/`

La API de ONTAP tomada es: `/storage/volumes`. Es necesario añadir la URL DE REST de ONTAP API

como valor para el parámetro path.

> Al añadir la ruta, asegúrese de haber eliminado la ""/" `symbol at the beginning of the URL. For the API `/storage/volumes`, agregar `storage/volumes.`

La URL adjunta es: `/gateways/{uuid}/storage/volumes`

Al ejecutar el `GET` En funcionamiento, la URL generada es la siguiente:
`GEThttps://<hostname\>/api/gateways/<cluster_UUID\>/storage/volumes`

La `/api` La etiqueta de la URL DE REST de ONTAP se elimina en la URL adjunta y se conserva la de la API de puerta de enlace.

Comando de rizo de muestra

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-
9876567890123/storage/volumes" -H "accept: application/hal+json" -H
"Authorization: Basic <Base64EncodedCredentials>"
```

La API muestra la lista de volúmenes de almacenamiento que contiene ese clúster. El formato de respuesta es el mismo que recibe cuando ejecuta la misma API desde ONTAP. Los códigos de estado devueltos son los códigos de estado de REST de ONTAP.

Configuración del alcance de la API

Todas las API tienen un contexto dentro del ámbito del clúster. Las API que operan sobre la base de máquinas virtuales de almacenamiento también tienen el clúster como el alcance, es decir, las operaciones de API se realizan en una máquina virtual de almacenamiento particular dentro de un clúster gestionado. Cuando ejecute el `/gateways/{uuid}/{path}` API, asegúrese de introducir el UUID de clúster (UUID de origen de datos de Unified Manager) para el clúster en el que se ejecuta la operación. Para establecer el contexto de una máquina virtual de almacenamiento determinada dentro de ese clúster, introduzca la clave de la máquina virtual de almacenamiento como el parámetro X-Dot-SVM-UUID o el nombre de la máquina virtual de almacenamiento como el parámetro X-Dot-SVM-Name. El parámetro se añade como filtro del encabezado de cadena y la operación se ejecuta dentro del ámbito de ese equipo virtual de almacenamiento dentro de ese clúster.

Comando de rizo de muestra

```
curl -X GET "https://<hostname>/api/gateways/e4f33f90-f75f-11e8-9ed9-
00a098e3215f/storage/volume" -H "accept: application/hal+json" -H "X-Dot-
SVM-UUID: d9c33ec0-5b61-11e9-8760-00a098e3215f"
-H "Authorization: Basic <Base64EncodedCredentials>"
```

Para obtener más información sobre el uso de las API de REST de ONTAP, consultehttps://docs.netapp.com/us-en/ontap-automation/index.html["Automatización de la API DE REST de ONTAP"]

Realización de tareas administrativas mediante API

Puede usar las API en `administration` Categoría para modificar la configuración de copia de seguridad, verificar la información del archivo de copia de seguridad y los certificados del clúster, así como gestionar los clústeres de ONTAP como orígenes de datos de Active IQ Unified Manager.

Debe tener la función Administrador de aplicaciones para ejecutar estas operaciones. También puede usar la interfaz de usuario web de Unified Manager para configurar estos ajustes.

Verbo HTTP	Ruta	Descripción

`GET`
 	
`PATCH`
	`/admin/backup-settings`
	
	`/admin/backup-settings`
		Puede utilizar el `GET` Método para ver la configuración de la programación de backup configurada en Unified Manager de forma predeterminada. Puede verificar lo siguiente:
		• Si la programación está habilitada o deshabilitada
		• Frecuencia del backup programado (diario o semanal)
		• Hora del backup
		• Número máximo de archivos de copia de seguridad que se deben conservar en la aplicación
		
		La hora de la copia de seguridad se encuentra en la zona horaria del servidor.
		
		La configuración de backup de la base de datos se encuentra disponible en Unified Manager de forma predeterminada, y no se puede crear una programación de backup. Sin embargo, puede utilizar la `PATCH` método para modificar la configuración predeterminada.

Verbo HTTP	Ruta	Descripción
GET	/admin/backup-file-info	Se genera un archivo de volcado de backup cada vez que se modifica la programación de backup para Unified Manager. Puede utilizar este método para comprobar si el archivo de copia de seguridad se genera según la configuración de copia de seguridad modificada y si la información del archivo coincide con la configuración modificada.
GET	/admin/datasource-certificate	Puede usar este método para ver el certificado de origen de datos (clúster) desde el almacén de confianza. Es necesario validar el certificado antes de agregar un clúster de ONTAP como origen de datos de Unified Manager.
GET POST PATCH DELETE	/admin/datasources/clusters /admin/datasources/clusters/{key}	Puede utilizar el GET Método para recuperar los detalles de los orígenes de datos (clústeres de ONTAP) gestionados por Unified Manager. También puede agregar un clúster nuevo a Unified Manager como origen de datos. Para añadir un clúster, debe conocer el nombre de host, el nombre de usuario y la contraseña. Para modificar y eliminar un clúster gestionado como origen de datos por Unified Manager, utilice la clave de clúster de ONTAP.

Gestionar usuarios mediante API

Puede usar las API del security Categoría para controlar el acceso del usuario a los objetos de clúster seleccionados en Active IQ Unified Manager. Es posible añadir usuarios locales o usuarios de la base de datos. También puede agregar usuarios o grupos remotos que pertenecen a un servidor de autenticación. Según los privilegios de los roles que se asignan a los usuarios, pueden gestionar los objetos de almacenamiento o ver los datos en Unified Manager.

Debe tener la función Administrador de aplicaciones para ejecutar estas operaciones. También puede usar la interfaz de usuario web de Unified Manager para configurar estos ajustes.

Las API bajo el `security` category utiliza el parámetro users, que es el nombre de usuario, y no el parámetro key como identificador único de la entidad de usuario.

Verbo HTTP	Ruta	Descripción

`GET`
 	
`POST`
	`/security/users`
	
	`/security/users`
		Es posible usar estos métodos para obtener los detalles de los usuarios o añadir un usuario nuevo a Unified Manager.
		
		Puede añadir roles específicos a los usuarios en función de sus tipos de usuario. Mientras añade usuarios, debe proporcionar contraseñas para el usuario local, el usuario de mantenimiento y el usuario de la base de datos.

`GET`
 	
`PATCH`
 	
`DELETE`
	`/security/users/{name}`	El método GET permite recuperar todos los detalles de un usuario, como el nombre, la dirección de correo electrónico, el rol, el tipo de autorización. El método DE REVISIÓN permite actualizar los detalles. El método DELETE le permite eliminar al usuario.

Ver las métricas de rendimiento mediante API

Active IQ Unified Manager le proporciona un conjunto de API en `/datacenter` categoría que permite ver los datos de rendimiento de los clústeres y los objetos de almacenamiento en un centro de datos. Estas API recuperan los datos de rendimiento de los diferentes objetos de almacenamiento, como clústeres, nodos, LUN, volúmenes, agregados Máquinas virtuales de almacenamiento, interfaces FC, puertos FC, puertos Ethernet e interfaces IP.

La `/metrics` y.. `/analytics` Las API ofrecen distintas vistas de las métricas de rendimiento, mediante las cuales, puede obtener un análisis de los siguientes niveles de detalles sobre los siguientes objetos de almacenamiento en su centro de datos:

- de clúster
- nodos
- Máquinas virtuales de almacenamiento
- agregados
- volúmenes

- LUN
- Interfaces FC
- Puertos FC
- Puertos Ethernet
- Interfaces IP

La siguiente tabla dibuja una comparación entre `/metrics` y.. `/analytics` API con respecto a los detalles de los datos de rendimiento recuperados.

Métricas	**Análisis**
Detalles de rendimiento para un único objeto. Por ejemplo, la `/datacenter/cluster/clusters/{key}/metrics` API requiere que se introduzca la clave de clúster como el parámetro path para recuperar las métricas de ese clúster específico.	Detalles de rendimiento para varios objetos del mismo tipo en un centro de datos. Por ejemplo, la `/datacenter/cluster/clusters/analytics` La API recupera las métricas colectivas de todos los clústeres de un centro de datos.
Muestra de métricas de rendimiento para un objeto de almacenamiento según el parámetro de intervalo de tiempo para la recuperación.	El valor agregado de alto nivel de rendimiento para un determinado tipo de objeto de almacenamiento durante un determinado período (por encima de 72 horas).
Se recuperan detalles básicos del objeto, como los detalles de un nodo o de un clúster.	No se recuperan detalles específicos.
Los contadores acumulados, como mínimo, máximo, percentil 95o y los valores de rendimiento promedio durante un período de tiempo se recuperan para un único objeto, como contadores de lectura, escritura, total y otros.	Se muestra un único valor agregado para todos los objetos del mismo tipo.

Métricas	Análisis
El intervalo de tiempo y los datos de muestra se basan en la siguiente programación: El intervalo de tiempo de los datos. Los ejemplos pueden ser 1h, 12h, 1d, 2d, 3d, 15d, 1w, 1 m, 2 m, 3 m, 6 millones Recibirá muestras de 1 hora si el intervalo es superior a 3 días (72 horas); de lo contrario, son muestras de 5 minutos. El período de cada intervalo de tiempo es el siguiente: • 1h: Métricas de la última hora muestreadas en 5 minutos. • 12h: Métricas de las últimas 12 horas muestreadas en 5 minutos. • 1d: Métricas durante el día más reciente muestreadas durante 5 minutos. • 2d: Métricas de los últimos 2 días muestreadas durante 5 minutos. • 3d: Métricas de los últimos 3 días muestreadas en 5 minutos. • 15d: Métricas de los últimos 15 días muestreadas durante 1 hora. • 1w: Métricas de la semana más reciente muestreadas durante 1 hora. • 1 m: Métricas durante el último mes muestreadas durante 1 hora. • 2 m: Métricas de los últimos 2 meses, muestreadas en 1 hora. • 3M: Métricas de los últimos 3 meses muestreadas durante 1 hora. • 6m: Métricas de los últimos 6 meses muestreados en 1 hora. Valores disponibles: 1h, 12h, 1d, 2d, 3d, 15d, 1w, 1 m, 2 m, 3 m, 6 millones Valor predeterminado : 1h	Más de 72 horas. La duración sobre la que se calcula esta muestra se representa en el formato estándar ISO-8601.

Ejemplo de salida para API de métricas

Por ejemplo, la `/datacenter/cluster/nodes/{key}/metrics` API recupera los siguientes detalles (entre otros) de un nodo:

El percentil 95 del valor resumido indica que el 95% de las muestras recogidas para el período tienen un valor de contador inferior al valor especificado como percentil 95.

```
{
     "iops": {
       "local": {
         "other": 100.53,
         "read": 100.53,
         "total": 100.53,
         "write": 100.53
       },
       "other": 100.53,
       "read": 100.53,
       "total": 100.53,
       "write": 100.53
     },
     "latency": {
       "other": 100.53,
       "read": 100.53,
       "total": 100.53,
       "write": 100.53
     },
     "performance_capacity": {
       "available_iops_percent": 0,
       "free_percent": 0,
       "system_workload_percent": 0,
       "used_percent": 0,
       "user_workload_percent": 0
     },
     "throughput": {
       "other": 100.53,
       "read": 100.53,
       "total": 100.53,
       "write": 100.53
     },
     "timestamp": "2018-01-01T12:00:00-04:00",
     "utilization_percent": 0
   }
 ],
 "start_time": "2018-01-01T12:00:00-04:00",
 "summary": {
   "iops": {
     "local_iops": {
       "other": {
         "95th_percentile": 28,
         "avg": 28,
         "max": 28,
         "min": 5
       },
```

```
      "read": {
        "95th_percentile": 28,
        "avg": 28,
        "max": 28,
        "min": 5
      },
      "total": {
        "95th_percentile": 28,
        "avg": 28,
        "max": 28,
        "min": 5
      },
      "write": {
        "95th_percentile": 28,
        "avg": 28,
        "max": 28,
        "min": 5
      }
    },
```

Muestra de salida para las API de análisis

Por ejemplo, la `/datacenter/cluster/nodes/analytics` API recupera los siguientes valores (entre otros) de todos los nodos:

```
{     "iops": 1.7471,
     "latency": 60.0933,
     "throughput": 5548.4678,
     "utilization_percent": 4.8569,
     "period": 72,
     "performance_capacity": {
       "used_percent": 5.475,
       "available_iops_percent": 168350
     },
     "node": {
       "key": "37387241-8b57-11e9-8974-
00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a",
       "uuid": "95f94e8d-8b4e-11e9-8974-00a098e0219a",
       "name": "ocum-infinity-01",
       "_links": {
         "self": {
           "href": "/api/datacenter/cluster/nodes/37387241-8b57-11e9-8974-
00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a"
         }
       }
     },
     "cluster": {
       "key": "37387241-8b57-11e9-8974-
00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a",
       "uuid": "37387241-8b57-11e9-8974-00a098e0219a",
       "name": "ocum-infinity",
       "_links": {
         "self": {
           "href": "/api/datacenter/cluster/clusters/37387241-8b57-11e9-
8974-00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a"
         },
     "_links": {
       "self": {
         "href": "/api/datacenter/cluster/nodes/analytics"
       }
     }
   },
```


Lista de las API disponibles

En la siguiente tabla se describe el `/metrics` y.. `/analytics` API más detalles.

Las métricas de IOPS y rendimiento que devuelven estas API son, por ejemplo, valores dobles `100.53`. No se admite el filtrado de estos valores flotantes por los caracteres de tubería (|) y comodín (*).

HTTP Verbo	Ruta	Descripción
GET	/datacenter/cluster/clusters/{key}/metrics	Recupera los datos de rendimiento (muestra y resumen) de un clúster especificado por el parámetro de entrada de la clave de clúster. Se devuelve información, como la clave de clúster y el UUID, el intervalo de tiempo, las IOPS, el rendimiento y el número de muestras.
GET	/datacenter/cluster/clusters/analytics	Recupera métricas de alto nivel de rendimiento para todos los clústeres de un centro de datos. Puede filtrar los resultados en función de los criterios requeridos. Se devuelven valores, como el número de IOPS agregado, el rendimiento y el período de recogida (en horas).
GET	/datacenter/cluster/nodes/{key}/metrics	Recupera datos de rendimiento (muestra y resumen) de un nodo especificado por el parámetro de entrada de la clave del nodo. Se muestra información, como el UUID de nodo, el intervalo de tiempo, el resumen de las IOPS, el rendimiento, la latencia y el rendimiento, el número de muestras recogidas y el porcentaje utilizado.
GET	/datacenter/cluster/nodes/analytics	Recupera métricas de alto nivel de rendimiento para todos los nodos de un centro de datos. Puede filtrar los resultados en función de los criterios requeridos. Se devuelve información, como las claves de nodo y de clúster, y valores, como las IOPS agregadas, el rendimiento y el período de recogida (en horas).

HTTP Verbo	Ruta	Descripción
GET	/datacenter/storage/aggregates/{key}/metrics	Recupera datos de rendimiento (ejemplo y resumen) de un agregado especificado por el parámetro de entrada de la clave de agregado. Se muestra información, como el intervalo de tiempo, el resumen de IOPS, la latencia, el rendimiento y la capacidad de rendimiento, el número de muestras recogidas para cada contador y el porcentaje utilizado.
GET	/datacenter/storage/aggregates/analytics	Recupera métricas de alto nivel de rendimiento de todos los agregados de un centro de datos. Puede filtrar los resultados en función de los criterios requeridos. Se devuelve información, como las claves de agregado y de clúster, y valores, como las IOPS agregadas, el rendimiento y el período de recogida (en horas).
GET	/datacenter/storage/luns/{key}/metrics /datacenter/storage/volumes/{key}/metrics	Recupera datos de rendimiento (muestra y resumen) de un LUN o un recurso compartido de archivos (volumen) especificado por el parámetro de entrada de la clave de volumen o LUN. Información, como el resumen de la cantidad mínima, máxima y promedio de las IOPS de lectura, escritura y total, la latencia y el rendimiento, y se devuelve el número de muestras recogidas para cada contador.
GET	/datacenter/storage/luns/analytics /datacenter/storage/volumes/analytics	Recupera métricas de rendimiento de alto nivel para todas las LUN o volúmenes en un centro de datos. Puede filtrar los resultados en función de los criterios requeridos. Se devuelve información, como la máquina virtual de almacenamiento y las claves del clúster, así como valores, como el número de IOPS agregadas, el rendimiento y el período de recogida (en horas).

HTTP Verbo	Ruta	Descripción
GET	`/datacenter/svm/svms/{key}/metrics`	Recupera datos de rendimiento (muestra y resumen) de una máquina virtual de almacenamiento especificada por el parámetro de entrada de la clave de máquina virtual de almacenamiento. Un resumen de las IOPS basado en cada protocolo admitido, por ejemplo `nvmf, fcp, iscsi,` y.. `nfs`se devuelven , procesamiento, latencia y el número de muestras recogidas.
GET	`/datacenter/svm/svms/analytics`	Recupera métricas de alto nivel de rendimiento para todos los equipos virtuales de almacenamiento de un centro de datos. Puede filtrar los resultados en función de los criterios requeridos. Se devuelve información, como el UUID de máquinas virtuales de almacenamiento, las IOPS agregadas, la latencia, el rendimiento y el período de recogida (en horas).
GET	`/datacenter/network/ethernet/ports/{key}/metrics`	Recupera las métricas de rendimiento para un puerto ethernet específico especificado por el parámetro de entrada de la clave de puerto. Cuando se proporciona un intervalo (intervalo de tiempo) desde el intervalo admitido, la API devuelve los contadores acumulados, como valores mínimo, máximo y promedio de rendimiento durante el período de tiempo.

HTTP Verbo	Ruta	Descripción
GET	/datacenter/network/ethernet/ports/analytics	Recupera las métricas de alto nivel de rendimiento de todos los puertos ethernet del entorno del centro de datos. Se devuelve información, como la clave de clúster y nodo, y el UUID, el rendimiento, el período de recopilación y el porcentaje de utilización de los puertos. Puede filtrar el resultado por los parámetros disponibles, como la clave de puerto, el porcentaje de utilización, el nombre y el UUID del clúster y el nodo, etc.
GET	/datacenter/network/fc/interfaces/{key}/metrics	Recupera las métricas de rendimiento de una interfaz de FC de red específica especificada por el parámetro de entrada de la clave de interfaz. Cuando se proporciona un intervalo (intervalo de tiempo) desde el intervalo admitido, la API devuelve los contadores acumulados, como valores mínimo, máximo y promedio de rendimiento durante el período de tiempo.
GET	/datacenter/network/fc/interfaces/analytics	Recupera las métricas de alto nivel de rendimiento de todos los puertos ethernet del entorno del centro de datos. Se obtiene información, como la clave de interfaz del clúster y FC, y el UUID, el rendimiento, las IOPS, la latencia y la máquina virtual de almacenamiento. Puede filtrar el resultado por los parámetros disponibles, como el nombre y el UUID de la interfaz de FC y el clúster, la máquina virtual de almacenamiento, el rendimiento, etc.

HTTP Verbo	Ruta	Descripción
GET	/datacenter/network/fc/ports/{key}/metrics	Recupera las métricas de rendimiento de un puerto FC específico especificado por el parámetro de entrada de la clave de puerto. Cuando se proporciona un intervalo (intervalo de tiempo) desde el intervalo admitido, la API devuelve los contadores acumulados, como valores mínimo, máximo y promedio de rendimiento durante el período de tiempo.
GET	/datacenter/network/fc/ports/analytics	Recupera las métricas de rendimiento de alto nivel para todos los puertos FC del entorno de centro de datos. Se devuelve información, como la clave de clúster y nodo, y el UUID, el rendimiento, el período de recopilación y el porcentaje de utilización de los puertos. Puede filtrar el resultado por los parámetros disponibles, como la clave de puerto, el porcentaje de utilización, el nombre y el UUID del clúster y el nodo, etc.
GET	/datacenter/network/ip/interfaces/{key}/metrics	Recupera las métricas de rendimiento de una interfaz IP de red según lo especificado por el parámetro de entrada de la clave de interfaz. Cuando se proporciona un intervalo (intervalo de tiempo) desde el intervalo admitido, la API devuelve información, como el número de muestras, los contadores acumulados, el rendimiento y el número de paquetes recibidos y transmitidos.

HTTP Verbo	Ruta	Descripción
GET	/datacenter/network/ip/interfaces/analytics	Recupera las métricas de alto nivel de rendimiento de todas las interfaces IP de red del entorno del centro de datos. Se devuelve información, como la clave de interfaz IP y el UUID, el rendimiento, las IOPS y la latencia. Puede filtrar el resultado por los parámetros disponibles, como el nombre y el UUID de la interfaz IP y el clúster, las IOPS, la latencia, el rendimiento, etc.

Ver trabajos y detalles del sistema

Puede utilizar el `jobs` API en la `management-server` categoría para ver los detalles de ejecución de las operaciones asíncronas. La `system` API en la `management-server` Category le permite ver los detalles de la instancia en el entorno de Active IQ Unified Manager.

Ver trabajos

En Active IQ Unified Manager, las operaciones, como añadir y modificar recursos, se realizan mediante invocaciones de API síncronas y asíncronas. Un objeto Job creado para esa invocación puede realizar el seguimiento de las invocaciones programadas para la ejecución asíncrona. Cada objeto de trabajo tiene una clave única para su identificación. Cada objeto Job devuelve el URI del objeto Job al que tiene acceso y realiza un seguimiento del progreso del trabajo. Puede utilizar esta API para recuperar los detalles de cada ejecución.

Al usar esta API, puede consultar todos los objetos Job del centro de datos, incluidos los datos históricos. Al consultar todos los trabajos, de forma predeterminada, se devuelven los detalles de los últimos 20 trabajos activados a través de la interfaz de usuario web y la interfaz de API. Utilice los filtros incorporados para ver trabajos específicos. También puede utilizar la tecla Trabajo para consultar los detalles de un trabajo específico y ejecutar el siguiente conjunto de operaciones en los recursos.

Categoría	Verbo HTTP	Ruta	Descripción
servidor de gestión	OBTENGA	/management-server/jobs	Devuelve los detalles del trabajo de todos los trabajos. Sin ningún orden de clasificación, el último objeto de trabajo enviado se devuelve en la parte superior.

Categoría	Verbo HTTP	Ruta	Descripción
servidor de gestión	OBTENGA	`/management-server/jobs/{key}` Introduzca la clave de trabajo del objeto Job para ver los detalles específicos de ese trabajo.	Devuelve los detalles del objeto Job específico.

Ver los detalles del sistema

Mediante el uso de `/management-server/system` API, puede consultar los detalles específicos de cada instancia del entorno de Unified Manager. La API muestra información sobre el producto y los servicios, como la versión de Unified Manager instalada en el sistema, UUID, nombre del proveedor, SO del host y el nombre, Descripción y estado de los servicios que se ejecutan en la instancia de Unified Manager.

Categoría	Verbo HTTP	Ruta	Descripción
servidor de gestión	OBTENGA	`/management-server/system`	No se requiere ningún parámetro de entrada para ejecutar esta API. Los detalles del sistema de la instancia actual de Unified Manager se devuelven de forma predeterminada.

Gestionar eventos y alertas mediante API

La `events`, `alerts`, y. `scripts` API en la `management-server` La categoría le permite gestionar los eventos, las alertas y los scripts asociados con las alertas de su entorno Active IQ Unified Manager.

Ver y modificar eventos

Unified Manager recibe los eventos que se generan en ONTAP en los clústeres supervisados y gestionados por Unified Manager. Mediante estas API, puede ver los eventos generados para los clústeres y resolverlos y actualizarlos.

Ejecutando el `GET` método para `/management-server/events` API, puede consultar los eventos en su centro de datos, incluidos los datos históricos. Utilice los filtros incorporados, como el nombre, el nivel de impacto, el área de impacto, la gravedad, estado, nombre de recurso y tipo de recurso para ver eventos específicos. El tipo de recurso y los parámetros de área devuelven información sobre el objeto de almacenamiento en el que se produce el evento. El área de impacto devuelve la información sobre el problema sobre el que se genera el evento, como disponibilidad, capacidad, configuración, seguridad, protección y rendimiento.

Al ejecutar la operación DE REVISIÓN para esta API, puede habilitar el flujo de trabajo de resolución para el evento. Puede asignar un evento a usted mismo u otro usuario y confirmar la recepción del evento. Al realizar

los pasos en los recursos para resolver el problema que activó el evento, puede usar esta API para marcar el evento como solucionado.

Para obtener más información acerca de los eventos, consulte "Gestión de eventos".

Categoría	Verbo HTTP	Ruta	Descripción
servidor de gestión	OBTENGA	`/management-server/events` `/management-server/events/{key}`	Cuando ejecuta el método Get ALL, el cuerpo de respuesta consta de los detalles del evento de todos los eventos del centro de datos. Cuando se recuperan los detalles del evento por una clave específica, se pueden ver los detalles de un evento específico y se ejecuta el siguiente conjunto de operaciones en los recursos. El cuerpo de respuesta consta de los detalles de ese evento.
servidor de gestión	PARCHE	`management-server/events/{key}`	Ejecute esta API para asignar un evento o cambiar el estado a reconocido o resuelto. También puede utilizar este método para asignar el evento a usted mismo u otro usuario. Es una operación síncrona.

Gestión de alertas

Los eventos se generan de forma automática y continua. Unified Manager genera una alerta solo cuando un evento cumple ciertos criterios de filtro. Puede seleccionar los eventos para los que se deben generar alertas. Mediante el uso de `/management-server/alerts` API, es posible configurar alertas para que se envíen notificaciones automáticamente cuando se produzcan eventos o eventos específicos de ciertos tipos de gravedad.

Para obtener más información sobre las alertas, consulte "Gestión de alertas".

Categoría	Verbo HTTP	Ruta	Descripción
servidor de gestión	OBTENGA	`/management-server/alerts` `/management-server/alerts/{key}`	Consulte todas las alertas existentes en su entorno o una alerta específica con la clave de alerta. Puede ver la información sobre las alertas que genera su entorno, como la descripción de alertas, la acción, el ID de correo electrónico al que se envía la notificación, el evento y la gravedad.
servidor de gestión	PUBLICAR	`/management-server/alerts`	Este método le permite agregar alertas para eventos específicos. Debe añadir el nombre de alerta, el recurso físico o lógico o el evento donde corresponda la alerta, si está habilitada y si emite capturas SNMP. Puede añadir detalles adicionales sobre los que desea generar la alerta, como la acción, el ID de correo electrónico de notificación, los detalles del script, por si se añade un script de alerta, etc.
servidor de gestión	APLICAR PARCHES y ELIMINARLOS	`management-server/events/{key}`	Puede usar estos métodos para modificar y eliminar alertas específicas. Puede modificar distintos atributos, como la descripción, el nombre y la habilitación y deshabilitación de la alerta. Es posible eliminar una alerta cuando ya no se necesita.

Mientras se selecciona un recurso para añadir una alerta, tenga en cuenta que al seleccionar un clúster como el recurso no se seleccionan automáticamente los objetos de almacenamiento en ese clúster. Por ejemplo, si crea una alerta para todos los eventos críticos de todos los clústeres, solo recibirá alertas para los eventos críticos del clúster. No recibirá alertas sobre eventos críticos en nodos, agregados, etc.

Administrar scripts

Mediante el uso de `/management-server/scripts` API, también puede asociar una alerta a un script que se ejecuta cuando se activa una alerta. Es posible usar scripts para modificar o actualizar automáticamente varios objetos de almacenamiento en Unified Manager. El script está asociado a una alerta. Cuando un evento activa una alerta, se ejecuta el script. Puede cargar scripts personalizados y probar su ejecución cuando se genera una alerta. Es posible asociar una alerta a la secuencia de comandos para que se ejecute el script cuando se genera una alerta para un evento en Unified Manager.

Para obtener más información acerca de los scripts, consulte "Administrar scripts".

Categoría	Verbo HTTP	Ruta	Descripción
servidor de gestión	OBTENGA	`/management-server/scripts`	Utilice esta API para consultar todas las secuencias de comandos existentes en su entorno. Utilice el filtro estándar y las operaciones Order by para ver sólo secuencias de comandos específicas.
servidor de gestión	PUBLICAR	`/management-server/scripts`	Utilice esta API para agregar una descripción del script y cargar el archivo de script asociado a una alerta.

Gestionar cargas de trabajo mediante API

Las API descritas aquí abarcan varias funciones de administración del almacenamiento, como ver las cargas de trabajo de almacenamiento, crear LUN y recursos compartidos de archivos, gestionar niveles de servicio de rendimiento y políticas de eficiencia del almacenamiento y asignar las políticas en cargas de trabajo de almacenamiento.

Ver cargas de trabajo de almacenamiento mediante API

Las API que se enumeran aquí le permiten ver una lista consolidada de cargas de trabajo de almacenamiento para todos los clústeres ONTAP en su centro de datos. Las API también proporcionan una vista de resumen del número de cargas de trabajo de almacenamiento aprovisionadas en el entorno de Active IQ Unified Manager, y sus estadísticas de capacidad y rendimiento (IOPS).

Ver cargas de trabajo de almacenamiento

Puede usar el siguiente método para ver todas las cargas de trabajo de almacenamiento de todos los clústeres del centro de datos. Para obtener información sobre el filtrado de la respuesta en función de columnas específicas, consulte la documentación de referencia de API disponible en la instancia de Unified Manager.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	OBTENGA	`/storage-provider/workloads`

Ver resumen de las cargas de trabajo de almacenamiento

Puede utilizar el siguiente método para evaluar la capacidad utilizada, la capacidad disponible, los IOPS usados, las IOPS disponibles y el número de cargas de trabajo de almacenamiento gestionadas por cada nivel de servicio de rendimiento. Las cargas de trabajo de almacenamiento que se muestran pueden ser para cualquier LUN, recurso compartido de archivos NFS o recurso compartido CIFS. La API proporciona información general sobre las cargas de trabajo de almacenamiento, una descripción general de las cargas de trabajo de almacenamiento aprovisionadas por Unified Manager, una información general sobre centros de datos, una descripción general de todo, usado y el espacio y las IOPS disponibles en el centro de datos, en términos de niveles de servicio de rendimiento asignados. La información que se recibe en respuesta a esta API se utiliza para completar la consola en la interfaz de usuario de Unified Manager.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	OBTENGA	`/storage-provider/workloads-summary`

Gestión de extremos de acceso mediante API

Necesita crear extremos de acceso o interfaces lógicas (LIF), que se necesitan para aprovisionar las máquinas virtuales de almacenamiento (SVM), las LUN y los recursos compartidos de archivos. Puede ver, crear, modificar y eliminar los extremos de acceso de las SVM, las LUN o los recursos compartidos de archivos en el entorno de Active IQ Unified Manager.

Ver extremos de acceso

Se puede ver una lista de extremos de acceso en el entorno de Unified Manager mediante el siguiente método. Para consultar una lista de extremos de acceso de una SVM, una LUN o un recurso compartido de archivos concretos, debe introducir el identificador único de la SVM, la LUN o el recurso compartido de archivos. También es posible introducir la clave de extremo de acceso única para recuperar los detalles del extremo de acceso en particular.

Categoría	Verbo HTTP	Ruta

proveedor de almacenamiento	OBTENGA	`/storage-provider/access-endpoints`
		
		`/storage-provider/access-endpoints/{key}`

Agregar extremos de acceso

Puede crear extremos de acceso personalizados y asignarle propiedades necesarias. Debe introducir los detalles del extremo de acceso que desea crear como parámetros de entrada. Puede usar esta API, o la

interfaz de línea de comandos de System Manager o ONTAP para crear un extremo de acceso en cada nodo. Tanto las direcciones IPv4 como IPv6 son compatibles con la creación de extremos de acceso.

Debe configurar su SVM con una cantidad mínima de extremos de acceso por nodo para que el aprovisionamiento se realice correctamente de LUN y recursos compartidos de archivos. Debe configurar su SVM con al menos dos extremos de acceso por nodo, uno que admita CIFS y/o el protocolo NFS, otro que admita el protocolo iSCSI o FCP.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PUBLICAR	`/storage-provider/access-endpoints`

Eliminar extremos de acceso

Puede eliminar un extremo de acceso específico mediante el siguiente método. Debe proporcionar la clave de extremo de acceso como parámetro de entrada para eliminar un extremo de acceso determinado.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	ELIMINAR	`/storage-provider/access-endpoints/{key}`

Modificar los extremos de acceso

Puede modificar un extremo de acceso y actualizar sus propiedades mediante el método siguiente. Debe proporcionar la clave de extremo de acceso para modificar un extremo de acceso determinado. También debe introducir la propiedad que desea actualizar junto con su valor.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PARCHE	`/storage-provider/access-endpoints/{key}`

Gestión de la asignación de Active Directory mediante API

Puede utilizar las API que aparecen aquí para gestionar las asignaciones de Active Directory en la SVM que se necesitan para aprovisionar recursos compartidos de CIFS en las SVM. Es necesario configurar las asignaciones de Active Directory para asignar las SVM con ONTAP.

Ver las asignaciones de Active Directory

Puede ver los detalles de configuración de las asignaciones de Active Directory para una SVM mediante el siguiente método. Para ver las asignaciones de Active Directory en una SVM, debe introducir la clave de SVM. Para consultar los detalles de una asignación concreta, debe introducir la clave de asignación.

Categoría	Verbo HTTP	Ruta

proveedor de almacenamiento	OBTENGA	`/storage-provider/active-directories-mappings`
		
		`/storage-provider/active-directories-mappings/{key}`

Agregue la asignación de Active Directory

Puede crear asignaciones de Active Directory en una SVM mediante el método siguiente. Como parámetros de entrada, debe introducir los detalles de asignación.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PUBLICAR	`/storage-provider/active-directories-mappings`

Gestionar recursos compartidos de archivos mediante API

Puede utilizar el `/storage-provider/file-shares` API para ver, añadir, modificar y eliminar los volúmenes compartidos de archivos CIFS y NFS en su entorno de centro de datos.

Antes de aprovisionar los volúmenes de recursos compartidos de archivos, asegúrese de que la SVM se haya creado y aprovisionado con los protocolos compatibles. Si va a asignar niveles de servicio de rendimiento (PSLs) o políticas de eficiencia del almacenamiento (PEPs) durante el aprovisionamiento, se deben crear los PSLs o PES antes de crear los recursos compartidos de archivos.

Ver recursos compartidos de archivos

Puede usar el siguiente método para ver los volúmenes para compartir archivos disponibles en el entorno de Unified Manager. Cuando añadió un clúster ONTAP como origen de datos en Active IQ Unified Manager, las cargas de trabajo de almacenamiento para esos clústeres se añaden automáticamente a la instancia de Unified Manager. Esta API recupera los recursos compartidos de archivos de forma automática y manual se añaden a la instancia de Unified Manager. Para ver los detalles de un recurso compartido de archivos específico, ejecute esta API con la clave de recurso compartido de archivos.

Categoría	Verbo HTTP	Ruta

proveedor de almacenamiento	OBTENGA	`/storage-provider/file-shares`
		
		`/storage-provider/file-shares/{key}`

Agregar recursos compartidos de archivos

Puede utilizar el siguiente método para añadir recursos compartidos de archivos CIFS y NFS en la SVM. Debe introducir los detalles del recurso compartido de archivos que desea crear como parámetros de entrada. No se

puede usar esta API para añadir volúmenes de FlexGroup.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PUBLICAR	`/storage-provider/file-shares`

> En función de si se proporcionan los parámetros de la lista de control de acceso (ACL) o los parámetros de la política de exportación, se crean los recursos compartidos de archivos CIFS o NFS. Si no se proporcionan los valores para los parámetros ACL, no se crean los recursos compartidos de CIFS y los recursos compartidos de NFS se crean de forma predeterminada, proporcionando acceso a todos.

Creación de volúmenes de protección de datos: Cuando se agregan recursos compartidos de archivos a la SVM, el tipo de volumen que está montado, por defecto, es `rw` (lectura y escritura). Para crear volúmenes de protección de datos (DP), especifique `dp` como valor para `type` parámetro.

Eliminar recursos compartidos de archivos

Puede utilizar el siguiente método para eliminar un recurso compartido de archivos específico. Es necesario introducir la clave de recurso compartido de archivos como parámetro de entrada para eliminar un recurso compartido de archivos concreto.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	ELIMINAR	`/storage-provider/file-shares/{key}`

Modificar recursos compartidos de archivos

Puede utilizar el método siguiente para modificar un recurso compartido de archivos y actualizar sus propiedades.

Debe proporcionar la clave de recurso compartido de archivos para modificar un recurso compartido de archivos concreto. Además, debe introducir la propiedad que desea actualizar junto con su valor.

> Tenga en cuenta que sólo puede actualizar una propiedad en una única invocación de esta API. Para varias actualizaciones, debe ejecutar esta API tantas veces.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PARCHE	`/storage-provider/file-shares/{key}`

Gestionar las LUN mediante API

Puede utilizar el `/storage-provider/luns` API para ver, agregar, modificar y eliminar las LUN en su entorno de centro de datos.

Antes de aprovisionar las LUN, asegúrese de que la SVM se ha creado y aprovisionado con los protocolos

compatibles. Si va a asignar niveles de servicio de rendimiento (PSU) o políticas de eficiencia del almacenamiento (SUP) durante el aprovisionamiento, deben crearse los PSLs o SUP antes de crear la LUN.

Ver las LUN

Puede utilizar el siguiente método para ver las LUN en su entorno de Unified Manager. Cuando añadió un clúster ONTAP como origen de datos en Active IQ Unified Manager, las cargas de trabajo de almacenamiento para esos clústeres se añaden automáticamente a la instancia de Unified Manager. Esta API recupera todas las LUN se añaden de forma automática y manual a su instancia de Unified Manager. Para ver los detalles de una LUN específica, ejecute esta API con la clave LUN.

Categoría	Verbo HTTP	Ruta

proveedor de almacenamiento	OBTENGA	`/storage-provider/luns`
		
		`/storage-provider/luns/{key}`

Añada LUN

Puede usar el método siguiente para añadir LUN a las SVM.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PUBLICAR	`/storage-provider/luns`

En la solicitud curl, si proporciona un valor para el parámetro opcional volume_name_tag en la entrada, ese valor se usa al asignar un nombre al volumen durante la creación de la LUN. Esta etiqueta permite buscar el volumen fácilmente. Si se proporciona la clave de volumen en la solicitud, se omite el etiquetado.

Eliminar las LUN

Puede utilizar el siguiente método para eliminar una LUN específica. Debe proporcionar la clave de LUN para eliminar una LUN determinada.

Si ha creado un volumen en ONTAP y, a continuación, ha aprovisionado LUN a través de Unified Manager en ese volumen, cuando elimina todas las LUN con esta API, el volumen también se elimina del clúster de ONTAP.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	ELIMINAR	`/storage-provider/luns/{key}`

Modifique las LUN

Puede utilizar el siguiente método para modificar una LUN y actualizar sus propiedades. Debe proporcionar la clave LUN para modificar una LUN determinada. También debe introducir la propiedad LUN que desea actualizar, junto con su valor. Para actualizar los arrays LUN mediante esta API, debería revisar las recomendaciones de la sección ""recomendaciones para utilizar las API"".

Sólo puede actualizar una propiedad en una única invocación de esta API. Para varias actualizaciones, debe ejecutar esta API tantas veces.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PARCHE	`/storage-provider/luns/{key}`

Gestión de niveles de servicio de rendimiento mediante API

Puede ver, crear, modificar y eliminar niveles de servicio de rendimiento usando las API del proveedor de almacenamiento para su Active IQ Unified Manager.

Ver los niveles de servicio de rendimiento

Puede utilizar el siguiente método para ver los niveles de servicio de rendimiento para asignarles a cargas de trabajo de almacenamiento. La API enumera todos los niveles de servicio de rendimiento definidos por el sistema y creados por el usuario, y recupera los atributos de todos los niveles de servicio de rendimiento. Si desea consultar un nivel de servicio de rendimiento específico, debe introducir el ID único del nivel de servicio de rendimiento para recuperar los detalles.

Categoría	Verbo HTTP	Ruta

proveedor de almacenamiento	OBTENGA	`/storage-provider/performance-service-levels`
		
		`/storage-provider/performance-service-levels/{key}`

Agregue niveles de servicio de rendimiento

Puede utilizar el siguiente método para crear niveles de servicio de rendimiento personalizados y asignarles a sus cargas de trabajo de almacenamiento si los niveles de servicio de rendimiento definidos por el sistema no cumplen los objetivos de nivel de servicio requeridos para las cargas de trabajo de almacenamiento. Introduzca los detalles para el nivel de servicio de rendimiento que desea crear. Para las propiedades de IOPS, asegúrese de introducir un rango válido de valores.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PUBLICAR	`/storage-provider/performance-service-levels`

Elimine niveles de servicio de rendimiento

Puede utilizar el método siguiente para eliminar un nivel de servicio de rendimiento específico. No es posible eliminar un nivel de servicio de rendimiento si se asigna a una carga de trabajo o si es el único nivel de servicio de rendimiento disponible. Debe proporcionar el ID único del nivel de servicio de rendimiento como

parámetro de entrada para eliminar un nivel de servicio de rendimiento determinado.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	ELIMINAR	`/storage-provider/performance-service-levels/{key}`

Modifique los niveles de servicio de rendimiento

Puede utilizar el método siguiente para modificar un nivel de servicio de rendimiento y actualizar sus propiedades. No es posible modificar un nivel de servicio de rendimiento definido por el sistema o asignado a una carga de trabajo. Debe proporcionar el ID único de para modificar un nivel de servicio de rendimiento determinado. También debe introducir la propiedad IOPS que desea actualizar, junto con un valor válido.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PARCHE	`/storage-provider/performance-service-levels/{key}`

Ver las capacidades de agregado en función de los niveles de servicio de rendimiento

Puede utilizar el siguiente método para consultar las funcionalidades de agregado en función de los niveles de servicio de rendimiento. Esta API muestra la lista de agregados disponibles en el centro de datos e indica las funcionalidades en cuanto a los niveles de servicio de rendimiento que pueden admitir estos agregados. Al aprovisionar cargas de trabajo en un volumen, puede ver la funcionalidad de un agregado para admitir un nivel de servicio de rendimiento en particular y aprovisionar cargas de trabajo en función de esa funcionalidad. Su capacidad para especificar el agregado solo está disponible cuando se aprovisiona una carga de trabajo mediante API. Esta funcionalidad no está disponible en la interfaz de usuario web de Unified Manager.

Categoría	Verbo HTTP	Ruta

proveedor de almacenamiento	OBTENGA	`/storage-provider/aggregate-capabilities`
		
		`/storage-provider/aggregate-capabilities/{key}`

Gestión de políticas de eficiencia del almacenamiento mediante API

Puede ver, crear, modificar y eliminar políticas de eficiencia del almacenamiento usando las API del proveedor de almacenamiento.

Tenga en cuenta lo siguiente:

- No es obligatorio asignar una política de eficiencia de almacenamiento al crear una carga de trabajo en Unified Manager.
- No es posible anular la asignación de una política de eficiencia del almacenamiento de una carga de trabajo después de asignarla una política.
- Si una carga de trabajo tiene algunos valores de configuración de almacenamiento especificados en los volúmenes de ONTAP, como la deduplicación y la compresión, esta configuración puede sobrescribirse en la configuración especificada en la Política de eficiencia del almacenamiento que se aplica al añadir las cargas de trabajo de almacenamiento en Unified Manager.

Consulte las políticas de eficiencia del almacenamiento

Puede utilizar el siguiente método para ver las políticas de eficiencia del almacenamiento antes de asignarles cargas de trabajo de almacenamiento. Esta API enumera todas las políticas de eficiencia del almacenamiento definidas por el sistema y creadas por el usuario, y recupera los atributos de todas las políticas de eficiencia del almacenamiento. Si desea consultar una Política de eficiencia de almacenamiento específica, debe introducir el ID único de la política para recuperar sus detalles.

Categoría	Verbo HTTP	Ruta

proveedor de almacenamiento	OBTENGA	`/storage-provider/storage-efficiency-policies`
		
		`/storage-provider/storage-efficiency-policies/{key}`

Añada políticas de eficiencia del almacenamiento

Puede utilizar el siguiente método para crear políticas de eficiencia del almacenamiento personalizadas y asignarlas a sus cargas de trabajo de almacenamiento si las políticas definidas por el sistema no cumplen los requisitos de aprovisionamiento para las cargas de trabajo de almacenamiento. Introduzca los detalles de la Política de eficiencia del almacenamiento que desea crear como parámetros de entrada.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PUBLICAR	`/storage-provider/storage-efficiency-policies`

Eliminar políticas de eficiencia del almacenamiento

Puede utilizar el siguiente método para eliminar una directiva de eficiencia del almacenamiento específica. No puede eliminar una Política de eficiencia del almacenamiento si se asigna a una carga de trabajo o si es la única Política de eficiencia del almacenamiento disponible. Debe proporcionar el ID único de la Política de eficiencia del almacenamiento como parámetro de entrada para eliminar una determinada Política de eficiencia del almacenamiento.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	ELIMINAR	`/storage-provider/storage-efficiency-policies/{key}`

Modificar las políticas de eficiencia del almacenamiento

Puede utilizar el método siguiente para modificar una Política de eficiencia del almacenamiento y actualizar sus propiedades. No es posible modificar una Política de eficiencia del almacenamiento que esté definida por el sistema o que se asigne a una carga de trabajo. Debe proporcionar el ID exclusivo de la normativa de eficiencia del almacenamiento para modificar una determinada política de eficiencia del almacenamiento. Además, debe proporcionar la propiedad que desea actualizar, junto con su valor.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PARCHE	`/storage-provider/storage-efficiency-policies/{key}`

Flujos de trabajo API comunes para la gestión del almacenamiento

Los flujos de trabajo comunes proporcionan a los desarrolladores de aplicaciones cliente ejemplos de cómo puede llamar una aplicación cliente a las API de Active IQ Unified Manager para ejecutar funciones comunes de gestión del almacenamiento. Esta sección contiene algunos de estos flujos de trabajo de ejemplo.

Los flujos de trabajo describen algunos de los casos de uso de gestión del almacenamiento más utilizados, junto con códigos de muestra que puede utilizar. Cada una de las tareas se describe mediante un proceso de flujo de trabajo compuesto por una o más llamadas API.

Llamadas API que se usan en los flujos de trabajo

Es posible ver la página de documentación en línea desde la instancia de Unified Manager que incluye los detalles de cada llamada de API DE REST. Este documento no repite los detalles de la documentación en línea. Cada llamada API utilizada en los ejemplos de flujo de trabajo de este documento incluye solo la información necesaria para localizar la llamada en la página de documentación. Después de localizar una llamada API específica, puede revisar los detalles completos de la llamada, incluidos los parámetros de entrada, formatos de salida, códigos de estado HTTP y tipo de procesamiento de solicitudes.

Se incluye la siguiente información para cada llamada de API dentro de un flujo de trabajo para ayudar a localizar la llamada en la página de documentación:

- Categoría: Las llamadas API se organizan en la página de documentación en categorías o áreas relacionadas con la funcionalidad. Para ubicar una llamada API específica, desplácese hasta la parte inferior de la página y haga clic en la categoría API correspondiente.
- Verbo HTTP (call): El verbo HTTP identifica la acción realizada en un recurso. Cada llamada API se ejecuta a través de un único verbo HTTP.
- Ruta: La ruta determina el recurso específico al que se aplica la acción como parte de la realización de una llamada. La cadena de ruta de acceso se anexa a la URL de núcleo para formar la URL completa que

identifica el recurso.

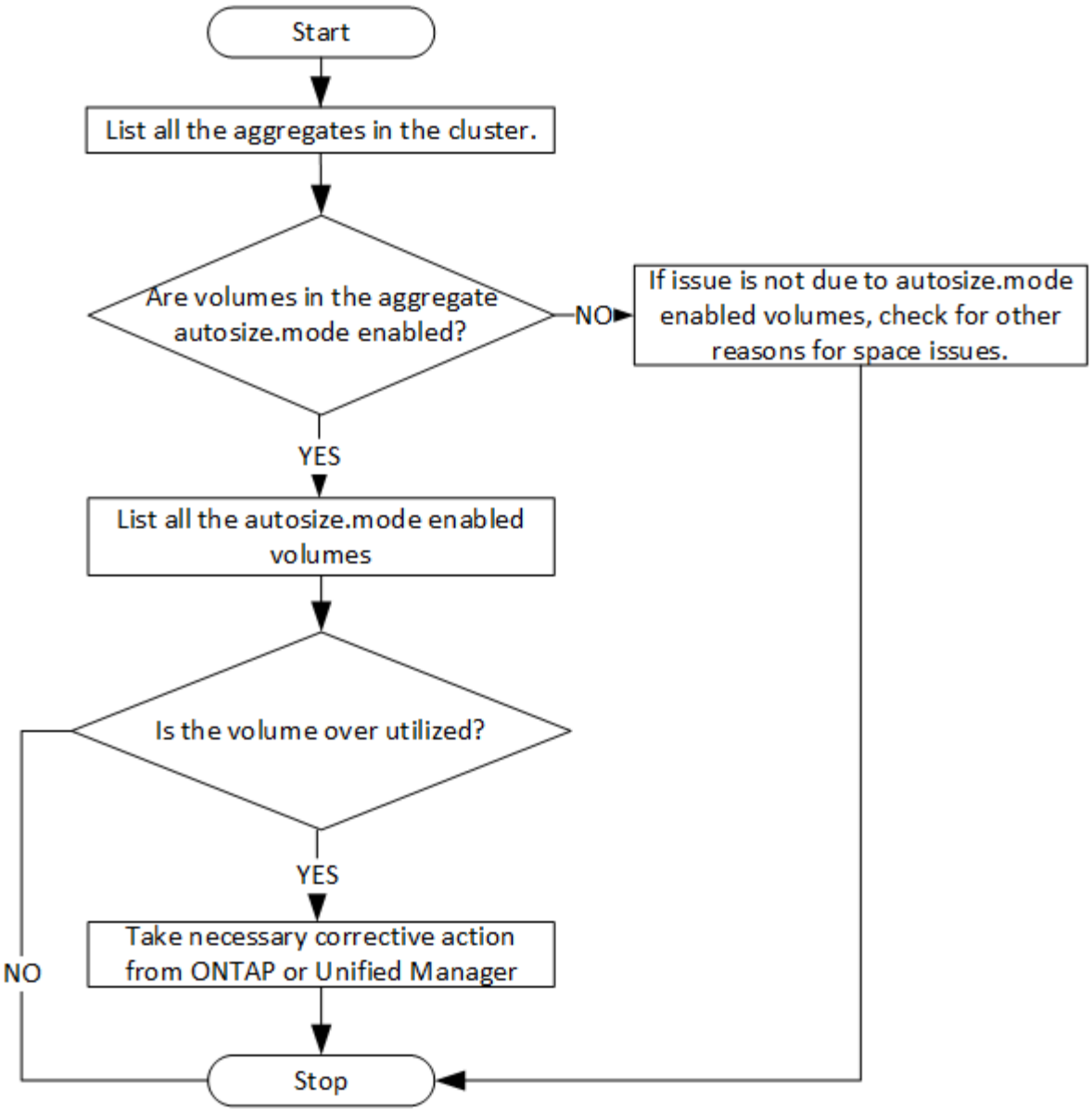
Determinar problemas de espacio en agregados mediante las API

Puede utilizar las API de centro de datos de Active IQ Unified Manager para supervisar la disponibilidad y el uso del espacio en los volúmenes. Puede determinar problemas de espacio de su volumen e identificar recursos de almacenamiento que estén desaprovechados o sobrecargados.

Las API del centro de datos para agregados recuperan la información relevante sobre el espacio disponible y el utilizado, y la configuración de eficiencia que permite ahorrar espacio. También puede filtrar la información recuperada en función de los atributos especificados.

Un método para determinar cualquier falta de espacio en los agregados es verificar si hay volúmenes en su entorno con el modo autosize habilitado. A continuación, debe identificar qué volúmenes se están utilizando en exceso y realizar cualquier acción correctiva.

El siguiente diagrama de flujo ilustra el proceso de recuperación de información acerca de los volúmenes con el modo de ajuste automático activado:



En este flujo se supone que los clústeres ya se han creado en ONTAP y se han añadido a Unified Manager.

1. Obtenga la clave de clúster a menos que conozca el valor:

Categoría	Verbo HTTP	Ruta
centro de datos	OBTENGA	`/datacenter/cluster/clusters`

2. Utilice la clave de clúster como el parámetro filter y consulte los agregados de ese clúster.

Categoría	Verbo HTTP	Ruta
centro de datos	OBTENGA	`/datacenter/storage/aggregates`

3. Desde la respuesta, analice el uso de espacio de los agregados y determine qué agregados tienen problemas de espacio. Para cada agregado con problema de espacio, obtenga la clave de agregado de la misma salida JSON.
4. Con cada clave de agregado, filtre todos los volúmenes que tengan el valor del parámetro autosize.mode como `grow`.

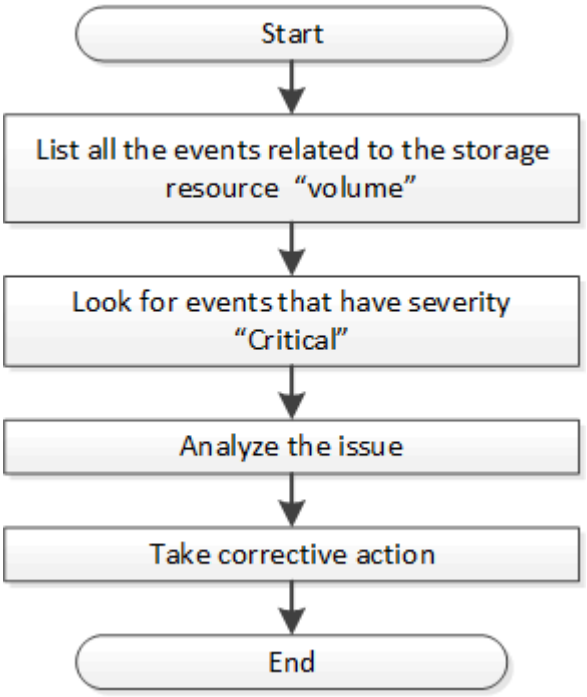
Categoría	Verbo HTTP	Ruta
centro de datos	OBTENGA	`/datacenter/storage/volumes`

5. Analice qué volúmenes se van a utilizar en exceso.
6. Realice cualquier acción correctiva necesaria, por ejemplo, mover el volumen entre agregados para resolver los problemas de espacio del volumen. Es posible realizar estas acciones desde la interfaz de usuario web de ONTAP o Unified Manager.

Determinar problemas en objetos de almacenamiento mediante las API de eventos

Cuando un objeto de almacenamiento de su centro de datos cruza un umbral, se obtiene una notificación de ese evento. Con esta notificación, puede analizar el problema y adoptar medidas correctivas mediante `events` API.

Este flujo de trabajo toma el ejemplo de un volumen como objeto de recurso. Puede utilizar el `events` Las API para recuperar la lista de eventos relacionados con un volumen, analizar los problemas críticos de ese volumen y, a continuación, tomar medidas correctivas para rectificar el problema.



Siga estos pasos para determinar los problemas en su volumen antes de seguir los pasos para solucionarlo.

Pasos

1. Analice las notificaciones de eventos críticos de Active IQ Unified Manager para los volúmenes en el

centro de datos.

2. Consulte todos los eventos de los volúmenes mediante los siguientes parámetros de la API /Management-Server/Events:
   `"resource_type": "volume"`
   `"severity": "critical"`

Categoría	Verbo HTTP	Ruta
servidor de gestión	OBTENGA	/management-servidor/eventos

3. Vea el resultado y analice los problemas en los volúmenes específicos.
4. Realice las acciones necesarias mediante las API de REST o la interfaz de usuario web de Unified Manager para resolver los problemas.

Solución de problemas de volúmenes de ONTAP mediante API de puerta de enlace

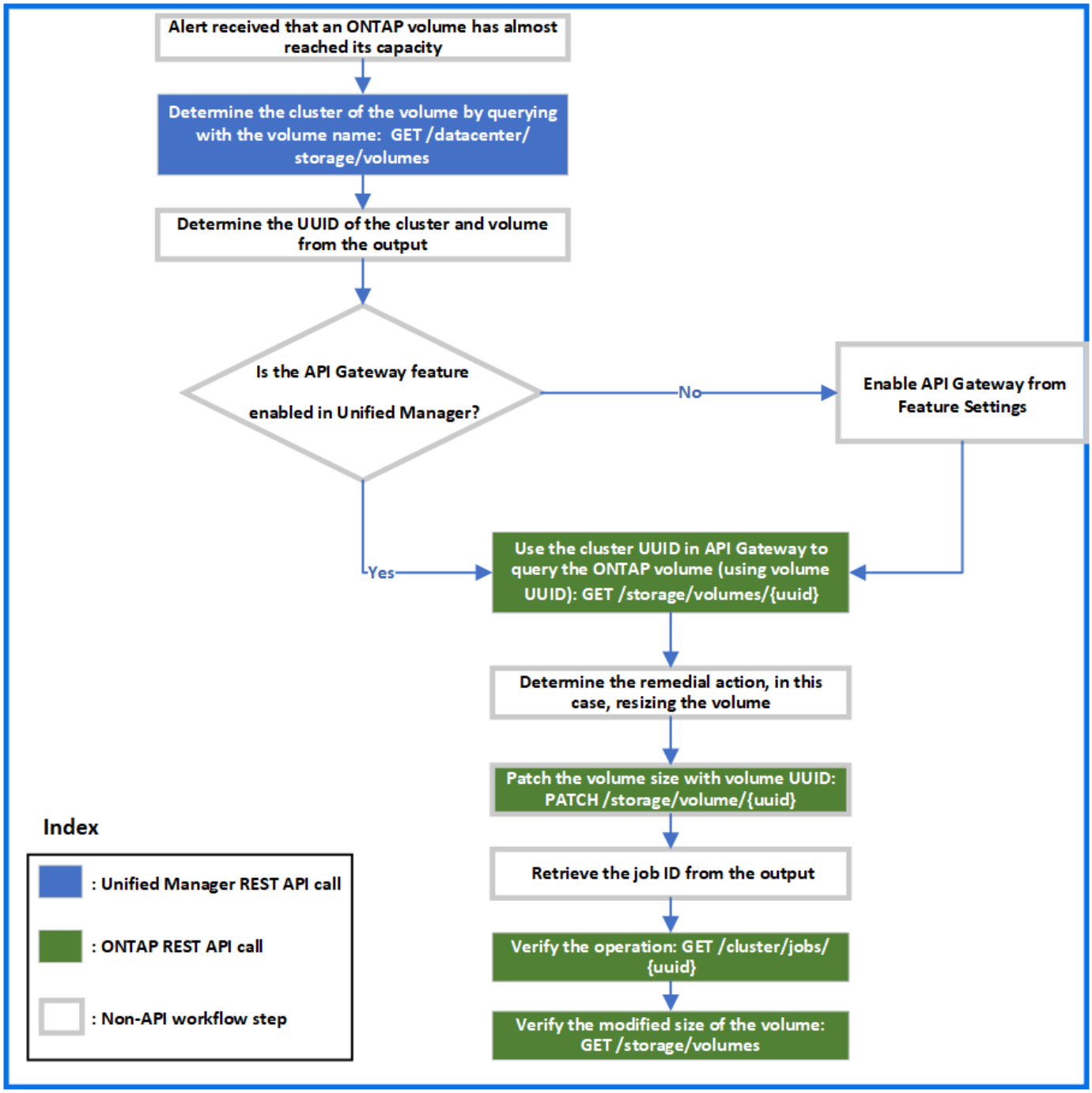
Las API de puerta de enlace actúan como puerta de enlace para invocar las API ONTAP para consultar información sobre los objetos de almacenamiento ONTAP y tomar medidas correctivas para abordar los problemas notificados.

Este flujo de trabajo requiere un caso de uso de muestra en el que se genera un evento cuando un volumen de ONTAP casi alcanza su capacidad. El flujo de trabajo también muestra cómo resolver este problema invocando una combinación de API REST de Active IQ Unified Manager y ONTAP.

Antes de ejecutar los pasos del flujo de trabajo, asegúrese de lo siguiente:

- Conoce las API de puerta de enlace y cómo se utilizan. Para obtener más información, consulte "Acceso a API de ONTAP a través de acceso de proxy".
- Conoce el uso de las API de REST de ONTAP. Para obtener información sobre el uso de las API de REST de ONTAP, consultehttps://docs.netapp.com/us-en/ontap-automation/index.html["Documentación de automatización de ONTAP"].
- Es administrador de aplicaciones.
- El clúster en el cual desea ejecutar las operaciones de API REST es compatible con ONTAP 9.5 o una versión posterior, y el clúster se añade a Unified Manager a HTTPS.

En el siguiente diagrama, se muestran cada paso del flujo de trabajo para solucionar el problema del uso de capacidad de volumen de ONTAP.



El flujo de trabajo abarca los puntos de invocación de las API DE REST de Unified Manager y ONTAP.

1. Observe el nombre del volumen desde el evento que notifica al uso de capacidad del volumen.
2. Con el nombre del volumen como valor del parámetro name, consulte el volumen ejecutando la siguiente API de Unified Manager.

Categoría	Verbo HTTP	Ruta
centro de datos	OBTENGA	`/datacenter/storage/volumes`

3. Recupere el UUID de clúster y el UUID de volumen de la salida.

4. En la interfaz de usuario web de Unified Manager, desplácese hasta **General** > **Configuración de funciones** > **puerta de enlace API** para verificar si la función API Gateway está activada. A menos que esté habilitado, las API de la categoría de puerta de enlace no estarán disponibles para que pueda invocar. Habilite la función si está deshabilitada.
5. Utilice el UUID de clúster para ejecutar la API ONTAP `/storage/volumes/{uuid}` A través de la pasarela API. La consulta devuelve los detalles del volumen cuando el UUID de volumen se pasa como el parámetro API.

   Para ejecutar las API de ONTAP mediante una puerta de enlace API, las credenciales de Unified Manager se pasan internamente para la autenticación; no es necesario ejecutar un paso de autenticación adicional para el acceso a cada clúster.

Categoría	Verbo HTTP	Ruta
Unified Manager: Puerta de enlace ONTAP: Almacenamiento	OBTENGA	API de puerta de enlace: `/gateways/{uuid}/{path}` API de ONTAP: `/storage/volumes/{uuid}`

   > En /gateways/{UUID}/{path}, el valor de {UUID} debe sustituirse por el UUID de clúster en el que se va a realizar la operación REST. {path} debe sustituirse por la URL DE REST de ONTAP /almacenamiento/volúmenes/{UUID}.

   La URL adjunta es: `/gateways/{cluster_uuid}/storage/volumes/{volume_uuid}`

   Al ejecutar la operación DE OBTENER, la URL generada es: `GEThttps://<hostname\>/api/gateways/<cluster_UUID\>/storage/volumes/{volume_uuid}`

   Comando de rizo de muestra

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-
9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7"
-H "accept: application/hal+json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

6. A partir de la salida, determine el tamaño, uso y medidas correctivas que se van a tomar. En este flujo de trabajo, la medida correctiva tomada es ajustar el tamaño del volumen.
7. Utilice el UUID de clúster y ejecute la siguiente API ONTAP a través de la puerta de enlace API para cambiar el tamaño del volumen. Para obtener información acerca de los parámetros de entrada de la puerta de enlace y las API ONTAP, consulte el paso 5.

Categoría	Verbo HTTP	Ruta
Unified Manager: Puerta de enlace ONTAP: Almacenamiento	PARCHE	API de puerta de enlace: `/gateways/{uuid}/{path}` API de ONTAP: `/storage/volumes/{uuid}`

Junto con el UUID de clúster y el UUID de volumen, debe introducir un valor para el parámetro size para el cambio de tamaño del volumen. Asegúrese de introducir el valor *in bytes*. Por ejemplo, si desea aumentar el tamaño de un volumen de 100 GB a 120 GB, introduzca el valor para el tamaño del parámetro al final de la consulta: `-d {\"size\": 128849018880}"`

Comando de rizo de muestra

```
curl -X PATCH "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-
9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7" -H
    "accept: application/hal+json" -H "Authorization: Basic
<Base64EncodedCredentials>" -d
    {\"size\": 128849018880}"
```

La salida JSON devuelve un UUID de trabajo.

8. Compruebe si el trabajo se ha ejecutado correctamente mediante el UUID de trabajo. Utilice el UUID de clúster y el UUID de trabajo para ejecutar la siguiente API ONTAP a través de la puerta de enlace API. Para obtener información acerca de los parámetros de entrada de la puerta de enlace y las API ONTAP, consulte el paso 5.

Categoría	Verbo HTTP	Ruta
Unified Manager: Puerta de enlace ONTAP: Cluster	OBTENGA	API de puerta de enlace: `/gateways/{uuid}/{path}` API de ONTAP: `/cluster/jobs/{uuid}`

Los códigos HTTP devueltos son los mismos que los códigos de estado HTTP de la API DE REST de ONTAP.

9. Ejecute la siguiente API de ONTAP para consultar los detalles del volumen cuyo tamaño ha cambiado. Para obtener información acerca de los parámetros de entrada de la puerta de enlace y las API ONTAP, consulte el paso 5.

Categoría	Verbo HTTP	Ruta
Unified Manager: Puerta de enlace ONTAP: Almacenamiento	OBTENGA	API de puerta de enlace: `/gateways/{uuid}/{path}` API de ONTAP: `/storage/volumes/{uuid}`

La salida muestra un mayor tamaño de volumen de 120 GB.

Flujos de trabajo API para la gestión de cargas de trabajo

Con Active IQ Unified Manager, puede aprovisionar y modificar cargas de trabajo de almacenamiento (LUN, recursos compartidos de archivos NFS y recursos compartidos CIFS). El aprovisionamiento consiste en varios pasos, desde la creación de la máquina virtual de almacenamiento (SVM) hasta la aplicación de políticas de nivel de servicio de rendimiento y eficiencia del almacenamiento en las cargas de trabajo de almacenamiento. La modificación de las cargas de trabajo consta de los pasos necesarios para modificar parámetros específicos y habilitar funciones adicionales en ellos.

Se describen los siguientes flujos de trabajo:

- Flujo de trabajo de aprovisionamiento de máquinas virtuales de almacenamiento (SVM) en Unified Manager.

  Este flujo de trabajo se debe realizar antes de aprovisionar las LUN o los recursos compartidos de archivos en Unified Manager.

- Aprovisionamiento de recursos compartidos de archivos.
- Aprovisionar las LUN.
- Modificar los LUN y los recursos compartidos de archivos (mediante el ejemplo de actualización del parámetro Performance Service Level para las cargas de trabajo de almacenamiento).
- Modificar un recurso compartido de archivos NFS para admitir el protocolo CIFS
- Modificar las cargas de trabajo para actualizar QoS a AQoS

Para cada flujo de trabajo de aprovisionamiento (LUN y recursos compartidos de archivos), asegúrese de haber completado el flujo de trabajo para verificar las SVM en los clústeres.

También debe leer las recomendaciones y las limitaciones antes de utilizar cada API en los flujos de trabajo. Los detalles pertinentes de las API están disponibles en sus secciones individuales enumeradas en los conceptos y referencias relacionados.

Verificación de las SVM en clústeres mediante API

Antes de aprovisionar recursos compartidos de archivos o LUN, debe comprobar si los clústeres tienen máquinas virtuales de almacenamiento (SVM) creadas en ellos.

En el flujo de trabajo se supone que los clústeres de ONTAP se añadieron a Unified Manager y se ha obtenido la clave de clúster. Los clústeres deben tener las licencias necesarias para aprovisionar LUN y recursos compartidos de archivos en ellos.

1. Comprobar si el clúster tiene una SVM creada.

Categoría	Verbo HTTP	Ruta
centro de datos	OBTENGA	`/datacenter/svm/svms` `/datacenter/svm/svms/{key}`

Muestra de rizo

```
curl -X GET "https://<hostname>/api/datacenter/svm/svms" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. Si no devuelve la clave SVM, cree la SVM. Para crear las SVM, debe contar con la clave de clúster en la que aprovisiona la SVM. También debe especificar el nombre de la SVM. Siga estos pasos.

Categoría	Verbo HTTP	Ruta
centro de datos	OBTENGA	`/datacenter/cluster/clusters` `/datacenter/cluster/clusters/{key}`

Obtenga la clave de clúster.

Muestra de rizo

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

3. En el resultado, obtenga la clave de clúster y después utilícela como entrada para crear la SVM.

Al crear la SVM, asegúrese de que sea compatible con todos los protocolos necesarios para aprovisionar las LUN y recursos compartidos de archivos en ellas, por ejemplo, CIFS, NFS, FCP, E iSCSI. Es posible que se produzca un error en los flujos de trabajo de aprovisionamiento si la SVM no admite los servicios necesarios. Es recomendable que los servicios para los respectivos tipos de cargas de trabajo estén habilitados en la SVM.

Categoría	Verbo HTTP	Ruta
centro de datos	PUBLICAR	`/datacenter/svm/svms`

Muestra de rizo

Introduzca los detalles del objeto de SVM como parámetros de entrada.

```
curl -X POST "https://<hostname>/api/datacenter/svm/svms" -H "accept:
application/json" -H "Content-Type: application/json" -H "Authorization:
Basic <Base64EncodedCredentials>" "{ \"aggregates\": [ { \"_links\": {},
\"key\": \"1cd8a442-86d1,type=objecttype,uuid=1cd8a442-86d1-11e0-ae1c-
9876567890123\",
\"name\": \"cluster2\", \"uuid\": \"02c9e252-41be-11e9-81d5-
00a0986138f7\" } ],
\"cifs\": { \"ad_domain\": { \"fqdn\": \"string\", \"password\":
\"string\",
\"user\": \"string\" }, \"enabled\": true, \"name\": \"CIFS1\" },
\"cluster\": { \"key\": \"1cd8a442-86d1-11e0-ae1c-
123478563412,type=object type,uuid=1cd8a442-86d1-11e0-ae1c-
9876567890123\" },
\"dns\": { \"domains\": [ \"example.com\", \"example2.example3.com\" ],
\"servers\": [ \"10.224.65.20\", \"2001:db08:a0b:12f0::1\" ] },
\"fcp\": { \"enabled\": true }, \"ip_interface\": [ { \"enabled\": true,
\"ip\": { \"address\": \"10.10.10.7\", \"netmask\": \"24\" },
\"location\": { \"home_node\": { \"name\": \"node1\" } }, \"name\":
\"dataLif1\" } ], \"ipspace\": { \"name\": \"exchange\" },
\"iscsi\": { \"enabled\": true }, \"language\": \"c.utf_8\",
\"ldap\": { \"ad_domain\": \"string\", \"base_dn\": \"string\",
\"bind_dn\": \"string\", \"enabled\": true, \"servers\": [ \"string\" ]
},
\"name\": \"svm1\", \"nfs\": { \"enabled\": true },
\"nis\": { \"domain\": \"string\", \"enabled\": true,
\"servers\": [ \"string\" ] }, \"nvme\": { \"enabled\": true },
\"routes\": [ { \"destination\": { \"address\": \"10.10.10.7\",
\"netmask\": \"24\" }, \"gateway\": \"string\" } ],
\"snapshot_policy\": { \"name\": \"default\" },
\"state\": \"running\", \"subtype\": \"default\"}"
```

El resultado de JSON muestra una clave de objeto de Job que puede utilizar para verificar la SVM que ha creado.

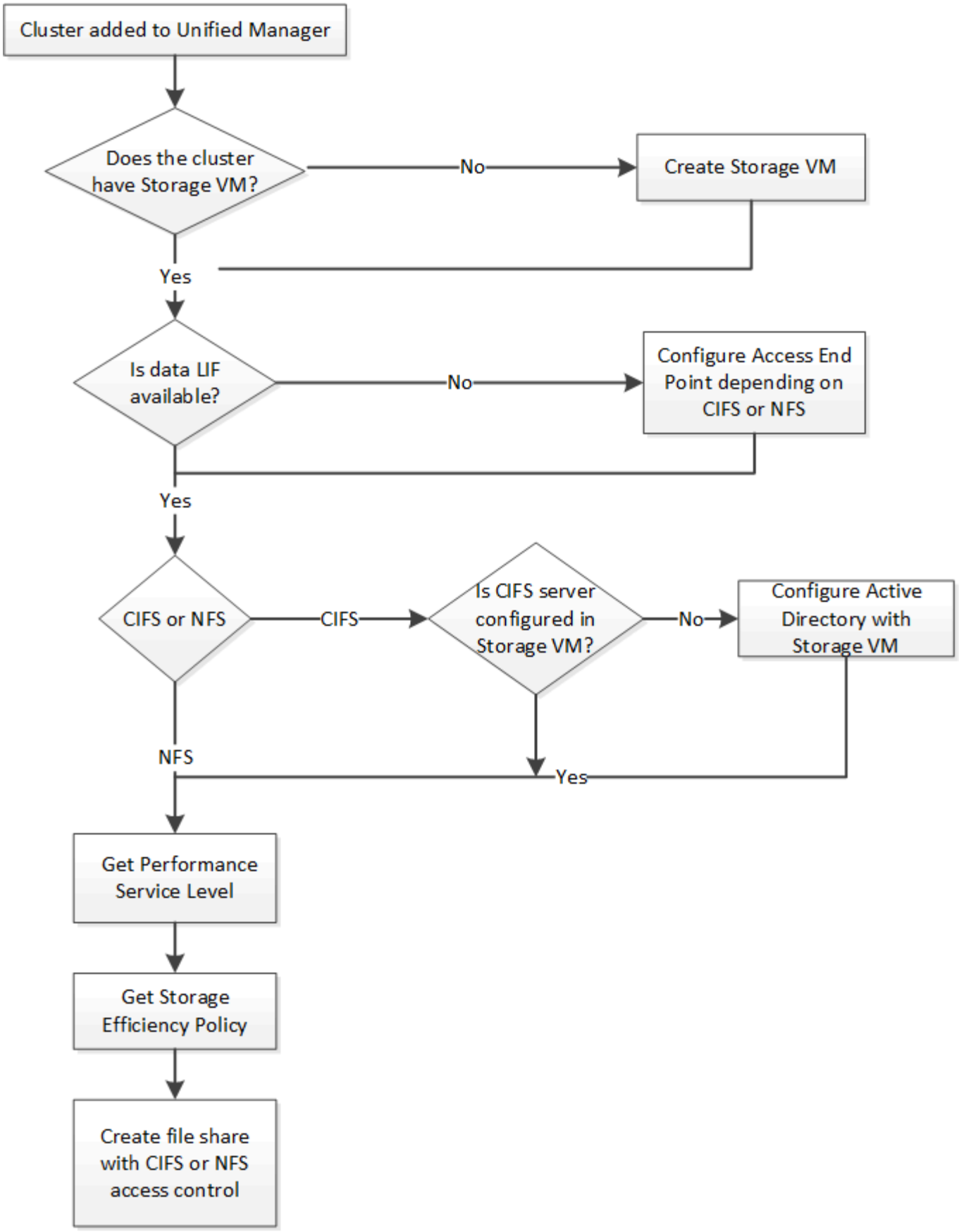
4. Compruebe la creación de la SVM mediante la clave de objeto de trabajo a consultar. Si la SVM se crea correctamente, se devuelve la clave SVM en la respuesta.

Categoría	Verbo HTTP	Ruta
servidor de gestión	OBTENGA	`/management-server/jobs/{key}`

Aprovisionamiento de recursos compartidos de archivos CIFS y NFS mediante API

Puede aprovisionar recursos compartidos de CIFS y recursos compartidos de archivos NFS en las máquinas virtuales de almacenamiento (SVM) mediante las API de aprovisionamiento proporcionadas como parte de Active IQ Unified Manager. Este flujo de trabajo de aprovisionamiento detalla los pasos para recuperar las claves de las SVM, los niveles de servicio de rendimiento y las políticas de eficiencia del almacenamiento antes de crear los recursos compartidos de archivos.

En el siguiente diagrama se ilustra cada paso de un flujo de trabajo de aprovisionamiento de recursos compartidos de archivos. Incluye aprovisionamiento de recursos compartidos CIFS y recursos compartidos de archivos NFS.


Cluster added to Unified Manager
Does the cluster have Storage VM?
No
Create Storage VM
Yes
Is data LIF available?
No
Configure Access End Point depending on CIFS or NFS
Yes
CIFS or NFS
CIFS
Is CIFS server configured in Storage VM?
No
Configure Active Directory with Storage VM
NFS
Yes
Get Performance Service Level
Get Storage Efficiency Policy
Create file share with CIFS or NFS access control

Asegúrese de lo siguiente:

- Los clústeres de ONTAP se añadieron a Unified Manager y se obtuvo la clave de clúster.
- Se han creado las instancias de SVM en los clústeres.
- Las SVM admiten servicios CIFS y NFS. El aprovisionamiento de recursos compartidos de archivos puede fallar si las SVM no admiten los servicios necesarios.
- El puerto FCP está en línea para el aprovisionamiento de puertos.

1. Determine si los LIF de datos o extremos de acceso están disponibles en la SVM en la que desea crear el recurso compartido de CIFS. Obtenga la lista de extremos de acceso disponibles en la SVM:

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	OBTENGA	`/storage-provider/access-endpoints` `/storage-provider/access-endpoints/{key}`

Muestra de rizo

```
curl -X GET "https://<hostname>/api/storage-provider/access-endpoints?resource.key=7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. Si su extremo de acceso está disponible en la lista, obtenga la clave de extremo de acceso; de lo contrario, cree el extremo de acceso.

Asegúrese de crear extremos de acceso que tengan habilitado el protocolo CIFS en ellos. El aprovisionamiento de recursos compartidos de CIFS produce un error a menos que se haya creado un extremo de acceso con el protocolo CIFS habilitado en él.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PUBLICAR	`/storage-provider/access-endpoints`

Muestra de rizo

Debe introducir los detalles del extremo de acceso que desea crear, como parámetros de entrada.

```
curl -X POST "https://<hostname>/api/storage-provider/access-endpoints"
-H "accept: application/json" -H "Content-Type: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>"
{ \"data_protocols\": \"nfs\",
\"fileshare\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=volume,uuid=f3063d27-2c71-44e5-9a69-a3927c19c8fc\" },
\"gateway\": \"10.132.72.12\",
\"ip\": { \"address\": \"10.162.83.26\",
\"ha_address\": \"10.142.83.26\",
\"netmask\": \"255.255.0.0\" },
\"lun\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=lun,uuid=d208cc7d-80a3-4755-93d4-5db2c38f55a6\" },
\"mtu\": 15000, \"name\": \"aep1\",
\"svm\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a178d39e12:type=vserver,uuid=1d1c3198-fc57-11e8-99ca-00a098d38e12\" },
\"vlan\": 10}"
```

El resultado de JSON muestra una clave de objeto de trabajo que se puede utilizar para verificar el extremo de acceso que se ha creado.

3. Compruebe el extremo de acceso:

Categoría	Verbo HTTP	Ruta
servidor de gestión	OBTENGA	`/management-server/jobs/{key}`

4. Determine si tiene que crear un recurso compartido CIFS o un recurso compartido de archivos NFS. Para crear recursos compartidos de CIFS, siga estos pasos:

   a. Determinar si el servidor CIFS está configurado en la SVM, que es determinar si se ha creado una asignación de Active Directory en la SVM.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	OBTENGA	`/storage-provider/active-directories-mappings`

   b. Si se crea la asignación de Active Directory, tome la clave de nuevo y cree el mapa de Active Directory en la SVM.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PUBLICAR	`/storage-provider/active-directories-mappings`

Muestra de rizo

Debe introducir los detalles para crear la asignación de Active Directory como parámetros de entrada.

```
curl -X POST "https://<hostname>/api/storage-provider/active-
directories-mappings" -H "accept: application/json" -H "Content-Type:
application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
{ \"_links\": {},
\"dns\": \"10.000.000.000\",
\"domain\": \"example.com\",
\"password\": \"string\",
\"svm\": { \"key\": \"9f4ddea-e395-11e9-b660-
005056a71be9:type=vserver,uuid=191a554a-f0ce-11e9-b660-005056a71be9\" },
\"username\": \"string\"}"
```

+
Se trata de una llamada síncrona y puede comprobar la creación de la asignación de Active Directory en la salida. En caso de error, se muestra el mensaje de error para que pueda solucionar y volver a ejecutar la solicitud.

5. Obtenga la clave de SVM de la SVM en la que desea crear el recurso compartido de CIFS o el recurso compartido de archivos NFS, como se describe en el tema de flujo de trabajo *verificando SVM en clústeres*.
6. Obtenga la clave para el nivel de servicio de rendimiento ejecutando la siguiente API y recuperando la clave de la respuesta.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	OBTENGA	`/storage-provider/performance-service-levels`

Para recuperar los detalles de los niveles de servicio de rendimiento definidos por el sistema, configure el `system_defined` introduzca el parámetro a. `true`. En el resultado, obtenga la clave del nivel de servicio de rendimiento que desea aplicar en el recurso compartido de archivos.

7. Opcionalmente, obtenga la clave de la Política de eficiencia del almacenamiento de la Política de eficiencia del almacenamiento que desea aplicar en el recurso compartido de archivos ejecutando la siguiente API y recuperando la clave de la respuesta.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	OBTENGA	`/storage-provider/storage-efficiency-policies`

8. Cree el recurso compartido de archivos. Puede crear un recurso compartido de archivos compatible tanto

con CIFS como NFS especificando la lista de control de acceso y la política de exportación. En los siguientes subpasos, se proporciona información si desea crear un recurso compartido de archivos para admitir solo uno de los protocolos en el volumen. También puede actualizar un recurso compartido de archivos NFS para incluir la lista de control de acceso después de crear el recurso compartido NFS. Para obtener información, consulte el tema *Modificar cargas de trabajo de almacenamiento*.

a. Para crear solo un recurso compartido de CIFS, recopile la información acerca de la lista de control de acceso (ACL). Para crear el recurso compartido CIFS, proporcione valores válidos para los siguientes parámetros de entrada. Para cada grupo de usuarios que asigne, se crea una ACL cuando se aprovisiona un recurso compartido de CIFS/SMB. En función de los valores introducidos para la asignación de ACL y Active Directory, el control de acceso y la asignación se determinan para el recurso compartido CIFS cuando se crea.

   Un comando curl con valores de ejemplo

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    },
```

b. Para crear únicamente un recurso compartido de archivos NFS, recopile la información acerca de la política de exportación. Para crear el recurso compartido de archivos NFS, proporcione valores válidos para los siguientes parámetros de entrada. La política de exportación, en función de sus valores, se asocia al recurso compartido de archivos NFS cuando se crea.

   Al aprovisionar el recurso compartido de NFS, puede crear una política de exportación proporcionando todos los valores necesarios o proporcionar la clave de la política de exportación y reutilizar una política de exportación existente. Si desea reutilizar una política de exportación para la máquina virtual de almacenamiento, deberá añadir la clave de política de exportación. A menos que conozca la clave, puede recuperar la clave de política de exportación mediante la `/datacenter/protocols/nfs/export-policies` API. Para crear una nueva política, debe introducir las reglas tal y como se muestran en la siguiente muestra. Para las reglas introducidas, la API intenta buscar una política de exportación existente conciliando el host, la máquina virtual de almacenamiento y las reglas. Si existe una política de exportación existente, se utiliza. De lo contrario, se creará una nueva política de exportación.

   Un comando curl con valores de ejemplo

```
"export_policy": {
      "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
      "name_tag": "ExportPolicyNameTag",
      "rules": [
        {
          "clients": [
            {
              "match": "0.0.0.0/0"
            }
```

Después de configurar la lista de control de acceso y la política de exportación, proporcione los valores válidos para los parámetros de entrada obligatorios para los recursos compartidos de archivos CIFS y NFS:

Política de eficiencia de almacenamiento es un parámetro opcional para crear recursos compartidos de archivos.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PUBLICAR	`/storage-provider/file-shares`

El resultado JSON muestra una clave de objeto Job que puede utilizar para verificar el recurso compartido de archivos que ha creado. . Verifique la creación del recurso compartido de archivos mediante la clave de objeto Job devuelta al consultar el trabajo:

Categoría	Verbo HTTP	Ruta
servidor de gestión	OBTENGA	`/management-server/jobs/{key}`

Al final de la respuesta, verá la clave del recurso compartido de archivos creado.

```
    ],
    "job_results": [
        {
            "name": "fileshareKey",
            "value": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6"
        }
    ],
    "_links": {
        "self": {
            "href": "/api/management-server/jobs/06a6148bf9e862df:-
2611856e:16e8d47e722:-7f87"
        }
    }
}
```

1. Compruebe la creación del recurso compartido de archivos ejecutando la siguiente API con la clave devuelta:

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	OBTENGA	`/storage-provider/file-shares/{key}`

Ejemplo de salida JSON

Puede ver que el método POST de `/storage-provider/file-shares` Invoca internamente todas las API necesarias para cada una de las funciones y crea el objeto. Por ejemplo, invoca el `/storage-provider/performance-service-levels/` API para asignar el nivel de servicio de rendimiento en el recurso compartido de archivos.

```
{
    "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6",
    "name": "FileShare_377",
    "cluster": {
        "uuid": "7d5a59b3-953a-11e8-8857-00a098dcc959",
        "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-00a098dcc959",
        "name": "AFFA300-206-68-70-72-74",
        "_links": {
            "self": {
                "href": "/api/datacenter/cluster/clusters/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-
00a098dcc959"
            }
```

```
        }
    },
    "svm": {
        "uuid": "b106d7b1-51e9-11e9-8857-00a098dcc959",
        "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-00a098dcc959",
        "name": "RRT_ritu_vs1",
        "_links": {
            "self": {
                "href": "/api/datacenter/svm/svms/7d5a59b3-953a-11e8-
8857-00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-
00a098dcc959"
            }
        }
    },
    "assigned_performance_service_level": {
        "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
        "name": "Value",
        "peak_iops": 75,
        "expected_iops": 75,
        "_links": {
            "self": {
                "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
            }
        }
    },
    "recommended_performance_service_level": {
        "key": null,
        "name": "Idle",
        "peak_iops": null,
        "expected_iops": null,
        "_links": {}
    },
    "space": {
        "size": 104857600
    },
    "assigned_storage_efficiency_policy": {
        "key": null,
        "name": "Unassigned",
        "_links": {}
    },
    "access_control": {
        "acl": [
            {
                "user_or_group": "everyone",
```

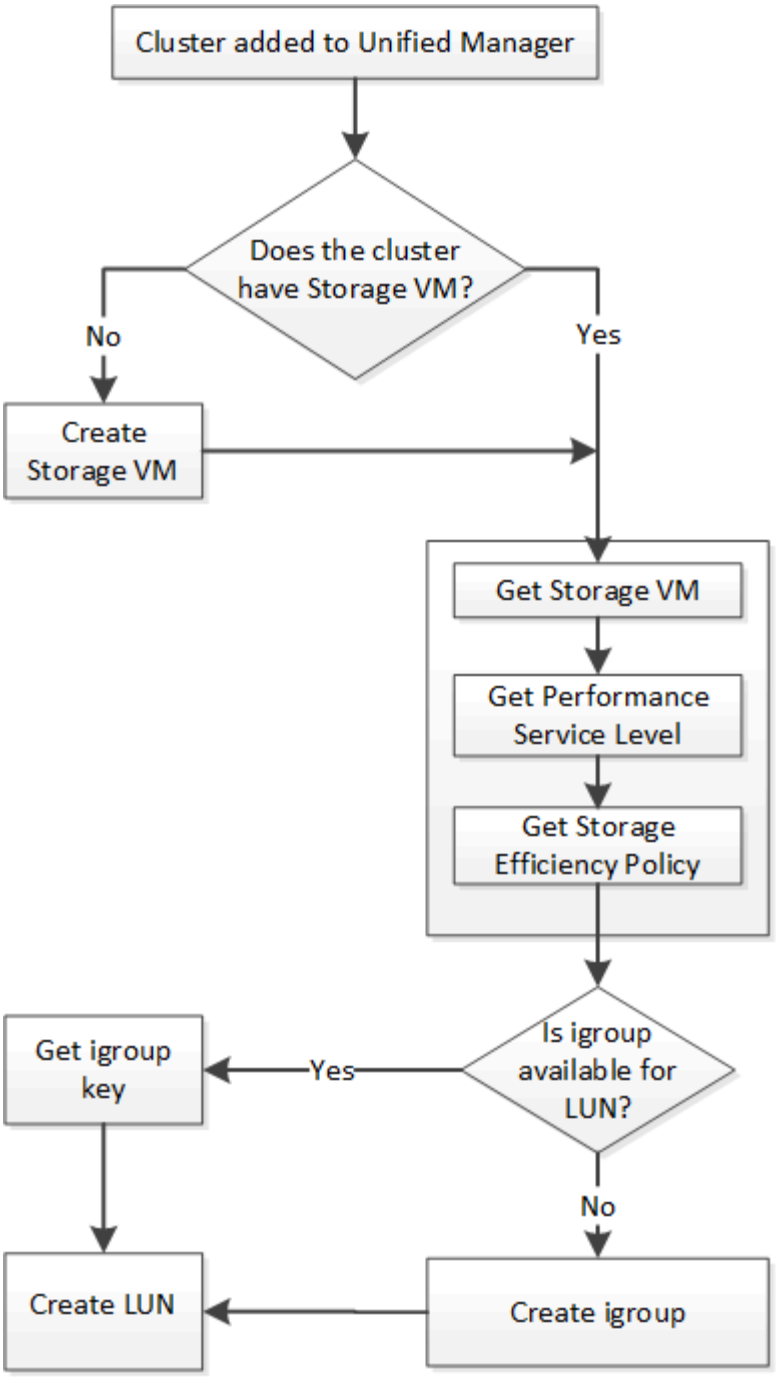
```
                "permission": "read"
            }
        ],
        "export_policy": {
            "id": 1460288880641,
            "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
            "name": "default",
            "rules": [
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
                    "index": 1,
                    "protocols": [
                        "nfs3",
                        "nfs4"
                    ],
                    "ro_rule": [
                        "sys"
                    ],
                    "rw_rule": [
                        "sys"
                    ],
                    "superuser": [
                        "none"
                    ]
                },
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
                    "index": 2,
                    "protocols": [
                        "cifs"
                    ],
                    "ro_rule": [
                        "ntlm"
                    ],
                    "rw_rule": [
```

```
                        "ntlm"
                    ],
                    "superuser": [
                        "none"
                    ]
                }
            ],
            "_links": {
                "self": {
                    "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
                }
            }
        }
    },
    "_links": {
        "self": {
            "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
        }
    }
}
```


Aprovisionamiento de LUN mediante API

Puede aprovisionar LUN en las máquinas virtuales de almacenamiento (SVM) mediante las API de aprovisionamiento que se proporcionan como parte de Active IQ Unified Manager. Este flujo de trabajo de aprovisionamiento detalla los pasos para recuperar las claves de las SVM, los niveles de servicio de rendimiento y las políticas de eficiencia del almacenamiento antes de crear la LUN.

En el siguiente diagrama se muestran los pasos del flujo de trabajo de aprovisionamiento de las LUN.



En este flujo de trabajo se supone que los clústeres de ONTAP se han añadido a Unified Manager y se ha obtenido la clave de clúster. En el flujo de trabajo también se supone que las SVM ya se han creado en los clústeres.

1. Obtenga la clave de SVM de la SVM en la que desea crear la LUN, como se describe en el tema *verificando SVM en clústeres* de flujo de trabajo.
2. Obtenga la clave para el nivel de servicio de rendimiento ejecutando la siguiente API y recuperando la clave de la respuesta.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	OBTENGA	`/storage-provider/performance-service-levels`

Para recuperar los detalles de los niveles de servicio de rendimiento definidos por el sistema, configure el `system_defined` introduzca el parámetro a. `true`. En la salida, obtenga la clave del nivel de servicio de rendimiento que desea aplicar en la LUN.

3. Opcionalmente, obtenga la clave de la Política de eficiencia del almacenamiento de la Política de eficiencia del almacenamiento que desea aplicar en la LUN ejecutando la siguiente API y recuperando la clave de la respuesta.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	OBTENGA	`/storage-provider/storage-efficiency-policies`

4. Determinar si se han creado los iGroups (iGroups) para otorgar acceso al destino de LUN que desea crear.

Categoría	Verbo HTTP	Ruta
centro de datos	OBTENGA	`/datacenter/protocols/san/igroups` `/datacenter/protocols/san/igroups/{key}`

Debe introducir el valor del parámetro para indicar la SVM para la que el igroup tiene acceso autorizado. Además, si desea consultar un igroup determinado, introduzca el nombre del igroup (clave) como parámetro de entrada.

5. En el resultado, si puede encontrar el igroup al que desea otorgar acceso, obtenga la clave. De lo contrario, cree el igroup.

Categoría	Verbo HTTP	Ruta
centro de datos	PUBLICAR	`/datacenter/protocols/san/igroups`

Debe introducir los detalles del igroup que desea crear como parámetros de entrada. Se trata de una llamada síncrona y puede comprobar la creación del igroup en el resultado. En caso de error, se muestra un mensaje para que solucione y vuelva a ejecutar la API.

6. Cree la LUN.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PUBLICAR	`/storage-provider/luns`

Para crear la LUN, asegúrese de haber añadido los valores recuperados como parámetros de entrada obligatorios.

Política de eficiencia de almacenamiento es un parámetro opcional para crear LUN.

Muestra de rizo

Debe introducir todos los detalles de la LUN que desea crear, como parámetros de entrada.

El resultado de JSON muestra una clave de objeto de Job que puede utilizar para verificar la LUN que ha creado.

7. Compruebe la creación de la LUN mediante la clave de objeto Job devuelta consultando el trabajo:

Categoría	Verbo HTTP	Ruta
servidor de gestión	OBTENGA	`/management-server/jobs/{key}`

Al final de la respuesta, ve la clave de la LUN creada.

8. Compruebe la creación de la LUN. Para ello, ejecute la siguiente API con la clave devuelta:

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	OBTENGA	`/storage-provider/luns/{key}`

Ejemplo de salida JSON

Puede ver que el método POST de `/storage-provider/luns` Invoca internamente todas las API necesarias para cada una de las funciones y crea el objeto. Por ejemplo, invoca el `/storage-provider/performance-service-levels/` API para asignar el nivel de servicio de rendimiento en la LUN.

== pasos de solución de problemas para el error en la creación o asignación de LUN

Al completar este flujo de trabajo, es posible que observe un error durante el proceso de creación de la LUN. Incluso si la LUN se crea correctamente, la asignación de LUN con el igroup puede generar un error debido a la falta de disponibilidad de un LIF DE SAN o un extremo de acceso en el nodo en el que crea la LUN. En caso de un fallo, puede ver el siguiente mensaje:

```
The nodes <node_name> and <partner_node_name> have no LIFs configured with
the iSCSI or FCP protocol for Vserver <server_name>. Use the access-
endpoints API to create a LIF for the LUN.
```

Siga estos pasos de solución de problemas para solucionar este error.

1. Cree un extremo de acceso compatible con el protocolo ISCSI/FCP en la SVM donde haya intentado crear la LUN.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PUBLICAR	`/storage-provider/access-endpoints`

Muestra de rizo

Debe introducir los detalles del extremo de acceso que desea crear, como parámetros de entrada.

> Asegúrese de que en el parámetro de entrada haya agregado la dirección para indicar el nodo de inicio de la LUN y la dirección ha_address para indicar el nodo asociado del nodo raíz. Cuando se ejecuta esta operación, se crean extremos de acceso tanto en el nodo de inicio como en el nodo del partner.

2. Consulte el trabajo con la clave de objeto Job que se devuelve en la salida JSON para verificar que se ha ejecutado correctamente para añadir los extremos de acceso en la SVM y que los servicios iSCSI/FCP se han habilitado en la SVM.

Categoría	Verbo HTTP	Ruta
servidor de gestión	OBTENGA	`/management-server/jobs/{key}`

Ejemplo de salida JSON

Al final del resultado, puede ver la clave de los extremos de acceso creados. En la siguiente salida, el valor "name": "AccessEndpointKey" indica el extremo de acceso creado en el nodo de inicio de la LUN, para el cual la clave es 9c964258-14ef-11ea-95e2-00a098e32c28. El valor "name": "AccessEndpointHAKey" indica el punto final de acceso creado en el nodo asociado del nodo principal, para el cual la clave es 9d347006-14ef-11ea-8760-00a098e3215f.

3. Modifique la LUN para actualizar el mapa de igroup. Para obtener más información acerca de la modificación del flujo de trabajo, consulte «Modificar las cargas de trabajo de almacenamiento».

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PARCHE	`/storage-provider/lun/{key}`

En la entrada, especifique la clave del igroup con la que desea actualizar el mapa de LUN, junto con la

clave LUN.

Muestra de rizo

El resultado JSON muestra una clave de objeto de trabajo que puede utilizar para verificar si la asignación se ha realizado correctamente.

4. Compruebe el mapa de LUN consultando la clave LUN.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	OBTENGA	`/storage-provider/luns/{key}`

Ejemplo de salida JSON

En el resultado se puede ver que la LUN se ha asignado correctamente con el igroup (clave d19ec2fa-fec7-11e8-b23d-00a098e32c28) con el que se aprovisionó inicialmente.

Modificación de las cargas de trabajo de almacenamiento mediante API

La modificación de las cargas de trabajo de almacenamiento consiste en actualizar las LUN o recursos compartidos de archivos con los parámetros que faltan o cambiar los parámetros existentes.

Este flujo de trabajo toma el ejemplo de actualización de niveles de servicio de rendimiento para LUN y recursos compartidos de archivos.

El flujo de trabajo supone que el LUN o el recurso compartido de archivos se han aprovisionado con niveles de servicio de rendimiento.

Modificación de los recursos compartidos de archivos

Al modificar un recurso compartido de archivos, puede actualizar los siguientes parámetros:

- Capacidad o tamaño.
- Configuración en línea o sin conexión.
- Política de eficiencia de almacenamiento.
- Nivel de servicio de rendimiento.
- Ajustes de la lista de control de acceso (ACL).
- Configuración de la directiva de exportación. También puede eliminar los parámetros de política de exportación y revertir las reglas de política de exportación predeterminadas (vacías) en el recurso compartido de archivos.

Durante una sola ejecución de API, solo puede actualizar un parámetro.

Este procedimiento describe cómo agregar un nivel de servicio de rendimiento a un recurso compartido de archivos. Puede utilizar el mismo procedimiento para actualizar cualquier otra propiedad de recurso compartido de archivos.

1. Obtenga la clave del recurso compartido de CIFS o del recurso compartido de archivos NFS del que desea actualizar. Esta API consulta todos los recursos compartidos de archivos en su centro de datos. Omita este paso si ya conoce la clave para compartir archivos.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	OBTENGA	`/storage-provider/file-shares`

2. Para ver los detalles del recurso compartido de archivos, ejecute la siguiente API con la clave de recurso compartido de archivos obtenida.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	OBTENGA	`/storage-provider/file-shares/{key}`

Vea los detalles del recurso compartido de archivos en el resultado.

```
"assigned_performance_service_level": {
        "key": null,
        "name": "Unassigned",
        "peak_iops": null,
        "expected_iops": null,
        "_links": {}
      },
```

3. Obtenga la clave del nivel de servicio de rendimiento que desea asignar en este recurso compartido de archivos. Actualmente no hay ninguna directiva asignada.

Categoría	Verbo HTTP	Ruta
Niveles de servicio de rendimiento	OBTENGA	`/storage-provider/performance-service-levels`

Para recuperar los detalles de los niveles de servicio de rendimiento definidos por el sistema, configure el `system_defined` introduzca el parámetro a. `true`. En el resultado, obtenga la clave del nivel de servicio de rendimiento que desea aplicar al recurso compartido de archivos.

4. Aplique el nivel de servicio de rendimiento en el recurso compartido de archivos.

Categoría	Verbo HTTP	Ruta
Proveedor de almacenamiento de NetApp	PARCHE	`/storage-provider/file-shares/{key}`

En la entrada, debe especificar solo el parámetro que desea actualizar, junto con la clave de recurso compartido de archivos. En este caso, es la clave del nivel de servicio de rendimiento.

Muestra de rizo

```
curl -X POST "https://<hostname>/api/storage-provider/file-shares"`-H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>" -d
"{
\"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-
fa163e82bbf2\" },
}"
```

El resultado de JSON muestra un objeto de trabajo que se puede usar para verificar que los extremos de acceso de los nodos raíz y asociados se hayan creado correctamente.

5. Compruebe si el nivel de servicio de rendimiento se ha agregado al recurso compartido de archivos utilizando la clave de objeto Job que se muestra en la salida.

Categoría	Verbo HTTP	Ruta
Servidor de gestión	OBTENGA	`/management-server/jobs/{key}`

Si consulta por el ID del objeto Job, verá si el recurso compartido de archivos se actualiza correctamente. En caso de que se produzca un error, solucione un error y vuelva a ejecutar la API. Una vez creada correctamente, consulte el recurso compartido de archivos para ver el objeto modificado:

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	OBTENGA	`/storage-provider/file-shares/{key}`

Vea los detalles del recurso compartido de archivos en el resultado.

```
"assigned_performance_service_level": {
        "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
        "name": "Value",
        "peak_iops": 75,
        "expected_iops": 75,
        "_links": {
            "self": {
                "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
            }
        }
```

Actualizando las LUN

Al actualizar una LUN, puede modificar los siguientes parámetros:

- Capacidad o tamaño
- Configuración en línea o sin conexión
- Política de eficiencia de almacenamiento
- Nivel de servicio de rendimiento
- Mapa de LUN

Durante una sola ejecución de API, solo puede actualizar un parámetro.

En este procedimiento, se describe cómo añadir un nivel de servicio de rendimiento a una LUN. Puede utilizar el mismo procedimiento para actualizar cualquier otra propiedad de LUN.

1. Obtenga la clave LUN de la LUN que desea actualizar. Esta API muestra detalles de todas las LUN del centro de datos. Evite este paso si ya conoce la clave LUN.

Categoría	Verbo HTTP	Ruta
Proveedor de almacenamiento de NetApp	OBTENGA	`/storage-provider/luns`

2. Vea los detalles de la LUN. Para ello, ejecute la siguiente API con la clave LUN que obtuvo.

Categoría	Verbo HTTP	Ruta
Proveedor de almacenamiento de NetApp	OBTENGA	`/storage-provider/luns/{key}`

   Vea los detalles de la LUN en el resultado. Puede ver que no hay ningún nivel de servicio de rendimiento asignado a esta LUN.

   Ejemplo de salida JSON

```
"assigned_performance_service_level": {
      "key": null,
      "name": "Unassigned",
      "peak_iops": null,
      "expected_iops": null,
      "_links": {}
    },
```

3. Obtenga la clave del nivel de servicio de rendimiento que desea asignar a la LUN.

Categoría	Verbo HTTP	Ruta
Niveles de servicio de rendimiento	OBTENGA	`/storage-provider/performance-service-levels`

Para recuperar los detalles de los niveles de servicio de rendimiento definidos por el sistema, configure el `system_defined` introduzca el parámetro a. `true`. En la salida, obtenga la clave del nivel de servicio de rendimiento que desea aplicar en la LUN.

4. Aplique el nivel de servicio de rendimiento en la LUN.

Categoría	Verbo HTTP	Ruta
Proveedor de almacenamiento de NetApp	PARCHE	`/storage-provider/lun/{key}`

En la entrada, debe especificar solo el parámetro que desea actualizar, junto con la clave LUN. En este caso, es la clave del nivel de servicio rendimiento.

Muestra de rizo

```
curl -X PATCH "https://<hostname>/api/storage-provider/luns/7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Content-Type: application/json" H "Authorization: Basic <Base64EncodedCredentials>" -d "{ \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-fa163e82bbf2\" }"
```

El resultado de JSON muestra una clave de objeto de trabajo que puede utilizar para verificar la LUN que ha actualizado.

5. Vea los detalles de la LUN. Para ello, ejecute la siguiente API con la clave LUN que obtuvo.

Categoría	Verbo HTTP	Ruta
Proveedor de almacenamiento de NetApp	OBTENGA	`/storage-provider/luns/{key}`

Vea los detalles de la LUN en el resultado. Puede ver que el nivel de servicio de rendimiento está asignado a esta LUN.

Ejemplo de salida JSON

```
     "assigned_performance_service_level": {
        "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
        "name": "Value",
        "peak_iops": 75,
        "expected_iops": 75,
        "_links": {
            "self": {
                "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
            }
```

Modificar un recurso compartido de archivos NFS mediante API para admitir CIFS

Es posible modificar un recurso compartido de archivos NFS para admitir el protocolo CIFS. Durante la creación de archivos compartidos, es posible especificar tanto los parámetros de la lista de control de acceso (ACL) como las reglas de política de exportación para el mismo recurso compartido de archivos. No obstante, si desea habilitar CIFS en el mismo volumen en el que se creó un recurso compartido de archivos NFS, es posible actualizar los parámetros de ACL en ese recurso compartido de archivos para admitir CIFS.

Lo que necesitará

1. Se debe haber creado un recurso compartido de archivos NFS con únicamente los detalles de la política de exportación. Para obtener información, consulte *Administrar recursos compartidos de archivos* y *Modificar las cargas de trabajo de almacenamiento*.
2. Debe tener la clave para compartir archivos para ejecutar esta operación. Para obtener información acerca de cómo ver los detalles de los recursos compartidos de archivos y recuperar la clave de uso compartido de archivos mediante el identificador de trabajo, consulte *Provisioning CIFS and NFS file shares*.

Esto se aplica a un recurso compartido de archivos NFS creado añadiendo solo reglas de política de exportación y no parámetros ACL. El recurso compartido de archivos NFS se modifica para incluir los parámetros ACL.

Pasos

1. En el recurso compartido de archivos NFS, realice un `PATCH` Operación con los detalles de ACL para permitir el acceso CIFS.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	PARCHE	`/storage-provider/file-shares`

Muestra de rizo

Según los privilegios de acceso que asigne al grupo de usuarios, como se muestra en el siguiente ejemplo, se crea una ACL y se asigna al recurso compartido de archivos.

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
```

Ejemplo de salida JSON

La operación devuelve el identificador de trabajo del trabajo que ejecuta la actualización.

2. Compruebe si los parámetros se han agregado correctamente consultando los detalles del recurso compartido de archivos para el mismo recurso compartido de archivos.

Categoría	Verbo HTTP	Ruta
proveedor de almacenamiento	OBTENGA	`/storage-provider/file-shares/{key}`

Ejemplo de salida JSON

```
"access_control": {
        "acl": [
            {
                "user_or_group": "everyone",
                "permission": "read"
            }
        ],
        "export_policy": {
            "id": 1460288880641,
            "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
            "name": "default",
            "rules": [
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
```

```
                    "index": 1,
                    "protocols": [
                        "nfs3",
                        "nfs4"
                    ],
                    "ro_rule": [
                        "sys"
                    ],
                    "rw_rule": [
                        "sys"
                    ],
                    "superuser": [
                        "none"
                    ]
                },
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
                    "index": 2,
                    "protocols": [
                        "cifs"
                    ],
                    "ro_rule": [
                        "ntlm"
                    ],
                    "rw_rule": [
                        "ntlm"
                    ],
                    "superuser": [
                        "none"
                    ]
                }
            ],
            "_links": {
                "self": {
                    "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
                }
            }
        }
    },
```

```
    "_links": {
        "self": {
            "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
        }
    }
```

Se puede ver la ACL asignada junto con la política de exportación para el mismo recurso compartido de archivos.

Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

"https://www.netapp.com/company/legal/trademarks/"

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

Código abierto

Información sobre los derechos de autor y las licencias de terceros utilizados en este producto.

"Aviso para Active IQ Unified Manager 9.12"

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.