

IBM System Storage DS Storage Manager Versión 10.8

Guía de instalación y soporte de host



Aviso

Antes de utilizar esta información y el producto al que da soporte, lea la información incluida en el apartado "Avisos" en la página 355.

Esta edición se aplica a la versión 10 modificación 83 de IBM DS Storage Manager, y a todos los releases y modificaciones posteriores, hasta que se diga lo contrario en nuevas ediciones.

Esta edición sustituye a GA32-2221-03.

© Copyright IBM Corporation 2012, 2013.

Contenido

Figuras	vii
----------------	------------

Tablas	ix
---------------	-----------

Acerca de este documento	xi
---------------------------------	-----------

Novedades de IBM DS Storage Manager versión 10.86	xii
Documentación relacionada	xiii
Documentación sobre Storage Manager en el sitio web de IBM	xiii
Ayuda en línea u diagnóstico de Storage Manager	xiv
Búsqueda de software, firmware de controlador y archivos léame de Storage Manager	xv
IBM System Storage Productivity Center	xv
Sitios web esenciales para la información de soporte	xvi
Obtención de información, ayuda y servicios	xvii
Antes de llamar	xvii
Uso de la documentación	xvii
Soporte y servicio de software	xviii
Soporte y servicio de hardware	xviii
Avisos y declaraciones de este documento	xviii
Recepción de actualizaciones de productos y notificaciones de soporte	xix

Capítulo 1. Preparación de la instalación 1

Introducción	1
Storage Manager software	1
Componentes de software de Storage Manager	2
Firmwares de controlador soportados	2
Tipos de configuraciones de instalación	3
Configuración de red	3
Configuraciones de conexión directa y SAN	7
Configuración de direcciones de controlador para instalación de software	8
Configuración de direcciones IP para controladores de subsistema de almacenamiento	8
Configuración de una dirección IP con el servidor DHCP/BOOTP	9
Asignación de direcciones TCP/IP estáticas a un subsistema de almacenamiento utilizando la dirección TCP/IP de puerto de gestión predeterminada de fábrica	11
Asignación de direcciones TCP/IP estáticas a subsistemas de almacenamiento utilizando una conexión de gestión dentro de banda	11
Asignación de direcciones TCP/IP estáticas utilizando la interfaz de servicio del puerto serie del controlador del subsistema de almacenamiento	12

Capítulo 2. Interfaz de Storage Manager 15

Ventana Gestión empresarial	15
-----------------------------	----

Uso de la pestaña Dispositivos	18
Uso de la pestaña Configuración	22
Ventana Gestión del subsistema	22
Apertura de la ventana Gestión del subsistema	23
Uso de la pestaña Resumen	24
Uso de la pestaña Almacenamiento y servicios de copia	24
Uso de la pestaña Correlaciones de host	28
Uso de la pestaña Hardware	29
Uso de la pestaña Configuración	30
Gestión de múltiples versiones de software	30

Capítulo 3. Instalación de Storage Manager 33

Requisitos previos a la instalación	33
Instalación de los paquetes de Storage Manager automáticamente con el asistente de instalación	34
Instalación de Storage Manager con una ventana de consola en Linux, AIX, HP-UX y Solaris	37
Instalación manual de los paquetes de Storage Manager	38
Secuencia de instalación de software	38
Instalación manual de Storage Manager	39
Desinstalación de Storage Manager	39
Desinstalación de Storage Manager en un sistema operativo Windows	40
Desinstalación de Storage Manager en un sistema operativo Linux, AIX o Solaris	40
Finalización de la instalación de Storage Manager	40
Realización de un descubrimiento automático de subsistemas de almacenamiento	41
Realización de un descubrimiento manual de subsistemas de almacenamiento	42
Definición de una contraseña de gestión del subsistema de almacenamiento	43
Especificar el nombre de los subsistemas de almacenamiento	43
Configuración de notificaciones de alerta	44
Gestión de la configuración iSCSI	46
Descarga de firmware de controlador, NVSRAM y ESM	50
Descarga de firmware de unidades	57
Características premium de Storage Manager	58
Habilitación de la versión de prueba de la característica Premium	60
Habilitación de una característica Premium permanente	60
Obtención del identificador de habilitación de características premium	60
Generación de un archivo de claves de característica	61
Habilitación de una característica premium	61
Inhabilitación de características premium	62
Guardar el perfil de subsistema de almacenamiento	63

Capítulo 4. Configuración del almacenamiento.	65
Descripción general de la partición del almacenamiento	65
Uso del asistente de tareas	66
Unidades admitidas por IBM System Storage DS Storage Manager	67
Reglas para seleccionar unidades al crear una matriz RAID	68
Atributos de unidad de estado sólido (SSD)	70
Atributos de unidades con capacidad T10PI	71
Atributos del Cifrado de disco completo (FDE)	77
Configuración de almacenamiento de disco	78
Creación de una agrupación de discos	84
Creación de una matriz	85
Matriz redundante de discos independientes (RAID)	86
Creación de una unidad lógica estándar	89
Creación de una unidad lógica ligera	90
Acerca de Dynamic Capacity Expansion	91
Visualización de operaciones en curso	91
Configuración de unidades de repuesto en caliente globales	92
Definición de un sistema operativo host predeterminado	94
Definición de un grupo de host	95
Definición de hosts heterogéneos	96
Definición de host y puertos del host	96
Correlación de LUN	97
Correlación de LUN con un Host o Grupo de host nuevo	97
Adición de LUN a un host o grupo de host existente	97
Configuración de IBM System Storage para IBM i	98
Configuración y uso de características premium opcionales	99
Acerca de Enhanced FlashCopy	99
Acerca de FlashCopy	100
Uso de VolumeCopy	101
Uso de la Duplicación remota mejorada (Enhanced Remote Mirroring)	101
Uso de la Duplicación global mejorada (Enhanced Global Mirroring)	102
Uso de la Memoria caché de lectura de rendimiento	102
Uso del Cifrado de disco completo	102
Uso de otras características	103
Uso de la memoria caché del controlador	103
Uso de reservas persistentes	104
Uso de la exploración de soportes	105
Ajuste de subsistemas de almacenamiento	109
Maximización del rendimiento con el equilibrio d carga	110
Equilibrio de la carga de E/S del canal de fibra	111
Optimización de la tasa de transferencia de E/S	112
Optimización de la tasa de solicitud de E/S	112
Uso de la interfaz de línea de comandos de Storage Manager y el Editor de scripts	115
Interfaz de línea de comandos de Storage Manager	115
Uso del Editor de scripts	115

Capítulo 5. Configuración de hosts	119
Arranque de un sistema operativo host con un arranque SAN	119
Descripción general de los controladores multi-ruta	121
Uso de controladores multi-ruta para gestionar automáticamente la migración tras error y restablecimiento de unidades lógicas	133
Uso de adaptadores de bus de host	136
Instalación de un controlador multi-ruta	138
Controladores multi-ruta AIX	147
Controlador Linux Device Mapper Multipath	147
Controlador Linux RDAC (MPP)	157
Controlador multi-ruta MAC OS	162
Controlador de Veritas DMP	162
Enlaces PV en HP-UX	162
Controladores de migración tras error en Solaris	167
Identificación de dispositivos	179
Uso del programa de utilidad SMdevices	179
Identificación de dispositivos en hostsAIX	180
Configuración de dispositivos	182
Uso del programa de utilidad hot_add	182
Uso del programa de utilidad SMrepassist	183
Detención y reinicio del software del agente de host	183
Definición de la profundidad de cola para dispositivos hdisk	184
Inhabilitación de la duplicación de memoria caché	186
Uso de la expansión de capacidad dinámica y la expansión de unidad lógica dinámica	186
Veritas Storage Foundation con SUSE Linux Enterprise Server	187
Veritas Storage Foundation 5.0 con Red Hat Enterprise Linux	188
Comprobación del tamaño de LUN	189
Redistribución de unidades lógicas	189
Sustitución de HBA en caliente	192
Valores del DSM de Windows y el RDAC de Linux	202
Valores de configuración para la detección de congestión de ruta y los estados de ruta en línea/fuera de línea	209
Configuración de detalles en el sistema de almacenamiento DS5000 y el host AIX para soportar T10PI	212
Configuración del cajón de almacenamiento DS5K	212
Configuración del host AIX	212

Capítulo 6. Trabajo con el Cifrado de disco completo	215
Cifrado de disco completo	216
Protección de datos contra infracción	216
Elección de la gestión de claves de seguridad externa o local	217
Uso de claves de seguridad	219
Uso de borrado seguro	230
Autorizaciones de seguridad FDE	231
Terminología de FDE	233
Antes de empezar	234

Instalación y configuración del servidor DS TKLM Proxy Code	235
Inicio, detención y reinicio del servidor DS TKLM Proxy Code	236
Modificación del archivo de configuración de servidor de código proxy de DS TKLM.	236
Instalación de DS TKLM Proxy Code	240
Configuración de cifrado de disco con unidades FDE	242
Instalación de unidades FDE	242
Habilitación de características premium	242
Seguridad de una matriz RAID	250
Desbloqueo de unidades de disco	256
Migración de subsistemas de almacenamiento (intercambio de cabezal) con unidades FDE	259
Borrado de unidades de disco	263
Unidades de disco de reserva activo globales	266
Archivos de registro	267
Preguntas frecuentes	267
Seguridad de matrices	267
Borrado seguro	268
Gestión local de claves de seguridad	269
Gestión externa de claves de seguridad.	269
Características premium	269
Unidades de repuesto en caliente globales.	270
Soporte de arranque	270
Estados bloqueado y desbloqueado	270
Copia de seguridad y recuperación	271
Otras	271

Capítulo 7. Resolución de problemas 273

Resolución de problemas de eventos críticos	273
Recuperación de almacenamientos intermedios de rastreo.	290
Validación de la base de datos de configuración	291
Guardar/restaurar la base de datos	292
Captura de datos de diagnóstico (DCC) de DS	293
Pasos de recuperación	294
Eventos DDC MEL	295
Resolución de errores de matriz de discos en AIX	296
IBM DS Storage Manager - Restablecer contraseña	301

Apéndice A. Host bus adapter settings 303

Ajuste de la configuración de HBA	303
Acceso a la configuración de HBA a través de Fast!UTIL	303
Configuración predeterminada del adaptador de bus de host	304
Configuración avanzada de HBA.	305
QLogic host bus adapter settings	306
Configuración de adaptador de bus de host JNI y QLogic	311
Configuración de tarjeta JNI HBA	312
Valores de HBA de QLogic	316

Apéndice B. Uso de un subsistema de almacenamiento con una configuración de VMware ESX Server . 319

Configuración de ejemplo	319
------------------------------------	-----

Requisitos de Software	320
Estación de gestión	320
Host (VMware ESX Server).	320
Requisitos de hardware	320
Restricciones de VMware ESX Server	321
Otra información sobre host VMware ESX Server	323
Configuración de subsistemas de almacenamiento para VMware ESX Server	323
Configuración de conexiones cruzadas para conexiones VMware	323
Correlación de LUN con una partición de almacenamiento en VMware ESX Server	324
Verificación de la configuración de almacenamiento para VMware	325

Apéndice C. Uso de Storage Manager con servicios de clúster de alta disponibilidad 327

Información general	327
Uso de servicios de clúster en sistemas AIX	327
Multiproceso de clúster de alta disponibilidad	328
Parallel System Support Programs y General Parallel File System	329
Diagramas de configuración de clúster GPFS, PSSP y HACMP	330
Uso de servicios de clúster en sistemas HP-UX	335
Uso de servicios de clúster en sistemas Solaris	336
Requisitos generales de Solaris	336
Dependencias del sistema	336

Apéndice D. Visualización y definición de atributos de gestor de datos de objeto (ODM) de AIX 339

Definiciones de atributo	339
Uso del comando lsattr para ver atributos de ODM	345

Apéndice E. Acerca del proveedor VDS/VSS 347

Apéndice F. Instalación del proveedor SMI-S. 349

Apéndice G. Accesibilidad 351

Avisos 355

Marcas registradas.	357
Notas importantes.	358

Glosario 361

Índice. 375

Figuras

1. Ejemplo de red utilizando subsistemas de almacenamiento de gestión en red y agente de host	4
2. Partes de la ventana Gestión empresarial	17
3. Configuración automática de la agrupación de discos	70
4. Puntos de comprobación de Protection Information (P)	72
5. Habilitación de T10 PI en una unidad lógica	74
6. Unidad RAID - Información de protección (T10 PI) - habilitada	75
7. Ejemplo - Unidad lógica 4 de matriz RAID 4 - T10PI no habilitada	76
8. Inhabilitación de T10PI.	77
9. Matriz RAID con capacidad FDE - detalles de seguridad	78
10. Asignación de un identificador de puerto para IBM i	98
11. Selección de IBM i como tipo de host	99
12. Ventana del Editor de scripts	116
13. Flujo de E/S en una ruta única óptima	122
14. Flujo de E/S en dos rutas óptimas	123
15. Uso de una ruta cuando la otra falla.	124
16. Migración tras error de E/S en un entorno de ruta única.	125
17. Migración tras error de E/S en un entorno multi-ruta.	126
18. Todas las rutas al controlador fallan en modo de migración tras error AVT/ADT y RDAC	128
19. Todas las rutas al controlador fallan en modo de migración tras error ALUA. Cinco primeros minutos de la migración tras error.	129
20. Todas las rutas al controlador fallan en modo ALUA. Cinco minutos de error	130
21. Ejemplo de configuración de HBA de host a subsistema de almacenamiento para todos los controladores multi-ruta excepto AIX fcp_array y Solaris RDAC	134
22. Ejemplo de configuración de HBA de host a subsistema de almacenamiento para controladores multi-ruta AIX fcp_array y Solaris RDAC	135
23. Esquema de distribución en zonas uno a uno	137
24. Esquema de distribución en zonas uno a dos	138
25. Unidades FDE con seguridad habilitada: Con las autorizaciones adecuadas, la lectura y escritura de datos se produce en estado Desbloqueado	221
26. Eliminación de una unidad FDE con seguridad habilitada del subsistema de almacenamiento: Sin las autorizaciones adecuadas, un disco FDE robado no se puede desbloquear y los datos permanecen cifrados	221
27. Cambio de la clave de seguridad	223
28. Cambio de la clave de seguridad - Completo	224
29. Propiedades de la unidad - Unidad FDE asegurada.	225
30. Seleccionar archivo - LockKeyID	227
31. Propiedades de unidad - Unidad FDE no asegurada.	228
32. Proceso de borrado seguro	231
33. Topología de gestión externa de claves de seguridad.	236
34. Ejemplo de configuración de VMware ESX Server	320
35. Configuración de conexiones cruzadas para conexiones VMware	324
36. Configuración de clúster con un subsistema de almacenamiento individual - una a cuatro particiones	330
37. Configuración de clúster con tres subsistemas de almacenamiento - una partición por subsistema	331
38. Configuración de clúster con cuatro subsistemas de almacenamiento - una partición por subsistema	332
39. Configuración de clúster RVSD con dos subsistemas de almacenamiento - dos particiones por subsistema	333
40. Configuración de clúster HACMP/GPFS con un subsistema de almacenamiento - una partición	334
41. Configuración de clúster HACMP/GPFS con dos subsistemas de almacenamiento - dos particiones por subsistema	335

Tablas

1. Datos mostrados en la vista de tabla	19	28. Opciones y parámetros del comando	
2. Adición de un subsistema de almacenamiento	20	multipath	156
3. Eliminación de subsistemas de		29. Resolución de problemas de Device Mapper	156
almacenamiento	21	30. Descripción de los parámetros de mppUtil	160
4. Eliminación simultánea de varios subsistemas	21	31. Registro de muestra de rutas preferida y	
5. Nodos de la pestaña Lógica	25	alternativa de unidad lógica	165
6. Tipos de nodos en el panel Topología	28	32. Parámetros de configuración del controlador	
7. Información de nodo del panel Correlaciones		de migración tras error	203
definidas	29	33. Parámetros de los valores de tiempo de	
8. Secuencia de instalación de paquetes de		espera	208
software de Storage Manager	38	34. Valores de configuración para la detección de	
9. Ejemplos de comandos de instalación del		congestión de ruta	209
paquete de Storage Manager	39	35. Autorizaciones de seguridad	231
10. Comandos de verificación de instalación del		36. Terminología de cifrado de disco completo	233
paquete de Storage Manager	39	37. Propiedades del archivo de configuración de	
11. Resumen de tipos, interfaces y prestaciones de		proxy	237
unidad compatibles	67	38. Eventos críticos	274
12. Metadatos de Protection Information (8 bytes)	71	39. Paso de recuperación 2	294
13. Tipos de unidades que se pueden utilizar en		40. Paso de recuperación 4	295
matrices y agrupaciones de discos	79	41. Paso de recuperación 5	295
14. Soportes de servicios de copia por matriz y		42. Eventos DDC MEL.	295
agrupación de discos	80	43. Errores de matriz de discos	296
15. Capacidad reservada en una agrupación de		44. QLogic model QLA234x, QLA24xx, QLE2462,	
discos	81	QLE2460, QLE2560, QLE2562, QMI2572,	
16. Lista de características soportadas en una		QMI3572, QMI2582	307
matriz o agrupación de discos.	82	45. QLogic model QL220x (for BIOS V1.81) host	
17. Descripciones de nivel RAID.	87	bus adapter settings by operating system	310
18. Tamaño máximo de Memoria caché de lectura		46. Valores de configuración para	
de rendimiento soportado por la memoria		FCE-1473/FCE-6460/FCX2-6562/FCC2-6562	312
caché de cada controlador instalado	102	47. Valores de configuración para	
19. Errores descubiertos durante una exploración		FCE-1063/FCE2-1063/FCE-6410/FCE2-6410	313
de soportes	107	48. Valores de configuración para FCI-1063	314
20. Opciones de ajuste del supervisor de		49. Valores de configuración para FC64-1063	316
rendimiento de la ventana Gestión del		50. Valores de configuración para QL2342	317
subsistema	110	51. Atributos para dispositivos dar	339
21. Políticas de equilibrio de carga soportadas		52. Atributos para dispositivos dac	341
por casa sistema operativo	110	53. Atributos para dispositivos hdisk	342
22. Modo de migración tras error para cada		54. Ejemplo 1: Visualización de la configuración	
sistema operativo	131	de atributos para un dar	345
23. Controlador multi-ruta por sistema operativo	133	55. Ejemplo 2: Visualización de la configuración	
24. Número de rutas que soporta cada		de atributos para un dac	345
controlador multi-ruta por sistema operativo	135	56. Ejemplo 3: Visualización de la configuración	
25. Parámetros de dsmUtil	144	de atributos para un hdisk	346
26. Versión mínima requerida para cada		57. Operaciones de teclado alternativas de	
componente	148	Storage Manager	352
27. Atributos y valores de parámetros del archivo			
multipath.conf	153		

Acerca de este documento

Lista las tareas para instalar Storage Manager y para la compatibilidad del sistema de host. Las tareas incluyen determinar el hardware y el software, integrar el hardware con la red e instalar el software de Storage Manager además de utilizar características de Storage Manager.

Este documento proporciona información sobre cómo planificar, instalar, configurar y trabajar con IBM® System Storage DS Storage Manager versión 10.83 o posterior, y para subsistemas de almacenamiento con la versión de controlador de firmware 7.8x.xx.xx o posterior. Si IBM DS Storage Manager es anterior al 10.83, consulte la IBM System Storage DS Storage Manager Version 10 - Installation and Host Support Guide (Guía de instalación y soporte de host). Este documento está dirigido a administradores de sistemas y almacenamiento encargados de instalar software de administración de almacenamiento. Para instalar y gestionar un subsistema de almacenamiento con Storage Manager, debe tener conocimientos sobre matriz redundante de discos independientes (RAID), Small Computer System Interface (SCSI), canal de fibra y la tecnología SATA. También deberá tener conocimientos básicos sobre los sistemas operativos aplicables que se utilizan con el software de gestión.

Nota: Las capturas de pantalla de la guía son ilustrativos y pueden diferir de la interfaz de usuario real en función de la versión de Storage Manager y del firmware del controlador.

A lo largo de este documento, el término *Storage Manager* se refiere a todos los niveles de release del software de host.

Utilice este documento para realizar las siguientes tareas:

- Determinar el hardware y el software necesarios para instalar Storage Manager.
- Integrar los componentes de hardware necesarios en su red.
- Instalar el software de Storage Manager.
- Actualizar el firmware de controlador, si fuera necesario.
- Identificar y utilizar las características de gestión de almacenamiento únicas en su instalación.

Importante: Consulte los archivos léame de Storage Manager para cualquier actualización de la lista de sistemas operativos compatibles. Consulte “Búsqueda de software, firmware de controlador y archivos léame de Storage Manager” en la página xv para obtener más información acerca de cómo acceder a los archivos léame de Storage Manager en la web.

Para obtener más información acerca de la terminología, consulte la sección de Ayuda de la ventana Gestión empresarial de Storage Manager, la ventana Gestión del subsistema o el “Glosario” en la página 361.

Al leer este documento, es importante entender la diferencia entre los dos términos siguientes:

Estación de gestión

Una estación de gestión es un sistema que se utiliza para gestionar el

subsistema de almacenamiento. Puede conectarse con el subsistema de almacenamiento de las formas siguientes:

- Por medio de una conexión Ethernet TCP/IP con los controladores del subsistema de almacenamiento
- A través de una conexión TCP/IP con el software del agente host instalado en un sistema principal, que a su vez está directamente vinculado al subsistema de almacenamiento mediante la ruta E/S de canal de fibra o por medio de una conexión Ethernet TCP/IP con los controladores

Sistema principal

Un sistema principal es un sistema que se conecta directamente con el subsistema de almacenamiento por medio de una vía de acceso de E/S de Canal de fibra. Este sistema se utiliza para realizar las siguientes tareas:

- Servir datos (por lo general, en forma de archivos) desde el subsistema de almacenamiento
- Funcionar como un punto de conexión con el subsistema de almacenamiento para una estación de gestión remota

Nota:

1. Los términos *host* y *sistema principal* se utilizan indistintamente en este documento.
2. Un sistema principal también puede funcionar como una estación de gestión.

Novedades de IBM DS Storage Manager versión 10.86

Lista las características que ofrece la versión 10.86 de DS Storage Manager.

Software XOR Engine: Software XOR Engine mejora el rendimiento del subsistema mientras se ejecutan aplicaciones de alto ancho de banda. Cuando se está grabando gran cantidad de datos en el subsistema, la paridad del servicio de hardware podría disminuir la tasa de grabado. El servicio de paridad de firmware aumenta la paridad de hardware, aumenta la cantidad de datos que se pueden grabar en el subsistema. Cuando la paridad de hardware está saturada, los trabajos de paridad se envían a Paridad de Firmware. Este servicio está disponible en los controladores en los que el ancho de banda debe aumentarse para ser compatible con los niveles de rendimiento de destino. La paridad RAID 5, y las paridades de RAID 6 P y Q (la paridad RAID 5 XOR es igual que la paridad RAID 6 P), pueden computarse en la paridad de firmware. Los servicios disponibles en el hardware RAID Parity Assist (RPA) también se pueden implementar (por ejemplo: copiar, comparar, definir). La interacción entre Software XOR Engine y Protection Information (PI) es similar a la interacción entre Protection Information (PI) y el servicio de paridad de hardware. Los campos PI en los bloques de paridad se computan utilizando los campos PI de los bloques de datos. Una lista publicada de errores relacionados con la alineación de los datos se incluye con el hardware Crystal Beach 3 (CB3) RPA. Todas las direcciones de origen y destino deben estar dentro de 64 bytes. Si los datos no están alineados correctamente, el chip CB3 se puede bloquear. Se usa FPE en vez de CB3 para RPA que no está alineado correctamente. El fallo de alineación más común que se implementa es la computación de de paridad para los bloques de caché que se incluyen en PI. CB3 también se utiliza para calcular CRCs para la copia de seguridad de la memoria caché en la memoria flash que se produce durante un fallo en la corriente. De

forma similar, los CRC se comprueban durante la restauración de la memoria caché. Si una operación de CRC no está alineada correctamente, se debe utilizar FPE para calcular o verificar el CRC.

Captura de carga de trabajo: puede utilizar este mecanismo para analizar el rendimiento del subsistema de almacenamiento. Este análisis se utilizaba para ajustar el sistema de host y el subsistema de almacenamiento para un rendimiento óptimo en las condiciones específicas de un lugar. Esta versión incluye una funcionalidad para el análisis fuera de línea del tráfico de E/S del host y las estadísticas de rendimiento. Los resultados del análisis se pueden utilizar para configurar los cambios para aumentar el rendimiento. Versiones posteriores incluirán una funcionalidad para capturar y formatear los datos para ASUP, y configurar cambios en tiempo real. Solo el personal de desarrollo y de asistencia puede controlar el análisis de la carga de trabajo y la recopilación de datos. Se debería utilizar como un proceso no intrusivo durante el funcionamiento normal del sistema de almacenamiento. Las prestaciones y la funcionalidad de Workload Capture es similar a la de otras herramientas de supervisión de rendimiento. Workload Capture no utiliza la interfaz SYMBol y no necesita que se ejecute IBM DS Storage Manager.

Ver solo gestión de contraseña: con la función de gestión de permisos de IBM DS Storage Manager, el nivel de seguridad único se aumenta a dos niveles de permisos de seguridad: permisos de vista y permisos de cambio de configuración. La autenticación de la gestión del subsistema de almacenamiento se asegura en el nivel de procedimiento SYMBol. Los procedimientos SYMBol que modifican la configuración del subsistema de almacenamiento y llevan a cabo operaciones destructivas se llaman procedimientos "activos", mientras que los procedimientos SYMBol que informan sobre los estados del subsistema de almacenamiento y sobre las configuraciones se llaman "procedimientos pasivos". Debe escribir la contraseña del subsistema para invocar los procedimientos SYMBol "activos". En este caso, la contraseña se define como "contraseña del subsistema administrativo". FDE necesita medidas de seguridad adicional para impedir que los usuarios no autorizados modifiquen o recuperen la clave de bloqueo FDE. Como medida de seguridad adicional, debe utilizar la "contraseña para visualización del subsistema" para lanzar la ventana de Gestión del Subsistema. Los usuarios que no están autorizados a modificar las configuraciones del subsistema de almacenamiento, pero que tienen permiso para ver las configuraciones de almacenamiento y gestionar las condiciones de salud, pueden llevar a cabo operaciones de gestión del subsistema de "solo visualización". La contraseña del subsistema para "permiso de solo visualización" se define como "contraseña para visualización del subsistema". A diferencia de la "Contraseña del subsistema administrativo", que está impuesto en la solicitud de procedimiento SYMBol, la autenticación de "contraseña para visualización del subsistema" se gestiona en el nivel de gestión de sesión. El subsistema de almacenamiento ofrece un repositorio persistente para "contraseña para visualización del subsistema" y validación de contraseña.

Documentación relacionada

Además de la información en este documento, están disponibles los recursos descritos en las siguientes secciones.

Documentación sobre Storage Manager en el sitio web de IBM

Hace una lista de las guías de software disponibles en el portal de asistencia y del procedimiento para acceder a ellas.

La siguiente documentación se puede descargar (PDF) en el sitio web de IBM:

- *IBM System Storage DS Storage Manager Command Line Interface and Script Commands Programming Guide*
- *IBM System Storage DS Storage Manager Copy Services User's Guide*
- *IBM System Storage DS4000 Fibre Channel and Serial ATA Intermix Premium Feature Installation Overview*

Para acceder a estos y otros documentos de IBM System Storage desde el Portal de soporte de IBM, complete los pasos indicados a continuación.

Nota: La primera vez que acceda al Portal de soporte de IBM, debe elegir la categoría de producto, la familia de productos y el número de modelo de sus subsistemas de almacenamiento. La siguiente vez que acceda al Portal de soporte de IBM, los productos seleccionados anteriormente se cargarán en el sitio web y solo se mostrarán los enlaces a sus productos. Para cambiar o añadir su lista de productos, pulse el enlace **Gestionar mis listas de productos**.

1. Vaya a <http://www.ibm.com/support/entry/portal>.
2. En **Elija sus productos**, expanda **Hardware**.
3. Pulse **Almacenamiento en sistema > Sistemas de disco > Sistemas de disco de gama media** (para subsistemas de almacenamiento DS4000 o DS5000) o **Sistemas de disco de nivel entrada** (para subsistemas de almacenamiento DS3000), y seleccione la casilla de su subsistema de almacenamiento.
4. En **Elija su tarea**, pulse **Documentación**.
5. En **Ver sus resultados**, pulse **Ver su página**.
6. En el recuadro **Documentación de producto**, pulse el enlace de la publicación a la que desea acceder.

Ayuda en línea u diagnóstico de Storage Manager

Puede acceder a los sistemas de ayuda desde las ventanas Gestión empresarial y Gestión del subsistema de Storage Manager pulsando **Ayuda** en la barra de herramientas o pulsando F1.

Ayuda de la ventana Gestión empresarial

Utilice este sistema de ayuda en línea para obtener más información acerca de cómo trabajar con el dominio de gestión en su totalidad.

Ayuda de la ventana Gestión del subsistema

Utilice este sistema de ayuda en línea para obtener más información acerca de cómo gestionar subsistemas de almacenamiento individuales.

Tras instalar Storage Manager, considere la instalación de la aplicación de diagnóstico y gestión del adaptador de bus de host (HBA), si estuviera disponible. Las aplicaciones QLogic SANsurfer y Emulex HBAnyware son programas de diagnóstico que puede utilizar para verificar el estado de las conexiones de E/S antes de utilizar el subsistema de almacenamiento.

Si su subsistema de almacenamiento está conectado a un HBA de canal de fibra en el servidor host de un entorno SAN, considere la adquisición de la aplicación de software IBM Tivoli Storage Manager para la gestión de SAN y la resolución de problemas.

Búsqueda de software, firmware de controlador y archivos léame de Storage Manager

Hace una lista de los pasos para descargar las últimas versiones del software de Storage Manager y del firmware de controlador desde el portal de asistencia.

El software Storage Manager y las versiones de firmware de controlador están disponibles en el DVD de Storage Manager y también pueden descargarse de Internet.

Importante: Antes de instalar Storage Manager, consulte el archivo léame. Los archivos léame actualizados contienen las últimas versiones de controlador de dispositivos, niveles de firmware, limitaciones y otros datos no presentes en este documento.

Para buscar firmware y archivos léame en el Portal de soporte de IBM, complete los pasos siguientes:

Nota: La primera vez que acceda al Portal de soporte de IBM, debe elegir la categoría de producto, la familia de productos y el número de modelo de sus subsistemas de almacenamiento. La siguiente vez que acceda al Portal de soporte de IBM, los productos seleccionados anteriormente se cargarán en el sitio web y solo se mostrarán los enlaces a sus productos. Para cambiar o añadir su lista de productos, pulse el enlace **Gestionar mis listas de productos**.

1. Vaya a <http://www.ibm.com/support/entry/portal>.
2. En **Elija sus productos**, expanda **Hardware**.
3. Pulse **Sistema de almacenamiento > Sistemas de disco > Sistemas de disco de gama media** y seleccione el recuadro de selección de su subsistema de almacenamiento.
4. Pulse **Seleccionar SO**, seleccione el recuadro correspondiente a su sistema operativo y pulse **Enviar**.
5. En **Elija su tarea**, pulse **Descargas**.
6. En **Ver sus resultados**, pulse **Ver su página**.
7. En el recuadro **Documentación de producto**, pulse el enlace de la publicación a la que desea acceder.

IBM System Storage Productivity Center

IBM System Storage Productivity Center (SSPC) es una solución de hardware y software integrada que proporciona un punto de entrada único para gestionar sistemas IBM System Storage DS3000, DS4000, DS5000, DS8000, clústers IBM System Storage SAN Volume Controller y otros componentes de su infraestructura de almacenamiento de datos. Así, puede utilizar IBM System Storage Productivity Center para gestionar diversas configuraciones de productos IBM System Storage desde una sola interfaz de gestión.

Para saber cómo integrar Storage Manager con IBM System Storage Productivity Center, consulte el Information Center de IBM System Storage Productivity Center en el siguiente sitio web:

publib.boulder.ibm.com/infocenter/tivihelp/v4r1/index.jsp

Sitios web esenciales para la información de soporte

Hace una lista de las páginas web que contienen información sobre Storage Manager, firmware y NVSRAM y las descargas.

Puede encontrar la información más actualizada sobre sus subsistemas de almacenamiento IBM y Storage Manager, incluyendo documentación y descargas de NVSRAM, software y firmware más recientes, en los siguientes sitios web:

Sistemas de almacenamiento de disco IBM System Storage

Encontrará enlaces a descargas de software y firmware, archivos léame y páginas de soporte para todos los sistemas de almacenamiento en disco IBM System Storage:

<http://www.ibm.com/systems/support/storage/disk>

IBM System Storage Interoperation Center (SSIC)

Encontrará información de soporte técnico para su subsistema de almacenamiento y configuración de host específica, incluyendo las últimas versiones de firmware para su sistema, con este programa de utilidad interactivo basado en la web:

<http://www.ibm.com/systems/support/storage/config/ssic>

IBM DS3000, DS4000, DS5000 y BladeCenter Boot Disk System Premium Feature Activation

Active una característica premium con este programa de utilidad basado en la web:

<http://www.ibm.com/storage/fasttkeys>

IBM System Storage Productivity Center

Encontrará la documentación más reciente para IBM System Storage Productivity Center, un nuevo sistema diseñado para proporcionar una consola de gestión central para IBM System Storage DS3000, DS4000, DS5000, DS8000 y SAN Volume Controller:

publib.boulder.ibm.com/infocenter/tivihelp/v4r1/index.jsp

IBM System Storage Support

Encontrará la información de soporte más reciente para sistemas operativos de host, HBA, agrupaciones en clúster, redes de área de almacenamiento (SAN), software de Storage Manager y firmware de controlador:

www.ibm.com/systems/support/storage

Soporte de red de área de almacenamiento (SAN)

Encontrará información sobre el uso de conmutadores SAN, incluyendo enlaces a documentación sobre SAN:

www.ibm.com/systems/support/storage/san

Soporte para servidores IBM System p AIX 5L y Linux

Encontrará la información de soporte más reciente para servidores System p AIX, Linux, BladeCenter y i5/OS:

www.ibm.com/systems/support/supportsite.wss/brandmain?brandind=5000025

Soporte para servidores IBM System x

Encontrará la información de soporte más reciente para servidores System x Intel- y basados en AMD:

<http://www.ibm.com/systems/support/>

System p y AIX Information Center

Encontrará información sobre cómo utilizar AIX con servidores System p y POWER:

[publib.boulder.ibm.com/infocenter/pseries/index.jsp?](http://publib.boulder.ibm.com/infocenter/pseries/index.jsp)

Productos IBM System Storage

Encontrará información sobre todos los productos IBM System Storage:

www.ibm.com/systems/storage

Centro de publicaciones de IBM

Encontrará publicaciones de IBM:

www.ibm.com/shop/publications/order/

Obtención de información, ayuda y servicios

Si necesita ayuda, servicios o asistencia técnica, o si desea más información sobre los productos IBM, IBM pone a su disposición una gran variedad de medios para ayudarle. Esta sección contiene información sobre dónde debe acudir para obtener información adicional sobre IBM y los productos IBM, qué hacer si tiene un problema con su sistema y a quién llamar para recibir servicio, en caso de ser necesario.

Antes de llamar

Hace una lista de los pasos para que resuelva el problema usted mismo sin necesidad de ponerse en contacto con IBM.

Antes de llamar, realice estos pasos para intentar resolver el problema:

- Compruebe todos los cables para asegurarse de que están conectados.
- Compruebe los interruptores de alimentación para asegurarse de que el sistema está encendido.
- Utilice la información de resolución de problemas de la documentación del sistema y utilice las herramientas de diagnóstico que se entregan con el sistema.
- Compruebe la información técnica, consejos, sugerencias y nuevos controladores de dispositivos en las páginas del sitio web de IBM System Storage Disk Support indicadas en esta sección.
- Utilice un foro de discusión de IBM en el sitio web de IBM para realizar preguntas.

Puede solucionar muchos problemas sin ayuda externa siguiendo los procedimientos de resolución de problemas que IBM proporciona en la ayuda en línea de Storage Manager o en los documentos que se proporcionan con el sistema o software. En la información que se entrega con el sistema también se describen las pruebas de diagnóstico que puede realizar. La mayoría de subsistemas, sistemas operativos y programas vienen con información que contiene procedimientos de resolución de problemas y explicaciones sobre mensajes de error y códigos de error. Si tiene la sospecha de que se ha producido un problema relacionado con el software, consulte la información del sistema operativo o del programa.

Uso de la documentación

La información sobre su sistema IBM y software instalado previamente, si existiese, está disponible en los documentos facilitados con su sistema; entre estos se incluyen libros impresos, documentos en línea, archivos léame y archivos de ayuda. Consulte la información de resolución de problemas en la documentación

del sistema para obtener instrucciones sobre la utilización de los programas de diagnóstico. La información de resolución de problemas o los programas de diagnóstico pueden indicarle que necesita controladores de dispositivo adicionales o actualizados u otro software.

Soporte y servicio de software

Hace una lista de las páginas web de soporte de IBM en las que puede obtener asistencia telefónica sobre problemas de software.

A través de la Línea de soporte de IBM, puede obtener asistencia telefónica para resolver problemas de utilización, configuración y software. Para obtener información sobre los productos incluidos en la Línea de productos de su país o región, vaya al siguiente sitio web:

www.ibm.com/services/sl/products

Para obtener más información sobre la Línea de soporte de IBM y otros servicios de IBM, vaya a los siguientes sitios web:

- www.ibm.com/services
- www.ibm.com/planetwide

Soporte y servicio de hardware

Contiene el sitio web para servicio de hardware con el horario disponible en EE. UU., Canadá y Reino Unido.

Puede recibir servicio de hardware a través de IBM Integrated Technology Services o a través de su distribuidor de IBM, si su distribuidor está autorizado por IBM para proporcionar servicio de garantía. Vaya al siguiente sitio web para consultar teléfonos de soporte:

www.ibm.com/planetwide

En Estados Unidos y en Canadá, el servicio y el soporte de hardware está disponible 24 horas al día, siete días a la semana. En el Reino Unido, estos servicios están disponibles de lunes a viernes, de 9 a.m. a 6 p.m.

Avisos y declaraciones de este documento

Este documento contiene los siguientes avisos, que resaltan información fundamental:

- **Nota:** Estos avisos proporcionan sugerencias, instrucciones o consejos importantes.
- **Importante:** estos avisos proporcionan información que podría ayudarle a evitar inconvenientes o problemas.
- **Atención:** Estos avisos indican la posibilidad de que se produzca un daño en los programas, en los dispositivos o en los datos. Los avisos de atención aparecen justo delante de la instrucción o situación en la que podría producirse un daño.
- **Precaución:** estas declaraciones indican situaciones que pueden ser potencialmente peligrosas para el usuario. Las declaraciones de precaución aparecen justo delante de la descripción de un paso de procedimiento o situación potencialmente peligrosos.

Recepción de actualizaciones de productos y notificaciones de soporte

Le informa sobre cómo recibir notificaciones de actualización de productos sobre el software de Storage Manager, el firmware del controlador, el firmware de ESM, y el firmware de la unidad.

Descargue las últimas versiones de los siguientes paquetes durante la instalación inicial y cuando estén disponibles actualizaciones de los productos:

- Software host Storage Manager
- Firmware de controlador de subsistema de almacenamiento
- Firmware ESM de alojamiento de expansión de almacenamiento de unidad
- Firmware de unidades

Importante: Mantenga su sistema actualizado con las últimas versiones de firmware y otras actualizaciones de productos suscribiéndose para recibir notificaciones de soporte. Vaya al siguiente sitio web y pulse **Mis notificaciones** para obtener más información sobre cómo registrarse para recibir notificaciones de soporte:

<http://www.ibm.com/systems/support>

También encontrará actualizaciones de productos y notificaciones de soporte si utiliza el sitio web del Portal de soporte de IBM en:

<http://www.ibm.com/support/entry/portal>

Capítulo 1. Preparación de la instalación

La siguiente información le ayudará a prepararse para instalar correctamente el software Storage Manager.

- “Storage Manager software”
- “Firmwares de controlador soportados” en la página 2
- “Tipos de configuraciones de instalación” en la página 3
- “Configuración de direcciones de controlador para instalación de software” en la página 8

Introducción

Hace una lista de los sistemas operativos con los que es compatible Storage Manager para los subsistemas de almacenamiento DS3000, DS4000 y DS5000, y también para los sistemas operativos que son compatibles cuando van junto con los subsistemas.

IBM System Storage DS Storage Manager consiste en un conjunto de herramientas cliente y host que puede utilizar para gestionar subsistemas de almacenamiento IBM DS3000, DS4000 y DS5000 desde una estación de gestión.

Storage Manager es compatible con los siguientes sistemas operativos:

- AIX
- Windows Server 2003, Windows Server 2008 y Windows Server 2012
- Linux (RHEL y SLES)
- HP-UX
- Solaris

Los subsistemas de almacenamiento DS3000, DS4000 y DS5000 también se soportan en asociación con hosts Apple Mac OS, VMware ESX Server y System p Virtual IO Server (VIOS), así como con i5/OS como cliente invitado en VIOS. IBM no proporciona software host para estos sistemas operativos. Debe instalar IBM DS Storage Manager en una estación de gestión que tenga instalado uno de los sistemas operativos indicados anteriormente.

Puede encontrar información sobre soporte de i5/OS en el siguiente sitio web:

www.ibm.com/systems/i/os/

Para obtener información adicional, consulte el Centro de interoperación de System Storage en el siguiente sitio web:

<http://www.ibm.com/systems/support/storage/config/ssic>

Storage Manager software

Lists the tasks you can perform using the Storage Manager software, including accessing premium features.

Storage Manager is used to configure, manage, and troubleshoot storage subsystems. It is used primarily to configure disk pools or RAID arrays and logical

drives, assign logical drives to hosts, replace and rebuild failed disk drives, expand the size of the disk pools, arrays and logical drives, and convert from one RAID level to another. Storage Manager enables troubleshooting and management tasks, such as checking the status of the storage subsystem components, updating the firmware of the RAID controllers, and managing the storage subsystem. Finally, the Storage Manager offers access to premium features such as FlashCopy, VolumeCopy, and Enhanced Remote Mirroring.

For the latest firmware versions that are supported by each storage subsystem model, see the readme file for your operating system.

Componentes de software de Storage Manager

Hace una lista de los componentes de software de Storage Manager y de las diferencias dependiendo del sistema operativo.

Storage Manager incluye los siguientes componentes de software cliente.

Nota: Los componentes de Storage Manager podrían variar en función del sistema operativo. Para Storage Manager versión 10.77.xx.xx y posteriores, el instalador Microsoft MPIO DSM es independiente del instalador de Storage Manager que le permite instalar los componentes indicados a continuación. No obstante, el instalador de Storage Manager y el de Microsoft MPIO DSM están incluidos en un solo paquete de código. Este paquete de código está disponible en el Portal de soporte de IBM.

Software SMruntime

Compilador Java™ de Storage Manager

Software SMesm

Paquete de entrega de firmware de ESM de Storage Manager

Software SMclient

Paquete cliente de Storage Manager

Software SMagent

Paquete agente de Storage Manager

Software SMutil

Paquete de programas de utilidad de Storage Manager

Firmwares de controlador soportados

Todas las versiones de firmware de controlador están disponibles sin costes en el sitio web de IBM.

Para lograr el mayor nivel de compatibilidad y menor número de operaciones sin errores, asegúrese de contar con la última versión de firmware de controlador disponible para su modelo de subsistema de almacenamiento.

Importante: Si la versión de Storage Manager es 10.84.xx.xx o posterior, el firmware del controlador debe ser 6.50.xx.xx o posterior.

Para obtener información detallada sobre cómo descargar el nivel de versiones de firmware más actual, consulte "Descarga de firmware de controlador, NVSRAM y ESM" en la página 50.

Tipos de configuraciones de instalación

Define una configuración de red y una configuración adjunta directa o adjunta a SAN.

Una estación de gestión puede tener cualquiera de las configuraciones siguientes:

Configuración de red (Fuera de banda)

Un sistema remoto, conectado a una red Ethernet, utilizado para gestionar uno o varios subsistemas de almacenamiento.

Configuración de conexión directa o conexión a SAN (dentro o fuera de banda)

Sistema que se conecta a un subsistema de almacenamiento por medio de una ruta de E/S de canal de fibra, iSCSI o SAS. Este host puede utilizar la ruta de E/S (dentro de banda) o sus puertos de red Ethernet (fuera de banda).

Configuración de red

Informa sobre tareas relacionadas con la red que debe realizar antes de instalar el Storage Manager.

Antes de instalar el software de Storage Manager, asegúrese de que los componentes de red están configurados y funcionan correctamente y que tiene toda la información sobre el host y el controlador necesaria para el funcionamiento correcto del software.

Nota: Cuando conecte el subsistema de almacenamiento a un conmutador Ethernet, defina los valores del puerto del conmutador para auto-negociar.

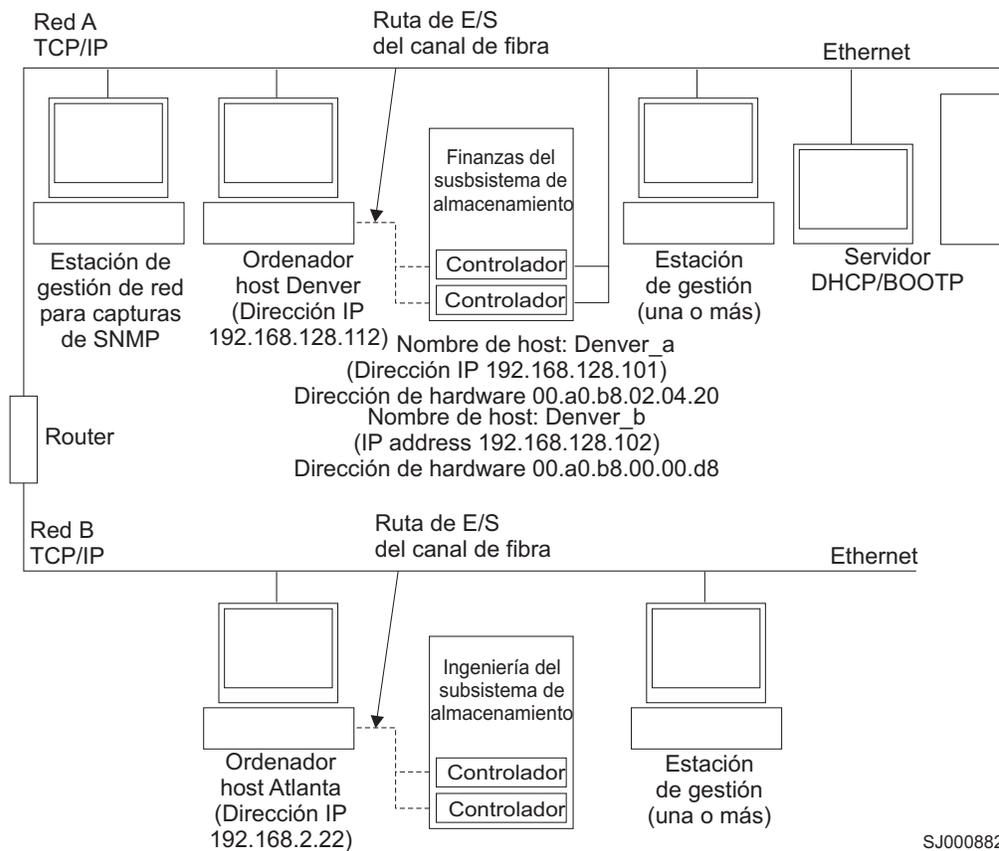


Figura 1. Ejemplo de red utilizando subsistemas de almacenamiento de gestión en red y agente de host

Revisión de un ejemplo de configuración de red

Revisa los componentes una red gestionada por un subsistema de almacenamiento y de un agente de host gestionado por un subsistema de almacenamiento.

La Figura 1 muestra un ejemplo de una red que contiene un subsistema de almacenamiento de gestión en red (Red A) y un subsistema de almacenamiento de gestión de agente de host (Red B).

Subsistema de almacenamiento de gestión en red: la Red A es un subsistema de almacenamiento de gestión en red. Tanto la estación de gestión como el subsistema de almacenamiento están conectados a la red Ethernet. La Red A contiene los componentes siguientes:

- Un servidor DHCP/BOOTP
- Una estación de gestión en red para condiciones de excepción de Protocolo simple de gestión de red (SNMP)
- Un sistema principal que está conectado con un subsistema de almacenamiento por medio de una ruta de E/S de canal de fibra
- Una estación de gestión que esté conectada mediante un cable Ethernet a los controladores del subsistema de almacenamiento

Nota: Si se utilizan las direcciones TCP/IP estáticas o direcciones TCP/IP predeterminadas del controlador, no tiene que configurar el servidor DHCP/BOOTP.

Subsistema de almacenamiento de gestión de agente de host: la Red B es un subsistema de almacenamiento de gestión de agente de host. Puede gestionar el subsistema de almacenamiento utilizando la misma ruta, de canal de fibra o SAS, que utiliza un servidor de host para enviar E/S entre el host y el subsistema de almacenamiento haciendo uso del software agente Storage Manager instalado en el servidor de host. Los puertos de gestión Ethernet del subsistema de almacenamiento normalmente no están conectados a la red Ethernet.

El agente Storage Manager requiere que se asigne/correlacione un LUN especial a la partición de host. A este LUN se le denomina LUN UTM o de acceso y es utilizado por el agente Storage Manager y el controlador para pasar información de gestión. Este LUN se asigna automáticamente a la partición de host como LUN 31 la primera vez que se asigna la unidad lógica a la partición de host. Dado que el LUN reduce en uno el número máximo de LUN/unidades lógicas que se pueden asignar al host, utilice la interfaz gráfica de usuario de gestión del subsistema de almacenamiento para desasignarlo sin el subsistema de almacenamiento se gestiona únicamente a través del método de fuera de banda.

Nota: El subsistema de almacenamiento se puede gestionar dentro y fuera de banda a la vez.

La Red B contiene los componentes siguientes:

- Un host que está conectado con un subsistema de almacenamiento por medio de una ruta de E/S soportada
- Una estación de gestión que está conectada mediante un cable Ethernet con el sistema principal

Configuración de una estación de gestión

Define una estación de gestión e informa sobre las tareas que lleva a cabo.

La *estación de gestión* es el servidor responsable de gestionar toda o parte de una red de almacenamiento. Esta se comunica con los agentes de gestión de la red en los nodos gestionados, utilizando un protocolo de gestión de la red como el protocolo simple de gestión de red(SNMP).

Los comandos de gestión del almacenamiento se envían a los controladores del subsistema de almacenamiento, donde el firmware del controlador los valida, ejecuta y devuelve información sobre el estado y configuración al software cliente.

Definición de una configuración de gestión en red (fuera de banda)

Le informa sobre cómo establecer una configuración de gestión en red (dentro de banda).

Los siguientes pasos proporcionan una visión general de las tareas necesarias para configurar la red para la instalación de una configuración de gestión en red (fuera de banda):

Importante: Un máximo de ocho estaciones de gestión pueden supervisar de manera simultánea un subsistema de almacenamiento de gestión fuera de banda. Este límite no se aplica a los servidores que gestionan el subsistema de almacenamiento a través del método de gestión dentro de banda.

1. Instale todos los componentes de hardware (sistemas principales, subsistemas de almacenamiento y cables) que desee conectar a la red. Para obtener más información sobre la instalación de componentes de hardware, consulte la documentación que se facilita con los mismos.
2. Establezca un convenio de denominación para los subsistemas de almacenamiento que se va a conectar a la red.
3. Anote el nombre de los subsistemas de almacenamiento y tipos de gestión.

Nota: En los pasos restantes, deberá registrar determinada información para su uso en el futuro, por ejemplo las direcciones IP y Ethernet del hardware.

4. Determine la dirección MAC Ethernet de hardware para cada controlador del subsistema de almacenamiento conectado a la red. Si utiliza una dirección IP de controlador predeterminada, vaya al paso 6. De otro modo, solicite al administrador de la red la dirección TCP/IP y el nombre del sistema principal de cada uno de los controladores de los subsistemas de almacenamiento de la red.
5. Configure el servidor DHCP/BOOTP para proporcionar información sobre la configuración de red para un controlador específico. Si utiliza direcciones IP de controlador estáticas, salte este paso.
6. Verifique que se ha instalado el software TCP/IP.
7. Configure el host o tabla de servidor de nombres de dominio (DNS).
8. Encienda los dispositivos conectados a la red.

Definición de una configuración de gestión de agente de host (dentro de banda)

Le informa sobre cómo establecer una configuración de agente de host gestionado (dentro de banda).

Los siguientes pasos proporcionan una visión general de las tareas necesarias para configurar una instalación de una configuración de gestión de agente de host (dentro de banda):

1. Instale todos los componentes de hardware (sistemas principales, subsistemas de almacenamiento y cables) que desee gestionar. Para obtener más información sobre la instalación de componentes de hardware, consulte la documentación que se facilita con los mismos. El sistema principal debe tener configuradas conexiones de E/S al subsistema de almacenamiento (por ejemplo, el host debe tener instalado un sistema operativo con el controlador de dispositivo aplicable para los adaptadores de bus de host).
2. Instale el software host Storage Manager y el software agente Storage Manager.
3. Establezca un convenio de denominación para los subsistemas de almacenamiento que se va a conectar a la red.
4. Anote el nombre de los subsistemas de almacenamiento y tipos de gestión.

Nota: En los pasos restantes, deberá registrar determinada información para su uso en el futuro, por ejemplo las direcciones IP y Ethernet del hardware.

5. Obtenga la dirección IP y nombre de host del sistema principal en el que se ejecutará el software de agente de host desde el administrador de red.

Nota: SAgent forma parte del paquete de software de Storage Manager y es necesario en el host conectado al subsistema de almacenamiento a través de cualquiera de las interfaces soportadas.

6. Verifique que se ha instalado el software TCP/IP.
7. Encienda los dispositivos conectados a la red.

Nota: Aunque no conecte el host y los puertos Ethernet de gestión de los subsistemas de almacenamiento a la red, el host utiliza igualmente TCP/IP para comunicarse con el agente de host. El agente de host se comunica con el controlador mediante la conexión de canal de fibra a través del *volumen de acceso*.

Configuraciones de conexión directa y SAN

Storage Manager soporta la gestión dentro de banda de subsistemas de almacenamiento con configuraciones de conexión directa o en un entorno SAN a través de conmutadores.

Definición de una configuración de conexión directa

Le informa sobre cómo conectarse directamente un subsistema de almacenamiento al Storage Manager.

Importante: Los subsistemas de almacenamiento con puertos iSCSI no soportan conexiones directas entre los sistemas host y los puertos iSCSI del subsistema.

Antes de comenzar, verifique que:

- Puede conectar uno o dos servidores a los subsistemas de almacenamiento.
- No se están utilizando conmutadores externos o conectores de canal de fibra externos.
- Consulte la *Guía de instalación y del usuario* para obtener más información sobre su subsistema de almacenamiento.

Complete los siguientes pasos para definir una configuración de conexión directa:

1. Conecte los HBA a cada controlador del subsistema de almacenamiento.
2. Utilice la característica de descubrimiento automático de Storage Manager para asegurarse de que se descubre el subsistema de almacenamiento.

Definición de una configuración de conexión a SAN

Le informa cómo conectar los subsistemas de almacenamiento a Storage Manager en una SAN.

Una configuración de conexión a SAN puede disponer de conexiones de canal de fibra, SAS o iSCSI.

Si utiliza HBA de canal de fibra en su configuración de conexión a SAN, las conexiones del HBA y el puerto de host de subsistema de almacenamiento deben estar aisladas en zonas de tejido para minimizar las posibles interacciones entre los puertos en un entorno de tejido SAN. A través de un conmutador de canal de fibra, SAS o Ethernet se pueden configurar varios subsistemas de almacenamiento al mismo conjunto de HBA. Para obtener más información sobre los esquemas de distribución en zonas de canal de fibra, consulte “Conexión de HBA en un entorno de conmutador de canal de fibra” en la página 136. Además, con conmutadores SAS y Ethernet se pueden implementar diferentes esquemas de distribución en zonas.

Atención: Una configuración de un solo HBA puede provocar la pérdida de acceso a datos en caso de error en la ruta. Si tiene un solo HBA en una configuración de conexión a SAN, ambos controladores del subsistema de almacenamiento estén conectados al HBA a través de un conmutador y en la misma zona SAN que el HBA.

Complete los siguientes pasos para definir una configuración de conexión a SAN:

1. Conecte los HBA al conmutador o conmutadores.
2. Conecte el subsistema de almacenamiento al conmutador o conmutadores.
3. Defina las distribuciones en zonas o VLAN necesarias en los conmutadores de canal de fibra o Ethernet, si fuera necesario.
4. Utilice la característica de descubrimiento automático de Storage Manager para asegurarse de que se descubre el subsistema de almacenamiento.

Configuración de direcciones de controlador para instalación de software

El modo en que planea gestionar los subsistemas de almacenamiento determinan dónde debe instalar los componentes de software. Antes de instalar los componentes de software, debe asignar direcciones IP a los controladores del almacenamiento.

Nota:

1. Los controladores deben estar conectados a un puerto LAN definido para negociar automáticamente la velocidad de datos. Cuando están conectados a un puerto de conmutador definido para una velocidad fija, los controladores no funcionan adecuadamente.
2. Para gestionar los subsistemas de almacenamiento a través de un cortafuegos, configúrelo para abrir el puerto 2463 a los datos TCP.

Configuración de direcciones IP para controladores de subsistema de almacenamiento

Hace una lista de los componentes del servidor DHCP o BOOTP y de la red y explica cómo se asignan las direcciones de IP a los controladores de subsistema de almacenamiento.

Complete los siguientes procedimientos tras instalar SMruntime y SMclient, como se describe en la sección sobre instalación para su sistema operativo de host.

Debe configurar un servidor DHCP o BOOTP y una red con los siguientes componentes:

- Un servidor DHCP o BOOTP
- Una estación de gestión en red para condiciones de excepción de Protocolo simple de gestión de red (SNMP)
- Un sistema principal que está conectado con un subsistema de almacenamiento por medio de una ruta de E/S de canal de fibra
- Una estación de gestión que esté conectada mediante un cable Ethernet a los controladores del subsistema de almacenamiento

Nota: Puede evitar las tareas relacionadas con el servidor DHCP/BOOTP y la red asignando direcciones IP estáticas al controlador. Si no quiere asignar direcciones TCP/IP estáticas con Storage Manager, utilizando las direcciones TCP/IP predeterminadas del subsistema de almacenamiento como se muestra en "Asignación de direcciones TCP/IP estáticas a un subsistema de almacenamiento utilizando la dirección TCP/IP de puerto de gestión predeterminada de fábrica" en la página 11, establezca una conexión de gestión dentro de banda con el subsistema de almacenamiento y cambie la dirección IP del puerto de gestión en la ventana Gestión del subsistema.

Si un controlador tiene dos puertos de gestión, ambos comparten la misma dirección de pasarela. La dirección de pasarela obtenida o facilitada más recientemente es la utilizada por ambos puertos. Así, es posible perder acceso en un puerto como resultado del cambio de la configuración del otro puerto. Si ambos puertos se configuran manualmente, se utilizará la dirección de pasarela facilitada más recientemente. Si un puerto se configura manualmente y DHCP está habilitado en el otro puerto, se utilizará la dirección de pasarela facilitada más recientemente. Por lo general, se trata de la dirección de pasarela facilitada por el servidor DHCP a menos que se cambie la configuración manual del otro puerto. En este caso, la dirección de pasarela se debe definir con el valor proporcionado por el controlador, que debe coincidir con la dirección de pasarela obtenido del servidor DHCP. Si DHCP está habilitado en ambos puertos, los servidores DHCP conectados a los dos puertos deben configurarse para proporcionar la misma dirección de pasarela. Si los servidores DHCP utilizan diferentes direcciones de pasarela, ambos puertos utilizarán la dirección de pasarela facilitada más recientemente.

Cualquier cambio realizado en el acceso de inicio de sesión remoto afectarán a ambos puertos. En otras palabras, si el acceso de inicio de sesión remoto se habilita o inhabilita en un puerto, también se habilitará o inhabilitará en el otro puerto. Como ocurre con la dirección de pasarela, la configuración más reciente aplicada al inicio de sesión remoto se aplicará a ambos puertos. Por ejemplo, si el acceso de inicio de sesión remoto se habilita en el puerto 1, también se habilitará en el puerto 2. Si posteriormente un servidor DHCP proporciona parámetros de configuración para el puerto 2 que incluyan la inhabilitación del acceso de inicio de sesión remoto, este se inhabilitará en ambos puertos.

Si un controlador tiene dos puertos de gestión, los dos puertos Ethernet deben estar en subredes diferentes. Si ambos puertos están en la misma subred, o si tienen la misma dirección de red (lógica Y dirección IP y máscara de subred), se mostrará la notificación de evento Error de configuración de subred.

Configuración de una dirección IP con el servidor DHCP/BOOTP

Este tema describe los pasos para definir el servidor y la red DHCP/BOOTP.

Complete los pasos siguientes para configurar la red y el servidor DHCP/BOOTP:

1. Consiga la dirección MAC de cada controlador de subsistema de almacenamiento. (Consulte el procedimiento "Identificación de direcciones MAC Ethernet").
2. Complete cuál de los pasos siguientes es aplicable para su servidor:
 - En un servidor DHCP, cree un registro de DHCP para cada una de las direcciones MAC. Establezca el mayor tiempo posible como duración del arrendamiento.
 - En un servidor BOOTP, edite el archivo `bootptab` para añadir las entradas que asocian la pestaña de la dirección MAC con la dirección TCP/IP.
3. Conecte los puertos Ethernet del subsistema de almacenamiento DS3000, DS4000 o DS5000 a la red.
4. Arranque el subsistema de almacenamiento.

Identificación de direcciones MAC Ethernet

Explica las direcciones de Control de acceso a soportes (MAC) del hardware de Ethernet que tienen los controladores, con el formato y con un ejemplo.

Para gestionar su subsistema de almacenamiento con el método de gestión directa, debe identificar la dirección de Control de acceso a soportes (MAC) Ethernet de hardware para cada controlador.

Todos los subsistemas de almacenamiento tienen una etiqueta con el número de dirección MAC Ethernet de hardware. El número tiene el formato *xx.xx.xx.xx.xx.xx*, donde *x* representa una letra o un número. Por ejemplo, una dirección MAC Ethernet podría ser 00.a0.b8.20.00.d8.

Las instrucciones y ubicaciones de la etiqueta de los subsistemas de almacenamiento particulares se indican en las secciones siguientes.

Identificación de direcciones MAC Ethernet en subsistemas de almacenamiento DS4800, DS5100 o DS5300: El tipo de sistema, número de modelo y número de serie se encuentran en la parte superior de cada unidad de controlador RAID. Las direcciones MAC están cerca de los puertos Ethernet de cada controlador RAID.

Nota: Puede acceder a los controladores desde la parte trasera del chasis de un DS4800, DS5100 o DS5300.

Identificación de las direcciones Ethernet MAC en un subsistema de almacenamiento DS3000, DS3500, DCS3700, DS3950, DS4200, DS4700, DS5020 o un subsistema de almacenamiento DCS3700 con Controladores del módulo de rendimiento: Las direcciones MAC de estos subsistemas de almacenamiento están cerca de los puertos Ethernet de cada controlador RAID.

Nota: Puede acceder a los controladores desde la parte trasera del chasis del subsistema de almacenamiento.

Identificación de direcciones MAC Ethernet en un subsistema de almacenamiento DS4400, o DS4500: Para identificar direcciones MAC Ethernet de hardware en subsistemas de almacenamiento DS4400 y DS4500, complete los pasos siguientes:

1. Retire el frontal del subsistema de almacenamiento y tire con cuidado de la parte inferior para soltar las patillas. Deslice el frontal hacia abajo.
2. En la parte frontal de cada controlador, busque la etiqueta que tiene la dirección MAC Ethernet de hardware. El número tendrá la forma *xx.xx.xx.xx.xx.xx* (por ejemplo, 00.a0.b8.20.00.d8).
3. Registre cada dirección MAC Ethernet.
4. Para volver a colocar el frontal, deslice el borde superior bajo el borde del chasis. A continuación presione el inferior del frontal hasta que las patillas encajen en los agujeros de montaje.

Identificación de direcciones MAC Ethernet en un subsistema de almacenamiento DS4100, o DS4300: Para identificar direcciones MAC Ethernet de hardware en sistemas 3542 (DS4100 o 1722 (DS4300), complete los pasos siguientes:

1. Localice la dirección MAC Ethernet en la parte trasera de la unidad, bajo los puertos de host de canal de fibra del controlador. El número tendrá la forma *xx.xx.xx.xx.xx.xx* (por ejemplo, 00.a0.b8.20.00.d8).
2. Registre cada dirección MAC Ethernet.

Asignación de direcciones TCP/IP estáticas a un subsistema de almacenamiento utilizando la dirección TCP/IP de puerto de gestión predeterminada de fábrica

Explica cómo asignar direcciones de TCP/IP estáticas a los controladores del subsistema de almacenamiento mediante las opciones predeterminadas de fábrica.

Complete los pasos siguientes para asignar direcciones TCP/IP estáticas a controladores del subsistema de almacenamiento, utilizando las direcciones TCP/IP predeterminadas asignadas a los controladores durante su fabricación:

1. Realice una conexión de gestión directa al subsistema de almacenamiento utilizando las direcciones TCP/IP predeterminadas para los controladores. Para conocer las direcciones TCP/IP predeterminadas para su subsistema de almacenamiento, consulte la *Guía del usuario e instalación* que se incluye con el hardware instalado en el puerto de gestión del controlador etiquetado como número 1 (#1).

- Controlador A: 192.168.128.101
- Controlador B: 192.168.128.102
- Máscara de subred: 255.255.255.0

Nota: Para un subsistema de almacenamiento que tiene dos puertos Ethernet por controlador (como DCS3700, DCS3700 con los controladores de módulo de rendimiento, DCS3860, DS5020, DS3500, DS5100 y DS5300), utilice el puerto Ethernet que está etiquetado como número 2 (#2). Las direcciones IP predeterminadas del segundo puerto Ethernet son las siguientes:

- Controlador A: 192.168.129.101
- Controlador B: 192.168.129.102
- Máscara de subred: 255.255.255.0

2. Inicie SMclient. Se abrirá la ventana Gestión empresarial.
3. En la ventana de Gestión empresarial, pulse en el nombre de subsistema de almacenamiento predeterminado. Se abrirá la ventana Gestión del subsistema.
4. En la ventana Gestión del subsistema, pulse con el botón derecho en el icono del controlador y seleccione **Cambiar > Configuración de red** en el menú. Se abrirá la ventana Cambiar configuración de red.
5. En la ventana Cambiar configuración de red, pulse las pestañas **Controlador A** y **Controlador B** y escriba las nuevas direcciones TCP/IP en los campos aplicables. Pulse **Aceptar**.
6. Cierre la ventana Subsistema de Gestión, espere 5 minutos y suprima la entrada del subsistema de almacenamiento predeterminado en la ventana Gestión de empresa.
7. Añada una nueva entrada de subsistema de almacenamiento en la ventana Gestión empresarial utilizando la nueva dirección TCP/IP.

Asignación de direcciones TCP/IP estáticas a subsistemas de almacenamiento utilizando una conexión de gestión dentro de banda

Para host conectados a un subsistema de almacenamiento a través de una ruta de E/S de canal ed fibra, complete los siguientes pasos si desea asignar una dirección TCP/IP estática a los controladores del subsistema de almacenamiento a través del host con conectividad de canal de fibra y del puerto del host de canal de fibra del subsistema de almacenamiento.

Para completar este procedimiento debe disponer de los componentes siguientes:

- Un sistema principal que está conectado con un subsistema de almacenamiento por medio de una ruta de E/S de canal de fibra
- Una estación de gestión que esté conectada mediante un cable Ethernet a los controladores del subsistema de almacenamiento

Nota: No se puede realizar la gestión dentro de banda con un host que tenga conexiones iSCSI al subsistema de almacenamiento hasta que se haya configurado. En su lugar, utilice otros métodos de esta sección para asignar una dirección TCP/IP estática a los puertos de gestión del controlador del subsistema de almacenamiento.

1. Instale el software de cliente DS Storage Manager en el host y asegúrese de que el software SMagent está instalado y en ejecución.
2. Inicie el software de cliente DS Storage Manager. Se abrirá la ventana de Gestión empresarial.
3. Añada el subsistema de almacenamiento al dominio de Gestión empresarial utilizando la dirección IP del host con conectividad de canal de fibra al subsistema de almacenamiento.
4. En la ventana de Gestión empresarial, pulse en el nombre de subsistema de almacenamiento que se acaba de descubrir. Se abrirá la ventana de Gestión del subsistema.
5. En la ventana Gestión del subsistema, pulse con el botón derecho en el icono Controlador y seleccione **Cambiar > Configuración de red** en el menú desplegable. Se abrirá la ventana Cambiar configuración de red.
6. En la ventana Cambiar configuración de red, pulse las pestañas Controlador A y Controlador B y escriba las nuevas direcciones TCP/IP en los campos aplicables.
7. Pulse **Aceptar**.
8. Cierre la ventana Gestión del subsistema.
9. Espere al menos cinco minutos.
10. Suprime la entrada del subsistema de almacenamiento existente en la ventana Gestión empresarial.
11. Si procede, cambie la dirección IP del puerto Ethernet en la estación de gestión por un valor que esté en la misma subred TCP/IP que las direcciones IP del puerto Ethernet del controlador que acaba de asignar.
12. Salga de DS Storage Manager.
13. Reinicie.
14. Realice el cableado Ethernet hacia los puertos de gestión del controlador.
15. Añada una nueva entrada del subsistema de almacenamiento en la ventana Gestión empresarial utilizando las nuevas direcciones IP asignadas.

Asignación de direcciones TCP/IP estáticas utilizando la interfaz de servicio del puerto serie del controlador del subsistema de almacenamiento

Nota : Para gestionar subsistemas de almacenamiento por medio de un cortafuegos, configure el cortafuegos para que abra el puerto 2463 a los datos TCP.

Para completar este procedimiento debe disponer de los componentes siguientes:

- Un cable de módem nulo con conectores hembra DB-9 en ambos extremos, utilizado para conectar el puerto serie del host al puerto serie del controlador.

- Una aplicación de software de emulación de terminal, tales como Procomm o Microsoft Windows Hyperterm, instalada en el sistema host.

Nota:

1. La configuración de la sesión de terminal debe tener los siguientes valores: 38400 baudios, 8 bits de datos, 1 bit de parada, sin paridad.
 2. Si el ajuste de velocidad en baudios del controlador es distinto al del termina, envíe un carácter de "interrupción" para hacer que el controlador cambie al siguiente ajuste de velocidad en baudios disponible. Repita el envío del carácter de "interrupción" hasta que se muestre el mensaje "Pulse espacio para definir la velocidad en baudios".
- Controlador de versión de firmware 7.77.xx.xx o superior y sus archivos NVSRAM asociados instalados.

Siga los pasos siguientes para ver y asignar una nueva dirección IP al puerto de gestión del controlador:

1. Pulse **Intro**. Si se muestra este carácter (->), escriba **Exit** y pulse **Intro**. De lo contrario, continúe con el siguiente paso.
2. En la sesión de emulador de terminal, envíe el carácter de "interrupción". Por ejemplo, utilice **CNTL+BREAK** para Microsoft Windows Hyperterm o **ALT+B** para Procomm.
3. Introduzca la letra mayúscula **S** y pulse **Intro** cuando se muestre el siguiente mensaje: Pulse durante 5 segundos: para <S> Interfaz de servicio, <BREAK> para velocidad en baudios.
4. Introduzca la contraseña **DSSStorage** (diferencia entre mayúsculas y minúsculas) en los 60 segundos posteriores a la visualización de este mensaje: Introduzca la contraseña para acceder a la interfaz de servicio (tiempo de espera 60 segundos).

Nota: Si el controlador no cuenta con la versión de firmware 7.77.xx.xx o superior y sus archivos NVSRAM asociados instalados, esta contraseña no será aceptada, y deberá seguir uno de los dos métodos para cambiar la configuración IP de los puertos Ethernet del controlador. Consulte el apartado "Asignación de direcciones TCP/IP estáticas a un subsistema de almacenamiento utilizando la dirección TCP/IP de puerto de gestión predeterminada de fábrica" en la página 11 y "Asignación de direcciones TCP/IP estáticas a subsistemas de almacenamiento utilizando una conexión de gestión dentro de banda" en la página 11 para obtener más información.

5. Escriba 1 o 2 para visualizar o cambiar la configuración IP cuando se muestre el siguiente menú:

Menú principal de interfaz de servicio =====

- 1) Mostrar configuración IP
- 2) Cambiar configuración IP
- 3) Restablecer contraseña de administrador de matriz de almacenamiento Q) Salir del menú

Si elige la opción 2, siga la solicitud para definir la configuración IP del puerto seleccionado. Es necesario reiniciar el controlador para que los cambios surtan efecto.

Nota: Debe seguir estos pasos en ambos controladores.

Capítulo 2. Interfaz de Storage Manager

Describe el diseño básico del software Storage Manager, donde la versión de Storage Manager es 10.84.xx.xx y la versión de firmware del controlador es 7.84.xx.xx.

En este capítulo se describe el diseño básico del software Storage Manager en un subsistema en el que la versión de Storage Manager es 10.84.xx.xx y la versión de firmware del controlador es 7.84.xx.xx.

Storage Manager tiene dos ventanas que proporcionan funcionalidades de gestión y una representación gráfica de sus subsistemas de almacenamiento: la ventana Gestión empresarial y la ventana Gestión del subsistema.

Utilice la ventana Gestión empresarial para añadir los subsistemas de almacenamiento que desee gestionar y supervisar. A través de la ventana Gestión empresarial, recibe notificaciones de alerta de errores críticos que afectan a los subsistemas de almacenamiento. Si se le notifica en la ventana Gestión empresarial que un subsistema de almacenamiento no tiene estado óptimo, puede abrir la ventana Gestión del subsistema para el subsistema de almacenamiento afectado para ver información detallada sobre las condiciones del mismo.

Importante: Dependiendo de su versión de Storage Manager y del firmware del controlador, las vistas, opciones de menú y funcionalidades pueden diferir de la información presentada en este documento. Para obtener información sobre la funcionalidad disponible, consulte los temas de ayuda en línea de Storage Manager.

Ventana Gestión empresarial

Lista las tareas que puede llevar a cabo con la ventana Gestión empresarial.

La ventana Gestión empresarial es la primera ventana que se abre al iniciar Storage Manager. Utilice la ventana Gestión empresarial para completar las siguientes tareas de gestión:

- Descubrir hosts y subsistemas de almacenamiento dentro y fuera de banda automáticamente en su subred local
- Añadir y eliminar manualmente hosts y subsistemas de almacenamiento
- Supervisar el estado de los subsistemas de almacenamiento e informar sobre el estado de alto nivel con el icono aplicable
- Configurar notificaciones de alerta por correo electrónico o protocolo simple de gestión de red (SNMP) e informar sobre eventos críticos en los destinos de alerta configurados

Nota: Un archivo de configuración local almacena toda la información sobre los subsistemas de almacenamiento añadidos y destinos de correo electrónico o SNMP configurados.

- Abrir la ventana Gestión del subsistema aplicable para un subsistema de almacenamiento seleccionado para realizar operaciones de gestión y configuración detalladas

- Ejecutar scripts para realizar tareas de gestión básicas en un subsistema de almacenamiento concreto

Nota: Por ejemplo, podría ejecutar scripts para crear unidades lógicas nuevas o descargar firmware de controlador nuevo. Para obtener más información sobre la ejecución de scripts, consulte la *IBM System Storage DS Storage Manager Command Line Interface and Script Commands Programming Guide* o los temas de ayuda en línea de la ventana Gestión empresarial.

- Planificar el guardado o guardar automáticamente una copia de los datos de soporte cuando el proceso de supervisión del cliente detecta un evento crítico.
- Actualizar el firmware de controlador entre las principales versiones de firmware de controlador (por ejemplo, actualizar el firmware de controlador de la versión 6.xx.xx.xx a la versión 7.xx.xx.xx). Esta funcionalidad es igual que la de la herramienta de actualización independiente IBM System Storage Controller Firmware. Esta herramienta está integrada en el cliente IBM DS Storage Manager versión 10.50.xx.xx y posteriores.
- Planificar la recopilación de toda la información de soporte en uno o todos los subsistemas de almacenamiento a intervalos definidos.
- Recuperar inventario de firmware de todos los subsistemas de almacenamiento.

Para mostrar y ocultar las barras Herramienta y Estado, seleccione Vista en el menú y seleccione o desmarque las opciones Herramienta o Estado.

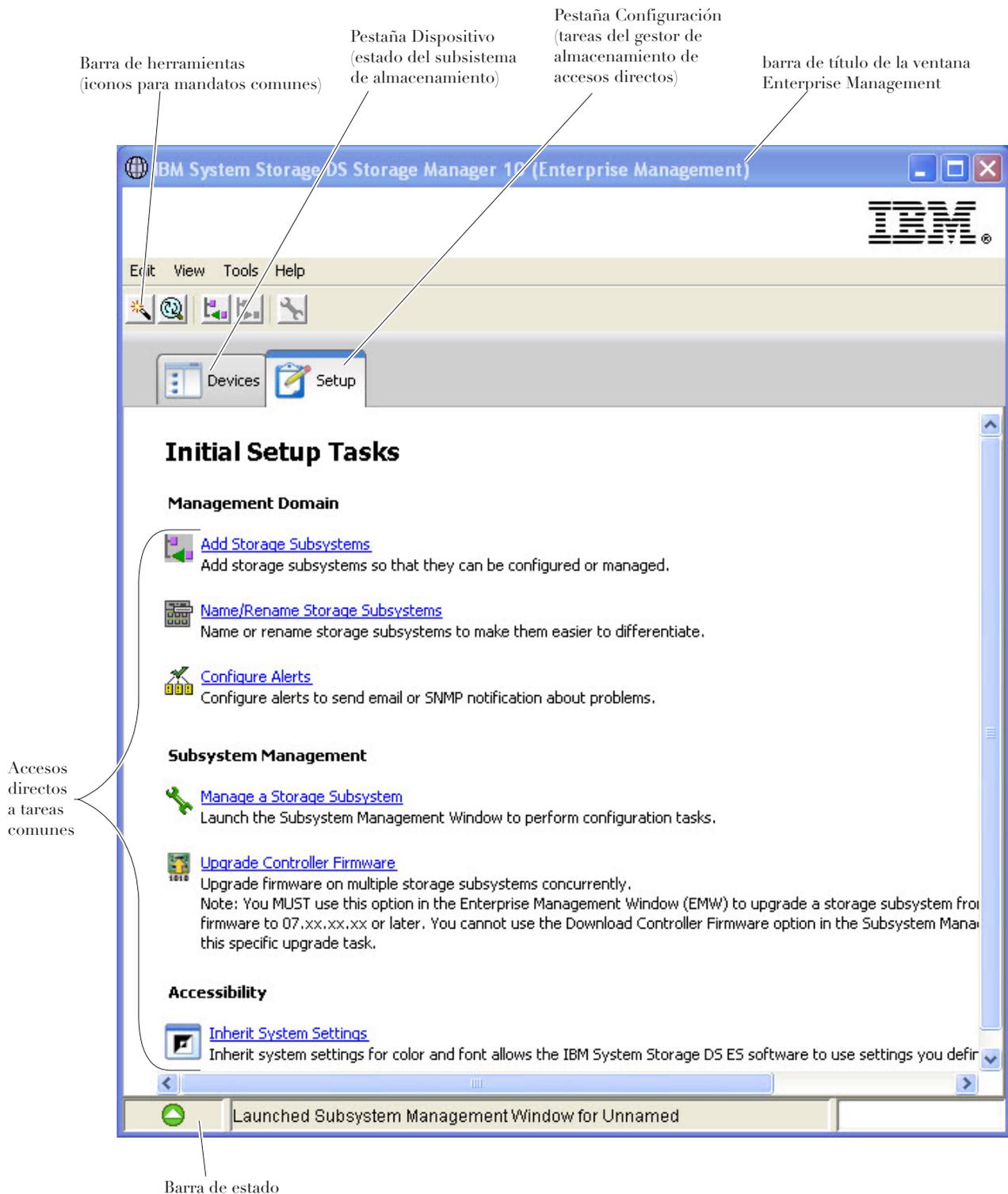


Figura 2. Partes de la ventana Gestión empresarial

Uso de la pestaña Dispositivos

Describe las dos vistas: vista de árbol y vista de tabla de la pestaña Dispositivos en la ventana Enterprise Management y las tareas que puede llevar a cabo en cada vista.

La pestaña **Dispositivos** de la ventana Gestión empresarial presenta dos vistas de los subsistemas de almacenamiento gestionados por la estación de gestión: una vista de árbol y una vista de tabla.

Vista de árbol

La vista de árbol proporciona una vista jerárquica de los nodos del subsistema de almacenamiento. La vista de árbol muestra dos tipos de nodos:

- Subsistemas de almacenamiento descubiertos
- Subsistemas de almacenamiento sin identificar

El nodo Subsistemas de almacenamiento descubiertos y el nodo Subsistemas de almacenamiento sin identificar son nodos hijo del nodo Estación de gestión.

El nodo Subsistemas de almacenamiento descubiertos tiene sus propios nodos hijo que representan los subsistemas de almacenamiento gestionados actualmente por la estación de gestión. Cada subsistema de almacenamiento se etiqueta con su nombre de máquina y siempre está presente en la vista de árbol. Cuando se añaden subsistemas de almacenamiento y hosts con subsistemas de almacenamiento asociados a la ventana Gestión empresarial, los subsistemas de almacenamiento pasan a ser nodos hijo del nodo Subsistemas de almacenamiento descubiertos.

Nota: Si mueve el ratón sobre el nodo Subsistemas de almacenamiento descubiertos, aparecerá una ayuda contextual indicando la dirección IP del controlador.

El nodo Subsistemas de almacenamiento sin identificar muestra los subsistemas de almacenamiento a los que la estación de gestión no puede acceder debido a problemas de conexión de la red, a que el subsistema está apagado o a que un nombre no existe.

En los nodos de la vista de árbol puede llevar a cabo las siguientes acciones:

- Pulse dos veces en el nodo Subsistemas de almacenamiento descubiertos y el nodo Subsistemas de almacenamiento sin identificar para expandir o contraer la vista de nodos hijo.
- Pulse dos veces en el nodo del subsistema de almacenamiento para lanzar la ventana Gestión del subsistema para ese subsistema de almacenamiento.
- Pulse con el botón derecho en el nodo Subsistemas de almacenamiento descubiertos para abrir un menú que contiene las acciones aplicables para ese nodo.

El menú del botón derecho del nodo Subsistemas de almacenamiento descubiertos contiene estas opciones:

- **Añadir subsistema de almacenamiento**
- **Descubrimiento automático**
- **Renovar**
- **Recopilar datos de soporte**

- automáticamente
- crear/editar planificación

El menú del botón derecho de los nodos de subsistemas de almacenamiento contiene estas opciones:

- Gestionar subsistema de almacenamiento
- Ubicar subsistema de almacenamiento
- Ejecutar script
- Cargar configuración de subsistema de almacenamiento
- Actualizar firmware de controlador
- Renovar
- Eliminar subsistema de almacenamiento
- Eliminar conexión de gestión
- Configurar alertas
- Recopilar datos de soporte automáticamente
- Crear/Editar planificación de recopilación de datos de soporte
- Renombrar subsistema de almacenamiento
- Comentario

Estas opciones también se incluyen entre otras opciones del menú **Editar** y **Herramientas**. Para obtener más información, consulte el tema de la ayuda en línea *Uso de la ventana Gestión empresarial*.

Vista de tabla

En la vista de tabla, cada subsistema de almacenamiento es una fila de la tabla. Las columnas de la vista de tabla muestran datos sobre el subsistema de almacenamiento gestionado.

Tabla 1. Datos mostrados en la vista de tabla

Columna	Descripción
Nombre	El nombre del subsistema de almacenamiento gestionado Nota: Si no se nombra el subsistema de almacenamiento gestionado, el nombre predeterminado será Unnamed.
Tipo	El tipo del subsistema de almacenamiento gestionado, representado por un icono
Estado	Icono y etiqueta de texto que informan sobre el estado verdadero del subsistema de almacenamiento gestionado
Conexiones de gestión	Son posibles los siguientes tipos de conexión: <ul style="list-style-type: none"> • Fuera de banda: este subsistema de almacenamiento es un subsistema de almacenamiento fuera de banda. • Dentro de banda: este subsistema de almacenamiento es un subsistema de almacenamiento dentro de banda gestionado a través de un host individual. • Fuera de banda, Dentro de banda: este subsistema de almacenamiento es un subsistema de almacenamiento tanto dentro como fuera de banda. Pulse Detalles para ver más información sobre cualquiera de estas conexiones.

Tabla 1. Datos mostrados en la vista de tabla (continuación)

Columna	Descripción
Comentario	Cualquier comentario que haya incluido sobre el subsistema de almacenamiento gestionado específico

Ordene las filas de la vista de tabla en orden ascendente o descendente pulsando la cabecera de una columna o seleccionando una de estas opciones de menú:

- **Ver > Por nombre**
- **Ver > Por estado**
- **Ver > Por conexión de gestión**
- **Ver > Por comentario**

Para cambiar el modo en que aparecen los subsistemas de almacenamiento gestionados en la vista de tabla, complete una de las acciones siguientes:

- Para mostrar todos los subsistemas de almacenamiento gestionados conocidos en la vista de tabla, seleccione el nodo Estación de gestión.
- Para mostrar solo el subsistema de almacenamiento en la vista de tabla, seleccione un nodo de subsistema de almacenamiento en la vista de árbol.

Nota: Si selecciona un nodo Sin identificar en la vista de árbol se mostrará una vista de tabla vacía.

Visualización de subsistemas gestionados en la vista de tabla

Para cambiar el modo en que aparecen los subsistemas de almacenamiento gestionados en la vista de tabla.

- Para mostrar todos los subsistemas de almacenamiento gestionados conocidos en la vista de tabla, seleccione el nodo Storage Manager.
- Seleccione un nodo de Subsistemas de almacenamiento descubiertos o Subsistemas de almacenamiento no descubiertos en la vista de árbol para mostrar todos los subsistemas de almacenamiento asociados a ese host específico en la vista de tabla.

Nota: Si no ha añadido ningún subsistema de almacenamiento, la vista de tabla estará vacía.

- Para mostrar solo el subsistema de almacenamiento en la vista de tabla, seleccione un nodo de subsistema de almacenamiento en la vista de árbol.

Nota: Si selecciona un nodo Sin identificar en la vista de árbol se mostrará una vista de tabla vacía.

Adición y eliminación de un subsistema de almacenamiento

Para añadir un subsistema de almacenamiento, en Storage Manager realicé una de las opciones siguientes.

Tabla 2. Adición de un subsistema de almacenamiento

Ubicación	Procedimiento
Vista de árbol	Pulse con el botón derecho en el nodo raíz de la vista de árbol y seleccione Añadir subsistema de almacenamiento en el menú emergente

Tabla 2. Adición de un subsistema de almacenamiento (continuación)

Ubicación	Procedimiento
Barra de herramientas	Pulse en el icono para añadir el subsistema de almacenamiento
Menú Editar	Seleccione Editar>Añadir subsistema de almacenamiento
Pestaña Configuración	Seleccione Añadir subsistema de almacenamiento

Para eliminar un subsistema de almacenamiento, en Storage Manager realicé una de las opciones siguientes. La eliminación de un subsistema solo elimina el icono, no el propio subsistema. Puede seleccionar más de un subsistema a la vez.

Tabla 3. Eliminación de subsistemas de almacenamiento

Ubicación	Procedimiento
Vista de árbol	Pulse con el botón derecho en el subsistema de almacenamiento que desea eliminar de la vista de árbol y seleccione Eliminar > Subsistema de almacenamiento en el menú emergente
Barra de herramientas	Seleccione el subsistema de almacenamiento que desea eliminar de la vista de árbol o tabla y pulse en el icono para eliminar el mismo
Menú Editar	Seleccione el subsistema de almacenamiento que desea eliminar de la vista de árbol o tabla y seleccione Editar > Eliminar > Subsistema de almacenamiento

Eliminación simultánea de varios subsistemas de almacenamiento

Si gestiona diversos subsistemas de almacenamiento puede eliminar dos o más subsistemas de almacenamiento continuos o discontinuos a la vez utilizando la vista de tabla.

Nota: Solo eliminará el icono de la vista de árbol o tabla, no los subsistemas de almacenamiento.

Tabla 4. Eliminación simultánea de varios subsistemas

Ubicación	Procedimiento
Vista de árbol	Pulse el nodo Subsistemas de almacenamiento descubiertos para mostrar los subsistemas de almacenamiento que gestiona

Tabla 4. Eliminación simultánea de varios subsistemas (continuación)

Ubicación	Procedimiento
Vista de tabla	<p>Para eliminar subsistemas de almacenamiento continuos, pulse el primer subsistema de almacenamiento que desee eliminar. Mantenga pulsada la tecla Mayús. y pulse el último subsistema de almacenamiento que desee eliminar. Con los subsistemas de almacenamiento seleccionados resaltados en la vista de tabla, pulse con el botón derecho y seleccione Eliminar en el menú emergente. Para eliminar subsistemas de almacenamiento discontinuos, mantenga pulsada la tecla Control y pulse los subsistemas de almacenamiento que desee eliminar. Con los subsistemas de almacenamiento seleccionados resaltados en la vista de tabla, pulse con el botón derecho y seleccione Eliminar en el menú emergente.</p>

Uso de la pestaña Configuración

Describe la pestaña Configuración en la ventana Gestión empresarial y las tareas que puede llevar a cabo.

La pestaña **Configuración** de la ventana Gestión empresarial es una pasarela a las tareas que puede llevar a cabo al configurar un subsistema de almacenamiento. Utilice la pestaña Configuración de la ventana Gestión empresarial para completar las siguientes tareas:

- Añadir un subsistema de almacenamiento
- Nombrar o renombrar un subsistema de almacenamiento
- Configurar una alerta
- Abrir la ventana Gestión del subsistema para gestionar un subsistema de almacenamiento
- Actualizar el firmware de controlador
- Abrir la ventana Heredad configuración de sistemas

Ventana Gestión del subsistema

Describe cómo se lanza la ventana Gestión de subsistema y las tareas que puede realizar con esa ventana.

La ventana Gestión del subsistema es software basado en tecnología Java que se inicia desde la ventana Gestión empresarial. Cada ventana Gestión del subsistema proporciona funciones de gestión para un subsistema de almacenamiento concreto. Puede tener más de una ventana Gestión del subsistema abierta para gestionar diferentes subsistemas de almacenamiento. La ventana Gestión del subsistema permite realizar las siguientes funciones:

- Acceder a opciones del subsistema de almacenamiento, como ubicar un subsistema de almacenamiento, configurar un subsistema de almacenamiento, renombrar un subsistema de almacenamiento o cambiar una contraseña
- Configurar agrupaciones de discos o matrices y unidades lógicas estándar o ligeras desde su capacidad de subsistema de almacenamiento, definir hosts o

- grupos de host y conceder acceso a hosts o grupos de hosts a conjuntos de unidades lógicas estándar o ligeras denominadas particiones de almacenamiento
- Supervisar el estado de los componentes del subsistema de almacenamiento e informar sobre un estado detallado utilizando los iconos aplicables
 - Acceder a los procedimientos de recuperación aplicables para un componente lógico o componente de hardware que haya fallado
 - Ver el registro de eventos del subsistema de almacenamiento
 - Ver información de perfil sobre componentes de hardware, como controladores y unidades, y obtener una visión física de las unidades de los alojamientos de hardware
 - Acceder a opciones de gestión de controlador, como el cambio de propiedad de unidades lógicas o el establecimiento en línea o fuera de línea de un controlador
 - Acceder a opciones de gestión de unidades, como la asignación de repuestos en caliente y la ubicación de las unidades
 - Supervisar el rendimiento del subsistema de almacenamiento
 - Configurar servicios de copia como Enhanced Flashcopy, Flashcopy, VolumeCopy y Duplicación remota

Si el subsistema de almacenamiento tiene firmware de controlador versión 7.70.xx.xx, su ventana Gestión del subsistema no se podrá abrir a menos que se facilite una contraseña segura. Las contraseñas seguras deben contener entre 8 y 30 caracteres y estar formadas al menos por un número, una letra minúscula, una letra mayúscula y un carácter no alfanuméricos (por ejemplo, < > ! @ + #). No se permiten espacios y se diferencia entre mayúsculas y minúsculas.

En los subsistemas de almacenamiento con firmware de controlador distinto a la versión 7.70.xx.xx, se le pedirá esta contraseña si no se ha especificado ninguna para el subsistema de almacenamiento cuando intente abrir la ventana Gestión del subsistema para el mismo. IBM recomienda crear una contraseña de gestión del subsistema para evitar cambios no autorizados en la configuración de Gestión del subsistema.

Apertura de la ventana Gestión del subsistema

Lista los cuatro métodos para abrir la ventana Gestión de subsistema

Para abrir la ventana gestión del subsistema desde la ventana Gestión empresarial, realice una de las acciones siguientes:

- Pulse la pestaña **Dispositivos** y pulse dos veces en el nombre del subsistema de almacenamiento que desea gestionar.
- Pulse la pestaña **Dispositivos**, pulse con el botón derecho en el nombre del subsistema de almacenamiento que desea gestionar y seleccione **Gestionar subsistema de almacenamiento**.
- Pulse la pestaña **Dispositivos** y seleccione **Herramientas > Gestionar subsistema de almacenamiento**.
- Pulse la pestaña **Configuración** y seleccione **Gestionar subsistema de almacenamiento**. En la ventana Seleccionar subsistema de almacenamiento, seleccione el nombre del subsistema de almacenamiento que desea gestionar y pulse **Aceptar**.

Dentro de la ventana Gestión del subsistema solo puede gestionar un subsistema de almacenamiento. No obstante, puede abrir más de una ventana Gestión del subsistema desde la ventana Gestión empresarial para gestionar diversos subsistemas de almacenamiento a la vez.

La ventana Gestión del subsistema le proporciona las siguientes opciones para gestionar su subsistema de almacenamiento.

El diseño de la pantalla y las opciones de menú de la ventana Gestión del subsistema han cambiado en IBM System Storage DS Storage Manager versión 10.83 y posteriores, así como en el firmware de controlador 7.83.xx.xx y posteriores. Todas las funciones de gestión del subsistema implementadas en las versiones anteriores siguen siendo válidas. Sin embargo, las opciones de menú pueden ser diferente. Explore el software y consulte la ayuda en línea para familiarizarse.

Uso de la pestaña Resumen

Hace una lista de la información que puede ver en la pestaña resumen de la ventana Gestión del subsistema.

La pestaña **Resumen** de la ventana Gestión del subsistema muestra información sobre el subsistema de almacenamiento. La pestaña Resumen también incluye enlaces a la ventana Perfil del subsistema de almacenamiento, temas de ayuda en línea relevantes y al tutorial sobre conceptos de almacenamiento. También se muestra el enlace a Recovery Guru cuando el subsistema de almacenamiento requiere atención.

En la pestaña Resumen puede ver la siguiente información:

- Estado del subsistema de almacenamiento
- Información sobre la versión del software IBM DS Storage Manager y el firmware del controlador
- Capacidad del subsistema de almacenamiento
- Agrupaciones de discos y matrices, unidades lógicas y configuraciones de servicios de copia como FlashCopy, VolumeCopy y la duplicación remota mejorada del subsistema de almacenamiento
- Hosts, correlaciones y particiones de almacenamiento del subsistema de almacenamiento
- Número de características premium disponibles, activas, habilitadas o deshabilitadas de su subsistema de almacenamiento
- Componentes de hardware del subsistema de almacenamiento
- Documentación online disponible para obtener información sobre su subsistema de almacenamiento

Uso de la pestaña Almacenamiento y servicios de copia

Informa sobre la vista de árbol de los nodos lógicos que proporciona la pestaña Storage & Copy Services.

La pestaña **Almacenamiento y servicios de copia** proporciona una vista de árbol estructurado de los nodos lógicos. Pulse el signo (+) o menos (-) situado junto a los nodos para expandir o contraer la vista. Pulse con el botón derecho en un nodo para abrir un menú que contiene las acciones aplicables para ese nodo.

Nodos de la pestaña Lógica

El subsistema de almacenamiento, o nodo raíz, tiene los tipos de nodo hijo indicados en la tabla siguiente.

Tabla 5. Nodos de la pestaña Lógica

Nodos hijo del nodo raíz	Descripción de los nodos hijo
Todos los objetos lógicos	Este nodo le permite ver información sobre todos los objetos lógicos que componen su subsistema de almacenamiento. Utilice el menú desplegable Tipo de objeto del panel Ver para seleccionar un tipo de objeto concreto. Se trata de una forma útil de ver información sobre el estado y capacidad de una agrupación de discos o matriz, o ver todas las unidades lógicas de repositorio asociadas o no asociadas con una unidad lógica de base con las características premium Imagen de FlashCopy, Imagen de FlashCopy mejorada y Grupo de consistencia.
Capacidad total sin configurar	Este nodo representa la suma de la capacidad de todas las unidades sin asignar que no están en una agrupación de de discos o matriz.
Capacidad sin configurar	Este nodo representa la capacidad del subsistema de almacenamiento que no está configurada en una matriz. Si su subsistema de almacenamiento contiene unidades con diferentes tipos de soporte (unidades de disco duro o unidades de estado sólido) y diferentes tipos de interfaz, aparecerán diversos nodos sin configurar. Cada tipo de unidad tiene un nodo Capacidad sin configurar asociado que se muestra bajo el nodo Capacidad total sin configurar si existen unidades sin asignar disponibles en un alojamiento de unidad.

Tabla 5. Nodos de la pestaña Lógica (continuación)

Nodos hijo del nodo raíz	Descripción de los nodos hijo
Agrupaciones de discos	<p>IBM Storage Manager muestra un nodo Agrupaciones de discos si se han configurado una o varias agrupaciones de discos para su subsistema de almacenamiento. Expanda el nodo Agrupaciones de discos para ver las agrupaciones de discos individuales. Si se ha habilitado la característica premium Flashcopy, puede tener nodos hijos de imágenes FlashCopy. El nodo Agrupación de discos tiene varios tipos de nodo hijo.</p> <ul style="list-style-type: none"> • Unidad lógica — Este nodo representa una unidad lógica configurada y definida (unidad lógica estándar o ligera). En un nodo Agrupaciones de discos pueden existir diversos nodos Unidad lógica. • Capacidad libre — Este nodo representa una región de capacidad que puede utilizar para crear una o varias unidades lógicas en la agrupación de discos. En cada nodo Agrupación de discos puede existir un nodo Capacidad libre. • Imágenes de Flashcopy mejorado — Este nodo representa una imagen lógica puntual de una unidad lógica de base seleccionada. Una unidad lógica de base es una unidad lógica estándar o ligera origen de una imagen de FlashCopy mejorada. • Grupos de Flashcopy mejorado — Este nodo representa la secuencia de imágenes de FlashCopy mejorado de la misma unidad lógica de base. • Unidades lógicas de Flashcopy mejorado — Este nodo indica que ha creado una vista de una imagen de FlashCopy mejorado. Las unidades lógicas de FlashCopy mejorado se crean para permitir a un host acceder a una imagen de FlashCopy mejorado como si se tratase de una unidad lógica. • Unidades lógicas primarias y secundarias — Este nodo indica si la unidad lógica del par de unidades lógicas de duplicación remota mejorada es primaria o secundaria.

Tabla 5. Nodos de la pestaña Lógica (continuación)

Nodos hijo del nodo raíz	Descripción de los nodos hijo
Matrices	<p>El nodo Unidad lógica y el nodo Capacidad libre son nodos hijo estándar. Si se ha habilitado la característica premium Imagen de Flashcopy mejorado, puede tener nodos hijos Imágenes de FlashCopy mejorado.</p> <ul style="list-style-type: none"> • Unidad lógica — Este nodo representa una unidad lógica configurada y definida. Una matriz soporta solo unidades lógicas estándar. En un nodo Matriz pueden existir diversos nodos Unidad lógica. • Capacidad libre — Este nodo representa una región de capacidad que puede utilizar para crear una o varias unidades lógicas en la matriz. En un nodo Matriz pueden existir diversos nodos Capacidad libre. • Imágenes de Flashcopy mejorado — Este nodo representa una imagen lógica puntual de una unidad lógica de base seleccionada. Una unidad lógica de base es una unidad lógica estándar o ligera origen de una imagen de FlashCopy mejorada. • Grupos de Flashcopy mejorado — Este nodo representa la secuencia de imágenes de FlashCopy mejorado de la misma unidad lógica de base. • Unidades lógicas de Flashcopy mejorado — Este nodo representa las imágenes de FlashCopy mejorado de unidades lógicas de base visibles para un host. • Unidades lógicas primarias y secundarias — Este nodo indica si la unidad lógica del par de unidades lógicas de duplicación remota mejorada es primaria o secundaria. • Unidad lógica de Flashcopy — Se trata de nodos hijo de sus unidades lógicas de base asociadas.
Grupos de consistencia	<p>Si se ha habilitado la característica premium Flashcopy mejorado, puede tener los siguientes nodos hijo Grupo de consistencia:</p> <ul style="list-style-type: none"> • Grupo de consistencia — Este nodo representa un nodo de agrupación que incluye todos los nodos hijo creados para este grupo de consistencia. Expandir este nodo para ver los nodos hijo. • Imágenes de Flashcopy mejorado — Este nodo representa una colección de imágenes lógicas puntuales de las unidades lógicas que pertenecen a un grupo de consistencia. • Unidades lógicas miembro — Este nodo es una colección de las unidades lógicas que pertenecen a este grupo de consistencia. • Unidades lógicas de Flashcopy mejorado — Este nodo representa las imágenes de FlashCopy mejorado de unidades lógicas miembro visibles para un host.
Grupos de duplicación global mejorada	<p>Se trata de unidades lógicas especiales del subsistema de almacenamiento creadas como recurso para los controladores de los subsistemas de almacenamiento local y subsistemas de almacenamiento remoto. El controlador almacena información duplicada en la unidad lógica de repositorio de duplicaciones, incluyendo información sobre las escrituras remotas que aún no se han grabado en las unidades lógicas secundarias.</p>

Uso de la pestaña Correlaciones de host

Informa sobre los dos paneles: el panel de Correlaciones de host y el panel de Correlaciones definidas en la pestaña Correlaciones en la ventana de Gestión del subsistema.

La pestaña **Correlaciones** de la ventana Gestión del subsistema tiene dos paneles: el panel Correlaciones de host y el panel Correlaciones definidas.

Panel Correlaciones de host

El panel Correlaciones de host muestra una vista de árbol estructurado de los nodos lógicos relacionados con las particiones de almacenamiento. Pulse el signo (+) o menos (-) situado junto a los nodos para expandir o contraer la vista. Puede pulsar con el botón derecho en un nodo para abrir un menú emergente que contiene las acciones aplicables para ese nodo.

El subsistema de almacenamiento, o nodo raíz, tiene estos tipos de nodo hijo.

Tabla 6. Tipos de nodos en el panel Topología

Nodos hijo del nodo raíz	Descripción de los nodos hijo
Correlaciones sin definir	El nodo Correlaciones sin definir tiene un tipo de nodo hijo: <ul style="list-style-type: none">• Correlación sin definir individual: Representa una unidad lógica con una correlación sin definir. En un nodo Correlaciones sin definir pueden existir diversos nodos Unidad lógica.
Grupo predeterminado	<p>Nota: Si la característica premium Partición del almacenamiento de Storage Manager está inhabilitada, todas las unidades lógicas creadas están en el Grupo predeterminado.</p> El nodo Grupo predeterminado tiene dos tipos de nodo hijo: <ul style="list-style-type: none">• Grupo de host: Se indican los grupos de host definidos que no participan en una correlación específica. Este nodo puede tener nodos hijo de host, que pueden tener nodos de puerto de host hijo.• Host: Se indican los grupos de host definidos que no forman parte de un grupo de host específico pero sí del Grupo predeterminado y no participan en una correlación específica. Este nodo puede tener nodos de puerto de host hijo.
Identificador de puerto de host sin asociar	Un nodo Identificador de puerto de host sin asociar tiene un tipo de nodo hijo. <ul style="list-style-type: none">• Identificador de puerto de host – Identificador de puerto de host que se ha asociado con ningún host.
Grupo de host	Un nodo Grupo de host tiene un tipo de nodo hijo. <ul style="list-style-type: none">• Host – Se indican los host definidos que pertenecen a este grupo de host definido. Este nodo puede tener nodos de puerto de host hijo. <p>Nota: Los nodos hijo de este grupo de host también pueden participar en correlaciones específicas con el host individual en vez de con el grupo de host.</p>

Tabla 6. Tipos de nodos en el panel Topología (continuación)

Nodos hijo del nodo raíz	Descripción de los nodos hijo
Host	Un nodo Host tiene un tipo de nodo hijo: <ul style="list-style-type: none"> • Puertos de host: Este nodo tiene nodos hijo que representan todos los puertos de host o puertos individuales de un adaptador de host asociados con este host.

El icono **Partición de almacenamiento**, cuando está presente en el panel Correlaciones de host, indica que se ha definido una partición de almacenamiento para un grupo de host o host. Este icono también aparece en la barra de estado si se ha habilitado esta función.

Panel Correlaciones definidas

El panel Correlaciones definidas muestra las correlaciones asociadas con un nodo seleccionado en el panel Topología.

Tabla 7. Información de nodo del panel Correlaciones definidas

Nombre de columna	Descripción
Nombre de unidad lógica	El nombre de unidad lógica proporcionado por el usuario. La unidad lógica de acceso configurada de fábrica también aparece en esta columna. Nota: Para que un subsistema de almacenamiento con una conexión dentro de banda habilite IBM Storage Manager para comunicarse con el mismo, se necesita una correlación de unidad lógica de acceso. Para subsistemas de almacenamiento con conexiones fuera de banda, puede eliminar la correlación de unidad lógica de acceso.
Accesible por	El Grupo predeterminado, grupo de host definido o host definido al que se ha concedido acceso a la unidad lógica en la correlación.
LUN	El LUN asignado a la unidad lógica específica que el host o hosts utilizan para acceder a dicha unidad lógica.
Capacidad de unidad lógica	La capacidad de la unidad lógica en unidades de GB.
Tipo	El tipo de la unidad lógica, por ejemplo unidad lógica estándar o unidad lógica FlashCopy.

Puede pulsar con el botón derecho en el nombre de una unidad lógica en el panel Correlaciones definidas para abrir un menú. El menú contiene opciones para cambiar y eliminar las correlaciones.

Uso de la pestaña Hardware

Informa sobre el panel de diseño de Hardware y el panel de propiedades en la pestaña Hardware de la ventana de Gestión del subsistema.

La pestaña **Hardware** dispone de dos paneles: el panel Diseño de hardware o Ubicación de hardware en la izquierda y el panel Propiedades en la derecha. El panel Ubicación de hardware proporciona una vista de los componentes de hardware de un subsistema de almacenamiento, incluyendo su estado.

El panel Ubicación de hardware proporciona información para el componente de hardware seleccionado en el panel Hardware. La información del panel Propiedades es específica de cada componente de hardware. Si selecciona un icono de controlador en el panel Hardware, en el panel Propiedades se mostrará una lista de propiedades de este controlador. Si selecciona un icono de unidad en el panel Hardware, en el panel Propiedades se mostrará una lista de propiedades de esa unidad.

Ver

El comando de **Visualización de componentes de alojamiento** de cada alojamiento muestra el estado de los componentes secundarios del alojamiento, por ejemplo las fuentes de alimentación, los ventiladores y los sensores de temperatura. Puede seleccionar **Tipo de unidad** y pulsar **Mostrar** en el panel Ubicación de hardware para identificar unidades de un tipo, velocidad y capacidad concretos. Se mostrará un triángulo verde en las unidades relevantes.

Uso de la pestaña Configuración

Hace una lista de los enlaces y las tareas que puede llevar a cabo en la pestaña configuración de la ventana de Gestión del subsistema.

La pestaña **Configuración** de la ventana Gestión del subsistema proporciona enlaces a las siguientes tareas:

- Ubicar subsistema de almacenamiento
- Renombrar subsistema de almacenamiento
- Cambiar el orden de vista del hardware
- Establecer una contraseña del subsistema de almacenamiento
- Gestionar características Premium
- Crear almacenamiento
- Guardar configuración

Tareas opcionales:

- Definir hosts manualmente
- Correlacionar unidades lógicas
- Configurar Puertos de gestión Ethernet

Pulse en un enlace para abrir la ventana correspondiente.

Gestión de múltiples versiones de software

Explica cómo se selecciona de forma automática la versión de Storage Manager para su uso en caso de que la versión de firmware en varios subsistemas de almacenamiento sea diferente.

Cuando abre la ventana Gestión del subsistema para gestionar un subsistema de almacenamiento, se abre la versión del software Storage Manager aplicable a la versión de firmware. Por ejemplo, puede gestionar dos subsistemas de almacenamiento que utilicen el software Storage Manager; un subsistema de almacenamiento con la versión de firmware 6.14 y el otro con la versión de firmware 7.5x. Al abrir la ventana Gestión del subsistema para uno de los subsistemas de almacenamiento, se utiliza la versión correcta. El subsistema de almacenamiento con versión de firmware 6.14 utiliza la versión 9.14 del software Storage Manager, y el subsistema de almacenamiento con versión de firmware 7.5x

utiliza la versión 10.5x del software Storage Manager. Puede comprobar la versión que utiliza actualmente pulsando **Ayuda > Acerca de** en la ventana Gestión del subsistema.

Nota: Si gestiona diversos subsistemas y estos tienen versiones de firmware de controlador diferentes, las ventanas Gestión del subsistema pueden ofrecer distintas sensaciones.

Capítulo 3. Instalación de Storage Manager

Hace una lista de los sistemas operativos de estación de gestión para Storage Manager y contiene enlaces a varias secciones relacionadas con la instalación de Storage Manager.

Este capítulo describe los requisitos y procedimientos necesarios para la instalación del software Storage Manager.

Para la instalación de Storage Manager en sistemas operativos de tipo Unix, su sistema debe tener capacidades de gráficos para utilizar el asistente de instalación. Si su sistema no tuviera capacidades de gráficos, puede utilizar el comando de shell para instalar Storage Manager sin gráficos. Consulte “Instalación de Storage Manager con una ventana de consola en Linux, AIX, HP-UX y Solaris” en la página 37 para obtener más información. También puede saltar esta sección e instalar los paquetes de software host autónomos. Consulte “Instalación manual de Storage Manager” en la página 39 y siga los procedimientos mencionados. Todos los paquetes se incluyen en el DVD de instalación. Los sistemas operativos de estación de gestión compatibles con Storage Manager son:

- AIX
- Windows 7, Windows Vista, Windows XP (Service Pack 2), Windows Server 2003, Windows Server 2008 y Windows Server 2012
- Linux: RHEL y SLES (x86, x86_64 y Linux en POWER)
- HP-UX (ediciones PA-RISC y IA64)
- Oracle Solaris (SPARC y ediciones x86)

Nota: La versión IA64 de Storage Manager no está disponible en la edición IA64 de los sistemas operativos Microsoft Windows y Linux. Si gestiona un subsistema con una versión del firmware de controlador anterior a 6.50.xx.xx, debe utilizar una versión anterior del software Storage Manager instalada en una estación de trabajo de gestión independiente.

Las instrucciones de instalación constan de las siguientes secciones:

- “Requisitos previos a la instalación”
- “Instalación de los paquetes de Storage Manager automáticamente con el asistente de instalación” en la página 34
- “Instalación manual de los paquetes de Storage Manager” en la página 38
- “Finalización de la instalación de Storage Manager” en la página 40

Para instalar Storage Manager, consulte “Desinstalación de Storage Manager” en la página 39.

Atención: Para las configuraciones en clúster, complete todos los procedimientos de configuración aplicables para cada subsistema de almacenamiento antes de instalar el software Storage Manager en un segundo host o servidor en clúster.

Requisitos previos a la instalación

Le informa sobre los requisitos de hardware, software y de configuración de la estación de gestión

Nota: Con Storage Manager versión 10.84.xx.xx o posterior, el firmware de controlador mínimo debe ser 6.50.xx.xx o posterior. Las versiones de firmware de controlador anteriores a 6.50.xx.xx no tienen soporte ni se gestionan.

La estación de gestión debe cumplir los siguientes requisitos de hardware, software y configuración:

- Velocidad de microprocesador de 2 GHz o superior.
- Mínimo 2 GB de memoria del sistema. Si se instalan otras aplicaciones en la estación de gestión, podría necesitarse memoria adicional.
- Mínimo 1,5 GB de espacio de disco libre para la herramienta y los paquetes de soporte guardados.
- La pila TCP/IP debe estar habilitada.

Instalación de los paquetes de Storage Manager automáticamente con el asistente de instalación

Describe el proceso de instalación con el asistente de instalación de Storage Manager en sistemas operativos basados en Windows y Unix.

Puede instalar el software Storage Manager automáticamente utilizando el asistente de instalación de Storage Manager, o realizar la instalación de forma manual. Esta sección describe el proceso de instalación con el asistente de instalación de Storage Manager.

Antes de instalar el software Storage Manager, lea o “Instalación de Storage Manager en Windows” o la sección “Instalación de Storage Manager en Linux, AIX, HP-UX, o Solaris” en la página 36.

Instalación de Storage Manager en Windows

Si su estación de gestión tiene un sistema operativo Windows, complete los siguientes pasos para instalar Storage Manager con el asistente de instalación:

1. Descargue los archivos del DVD de Storage Manager o del sitio web de soporte de disco de System Storage a un directorio de su sistema. La unidad predeterminada para Windows es C.
2. Pulse dos veces en el icono ejecutable del paquete de **IBM DS Storage Manager** (o SMIA).
3. Siga las instrucciones del asistente de instalación para instalar el software Storage Manager. El directorio predeterminado es

C:\Archivos de programa\IBM_DS

o bien

C:\Archivos de programa(x86)\IBM_DS

4. Cuando seleccione el tipo de instalación, podrá elegir una de las siguientes opciones:

Atención: El paquete de Storage Manager SMIA versión 10.77.xx.xx y posteriores no instalará el controlador de MPIO DSM para soportar diversas rutas en el tipo de instalación de host o en el tipo de instalación habitual cuando se instala el paquete de SMIA en la versión de servidor de sistemas operativos Microsoft Windows. Existe un paquete de SMIA diferente para instalar MPIO DSM. El instalador de Storage Manager y el de Microsoft MPIO DSM están incluidos en un solo paquete de código. Este paquete de código está disponible en el Portal de soporte de IBM.

- **Instalación habitual (completa):** Instala los paquetes del software Storage Manager necesarios para gestionar el subsistema de almacenamiento desde el host y proporcionar conectividad de E/S al subsistema de almacenamiento
 - **Estación de gestión:** Instala los paquetes necesarios para gestionar y supervisar el subsistema de almacenamiento (SMclient)
 - **Host:** Instala los paquetes necesarios para proporcionar conectividad de E/S al subsistema de almacenamiento (SMagent y SMutil)
 - **Personalizada:** Le permite seleccionar los paquetes que desea instalar.
5. Instale la unidad de MPIO DSM según sea necesario para soportar rutas múltiples pulsando dos veces en el paquete IBM DS Storage Manager MPIO DSM y siguiendo las instrucciones del asistente de instalación.

Nota: Este paso solo se aplica a Storage Manager versión 10.77.xx.xx y posteriores.

6. Pulse **Inicio > Todos los programas > Cliente DS Storage Manager 10 > Cliente Storage Manager 10** para iniciar el programa cliente Storage Manager. Añada los subsistemas de almacenamiento que desee gestionar y supervisar en la ventana Gestión empresarial del programa cliente Storage Manager.
7. Pulse con el botón derecho el subsistema y seleccione **Recopilar datos de soporte > Crear/Editar planificación**. Se abrirá la ventana **Planificar recopilación de datos de soporte**.
8. Defina una planificación/hora y especifique la ubicación en la que almacenar los datos de soporte durante la recopilación de datos de soporte de los subsistemas de almacenamiento que ha añadido.

Nota: Puede planificar días del mes (1 a 31) o días de la semana (lunes a domingo) para la recopilación de datos de soporte automática. Un subsistema solo puede tener una planificación. Puede seleccionar los subsistemas para los que desea una planificación idéntica. Los datos de soporte se guardan en la unidad local de la ubicación especificada. El nombre del informe incluye la fecha en que se generó el informe. El sistema permite un máximo de cinco informes de datos de soporte. Si se genera un informe cuando ya existen cinco, el informe más antiguo se suprime y se guarda el nuevo.

9. Seleccione **Recopilar datos de soporte > Automáticamente**. Se abrirá la ventana **Recopilación automática de datos de soporte**.

Nota: Para la Recopilación automática de datos de soporte, debe estar habilitado el servicio de control de Storage Manager.

10. Seleccione los subsistemas de los que desea un informe automático en caso de evento crítico y especifique la ubicación de su unidad local en la que desea guardarlos.

Durante la instalación, se le hará la pregunta ¿Desea iniciar automáticamente el supervisor? . Esta pregunta se refiere al servicio de Supervisor de eventos de Microsoft Windows. El Supervisor de eventos debe estar habilitado para la sincronización de ESM automática y la recopilación automática de paquetes de soporte de eventos críticos. Para habilitar el Supervisor de eventos, seleccione **Iniciar supervisor automáticamente**.

Para completar la instalación de Storage Manager, consulte “Finalización de la instalación de Storage Manager” en la página 40.

Instalación de Storage Manager en Linux, AIX, HP-UX, o Solaris

Si su estación de gestión tiene un sistema operativo basado en Unix como Linux, AIX, HP-UX o Solaris, complete los pasos indicados a continuación para instalar Storage Manager con el asistente de instalación:

1. Descargue los archivos del DVD de Storage Manager o del sitio web de soporte de disco de System Storage al sistema de archivos raíz de su sistema.
2. Inicie sesión como usuario raíz.
3. Si el archivo `.bin` del paquete de software de Storage Manager no tiene permiso ejecutable, utilice el comando `chmod +x` para hacerlo ejecutable.
4. Ejecute el archivo `.bin` y siga las instrucciones del asistente de instalación para instalar el software. El directorio predeterminado es `/opt/IBM_DS`

Cuando seleccione el tipo de instalación, podrá elegir una de las siguientes opciones:

- **Instalación habitual (completa):** Instala los paquetes del software Storage Manager necesarios para gestionar el subsistema de almacenamiento desde el host y proporcionar conectividad de E/S al almacenamiento
 - **Estación de gestión:** Instala los paquetes necesarios para gestionar y supervisar el subsistema de almacenamiento (SMruntime y SMclient)
 - **Host:** Instala los paquetes necesarios para proporcionar conectividad de E/S al subsistema de almacenamiento (SMruntime, SMagent y SMutil)
 - **Personalizada:** Le permite seleccionar los paquetes que desea instalar.
5. Escriba `SMclient` en la ventana de la consola y pulse Intro para iniciar el programa cliente Storage Manager. Añada los subsistemas de almacenamiento que desee gestionar y supervisar en la ventana Gestión empresarial del programa cliente Storage Manager.
 6. Pulse con el botón derecho el subsistema y seleccione **Recopilar datos de soporte > Crear/Editar planificación**. Se abrirá la ventana **Planificar recopilación de datos de soporte**.
 7. Defina una planificación/hora y especifique la ubicación en la que almacenar los datos de soporte durante la recopilación de datos de soporte de los subsistemas de almacenamiento que ha añadido.

Nota: Puede planificar días del mes (1 a 31) o días de la semana (lunes a domingo) para la recopilación de datos de soporte automática. Un subsistema solo puede tener una planificación. Puede seleccionar los subsistemas para los que desea una planificación idéntica. Los datos de soporte se guardan en la unidad local de la ubicación especificada. El nombre del informe incluye la fecha en que se generó el informe. El sistema permite un máximo de cinco informes de datos de soporte. Si se genera un informe cuando ya existen cinco, el informe más antiguo se suprime y se guarda el nuevo.

8. Pulse con el botón derecho en el subsistema de almacenamiento. Seleccione **Recopilar datos de soporte > Automáticamente**. Se abrirá la ventana **Recopilación automática de datos de soporte**.

Nota: Para la Recopilación automática de datos de soporte, debe estar habilitado el servicio de control de Storage Manager.

9. Seleccione los subsistemas de los que desea un informe automático en caso de evento crítico y especifique la ubicación de su unidad local en la que desea guardarlos.

10. Configure, o instale y configure el controlador multi-ruta para gestionar rutas a la unidad lógica correlacionada del subsistema de almacenamiento.

Durante la instalación, se le hará la pregunta ¿Desea iniciar automáticamente el supervisor? . Ésta pregunta se refiere al servicio del Supervisor de eventos. El Supervisor de eventos debe estar habilitado para la sincronización de ESM automática y la recopilación automática de paquetes de soporte de eventos críticos. Para habilitar el Supervisor de eventos, seleccione **Iniciar supervisor automáticamente**.

Para completar la instalación de Storage Manager, consulte “Finalización de la instalación de Storage Manager” en la página 40.

Instalación de Storage Manager con una ventana de consola en Linux, AIX, HP-UX y Solaris

Describe el proceso de instalación para Storage Manager en modo silencioso. Esto se puede aplicar cuando las estaciones de gestión basadas en Unix no tienen un adaptador de gráficos.

En estaciones de gestión sin adaptador de gráficos, el paquete de software Storage Manager se puede instalar en silencio con la opción `-i silent` o `-i console`. Este método de instalación también se puede utilizar en entornos de sistema operativo Windows.

La opción `-i silent` hace que se instale el paquete Storage Manager Software Installer utilizando los valores predeterminados del instalador. La opción `-i console` solicita al usuario las opciones instaladas antes de que se inicie la instalación del software, al igual que el asistente de instalación. No obstante las solicitudes se muestran en el texto de la ventana de consola en vez en ventanas gráficas.

En el siguiente ejemplo se muestran partes del texto de instalación de la ventana de consola de Storage Manager con la opción `-i silent` y `-i console`.

```
[usr@RHManaStation ~]# ./SMIA-LINUX-10.60.A5.17.bin -i console
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system environment...

Launching installer...

Preparing CONSOLE Mode Installation...
=====
Choose Locale...
-----

    1- Deutsch
    ->2- English
    3- Español
    4- Français
    5- Italiano
    6- Português (Brasil)

CHOOSE LOCALE BY NUMBER:
2
... ..
```

```
[usr@RHManaStation ~]# ./SMIA-LINUX-10.60.A5.17.bin -i silent
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system environment...
```

```
Launching installer...
```

```
Preparing SILENT Mode Installation...
```

```
=====
IBM System Storage DS Storage Manager 10
(created with InstallAnywhere by Macrovision)
-----
```

```
-----
Installing...
-----
```

```
[=====|=====|=====|=====]
[-----|-----|-----|-----]
```

```
... ..
```

Instalación manual de los paquetes de Storage Manager

Para sistemas operativos de tipo Unix como AIX, Linux, Sun Solaris y HP-UX, se facilitan paquetes del software Storage Manager individuales. Consulte Tabla 8 para conocer la secuencia de instalación de cada paquete de software.

Utilice el procedimiento indicado en esta sección para instalar el software Storage Manager de forma manual en una estación de gestión. Asegúrese de instalar los paquetes en el orden adecuado.

Importante:

1. No existe opción de instalación manual para sistemas operativos Windows. Para todas las instalaciones de Storage Manager en Windows, los paquetes de software individuales se incluyen en un instalador de software Storage Manager individual.

Secuencia de instalación de software

Instale los paquetes de software de Storage Manager en la secuencia mostrada en Tabla 8.

Nota: Estos paquetes están disponibles para servidores UNIX sin interfaz gráfica de usuario.

Tabla 8. Secuencia de instalación de paquetes de software de Storage Manager

Paso	Paquete
1	SMruntime
2	SMesm
3	SMclient ¹
4	SMagent
5	SMutil

¹SMclient depende de SMruntime, compilador Java para SMclient. SMruntime se debe instalar en primer lugar.

Instalación manual de Storage Manager

Antes de instalar el software Storage Manager, asegúrese de que los archivos de Storage Manager están disponibles en un directorio del sistema.

Para su instalación, modifique los siguientes comandos según sea necesario. No es necesario reiniciar el sistema durante el proceso de instalación. El proceso de verificación devuelve una tabla que describe la instalación del software, incluyendo el nombre del archivo del paquete, el número de versión, la acción y el estado de la acción.

1. Instale el <SMpackage> escribiendo el comando adecuado para su sistema operativo.

Nota: Los comandos de instalación manual indicados en la siguiente tabla sirven *solo* para sistemas operativos basados enUNIX.

Tabla 9. Ejemplos de comandos de instalación del paquete de Storage Manager

Sistema operativo	Nombre de paquete	Comando de instalación
AIX	SMruntime.AIX-10.xx.xx.xx.bff	#installp -a -d /path_name/ SMruntime.AIX-10.xx.xx.xx.bff SMruntime.aix.rte
HP-UX	SMruntime_10.xx.xx.xx.depot	#swinstall -s /cdrom/HP-UX/ SMruntime_10.xx.xx.xx.depot
Solaris	SMruntime-SOL-10.xx.xx.xx.pkg	#pkgadd -d path/SMruntime-SOL- 10.xx.xx.xx.pkg
Linux en POWER	SMruntime-LINUX-10.xx.xx.xx-x.i586.rpm	#rpm -ihv SMruntime-LINUX- 10.xx.xx.xx-x.i586.rpm

2. Compruebe si la instalación ha sido correcta escribiendo el comando adecuado para su sistema operativo.

Tabla 10. Comandos de verificación de instalación del paquete de Storage Manager

Sistema operativo	Comando de verificación
AIX	# ls1pp -ah <SMpackage>.aix.rte
HP-UX	# swverify -v <SMpackage>
Solaris	# pkginfo -l <SMpackage>
Linux on POWER	# rpm -qa grep <SMpackage>

Si el proceso de verificación devuelve un error, póngase en contacto con su representante de servicios de IBM.

Desinstalación de Storage Manager

Utilice el procedimiento aplicable de esta sección para desinstalar Storage Manager en un sistema operativo Windows o de tipo Unix.

Desinstalación de Storage Manager en un sistema operativo Windows

Para desinstalar el software en un sistema operativo Windows, complete los pasos siguientes:

1. Abra la ventana Panel de control.
2. Si tiene Windows 2003 o Windows XP, pulse dos veces en **Añadir o quitar programas**. Si tiene Windows 2008 o Windows 2012, realice una doble pulsación en **Programas y características**. Se abrirá la ventana nueva.
3. Seleccione **Software del host del gestor de almacenamiento DS de IBM versión 10.8x**, donde *x* es el número de versión aplicable de su software.
4. Pulse **Cambiar/Quitar** y siga las instrucciones del asistente de Desinstalación de Storage Manager 10 para desinstalar el software Storage Manager. El proceso de desinstalación del software podría dejar archivos creados por Storage Manager una vez completada la instalación. Estos archivos podrían incluir archivos de rastreo, archivos de repositorio y otros archivos administrativos. Suprima estos archivos manualmente para eliminar completamente Storage Manager.

Desinstalación de Storage Manager en un sistema operativo Linux, AIX o Solaris

Para desinstalar el software en un sistema operativo de tipo Unix, complete los pasos siguientes:

1. Abra el directorio `/opt/IBM_DS/Uninstall` IBM System Storage DS Storage Manager 10, que contiene el binario del desinstalador.
2. ejecute el script `Uninstall_IBM_System_Storage_DS_Storage_Manager_10` en la ventana de consola para desinstalar el software Storage Manager. El proceso de desinstalación del software podría dejar archivos que no formaban parte de la instalación original. Estos archivos podrían incluir archivos de rastreo, archivos de repositorio y otros archivos administrativos. Suprima estos archivos manualmente para eliminar completamente Storage Manager.

Finalización de la instalación de Storage Manager

Esta sección contiene los procedimientos para utilizar las características de Gestión empresarial y Gestión del subsistema de Storage Manager para completar las tareas de instalación de Storage Manager en todos los sistemas operativos de host.

Para completar una instalación de Storage Manager, debe seguir los pasos indicados a continuación:

- Realice un descubrimiento automático inicial de subsistemas de almacenamiento
- Realice un descubrimiento manual inicial de subsistemas de almacenamiento
- Nombre los subsistemas de almacenamiento
- Configure las notificaciones de alerta
- Cree una planificación para recopilar automáticamente datos de soporte para los subsistemas de almacenamiento gestionados
- Habilite los datos de soporte recopilados en caso de suceso crítico
- Configure los valores iSCSI para subsistemas de almacenamiento con puertos iSCSI

- Compruebe y actualice el código del controlador, ESM, y el firmware de la unidad de disco a la última versión, como se indica en el portal de soporte de IBM
- Habilite las funciones avanzadas del subsistema de almacenamiento
- Guarde un perfil de subsistema de almacenamiento y datos de soporte

Cada uno de estos procedimientos se describen en detalle en las siguientes secciones.

Cuando inicie Storage Manager se abrirá la ventana Gestión empresarial. Puede utilizar dicha ventana para realizar las siguientes tareas:

- Añadir y descubrir los subsistemas de almacenamiento
- Ver todos los subsistemas de almacenamiento en su dominio de gestión
- Realizar tareas de gestión del subsistema de almacenamiento con el editor de scripts

Realización de un descubrimiento automático de subsistemas de almacenamiento

Siga los pasos indicados a continuación para realizar un descubrimiento automático inicial en sus subsistemas de almacenamiento:

1. En sistemas operativos Windows, pulse **Inicio > Todos los programas > DS Storage Manager 10 Client > DS Storage Manager 10 Client**. En sistemas operativos UNIX, abra la ventana de consola. Especifique `SMclient` y pulse la tecla Intro. El software cliente Storage Manager se iniciará y se mostrarán las ventanas Gestión empresarial y Confirmar descubrimiento automático inicial.
2. Pulse **Sí** para comenzar el descubrimiento automático inicial de los hosts y subsistemas de almacenamiento conectados a la subred local.

Una vez finalizado el proceso de descubrimiento automático inicial, en la ventana Gestión empresarial se visualizan todos los hosts y subsistemas de almacenamiento que están conectados a la subred local.

Nota: La ventana Gestión empresarial tardará un minuto o más en renovarse tras el descubrimiento automático inicial. Si el subsistema de almacenamiento no se descubre automáticamente, compruebe las conexiones de red (gestión fuera de banda) o del puerto HBA del servidor al puerto de host del subsistema de almacenamiento. Para intentar añadir el subsistema de forma manual, pulse **Editar > Añadir subsistema de almacenamiento**.

3. Compruebe que todos los host y subsistemas de almacenamiento se muestran en la ventana Gestión empresarial.
 - Si no se muestra algún host o subsistema de almacenamiento, realice las tareas siguientes:
 - a. Compruebe el hardware y las conexiones de hardware para detectar posibles problemas. Consulte la *Guía de instalación y del usuario* para de su subsistema de almacenamiento para conocer los procedimientos específicos.
 - b. Consulte la ayuda en línea de Gestión empresarial para obtener información adicional sobre el descubrimiento de subsistemas de almacenamiento.
 - c. Si utiliza el método de gestión de red (normalmente conocido como gestión fuera de banda), compruebe que todos los hosts y subsistemas de almacenamiento están conectados a la misma red de subred y que la información de la pasarela está definida en los puertos Ethernet. Para

obtener más información sobre los puertos de gestión Ethernet del subsistema de almacenamiento, consulte “Configuración de direcciones IP para controladores de subsistema de almacenamiento” en la página 8. Si está utilizando el método de agente de host (normalmente conocido como gestión dentro de banda), asegúrese de que se ha realizado la conexión de canal de fibra, SASA o iSCSI entre el host y los subsistemas de almacenamiento.

- d. Asegúrese de haber completado todos los pasos de preparación para configurar el subsistemas de almacenamiento para un sistema gestionado en la red. Utilice la opción **Añadir dispositivo** para añadir la dirección IP del subsistema de almacenamiento. Añada ambas direcciones IP del controlador; de lo contrario, se mostrará el mensaje de error **dispositivo gestionado parcialmente** al intentar gestionar el subsistema de almacenamiento.

Nota: Para utilizar el método de descubrimiento automático, el subsistema de almacenamiento y este host deben estar en la misma subred. De lo contrario, utilice el método manual para añadir un subsistema de almacenamiento.

- Si utiliza el método de gestión host-agente, complete los pasos siguientes:
 - a. Asegúrese de que SMagent se ha instalado en el sistema principal.
 - b. Compruebe que dispone de una conexión de canal de fibra, SAS o iSCSI entre el subsistema de almacenamiento y el host en el que está instalado SMagent. Compruebe la distribución en zonas del conmutador SAN o la configuración VLAN según sea necesario.
 - c. Compruebe si ha completado todos los pasos e preparación y siga los pasos indicados a continuación:
 - 1) Ejecute el programa de utilidad hot_add.
 - 2) Reinicie el SMagent.
 - 3) Pulse con el botón derecho en el host y pulse **Herramientas > Re-examinar hosts** en la ventana Gestión empresarial.

Nota: En determinadas situaciones, los subsistemas de almacenamiento podría aparecer duplicados en la vista de árbol de la pestaña **Dispositivo** tras un descubrimiento automático. Puede eliminar un icono de gestión del almacenamiento duplicado del árbol de dispositivos utilizando la opción **Eliminar dispositivo** de la ventana Gestión empresarial.

4. Verifique si el estado de cada uno de los subsistemas de almacenamiento es Óptimo. Si el estado de un dispositivo es Sin respuesta, pulse con el botón derecho en el dispositivo y seleccione **Eliminar dispositivo** para suprimirlo del dominio de gestión. Compruebe que el subsistema de almacenamiento está encendido y complete el proceso de inicio de jornada. A continuación utilice la opción **Añadir dispositivo** para volver a añadirlo al dominio de gestión. Consulte la ayuda en línea de la ventana Gestión empresarial para obtener instrucciones sobre la eliminación y adición de dispositivos.

Realización de un descubrimiento manual de subsistemas de almacenamiento

Puede añadir hosts o subsistemas de almacenamiento manualmente; utilice esta opción para gestionar de forma selectiva un grupo de subsistemas de almacenamiento desde un SMclient. También puede utilizar esta opción para añadir y gestionar dispositivos no descubiertos durante el descubrimiento inicial del SMclient.

En la ventana Gestión empresarial, pulse **Editar > Añadir subsistema de almacenamiento**. Se abrirá la ventana **Añadir nuevo subsistema de almacenamiento - Manual**. Puede añadir subsistemas de almacenamiento para su gestión. Consulte la ayuda en línea para saber cómo añadir subsistemas.

Importante:

1. Cuando añada nuevos subsistemas de almacenamiento a los subsistemas de almacenamiento existentes en una SAN que se gestionan por medio del software del agente del sistema principal, deberá detener y volver a iniciar el servicio del agente del sistema principal. Al reiniciarse el servicio del agente del sistema principal, se detectará el nuevo subsistema de almacenamiento. A continuación, vaya a la ventana Gestión empresarial y pulse **Herramientas > Re-examinar** para añadir el nuevo subsistema de almacenamiento al dominio de gestión.
2. Cuando añada nuevos subsistemas de almacenamiento a los subsistemas de almacenamiento existentes que se gestionan mediante la utilización del método de gestión directa, asegúrese de especificar las direcciones IP de los dos controladores.

Definición de una contraseña de gestión del subsistema de almacenamiento

La funcionalidad de contraseñas de gestión del subsistema de almacenamiento difiere entre determinadas combinaciones de Storage Manager y versiones de firmware de controlador.

En una ventana se le pedirá que defina una contraseña de gestión del subsistema cada vez que inicie la ventana Gestión del subsistema de un subsistema de almacenamiento que no tenga una contraseña definida. Además, la contraseña caduca tras un determinado periodo de inactividad de la ventana Gestión del subsistema. Las contraseñas seguras deben contener entre 8 y 30 caracteres y estar formadas al menos por un número, una letra minúscula, una letra mayúscula y un carácter no alfanumérico (por ejemplo, < > ! @ + #). No se permiten espacios y se diferencia entre mayúsculas y minúsculas. Los subsistemas de almacenamiento con versión de firmware de controlador 7.70.xx.xx no permiten que se abra la ventana Gestión del subsistema si no se ha definido una contraseña para el subsistema de almacenamiento. Dichas restricciones no se aplican con otras versiones de firmware de controlador.

Importante: Asegúrese de que la información sobre contraseñas se guarda en un lugar seguro y accesible. Póngase en contacto con el soporte técnico de IBM para recibir ayuda si olvida la contraseña de su subsistema de almacenamiento.

Especificar el nombre de los subsistemas de almacenamiento

Durante la configuración de la red, decida el convenio de denominación de los subsistemas de almacenamiento. Por ejemplo, puede utilizar el tipo de dispositivo seguido del número de serie: 1815 1312345 XXXX xxx xxxx. Cuando instala el software Storage Manager y lo inicia por primera vez, todos los subsistemas de almacenamiento del dominio de gestión se muestran como <unnamed>. Utilice la ventana Gestión del subsistema para renombrar cada subsistema de almacenamiento.

Cuando especifique el nombre de los subsistemas de almacenamiento, tenga en cuenta los factores siguientes:

- Existe un límite de 30 caracteres. Todos los espacios iniciales y finales se suprimen del nombre.
- Utilice un esquema de denominación exclusivo y significativo que sea fácil de entender y de recordar.
- Evite utilizar nombres arbitrarios o nombres que puedan dejar de ser significativos rápidamente.
- El software añade el prefijo Storage Subsystem cuando muestra los nombres de los subsistemas de almacenamiento. Por ejemplo, si nombra un subsistema de almacenamiento Engineering, se mostrará como Storage Subsystem Engineering.

Para nombrar sus subsistemas de almacenamiento, complete los siguientes pasos:

1. En la ventana Gestión empresarial, pulse con el botón derecho en el subsistema de almacenamiento y seleccione **Renombrar**. Se abrirá la ventana Renombrar subsistema de almacenamiento.

Nota: Si alguno de los hosts ejecuta controladores de migración tras error de ruta, actualice el nombre del subsistema de almacenamiento en su archivo de configuración de controladores de migración tras error antes de rearrancar el sistema host para establecer acceso ininterrumpido para el subsistema de almacenamiento.

2. Escriba el nombre del subsistema de almacenamiento y pulse **Aceptar**.
3. Pulse **Sí** en la pantalla de aviso.
4. Repita este procedimiento para cada subsistema de almacenamiento que no tenga un nombre. Para obtener más información, consulte el tema que trata acerca del cambio del nombre de los subsistemas de almacenamiento en la ayuda en línea de la ventana Subsystem Management.
5. Continúe con el apartado “Configuración de notificaciones de alerta”.

Configuración de notificaciones de alerta

Tras añadir dispositivos al dominio de gestión, puede definir notificaciones de alerta para informar sobre eventos críticos en los subsistemas de almacenamiento. Las opciones de notificación de alertas disponibles son las siguientes:

- Notificación a una estación de gestión en red designada utilizando interrupciones de protocolo simple de gestión de red (SNMP)
- Notificación a direcciones de correo electrónico designadas
- Notificación a buscapersonas alfanuméricos designados (requiere software independiente para convertir mensajes de correo electrónico)

Nota: Sólo puede supervisar los subsistemas de almacenamiento que se encuentran dentro del dominio de gestión. Si no instala el servicio Event Monitor, la ventana Enterprise Management deberá permanecer abierta. Si cierra la ventana, no recibirá ninguna notificación de alerta de los subsistemas de almacenamiento gestionados. Consulte la ayuda en línea de la ventana Gestión empresarial para obtener más información.

Notificaciones de alerta con interrupciones SNMP

Para configurar notificaciones de alerta a una estación de gestión en red utilizando interrupciones SNMP, complete los pasos siguientes:

1. Inserte el DVD de Storage Manager en la unidad de DVD de una estación de gestión en red. Sólo deberá establecer la estación de gestión designada una vez.

2. Copie el archivo SMxx.x.MIB del directorio SMxxMIB en la estación de gestión de red.
3. Siga los pasos requeridos por su estación de gestión en red para compilar el archivo Management Information Base (MIB). (Para conocer más detalles, póngase en contacto con su administrador de red o consulte la documentación de su producto de gestión de almacenamiento concreto).

Notificaciones de alerta sin interrupciones SNMP

Para configurar notificaciones de alerta sin interrupciones SNMP, pulse **Subsistema de almacenamiento > Editar > Configurar alertas** en la ventana Gestión empresarial.

Recopilación automática de paquete de soporte

Desde la versión 10.83 de Storage Manager, la capacidad para recopilar automáticamente datos de soporte de subsistemas de almacenamientos gestionados de manera periódica forma parte del software cliente. La información de las colecciones de datos de soporte guardadas puede ser útil para resolver problemas y recuperar el subsistema de almacenamiento en caso de error grave. Para crear una planificación de recopilación automática de datos de soporte, seleccione **Herramientas > Recopilar datos de soporte > Crear/Editar** en la ventana Gestión empresarial. Cuando se abra la ventana **Planificar recopilación de datos de soporte**, seleccione el subsistema de almacenamiento y pulse **Crear/Editar** para crear la planificación y recopilar datos de soporte a diario, de forma semanal, mensual o anual. Puede crear la planificación para diversos subsistemas de almacenamiento a la vez manteniendo pulsada la tecla Control mientras selecciona los subsistemas. No obstante, IBM recomienda escalonar la recopilación de datos cuando se gestionan diversos subsistemas. Consulte la ayuda en línea para obtener más información sobre la recopilación periódica de datos de soporte. Además de recopilar datos de soporte de manera automática y periódica, el cliente Storage Manager tiene la capacidad de recopilar datos de soporte cuando se producen eventos críticos en el subsistema de almacenamiento gestionado. Seleccione **Herramientas > Recopilar datos de soporte > Automáticamente** en la ventana Gestión empresarial para configurarla. Haga los cambios necesarios cuando se abra la ventana **Recopilación automática de datos de soporte**. Consulte la ayuda en línea para obtener más información.

La planificación se almacena en la estación de gestión en la que se define. La estación de gestión debe estar activa y en ejecución, y debe tener conexión de gestión con los subsistemas de almacenamiento para que se cree automáticamente el paquete de soporte. Los nombres de los archivos guardados también incluirán la fecha. El código de Storage Manager mantiene un máximo de cinco archivos. Si ya existen cinco archivos, el código suprimirá el archivo más antiguo antes de guardar uno nuevo. Si no hay espacio de disco suficiente para guardar un nuevo archivo, el código de Storage Manager suprimirá archivos empezando por el más antiguo, hasta que se disponga de espacio suficiente.

Nota: El cliente Storage Manager no tiene que estar en ejecución para que se recopilen los datos de soporte. No obstante el servicio de supervisión de soporte de IBM DS Storage Manager sí debe estar en ejecución. Además, para evitar la supresión de datos de soporte cuando el directorio del repositorio está lleno, seleccione una ubicación de repositorio con espacio suficiente.

Uso de scripts de SM para configurar y gestionar la recopilación automática de paquetes de soporte

En vez de utilizar las opciones de menú de la ventana Gestión empresarial, puede configurar la recopilación automática de paquetes de soporte, mostrar la planificación actual y planificar la recopilación desde la interfaz de línea de comandos de su estación de gestión. Para obtener más información sobre estos comandos, consulte la *IBM System Storage DS3000, DS4000, and DS5000 Command Line Interface and Script Commands Programming Guide* o la ayuda en línea. Debe ejecutar estos comandos desde la estación de gestión en la que haya instalado Storage Manager, no desde la ventana de scripts que se inicia desde la ventana Gestión empresarial de Storage Manager. Además, no especifique la dirección IP del subsistema de almacenamiento como parte del comando SMcli y no inicie el comando supportBundle con el parámetro '-c'. Utilice el subsystemName del subsistema de almacenamiento gestionado como valor de comando de script. Para conocer el subsystemName, ejecute el siguiente comando con el parámetro -d.

```
C:\Program Files (x86)\IBM_DS\client>smcli -d
DS3400A          fe80:0:0:0:2a0:b8ff:fe5a:ae42
DS3524-DTL139140 ds3524dta.net.com ds3524dtb.net.com
DS3524-DTL       ds3524dt1.net.com ds3524dt2.net.com
DS5100-DTL       ds5k-a.net.com ds5k-b.net.com
```

DS3400A, DS3524-DTL139140, DS3524-DTL y DS5100-DTL son los nombres de los subsistemas de almacenamiento. Para habilitar la recopilación automática de paquetes de soporte todas las semanas de domingo a martes a las 2:00AM en el subsistema de almacenamiento DS3524-DTL139140

```
C:\Program Files (x86)\IBM_DS\client>smcli -supportBundle schedule
enable DS3524-DTL139140 daysofweek=[Sunday Tuesday] startTime=02:00
```

Ambos comandos se ejecutan desde la interfaz de línea de comandos de la estación de gestión.

Nota: Si su estación de gestión está en un sistema operativo Windows, debe ser el administrador para ejecutar estos comandos.

Gestión de la configuración iSCSI

Pulse la pestaña **Configuración** en la ventana Gestión del subsistema.

Nota: El enlace a **Gestión de configuración iSCSI** o **Configuración de puertos de host iSCSI** de la ventana Gestión del subsistema solo está disponible para subsistemas de almacenamiento que soportan conexiones a host iSCSI. En el momento de crear este documento, los siguientes subsistemas de almacenamiento soportan la conexión a host iSCSI.

- DS3300
- DS3500
- DCS3700 con Controladores del módulo de rendimiento
- DS3950
- DS5020
- DS5100/5300

Las siguientes opciones iSCSI están disponibles en el menú **Gestión del subsistema de almacenamiento** y se describen en las siguientes secciones:

Nota: La selección de menú de estas opciones iSCSI cambia en función de su versión de firmware de controlador. Consulte la ayuda en línea para conocer las opciones de menú adecuadas.

- “Cambio de la autenticación del destino”
- “Especificación de permisos de autenticación mutua”
- “Cambio de la identificación de destino”
- “Cambio del descubrimiento de destino”
- “Configuración de puertos de hosts iSCSI”
- “Visualización o finalización de una sesión iSCSI” en la página 48
- “Visualización de estadísticas iSCSI” en la página 48

Cambio de la autenticación del destino

Seleccione **Cambio de la autenticación del destino** para especificar el secreto de protocolo de autenticación por desafío mutuo (CHAP) de destino que el iniciador debe utilizar durante la fase de negociación del inicio de sesión iSCSI. De forma predeterminada, se selecciona **Ninguno**. Para cambiar la selección, pulse **CHAP** e introduzca el secreto CHAP. También puede seleccionar la opción de generar un secreto aleatorio. Esto habilita el CHAP unidireccional.

Especificación de permisos de autenticación mutua

Antes de seleccionar **Especificar permisos de autenticación mutua**, debe definir un puerto de host para el iniciador y habilitar Autenticación de destino. Una vez indicado el puerto de host, seleccione el host de la lista y pulse **Secreto Chap** para especificar el secreto que se indica al iniciador desde el destino y autenticarlo. Esto habilita el CHAP mutuo (2 direcciones).

Cambio de la identificación de destino

Seleccione **Cambiar identificación de destino** para especificar el alias de destino que se utilizará durante el descubrimiento del dispositivo. Debe proporcionar un nombre único compuesto por menos de 30 caracteres para el destino.

Nota: Se conectará al destino con el IQN cualificado completo que aparece sobre el alias.

Cambio del descubrimiento de destino

Seleccionar **Cambio de descubrimiento de destino** para llevar a cabo el descubrimiento de dispositivos con el servicio de nombre simple iSCSI (iSNS). Después de seleccionar esta opción, seleccione el recuadro de selección **Utilizar servidor iSNS**. También puede indicar si el servidor iSNS va a descubrirse utilizando un servidor DHCP en la red y puede especificar manualmente una dirección de Protocolo Internet versión 4 (IPv4) o IPv6. Pulsando en la pestaña **Avanzado**, puede asignar un puerto TCP/IP diferente para su servidor iSNS, para mayor seguridad.

Nota: Para proporcionar la información necesaria de inicio de sesión del puerto para un descubrimiento de dispositivo correcto, todos los puertos iSCSI han de poder comunicarse con el mismo servidor iSNS.

Configuración de puertos de hosts iSCSI

Seleccione **Configurar puertos de hosts iSCSI** para configurar todos los valores TCP/IP. Puede indicar si se habilita o inhabilita IPv4 y IPv6 en todos los puertos. También puede asignar estadísticamente direcciones IP o dejar que sean descubiertas utilizando DHCP. En **Configuración IPv4 avanzada**, puede asignar etiquetas VLAN (802.1Q) o definir la prioridad Ethernet (802.1P). En **Configuración de puerto de host avanzada**, puede especificar un puerto TCP/IP

iSCSI único para ese puerto de destino. Desde esta opción también puede habilitar tramas de gran tamaño. Las grandes tamaños compatibles son 1500 y 9000.

Visualización o finalización de una sesión iSCSI

Seleccione **Ver/finalizar sesiones iSCSI** para ver todas las sesiones iSCSI conectadas al destino. Desde esta página, también puede cerrar un sesión existente forzando un cierre de sesión ASYNC de destino de la sesión del iniciador.

Visualización de estadísticas iSCSI

Seleccione **Ver estadísticas iSCSI** para ver una lista de todos los datos de sesión iSCSI, por ejemplo el número de errores de asimilación de cabeceras, el número de errores de asimilación de datos y el recuento de unidades de datos de protocolo correctas. También puede establecer una cuenta de línea base tras una acción correctiva para determinar si se ha resuelto el problema.

Uso de un servidor iSNS

Hay varios factores a tener en cuenta para utilizar correctamente un servidor iSNS. Asegúrese de asignar correctamente su dirección de servidor iSNS facilitada durante el descubrimiento DHCP de su iniciador o destino. Esto le permitirá realizar un descubrimiento sencillo cuando utilice soluciones basadas en el iniciador. Si no puede hacerlo, debe asignar manualmente el servidor iSNS a sus iniciadores de software y hardware, y asegurarse de que todos los puertos iSCSI e iniciadores iSCSI del subsistema de almacenamiento están en el mismo segmento de red (o asegurarse de que el direccionamiento entre los segmentos de red separados es correcto). Si no lo hace, no podrá descubrir todos los puertos durante el proceso de descubrimiento de iSCSI y es posible que no pueda realizar correctamente una migración tras error del controlador o la vía de acceso.

Uso de DHCP

No utilice DHCP para los portales de destino. Si utiliza DHCP, debe asignar reservas de DHCP para que los alquileres se mantengan de forma coherente en los reinicios del subsistema de almacenamiento. Si no se facilitan las reservas de IP estáticas, los puertos del iniciador pueden perder la comunicación con el controlador y quizá no puedan volver a conectarse al dispositivo.

Usando iniciadores de hardware soportados

Antes de instalar y configurar estos adaptadores, asegúrese de que ha instalado la aplicación de gestión y firmware más recientes. A continuación, configure cada adaptador uno por uno. En una configuración con un subsistema con controlador individual, en la que los adaptadores iSCSI y los puertos de destino están en el mismo segmento de red, cada adaptador se puede conectar a cualquier puerto de destino. En configuraciones complejas, cada adaptador se puede conectar a un dispositivo de controlador. Para asegurarse de que la migración tras error se realiza correctamente, conecte cada adaptador iSCSI del servidor a uno de los siguientes elementos:

- - **Adaptador iSCSI único en el servidor** - El puerto del adaptador iSCSI debe poder iniciar sesión en los puertos host del controlado A y B. El puerto iSCSI se configura como multihome con las subredes de puerto iSCSI del controlador A y B.
- - **Varios adaptadores iSCSI en el servidor** - Cada puerto de adaptador dispone de una ruta única a cada puerto de host iSCSI del controlador. Cada puerto de adaptador iSCSI y puerto de host de controlador iSCSI asociado, debe estar en una subred diferente a la de otros partes de adaptador y puerto de host de controlador iSCSI

Si utiliza un adaptador de iniciador de hardware Qlogic, complete los pasos siguientes para iniciar sesión en todos los puertos de destino disponibles del iniciador de hardware. Para otros adaptadores de iniciador de hardware, consulte las publicaciones de los mismos para obtener información sobre el inicio de sesión en todos los puertos de destino disponibles.

Para consultar una lista de todos los iniciadores de hardware soportados, vaya a <http://www.ibm.com/systems/support/storage/config/ssic>.

Para iniciar sesión en todos los puertos de destino disponibles desde el iniciador de hardware Qlogic, complete los pasos indicados a continuación.

Nota: Si no lleva a cabo los pasos del siguiente procedimiento podrían producirse inconsistencias de migración tras error de ruta y el subsistema de almacenamiento podría no funcionar correctamente.

1. Inicie el programa de utilidad de gestión SANsurfer.
2. Conecte con el sistema que esté ejecutando el agente qlremote.
3. Seleccione el adaptador que desee configurar.
4. Seleccione **Puerto 0** o **Puerto 1** para el adaptador.
5. Pulse **Configuración de destino**.
6. Pulse en el signo más (+) en el extremo derecho de la ventana.
7. Escriba la dirección IPv4 o IPv6 del puerto de destino al que se quiere conectar.
8. Pulse **Aceptar**.
9. Seleccione **Parámetros de configuración**.
10. Desplácese hasta ver ISID. Para la conexión 0, el último carácter que se debe indicar debe ser 0. Para la conexión 1, debe ser 1, para la conexión 2, debe ser 2, y así sucesivamente.
11. Repita los pasos 6 a 10 para cada conexión al destino que desee crear.
12. Cuando se hayan conectado todas las sesiones, seleccione **Guardar configuración de destino**. Si utiliza el HBA PCI de puerto único o dual iSCSI QLogic para IBM System x para soportar IPv6, debe permitir al firmware del adaptador de bus de host asignar la dirección de enlace local.

Uso de IPv6

Los puertos iSCSI del subsistema de almacenamiento soportan el Protocolo Internet versión 6 (IPv6) TCP/IP. Tenga en cuenta que únicamente se pueden configurar los cuatro octetos finales si está asignando manualmente la dirección de enlace local. Los cuatro octetos iniciales son fe80:0:0:0. Se requiere la dirección completa de IPv6 cuando se está intentando conectar con el destino desde un iniciador. Si no proporciona la dirección completa del IPv6, es posible que el iniciador no se conecte correctamente.

Configuración de valores de red para conexión de host iSCSI

Si utiliza un subsistema de almacenamiento que soporta la conexión de host iSCSI en una topología de red compleja, debe enfrentarse a determinados desafíos. De ser posible, aisle el tráfico iSCSI en una red dedicada. Si no fuera posible y utiliza un iniciador basado en hardware, el tiempo de espera de mantenimiento de activación debe estar definido en 120 segundos. Para establecer el tiempo de espera excedido de mantenimiento de activación, siga estos pasos:

1. Inicie el programa de utilidad de gestión SANsurfer y conéctese al servidor.
2. Seleccione el adaptador y el puerto del adaptador que ha de configurarse.

3. Seleccione las opciones del puerto el firmware.

El tiempo de espera excedido de conexión predeterminado es de 60 segundos. Este valor es adecuado para topologías de red simples. No obstante, en una configuración más compleja, si se produce una convergencia de redes y no utiliza dominios Fast Spanning Tree o Separate Spanning Tree, podría exceder el tiempo de espera de E/S. Si utiliza un iniciador de software Linux iSCSI, modifique el parámetro `ConnFailTimeout` para solucionar este problema. El valor de `ConnFailTimeout` debe ser 120 segundos.

Configuración de los valores de unidad de transmisión máxima

Todos los dispositivos de un enlace que deben comunicarse entre ellos (como los dispositivos de la misma VLAN) deben configurarse con el mismo tamaño de unidad de transmisión máxima (MTU). El tamaño de MTU es un elemento de configuración, o está codificado en el dispositivo, y no se negocia entre puntos finales durante el inicio de sesión o establecimiento de la conexión. Si un dispositivo recibe un paquete más grande que el tamaño de MTU, descartará dicho paquete. Si un direccionador recibe un paquete cuyo tamaño no supera el tamaño de MTU del enlace en el que se ha recibido pero si el tamaño de MTU del enlace de envío, el direccionador fragmenta el paquete (IPv4) o devuelve un mensaje de error ICMP paquete demasiado grande. Asegúrese de que todos los componentes de un enlace de red utilizan el mismo valor de tamaño de MTU.

Para subsistemas de almacenamiento que soportan iSCSI, el valor predeterminado de MTU es 1500 bytes. Existe una opción para seleccionar 9000 bytes para tramas de gran tamaño. Para que las tramas de gran tamaño extremo a extremo funcionen correctamente, estas tramas (gran MTU) deben estar habilitadas en todos los componentes (host, conmutador, direccionadores y destinos). Si las tramas de gran tamaño no están habilitadas en todos los componentes, se pueden producir una o varias de las siguientes condiciones:

- Se descartan tramas.
- No se descartan tramas debido a mensajes de error sobre el gran tamaño del paquete.
- Se fragmentan tramas de gran tamaño.

Consideraciones sobre Microsoft iSCSI Software Initiator

La E/S multi-ruta nativa(MPIO) facilitada con Microsoft iSCSI Software Initiator (versión 2.03 o posterior) no es compatible. Puede utilizar el DSM proporcionado con Storage Manager para asegurarse de que la migración tras error y el acceso E/S son correctos. Si se utiliza el MPIO de Microsoft iSCSI Software Initiator, se producirán efectos indeseados.

Descarga de firmware de controlador, NVSRAM y ESM

Esta sección proporciona instrucciones para descargar firmware de controlador de subsistema de almacenamiento, NVSRAM, ESM de alojamiento de almacenamiento y unidades. Normalmente, la secuencia de descarga de firmware para el subsistema de almacenamiento es la siguiente:

1. Firmware de controlador
2. NVSRAM de controlador
3. Firmware de ESM
4. Firmware de unidades

Consulte el archivo léame facilitado con el firmware de controlador, NVSRAM, ESM y unidad actualizado para conocer los cambios necesarios a realizar en la secuencia de descarga de firmware.

Importante:

1. Para llevar a cabo los siguientes procedimientos se supone que utiliza la última versión del firmware del controlador. Acceda a las últimas versiones de firmware de controlador de subsistema de almacenamiento, NVSRAM y ESM de alojamiento de almacenamiento en el Portal de soporte de IBM en <http://www.ibm.com/support/entry/portal>. Para obtener los archivos léame de Storage Manager más recientes para su sistema operativo, consulte “Búsqueda de software, firmware de controlador y archivos léame de Storage Manager” en la página xv.
2. IBM soporta la descarga de firmware de controlador de subsistema de almacenamiento y ESM con E/S, en ocasiones denominada *descarga de firmware simultánea*, con algunos subsistemas de almacenamiento. Antes de proceder con una descarga de firmware simultánea, revise el archivo léame facilitado con el código de firmware o el software host de Storage Manager en su sistema operativo para conocer las limitaciones.
3. Suspenda toda actividad de E/S mientras descarga firmware y NVSRAM en un subsistema de almacenamiento con un solo controlador. Si no suspende la actividad de E/S, el servidor de host recibirá solicitudes de E/S erróneas porque habrá conexiones redundantes entre dicho servidor de host y el subsistema de almacenamiento.
4. Compruebe siempre el archivo léame del firmware del controlador del subsistema de almacenamiento para conocer las dependencias de firmware de controladores y requisitos previos antes de aplicar actualizaciones de firmware al subsistema de almacenamiento. Actualizar componentes del firmware del subsistema de almacenamiento sin tener en cuenta las dependencias o requisitos previos podría causar tiempo de inactividad (para solucionar los problemas o recuperación).
5. Degradar el firmware del controlador no es una función soportada. Esta opción se debe utilizar **solo** bajo la dirección del soporte de IBM. La degradación del firmware 07.xx al 06.xx no se soporta y en caso de que lo intente se le mostrará un error.

Si su firmware de controlador existente es el 06.1x.xx.xx o posterior, tiene la opción de seleccionar el de NVSRAM para descargarlo a la vez que actualiza o descarga el nuevo firmware de controlador. Además, tiene la posibilidad de descargar el firmware y NVSRAM inmediatamente pero activarlo más adelante, cuando sea más conveniente. Consulte la ayuda en línea para obtener más información.

Nota: La opción de activación del firmware posteriormente no se soporta en el subsistema de almacenamiento DS4400.

Determinación de los niveles de firmware

Antes de descargar una actualización de firmware, asegúrese de que conoce la versión de firmware actual. Hay tres métodos diferentes para determinar la versión de firmware del subsistema de almacenamiento, el alojamiento de almacenamiento, las unidades y el ESM. Cada método utiliza el cliente de Storage Manager que gestiona el subsistema de almacenamiento con el alojamiento de almacenamiento asociado.

Método uno:

Vaya a la ventana Gestión del subsistema y seleccione la opción de menú para mostrar el perfil del subsistema de almacenamiento. Cuando se abra la ventana Perfil del subsistema de almacenamiento, pulse la pestaña **Resumen** y desplácese hasta la página **Supervisor** para ubicar la siguiente información. La página **Ver inventario de firmware o Ver perfil del subsistema de almacenamiento** contiene

toda la información de perfil del subsistema de almacenamiento, incluyendo la versión de firmware. Un ejemplo sería como en -

Versión de firmware de controlador de subsistema de almacenamiento

Ver Perfil de subsistema de almacenamiento:

Consulte el ejemplo siguiente para conocer la información de perfil.

```
INVENTARIO DE FIRMWARE
IBM DS Storage Manager 10
  Versión de SMW:          10.84.G5.21
  Fecha del informe:      Jue Oct 09 21:13:34 CST 2012

Subsistema de almacenamiento
Nombre del subsistema de almacenamiento: DCS3700
Versión del paquete actual:              07.84.39.00
Versión de NVSRAM actual:                N1818D37R0784V04
Versión de paquete intermedio:           Ninguna
Versión NVSRAM intermedia:               Ninguna
```

Controladores

```
Ubicación:                      Alojamiento 1, Ranura A
Versión del paquete actual:      07.84.39.00
Versión de NVSRAM actual:       N1818D37R0784V04
ID de placa:                     2660
ID de submodelo:                162

Ubicación:                      Alojamiento 1, Ranura B
Versión del paquete actual:      07.84.39.00
Versión de NVSRAM actual:       N1818D37R0784V04
ID de placa:                     2660
ID de submodelo:                162
```

Fuentes de alimentación

```
Ubicación:                      Alojamiento 1, derecha
Versión de firmware:            No disponible

Ubicación:                      Alojamiento 1 DESCONCIDA
Versión de firmware:            No disponible
```

Unidad

```
Alojamiento, Cajón, Ranura:      Fabricante:
ID producto:                     Tipo unidad:      Capacidad:
Versión firmware unidad:         Versión FPGA: (sólo SSD )

Alojamiento 1, Cajón 1, Ranura 2  IBM-ESXS
ST9300603SS F Serial Attached SCSI (SAS) 278,896 GB
B53B                             No disponible

Alojamiento 1, Cajón 1, Ranura 3  IBM-ESXS
CBRCA300C3ETS0 N Serial Attached SCSI (SAS) 278,896 GB
C610                             No disponible
```

Método dos:

Complete el procedimiento aplicable de las opciones siguientes para obtener la versión de firmware especificada.

Para obtener la versión de firmware del controlador:

Pulse el icono **Controlador** en la pestaña **Hardware** de la ventana Gestión del subsistema. En una ventana nueva se mostrará la información del controlador.

Debe realizar esta acción en cada controlador.

Para obtener la versión de firmware de la unidad:

Pulse el icono **Controlador** en la pestaña **Hardware** de la ventana Gestión del subsistema. En una ventana nueva se mostrará la información del firmware de la unidad.

Debe realizar esta acción en cada controlador.

Para obtener la versión de firmware de ESM:

Pulse el icono **Controlador** en la pestaña **Hardware** de la ventana Gestión del subsistema. En una ventana nueva se mostrará la información del firmware de ESM.

Debe realizar esta acción en cada controlador.

Descarga del firmware de controlador y NVSRAM

Nota: Realice la operación Recopilar todos los datos de soporte antes de actualizar el firmware del controlador y NVSRAM. Consulte “Resolución de problemas de eventos críticos” en la página 273 para conocer los procedimientos de recopilación de datos.

Esta sección proporciona instrucciones para descargar firmware del controlador del subsistema de almacenamiento y NVSRAM. Normalmente, la secuencia de descarga de firmware de subsistema de almacenamiento comienza por el firmware del controlador, seguido por el de NVSRAM, ESM y unidades.

Importante: Si está actualizando desde la versión 06.xx a 07.xx, debe utilizar la herramienta de actualización de firmware del controlador. Consulte “Uso de IBM System Storage Controller Firmware Upgrade Tool” en la página 54. Si ya tiene el nivel de firmware 07.xx, no necesita utilizar la herramienta de actualización de firmware del controlador para actualizar a otro nivel 07.xx. No obstante, la herramienta de actualización tiene prestaciones de diagnóstico que podrían ser de utilidad.

Para descargar la versión de firmware 06.1x.xx.xx o posterior, y NVSRAM, complete los pasos siguientes:

1. En la ventana Gestión empresarial, seleccione un subsistema de almacenamiento.
2. Pulse **Herramientas > Actualizar firmware de controlador**. Se abre la ventana Actualizar firmware de controlador.

Nota: Si el firmware del controlador es el 7.77.xx.xx o posterior, el sistema ejecutará automáticamente una comprobación pre-actualización que durará varios minutos. La actualización del firmware se realizará solo si dicha comprobación es correcta. Con las versiones de firmware 06.1x.xx.xx y posteriores instaladas en el subsistema de almacenamiento, puede descargar el archivo NVSRAM con el archivo de firmware. Esta característica de descarga no se soporta en subsistemas de almacenamiento con firmware de controlador 05.4x.xx.xx o anterior. Si dispone de una versión de firmware de controlador 05.4x.xx.xx o anterior, solo se mostrará una ventana para la descarga del firmware.

El software Storage Manager comprueba el estado de cada subsistema de almacenamiento y muestra una lista de los subsistemas de almacenamiento que necesitan actualización.

3. Seleccione todos los subsistemas de almacenamiento que quiera actualizar. Pulse **Firmware**. Se abrirá la ventana Descargar firmware.

Nota: Si quiere actualizar varios subsistemas a la vez, todos ellos deben ser del mismo tipo.

Uso de IBM System Storage Controller Firmware Upgrade Tool

La siguiente información describe cómo utilizar IBM System Storage Controller Firmware Upgrade Tool para actualizar su firmware de controlador DS4800, DS4700 o DS4200 Express de 06.xx a 07.xx.

Importante:

- Utilice Controller Firmware Upgrade Tool solo cuando migre controladores DS4800, DS4700 y DS4200 de la versión 06.xx a la versión 07.xx.
- Esta herramienta está prevista para actualizaciones estándar del firmware de controlador, ESM o unidad (actualizaciones de hebra de código 6.xx.xx.xx o 7.xx.xx.xx). Para llevar a cabo una actualización de firmware de controlador, ESM o unidad estándar, consulte “Descarga de firmware de controlador, NVSRAM y ESM” en la página 50.
- En Storage Manager versión 10.50 y posteriores, Controller Firmware Upgrade Tool forma parte de la ventana Gestión empresarial y ya no es una herramienta independiente. Pulse **Herramientas > Upgrade Firmware de controlador** para abrir la ventana Actualización de firmware de controlador.

Atención: Asegúrese de que el firmware que descarga es compatible con el software Storage Manager instalado en su subsistema de almacenamiento. Si descarga un firmware incompatible, podría perder acceso a las unidades del subsistema de almacenamiento. Si fuera necesario, actualice Storage Manager antes de utilizar IBM System Storage Controller Firmware Upgrade Tool.

Antes de utilizar IBM System Storage Controller Firmware Upgrade Tool, asegúrese de que comprende las siguientes directrices.

- Se debe realizar una copia de seguridad de todos los datos de los subsistemas de almacenamiento DS4800, DS4700 y DS4200s y guardar las configuraciones del sistema existentes. Cuando la herramienta haya completado una actualización, los controladores no podrán volver a los niveles de versión de firmware anteriores.
- Debe realizar la actualización fuera de línea. Debe realizar la instalación general de Storage Manager en un entorno de host existente en línea. Para que los controladores de migración tras error se apliquen, debe reentrancar el host.
- Todos los dispositivos debe tener un estado Óptimo antes de descargar el firmware. Utilice el programa de utilidad de comprobación de estado para verificar si los dispositivos tienen estado Óptimo.
- También debe comprobar el nivel de firmware actual.
- No realice cambios en su configuración ni elimine unidad o alojamientos durante el proceso de actualización.
- Para obtener información sobre las versiones de firmware actuales, consulte “Búsqueda de software, firmware de controlador y archivos léame de Storage Manager” en la página xv con el fin de saber cómo acceder a los archivos léame de Storage Manager más actuales en la web.

Comprobación del estado de los dispositivos: Para determinar el estado de su dispositivo, complete los pasos siguientes:

1. Desde la ventana Gestión del subsistema en el Gestor de almacenamiento, haga clic derecho en el subsistema de almacenamiento. Storage Manager establece comunicación con cada dispositivo gestionado y determina el estado actual del dispositivo.

Existen seis condiciones de estado posibles:

- **Óptimo:** Cada componente del dispositivo gestionado está en condición de trabajo óptima.
 - **Requiere atención:** Existe un problema con el dispositivo gestionado que necesita intervención para su corrección.
 - **Reparación:** Se ha corregido una condición Requiere atención y el dispositivo gestionado se está cambiando actualmente al estado Óptimo.
 - **Sin respuesta:** La estación de gestión no se puede comunicar con el dispositivo, un controlador o ambos controladores del subsistema de almacenamiento.
 - **Contactando dispositivo:** Storage Manager está estableciendo contacto con el dispositivo.
 - **Requiere actualización:** El subsistema de almacenamiento está ejecutando un nivel de firmware que ha dejado de ser soportado por Storage Manager.
2. Si el estado no es Óptimo, haga clic en **Recovery Guru** en la ventana Gestión del subsistema para obtener información detallada sobre la recuperación del sistema antes de descargar el firmware. Si falla en la recuperación del sistema, comuníquese con un representante de soporte técnico de IBM para obtener una resolución de fallas.

Apertura y uso de la Herramienta de actualización del firmware de controlador:

Para utilizar la Herramienta de actualización del firmware de controlador, pulse **Herramientas > Actualización de firmware** en la ventana Gestión empresarial. Se abrirá la ventana Actualización de firmware. La Herramienta de actualización del firmware completa una comprobación de diagnóstico en estos subsistemas para determinar si su estado es adecuado para realizar una actualización de firmware de controlador.

Nota:

- Ante cualquier condición distinta a Óptima, debe ponerse en contacto con el soporte de IBM para recibir asistencia. Consulte “Soporte y servicio de software” en la página xviii para obtener información adicional.
- Con esta herramienta solo puede actualizar de una versión principal a otra versión principal (por ejemplo de 06.xx. s 07.xx). No intente realizar este tipo de actualización de firmware desde la ventana Gestión del subsistema.
- Tras haber actualizado al nivel de firmware 07.xx, no necesita utilizar la Herramienta de actualización del firmware. Utilice la ventana Gestión del subsistema para realizar actualizaciones de firmware en el futuro.

Para obtener más información sobre el uso de la herramienta, pulse el botón **Ayuda** en la Herramienta de actualización del firmware de controlador.

Adición de un subsistema de almacenamiento: Para añadir un subsistema de almacenamiento con la Herramienta de actualización del firmware de controlador, complete los pasos siguientes:

1. Pulse **Añadir**. Se abrirá la ventana Seleccionar método de adición.
2. Pulse **Automático** o **Manual**.
3. Pulse **Aceptar** para comenzar a añadir subsistemas de almacenamiento.
4. Si desea ver problemas con un subsistema de almacenamiento que podrían impedir la actualización de firmware, pulse **Ver registro**.

Descarga de firmware:

1. Seleccione el subsistema de almacenamiento que desea activar. Se habilitará el botón **Descargar**.
2. En la barra de herramientas de la ventana Gestión empresarial, pulse **Herramientas > Actualizar firmware**. Se abrirá la ventana Descargar firmware.
3. Pulse **Examinar** y seleccione el archivo de firmware de controlador que desea descargar de este directorio.
4. Pulse **Examinar** y seleccione el archivo NVSRAM en este directorio.
5. Pulse **Aceptar**. Comenzará la descarga de firmware. Se mostrará una barra de estado en la ventana Actualización de firmware de controlador.

Visualización del archivo de registro de la Herramienta de actualización del firmware de controlador de IBM System Storage: El archivo de registro de la Herramienta de actualización del firmware de controlador documenta cualquier problema con el sistema de almacenamiento que pudiera impedir la actualización del firmware. Si experimenta problemas al actualizar el firmware, pulse **Ver registro** para abrir el archivo de registro. Corrija los problemas indicados en el archivo de registro antes de intentar descargar el firmware de nuevo.

Descarga de firmware de ESM

Esta sección proporciona instrucciones para descargar firmware de ESM de alojamiento de almacenamiento. Normalmente, la secuencia de descarga de firmware de subsistema de almacenamiento comienza por el firmware del controlador, seguido por el de NVSRAM, ESM y unidades.

Para descargar firmware de ESM, realice los pasos siguientes:

1. En la ventana Gestión del sistema, seleccione **Actualizar > Firmware de ESM**. Se abrirá la ventana Descargar firmware de tarjeta de entorno.
2. Pulse **Seleccionar todo** para dirigir la descarga a todos los alojamientos de almacenamiento. También puede seleccionar un alojamiento de almacenamiento o varios, pulsando Ctrl al realizar la selección.

Nota: Si ha seleccionado diversos alojamientos, suspenda toda la actividad de E/S durante la descarga. Si selecciona solo un alojamiento de almacenamiento cada vez, puede descargar firmware de ESM mientras el servidor lleva a cabo actividad de E/S.

3. Pulse **Examinar** para identificar y seleccionar el nombre del archivo de firmware de ESM y pulse **Inicio** para comenzar con la descarga.
4. En la ventana Confirmar descarga, escriba sí y pulse **Aceptar** para iniciar el proceso de descarga.
5. Una vez terminada la descarga de firmware de ESM de todos los alojamientos seleccionados, pulse **Cancelar** para cerrar la ventana.

Cuando instala un nuevo ESM en un alojamiento de almacenamiento existente de un subsistema de almacenamiento que soporta la sincronización de firmware ESM automática, el firmware del nuevo ESM se sincroniza automáticamente con el firmware del ESM existente. Esto resuelve automáticamente cualquier condición de discrepancia entre firmwares de ESM.

Para habilitar la sincronización automática de firmware de ESM, asegúrese de que su sistema satisface los requisitos siguientes:

- El supervisor de sucesos de Storage Manager está instalado y en ejecución.
- El subsistema de almacenamiento debe estar definido en la ventana Gestión empresarial del cliente Storage Manager (SMclient).

Nota: En el momento de crear este documento, Storage Manager soporta la sincronización de firmware de ESM automática solo con los alojamientos de almacenamiento EXP710 y EXP810. Póngase en contacto con IBM para obtener información sobre el soporte de otros tipos de alojamiento de almacenamiento en el futuro. Para corregir la falta de adaptación de ESM a los alojamientos de almacenamiento sin soporte de sincronización de firmware de ESM automática, debe descargar el archivo de firmware de ESM correcto con la función de descarga de la ventana Gestión del subsistema del SMclient.

Descarga de firmware de unidades

Esta sección proporciona instrucciones para descargar firmware de unidades. Se pueden actualizar a la vez hasta cuatro tipos de unidad diferentes. Las unidades se consideran de tipo diferente si facilitan identificadores distintos cuando se realiza una consulta. Consulte la ayuda en línea para obtener información adicional.

Importante:

1. Para llevar a cabo los siguientes procedimientos se supone que cuenta con la última versión del firmware del controlador. Si tiene una versión de firmware anterior, consulte “Búsqueda de software, firmware de controlador y archivos léame de Storage Manager” en la página xv para obtener la versión de firmware aplicable.
2. IBM soporta la descarga de firmware con E/S, en ocasiones denominada *descarga firmware simultánea*. Esta característica no es compatible con el firmware de unidades. Para actualizar el firmware de las unidades y conversor ATA, debe planificar tiempo de inactividad.

Para descargar firmware de unidades para Storage Manager, complete los pasos siguientes:

1. Antes de iniciar el proceso de descarga de firmware de unidades, complete las tareas siguientes:
 - a. Detenga toda la actividad de E/S antes de descargar firmware de unidades en un subsistema de almacenamiento.
 - b. Realice una copia de seguridad completa de todos los datos de las unidades cuyo firmware desee actualizar.
 - c. Desmante los sistemas de archivos de todas las unidades lógicas que accedan a las unidades cuyo firmware desee actualizar.
2. En la ventana Gestión empresarial, seleccione un subsistema de almacenamiento.
3. En la barra de menús de ventana Gestión del subsistema, pulse **Actualizar > Firmware de la unidad**. Se abre la página Introducción. Lea las instrucciones y pulse **Siguiente**.

Nota: Con Storage Manager, puede descargar simultáneamente y actualizar hasta cuatro paquetes de firmware distintos.

4. Pulse **Añadir** para ubicar el directorio del servidor que contiene el firmware que pretende descargar.
5. Seleccione el firmware que desea descargar y pulse **Aceptar**. El archivo se mostrará en la ventana Paquetes seleccionados.
6. Repita los pasos 4 y 5 para los paquetes para los que desee descargar firmware, hasta un máximo de cuatro, y pulse **Siguiente**. Los archivos adicionales se mostrarán en la ventana Paquetes seleccionados.

7. Tras especificar los paquetes de firmware que quiere descargar, pulse **Siguiente**.
8. La página **Unidades compatibles** muestra una lista de las unidades que son compatibles con los tipos de paquetes de firmware que seleccione. En dicha lista, seleccione las unidades para las que pensado descargar el firmware de la unidad. Puede mantener pulsada la tecla Ctrl para seleccionar diversas unidades individualmente o la tecla Mayús. para seleccionar diversas unidades indicadas en series. Pulse **Seleccionar todo** para seleccionar todas las unidades.

Nota: El firmware que vaya a descargar debe aparecer en la páginas Unidades compatibles. Si el identificador de producto de sus unidades coincide con el tipo de firmware y este no aparece como compatible en la página, póngase en contacto con el representante de soporte técnico de IBM para obtener instrucciones adicionales.

9. Pulse en **Finish** para iniciar la descarga del firmware de unidad en cada unidad compatible que ha seleccionado en el paso 8.
10. Cuando se abra la ventana Descargar firmware de la unidad - ¿Seguro que quiere continuar?, escriba yes (sí) y pulse **Aceptar** para iniciar la descarga del firmware de unidad. Se abrirá la ventana Progreso de descarga. Espere hasta que el proceso de descarga termine. Cada unidad para la que se vaya a descargar firmware aparecerá como en curso hasta que la descarga se haya completado correctamente o haya fallado.
11. Si esta falla, complete los pasos siguientes:
 - a. Pulse **Guardar como** para guardar el registro de errores.
 - b. En la barra de menú de la ventana Gestión del subsistema, pulse la opción de menú para mostrar el registro de sucesos del subsistema de almacenamiento y complete las tareas siguientes necesarias para guardar el mismo antes de ponerse en contacto con su representante de servicios IBM y proceder con el siguiente paso.
 - 1) Pulse **Seleccionar todo**.
 - 2) Pulse **Guardar registro de sucesos del subsistema de almacenamiento**.
12. Cuando el botón **Cerrar** pase a estar activo, el proceso de descarga del firmware se habrá completado. Pulse **Cerrar** para salir de la ventana Progreso de descarga.
13. Utilice cualquiera de los procedimientos siguientes para determinar o verificar qué nivel de firmware de unidad tiene una unidad concreta:
 - Pulse con el botón derecho en la página Lógica o Física de la ventana Gestión del subsistema y pulse **Propiedades**. La versión de firmware de unidad asociada se mostrará en la tabla de propiedades de la unidad.
 - Seleccionar **Monitorear > Informes > Perfil del subsistema de almacenamiento** en la página Lógica o Física de la ventana Gestión del subsistema.

características premium de Storage Manager

Storage Manager soporta las siguientes características premium, disponibles para su compra independiente en IBM o en un IBM Business Partner:

Servicios de copia

Los siguientes servicios de copia están disponibles con Storage Manager:

- Enhanced FlashCopy y FlashCopy
- VolumeCopy

- Opción de duplicación remota mejorada
- Opción de duplicación global mejorada

Para obtener más información sobre los servicios de copia, consulte la *IBM System Storage DS Storage Manager Copy Services User's Guide*.

Partición de almacenamiento

La partición del almacenamiento es estándar en todos los subsistemas de almacenamiento soportados por las versiones de firmware de controlador DS3000, DS4000 y DS5000. Para obtener más información sobre la partición del almacenamiento, consulte la "Descripción general de la partición del almacenamiento" en la página 65.

Característica premium FC/SATA Intermix

La característica premium Serial ATA Intermix y canal de fibra IBM System Storage DS3000, DS4000 y DS5000 soporta la adjunción simultánea de los alojamientos de almacenamiento de canal de fibra y SATA a una configuración de subsistema de almacenamiento individual. Puede utilizar esta característica premium Intermix para crear y gestionar distintas matrices compiladas a partir de discos SATA o de canal de fibra y asignar unidades lógicas a las aplicaciones adecuadas, utilizando un subsistema de almacenamiento individual.

Para obtener información sobre el uso de la característica premium Intermix, incluyendo datos sobre configuración, versiones de firmware necesarias para configuraciones de Intermix específicas y requisitos de configuración, consulte la *IBM System Storage DS Storage Manager Fibre Channel and Serial ATA Intermix Premium Feature Installation Overview*. Consulte con su representante o distribuidor de IBM para obtener información sobre el futuro soporte del subsistema de almacenamiento en relación con la característica premium Intermix FC/SATA.

Características premium de mejora de hardware

A continuación se indican las características premium que proporcionan soporte para determinadas configuraciones de hardware de almacenamiento, por ejemplo:

- un determinado número de ranuras de unidad soportado en los subsistemas de almacenamiento
- determinados tipos de alojamientos de almacenamiento (por ejemplo, accesorios EXP5060 o los ocho accesorios EXP5060)
- determinados tipos de unidad (por ejemplo, unidades de estado sólido)

Esta categoría de características premium incluye también la característica premium de mejora del rendimiento del controlador.

Cifrado de disco completo

El uso de cifrado de disco completo (FDE) protege los datos contra amenazas cuando una unidad FDE está fuera del control de su propietario.

Complete las tareas siguientes para habilitar una característica premium en su subsistema de almacenamiento:

- "Obtención del identificador de habilitación de características premium" en la página 60
- "Generación de un archivo de claves de característica" en la página 61
- "Habilitación de una característica premium" en la página 61

Nota: El procedimiento para habilitar una característica premium depende de su versión de Storage Manager.

- “Inhabilitación de características premium” en la página 62

Para obtener la serie de identificación de la característica premium del subsistema de almacenamiento, asegúrese de que un unidad de controlador y los alojamientos de almacenamiento están conectados, la alimentación está activada y estos están gestionados por elSMclient.

Habilitación de la versión de prueba de la característica Premium

Nota: Esta versión de prueba sólo se ofrece en los subsistemas de almacenamiento DS3500, DCS3860 y DCS3700 así como en los subsistemas de almacenamiento DCS3700 con Controladores de módulo de rendimiento.

Los subsistemas de almacenamiento IBM con firmware de controlador versión 7.83 y posteriores proporcionan versiones de prueba de determinadas características premium durante 90 días. Tras completar 30 días y 3 días antes de que expire el periodo de prueba se enviarán alertas. La característica premium permanente se puede comprar y activar en cualquier momento durante el periodo de prueba de 90 días. Si la característica premium permanente se activa durante el periodo de prueba, las configuraciones del subsistema de almacenamiento creadas durante dicho periodo de prueba continuarán siendo válidas. Si no compra la característica premium, deberá suprimir las configuraciones del subsistema de almacenamiento creadas con la versión de prueba de la característica. Además, el subsistema de almacenamiento cambiará al estado "sin conformidad" en relación con la característica premium de prueba. Para habilitar la versión de prueba de una característica premium, pulse **Probar ahora** en la ventana **Característica y paquete de características premium**.

Habilitación de una característica Premium permanente

Debe obtener la característica Premium permanente, generar una clave única para la misma y luego habilitar la característica Premium permanente. Puede deshabilitar también la característica Premium permanente.

Obtención del identificador de habilitación de características premium

Cada subsistema de almacenamiento tiene su propio identificador de habilitación de características premium único. Con este identificador se garantiza que un archivo de claves de función en particular sólo podrá aplicarse a ese subsistema de almacenamiento.

Antes de obtener el identificador, debe cumplir los siguientes requisitos previos:

1. Asegúrese de que tiene el código de activación de características en la tarjeta de activación web, así como el modelo, tipo de sistema y número de serie del subsistema de almacenamiento.
2. Asegúrese de que la unidad del controlador y el alojamiento de expansión del almacenamiento están conectados, encendidos y configurados.

Para obtener el identificador, complete los siguientes pasos:

1. Pulse **Inicio > Programas > Storage Manager xx Cliente**. Se abrirá la ventana Gestión empresarial.

2. En la ventana Gestión empresarial, pulse dos veces en el subsistema de almacenamiento para el que desea habilitar la característica premium. Se abrirá la ventana Gestión del subsistema correspondiente al subsistema de almacenamiento seleccionado.
3. Complete las siguientes acciones, dependiendo de su versión de Storage Manager:
 - Si utiliza Storage Manager versión 9.x o anteriores, pulse **Subsistema de almacenamiento > Características premium > Lista**. Se abrirá la ventana Lista de características premium y se mostrará el identificador de habilitación.
 - Si utiliza Storage Manager versión 10.x o posteriores, pulse **Subsistema de almacenamiento > Características premium....** Se abrirá la ventana Características premium e información sobre paquete de características.El identificador se mostrará en la parte inferior de la nueva ventana.
4. Anote el identificador de habilitación de características.

Nota: Para evitar errores al registrar el identificador, copie el mismo, de 32 caracteres, y péguelo en el campo de solicitud de clave de característica premium.

5. Pulse **Cerrar** para cerrar la ventana.
6. Continúe con “Generación de un archivo de claves de característica”.

Nota: Para comprobar el estado de una característica premium existente de Storage Manager versión 9.x o anteriores, seleccione **Subsistema de almacenamiento > Características premium > Lista** en el menú.

Generación de un archivo de claves de característica

Puede generar el archivo de claves con la herramienta de Activación de características premium que encontrará en <http://www.ibm.com/storage/fasttkeys>.

1. Complete los pasos indicados en el sitio web.

Nota: Asegúrese de seleccionar la característica premium o paquete de características adecuado cuando se le solicite.

El archivo de claves de características está disponible para su descarga en la página web, y se le puede enviar por correo electrónico.

2. En su unidad de disco duro, cree un nuevo directorio (por ejemplo, nombre el directorio FlashCopyfeaturekey).
3. Guarde el archivo de claves de características premium en el nuevo directorio.

Si se pierde la clave de las características o se cambia su identificador y la característica premium deja de estar en conformidad, puede solicitar el archivo de claves de reactivación en <http://www.ibm.com/storage/fasttkeys>. Debe tener el mismo tipo de sistema, modelo y número de serie que utilizó para generar los archivos de claves de características inicialmente.

Habilitación de una característica premium

Para habilitar una característica premium, siga el procedimiento aplicable para su versión de Storage Manager.

Habilitación de características premium y el paquete de características en Storage Manager 10.x o posterior

Para habilitar una característica premium en Storage Manager versión 10.x o posterior, complete los siguientes pasos:

1. En la ventana Gestión del subsistema, pulse **Subsistema de almacenamiento > Características premium....** Se abrirá la ventana Características premium e información sobre paquete de características.
2. Para habilitar una característica premium de la lista, pulse **Permitir** o **Utilizar** archivo de claves, dependiendo de la versión del firmware del controlador. Se abrirá una ventana que le permite seleccionar el archivo de claves de la característica premium para habilitar la misma. Siga las instrucciones en pantalla.
3. Compruebe que la característica premium está habilitada inspeccionando la lista mostrada de características premium en la ventana Características premium e información sobre paquete de características.
4. Pulse **Cerrar** para cerrar la ventana Características premium e información sobre paquete de características.

Habilitación del paquete de características

1. Pulse **Cambiar** en la ventana Características premium e información sobre paquete de características.
2. Se abrirá una ventana para que seleccione el archivo de claves del paquete de características. Seleccione un archivo de claves y pulse **Aceptar**.
3. Revise el contenido del campo **Paquete de características instalado en el subsistema de almacenamiento** para comprobar si se ha instalado el paquete de características.

Importante: La habilitación de un paquete de características premium requiere reiniciar los controladores. Si el subsistema de almacenamiento para el que se va a habilitar el paquete de características premium está en ejecución, asegúrese de planificar un tiempo de inactividad para reiniciar los controladores.

Inhabilitación de características premium

En condiciones de sistema operativo normales, no tiene que inhabilitar las características premium. No obstante, si desea hacerlo, asegúrese de que dispone del archivo de claves o la tarjeta de titularidad de las características premium con el código de activación de las mismas para generar el archivo de claves. Necesitará este archivo de claves para rehabilitar las características premium más adelante.

Nota:

1. Si desea habilitar la característica premium en el futuro, debe volver a aplicar el archivo de claves de esa característica.
2. Puede inhabilitar la opción de duplicación remota sin desactivar la característica. Si la característica está inhabilitada pero activada, podrá realizar todas las operaciones de duplicación en espejos remotos existentes. No obstante, si la característica está inhabilitada, no puede crear ningún espejo remoto nuevo. Para obtener más información sobre la activación de la opción de espejo remoto, consulte la Guía del usuario de servicios de copia de *IBM System Storage DS* o el apartado "Uso del asistente de activación de espejo remoto" en la ayuda en línea de Storage Manager.
3. Si se inhabilita una característica premium, puede acceder al sitio web y repetir este proceso siguiendo la opción de reactivación de características premium.

Inhabilitación de características premium en Storage Manager 10.x o posterior

Para inhabilitar una característica premium en Storage Manager versión 10.x o posterior, complete los siguientes pasos:

1. En la ventana Gestión del subsistema, pulse **Subsistema de almacenamiento > Características premium**. Se abrirá la ventana Características premium e información sobre paquete de características.
2. Seleccione la característica premium que desea inhabilitar y pulse **Inhabilitar**.

Para obtener asistencia adicional, póngase en contacto con su proveedor de servicios de IBM.

Guardar el perfil de subsistema de almacenamiento

Importante: Debe guardar un perfil de subsistema de almacenamiento siempre que modifique las matrices y unidades lógicas en su subsistema de almacenamiento. El perfil guardado contiene información detallada sobre el controlador, incluyendo información sobre la configuración de los discos físicos y lógicos, que le puede ayudar a recuperar la configuración en caso de error catastrófico. No guarde un perfil de un subsistema de almacenamiento en ese mismo subsistema de almacenamiento.

Para guardar un perfil de subsistema de almacenamiento, seleccione la opción de menú para mostrar el perfil del subsistema en la ventana Gestión del sistema y pulse **Guardar como** cuando se abra la ventana Perfil del subsistema de almacenamiento. Para guardar el perfil completo, seleccione la pestaña **Todo**. También puede seleccionar la opción de menú para guardar los datos soportados y recopilar todos los tipos de datos de inventario, estado, diagnóstico y rendimiento del subsistema de almacenamiento y guardarlos en un archivo comprimido único.

Capítulo 4. Configuración del almacenamiento

Una vez instalado Storage Manager, debe configurar el subsistema o subsistemas de almacenamiento. Los siguientes temas de este capítulo describen las tareas que son necesarias para la configuración:

- “Descripción general de la partición del almacenamiento”
- “Uso del asistente de tareas” en la página 66
- “Configuración de unidades de repuesto en caliente globales” en la página 92
- “Configuración de almacenamiento de disco” en la página 78
- “Definición de un sistema operativo host predeterminado” en la página 94
- “Definición de un grupo de host” en la página 95
- “Definición de hosts heterogéneos” en la página 96
- “Definición de host y puertos del host” en la página 96
- “Correlación de LUN” en la página 97
- “Uso de la Memoria caché de lectura de rendimiento” en la página 102

Hacia el final de este capítulo, los siguientes temas proporcionan información opcional que puede aplicarse a la configuración de sus subsistemas de almacenamiento:

- “Configuración de IBM System Storage para IBM i” en la página 98

Nota: Esta sección se aplica solo a las configuraciones de almacenamiento que utilizan el sistema operativo IBM i.

- “Configuración y uso de características premium opcionales” en la página 99

Nota: Esta sección se aplica solo a los subsistemas de almacenamiento con características premium.

- “Uso de otras características” en la página 103
- “Ajuste de subsistemas de almacenamiento” en la página 109

Nota: De forma predeterminada, la pestaña **Configuración** de la ventana Gestión empresarial se abre cuando inicia Storage Manager. Consulte “Ventana Gestión empresarial” en la página 15 para ver una descripción detallada de la ventana Gestión empresarial.

Descripción general de la partición del almacenamiento

Antes de crear particiones de almacenamiento, tenga en cuenta la siguiente información:

- El Asistente de tareas de Storage Manager proporciona un asistente de Partición del almacenamiento que puede utilizar para definir su host y puertos de hosts y correlacionar LUN con las particiones de almacenamiento. Si su subsistema de almacenamiento ejecuta el firmware de controlador 05.xx.xx.xx, no puede utilizar el asistente. Ambos tipos de procedimiento se documentan en esta sección.
- En estos procedimientos se presupone que ya ha creado una conexión física entre el host y los controladores del subsistema de almacenamiento y ha conectado y distribuido en zonas el conmutador (si aplicable). Si no ha completado estas conexiones, Storage Manager no puede mostrar los nombres de puerto de ámbito mundial (WWPN) ni los nombres iqn iSCSI de los HBA

durante estos procedimientos. En este caso, deberá escribir los WWPN en los campos aplicables durante el procedimiento descrito en “Definición de host y puertos del host” en la página 96.

- Cree el grupo de host a nivel del subsistema de almacenamiento. No cree grupos de hosts a nivel de grupo predeterminado.

Nota: Si tiene una configuración de DS4100 o DS4300 y la partición no está habilitada, puede utilizar el grupo de host predeterminado.

- En caso de diversos HBA del host conectados al subsistema de almacenamiento, cree una partición de host única para incluir todos ellos. Utilice la definición del grupo de host solo para agrupar un conjunto de hosts que compartan el mismo conjunto de unidades lógicas.
- En una partición en clúster, realice correlaciones de unidad lógica a nivel del grupo de host para que todos los host puedan reconocer el mismo almacenamiento. En una partición normal, realice correlaciones de unidad lógica a nivel del host.
- Para configurar y asignar IBM i LUN en subsistemas de almacenamiento DS5300 y DS5100 con el asistente, consulte “Configuración de IBM System Storage para IBM i” en la página 98 para obtener información específica sobre la configuración de IBM i.

Uso del asistente de tareas

El Asistente de tareas de Storage Manager proporciona una ubicación central desde la que puede seleccionar llevar a cabo las tareas más comunes de las ventanas Gestión empresarial y Gestión del subsistema. Puede utilizar el Asistente de tareas para completar muchos de los procedimientos descritos en esta sección.

Importante: Si tiene la versión de firmware de controlador 7.50 o posterior, las descripciones de tareas de Storage Manager podrían diferir ligeramente de las tareas de las listas siguiente.

En la ventana Gestión del subsistema, el Asistente de tareas de la pestaña Configuración (dependiendo de la versión de firmware de controlador) consiste en atajos a estas tareas:

- Configuración de los subsistemas de almacenamiento
- Definición de hosts
- Creación de una nueva partición de almacenamiento
- Correlación de unidades lógicas adicionales
- Guardado de configuraciones

Si existe algún problema con el subsistema de almacenamiento, se mostrará un atajo a Recovery Guru. Utilice Recovery Guru para conocer más detalles sobre el problema y buscar soluciones para corregirlo.

Importante: Si tiene la versión de firmware de controlador 7.50 o posterior, el procedimiento de Storage Manager para acceder a la funcionalidad del Asistente de tareas podría ser ligeramente diferente. No existe ningún botón ni ventana independiente para el Asistente de tareas. Pulse la pestaña **Configuración** en la ventana Gestión del subsistema para acceder al menú del Asistente de tareas de la ventana Tareas de configuración iniciales.

Nota: El Asistente de tareas se invocará automáticamente cada vez que abra la ventana Gestión del subsistema, a menos que seleccione la casilla de verificación **No mostrar de nuevo el asistente de tareas al iniciar** de la parte inferior de la ventana.

Unidades admitidas por IBM System Storage DS Storage Manager

El subsistema DS soporta los tipos de soporte disco duro y disco de estado sólido.

Dependiendo de los modelos, el subsistema DS soporta algunas o todas las interfaces de unidad de disco siguientes:

SATA En determinados alojamientos, las unidades de disco SATA requieren un conversor ATA o un intermediario FC-SATA como ayuda para insertar la unidad en la ranura con un conector FC.

Nota: Las unidades SATA y los conversores ATA o intermediarios FC-SATA se venden como identidad única.

Canal de fibra (FC)

No existen requisitos especiales para las unidades FC.

SAS Para alojamientos con plano medio FC, la unidad SAS requiere el intermediario FC-SAS como ayuda para insertarla en la ranura con un conector FC. Esta categoría también incluye las unidades NL SAS.

Nota: Las unidades SAS y los intermediarios FC-SAS se venden como identidad única y se conocen como unidad FC-SAS.

Además de las diferencias de los tipos de unidad de disco e interfaces, existen determinadas diferencias con respecto a las prestaciones de la unidad, como la Información de protección T10 (T10PI) o el Cifrado de disco completo/auto-cifrado(FDE/SED). Las capacidades de unidad están disponibles para la mayoría de los tipos de soporte de unidad compatibles, interfaces de unidad y prestaciones de unidad. El subsistema DS no es compatible con todos los tipos de soporte de unidad. Para obtener más información sobre los tipos de unidad disponibles y compatibles con un subsistema de almacenamiento concreto, consulte **RFA del subsistema DS**. Para obtener más información sobre la lista de componentes de FRU para las unidades compatibles en un modelo de subsistema de almacenamiento, también puede consultar la Guía del usuario, mantenimiento e instalación del subsistema de almacenamiento DS. En la Tabla 11, se muestra un resumen de los tipos de unidades, interfaces de unidad y prestaciones de unidad compatibles.

Tabla 11. Resumen de tipos, interfaces y prestaciones de unidad compatibles

Unidades compatibles mediante el Gestor de almacenamiento DS de IBM	Interfaz de unidad	Prestación T10 PI	Prestación SED	Sin prestación SED
Unidad de disco duro	SATA	N/A	N/A	N/A
	Canal de fibra (FC)	Sí	Sí	Sí
		N/A	Sí	Sí
	NL SAS/SAS	Sí	Sí	Sí
N/A		Sí	Sí	

Tabla 11. Resumen de tipos, interfaces y prestaciones de unidad compatibles (continuación)

Unidades compatibles mediante el Gestor de almacenamiento DS de IBM	Interfaz de unidad	Prestación T10 PI	Prestación SED	Sin prestación SED
Unidad de estado sólido	FC	N/A	N/A	Sí
	SAS	N/A	N/A	Sí

En Gestión del subsistema, la pestaña Física o Hardware tiene botones o una lista desplegable que le ayuda a identificar varios tipos de unidad en un alojamiento determinado dependiendo de la versión del firmware del controlador. Al pulsar el botón o hacer una selección en la lista desplegable, en el panel de vista física se resaltan todas las unidades que cumplen la definición del botón. En el alojamiento, si todas las unidades se adaptan a la definición del botón, este se inhabilitará.

Reglas para seleccionar unidades al crear una matriz RAID

Esto es lo que debe tener en cuenta al seleccionar unidades para una matriz RAID

- La matriz RAID se puede crear utilizando solo unidades con la misma interfaz de unidad.
Por ejemplo, no puede crear una matriz RAID con unidades FC, SAS y SATA aunque las unidades SATA y SAS tengan mediadores para poder actuar como unidades FC. Además, las unidades con una interfaz específica no se pueden utilizar como unidades de repuesto en una matriz RAID con interfaz distinta.
- Una matriz RAID no puede tener una combinación de unidades de disco duro giratorio y unidades de estado sólido.
- Dado que las unidades NL-SAS y SAS operan a diferentes velocidades de rotación, no mezcle unidades NL-SAS y SAS en la misma matriz RAID. Las NL-SAS operan a 7200 rpm y las SAS a 10K o 15K rpm. En una matriz RAID compuesta de unidades SAS y NL-SAS, es posible utilizar una NL-SAS para sustituir a una unidad SAS que haya fallado o una unidad SAS para sustituir a una unidad NL-SAS que haya fallado.
- No mezcle las unidades con la misma interfaz que operen a diferentes velocidades de rotación en la misma matriz RAID. La interfaz gráfica de usuario de Storage Manager o la interfaz de línea de comandos de SM no impiden esta configuración. Si no hay disponible una unidad adecuada, el firmware del controlador podría seleccionar una unidad de repuesto en caliente disponible con velocidad de rotación diferente como repuesto de una unidad que haya fallado. En caso de que la unidad de repuesto en caliente tenga una velocidad de rotación inferior, sustituya la unidad errónea lo antes posible.
- Si no hay disponible una unidad de la velocidad de rotación necesaria, IBM puede proporcionar una unidad similar con velocidad de rotación superior como FRU de sustitución. Cuando se utiliza una unidad con mayor velocidad de rotación, el rendimiento de la matriz o agrupación de discos no se ve afectada.
- En una matriz RAID, las unidades con prestaciones distintas como T10PI o FDE se pueden mezclar con unidades sin dichas prestaciones solo si una de las prestaciones de unidad no está habilitada en la matriz RAID. Por ejemplo, puede crear una matriz RAID con unidades T10PI y no T10PI. Sin embargo, la matriz creada no podrá operar con la funcionalidad T10PI habilitada.

- Las unidades con velocidad de rotación inferior se pueden utilizar como repuesto para matrices con unidades de mayor velocidad de rotación. Se recomienda no mezclar unidades con diferente velocidad de rotación en la misma matriz RAID ya que el rendimiento de la matriz o agrupación de discos podría verse degradado por las unidades de menor velocidad.
- En una matriz RAID se pueden mezclar unidades de distintos tamaños. No obstante, todas las unidades de la matriz creada tendrán el tamaño de la unidad más pequeña de la misma.
- Una matriz con prestaciones adicionales habilitadas, como FDE y T10PI, no puede utilizar unidades sin dichas prestaciones habilitadas como repuesto de una matriz que haya fallado. Por ejemplo, una matriz RAID con T10PI y FDE habilitado requiere una unidad con T10PI y FDE como repuesto.
- Las agrupaciones de discos solo pueden estar compuestas por unidades de disco duro giratorio con interfaz de disco SAS. Las agrupaciones de discos soportan Enhanced FlashCopy, la duplicación Metro Mirror y la Duplicación global, pero no Legacy FlashCopy. Una agrupación de discos no puede tener unidades con distintas capacidades y diferentes ejes.
- Las unidades 2 TB NL-SAS (FC#3450, 3451) no tienen soporte para T10 PI. Si está utilizando estas unidades en un subsistema DCS3700 con Controladores del módulo de rendimiento, debe crear manualmente una matriz o agrupación de discos para evitar la habilitación T10 PI. Para crear manualmente una agrupación de discos, pulse **No** en la ventana **Configuración automática de agrupación de discos** y quite la marca de **Filtrar selección de unidades para mostrar sólo las unidades con capacidad para T10 PI (T10 Información de protección)**. Para crear una unidad lógica con capacidad para T10 PI, todas las unidades deben tener capacidad para T10 PI.

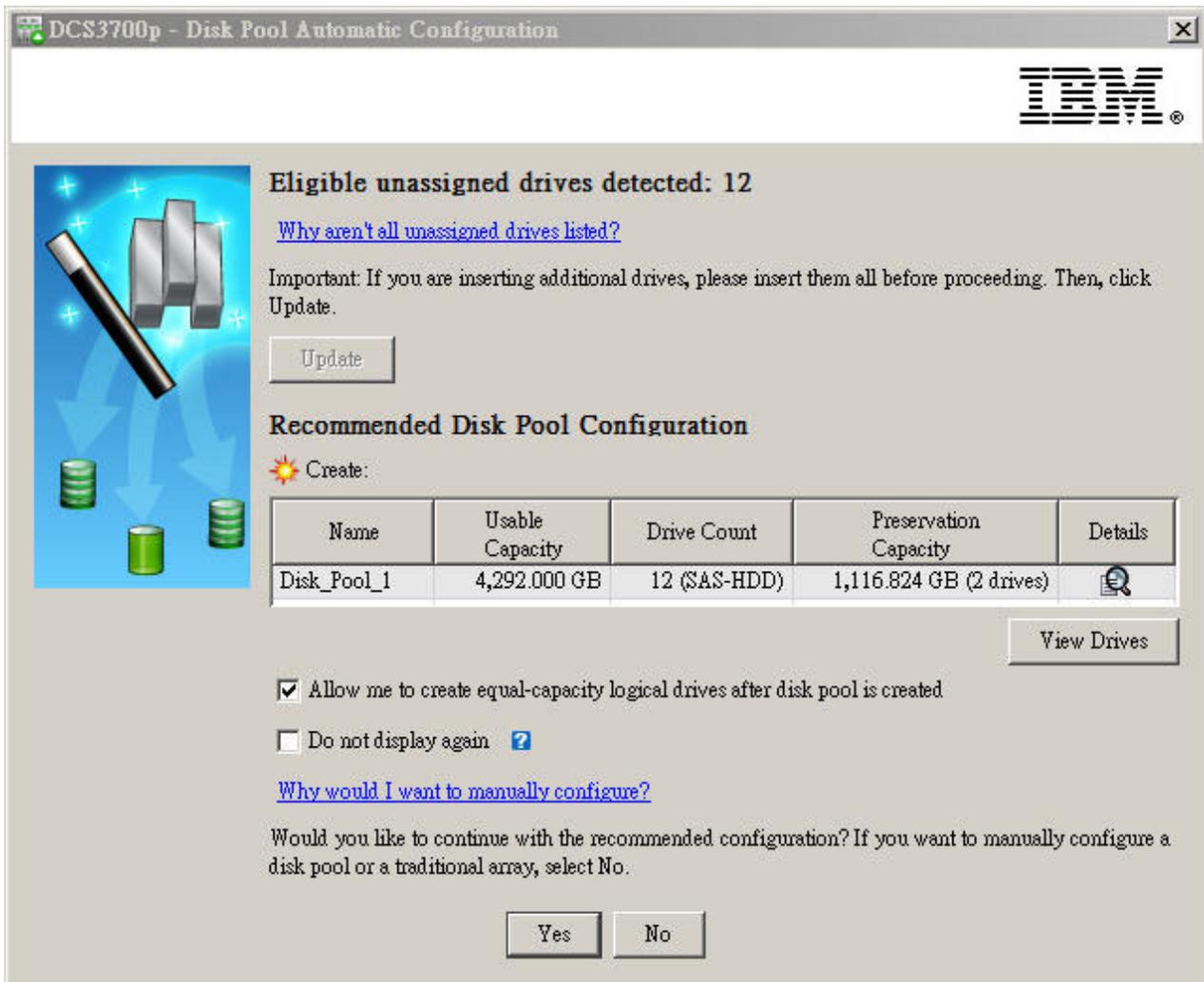


Figura 3. Configuración automática de la agrupación de discos

Atributos de unidad de estado sólido (SSD)

Las unidades de estado sólido son unidades que almacenan datos en un chip de memoria de actualización instantánea en vez de hacerlo en superficies de disco duro rotativas, lo cual resulta en velocidades de escritura/lectura de acceso aleatorio más rápidas.

Dado que los dispositivos flash tienen determinadas limitaciones de recuento de ciclo de escritura, estas unidades contienen chips de memoria de actualización instantánea de repuesto adicionales para dar soporte al uso del ciclo de escritura durante el periodo de garantía de la unidad. muestra una unidad de disco SSD y el porcentaje de bloques de repuesto restantes de la misma. SSD se soporta en las versiones de firmware de controlador 7.60.xx.xx y posteriores dado que soporta la exploración de soportes para unidades lógicas de matrices RAID compuestas de unidades SSD. Sin embargo, se recomienda utilizar un firmware de controlador versión 7.77.xx.xx o posterior.

Para los subsistemas con el firmware del controlador versión 7.8x.xx.xx o posterior, los subsistemas de almacenamiento DS5100/5300 y DS5020 pueden tener un

máximo de 20 unidades SSD en una configuración de subsistema de almacenamiento determinado. Los subsistemas de almacenamiento DS3500, DCS3860 y DCS3700 así como los subsistemas de almacenamiento DCS3700 con Controladores de módulo de rendimiento pueden tener un máximo de 24 unidades. Además, para subsistemas DS5100/5300, no debe tener más de cuatro SSD por alojamiento de expansión de unidad y debe dispersar los SSD en el mayor número de canales de unidad distintos posible. De esta forma garantizará el rendimiento óptimo de su subsistema de almacenamiento.

Atributos de unidades con capacidad T10PI

Las unidades con capacidad T10PI soportan la extensión estándar T10 Protection Information (T10 PI o T10PI) especificada para el protocolo SCSI. El estándar T10PI también se conoce como T10 DIF (Data Integrity Field).

Este estándar se ha diseñado para proporcionar un nivel extra de integridad de datos mediante el guardado de cada bloque de datos de usuario con 8 bytes de metadatos de integridad mientras los datos se transfieren entre el controlador de almacenamiento y las unidades de disco con T10PI inicializado. Este nivel extra de integridad de datos también se extiende al servidor cuando el subsistema de almacenamiento está conectado para E/S a servidores IBM Power que ejecuten el sistema operativo AIX. El soporte T10 PI en sistemas operativos AIX incluye los metadatos de Information Protection con datos de usuarios transferidos entre el servidor AIX y el controlador de almacenamiento. El estándar T10PI se ha diseñado para proporcionar al usuario protección extremo a extremo y corrección ante corrupción de datos en silencio debido a errores del controlador de dispositivo, errores del sistema de archivos o escrituras mal direccionadas, pérdidas, fantasmas o rotas.

Las unidades con capacidad T10PI se inicializan como unidades T10PI de Tipo 2. Estas unidades tienen sectores de 520 bytes en vez de sectores estándar de 512 bytes. Los 8 bytes adicionales contienen los metadatos de Protection Information descritos en Tabla 12, que se pueden utilizar para verificar los datos en curso y en reposo.

Tabla 12. Metadatos de Protection Information (8 bytes)

Byte #1	Byte #2	Byte #3	Byte #4	Byte #5	Byte #6	Byte #7	Byte #8
Protección de bloque lógico (2 bytes) <ul style="list-style-type: none"> • CRC 16-bits • El receptor calcula los CRC de los datos recibidos y los compara con los CRC recibidos • Protege la porción de datos del sector 		Etiqueta de aplicación de bloque lógico (2 bytes) <ul style="list-style-type: none"> • Debe pertenecer al cliente de la aplicación (iniciador) o servidor del dispositivo (destino) • Comprobado solo por el propietario 		Etiqueta de referencia de bloque lógico (4 bytes) <ul style="list-style-type: none"> • El receptor compara opcionalmente con el valor esperado • Protección ante escenarios de escritura fuera de solicitud o con dirección errónea 			

Este subsistema de almacenamiento DS soporta el esquema de protección host T10PI Type1. Figura 4 en la página 72 muestra dónde se comprueban los metadatos de Protection Information, desde la aplicación en el host a la unidad en el subsistema de almacenamiento.

Protection Information (PI) Check Points

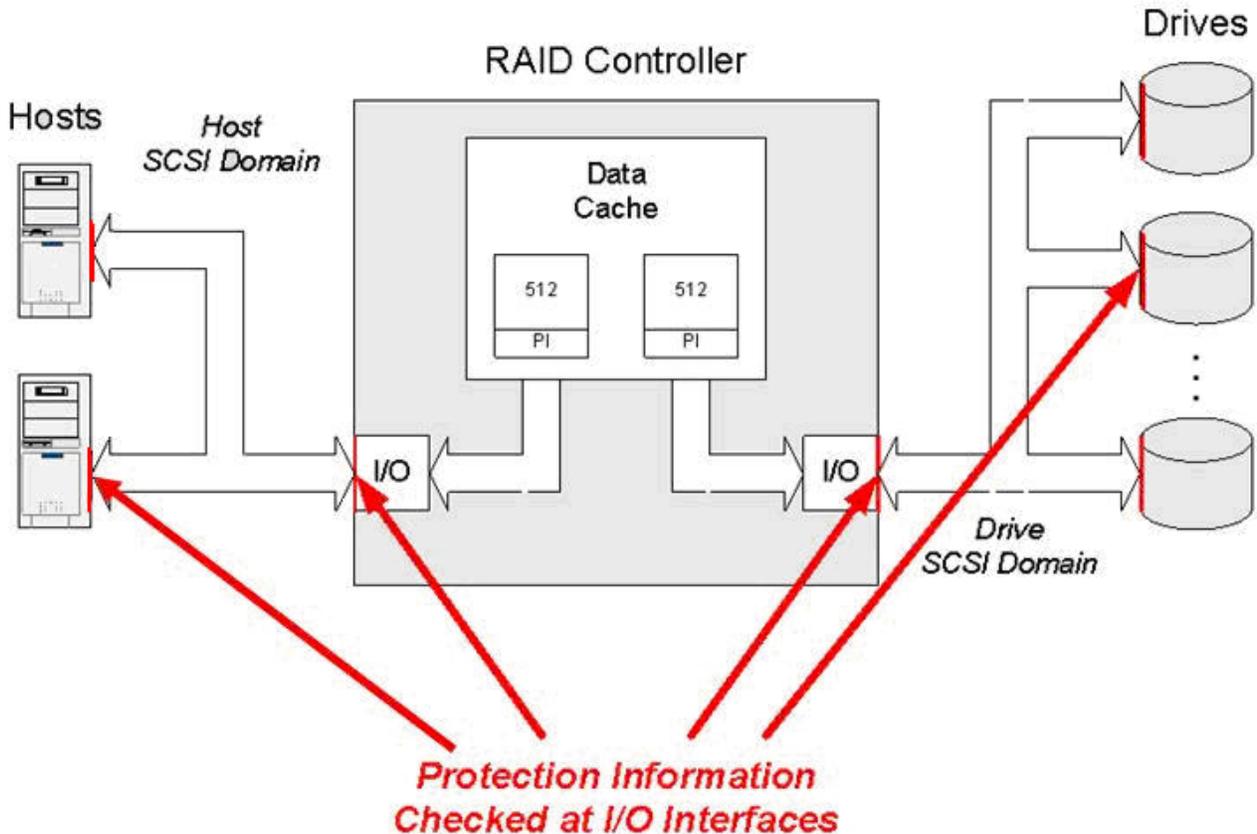


Figura 4. Puntos de comprobación de Protection Information (P)

Reglas para habilitar las funciones T10PI

Para habilitar funciones T10 PI en un subsistema de almacenamiento DS, asegúrese de que se cumplen las condiciones siguientes.

Funcionalidad T10PI soportada por el firmware de controlador

La funcionalidad T10PI es habilitada por el firmware del controlador en vez de por una característica premium. El firmware de controlador que soporta T10PI es 7.77.xx.xx o posterior. Actualmente, sólo los subsistemas DS3950, DS5020, DCS3700 y DS5100/DS5300 tienen soporte para T10 PI. Un subsistema de almacenamiento DCS3700 con Controladores del módulo de rendimiento tiene soporte para T10 PI si el firmware del controlador es 7.83.xx.xx o posterior. Un subsistema de almacenamiento DS3500 es compatible con T10PI si el firmware del controlador es 7.86.xx.xx. Póngase en contacto con su proveedor o representante de IBM para conocer el soporte de T10PI en otros subsistemas de almacenamiento DS en el futuro.

Nota: Las unidades T10PI se pueden utilizar en subsistemas de almacenamiento con un firmware de controlador que no soporte la funcionalidad T10PI. En esos casos, las unidades T10 PI reciben el mismo tratamiento que las unidades sin capacidad T10PI.

Interfaz host de Canal de fibra (FC)

La interfaz de host de Canal de fibra (FC) se debe instalar en el subsistema

de almacenamiento DS. Además, las unidades lógicas con T10PI habilitado deben estar correlacionadas con un puerto de host descubierto a través del puerto de canal de fibra del subsistema de almacenamiento. Por ejemplo, si el controlador tiene instalada la interfaz de host FC, iSCSI o SAS al mismo tiempo, las unidades lógicas con habilitación para T10PI sólo se pueden correlacionar con el puerto de host descubierto por medio del puerto FC. Si intenta correlacionar una unidad lógica con T10PI habilitado con un puerto de host descubierto a través de la interfaz iSCSI se producirá un error.

(Para servidor AIX) Archivo NVSRAM con tipo de host T10PI habilitado

Los archivos NVRAM proporcionados con la versión de firmware de controlador 7.77.xx.xx o posterior deben estar instalados en el subsistema de almacenamiento. Estos archivos NVSRAM deben tener el conjunto de bits de habilitación de T10PI en la región de tipo de host AIX y AIXAVT para ampliar la funcionalidad T10PI al servidor. Sin este conjunto de bits en la región del tipo de host, la funcionalidad T10PI se puede habilitar solo entre el controlador del subsistema y las unidades.

Nota: Consulte el SSIC para obtener información sobre los tipos de adaptadores FC soportados por los controladores de dispositivos, versiones de firmware y versiones de los sistemas operativos AIX necesarios que proporcionan soporte de T10PI en el servidor.

Creación de una matriz con capacidad para T10 PI

Realice los pasos siguientes antes de crear una matriz con capacidad para T10 PI.

1. Pulse **Capacidad total sin configurar**. Se abre la ventana **Crear matriz**.
2. Si está utilizando varios tipos de unidades, seleccione **HDD-SAS** en **Tipo de unidad**.
3. Marque el recuadro de selección **Filtrar selección de unidades para mostrar únicamente las que tienen capacidad para T10 PI (Protección de información)**.
4. Vaya a “Creación de una matriz” en la página 85.

Creación de una agrupación de discos con capacidad para T10 PI

Realice los pasos siguientes antes de crear una agrupación de discos con capacidad para T10 PI.

1. Pulse **Capacidad total sin configurar**.
2. Si está utilizando varios tipos de unidades, seleccione **HDD-SAS** en **Tipo de unidad**.
3. Seleccione **Sólo unidades con capacidad para T10 PI** en **Confirmación de datos**.
4. Vaya a “Creación de una agrupación de discos” en la página 84.

Habilitación e inhabilitación de una matriz RAID con capacidad T10PI

Para crear una matriz RAID con capacidad T10PI, todas las unidades de la matriz RAID deben contar con capacidad T10PI.

Esta tarea presupone que utiliza una interfaz de gestión del subsistema para definir la matriz.

Para habilitar la capacidad T10PI en una matriz RAID:

Nota: Las capturas de pantalla de esta sección son solo ilustrativas y pueden diferir de la interfaz de usuario real dependiendo de la versión de Storage Manager y del firmware del controlador.

- En el diálogo Especificar capacidad/nombre (crear unidad lógica), pulse **Habilitar T10 PI (información de protección) (T10 PI) en la nueva unidad lógica** como se muestra en Figura 5.

Nota: Si crea una unidad lógica sin funcionalidad T10PI, no se podrá convertir en una unidad lógica con capacidad T10PI más tarde.

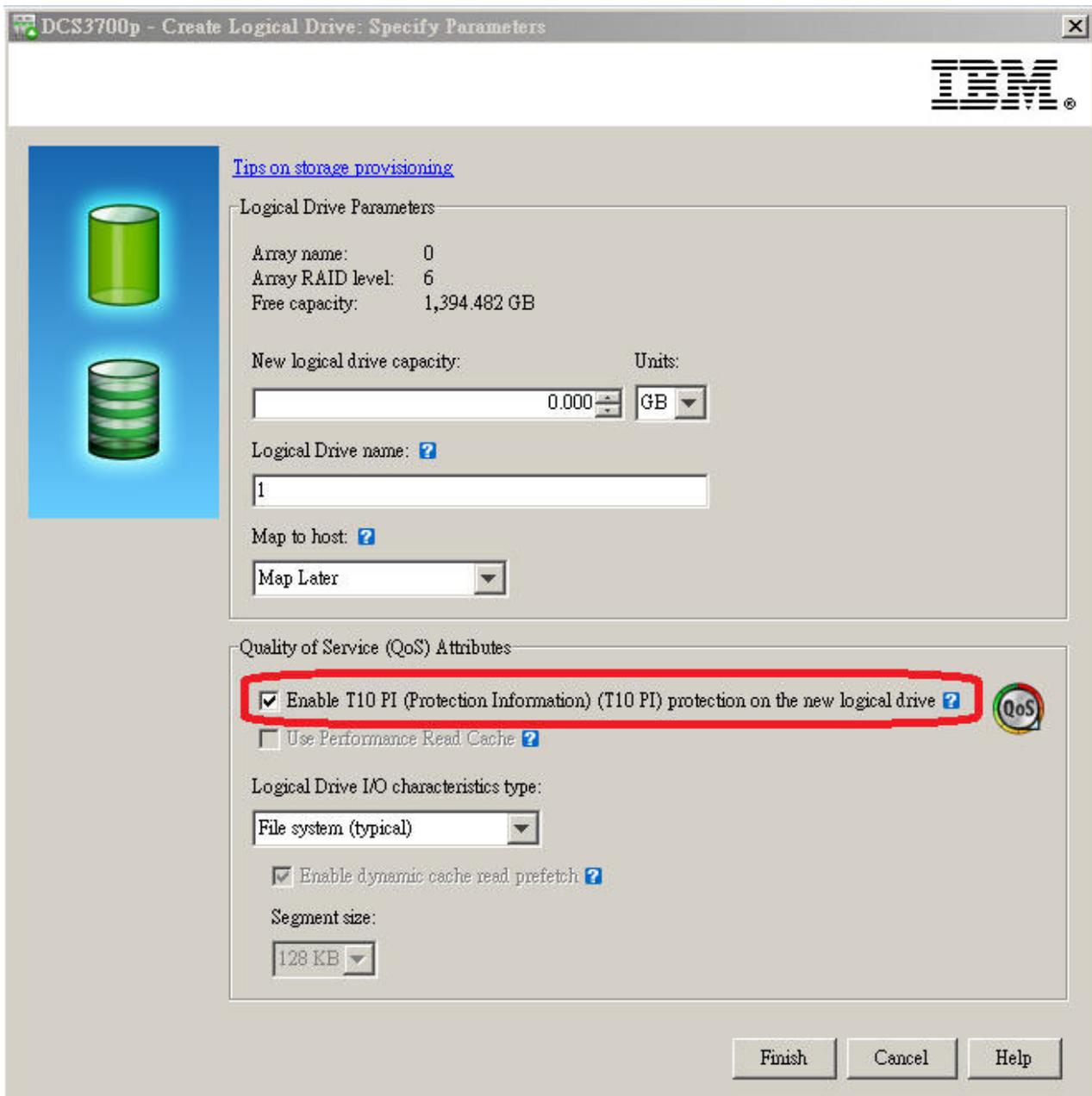


Figura 5. Habilitación de T10 PI en una unidad lógica

Nota: También existe un parámetro adicional en los comandos SMcli adecuados para indicar si una unidad lógica se crea con T10PI habilitado.

Figura 6 en la página 75 muestra una matriz RAID y su unidad lógica con la

funcionalidad T10PI habilitada. El icono en forma de escudo indica que la matriz es una matriz RAID con capacidad T10PI.

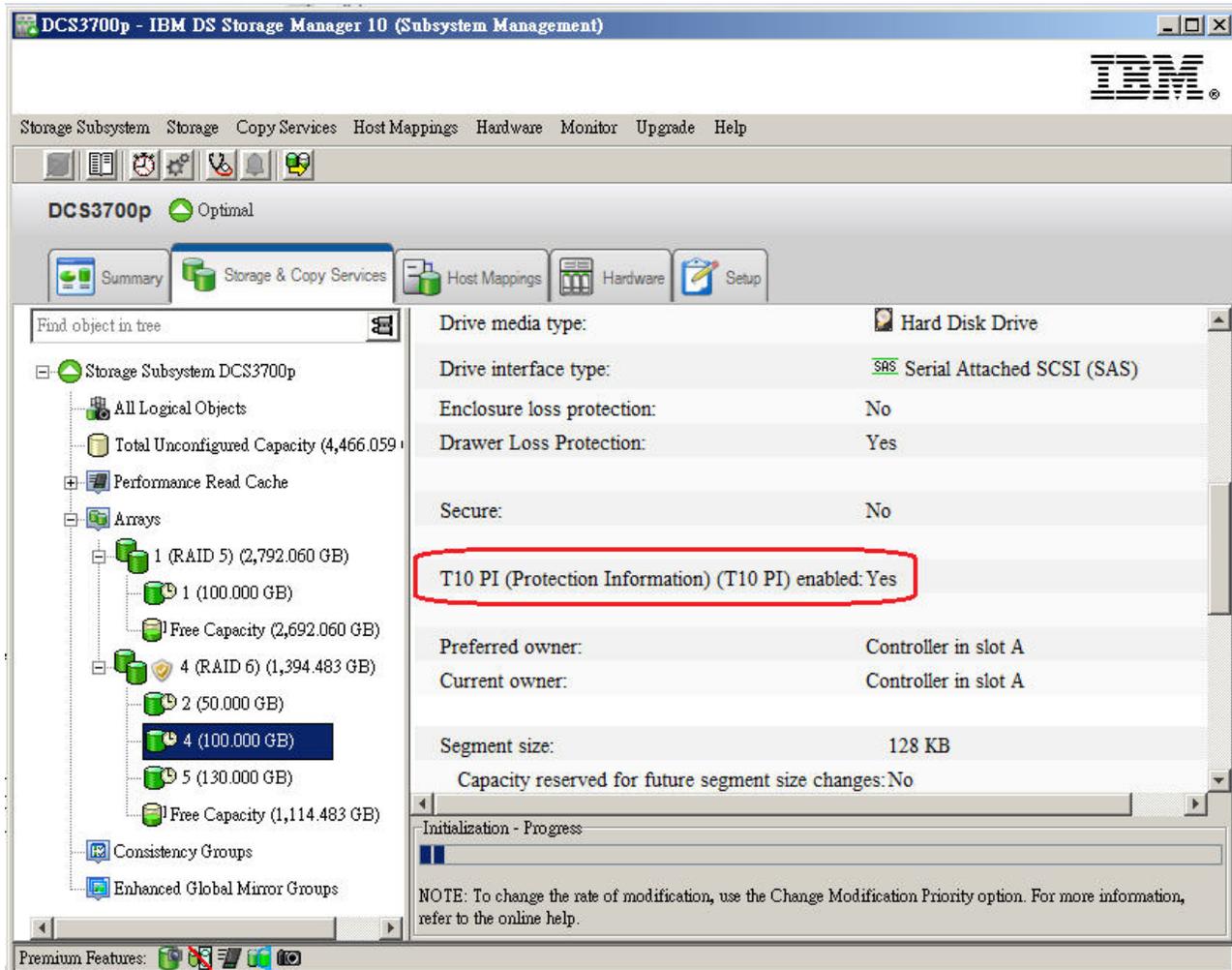


Figura 6. Unidad RAID - Información de protección (T10 PI) - habilitada

Nota: No tiene por qué crear todas las unidades lógicas de una matriz RAID con capacidad T10PI con T10PI habilitada. Por ejemplo, la unidad lógica 4 de la matriz RAID 4 no tiene capacidad T10PI pero las unidades lógicas 2 y 5 tiene capacidad T10PI, como se muestra en Figura 7 en la página 76. No obstante, solo puede habilitar la funcionalidad T10PI en el momento de la creación, se recomienda crear una unidad lógica con T10PI y después inhabilitar esta funcionalidad si fuera necesario.

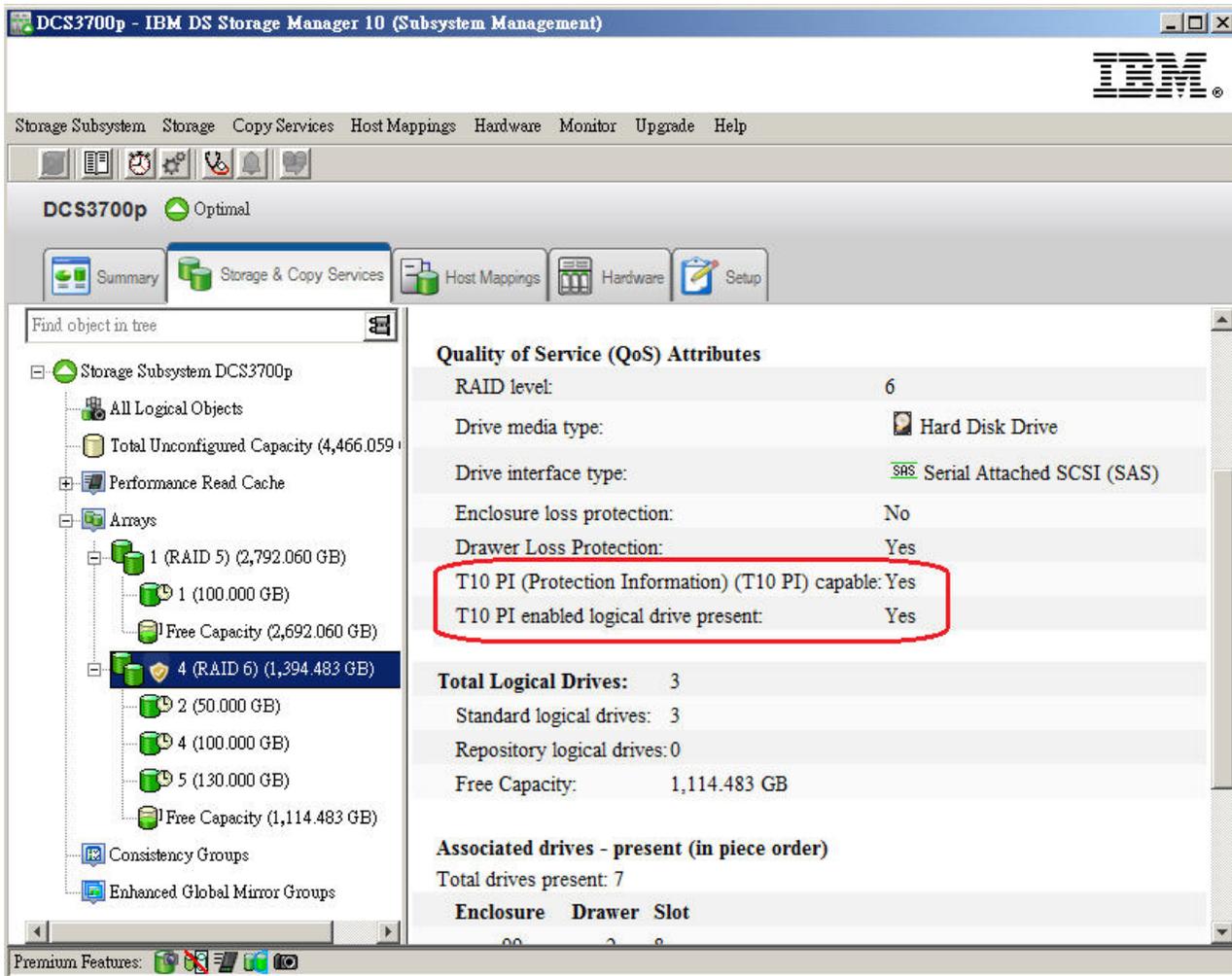


Figura 7. Ejemplo - Unidad lógica 4 de matriz RAID 4 - T10PI no habilitada

Para deshabilitar la capacidad T10PI de una matriz RAID:

- Pulse con el botón derecho en la unidad cuya capacidad T10PI va a deshabilitar y seleccione **Deshabilitar T10PI (Información de protección) (T10PI)** como se muestra en Figura 8 en la página 77.

Notas:

- También existe un comando SMcli para deshabilitar la capacidad T10PI.
- Una vez que deshabilite la capacidad T10PI en una unidad lógica, no podrá volver a habilitar T10 PI en la misma unidad lógica; debe suprimir la unidad y volver a crearla con la capacidad T10PI habilitada.

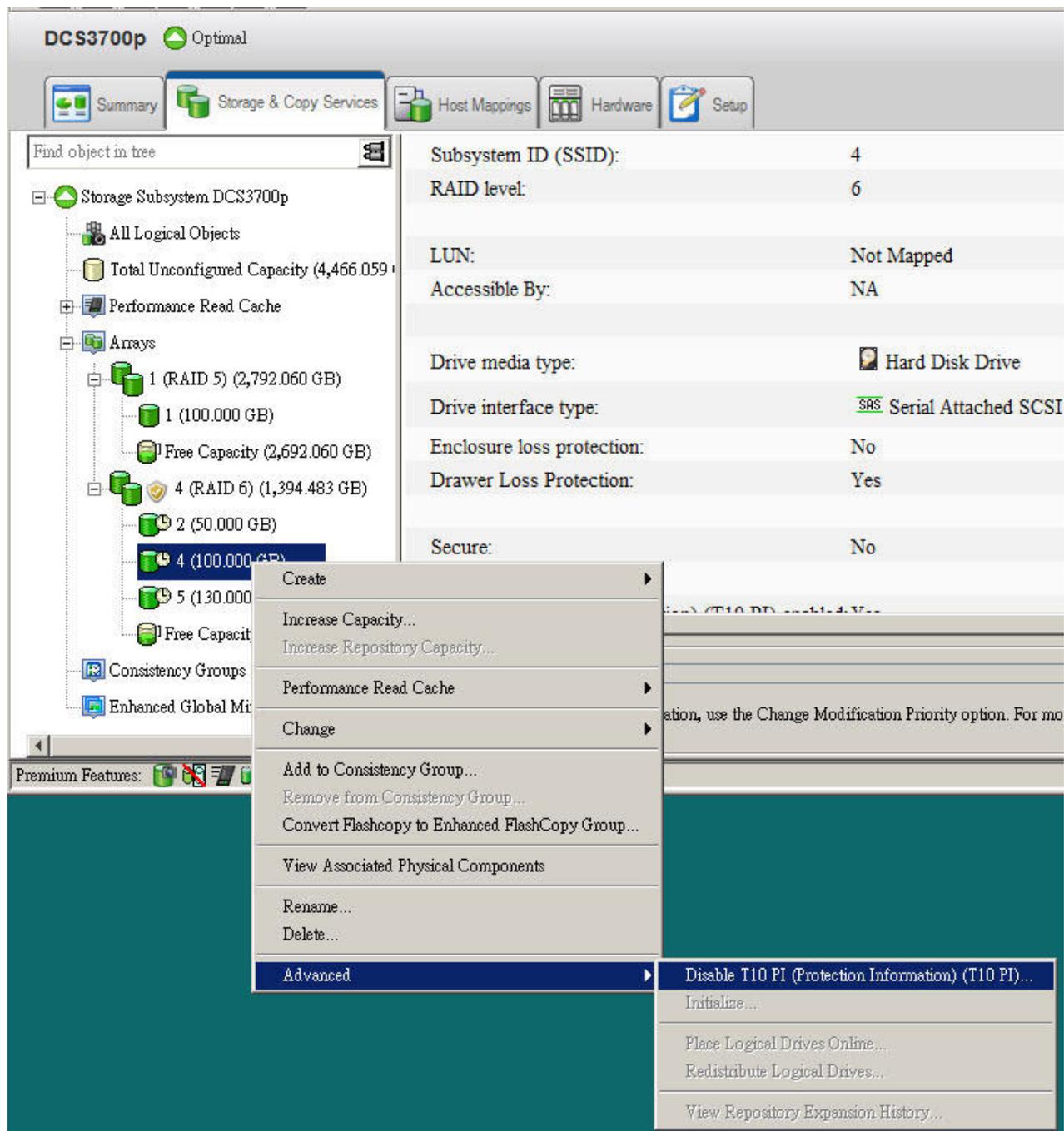


Figura 8. Inhabilitación de T10PI

Atributos del Cifrado de disco completo (FDE)

Las unidades de cifrado de disco completo (FDE) o autocifrado (SED) tienen mecanismos de cifrado incorporados para proteger la información de la unidad del acceso no autorizado desde fuera del subsistema de almacenamiento DS .

La unidad FDE/SED asegurada se bloquea cuando se conecta la alimentación. Desbloquee la unidad enviando la clave de seguridad adecuada desde el controlador a la unidad. Gestione la clave de seguridad a nivel local dentro del

controlador o mediante un gestor de claves externo como IBM Tivoli Key Lifecycle Manager (TKLM). Para mayor seguridad, la unidad se cifra antes de ser grabada, evitando que se exploren los datos de la superficie del disco cuando la unidad falla o se retira del uso activo. La matriz RAID con capacidad FDE/agrupación de discos se muestra con el icono de desbloqueo si la matriz/agrupación de discos no está asegurada y con el icono de bloqueo si la matriz/agrupación de discos está asegurada; como se muestra en la Figura_10. Para obtener más información sobre las unidades de FDE, consulte Capítulo 6, “Trabajo con el Cifrado de disco completo”, en la página 215.

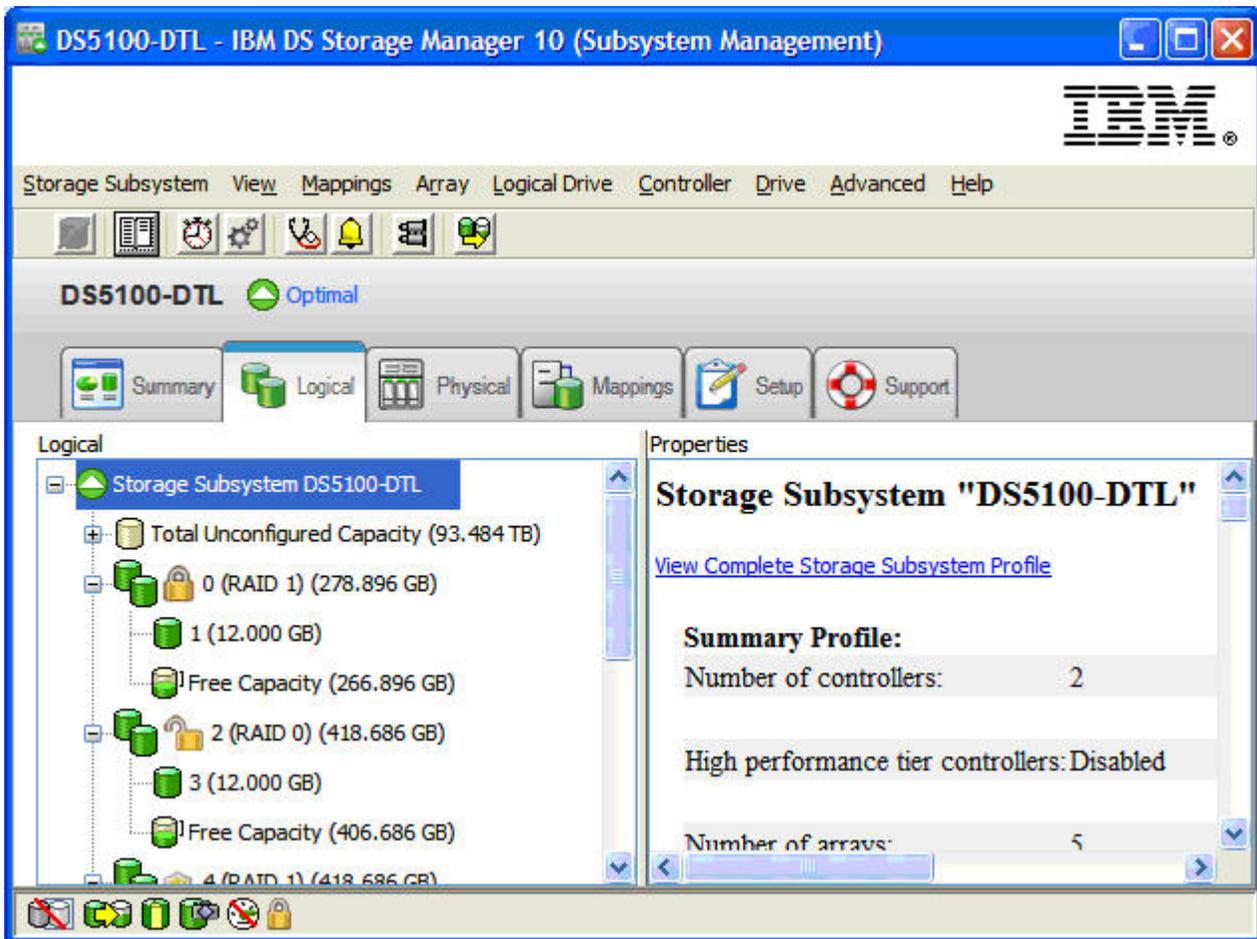


Figura 9. Matriz RAID con capacidad FDE - detalles de seguridad

Configuración de almacenamiento de disco

Puede utilizar IBM DS Storage Manager versión 10.83 con la versión de controlador de firmware 7.83 para configurar una colección de unidades en una agrupación de discos, matriz, o ambos. Las agrupaciones de discos o matrices contienen discos de las mismas o similares características. Las características utilizadas para determinar unidades similares son:

- **Tipo de unidad** — Los tipos de unidad soportados para una matriz son canal de fibra, SATA, FC-SAS o SAS. Una agrupación de discos puede estar formada únicamente por unidades SAS.
- **Tipo de soporte de unidades** — Los soportes de unidades compatibles con una matriz son unidad de disco dura (HDD) o disco de estado sólido (SSD). Una

agrupación de discos puede estar formada únicamente por unidades SAS HDD. Las unidades SAS SSD no son compatibles con las agrupaciones de discos.

Tabla 13. Tipos de unidades que se pueden utilizar en matrices y agrupaciones de discos

Tipo de unidad	Matriz	Agrupación de discos
Disco SAS	Sí	Sí
Disco SAS - T10 PI	Sí	Sí
Disco SAS - SED	Sí	Sí
Disco SATA	Sí	Sí
Disco FC	Sí	No
Disco FC - SED	Sí	No
Disco FC-SAS	Sí	No
SSD	Sí	No

- **Velocidad de rotación** - La velocidad de rotación de las unidades de una agrupación de discos o una matriz debe ser la misma. Es posible crear matrices o agrupaciones de discos con unidades de velocidades de rotación diferentes, pero su configuración no será óptima.

Nota: Desde la interfaz de usuario de Storage Manager no puede crear una agrupación de discos con unidades de la velocidad de rotación diferente. Para crear una agrupación de discos con unidades de velocidad de rotación diferente, tendrá que utilizar un comando SMCLI.

- **Nivel de seguridad** - Si a una agrupación de discos o matriz se le va a asignar un determinado nivel de seguridad, la seguridad de todas las unidades debe ser la misma.
- **Capacidad**— Para utilizar de forma eficaz las unidades de una agrupación de discos o matriz, la capacidad de las unidades debe ser la misma. Si las unidades de una agrupación de discos o una matriz tienen capacidades diferentes, el software de gestión de almacenamiento sólo utiliza una capacidad igual a la de la unidad más pequeña de la agrupación de discos o matriz. Por ejemplo, si la agrupación de discos está formada por varias unidades de 4 GB y 8 GB, DS Storage Manager utilizará hasta 4 GB de cada unidad, dejando 4 GB de las unidades de 8 GB sin utilizar.

Una *matriz* es un conjunto de unidades de canal de fibra, SAS, SATA o unidades de estado sólido que se agrupan de forma lógica para formar una matriz redundante de discos independientes (RAID). Dependiendo de las necesidades, en un sistema de almacenamiento se pueden crear matrices diferentes con distintas características RAID: niveles de RAID, tamaño de segmentos y ancho de fragmento. Las matrices pueden ser estándar o seguras (con cifrado completo de discos).

Una *agrupación de discos* es un método alternativo para organizar discos SAS en unidades de discos lógicas dentro de un subsistema de almacenamiento y presentarlas al host. Las agrupaciones de discos pueden ser estándar o seguras (con cifrado completo de discos). Puede utilizar IBM DS Storage Manager versión 10.83 con la versión de controlador de firmware 7.83 para configurar una colección de unidades en una agrupación de discos, matriz, o ambos. Actualmente, los sistemas de almacenamiento DS3500, DCS3860, DCS3700 y los subsistemas de almacenamiento DCS3700 con controladores del módulo de rendimiento admiten la agrupación de discos, si la versión de firmware del controlador es 7.83 o posterior.

Tabla 14. Soportes de servicios de copia por matriz y agrupación de discos

Servicio de copia	Matriz	Agrupación de discos
Unidad lógica FlashCopy	Sí	No
Enhanced FlashCopy	Sí	Sí
VolumeCopy	Sí	Sí
Duplicación remota	Sí	Sí
Global Mirroring	Sí	Sí

Comparaciones entre agrupación de discos y matriz

Las agrupaciones de discos se diferencian de las matrices en muchos aspectos.

Protección RAID - Una matriz puede crearse utilizando uno de estos niveles RAID: 0, 1, 10, 3, 5 o 6. Los datos y segmentos de paridad se fragmentan en las unidades tal y como indica el nivel RAID. La tabla 14 contiene información sobre el nivel RAID que debe seleccionar para una matriz. En la matriz, el fragmento RAID cubre un segmento en cada una de las unidades que forman la matriz RAID. Entre los LBA de las matrices RAID y la ubicación física de los datos en los discos de la matriz, existe casi una relación directa.

No puede especificar el nivel RAID para una agrupación de discos. Las agrupaciones de discos se dividen en trozos de 4 GB, denominados D-chunks, de espacio de disco. Cada D-chunk está compuesto de fragmentos de 512 MB, denominados D-pieces. Diez D-pieces de un D-chunk deben escribirse en 10 discos diferentes. Si eso no es posible, la agrupación de discos se degrada (si alguna de las diez piezas no se puede escribir en un disco independiente) o falla (si dos o más de las diez piezas no se pueden escribir en un disco independiente). Cada D-pieza está compuesta por 4096 segmentos de 128 KB. Un segmento de cada una de las diez D-pieces forma un fragmento RAID 6 8D+P+Q. En otras palabras, en un D-chunk de 4 GB, los datos y la paridad RAID se almacenan en 4096 fragmentos 8D+P+Q RAID-6. Los datos se almacenan de forma contigua en el fragmento RAID y el D-chunk. Las unidades lógicas de la agrupación de discos se crean con uno o más trozos de 4 GB de espacio de disco. Si hay más de 11 discos en una agrupación de discos, los datos se distribuirán a todas las unidades como múltiplos de trozos de 4 GB. Debido al patrón de asignación de D-chunks en las unidades de disco, no existe una relación clara y directa entre los LBA de la agrupación de discos y la ubicación física de los datos en los discos. Cuantas más unidades tenga una agrupación de discos, más datos se distribuirán entre las unidades.

Características de una matriz RAID - Cuando crea una matriz, puede dictar qué fragmento RAID debe ser, dependiendo del número de unidades de la matriz, el nivel RAID y el tamaño de segmentos de los datos de cada unidad. En algunas aplicaciones, se puede crear una matriz con un fragmento RAID ajustando el tamaño de segmentos y el ancho del fragmento RAID. Esto permite una escritura completa del fragmento al controlador, lo cual puede resultar en un mejor rendimiento de escritura. No obstante, no puede ajustar el tamaño de segmentos y el ancho de fragmento RAID de una agrupación de discos durante la implementación actual. Las agrupaciones de discos se pueden crear con más de las 11 unidades mínimas determinadas. No obstante, los datos RAID distribuidos entre las unidades siempre tendrán la característica RAID 6 8D+P+Q y un tamaño de segmento de 128 KB.

Repuesto en caliente - En caso de que falle una unidad, las matrices utilizan repuestos en caliente globales y dedicados para la reconstrucción de las mismas, mientras que en las agrupaciones de discos, un determinado porcentaje de cada unidad de ellas se reserva para la reconstrucción. Tabla 15 muestra el recuento equivalente de capacidad de las unidades reservada en función del tamaño de las agrupaciones de discos. Entre las ventajas de la capacidad reservada para la reconstrucción o repuesto en caliente se incluyen:

1. *Mejora del tiempo de reconstrucción* - Dado que cada unidad de la agrupación de discos tienen una capacidad reservada para los datos de reconstrucción, todas las unidades de una agrupación de discos se pueden utilizar para escribir datos de reconstrucción. En el caso de las matrices y las unidades de sustitución en caliente, solo hay disponible una unidad para la escritura de datos de reconstrucción, lo cual provoca cuellos de botella durante el proceso de reconstrucción.
2. *Sin unidades en espera*. Se han dado casos en los que las unidades de sustitución en caliente han fallado durante la reconstrucción debido a defectos en el plato de disco u otros defectos de hardware causados por la inactividad de las unidades. Al no dedicar unidades a los datos de reconstrucción, todas las unidades de la agrupación de discos se utilizan en todo momento.
3. *Mejora en el tiempo de copia* Cuando se sustituye la unidad que ha fallado, también mejora el tiempo de copia puesto que todas las unidades participan en la misma. Los segmentos reconstruidos de diversas unidades de la agrupación de discos se recuperan y escriben en las unidades sustituidas. En una matriz, los datos reconstruidos de una unidad se copian de nuevo en la unidad sustituida.

Tabla 15. Capacidad reservada en una agrupación de discos

Número de unidades de una agrupación de discos	Número de unidades reservadas
11	1
12-31	2
32-63	3
64-127	4
128-191	6
192	7

Eficiencia de almacenamiento - Si una matriz se divide en diversas unidades lógicas, a cada unidad lógica se le asigna una porción fija de la matriz. La capacidad no utilizada de algunas unidades lógicas no se puede utilizar como capacidad adicional en otras unidades lógicas o para crear nuevas unidades lógicas. Las unidades lógicas de una agrupación de discos se gestionan juntas. No hay asignación fija de capacidad para cada unidad lógica. Esto permite que una unidad lógica utilice su porción de la agrupación de discos y ofrezca toda la capacidad no utilizada de la agrupación a unidades lógicas de una agrupación que la necesite o para crear unidades lógicas adicionales. Si una matriz se divide en diversas unidades lógicas, a cada unidad lógica se le asigna una porción fija de la matriz. El tamaño de la unidad lógica se puede aumentar según sea necesario si hay espacio disponible en la matriz. No obstante, la capacidad sin utilizar de una unidad lógica no se puede liberar para la creación de nuevas unidades lógicas o como capacidad adicional para otra unidad lógica de la matriz. La única forma de liberar espacio en una unidad lógica existente es realizar una copia de seguridad de los datos de la misma, suprimir la unidad lógica, volver a crearla con una

capacidad menor y restaurar los datos copiados en dicha unidad menor. Si una agrupación de discos se divide en unidades lógicas, estas se pueden crear como unidades lógicas ligeras, a las cuales solo se les asigna físicamente una fracción del disco duro de la agrupación de discos en el momento de su creación. A medida que la unidad lógica necesita más espacio físico, se le asignará espacio de la capacidad libre de la agrupación de discos en D-chunks de 4 GB, garantizando la provisión adecuada a la unidad lógica sin dejar capacidad sin utilizar.

Tabla 16. Lista de características soportadas en una matriz o agrupación de discos.

Características	Matriz	Agrupación de discos
Protección de pérdida de alojamiento	Sí ¹	Sí ²
Protección de pérdida de cajón	Sí ¹	Sí ²
Expansión de unidad lógica dinámica	Sí	Sí
Expansión de matriz/agrupación de discos dinámica	Sí	Sí
Suministro ligero	No	Sí

Nota:

1. El número máximo de unidades de una matriz para la protección de pérdida de cajón o alojamiento depende del nivel RAID de la matriz. Para RAID 1, 10, 3 y 5 matrices, es decir una unidad por alojamiento o cajón, y para matrices de RAID 6 dos unidades por alojamiento o cajón.
2. El número máximo de unidades de una agrupación de discos por alojamiento o cajón para la protección de pérdida de cajón o alojamiento es de 2.

Unidades lógicas

En una agrupación de discos o matriz, las unidades se organizan en unidades lógicas. Una unidad lógica es un componente lógico que un host utiliza para organizar el almacenamiento de datos en un subsistema de almacenamiento. El sistema operativo del host ve una unidad lógica como una sola unidad aunque los datos se escriben en varias unidades físicas de la agrupación de discos o matriz. A cada unidad lógica se le asigna un número de unidad lógica (LUN) que el host utiliza para acceder a la misma. Un host asociado a un subsistema de almacenamiento escribe datos en las unidades lógicas y lee datos de las unidades lógicas. Las unidades lógicas no pueden extenderse a lo largo de múltiples agrupaciones de discos o matrices. Una agrupación de discos o matriz puede tener una o varias unidades lógicas, dependiendo de las necesidades. Además, no existe un límite en el tamaño de las unidades lógica de una matriz. Pueden ser tan grandes como la propia matriz. No obstante, en la implementación actual de la agrupación de discos, el tamaño máximo de las unidades lógicas que se pueden crear en una agrupación de discos es de 64 TB. Póngase en contacto con los vendedores o representantes de IBM para cambiar este límite.

Con la versión de firmware del controlador 7.83 y posterior, en un subsistema de almacenamiento IBM DS compatible con las agrupaciones de discos, puede crear un nuevo tipo de unidad lógica a la que se denomina "volumen ligero" o "unidad lógica ligera". Las unidades lógicas ligeras, que se pueden crear con la asignación de disco física real, solo ocupan un porcentaje del tamaño de la unidad lógica. La

unidad lógica se presenta al host como disco con capacidad total. La asignación física de disco real aumentará en asignaciones múltiplo de 4 GB según sea necesario. Una alerta de nivel de uso se muestra cuando el uso del repositorio alcanza un cierto nivel. El usuario puede configurar capacidad adicional como sea necesario. Puede crear una unidad lógica estándar en una agrupación de discos o matriz. No obstante, las unidades lógicas ligeras solo se pueden crear en las agrupaciones de discos. La provisión ligera es la capacidad de crear unidades lógicas ligeras en el subsistema. Esto se facilita de manera gratuita con la versión necesaria del firmware del controlador de su subsistema de almacenamiento IBM DS. Actualmente, solo los subsistemas de almacenamiento DS3500 y DCS3700, y los subsistemas de almacenamiento DCS3700 con los Controladores del módulo de rendimiento admiten el aprovisionamiento liviano.

Cuando crea una unidad lógica estándar, asigna el almacenamiento disponible, configurando la capacidad de una unidad lógica estándar para satisfacer las necesidades de las aplicaciones en cuanto a disponibilidad de datos y rendimiento de E/S. Para aumentar el almacenamiento disponible para escrituras de datos de E/S, debe añadir unidades adicionales a la agrupación de discos o matriz. Las unidades lógicas ligeras le permiten crear unidades lógicas virtuales grandes con asignaciones de almacenamiento físico pequeñas, que se pueden aumentar con el tiempo para satisfacer la demanda de capacidad creciente. A medida que aumenta la necesidad de almacenamiento, puede aumentar la cantidad de capacidad de almacenamiento físico según sea necesario. El uso de unidades lógicas ligeras le ayuda a reducir la posibilidad de tener un exceso de capacidad sin utilizar en la agrupación de discos.

Las unidades lógicas ligeras son unidades lógicas con una gran capacidad virtual disponible para la escritura de datos de E/S del host, pero no toda su capacidad virtual se asocia con la capacidad física asignada. Al configurar una unidad lógica ligera, debe especificar dos tipos de capacidad: la capacidad virtual y la capacidad preferida/física. La capacidad virtual es la capacidad que se indica al host. El valor mínimo que puede especificar para la capacidad virtual es de 32 MB, el máximo es de 64 TB. La capacidad física (también denominada capacidad provista y capacidad preferida) es la cantidad de espacio en el disco físico que actualmente asignada para la escritura de datos. Los administradores pueden aumentar la capacidad física a medida que aumenta la demanda. Puede aumentar la capacidad física manual o automáticamente especificando el tamaño máximo de la capacidad física. El controlador incrementará de manera automática la capacidad física que necesita en incrementos de 4 GB. Si selecciona el método manual, el valor mínimo que puede especificar para la capacidad física es 4 GB; el máximo es 64 TB. Debe especificar la capacidad física en incrementos de 4 GB. IBM DS Storage Manager traduce la capacidad física especificada en porcentaje de capacidad virtual asignada a la unidad lógica ligera. Normalmente, la capacidad física asignada es mucho menor que la cantidad especificada para la capacidad virtual al crear la unidad lógica ligera. El aumento automático de la capacidad física es el método más utilizado.

Cuando se crea la unidad lógica ligera, también se crea una unidad lógica de repositorio para ella. El tamaño inicial de la unidad lógica de repositorio es la capacidad preferida en el asistente "crear la unidad lógica". La capacidad preferida predeterminada de la unidad lógica de repositorio es 4 GB. El administrador puede configurar dos atributos como ayuda para supervisar el uso de la capacidad de la unidad lógica de repositorio y evitar el fallo de una solicitud de escritura del host debido a una insuficiencia de la capacidad. El administrador puede definir un porcentaje de umbral de aviso de uso de la unidad lógica de repositorio para IBM DS Storage Manager con el fin de generar una alerta cuando se haya utilizado el

porcentaje de capacidad especificado. Para permitir que el subsistema amplíe de forma automática la capacidad provista en una cantidad especificada cuando se alcance el umbral de alerta de uso del repositorio, el administrador especifica un valor máximo de expansión para la política de expansión automática.

Existen algunas diferencias entre las unidades lógicas estándar y las unidades lógicas ligeras:

- **Nivel RAID** — El nivel RAID de una agrupación de discos o matriz determina cómo y dónde se distribuyen los datos redundantes en las unidades lógicas. El software de gestión de almacenamiento asigna automáticamente 10+P+Q RAID 6 a todas las unidades lógicas de una agrupación de discos. Para las unidades lógicas de una matriz, el software de gestión de almacenamiento le permite elegir el tipo de RAID. Puede crear una unidad lógica estándar en una agrupación de discos o en una matriz. No obstante, las unidades lógicas ligeras solo pueden crearse en una agrupación de discos.
- **Asignación de capacidad** — En una unidad lógica estándar puede asignar la capacidad de almacenamiento disponible de manera anticipada. En las unidades lógicas ligeras especifica una capacidad virtual y una capacidad preferida, y aumenta la capacidad física para satisfacer las necesidades reales de capacidad con el tiempo.
- **Expansión de capacidad** — Puede aumentar la capacidad de una unidad lógica estándar en incrementos de cualquier tipo. Para las unidades lógicas ligeras debe asignar la capacidad en incrementos de 4 GB, ya que las agrupaciones de discos se crean en espacio de disco con capacidad múltiplo de 4 GB.
- **Uso de repuestos en caliente** — Puede designar una unidad de repuesto en caliente para las unidades lógicas de una matriz para utilizarla en la recuperación en caso de fallo de una unidad. Los repuestos en caliente no se utilizan en las agrupaciones de discos. En estas, se reserva un porcentaje de cada unidad de disco de la misma para datos de reconstrucción, que se utilizarán en caso de fallo de una unidad.

Creación de una agrupación de discos

Para crear una agrupación de discos a partir de nodos de capacidad sin configurar, siga los pasos indicados a continuación en la ventana Gestión del subsistema:

Nota: En un subsistema DCS3700 con Controladores del módulo de rendimiento, las unidades 2 TB NL-SAS no tienen soporte para T10 PI. Por lo tanto, debe crear manualmente la agrupación de discos, si está utilizando dichas unidades. Esto evita la habilitación de T10 PI. Para crear manualmente una agrupación de discos, pulse **No** en la ventana **Configuración automática de agrupación de discos**.

1. Para crear una agrupación de discos, realice una de las acciones siguientes:
 - En la pestaña Servicio de almacenamiento y copia, pulse el botón derecho del ratón sobre **Capacidad sin configurar (HDD, SAS)** y seleccione **Crear agrupación de discos**.
 - En la pestaña Servicios de almacenamiento y copia, seleccione **Capacidad total sin configurar** y, en la ventana de gestión de subsistema, seleccione **Almacenamiento > Agrupación de discos > Crear**.

Se abrirá la ventana Crear agrupación de discos.

2. Introduzca un nuevo nombre para la agrupación de discos en **Nombre de la agrupación de discos** y seleccione la agrupación de discos deseada de la lista.
3. Seleccione **Crear agrupación de discos segura** si así lo desea.

Nota: Solo puede crear una agrupación de discos segura si tiene unidades FDE y la característica premium FDE habilitada.

4. Pulse **Ver los valores de notificación**. Podrá ver y cambiar los umbrales de notificación de aviso temprano y aviso crítico.
5. Pulse **Crear**. Espere hasta que se haya creado la agrupación de discos.

Al abrirse la ventana **Gestión del subsistema** o al suprimir una unidad lógica, agrupación de discos o matriz, la ventana **Configuración automática de agrupación de discos** emergerá si -

- No ha creado una agrupación de discos y tiene unidades sin asignar en el subsistema.
- No ha creado una agrupación de discos y tiene unidades sin asignar en el subsistema del mismo tipo que en la agrupación de discos.
- Ha creado diversas agrupaciones de discos y tiene unidades sin asignar en el subsistema del mismo tipo que en la agrupación de discos.

Adición de capacidad a una agrupación de discos existente

Puede añadir capacidad a una agrupación de discos existente. En la pestaña Servicios de copia y almacenamiento, seleccione la agrupación de discos a la que desea añadir capacidad y realice una de las acciones siguientes:

- Seleccione **Almacenamiento > Agrupación de discos > Añadir unidades** en la ventana de gestión del subsistema.
- Pulse el botón derecho del ratón sobre la agrupación de discos a la que quiere añadir unidades y seleccione **Añadir unidades**.

Cambio de la configuración de una agrupación de discos

Puede cambiar los umbrales de notificación de aviso temprano y aviso crítico, la prioridad de reconstrucción y la capacidad de conservación de una agrupación de discos existente. En la pestaña Servicios de copia y almacenamiento, seleccione la agrupación de discos y realice una de las acciones siguientes:

- Seleccione **Almacenamiento > Agrupación de discos > Cambiar > Configuración** en la ventana de gestión del subsistema.
- Pulse el botón derecho del ratón sobre la agrupación de discos para la que quiere cambiar la configuración y seleccione **Cambiar > Configuración**.

Se abrirá la ventana **Cambiar configuración de agrupación de discos**. Puede aumentar o disminuir el umbral de aviso temprano y aviso crítico, que es un porcentaje de la capacidad de la agrupación de discos. Deslice la regla para modificar la prioridad de reconstrucción degradada, la prioridad de reconstrucción crítica y la prioridad de operación de fondo.

Pulse **Aceptar** para guardar los valores.

Creación de una matriz

Para crear una matriz a partir de nodos de capacidad sin configurar, siga los pasos indicado a continuación en la ventana Gestión de subsistema:

1. Utilice cualquiera de los dos métodos siguientes para crear una nueva matriz:
 - Seleccione **Capacidad total sin configurar** y pulse **Matriz > Crear**.
 - Seleccione y pulse con el botón derecho en **Capacidad total sin configurar** y pulse **Crear matriz**.

Se abrirá la ventana Introducción (Crear matriz).

2. Pulse **Siguiente**. Se abrirá la ventana Nombre de matriz y Selección de unidad (Crear matriz).

Nota: Si está utilizando unidades 2 TB NL-SAS en un subsistema de almacenamiento DCS3700 con Controladores del módulo de rendimiento, seleccione **Manual** para **Selección de unidad**.

3. Realice la acción aplicable para los siguientes campos:
 - **Nombre de matriz:** Escriba un nombre para la nueva matriz. El nombre puede tener un máximo de 30 caracteres.
 - **Selección de unidad:** Seleccione **Automática** o **Manual (Avanzada)**.

Automática

Elija en una lista de opciones de capacidad y unidades generada automáticamente. Esta opción está preseleccionada de manera predeterminada.

Manual (Avanzada)

Elija unidades específicas para obtener capacidad para la nueva matriz.

- Pulse **Siguiente**. Se abrirá la ventana Nivel de RAID y capacidad (Crear matriz).
4. especifique el nivel de RAID (protección de redundancia).
 5. Seleccione el número de unidades (capacidad general) para la nueva matriz.
 6. Pulse **Finalizar**. Se abrirá la ventana Matriz creada.
 7. Si desea continuar con el proceso para crear una unidad lógica, pulse **Sí**; si desea esperar para crear una unidad lógica en otro momento, pulse **No**.

Matriz redundante de discos independientes (RAID)

La Matriz redundante de discos independientes (RAID) está disponible en todos los sistemas operativos y se basa en una serie de configuraciones, denominadas *niveles*, para determinar como se escriben y recuperan los datos del usuario y de redundancia de las unidades. El firmware de controlador del subsistema de almacenamiento soporta seis niveles de configuración RAID:

- RAID-0
- RAID-1
- RAID-3
- RAID-5
- RAID-6
- RAID-10

Cada nivel ofrece un rendimiento y características de protección diferentes. RAID-1, RAID-3, RAID-5 y RAID-6 escriben los datos de redundancia en el soporte de unidad para tolerancia al error. Los datos de redundancia pueden ser una copia de los datos (duplicados) o un código de corrección de error derivado de los datos. Si falla una unidad, los datos de redundancia se almacenan en una unidad diferente a la de los datos que protegen. Los datos de redundancia se utilizan para reconstruir la información de la unidad en una unidad de repuesto en caliente. RAID-1 utiliza la duplicación para la redundancia. RAID-3, RAID-5 y RAID-6 utilizan la información de redundancia, denominada en ocasiones *paridad*, construida a partir de bytes de datos y unida a los datos en cada disco.

Tabla 17. Descripciones de nivel RAID

Nivel RAID	Breve descripción	Descripción detallada
RAID-0 Nota: RAID-0 no proporciona redundancia de datos.	No redundante, modo de escritura en bandas	RAID-0 ofrece simplicidad, pero no proporciona redundancia de datos. Una matriz RAID-0 dispersa los datos en todas las unidades de la matriz. Normalmente esto proporciona el mejor rendimiento, pero no existe protección ante errores de una unidad individual. Si una unidad de la matriz falla, fallarán todas las unidades lógicas de dicha matriz. Este nivel de RAID no se debe utilizar para necesidades altas de disponibilidad de los datos. RAID-0 es más adecuado para datos no fundamentales.
RAID-1 o RAID-10	Modo de duplicación/ escritura en bandas	<ul style="list-style-type: none"> • Para RAID-1 se necesitan un mínimo de dos unidades: una para los datos del usuario y otra para los datos duplicados. La implementación por parte de subsistemas de almacenamiento DS3000, DS4000 o DS5000 de RAID-1 es una combinación de RAID-1 y RAID-10, dependiendo del número de unidades seleccionadas. Si solo se seleccionan dos unidades, se implementa RAID-1. Si selecciona cuatro o más unidades (en múltiplos de dos), se configura automáticamente RAID 10 en la matriz; dos unidades se dedican a los datos del usuario y otras dos a los datos duplicados. • RAID-1 proporciona un alto rendimiento y la mejor disponibilidad de datos. En una unidad lógica RAID-1, los datos se escriben en dos discos duplicados simultáneamente. En una unidad lógica RAID-10, los dtos se escriben en bandas en los pares duplicados. • RAID-1 utiliza la duplicación del disco para realizar una copia exacta de una unidad en otra unidad. Si falla una unidad en una matriz RAID-1, la unidad duplicada se hace cargo. • RAID-1 y RAID-10 son costosos en cuanto a capacidad. La mitad de las unidades se utiliza para datos redundantes.
RAID-3	Modo de ancho de banda alto	<ul style="list-style-type: none"> • RAID-3 requiere un disco dedicado en la unidad lógica para conservar la información de redundancia (paridad). Los datos del usuario se escriben en bandas en las unidades restantes. • RAID-3 es una buena opción para aplicaciones multimedia o de imágenes médicas que escriben y leen grandes cantidades de datos secuenciales. En estas aplicaciones, el tamaño de E/S es grande y todas las unidades operan en paralelo para hacerse cargo de una única solicitud, ofreciendo una gran velocidad de transferencia de E/S.

Tabla 17. Descripciones de nivel RAID (continuación)

Nivel RAID	Breve descripción	Descripción detallada
RAID-5	Modo de E/S alta	<ul style="list-style-type: none"> • RAID-5 escribe en bandas tanto los datos del usuario como la información de redundancia (paridad) en todas las unidades de la unidad lógica. • RAID-5 utiliza el equivalente de la capacidad de una unidad para la información de redundancia. • RAID-5 es una buena opción para entornos multi-usuario como bases de datos o almacenamientos de sistemas de archivos, donde el tamaño de E/S es pequeño y hay una alta proporción de actividad de lectura. Cuando el tamaño de E/S es pequeño y el tamaño de segmento se elige adecuadamente, se recupera una sola solicitud de lectura de una sola unidad individual. El resto de unidades están disponibles para encargarse simultáneamente a otras solicitudes de lectura de E/S y ofrecer grandes velocidades de solicitud de E/S.
RAID-6	Escritura en bandas a nivel de bloque con paridad dual distribuida	<p>RAID-6 es una evolución de RAID-5 y está diseñado para tolerar dos errores de unidad de disco simultáneos almacenando dos conjuntos de paridades distribuidas:</p> <ul style="list-style-type: none"> • RAID Nivel 6 utiliza el equivalente de la capacidad de dos unidades (de una matriz) para los datos de redundancia. • RAID Nivel 6 protege contra errores simultáneos de dos unidades almacenando dos conjuntos de paridades distribuidas. <p>Nota: No todos los subsistemas de almacenamiento DS soportan RAID-6. Compruebe la carta de anuncio de la <i>Installation, User's, and Maintenance Guide</i> de su subsistema de almacenamiento para determinar si este soporta RAID-6 y la versión mínima de firmware de controlador requerida.</p>

Nota: Una matriz utiliza un nivel RAID único, y todos los datos de redundancia de esa matriz se almacenan en la matriz.

La capacidad de la matriz es la capacidad agregada de las unidades que la forman, menos la capacidad reservada a los datos de redundancia. La cantidad de capacidad necesaria para los datos de redundancia depende del nivel RAID utilizado.

Para comprobar la redundancia, pulse **Avanzado > Recuperación > Comprobar redundancia de matriz**. La comprobación de redundancia lleva a cabo una de las acciones siguientes:

- Explora los bloques de una unidad lógica RAID-3, RAID-5 o RAID-6 y comprueba la información de redundancia de cada bloque
- Compara los bloques de datos en unidad duplicadas RAID-1

Importante: Cuando selecciona **Comprobar redundancia de matriz**, se abre un mensaje informándole de utilizar la opción solo cuando así se lo indique el Recovery Guru. También le informa de que si desea comprobar la redundancia para fines distintos a la recuperación, puede habilitar la comprobación de la misma a través de Media Scan.

Creación de una unidad lógica estándar

Una *unidad lógica estándar* es una estructura lógica y básica que crea para almacenar datos en el subsistema de almacenamiento. El sistema operativo reconoce una unidad lógica como si fuera una única unidad. Puede crear una unidad lógica desde una matriz. Elija un nivel de RAID para satisfacer las necesidades de disponibilidad de datos de sus aplicaciones y para maximizar el rendimiento de E/S de canal de fibra si ha creado una unidad lógica de una matriz.

Nota: En las configuraciones de clúster, si añade o suprime unidades lógicas, debe hacer que los nodos A y B las reconozcan.

Para crear una una unidad lógica, siga los pasos indicados a continuación en la ventana Gestión de subsistema:

1. En la página Lógica o Física de la ventana Introducción (Crear unidad lógica), pulse **Capacidad libre** en la matriz o agrupación de discos para la que desea crear una nueva unidad lógica, pulse con el botón derecho en la matriz o agrupación de discos, y pulse **Crear unidad lógica**.
2. En la ventana Especificar capacidad/nombre (Crear unidad lógica), especifique los siguientes parámetros para la unidad lógica que desea crear:

Nueva capacidad de la unidad lógica

La capacidad puede ser toda la capacidad sin configurar de una matriz o una porción de la capacidad de la matriz.

Unidades

Seleccione GB, MB o TB, dependiendo de la capacidad disponible.

Nombre

Escriba un nombre único para el subsistema de almacenamiento, con un máximo de 30 caracteres.

3. En la ventana “Parámetros avanzados de unidad lógica”, especifique las características de E/S aplicables (tipo de características, tamaño de segmento y multiplicador de lectura en caché) y pulse **Siguiente**. Se abrirá la ventana Especificar correlación unidad lógica a LUN (Crear unidad lógica).

Nota: Los valores de las características de E/S se pueden definir automáticamente o especificarse de forma manual, de acuerdo con uno de los usos de unidad lógica siguientes: sistema de archivos, base de datos o multimedia.

4. En la ventana Especificar correlación unidad lógica a LUN (Crear unidad lógica), especifique la correlación de unidad lógica a LUN.

La preferencia de correlación de unidad lógica a LUN puede ser una de las siguientes:

Correlación predeterminada

El valor automático especifica la asignación automática de un LUN a la unidad lógica, utilizando el siguiente LUN disponible en el grupo host predeterminado. Este valor concede acceso de la unidad lógica a grupos host o sistemas principales que no tienen correlaciones de unidad lógica a LUN específicas (las designadas por el nodo de grupo

host predeterminado en la vista Topología). Si la característica Partición de almacenamiento no está habilitada, debe especificar el valor Automático. Además, puede cambiar el tipo de host para que se adapte al sistema operativo de host.

Correlación posterior utilizando la vista Correlaciones

Este valor especifica que no va a asignar un LUN a la unidad lógica durante la creación. Este valor le permite definir una correlación unidad lógica a LUN específica y crear particiones de almacenamiento utilizando la opción **Correlaciones definidas**. Especifique este valor cuando habilite la partición del almacenamiento.

5. Pulse **Finalizar** para crear la unidad lógica. Se abrirá la ventana Creación correcta (Crear unidad lógica).
6. Si quiere crear otra unidad lógica, pulse **Sí** en la ventana Creación correcta (Crear unidad lógica) y siga con el paso 9; de lo contrario, pulse **No**. Cuando se abra la ventana Una vez completado (Crear unidad lógica), pulse **Aceptar**, y continúe con el paso 10.
7. En la ventana Asignar capacidad (Crear unidad lógica), elija la creación de la nueva unidad lógica en la capacidad libre de la misma matriz, la capacidad libre de una matriz diferente o capacidad sin configurar (crear una nueva matriz). Repita el proceso, comenzando por el paso 1. Se abrirá la ventana Completado (Crear unidad lógica).
8. Pulse **Aceptar**.
9. Registre la unidad lógica en el sistema operativo.

Tras crear las unidades lógicas con correlaciones unidad lógica a LUN automáticas, siga las instrucciones aplicables para su sistema operativo indicadas en "Identificación de dispositivos" en la página 179 para descubrir la nueva unidad lógica.

Creación de una unidad lógica ligera

Para crear una unidad lógica ligera en un subsistema de almacenamiento DS3500, DCS3700, o un subsistema de almacenamiento DCS3700 con controladores del módulo de rendimiento que cuentan con el firmware del controlador 7.8x.xx.xx o posterior:

1. Realice una de las acciones siguientes:
 - Pulse con el botón derecho en un nodo de capacidad libre de la agrupación de discos y seleccione **Crear unidad lógica**.
 - Seleccione un nodo de capacidad libre de la agrupación de discos y a continuación **Almacenamiento > Crear > Unidad lógica** en el menú principal.

Se abrirá la ventana **Crear unidad lógica: Especificar parámetros**.

2. Tras ponerle nombre y especificar la capacidad inicial, seleccione el recuadro de selección **Crear unidad lógica ligera** para crear la unidad lógica.

Nota: En una unidad lógica ligera, la memoria caché de lectura dinámica no está disponible.

3. Pulse **Siguiente**. Se abrirá la ventana **Crear unidad lógica: Elegir capacidad física**.
4. Para crear una unidad lógica ligera con los valores predeterminados, pulse **Finalizar**. Para cambiar cualquiera de los valores predeterminados, seleccione **Personalizar valores de capacidad (avanzado)** y pulse **Siguiente**. Se abrirá la ventana **Crear unidad lógica: Personalizar valores**.

5. Puede elegir su propia capacidad de expansión preferida, capacidad de expansión máxima y umbral de aviso de uso. Pulse **Finalizar**.

Ha creado una unidad lógica ligera.

Acerca de Dynamic Capacity Expansion

Dynamic Capacity Expansion (DCE) es una operación de modificación en el software de gestión de almacenamiento que aumenta la capacidad de una matriz o una agrupación de discos. Esta operación de modificación le permite agregar unidades sin asignar a una matriz o agrupación de discos. La adición de unidades sin asignar incrementa la capacidad libre en la matriz o la agrupación de discos. Puede utilizar esta capacidad para crear unidades lógicas adicionales o añadir capacidad de reserva para una agrupación de discos o una matriz. Esta operación se considera que es dinámica porque tiene la capacidad de acceder continuamente a datos de la matriz a lo largo de toda la operación. Tenga en cuenta estas directrices al añadir unidades sin asignar a una matriz o agrupación de discos:

- El número de unidades sin asignar que puede seleccionar para una operación de modificación de DCE está limitada por el firmware del controlador. Se pueden añadir dos unidades sin asignar a una matriz a la vez. Puede añadir un máximo de doce unidades a la vez por agrupación de discos. Sin embargo, después de haber completado una operación de DCE, puede añadir más unidades hasta alcanzar la capacidad deseada.
- Las unidades lógicas existentes en la matriz o la agrupación de discos no aumentan de tamaño al añadir unidades sin asignar para ampliar la capacidad libre. Esta operación redistribuye la capacidad actual de la unidad lógica existente en el mayor número de unidades de la matriz o la agrupación de discos.
- Las unidades sin asignar que añade a la matriz o agrupación de discos debe ser del mismo tipo de soporte e interfaz. Mezclar tipos de unidades diferentes dentro de una matriz única o agrupación de discos no está permitido. Siempre que sea posible, seleccione unidades que tengan una capacidad igual a la capacidad de las unidades actuales de la matriz o agrupación de discos. Las unidades con capacidades mayores o iguales a la capacidad de las unidades actuales de una agrupación de discos se puede añadir como parte de una operación de Dynamic Capacity Expansion. Sin embargo, si se añaden unidades con mayor capacidad que las actuales de una agrupación de discos, la capacidad por encima de la unidad más pequeña de la agrupación de discos no se utiliza y la cantidad no utilizada se presenta como capacidad inutilizable.
- En una matriz RAID Nivel 1, debe añadir dos unidades para asegurarse de que se configura la redundancia de datos.
- Sólo las unidades de seguridad se pueden añadir a una matriz o agrupación de discos con seguridad habilitada, o una matriz o agrupación de discos de seguridad.
- En una matriz o agrupación de discos con capacidad T10PI y una unidad lógica T10PI habilitado, solo puede añadir unidades con capacidad T10PI.

Visualización de operaciones en curso

La ventana Operaciones en curso muestra todas las operaciones que se están ejecutando actualmente en el subsistema de almacenamiento. Se trata de una ventana de solo visualización en la que puede supervisar el progreso. Mientras la ventana Operaciones en curso está abierta puede llevar a cabo otras tareas en la ventana Gestión del subsistema.

Puede ver el progreso de lo siguiente

- **Expansión de capacidad dinámica (DCE)** – Adición de capacidad a una matriz
- **Migración RAID dinámica (DRM)** –Cambio del nivel RAID de una matriz
- Comprobación de la redundancia de datos de una matriz
- Desfragmentación de una matriz
- Inicialización de una unidad lógica
- **Expansión de unidad lógica dinámica (DVE)** – Adición de capacidad a una unidad lógica
- **Tamaño de segmentos dinámico (DSS)** – Cambio del tamaño de segmentos de una unidad lógica
- **Reconstrucción** – Reconstrucción de datos de paridad debido a sectores ilegibles o unidad errónea
- **Copia** – Copia de datos de una unidad de repuesto en caliente a una nueva unidad de sustitución
- VolumeCopy
- Sincronización de una duplicación remota

Hallará más información en la ayuda en línea.

Configuración de unidades de repuesto en caliente globales

Puede asignar unidades físicas disponibles en el subsistema de almacenamiento como *unidades de repuesto en caliente* para conservar la disponibilidad de los datos. Un repuesto en caliente global no contiene datos y actúa como sistema en espera en caso de que una unidad falle en una matriz RAID 1, RAID 10, RAID 3, RAID 5 o RAID 6. Los repuestos en caliente globales no se utilizan como repuesto de una agrupación de discos. Las agrupaciones de discos se crean con capacidad reservada distribuida en todas las unidades de la agrupación para reconstruir datos en caso de que una unidad falle. Si una unidad de una matriz falla, los controladores utilizan de forma automática una unidad de repuesto en caliente para sustituir la unidad física que haya fallado mientras el subsistema de almacenamiento sigue en funcionamiento. El controlador utiliza los datos de redundancia para reconstruir automáticamente los datos de la unidad física que ha fallado en la unidad de sustitución (repuesto en caliente). Esto se denomina *reconstrucción*. La unidad de repuesto en caliente añade otro nivel de redundancia al subsistema de almacenamiento. Si una unidad física falla en el subsistema de almacenamiento, la unidad de repuesto en caliente se sustituye automáticamente sin necesidad de un intercambio físico.

Asignación de unidades de repuesto en caliente

Hay dos maneras de asignar unidades de repuesto en caliente a las matrices definidas en el subsistema de almacenamiento:

- **Asignación automática de unidades:** Si selecciona esta opción, las unidades de repuesto en caliente se crean automáticamente para dar la mejor cobertura en caliente utilizando las unidades disponibles. Esta opción siempre está disponible.
- **Asignación manual de unidades individuales:** Si selecciona esta opción, se crean unidades de repuesto en caliente a partir de dichas unidades que han sido seleccionadas previamente.

Si opta por asignar manualmente las unidades de repuesto en caliente, seleccione una unidad con capacidad igual o mayor a la capacidad total de la unidad que desea cubrir con el repuesto en caliente. Por ejemplo, si tiene una unidad de 18 GB con capacidad configurada de 8 GB, puede utilizar una unidad de 9 GB o más

como repuesto en caliente. Por lo general, no debe asignar una unidad como repuesto en caliente a menos que su capacidad sea igual o superior a la capacidad de la unidad más grande del subsistema de almacenamiento. Para una protección de datos máxima, en configuraciones de discos duros de capacidad combinada, debe utilizar sólo las unidades con mayor capacidad como unidades de repuesto en caliente. También hay una opción que permite cancelar la asignación de unidades individuales de forma manual.

Si falla una unidad de la matriz, el repuesto en caliente puede ser sustituido de manera automática por la unidad que ha fallado, sin necesidad de su intervención. Si hay un repuesto en caliente disponible cuando una unidad falla, el controlador utiliza los datos de redundancia para reconstruir los datos en el repuesto en caliente.

Nota: Las unidades con diferentes protocolos de interfaz o tecnologías no pueden utilizarse como repuestos en caliente entre ellas. Por ejemplo, las unidades SATA y de canal de fibra no pueden actuar como repuestos en caliente entre sí.

1. Para asignar unidades de repuesto en caliente, realice uno de los pasos siguientes:
 - En la pestaña Servicios de Almacenamiento y copia, pulse el botón derecho del ratón sobre el subsistema de almacenamiento y seleccione **Configuración > Cobertura de repuesto en caliente**.
 - En la pestaña Configuración, seleccione **Crear Almacenamiento > Configurar repuestos en caliente**.
2. Seleccione Automático o Manual. Si selecciona Automático, el subsistema de almacenamiento asigna automáticamente una unidad como repuesto en caliente. Posteriormente, puede ver/cambiar la cobertura de repuesto en caliente.
3. Para seleccionar manualmente unidades de repuesto en caliente, selecciona la matriz y pulse en **Asignar**.
4. Seleccione unidades como repuesto en caliente y pulse **Aceptar**.

Restauración de datos de unidades de repuesto en caliente

Una vez sustituida físicamente la unidad que ha fallado, puede utilizar cualquier de las opciones siguientes para restaurar los datos:

- Cuando haya sustituido la unidad que haya fallado, los datos del repuesto en caliente se copian en la unidad de sustitución. Esta acción se denomina *copia*.
- Puede asignar el repuesto en caliente como miembro permanente de la matriz. La función de realización de copias no es necesaria para esta opción.

Nota: Si la versión de firmware del controlador es 10.84 o posterior, la unidad de repuesto en caliente funciona en modalidad de copia.

Aunque no disponga de un repuesto en caliente, también puede sustituir una unidad que haya fallado mientras la matriz está en funcionamiento. Si la unidad forma parte de una matriz RAID Nivel 1, RAID Nivel 3, RAID Nivel 5, RAID Nivel 6 o RAID Nivel 10, el controlador utiliza los datos de redundancia para reconstruir automáticamente los datos en la unidad de sustitución.

Si selecciona **Cancelar asignación de unidades manualmente** se cancelará la asignación de las unidades de repuesto en caliente seleccionada en la pestaña Físicas. Esta opción no está disponible si no ha seleccionado ninguna unidad en la pestaña Físicas.

Definición de un sistema operativo host predeterminado

Antes de utilizar las unidades lógicas en un sistema principal, debe especificar el tipo de host adecuado. El tipo de host determina cómo trabajan los controladores del subsistema de almacenamiento con cada sistema operativo de los hosts a los que están conectados. Si todos los sistemas principales conectados al mismo subsistema de almacenamiento se ejecutan en el mismo sistema operativo y no quiere definir particiones, puede definir un tipo de host predeterminado.

Para verificar el tipo de host predeterminado actual, complete los siguientes pasos:

1. En la ventana Gestión del subsistema pulse **Ver perfil del subsistema de almacenamiento**. Se abrirá la ventana Perfil del subsistema de almacenamiento.
2. Pulse en la pestaña **Correlaciones de host**. Pulse el botón derecho del ratón sobre **Grupo predeterminado** y seleccione **Cambiar sistema operativo de host predeterminado**. El nombre de tipo de host del índice que tiene la palabra Base es el tipo de host predeterminado.
3. Pulse **Cerrar**.

Nota: Para habilitar la funcionalidad multi-ruta de acceso a unidades lógicas asimétricas (ALUA), debe seleccionar el tipo de host ALUA para la partición de host o grupo de host predeterminado.

El valor de tipo de host que especifica al configurar Storage Manager determina cómo trabajan los controladores de subsistema de almacenamiento con los sistemas operativos en los hosts conectados. Todos los puertos HBA de canal de fibra definidos con el mismo tipo de host reciben el mismo tratamiento por parte de los controladores del subsistema de almacenamiento. Esta determinación se basa en las especificaciones definidas por el tipo de host. Entre las especificaciones que varían en función del valor de tipo de host se incluyen las siguientes:

Transferencia automática de unidad/ALUA

Habilita o inhabilita la característica de transferencia automática de unidad lógica (ADT). Desde la versión de firmware de controlador 7.83.xx.xx, el valor se utiliza para habilitar o inhabilitar la funcionalidad ALUA.

Permitir reservas en LUN sin propiedad

Determina la respuesta del controlador a comandos de reserva/release recibidos para LUN que no son propiedad del controlador.

Creación de informes de errores aplazados

Determina se informa al host de los errores aplazados del controlador del subsistema de almacenamiento.

No enviar informe de atención de unidad única de proveedor como condición de comprobación

Determina si el controlador especifica una atención de unidad única de proveedor como estado de condición de comprobación.

Nombre mundial en consulta estándar

Habilita o inhabilita las consultas estándar ampliadas.

Ignorar propiedad UTM LUN

Determina el modo en que se informa sobre un LUN de acceso universal (UTM LUN). Storage Manager utiliza el UTM LUN para comunicarse con el subsistema de almacenamiento en configuraciones de gestión dentro de banda.

Informar sobre ruta preferida de LUN en datos de consulta estándar

Comunica la ruta preferida de LUN en los bits 4 y 5 de los datos de consulta estándar byte 6.

Habilitar soporte de host para T10PI

Habilitar o inhabilitar soporte de host para T10PI. En caso de estar inhabilitado, el controlador ocupa los 8 bytes adicionales con información T10PI antes de enviar los datos al host.

En la mayoría de las configuraciones de subsistemas de almacenamiento, los valores NVSRAM de cada tipo de host soportado en un entorno de sistema operativo particular son suficientes para conectar un host al subsistema de almacenamiento. No necesita cambiar ninguno de los valores de tipo de host para NVSRAM. Si considera que debe cambiar los valores NVSRAM, póngase en contacto con su representante de soporte de IBM antes de continuar.

Para definir un tipo de host predeterminado, complete los pasos siguientes:

1. Pulse **Correlaciones de host > Grupo predeterminado > Cambiar sistema operativo de host predeterminado**. Se abrirá la ventana Tipo de host predeterminado.
2. En la lista, seleccione el tipo de host.
3. Pulse **Aceptar**.

Nota:

En el entorno Veritas Storage Foundation Linux, el tipo de host predeterminado debe ser 13.

El tipo de host VMWARE se ha añadido a NVSRAM como tipo de host adicional. DS4200 y DS4700 utilizarán el índice 21.

El resto de sistemas soportados utilizarán el índice 16.

Aunque no es necesario, si utiliza un tipo de host Linux para un host VMWARE, se recomienda moverse al tipo de host VMWARE puesto que cualquier actualización del firmware del controlador y NVSRAM continuarían requiriendo la ejecución de scripts, mientras que el uso VMWARE no requiere dicha ejecución.

- Tras cambiar el tipo de host no es necesario reiniciar los controladores
- El host deberá reiniciarse
- Los cambios de tipos de host deben realizarse en condiciones de E/S bajas

Definición de un grupo de host

Un *grupo de host* es una entidad de la topología de partición del almacenamiento que define un conjunto lógico de sistemas principales que necesitan disponer de acceso compartido a una o más unidades lógicas. Puede otorgar acceso a particiones del almacenamiento a hosts individuales en un grupo de hosts definido, independientemente del grupo de hosts. Puede realizar correlaciones de unidad lógica-a-LUN al grupo de hosts o a un host específico del grupo de hosts.

Debe crear el grupo de host a nivel del subsistema de almacenamiento; no cree grupos de host a nivel del grupo predeterminado. No obstante, puede utilizar el grupo de host predeterminado si ejecuta una configuración de subsistema de almacenamiento si partición habilitada.

Para definir un grupo de host, realice los pasos siguientes:

1. Pulse la pestaña **Correlaciones de host** en la ventana Gestión del subsistema.
2. En la sección Topología de la página Correlaciones de host, seleccione el nombre del subsistema de almacenamiento o grupo predeterminado y pulse el botón derecho del ratón sobre **Definir > Grupo de host**.

Nota: Asegúrese de que el subsistema de almacenamiento está resaltado en el panel izquierdo de la ventana Gestión del subsistema. No resalte Correlaciones sin definir.

3. Escriba un nombre para el nuevo grupo de host. Pulse **Aceptar**.

Definición de hosts heterogéneos

La característica de hosts heterogéneos habilita hosts que se ejecutan en diferentes sistemas operativos para acceder a un único subsistema de almacenamiento. Storage Manager soporta hasta 512 particiones del almacenamiento en algunos subsistemas, lo cual permite a un subsistema de almacenamiento de tipo host múltiple compartir capacidad de almacenamiento, consolidar el almacenamiento y reducir los costes de gestión del mismo.

Los sistemas principales se pueden ejecutar en diferentes sistemas operativos o variantes del mismo sistema operativo. Cuando define un tipo de host en la ventana Definir nuevo puerto de host, la característica de hosts heterogéneos permite a los controladores del subsistema de almacenamiento adaptar su comportamiento (por ejemplo la creación de informes de LUN y condiciones de error) a las necesidades del sistema operativo o variante del host que envía la información.

Nota:

1. Durante la definición de puertos host, debe definir cada tipo de host en función del sistema operativo aplicable, de forma que el firmware de cada controlador pueda responder correctamente al host.
2. Debe habilitar la partición del almacenamiento, que es una característica premium. Debe utilizar la clave de partición que guardó durante la instalación o ir a la página web de códigos de características de IBM para reactivar y obtener una nueva clave de característica. Para obtener más información sobre las características premium, consulte “características premium de Storage Manager” en la página 58.
3. Todos los puertos HBA que están conectados al subsistema de almacenamiento desde un servidor deben estar definidos en una partición de host única.

Nota: Para habilitar la funcionalidad multi-ruta de acceso a unidades lógicas asimétricas (ALUA), debe seleccionar el tipo de host ALUA para la partición de host o grupo de host predeterminado.

Definición de host y puertos del host

Para definir el host y los puertos del host utilizando el asistente Definir un host y los puertos del host, complete los pasos siguientes:

1. En la sección Topología de la página Vista de correlaciones, pulse con el botón derecho el nuevo grupo de host y seleccione **Definir host**. Se abrirá la ventana Introducción (Definir host).
2. Pulse **Siguiente**. Se abre la ventana Especificar identificadores de puerto de host (definir host).

3. Seleccione la interfaz de puerto de host que quiera en **Elegir un tipo de interfaz de host**.

Nota: Si está configurando almacenamiento para IBM i, utilice el puerto en el primer adaptador. IBM i necesita dos adaptadores para una configuración válida.

4. Si la conectividad HBA está correctamente configurada, seleccione **Añadir mediante la selección de un identificador de puerto de host no asociado conocido** para añadir un puerto de host. Para especificar WWPN manualmente, seleccione **Añadir mediante la creación de un identificador de puerto de host nuevo**.
5. Especifique el Identificador de puerto de host en **Alias** y pulse **Añadir**. Se añade a la Lista de grupo de host. Pulse **Siguiente**.
6. Repita los pasos 3 y 4 para añadir todos los hosts.
7. Para eliminar cualquiera de los Identificadores de puerto de host que ha añadido, seleccione Identificadores de puerto de host en **Identificadores de puerto de host a asociar con el host** y pulse **Eliminar**.
8. Seleccione el tipo de host y pulse **Siguiente**.
9. Seleccione **Sí** o **No** para compartir acceso a las mismas unidades lógicas con otros hosts. Pulse **Siguiente**.
10. Revise la información para ver si es precisa. Pulse **Finalizar** para realizar esta tarea. Si quiere definir otro host, seleccione **Sí** y vuelva a repetir el procedimiento.

Correlación de LUN

En esta sección se describe cómo correlaciona LUN a una partición de almacenamiento con los siguientes procedimientos:

- “Correlación de LUN con un Host o Grupo de host nuevo”
- “Adición de LUN a un host o grupo de host existente”

Correlación de LUN con un Host o Grupo de host nuevo

Para correlaciones LUN con una partición recién creada, siga los pasos indicados a continuación:

1. Seleccione la vista Correlaciones de la ventana Gestión del subsistema.
2. En la sección Topología, pulse con el botón derecho en el host en el que desea correlacionar los LUN y seleccione **Definir partición de almacenamiento**. Se abrirá la ventana Definir partición de almacenamiento.
3. En la ventana Definir partición de almacenamiento, seleccione **Host** o **Grupo de host** y pulse **Siguiente**.
4. Seleccione la unidad lógica.
5. Acepte el identificador de LUN predeterminado o cámbielo y pulse **Añadir**.
6. Repita el paso 5 para todos los LUN que desee correlacionar con la partición.

Nota: También puede utilizar el asistente Partición del almacenamiento del Asistente de tareas de Storage Manager para correlacionar LUN con una nueva partición del almacenamiento.

Adición de LUN a un host o grupo de host existente

Para correlaciones nuevos LUN con una partición existente, complete los pasos siguientes. Repita estos pasos para cada LUN que desee añadir a la partición.

1. Pulse la pestaña **Correlaciones de host** en la ventana Gestión del subsistema.
2. En la sección Topología, pulse con el botón derecho en el host o grupo de host en el que desea correlacionar los LUN y seleccione **Definir correlaciones adicionales**. Se abrirá la ventana Definir correlaciones adicionales.
3. En la ventana Definir correlaciones adicionales, seleccione las opciones siguientes y pulse **Añadir**:
 - Grupos de host
 - Número de unidad lógica (LUN)(0-255)
 - Unidad lógica

Configuración de IBM System Storage para IBM i

Utilice la información de las siguientes secciones, junto con las secciones “Configuración de almacenamiento de disco” en la página 78 y “Definición de un grupo de host” en la página 95, para configurar y asignar LUN de IBM i en los subsistemas de almacenamiento DS5100 y DS5300 con el software Storage Manager.

Asignación de un identificador de puerto para IBM i

Cuando utiliza Storage Manager para indicar un identificador de puerto para IBM i, el puerto está en el primer adaptador. IBM i requiere dos adaptadores para que la configuración sea válida. La siguiente ilustración muestra la ventana de configuración en la que asignará el identificador de puerto.

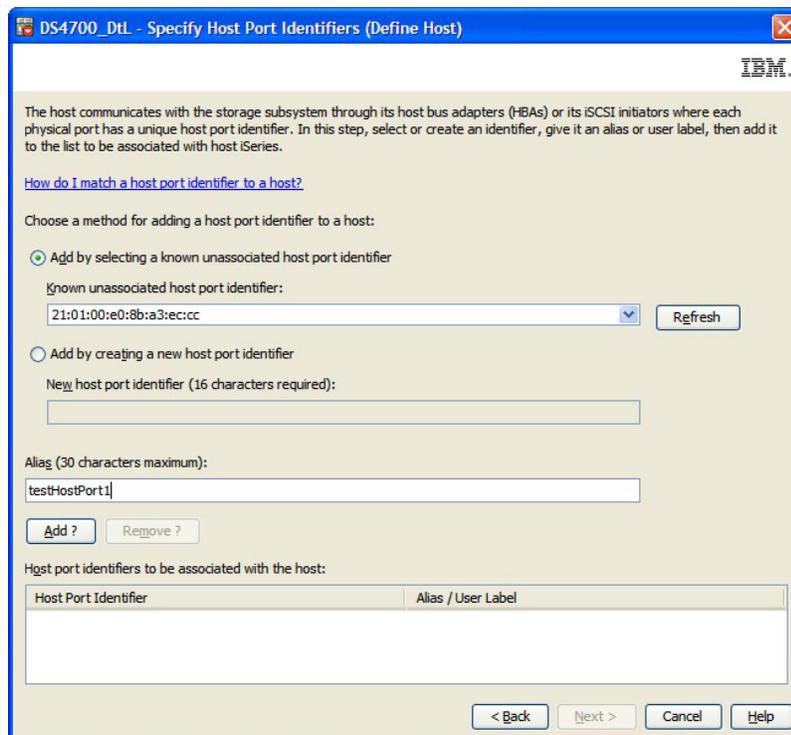


Figura 10. Asignación de un identificador de puerto para IBM i

Definición de IBM i como tipo de host

Cuando utilice Storage Manager para definir un tipo de host, seleccione **IBM i** en la lista **Tipo de host (sistema operativo)**.

Importante: En configuraciones avanzadas, se puede asignar un LUN 0 a un grupo o definición de host que no permita IBM i como tipo de host. Para solucionar este problema, elimine el valor LUN 0, cambie el sistema operativo por IBM i y después añada el LUN eliminado previamente.

La siguiente ilustración muestra la ventana de configuración donde definirá IBM i como tipo de host.

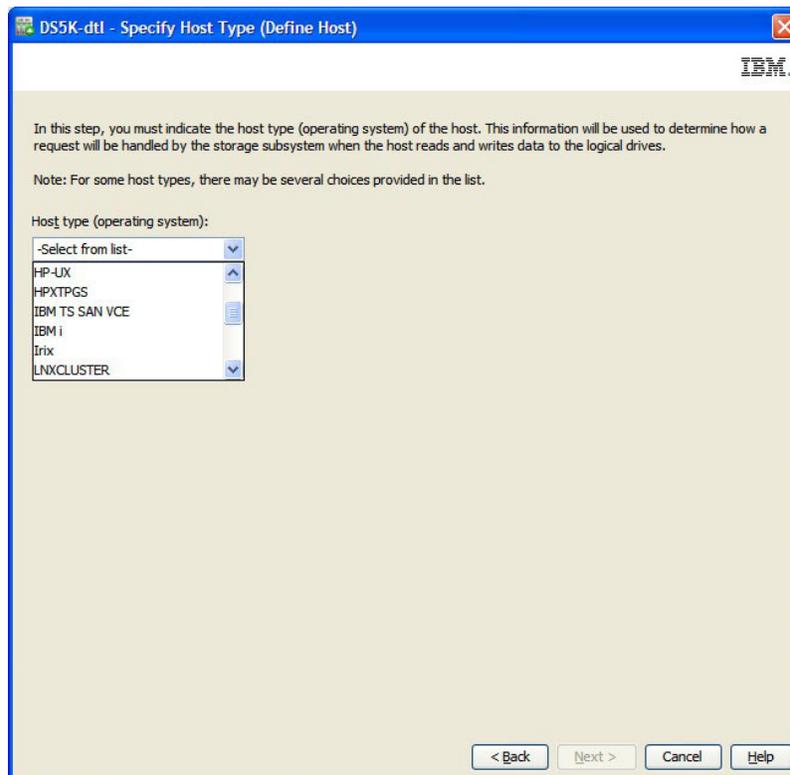


Figura 11. Selección de IBM i como tipo de host

Configuración y uso de características premium opcionales

Esta sección describe las características premium opcionales, incluyendo FlashCopy, Enhanced FlashCopy, VolumeCopy, la duplicación remota y el cifrado de disco completo.

Nota: Para obtener más información sobre estas características premium opcionales, consulte la *IBM System Storage DS Storage Manager Copy Services User's Guide* o póngase en contacto con su proveedor de IBM o representante de marketing de IBM.

Acerca de Enhanced FlashCopy

El DS Storage Manager con la versión del firmware del controlador 7.8x.xx.xx o posterior, ofrece la característica Enhanced FlashCopy, que le permite realizar una copia lógica del contenido de una unidad lógica estándar o una unidad lógica

ligera en un punto determinado del tiempo. Estas imágenes de punto en el tiempo de las unidades lógicas se denominan imágenes de Enhanced FlashCopy. Realizar imágenes de Enhanced FlashCopy es útil cuando necesite retroceder a un conjunto de datos conocido de un punto específico en el tiempo. Por ejemplo, puede crear una imagen de Enhanced FlashCopy como copia de seguridad y utilizarla durante una operación de recuperación. Imágenes de Enhanced FlashCopy de una unidad lógica de base se gestionan como miembros de un grupo de Enhanced FlashCopy. Un grupo de Enhanced FlashCopy puede tener hasta 32 imágenes y una unidad lógica de base permite la creación de hasta cuatro grupos de Enhanced FlashCopy.

Al realizar una imagen de Enhanced FlashCopy de una unidad lógica, DS Storage Manager guarda la imagen en un repositorio asociado con un grupo de Enhanced FlashCopy. Para ofrecer acceso a host a las imágenes de Enhanced FlashCopy almacenadas en un repositorio de grupo de Enhanced FlashCopy, debe crear una unidad lógica de esa imagen.

Debe recordar algunos detalles importantes acerca de las relaciones entre una imagen de Enhanced FlashCopy, un grupo de Enhanced FlashCopy y una unidad lógica de Enhanced FlashCopy:

- Las imágenes de Enhanced FlashCopy se crean en el contexto de un grupo de Enhanced FlashCopy.
- Un grupo de Enhanced FlashCopy es una secuencia de imágenes de Enhanced FlashCopy de una única unidad lógica estándar asociada o unidad lógica ligera. Una unidad lógica utilizada para crear una imagen de Enhanced FlashCopy se conoce como unidad lógica de base.
- Un grupo de Enhanced FlashCopy tiene exactamente un repositorio que se utiliza para guardar las imágenes de Enhanced FlashCopy mejoradas que forman parte del grupo de Enhanced FlashCopy.
- Todas las imágenes de Enhanced FlashCopy de un repositorio de grupo de Enhanced FlashCopy están asociadas directamente con ese grupo de Enhanced FlashCopy.
- Un grupo de Enhanced FlashCopy tiene una asociación con una única unidad lógica.
- Todas las unidades lógicas de Enhanced FlashCopy están asociadas directamente con una imagen de Enhanced FlashCopy.
- Todas las unidades lógicas de Enhanced FlashCopy tienen una relación permanente con la unidad lógica de base de la imagen de Enhanced FlashCopy para la que se creó inicialmente la unidad lógica.
- El repositorio asociado con la unidad lógica de Enhanced FlashCopy está asociado con un grupo de Enhanced FlashCopy.

Acerca de FlashCopy

Una unidad lógica de FlashCopy es una imagen lógica de un punto en el tiempo de una unidad lógica, denominada unidad lógica de base. Una unidad lógica de FlashCopy tiene las siguientes características:

- Se crea rápidamente y necesita menos espacio de disco que una unidad lógica real.
- Se le puede asignar una dirección de host, de forma que puede realizar copias de seguridad con la unidad lógica de FlashCopy mientras la unidad lógica de base está en línea y accesible.
- Puede utilizar la unidad lógica de FlashCopy para llevar a cabo pruebas de aplicaciones o el desarrollo y análisis del escenario. Esto no afecta al entorno de producción real.

- El número máximo de unidad lógicas de FlashCopy permitido es la mitad del total de unidades lógicas soportadas por su modelo de controlador.

Nota: El subsistema de almacenamiento puede utilizar simultáneamente las características FlashCopy y Enhanced FlashCopy. No obstante, cada unidad lógica de base puede utilizar FlashCopy o Enhanced FlashCopy, pero no ambas. Para obtener más información sobre la característica FlashCopy y sobre cómo gestionar unidades lógicas de FlashCopy, consulte la ayuda en línea de la ventana Gestión del subsistema Storage Manager.

Importante: La unidad de FlashCopy no se puede correlacionar o añadir al mismo servidor en el que está la unidad lógica de FlashCopy en un entorno Windows 2000, Windows Server 2003 o NetWare. Debe correlacionar la unidad lógica de FlashCopy con otro servidor.

Para crear una unidad lógica de FlashCopy, complete estos pasos:

1. Para asegurarse de que dispone de la imagen en el tiempo exacta de la unidad lógica de base, detenga las aplicaciones y vacíe la E/S de la memoria caché en la unidad lógica de base.
2. Abra la ventana Gestión del subsistema. En la página Lógica, pulse con el botón derecho en la unidad lógica de base.
3. Seleccione **Crear unidad lógica de FlashCopy**. Se iniciará el asistente de Creación de unidades lógicas de FlashCopy.
4. Siga las instrucciones en pantalla.
5. Consulte la ayuda en línea de la ventana Gestión del subsistema para obtener instrucciones para la adición de una unidad lógica deFlashCopy al host.

Uso de VolumeCopy

La característica VolumeCopy es un mecanismo basado en firmware para duplicar datos de unidades lógicas dentro de un subsistema de almacenamiento. Esta característica está diseñada como herramienta de gestión del sistema para tareas como la reasignación de datos a otras unidades para actualizaciones de hardware o gestión del rendimiento, la realización de copias de seguridad de los datos o la restauración de datos de unidad lógica de instantánea. Los usuarios envían solicitudes deVolumeCopy especificando dos unidades compatibles. Una unidad se designa como el *origen* y la otra como el *destino*. La solicitud de VolumeCopy es persistente, por lo que cualquier resultado relevante del proceso de copia se puede comunicar al usuario. Para obtener más información sobre esta característica, póngase en contacto con su proveedor o representante de marketing de IBM.

Uso de la Duplicación remota mejorada (Enhanced Remote Mirroring)

La Duplicación remota mejorada es una característica premium que se utiliza para replicación en línea, en tiempo real, de datos entre los subsistemas de almacenamiento de distintas ubicaciones. Mediante la opción Duplicación remota, puede designar un segundo subsistema de almacenamiento para gestionar las operaciones de E/S normales si falla el primer subsistema de almacenamiento. Para obtener más información sobre esta característica, consulte la *IBM System Storage DS Storage Manager Version 10 Copy Services User's Guide* (Guía del usuario de los servicios de copia), o póngase en contacto con el distribuidor o representante de ventas de IBM.

Uso de la Duplicación global mejorada (Enhanced Global Mirroring)

La Duplicación global mejorada es una característica premium que se utiliza para replicar datos entre el sitio local y el sitio remoto en un escenario asíncrono. Esta característica permite conectividad de tejido a bajo coste (iSCSI) y crea una imagen temporal en la unidad lógica primaria. Sincroniza de forma periódica con la unidad lógica secundaria, minimizando así el impacto en el rendimiento del sistema en redes que no sean de alta velocidad, en horas punta. Para obtener más información sobre esta característica, consulte la *IBM System Storage DS Storage Manager Version 10 Copy Services User's Guide* (Guía del usuario de los servicios de copia), o póngase en contacto con el distribuidor o representante de ventas de IBM.

Uso de la Memoria caché de lectura de rendimiento

La Memoria caché de lectura de rendimiento es una característica premium que se utiliza para colocar en memoria caché los datos leídos recientemente de las unidades lógicas. Esta característica aumenta de forma significativa el rendimiento de la lectura de datos en los datos almacenados en la memoria caché. Para su uso, no hace falta configuración/administración adicional. El tamaño de la Memoria caché de lectura de rendimiento depende del tamaño de memoria caché del controlador instalado.

Nota: Actualmente, esta característica se admite en los subsistemas de almacenamiento DS3500, DCS3860 y DCS3700 con unidades de estado sólido.

Tabla 18. Tamaño máximo de Memoria caché de lectura de rendimiento soportado por la memoria caché de cada controlador instalado

Tamaño de memoria caché de controlador instalado	Tamaño máximo soportado de Memoria caché de lectura de rendimiento (por controlador)
1 GB	1 TB
2 GB	2 TB
4 GB	4 TB
>4 GB	5 TB

Uso del Cifrado de disco completo

El Cifrado de disco completo (FDE) es una característica premium que evita el acceso no autorizado a los datos de una unidad que se haya retirado físicamente de un subsistema de almacenamiento. Los controladores del subsistema de almacenamiento tienen una clave de seguridad. Las unidades aseguradas solo proporcionan acceso a los datos a través de un controlador con la clave de seguridad adecuada. El FDE es una característica premium del software de gestión del almacenamiento y debe ser habilitada por su proveedor del almacenamiento.

Nota: No todos los subsistemas de almacenamiento DS soportan el FDE. Compruebe la carta de anuncio de la *Installation, User's, and Maintenance Guide* de su subsistema de almacenamiento para determinar si este soporta FDE.

La característica premium FDE requiere unidades con capacidad de seguridad. Las unidades con capacidad de seguridad cifran los datos durante las operaciones de escritura y los descifran durante las operaciones de lectura. Cada unidad con capacidad de seguridad tiene una clave de cifrado de unidad única.

Cuando crea una matriz asegurada a partir de unidades con capacidad de seguridad, las unidades de la matriz pasan a estar aseguradas. Cuando una unidad con capacidad de seguridad pasa a estar asegurada, requiere la clave de seguridad adecuada para leer o escribir datos. Las unidades con capacidad de seguridad trabajan de la misma forma que cualquier otra unidad hasta que son aseguradas.

Para obtener más información sobre cómo configurar y utilizar el FDE, consulte Capítulo 6, “Trabajo con el Cifrado de disco completo”, en la página 215.

Uso de otras características

Esta sección describe otras características disponibles en Storage Manager.

Uso de la memoria caché del controlador

El almacenamiento en caché de escritura permite a la memoria caché del controlador almacenar operaciones de escritura del sistema principal y, como resultado, mejora el rendimiento del sistema. Sin embargo, un controlador puede fallar con datos del usuario en la memoria caché que no hayan sido transferidos a la unidad lógica. Además, la memoria caché puede fallar mientras contiene datos no escritos. La duplicación de memoria caché de escritura protege el sistema de las siguientes posibilidades. La duplicación de la memoria caché de escritura permite que se dupliquen los datos almacenados en dos controladores redundantes con el mismo tamaño de caché. Los datos que se escriben en la memoria caché de un controlador también se escriben en la memoria caché del otro controlador. Es decir, si un controlador falla, el otro controlador completa todas las operaciones de escritura pendientes.

Nota: Puede habilitar el parámetro de duplicación de la memoria caché de escritura para cada unidad lógica, pero cuando se habilita la duplicación, la mitad del tamaño total de caché de cada controlador se reserva para duplicar los datos de la caché del otro controlador.

Para evitar la pérdida de datos o daños, el controlador escribe periódicamente los datos de la caché en la unidad lógica. Cuando la memoria caché tiene un porcentaje de inicio especificado de datos no escritos, el controlador escribe los datos de la caché en la unidad lógica. Cuando se vacía la caché hasta un porcentaje de detención especificado, el vaciado se detiene. Por ejemplo, la configuración de inicio predeterminada de una unidad lógica es 80% del tamaño total de memoria caché y la configuración de detención es 20%. Con esta configuración, el controlador comienza a vaciar los datos de la memoria caché cuando esta alcanza el 80% de su capacidad y se detiene el vaciado llega al 20% de su capacidad.

Para una mayor seguridad de los datos, puede elegir porcentajes de inicio y detención bajos, por ejemplo 25% para el inicio y 0% para la detención. No obstante, los valores de inicio y detención bajos aumentan las posibilidades de que datos que se necesiten para la lectura de un sistema principal no estén en la memoria caché. Si no hay datos suficientes en la caché, el porcentaje de coincidencia de memoria caché disminuye y por tanto la tasa de solicitud de E/S también se ve reducida. También aumenta el número de escrituras de disco necesarias para mantener el nivel de la caché, aumentando la sobrecarga del sistema y disminuyendo el rendimiento.

Si se produce un corte de energía, los datos de la caché no escritos en la unidad lógica podrían perderse, incluso aunque se hayan duplicado en la memoria caché

de ambos controladores. Existen baterías de copia de seguridad en el alojamiento del controlador que protegen la memoria caché ante cortes de energía.

Nota: El intervalo de cambio de CRU de la batería de copia de seguridad es de tres años a partir de la fecha de instalación de la misma para todos los modelos de los subsistemas de almacenamiento DS4000: DS4100, DS4300 y DS4400. Para el resto de CRU de baterías de copia de seguridad de memoria caché de subsistemas de almacenamiento DS4000 no existe intervalo de sustitución.

El software Storage Manager cuenta con un reloj de batería que puede definir al sustituir una batería. Este reloj realiza el seguimiento del tiempo de la batería (en días) para que sepa cuándo debe sustituir la misma.

Nota:

1. En los sistemas de disco DS4100 y DS4300, o DS4300 Turbo, la CRU de la batería se encuentra dentro de la CRU de cada controlador.
2. En el DS4800, DS5100 y DS5300, la CRU de la batería se encuentra en la CRU de las baterías interconectadas. El almacenamiento en memoria caché se deshabilita cuando las baterías están bajas o descargadas. Si habilita un parámetro denominado almacenamiento en caché sin baterías en una unidad lógica, la escritura en caché continuará incluso cuando se hayan retirado las baterías del alojamiento del controlador.

Atención: Para una mayor integridad de los datos, no habilite el parámetro almacenamiento en caché sin baterías, porque si el alojamiento del controlador no cuenta con baterías en funcionamiento y se produce un corte de energía los datos de la memoria caché se perderán. En su lugar, póngase en contacto con el servicio de IBM para obtener una batería de sustitución tan pronto como sea posible para minimizar el tiempo que el subsistema de almacenamiento funciona con el almacenamiento en caché deshabilitado.

Uso de reservas persistentes

Atención: Utilice la opción Reservas persistentes solo siguiendo directrices de un representante de soporte técnico de IBM.

Utilice la opción Reservas persistentes para ver y borrar reservas de unidad lógica y registros asociados. Las reservas persistentes se configuran y gestionan a través del software de servidor en clúster e impiden a otros host acceder a unidades lógicas particulares.

A diferencia de otros tipos de reservas, una reserva persistente se utiliza para realizar las siguientes funciones:

- Reservar el acceso a diversos puertos de host y proporcionar diferentes niveles de control de acceso
- Realizar consultas al subsistema de almacenamiento sobre puertos registrados y reservas
- Proporcionar persistencia de reservas e caso de pérdida de alimentación del sistema de almacenamiento

Puede utilizar el software Storage Manager para gestionar reservas persistentes desde la ventana Gestión del subsistema. Puede utilizar la opción Reservas persistentes para realizar las siguientes tareas:

- Ver información de registro y reservas de todas las unidades lógicas del subsistema de almacenamiento
- Guardar información detallada sobre reservas y registros de las unidades lógicas
- Borrar todos los registros y reservas de una unidad lógica individual o todas las unidades lógicas del subsistema de almacenamiento

Para obtener más información, consulte la ayuda en línea de la ventana Gestión del subsistema. También puede gestionar las reservas persistentes a través del motor de scripts y la interfaz de la línea de comandos. Para obtener más información, consulte la ayuda en línea de la ventana Gestión empresarial.

Uso de la exploración de soportes

La *exploración de soportes* es un proceso en segundo plano que se ejecuta en todas las unidades lógicas del subsistema de almacenamiento para las que está habilitado, permitiendo detectar errores en el soporte de la unidad. La característica de Exploración de soportes comprueba los discos físicos en busca de defectos leyendo los datos en bruto del disco y volviéndolos a escribir en caso de error. La ventana de habilitar la exploración de soportes es que el proceso puede encontrar errores de soporte antes de interrumpir las funciones de lectura y escritura normales de la unidad lógica. El proceso de exploración de soportes explora toda la unidad lógica para comprobar que es accesible.

Nota: La operación de exploración de soportes en segundo plano no explora las unidades de repuesto en caliente ni los discos duros óptimos sin utilizar (los que no son parte de una unidad lógica definida). Para realizar una operación de exploración de soportes en unidades de repuesto en caliente o discos óptimos sin utilizar, debe convertirlos en unidades lógicas a determinados intervalos planificados y revertirlos a su estado de repuesto en caliente o sin utilizar tras la exploración.

Hay dos formas de realizar una exploración de soportes:

Comprobaciones de redundancia de unidad lógica no habilitada

Si se habilita la exploración de soportes sin habilitar las comprobaciones de datos de redundancia de las unidades lógicas, el subsistema de almacenamiento explora todos los bloques de las unidades lógicas, incluyendo los bloques de redundancia, pero no comprueba la precisión de dichos datos de redundancia.

Se trata del valor predeterminado cuando utiliza Storage Manager para crear unidades lógicas.

Comprobaciones de redundancia de unidad lógica habilitada

Si se habilita la exploración de soportes habilitando las comprobaciones de datos de redundancia de las unidades lógicas RAID-3 o RAID-6, una comprobación de datos de redundancia explora los bloques de datos, calcula los datos de redundancia y los compara con la información de redundancia de lectura de cada bloque. A continuación, repara los errores de redundancia en caso de ser necesario. Para unidades lógicas RAID-1, una comprobación de datos de redundancia compara los bloques de datos de las unidades duplicadas y corrige cualquier inconsistencia de datos.

No utilice este valor en subsistemas de almacenamiento DS antiguos como DS4500, DS4400, DS4300 o DS4100; la comprobación de redundancia tiene efectos negativos en el rendimiento del subsistema de almacenamiento.

En subsistemas de almacenamiento más nuevos como DS5100, DS5300, DS5020 o DS3950, este valor no provoca degradación del rendimiento.

Cuando se habilita, la exploración de soportes se ejecuta en todas las unidades lógicas del subsistema de almacenamiento que cumplen las siguientes condiciones:

- La unidad lógica se encuentra en un estado óptimo.
- No existen operaciones de modificación en curso.
- El parámetro Exploración de soportes está habilitado.

Nota: La Exploración de soportes debe habilitarse para todo el subsistema de almacenamiento y en cada unidad lógica del subsistema de almacenamiento para proteger la unidad lógica de errores debidos a anomalías de soportes.

La exploración de soportes solo lee bandas de datos, a menos que haya algún problema. Cuando no se puede leer un bloque de la banda, el comentario de lectura se reintenta un determinado número de veces. Si la lectura sigue fallando, el controlador calcula cómo debe ser el bloque y emite un comando de escritura con verificación en la banda. Cuando el disco intenta completar el comando de escritura, si el bloque no se puede escribir, la unidad reasigna sectores hasta que se puedan escribir los datos. A continuación, la unidad informa de la escritura correcta y la exploración de soportes comprueba la misma con otra lectura. No deberían producirse problemas adicionales con la banda. Si se dan problemas adicionales, el proceso se repite hasta que se realice la escritura correctamente, o hasta que la unidad falle debido a numerosos errores de escritura consecutivos y se haga cargo una unidad de repuesto en caliente. Las reparaciones se realizan solo en caso de escrituras correctas, y son las unidades las encargadas de dichas reparaciones. El controlador solo emite comandos de escritura con verificación. Así, las bandas de datos se pueden leer repetidamente y se puede informar de la existencia de sectores inadecuados, pero el controlador calcula la información que falta con RAID.

En subsistemas de almacenamiento con controlador dual, dos controladores pueden hacerse cargo de la E/S (los controladores A y B). Cada unidad lógica que cree tiene un controlador preferido que normalmente gestiona su E/S. Si un controlador falla, la E/S de las unidades lógicas *propiedad* del controlador que ha fallado pasa al otro controlador. La E/S de la exploración de soportes no se ve afectada por fallos del controlador y la exploración continúa en todas las unidades lógicas aplicables cuando solo existe un controlador activo.

Si una unidad falla durante el proceso de exploración de soportes debido a errores, se inician las tareas de reconstrucción normales en el sistema operativo del controlador y la exploración de soportes intenta reconstruir la matriz utilizando una unidad de repuesto en caliente. Mientras se realiza el proceso de reconstrucción, no se realizan más exploraciones de soportes en la matriz.

Nota: Dado que para la exploración de soportes se generan lecturas de E/S adicionales, el impacto podría verse afectado en función de los siguientes factores:

- La cantidad de capacidad de almacenamiento configurada en el subsistema de almacenamiento. Cuanto mayor sea la capacidad de almacenamiento configurada en el subsistema de almacenamiento, mayor será el impacto del rendimiento.
- La duración de la exploración configurada para las operaciones de exploración de soportes. Cuanto mayor sea la exploración, menor será el impacto en el rendimiento.

- El estado de la opción de comprobación de redundancia (habilitada o inhabilitada). Si la comprobación de redundancia está habilitada, el impacto en el rendimiento será mayor.

Errores indicados por la exploración de soportes

El proceso de exploración de soportes se ejecuta de manera continuada en segundo plano cuando está habilitado. Cada vez que se completa una exploración de soportes de todas las unidades lógicas de un subsistema de almacenamiento, otra comienza de forma inmediata. El proceso de exploración de soportes descubre los errores e informa de ellos al registro de eventos principal (MEL) del subsistema de almacenamiento. La siguiente tabla muestra los errores descubiertos durante una exploración de soportes.

Tabla 19. Errores descubiertos durante una exploración de soportes

Error	Descripción	Resultado
Error de soporte no recuperado	La unidad no ha podido leer los datos en su primer intento ni en intentos posteriores.	En unidades lógicas o matrices con protección de redundancia (RAID-1, RAID-3 y RAID-5), los datos se reconstruyen, rescriben en la unidad y verifican. El error se envía al registro de eventos. En unidades lógicas o matrices sin protección de redundancia (unidades lógicas RAID-0 y RAID-1, RAID-3, RAID-5 y RAID-6 degradadas), el error no se corrige pero se informa de él al registro de eventos.
Error de soporte recuperado	La unidad no ha podido leer los datos en su primer intento pero sí en intentos posteriores. Nota: La exploración de soportes realiza tres intentos para leer los bloques erróneos.	Los datos se rescriben en la unidad y verifican. El error se envía al registro de eventos.
No coincidencia de redundancia	Se detectan errores de redundancia. Nota: Este error solo se puede dar cuando se ha seleccionado el recuadro de comprobación de redundancia opcional, la exploración de soportes está habilitada y la unidad lógica o matriz no es RAID-0.	Las 10 primeras faltas de coincidencia de redundancia detectadas en una unidad lógica se envían al registro de eventos.
Error irreparable	Los datos no se han podido leer y la información de paridad o redundancia no se ha podido utilizar para reconstruirlos. Por ejemplo, no se puede utilizar información de redundancia para reconstruir datos en una unidad lógica degradada.	El error se envía al registro de eventos.

Configuración de la exploración de soportes

Para maximizar la protección y minimizar el impacto del rendimiento de E/S, el subsistema de almacenamiento se facilita de fábrica como los siguientes valores de exploración de soportes predeterminados:

- La opción de exploración de soportes está habilitada para todas las unidades lógicas del subsistema de almacenamiento. Así, cada vez que se crea una unidad lógica, esta se crea con la opción de exploración de soportes habilitada. Si desea inhabilitar la exploración de soportes, debe inhabilitarla de manera manual para cada unidad lógica.
- La duración de la exploración de soportes está definida en 30 días. Este es el tiempo en el que los controladores del subsistema de almacenamiento deben completar la exploración de soportes de una unidad lógica. El controlador utiliza la duración de la exploración de soportes, y la información sobre qué unidades lógicas debe explorar, para determinar una velocidad constante para realizar las actividades de exploración de soportes. La duración de la exploración de soportes se mantiene independientemente de la actividad de E/S del host.

Treinta días es el valor de duración máximo. Si desea explorar los soportes con mayor frecuencia, debe cambiar este valor manualmente. Este valor se aplica a todas las unidades lógicas del subsistema de almacenamiento. Por ejemplo, no puede definir la duración de la exploración de soportes de una unidad lógica en dos días y la de otras en treinta días.

- De manera predeterminada, la opción de comprobación de redundancia no está habilitada en las versiones de firmware de controlador anteriores a la versión 7.60.39.00. Para versiones de firmware de controlador anteriores a la versión 7.60.39.00, debe definir esta opción manualmente para cada unidad lógica en la que desee comprobar los datos de redundancia.

Para versiones de firmware de controlador 7.60.39.00 y posteriores, la opción de comprobación de redundancia se habilita de forma predeterminada en todas las unidades lógicas nuevas. Si desea que en una unidad lógica existente creada antes de la versión 7.60.39.00 o posteriores instalada se habilite la opción de comprobación de redundancia, debe habilitar esta opción de forma manual.

Sin la comprobación de redundancia habilitada, el controlador lee la banda de datos para confirmar que se pueden leer todos los datos. Si puede leer todos los datos, descarta los datos y se mueve a la siguiente banda. Cuando no puede leer un bloque de datos, reconstruye los datos a partir de los bloques restantes y el bloque de paridad y emite un comando de escritura con verificación para el bloque que no ha podido leer. Si el bloque no tiene errores de datos, la exploración de soportes utiliza la información actualizada y verifica si el bloque se ha arreglado. Si el bloque no se puede rescribir, la unidad asigna otro bloque para utilizar los datos. Cuando los datos se escriben correctamente, el controlador verifica si el bloque se ha arreglado y pasa a la siguiente banda.

Nota: Con la comprobación de redundancia, la exploración de soportes realiza el mismo proceso que sin ella pero, además, se recalcula y verifica el bloque de paridad. Si la paridad tiene errores de datos, se rescribe. El recálculo y comparación de los datos de paridad requieren E/S, lo cual puede afectar al rendimiento.

Importante: Los cambios en la configuración de la exploración de datos no entrarán en vigor hasta que se haya completado el ciclo de exploración de soportes actual.

Para cambiar la configuración de la exploración de soportes para un subsistema de almacenamiento completo, siga los pasos indicados a continuación:

1. Seleccione la entrada del subsistema de almacenamiento en la pestaña Lógica o Física de la ventana Gestión del subsistema.
2. Pulse **Subsistema de almacenamiento > Cambiar > Configuración de exploración de soportes**.

Para cambiar la configuración de la exploración de soportes para una unidad lógica, siga los pasos indicados a continuación:

1. Seleccione la entrada de la unidad lógica en la pestaña **Lógica** o **Física** de la ventana Gestión del subsistema.
2. Pulse **Subsistema de almacenamiento > Cambiar > Configuración de exploración de soportes**.

Duración de la exploración de soportes

Cuando se habilita la exploración de soportes, se especifica una ventana de duración (en días), que indica cuanto tiempo da el subsistema de almacenamiento al proceso de exploración de soportes para comprobar todas las unidades lógicas aplicables. La ventana de duración se puede reducir o aumentar de acuerdo con las necesidades del cliente. Cuanto menor sea la duración, más a menudo se explorará una unidad y, en consecuencia, más sólida será la situación. No obstante, cuanto más a menudo se explora una unidad, mayor será el impacto en el rendimiento.

Siempre que el subsistema de almacenamiento tiene tiempo de inactividad, comienza o continúa operaciones de exploración de soportes. Si se recibe trabajo de E/S de disco generado por aplicaciones, este tiene prioridad. Por ello, el proceso de exploración de soportes puede ser más lento, más rápido, o en algunos casos suspenderse, según los cambios requeridos por el trabajo. Si un subsistema de almacenamiento recibe una gran cantidad de trabajo de E/S de disco generado por aplicaciones, la exploración de soportes puede retrasar sus operaciones. A medida que el subsistema de almacenamiento se acerca al fin de la ventana de duración durante la que debe completar la exploración de soportes, una aplicación en segundo plano comienza a aumentar la prioridad (es decir, se dedica más tiempo al proceso de exploración de datos). Este aumento de la prioridad solo aumenta en cierta manera, ya que la prioridad del subsistema de almacenamiento es la E/S de disco generada por aplicaciones. En este caso, es posible que la duración de la exploración de soportes sea mayor que la configuración.

Nota: Si cambia el valor de duración de la exploración de soportes, los cambios no entrarán en vigor hasta que se complete el ciclo de exploración de soportes actual o se restablezca el controlador.

Ajuste de subsistemas de almacenamiento

La información de esta sección describe los datos del supervisor de rendimiento y las opciones de ajuste disponibles en Storage Manager para optimizar el subsistema de almacenamiento y el rendimiento de las aplicaciones. Utilice el supervisor de rendimiento de la ventana Gestión del subsistema para supervisar el rendimiento del subsistema de almacenamiento en tiempo real y guardar datos de rendimiento en un archivo para su análisis posterior. Puede especificar las unidades lógicas y controladores que desea supervisar, así como el intervalo de sondeo. También puede recibir el total de subsistemas de almacenamiento, que son los datos que combinan las estadísticas de ambos controladores en un par de controladores activo-activo.

Tabla 20. Opciones de ajuste del supervisor de rendimiento de la ventana Gestión del subsistema

Campo de datos	Descripción
E/S totales	E/S totales de este dispositivo desde que comenzó la sesión de sondeo.
Porcentaje de lectura	Porcentaje de E/S totales que son operaciones de lectura de este dispositivo. El porcentaje de escritura se calcula restando este valor a 100.
Porcentaje de coincidencia de memoria caché	Porcentaje de operaciones de lectura procesadas con datos de la memoria caché, en vez de necesita la lectura de la unidad lógica.
KB Current por segundo	Durante el intervalo de sondeo, la <i>velocidad de transferencia</i> es la cantidad de datos, en KB, que se mueven por la ruta de E/S de canal de fibra en 1 segundo (también denominado rendimiento).
KB máximos por segundo	La velocidad de transferencia máxima alcanzada durante la sesión del sondeo del supervisor de rendimiento.
E/S actuales por segundo	El número medio de solicitudes de E/S atendidas por segundo durante el intervalo de sondeo actual (también denominado velocidad de solicitud de E/S).
E/S máxima por segundo	El número máximo de solicitudes de E/S atendidas por segundo durante un intervalo de 1 segundo durante toda la sesión de sondeo.

Maximización del rendimiento con el equilibrio d carga

El equilibrio de carga es la redistribución de las solicitudes de lectura y escritura entre el servidor y el subsistema de almacenamiento para maximizar el resultado. El equilibrio de carga es muy importante en configuraciones de gran carga de trabajo o configuraciones donde los niveles de servicio coherente serán fundamentales. El controlador multi-ruta equilibra la carga de trabajo de E/S de manera transparente, sin intervención del administrador. Sin software multi-ruta, un servidor que envía solicitudes de E/S por diversas rutas puede operar con grandes cargas de trabajo en algunas rutas mientras otras no se utilizan de manera eficiente.

El controlador multi-ruta determina qué rutas hasta un dispositivo están en estado activo y se pueden utilizar para el equilibrio de carga. El equilibrio de carga utiliza uno de estos tres algoritmos: *round robin*, *menor profundidad de cola* o *menor peso de ruta*. Diversas opciones para configurar las políticas de carga le permiten optimizar el rendimiento de E/S cuando se configuran interfaces de host combinado. Las políticas de equilibrio de carga que puede elegir dependen de su sistema operativo. El equilibrio de carga se lleva a cabo en diversas rutas hacia el mismo controlador, pero no en ambos controladores.

Tabla 21. Políticas de equilibrio de carga soportadas por casa sistema operativo

Sistema operativo	Controlador multi-ruta	Política de equilibrio de carga
AIX	MPIO	Round robin, prioridad de ruta seleccionable
Red Hat Enterprise Linux 4 Update 7	RDAC	Round robin, menor profundidad de cola
Solaris	MPxIO	Round robin

Tabla 21. Políticas de equilibrio de carga soportadas por casa sistema operativo (continuación)

Sistema operativo	Controlador multi-ruta	Política de equilibrio de carga
SUSE Linux Enterprise 9 Service Pack 4	RDAC	Round robin, menor profundidad de cola
Windows	MPIO	Round robin, menor profundidad de cola, menor peso de ruta

Round robin con subconjunto

La política de equilibrio de carga de E/S round robin con subconjunto direcciona las solicitudes de E/S, en rotación, a cada ruta de datos disponible hasta el controlador que posee las unidades lógicas. Esta política trata todas las rutas hasta el controlador que posee la unidad lógica del mismo modo para actividad de E/S. Las rutas al controlador secundario se ignoran hasta que cambia la propiedad. La asunción en la política round robin es que todas las rutas de datos son iguales. Con soporte de host combinado, las rutas de datos podrían tener diferentes anchos de banda o diferentes velocidades de transferencia de datos.

Menor profundidad de cola con subconjunto

La política de menor profundidad de cola con subconjunto también se conoce como política de menor E/S o menos solicitudes. Esta política envía la siguiente solicitud de E/S a la ruta de datos que tenga el menos número de solicitudes de E/S pendientes en cola. Para esta política, las solicitudes de E/S son simplemente un comando en cola. El tipo de comando o el número de bloques asociados con el comando no se tienen en cuenta. La política de menor profundidad de cola con subconjunto trata las solicitudes de grandes bloques y las solicitudes de bloques pequeños de la misma forma. La ruta de datos seleccionada es una de las rutas del grupo de rutas del controlador que posee la unidad lógica.

Menor peso de ruta con subconjunto

La política de menor peso de ruta con subconjunto asigna un factor de peso a cada ruta de datos hacia una unidad lógica. Las solicitudes de E/S se envían a la ruta con menor valor de peso hasta el controlador que posee la unidad lógica. Si más de una ruta de datos a la unidad lógica tiene el mismo valor de peso, se utiliza la política de selección de ruta round robin con subconjunto para enviar solicitudes de E/S entre las rutas con el mismo valor de peso.

Equilibrio de la carga de E/S del canal de fibra

El campo de datos **E/S total** de la ventana Gestión del subsistema se utiliza para supervisar la actividad de E/S del canal de fibra hacia un controlador específico y una unidad lógica específica. Este campo le ayuda a identificar posibles zonas activas de E/S.

Puede identificar modelos de E/S de canal de fibra de las unidades lógicas individuales y compararlos con las expectativas según la aplicación. Si un controlador tiene más actividad de E/S de lo previsto, pulse **Matriz > Cambiar propiedad** para mover una matriz al otro controlador del subsistema de almacenamiento.

Equilibrar cargas de E/S de canal de fibra entre controladores y unidades lógicas es complicado porque las cargas de E/S cambian constantemente. Las unidades

lógicas y los datos a los que se accede en la sesión de sondeo dependen de las aplicaciones y usuarios que estén activos durante dicho periodo. Es importante supervisar el rendimiento durante diferentes períodos de tiempo y recopilar datos a intervalos regulares para identificar las tendencias de rendimiento. El supervisor de rendimiento le permite guardar datos en un archivo de texto delimitado por comas que se puede importar a una hoja de cálculo para su posterior análisis.

Si observa que la carga de trabajo del subsistema de almacenamiento (estadística total de E/S de canal de fibra) aumenta con el tiempo mientras que el rendimiento de las aplicaciones disminuye, es posible que tenga que añadir subsistemas de almacenamiento para la empresa.

Optimización de la tasa de transferencia de E/S

Las tasas de transferencia del controlador vienen determinadas por el tamaño de E/S de la aplicación y la tasa de solicitud de E/S. Un tamaño de solicitud de E/S de aplicación pequeño resulta en una tasa de transferencia más baja pero proporciona una tasa de solicitud de E/S mayor y un tiempo de respuesta más corto. Con tamaños de solicitud de E/S de aplicación más grandes, es posible disfrutar de tasas de rendimiento más altas. Comprender los patrones de E/S de las aplicaciones le ayudará a optimizar las tasas de transferencia de E/S máximas posibles para un subsistema de almacenamiento determinado.

Una de las maneras de mejorar la tasa de transferencia de E/S es mejorar la tasa de solicitud de E/S. Utilice los programas de utilidad del sistema operativo del sistema principal para recopilar datos sobre el tamaño de E/S para conocer las tasas de transferencia máximas posibles. A continuación, utilice las opciones de ajuste disponibles en Storage Manager para optimizar la tasa de solicitud de E/S y alcanzar la tasa de transferencia máxima posible.

Optimización de la tasa de solicitud de E/S

La tasa de solicitud de E/S se puede ver afectada por los siguientes factores:

- El patrón de acceso de E/S (aleatorio o secuencial) y el tamaño de E/S
- El estado de la escritura en memoria caché (habilitado o deshabilitado)
- El porcentaje de coincidencia de memoria caché
- El nivel RAID
- La prioridad de modificación de la unidad lógica
- El tamaño de segmento
- El número de unidades lógicas de las matrices o subsistema de almacenamiento
- La fragmentación de archivos

Nota: La fragmentación afecta a las unidades lógicas con patrones de acceso de E/S secuenciales, no a las que tienen patrones de acceso de E/S aleatorios.

Determinación del patrón de acceso de E/S y tamaño de E/S

Para determinar si el acceso de E/S tiene características secuenciales, habilite un multiplicador de lectura anticipada de memoria caché (por ejemplo, 4) pulsando **Unidad lógica > Propiedades**. A continuación, examine el porcentaje de coincidencia de memoria caché de la unidad lógica para ver si ha mejorado. Una mejora indica que la E/S tiene un patrón secuencial. Utilice los programas de utilidad del sistema operativo del sistema principal para determinar el tamaño de E/S habitual de una unidad lógica.

Habilitación de escritura en memoria caché

Las tasas más altas de escritura de E/S se producen cuando está habilitada la escritura en memoria caché, especialmente en relación con patrones de acceso E/S secuenciales. Independientemente del patrón de acceso E/S, asegúrese de habilitar la escritura en memoria caché para maximizar la tasa de E/S y reducir el tiempo de respuesta de las aplicaciones.

Optimización del porcentaje de coincidencia de memoria caché

Para obtener un rendimiento de aplicaciones óptimo es preferible tener un porcentaje de coincidencia de memoria caché alto, relacionado positivamente con la tasa de solicitud de E/S de canal de fibra.

Si el porcentaje de coincidencia de memoria caché de todas las unidades lógicas es bajo o tiende a la baja y es menor a la cantidad máxima de memoria caché del controlador instalada, deberá instalar más memoria.

Si una unidad lógica individual tiene un porcentaje de coincidencia de memoria caché bajo, puede habilitar la lectura adicional de la memoria caché para esa unidad lógica. La lectura adicional de la memoria caché puede aumentar el porcentaje de coincidencia de memoria caché para una carga de trabajo de E/S secuencial. Si la lectura adicional de la memoria caché está habilitada, esta capta más datos, normalmente de bloques de datos adyacentes de la unidad. Además de los datos solicitados, esta característica aumenta las posibilidades de satisfacer una futura solicitud de datos desde la memoria caché, en vez de requerir un acceso a unidad lógica.

Los valores de multiplicador de la lectura adicional de la memoria caché especifican el multiplicador que se debe utilizar para determinar el número de bloques de datos adicionales que se leen en la memoria caché. Si elige un multiplicador de lectura anticipada de la memoria caché más alto, puede aumentar el porcentaje de coincidencia de memoria caché.

Si determina que el patrón de acceso de E/S de canal de fibra tiene características secuenciales, defina un multiplicador de lectura adicional de memoria caché agresivo, (por ejemplo 8). A continuación, examine el porcentaje de coincidencia de memoria caché de la unidad lógica para ver si ha mejorado. Continúe personalizando la lectura adicional de la memoria caché de la unidad lógica hasta llegar al multiplicador óptimo (para un patrón de E/S aleatorio, el multiplicador óptimo es el 0).

Elección de los niveles adecuados de RAID

Utilice el porcentaje de lectura de una unidad lógica para determinar el comportamiento de la aplicación. Las aplicaciones con un porcentaje de lectura alto tienen un buen rendimiento con unidades lógicas RAID-5 debido al excelente rendimiento de lectura de la configuración RAID-5.

Nota: Esto solo es aplicable a la matriz tradicional. Las agrupaciones de discos siempre se crean con RAID 6 y 8D+P+Q.

Las aplicaciones con un porcentaje de lectura bajo (escritura intensiva) no tienen un buen rendimiento en unidades lógicas RAID-5 debido a la forma en que los controladores escriben los datos y datos de redundancia en las unidades de una unidad lógica RAID-5. Si hay un porcentaje bajo de actividad de lectura en comparación con la actividad de escritura, puede cambiar el nivel de RAID de una unidad lógica de RAID-5 a RAID-1 para disfrutar de un mejor rendimiento.

Elección de un valor de prioridad de modificación de unidad lógica óptimo

La prioridad de modificación define la cantidad de tiempo de procesamiento asignado a las operaciones de modificación de unidad lógica en comparación con el rendimiento del sistema. Cuanto mayor sea la prioridad, más rápido se completarán las operaciones de modificación de la unidad lógica, pero más espacio se da servicio al patrón de acceso de E/S del sistema.

Las operaciones de modificación de la unidad lógica incluyen la reconstrucción, la realización de copias, la inicialización, la exploración de medios, el cambio del nivel de RAID y el cambio del tamaño de segmentos. La prioridad de modificación se define para cada unidad lógica utilizando una barra deslizante en la ventana Unidad lógica - Propiedades. En la barra de velocidad de reconstrucción hay cinco ajustes, desde Baja a Superior. La velocidad real de cada valor está determinada por el controlador. Elija el valor Baja para maximizar la tasa de solicitud de E/S del canal de fibra. Si el controlador está desocupado (sin servicio a las tasas de solicitud de E/S) no tiene en cuenta los valores de la velocidad de las unidades lógicas individuales y procesa las operaciones de modificación de la unidad lógica lo más rápido posible.

Elección de un tamaño de segmento óptimo para una matriz

Un segmento es la cantidad de datos, en KB, que el controlador escribe en un único disco físico antes de escribir en la siguiente unidad. Un bloque de datos son 512 bytes de datos y es la unidad más pequeña de almacenamiento. El tamaño de un segmento determina el número de bloques de datos que contiene. Por ejemplo, un segmento de 8 KB contiene 16 bloques de datos y un segmento de 64 KB contiene 128 bloques de datos.

Nota: En una agrupación de discos, el tamaño del segmento siempre es de 128 KB. El tamaño del segmento en DS Storage Manager se expresa en KB.

Cuando crea una unidad lógica, el tamaño de segmentos por defecto es una buena opción para el uso esperado de la unidad lógica. Para cambiar el tamaño de segmento predeterminado, pulse en **Unidad lógica > Cambiar tamaño de segmento**.

Si el tamaño de E/S es mayor que el tamaño de segmento, aumente el tamaño de segmento para minimizar el número de unidades necesarias para satisfacer una solicitud de E/S. Esta técnica es aún más útil si dispone de patrones de acceso E/S aleatorios. Si utiliza un único disco físico para una única solicitud, el resto de discos físicos quedan disponibles para dar servicio simultáneamente a otras solicitudes.

Cuando se utiliza la unidad lógica en un solo usuario y entornos de E/S grandes como una aplicación multimedia, el rendimiento del almacenamiento se optimiza cuando se da servicio a una sola solicitud de E/S con una sola banda de datos de matriz (que es el tamaño del segmento multiplicado por el número de discos físicos de la matriz que se utilizan para solicitudes de E/S). En este caso, se utilizan diversos discos físicos para la misma solicitud, pero solo se accede una vez a cada disco físico.

Desfragmentación de archivos para minimizar el acceso al disco

Cada vez que accede a una unidad para leer o escribir un archivo, esto resulta en el movimiento de los cabezales de lectura/escritura. Compruebe que los archivos de la unidad lógica están desfragmentados. Cuando los archivos están desfragmentados, los bloques de datos que forman los archivos se encuentran unos

junto a los otros, evitando el movimiento de los cabezales de lectura y escritura adicional cuando se recuperan dichos archivos. Los archivos fragmentados disminuyen el rendimiento de las unidades lógicas con patrón de acceso de E/S secuencial.

Uso de la interfaz de línea de comandos de Storage Manager y el Editor de scripts

Esta sección describe la interfaz de línea de comandos de Storage Manager y el Editor de scripts

Interfaz de línea de comandos de Storage Manager

Atención: La interfaz de línea de comandos (CLI) no tiene ningún mecanismo para evitar que realice cambios de forma accidental en el subsistema de almacenamiento. Los comandos de script pueden dañar las configuraciones y causar la pérdida del acceso a datos si no se utilizan correctamente. Para evitar efectos dañinos en su configuración de almacenamiento o datos, utilice la interfaz gráfica de usuario (GUI) del cliente Storage Manager para gestionar las configuraciones de su subsistema de almacenamiento.

La interfaz de línea de comandos es una herramienta de software que le permite configurar y supervisar subsistemas de almacenamiento utilizando comandos de script. Haciendo uso de la CLI, puede ejecutar comandos desde una solicitud de sistema operativo, como la solicitud de comando de Windows, una consola de sistema operativo Linux o una de Solaris. Debe instalar el cliente IBM DS Storage Manager para ejecutar los comandos de script a través de una ventana de script, invocada desde la ventana Gestión empresarial del cliente IBM DS Storage Manager, o a través de una interfaz de línea de comandos con el programa SMcli. El motor de mandatos de script se instala automáticamente como parte de la instalación del cliente de IBM DS Storage Manager.

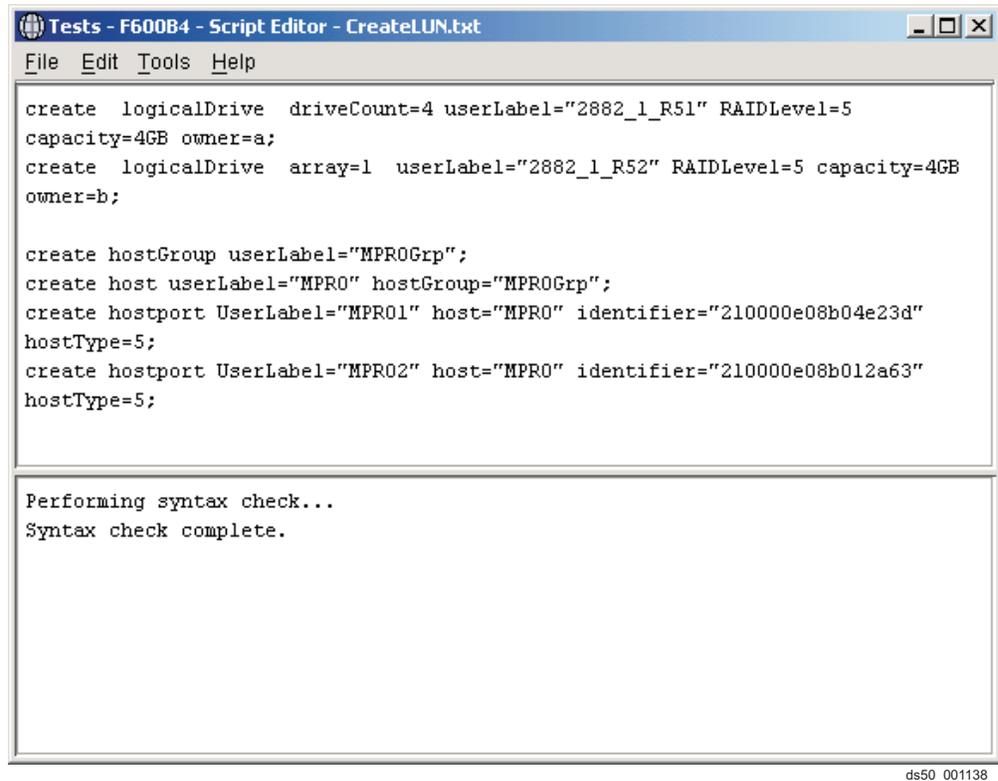
Cada comando realiza una acción específica que gestiona un subsistema de almacenamiento o devuelve información sobre el estado de un subsistema de almacenamiento. Puede introducir mandatos individuales o puede ejecutar archivos de script cuando necesite realizar operaciones más de una vez. Por ejemplo, puede ejecutar archivos de script cuando desee instalar la misma configuración en diversos subsistemas de almacenamiento. Con la CLI, puede cargar un archivo de script desde un disco y ejecutar el mismo. La CLI proporciona una forma de ejecutar los mandatos de gestión del almacenamiento en más de un subsistema de almacenamiento en red. Puede utilizar la CLI tanto en sitios de instalación como en entornos de desarrollo.

Para obtener más información sobre la CLI de Storage Manager, consulte la *IBM System Storage DS3000, DS4000, and DS5000 Command Line Interface and Script Commands Programming Guide*.

Uso del Editor de scripts

En vez de utilizar la interfaz gráfica de usuario para realizar funciones de gestión del subsistema de almacenamiento, se facilita una ventana de Editor de scripts para ejecutar comandos de gestión mediante scripts. Si utiliza la versión de firmware de controlador 5.4x.xx.xx o anterior, algunas de las funciones de la interfaz gráfica de usuario no están disponibles a través de los comandos de script.

Storage Manager 10.xx con firmware de controlador 07.xx.xx.xx y posterior, proporciona soporte completo para todas las funciones de gestión mediante comandos SMcli.



```
Tests - F600B4 - Script Editor - CreateLUN.txt
File Edit Tools Help

create logicalDrive driveCount=4 userLabel="2882_1_R51" RAIDLevel=5
capacity=4GB owner=a;
create logicalDrive array=1 userLabel="2882_1_R52" RAIDLevel=5 capacity=4GB
owner=b;

create hostGroup userLabel="MPROGrp";
create host userLabel="MPRO" hostGroup="MPROGrp";
create hostport UserLabel="MPRO1" host="MPRO" identifier="210000e08b04e23d"
hostType=5;
create hostport UserLabel="MPRO2" host="MPRO" identifier="210000e08b012a63"
hostType=5;

Performing syntax check...
Syntax check complete.
```

ds50_001138

Figura 12. Ventana del Editor de scripts

Importante: Tenga cuidado al ejecutar los comandos; el Editor de scripts no le solicita confirmación para las operaciones destructivas como los comandos para **Eliminar matrices** y **Restablecer la configuración del subsistema de almacenamiento**.

No todos los comandos de script se implementan en todas las versiones de firmware de controlador. Cuanto menos reciente sea la versión de firmware, más pequeño será el conjunto de comandos de script disponibles. Para obtener información sobre los comandos de script y las versiones de firmware, consulte la ventana Gestión empresarial de Storage Manager.

Para ver una lista de los comandos disponibles y su sintaxis, consulte la ayuda sobre referencia de comandos en línea.

Para abrir el Editor de scripts, complete los pasos siguientes:

1. Seleccione un subsistema de almacenamiento en la vista de árbol o la vista de tabla de la pestaña **Dispositivo**.
2. Pulse **Herramientas > Ejecutar script**.
3. Se abrirá la ventana del Editor de scripts. En la ventana se presentan la vista Script y la vista Resultado. Una barra de separación divide la ventana en la vista Script y la vista Resultado. Arrastre la barra de separación para redimensionar las vistas.

En la vista Script, puede especificar y editar comandos de script. La vista Resultado muestra los resultados de las operaciones. La vista Script soporta las siguientes pulsaciones de edición:

Ctrl+A

Selecciona todo en la ventana

Ctrl+C

Copia el texto marcado de la ventana en un almacenamiento intermedio de portapapeles de Windows

Ctrl+V

Copia el texto del almacenamiento intermedio de portapapeles de Windows en la ventana

Ctrl+X Borra (corta) el texto marcado en la ventana

Ctrl+Inicio

Mueve el cursor a la parte superior de la ventana de scripts

Ctrl+Fin

Mueve el cursor a la parte inferior de la ventana de scripts

La siguiente lista muestra las directrices generales para utilizar el Editor de scripts:

- Todas las sentencias debe finalizar con punto y coma (;).
- Cada comando y sus parámetros primarios y secundarios deben estar separados por un espacio.
- El Editor de scripts no diferencia entre mayúsculas y minúsculas.
- Cada sentencia nueva debe comenzar en una línea diferente.
- Se pueden añadir comentarios a los scripts para facilitarle a usted y a otros usuarios la comprensión del objetivo de las sentencias del comando.

El Editor de scripts soporta los dos formatos de comentario siguientes:

- Texto contenido tras dos barras oblicuas (//) hasta que se llega a un carácter de fin de línea

Por ejemplo:

```
//El siguiente comando asigna unidades de repuesto en caliente.  
set drives [1,2 1,3] hotspare=true;
```

El comentario //El siguiente comando asigna unidades de repuesto en caliente. se incluye para aclaración y no es procesado por el Editor de scripts.

Importante: Debe finalizar los comentarios que comiencen con // con un carácter de fin de línea, que debe insertar pulsando la tecla Intro. Si el motor de scripts no encuentra un carácter de fin de línea en el script tras procesar un comentario, se mostrará un mensaje de error y el script fallará.

- Texto entre los caracteres /* y */

Por ejemplo:

```
/* El siguiente comando asigna unidades de repuesto en caliente.*/  
set drives [1,2 1,3] hotspare=true;
```

El comentario /*El siguiente comando asigna unidades de repuesto en caliente.*/ se incluye para aclaración y no es procesado por el Editor de scripts.

Importante: El comentario debe comenzar con /* y finalizar con */. Si el motor de scripts no encuentra una notación de comentario al comienzo y final, se mostrará un mensaje de error y el script fallará.

Capítulo 5. Configuración de hosts

Después de configurar el subsistema o subsistemas de almacenamiento, utilice la información de este capítulo para habilitar todos los hosts de forma que se conecten a los subsistemas de almacenamiento. Este capítulo consta de las siguientes secciones:

- “Arranque de un sistema operativo host con un arranque SAN”
- “Uso de controladores multi-ruta para gestionar automáticamente la migración tras error y restablecimiento de unidades lógicas” en la página 133
- “Identificación de dispositivos” en la página 179
- “Configuración de dispositivos” en la página 182

Arranque de un sistema operativo host con un arranque SAN

El arranque SAN es la capacidad para arrancar un sistema operativo host desde un dispositivo de red de área de almacenamiento (SAN). En este caso, el dispositivo es un LUN de un subsistema de almacenamiento DS3000, DS4000 o DS5000. El arranque SAN se denomina también *arranque remoto*, en el que el LUN de arranque está en el subsistema de almacenamiento en vez de dentro del alojamiento del servidor y el servidor está conectado al subsistema de almacenamiento en una SAN. Las conexiones podrían ser conexiones directas o por medio del entorno de conexión a SAN - SAS, FC o iSCSI.

Con el arranque de SAN, se obtienen las siguientes ventajas:

Consolidación de servidores

Cada servidor puede arrancarse desde una imagen del sistema operativo de la SAN.

Recuperación simplificada de errores de servidor

No se necesita reinstalar el sistema operativo.

Recuperación rápida ante desastres

El subsistema de almacenamiento se puede replicar en un sitio de recuperación remoto.

Para implementar el arranque SAN se deben dar las siguientes condiciones:

- Configuración SAN, distribución en zonas de ambos dispositivos, configuraciones multi-ruta (si aplicable)
- Ruta activa única al LUN de arranque. Durante el proceso de instalación, solo debe estar habilitada una ruta al LUN de arranque antes de instalar y habilitar un controlador multi-ruta.
- BIOS de HBA; debe estar habilitado el arranque seleccionable o BIOS de arranque.

Para configurar un subsistema de almacenamiento para el arranque SAN, utilice las siguientes directrices:

1. Configure el entorno de conexión a SAN:
 - a. Cree la distribución en zonas SAN y reúna los dispositivos de canal de fibra en grupos lógicas en la configuración física del tejido. Cada dispositivo de una SAN debe ubicarse en diversas zonas.

- b. Elimine todas las rutas de los puertos HBA del servidor excepto una, al LUN de arranque. Para ello, inhabilite el puerto del conmutador del resto de rutas físicas.
2. Configure el subsistema de almacenamiento:
 - a. Cree el LUN.
 - b. Correlacione el LUN con el host como LUN 0.

Nota: Debe saber el WWNN del HBA, puede obtenerlo en la etiqueta del HBA.

3. Configure los HBA que desea arrancar desde SAN:
 - a. Compruebe que el BIOS de arranque está habilitado en el dispositivo HBA configurado para el host.
 - b. Cuando el host se esté iniciando, especifique el BIOS de arranque para su dispositivo HBA.
 - c. Seleccione el HBA que desea utilizar para el arranque SAN y configure el BIOS de forma que el LUN de arranque se designe como dispositivo de arranque preferido. Cuando el subsistema de almacenamiento haya descubierto el WWPN de los HBA, debe configurarlos como HBA del LUN de arranque, utilizando los procedimientos de correlación host.

Nota:

- 1) El HBA debe haber iniciado sesión en el subsistema de almacenamiento. Aunque aún no haya ningún LUN disponible, puede utilizar el BIOS para descubrir el subsistema de almacenamiento.
 - 2) Para obtener más información, consulte la documentación facilitada con su HBA.
- d. Guarde los cambios, salga del BIOS y reinicie el servidor. Ahora el BIOS se puede utilizar para descubrir el LUN recién configurado.
4. Inicie la instalación arrancando desde el soporte de instalación:
 - a. Durante la instalación, su soporte de sistema operativo le preguntará desde que unidad (o LUN) desea realizar la instalación. Seleccione la unidad que corresponde a su dispositivos de subsistema de almacenamiento.

Nota: Si durante la instalación se le piden controladores de dispositivos de otros fabricantes, seleccione el controlador de HBA disponible en otro tipo de soporte.

- b. Elija la opción predeterminada para la partición de disco.

Nota: Asegúrese de que el LUN elegido tiene el tamaño suficiente para el sistema operativo. Para Linux y la mayoría de sistemas operativos, 20 GB es suficiente para el dispositivo de arranque. Para las particiones de intercambio, asegúrese de que el tamaño es al menos igual al de la memoria física de su servidor.

5. Complete la instalación y finalice el procedimiento de arranque SAN:
 - a. Reinicie el servidor de nuevo y abra el menú de opciones de arranque. El dispositivo de arranque que ha configurado está listo para el arranque.
 - b. Seleccione la opción de arranque desde una unidad de disco duro/SAN, y seleccione el HBA asociado con el dispositivo de disco SAN en el que se ha completado la instalación. El dispositivo de arranque de instalación aparecerá ahora entre los dispositivos arrancables descubiertos en el HBA seleccionado.
 - c. Seleccione el dispositivo aplicable y realice el arranque.

- d. Defina el dispositivo de arranque instalado como dispositivo de arranque predeterminado para el sistema.

Nota: Este paso no es obligatorio. Sin embargo, el dispositivo de arranque instalado debe ser el dispositivo de arranque predeterminado para habilitar rearranques inesperados una vez completado este procedimiento.

- e. **Solo Linux – Para completar la instalación en Linux, complete los siguientes pasos:**

- 1) Compruebe que el enlace persistente de `/var/mpp/devicemapping` está actualizado. El archivo `/var/mpp/devicemapping` comunica a RDAC qué subsistema de almacenamiento debe configurar primero. Si se van a añadir subsistemas de almacenamiento adicionales al servidor, el subsistema de almacenamiento con el volumen de arranque/raíz siempre debe ser el primero en el archivo de correlaciones de dispositivos. Para actualizar este archivo, ejecute el comando siguiente:

```
# mppUpdate
```

- 2) Tras ejecutar el comando `# mppUpdate`, solicite el archivo `/var/mpp/devicemapping` con el siguiente comando:

```
# cat /var/mpp/devicemapping 0:<DS4x00 SAN Boot Device>
```

El subsistema de almacenamiento con el volumen de arranque/raíz debe estar en la entrada 0. Si el volumen de arranque/raíz no está en la entrada 0, edite el archivo para clasificar de nuevo las entradas del sub sistema de almacenamiento de forma que la matriz del volumen de arranque/raíz aparezca en la entrada 0.

- 3) Ejecute el comando `# mppUpdate`. La instalación se ha completado.

Ya pueden añadirse rutas adicionales entre el subsistema de almacenamiento y el servidor. Si el servidor se va a utilizar para gestionar el subsistema de almacenamiento, Storage Manager puede instalarse en el servidor.

Para obtener información adicional sobre el uso de controladores multi-ruta, consulte “Uso de controladores multi-ruta para gestionar automáticamente la migración tras error y restablecimiento de unidades lógicas” en la página 133.

Descripción general de los controladores multi-ruta

Una de las funciones principales de la característica de **migración tras error** es proporcionar gestión de rutas. Si existe más de una ruta desde el servidor al controlador, algunos controladores multi-ruta también pueden dispersar las E/S (entradas/salidas) entre las rutas. Por favor, consulte la documentación de su controlador de migración tras error multi-ruta para obtener más información.

Nota: Las conexiones entre los hosts y los subsistemas de almacenamiento de las figuras siguientes pretenden ilustrar el concepto de controlador multi-ruta. No se trata de recomendaciones.

LaFigura 13 en la página 122 yFigura 14 en la página 123 muestran el flujo de E/S en la ruta óptima única y las dos rutas desde el servidor al controlador.

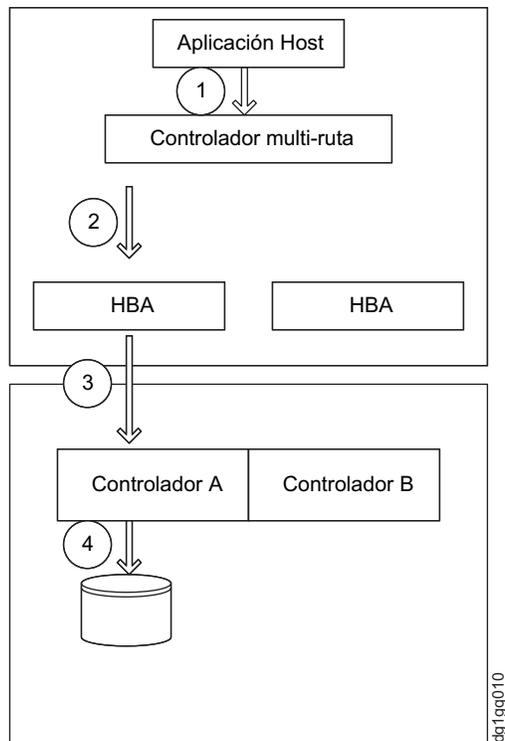


Figura 13. Flujo de E/S en una ruta única óptima

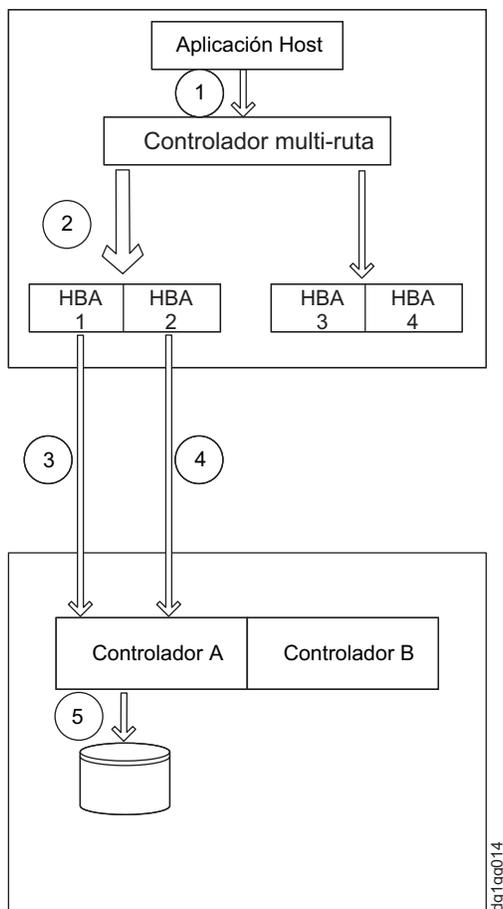


Figura 14. Flujo de E/S en dos rutas óptimas

La Figura 14 también ilustra que las E/S a la unidad lógica pueden rotar entre todas las rutas disponibles si el controlador multi-ruta es compatible.

Migración tras error

Los controladores multi-ruta supervisan las rutas de datos al subsistema de almacenamiento si no funcionan correctamente o en caso de diversos errores de enlace. Si los controladores multi-ruta detectan alguna de estas condiciones, comprueba la tabla de rutas en busca de rutas redundantes y controladores. El controlador de falla realiza una falla de ruta si las rutas al mismo controlador están disponibles. La Figura 15 en la página 124 muestra que el controlador multi-ruta utiliza solo una de las dos rutas al controlador porque la otra ruta falla. Si fallan todas las rutas a un controlador, el controlador multi-ruta realiza una migración tras error de controlador, como se muestra en la Figura 16 en la página 125 y la Figura 17 en la página 126. Aquí, cuando falla el controlador A, el controlador multi-ruta cambia la propiedad de la unidad lógica del controlador A al controlador B. Así, el controlador B recibe y procesa todas las E/S e la unidad lógica.

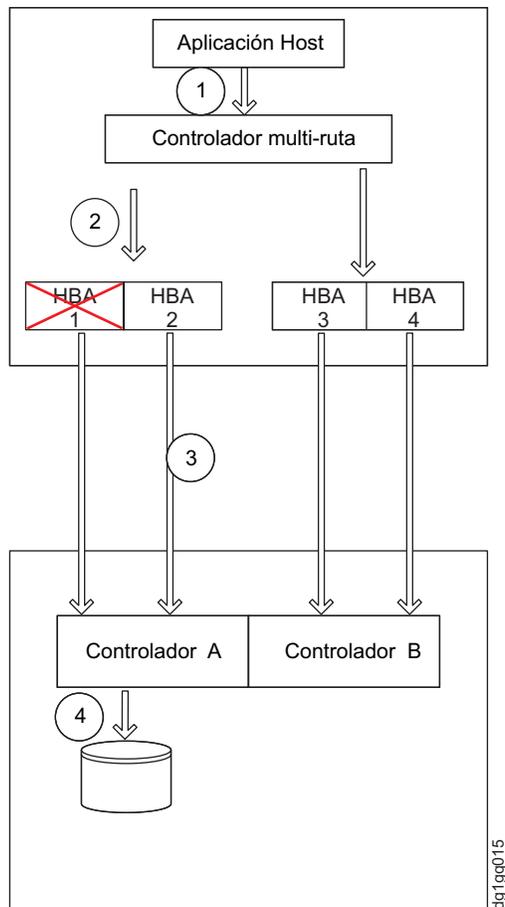


Figura 15. Uso de una ruta cuando la otra falla.

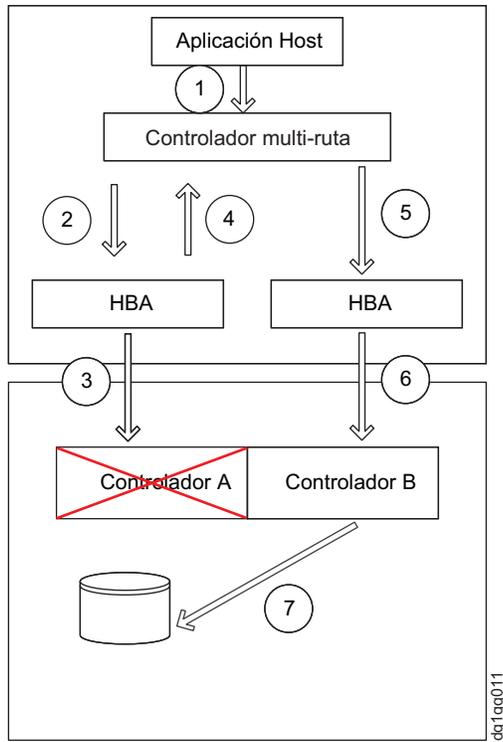


Figura 16. Migración tras error de E/S en un entorno de ruta única

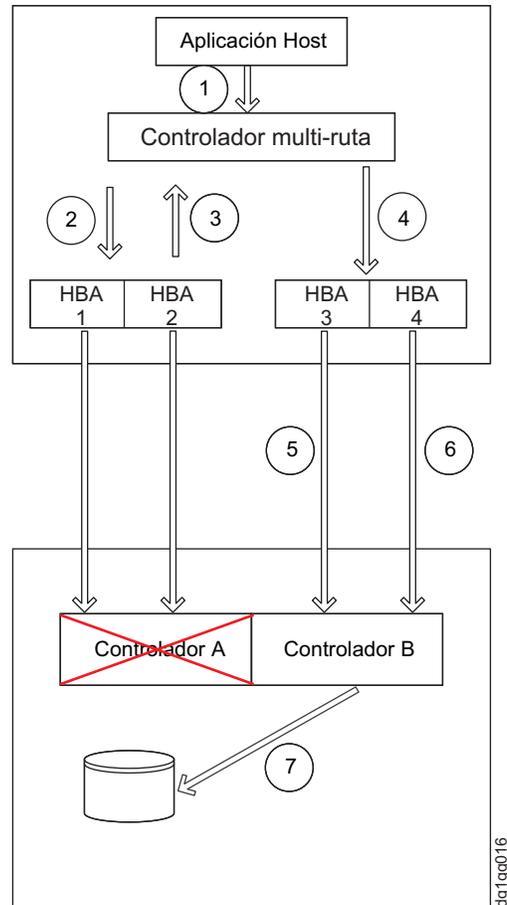


Figura 17. Migración tras error de E/S en un entorno multi-ruta

Dependiendo del firmware de controlador y el código de controlador multi-ruta, el controlador multi-ruta lleva a cabo diferentes acciones en caso de migración tras error en función del modo de migración tras error habilitado seleccionando el host adecuado indicado en la Tabla 22 en la página 131. Dependiendo de su versión de firmware de controlador, existen tres modos de migración tras error de controlador:

1. Modalidad de migración tras error Transferencia automática de volúmenes (AVT/ADT) - Si el tipo de host se configura para habilitar la modalidad de migración tras error AVT/ADT, el controlador multiruta redirigirá las E/S al controlador que quede. Puede configurar el controlador que quede de forma que asuma la propiedad de la unidad lógica y las E/S de procesos. La propiedad se puede establecer independientemente de si el controlador fallido está activo y ejecución. Esto es parecido a la situación en la que todas rutas a un controlador fallen, o falle el propio controlador. Las versiones de firmware de controlador 7.77.xx.xx o anteriores tienen soporte para esta modalidad de migración tras error.
2. Modo de migración tras error RDAC - Si el tipo de host está definido para **inhabilitar AVT/ADT** o **no ALUA**, el controlador multi-ruta emitirá una página de modo 2C al controlador superviviente para cambiar la propiedad de la unidad lógica al mismo. A continuación, este controlador asumirá la propiedad de la unidad lógica y procesará las E/S en él. El controlador superviviente asumirá la propiedad de la unidad lógica independientemente de que el otro controlador esté activo y en ejecución o no, como ocurre en los casos en los que

todas las rutas al controlador fallan o falla el propio controlador. Este modo de migración tras error se soporta con todas las versiones de firmware de controlador.

3. Modo de acceso asimétrico a unidad lógica (ALUA) - Con la versión de firmware de controlador 7.83.xx.xx y posteriores, si el tipo de host está definido para habilitar ALUA, el controlador multi-ruta redireccionará las E/S al controlador que funciona correctamente. Si el controlador "FALLIDO" está activo y en ejecución como ocurre cuando el controlador falla pero es óptimo, el controlador superviviente enviará las E/S al controlador "FALLIDO" para el procesamiento en vez de asumir la propiedad de la unidad lógica y procesar las E/S. Si esta condición persiste durante más de 5 minutos, el controlador superviviente dejará de enviar las E/S al otro controlador para el procesamiento y asumirá la propiedad y el procesamiento de las E/S a la unidad lógica.

Las ventajas de ALUA son:

- El servidor de "Arranque desde SAN" no fallará durante el arranque porque el LUN de arranque no está en la ruta o no es propiedad del controlador que está en la ruta explorada en primer lugar por el servidor durante el proceso de arranque del mismo. El servidor de arranque desde SAN está en el servidor cuyo disco de sistema operativo reside en una de las unidades lógicas del subsistema de almacenamiento en vez de internamente en el chasis del servidor.
- Eliminación innecesaria de migraciones tras error/suspensiones de unidades lógicas si se producen interrupciones de ruta intermitentes de corta duración (<5 minutos).
- Prevención de "ping pong de LUN" en determinadas condiciones en las que las unidades lógicas se correlacionan con servidores en un entorno de clúster.
- La unidad lógica opera como activa-activa en una configuración de controlador dual. Las E/S se pueden enviar a ambos controladores para el procesamiento independientemente de qué controlador posea la unidad lógica. En modo de migración tras error RDAC o AVT/ADT, solo el controlador que posee la unidad lógica puede procesar las E/S de la misma. Esto se denomina también modo de operación activa-pasiva en configuraciones de controlador dual.

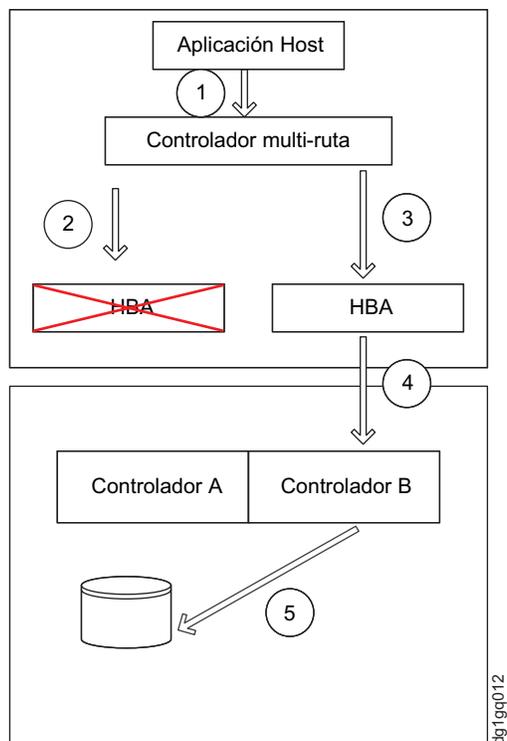


Figura 18. Todas las rutas al controlador fallan en modo de migración tras error AVT/ADT y RDAC

La Figura 18 ilustra la migración tras error cuando fallan todas las rutas al controlador pero el controlador es óptimo en los modos AVT/ADT y RDAC. En este escenario de migración tras error, la propiedad de la unidad lógica se transfiere al controlador B y este procesa todas las E/S a las unidades lógicas aunque el controlador A esté activo y sea óptimo y la migración está causada solo por un error en la ruta entre el host y el controlador A. La Figura 19 en la página 129 y la Figura 20 en la página 130 ilustran la migración tras error cuando fallan todas las rutas al controlador pero este es óptimo en modo de migración tras error ALUA.

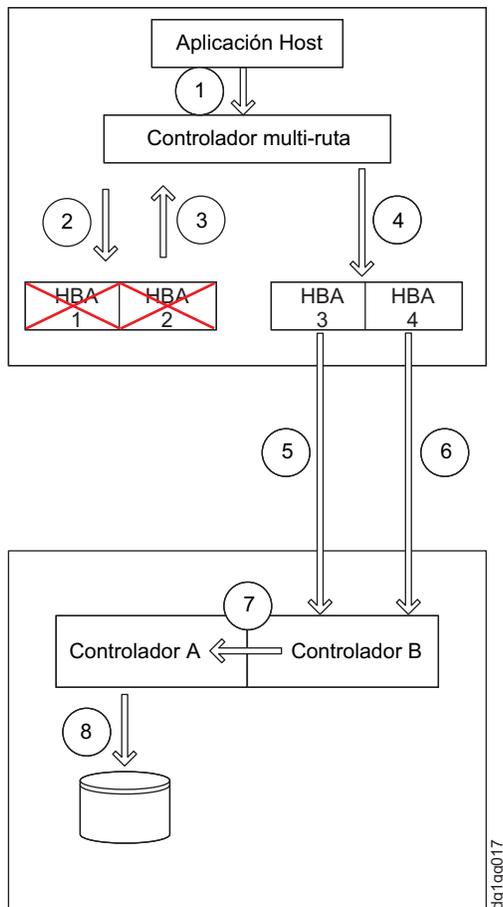


Figura 19. Todas las rutas al controlador fallan en modo de migración tras error ALUA. Cinco primeros minutos de la migración tras error.

Durante los cinco primeros minutos de la migración tras error, las E/S de la unidad lógica se envían internamente al controlador A para su procesamiento, como se muestra en la Figura 19. El controlador A sigue siendo el propietario de la unidad lógica. Tras estos cinco minutos, si la ruta al controlador A sigue fallando, el controlador B asume la propiedad y el procesamiento de las E/S a la unidad lógica, como se muestra en la Figura 20 en la página 130.

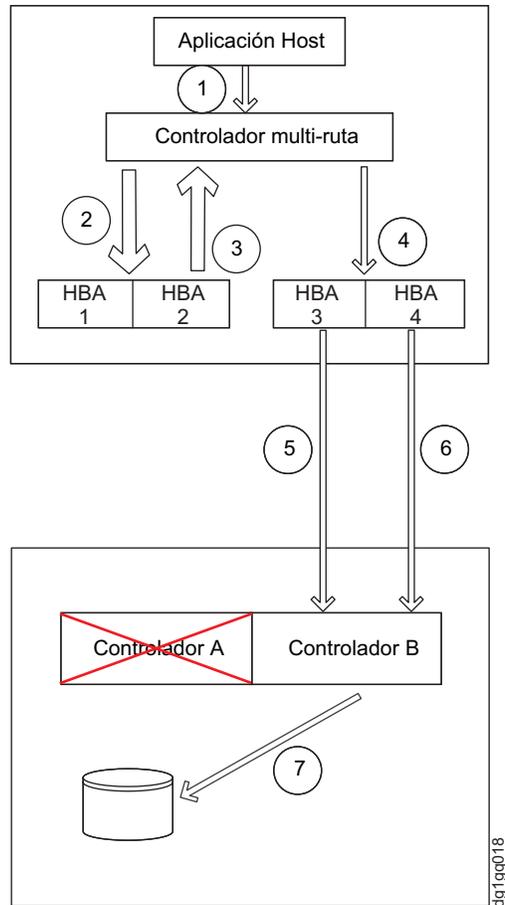


Figura 20. Todas las rutas al controlador fallan en modo ALUA. Cinco minutos de error

Cuando se opera en los modos de migración tras error 1 y 2 anteriores, el controlador dual del subsistema de almacenamiento opera en una combinación activa-pasiva desde la perspectiva del LUN correlacionado. Esto significa que las E/S solo se pueden enviar al controlador que posee el LUN correlacionado para su procesamiento. El otro controlador permanecerá en modo inactivo hasta que el controlador que posee el LUN o todas las rutas al mismo fallen. Las E/S enviadas al controlador que no posee el LUN correlacionado harán que el LUN migre a ese controlador (modo AVT/ADT) o falle en ese controlador (modo RDAC). En modo de migración tras error ALUA, los controladores duales operan ahora en una combinación activa-activa desde la perspectiva del LUN correlacionado. Las E/S se pueden enviar a ambos controladores para el procesamiento en vez de únicamente al controlador propietario. El controlador que no posee el LUN no tiene que operar en modo inactivo/pasivo hasta que el controlador propietario del LUN falla. Las E/S se direccionan automáticamente de forma interna al controlador que posee el LUN para su procesamiento. Además, la propiedad del LUN solo cambia cuando un controlador procesa más del 75% de las E/S del LUN durante un periodo de 5 minutos en modo ALUA.

Las versiones de firmware de controlador 7.77.xx.xx y anteriores soportan los modos de migración tras error AVT/ADT y RDAC. Las versiones de firmware de controlador 7.83.xx.xx y posteriores solo soportan los modos de migración tras error RDAC y ALUA. El modo AVT/ADT no es compatible con las versiones de firmware de controlador 7.83.xx.xx o posteriores. Tenga en cuenta que el mismo bit NVSRAM del controlador de la región de tipo de host se utiliza para habilitar

AVT/ADT o ALUA. Dependiendo de la versión del firmware de controlador, el bit se habilita en modo de migración tras error AVT/ADT o ALUA. Para habilitar el modo de migración tras error adecuado, debe seleccionar el tipo de host apropiado para la partición de host del servidor. En la siguiente tabla se indica el tipo de host para los diversos sistemas operativos y el modo de migración tras error habilitado para cada tipo de host:

Tabla 22. Modo de migración tras error para cada sistema operativo

Índice de host	Tipo de host (nombre completo)	Tipo de host (nombre abreviado) ₁	ADT/AVT ₂	RDAC	ALUA ₂
0	Valor predeterminado	Base	No	Sí	No
1	MacOS	MacOS	No	Sí	No
2	Windows Server 2003/Server 2008 Non-Clustered <Windows>	W2KNETNCL/Windows	No	Sí	No
3	Windows Server 2003/Server 2008 Non-Clustered <Windows>	W2KNETNCL/Windows Clustered	No	Sí	No
4	AIX con Veritas DMP	AIXAVT	Sí	No	No
5	Linux/ Linux con Veritas DMP	LNHAVT/Linux	Sí	No	No
6	AIX	AIX	No	Sí	No
7	HP-UX	HPX	Sí	No	No
8	Solaris (Sparc) <Solaris (con o sin MPXIO)>	SOL	No	Sí	No
9	Windows Server 2003/Server 2008 Clustered Non-Clustered (soporte DMP)	W2KNETNCLDMP <Windows DMP>	Sí	No	No
10	Unused 10/Irix ³	Unused10/Irix	No	Sí	No
11	Unused 11/Netware Failover ³	Unused11/Netware	No	Sí	No
12	IBM TS SAN VCE	IBM TS SAN VCE	Sí	No	No
13	Linux Cluster	LNXCUSTER/ LNXCCLVMWARE <Linux Cluster>	No	Sí	No
14	Solaris (con Veritas DMP)	SOLAVT	Sí	No	No
15	Windows Server 2003/Server 2008 Clustered Clustered (soporte DMP)	W2KNETCLDMP	Sí	No	No
16	VMWARE <VMWare>	VMWARE	Sí	No	No
17	HP-UX TPGS	HPXTPGS	No	Sí	No

Tabla 22. Modo de migración tras error para cada sistema operativo (continuación)

Índice de host	Tipo de host (nombre completo)	Tipo de host (nombre abreviado) ₁	ADT/AVT ₂	RDAC	ALUA ₂
18	Linux <Linux Non-ADT>	LNX <Linux Non-ADT>	No	Sí	No
19	IBM I/Os	IBM i	No	Sí	No
20	Onstor	Onstor	Sí	No	No
21	Windows ALUA	W2KALUA	No	No	Sí
22	Linux ALUA	LNXALUA	No	No	Sí
23	AIX ALUA w/ TPGS	AIXATPGSLUA	No	No	Sí
24	VMWARE ALUA w/ TPGS	VMWareTPGSALUA	No	No	Sí
25	Mac OS ALUA w/ TPGS	MacOSTPGSALUA	No	No	Sí
26	HP-UX ALUA w/ TPGS	HPXTPGSALUA	No	No	Sí
27	Solaris ALUA w/ TPGS	SOLTPGSALUA	No	No	Sí

Nota:

1. El nombre real podría ser ligeramente diferente dependiendo de la versión del archivo NVSRAM cargada. No obstante, el índice del tipo de host debería ser el mismo en todas las versiones.
2. Aunque el mismo bit NVSRAM habilita ADT/AVT dependiendo del firmware del controlador, solo los tipos de host ALUA (índice de host 21-27) deben utilizarse para habilitar el modo de migración tras error ALUA ya que se necesitan valores específicos de ALUA adicionales.
3. Los tipos de host de migración tras error Irix y Netware están definidos en los archivos NVSRAM en las versiones de firmware de controlador 7.77.xx.xx o anteriores. Para firmware de controlador 7.83.xx.xx o posterior, los servidores Netware e Irix no se soportan como conexión host; así, el tipo de host se cambia por 'Unused'.

Restablecimiento

Los controladores multi-ruta también supervisan el estado de las rutas que fallan de manera periódica y realizan el restablecimiento de la unidad lógica al controlador preferido una vez que se restaura la ruta errónea. En caso de que alguna de las diversas rutas al controlador falle y sea restaurada, el controlador multi-ruta comenzará a utilizar la ruta restaurada de nuevo para enviar E/S. El controlador multi-ruta utiliza el mismo modo (AVT/ADT, RDAC o ALUA) descrito en la sección de migración tras error para devolver la unidad lógica al controlador preferido.

La característica de restablecimiento automático de la unidad lógica del controlador multi-ruta puede estar inhabilitada en configuraciones de clúster de servidor para evitar problemas con el 'ping-pong de LUN' entre controladores en determinados escenarios de migración tras error.

Uso de controladores multi-ruta para gestionar automáticamente la migración tras error y restablecimiento de unidades lógicas

Los sistemas host conectados a un subsistema de almacenamiento DS3000, DS4000 o DS5000 para la actividad de E/S requieren un controlador multi-ruta (en ocasiones denominado controlador RDAC o de migración tras error) para la redundancia de rutas de canal de fibra. El controlador de migración tras error supervisa las rutas de E/S. Si se produce un error de componente en una de las rutas de canal de fibra, el controlador multi-ruta redirecciona todas las E/S hacia una ruta diferente. Su controlador multi-ruta depende del sistema operativo que tenga instalado.

En entornos Microsoft Windows otro controlador multi-ruta, denominado Windows RDAC, se facilitaba antes con el software Storage Manager versión 9 y anterior. El soporte de Windows RDAC finalizó con Storage Manager versión 10, y posteriores en conjunción con la versión de firmware de controlador 7.xx.xx.xx y posteriores. Además, ya no se ofrece soporte para AIX fcp_array. Los usuarios de AIX fcp_array deben migrar al controlador multi-ruta AIX MPIO lo antes posible.

Un adaptador de bus de host (HBA) de canal de fibra de IBM proporciona la interfaz entre un servidor de host y un subsistema de almacenamiento. Los HBA de canal de fibra de subsistema de almacenamiento son adaptadores de host de bus maestro de alto rendimiento, con acceso directo a la memoria diseñados para sistemas de alta gama. Estos HBA soportan todos los dispositivos periféricos de canal de fibra compatibles con conexiones de bucle privado, conexión directa y bucle en tejido. El controlador de dispositivo IBM Host Adapter permite a su sistema operativo comunicarse con el HBA de canal de fibra.

La Tabla 16 indica los controladores multi-ruta soportados por los diferentes sistemas operativos. Consulte el SSIC para determinar qué controlador multi-ruta es compatible con una determinada versión de SO y un modelo de subsistema de almacenamiento concreto.

Tabla 23. Controlador multi-ruta por sistema operativo

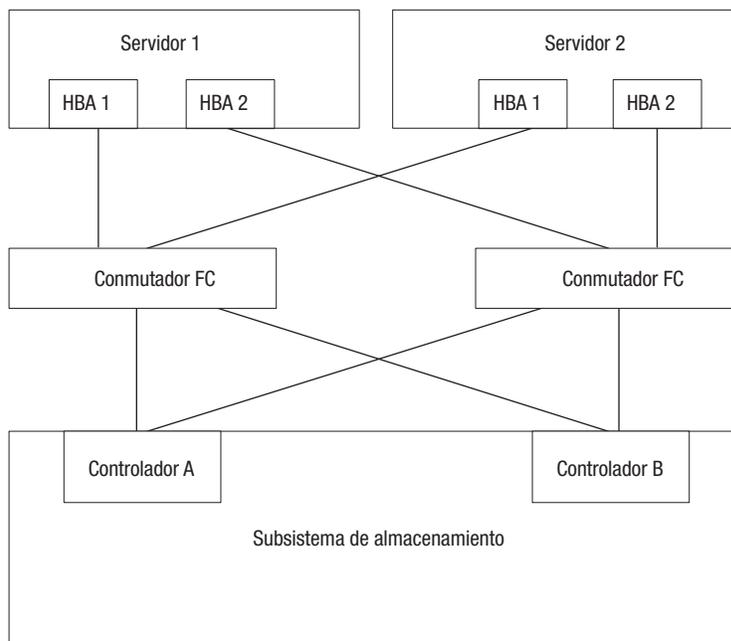
Sistema operativo	Controlador multi-ruta
AIX	fcp_array (también denominado RDAC), MPIO o SDDPCM
HP-UX	LVM , multi-ruta nativa o IBM SDD
Linux	MPP (también denominado Linux RDAC o RDAC), Veritas DMP, o (in-distro) Linux Device Mapper Multipath (DM-Multipath) nativo
Sistema operativo Mac	Proporcionado por el fabricante de HBA
NetWare	Novell MPE
Solaris	RDAC, MPxIO o Veritas DMP
SVC	SDD
VMware	NMP
Windows	MPIO DSM o Veritas DMP DSM

Con la excepción de Windows MPIO, los archivos del controlador multi-ruta no se incluyen en el DVD de Storage Manager. Compruebe SSIC y el archivo léame de Storage Manager para conocer las versiones de conjunto de archivo mínimas necesarias para su sistema operativo. Para saber cómo encontrar los archivos léame

en Internet, consulte “Búsqueda de software, firmware de controlador y archivos léame de Storage Manager” en la página xv. Para instalar el controlador multi-ruta, siga las instrucciones de “Instalación de un controlador multi-ruta” en la página 138.

Multi-ruta se refiere a la capacidad del host de reconocer diversas rutas al dispositivo de almacenamiento. Esto se realiza utilizando diversos puertos HBA o dispositivos del servidor de host conectados a conmutadores en tejido SAN, también conectados a varios puertos de los dispositivos de almacenamiento. Para los productos de almacenamiento denominados DS3000, DS4000 o DS5000, estos dispositivos tienen dos controles dentro del subsistema de almacenamiento que gestionan y controlan las unidades de disco. Estos controladores se comportan de manera activa o pasiva. De la propiedad y control de un LUN particular se encarga un controlador. El otro controlador está en modo pasivo hasta que se produce un error, momento en el cual la propiedad del LUN se transfiere a ese controlador. Cada controlador puede tener más de un puerto de tejido para la conectividad con el entorno de conexión a SAN.

La Figura 21 muestra un ejemplo de configuración multi-ruta para todos los sistemas operativos excepto configuraciones multi-ruta AIX fcp_array y Solaris RDAC. La Figura 22 en la página 135 muestra un ejemplo de configuración multi-ruta para AIX fcp_array, Microsoft Windows RDAC (ya no soportado) y Solaris RDAC.



Consulte “Unidades admitidas por IBM System Storage DS Storage Manager” en la página 67 para obtener más información.

Figura 21. Ejemplo de configuración de HBA de host a subsistema de almacenamiento para todos los controladores multi-ruta excepto AIX fcp_array y Solaris RDAC

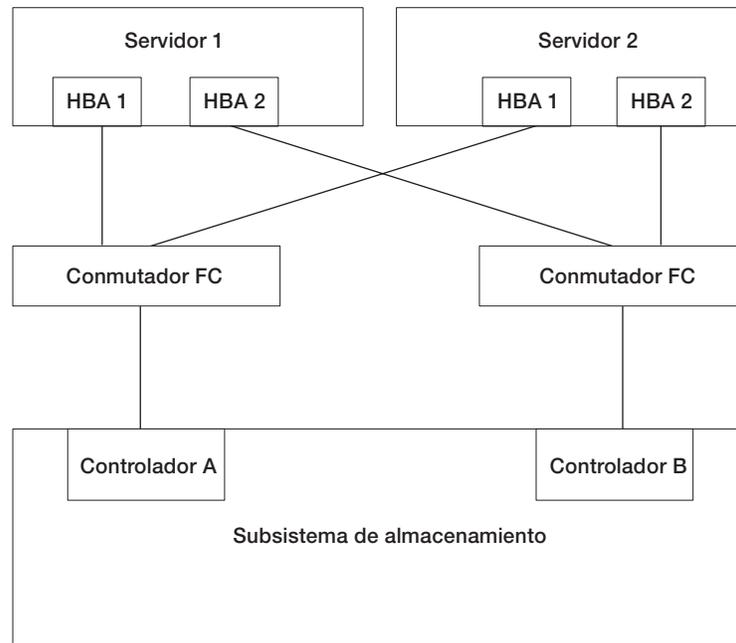


Figura 22. Ejemplo de configuración de HBA de host a subsistema de almacenamiento para controladores multi-ruta AIX fcp_array y Solaris RDAC

La mayoría de controladores multi-ruta soportan varias rutas. La Tabla 24 muestra el número de rutas que puede soportar cada controlador. Tenga en cuenta que AIX fcp_array y Solaris RDAC solo soportan dos rutas, una hacia cada controlador.

Tabla 24. Número de rutas que soporta cada controlador multi-ruta por sistema operativo

Controlador	Número de rutas	Valor predeterminado
AIX MPIO	Ilimitado	No aplicable
AIX RDAC	2	No aplicable
HP-UX nativo	65,536	No aplicable
HP-UX PVlinks	8,192	No aplicable
Linux MPP	Ilimitado	4
Linux Veritas DMP	Ilimitado	No aplicable
Sistema operativo Mac	Ilimitado	No aplicable
Solaris MPxIO	Ilimitado	No aplicable
Solaris RDAC	2	No aplicable
Solaris Veritas DMP	Ilimitado	No aplicable
SVC	32	No aplicable
VMware	Ilimitado - 8 o menos para un mejor rendimiento	No aplicable
Windows MPIO DSM	32 rutas por LUN, 16 por controlador	4
Windows Veritas DMP DSM	Ilimitado	No aplicable

Uso de adaptadores de bus de host

Esta sección ofrece una visión general básica sobre los adaptadores de bus de host (HBA), así como instrucciones para conectar HBA en un entorno con conmutador de canal de fibra.

Comprensión de los adaptadores de bus de host

Los adaptadores de bus de host (HBA) se utilizan para conectar servidores a topologías de canal de fibra. La función de un HBA es similar a la de los adaptadores de red utilizados para acceder a recursos LAN. El controlador de dispositivo de un HBA normalmente se encarga de proporcionar soporte a una topología de canal de fibra, bien sea punto a punto, en bucle o de tejido. Los subsistemas de almacenamiento DS3000, DS4000 y DS5000 aceptan adaptadores de bus de host (HBA) de canal de fibra (FC), SCSI con conexión en serie (SAS), canal de fibra en Ethernet (FCoE) e iSCSI para conectar los servidores de host a los subsistemas de almacenamiento. Estos subsistemas de almacenamiento también soportan iSCSI a través de los adaptadores NIC Ethernet normales. No obstante, los subsistemas de almacenamiento DS3000, DS4000 y DS5000 no aceptan todos los HBA. Para obtener información detallada sobre soporte de HBA, vaya a <http://www.ibm.com/systems/support/storage/config/ssic>.

Consulte la documentación para obtener información sobre los valores de HBA que se pueden personalizar para un entorno de sistema operativo concreto. Esta documentación también incluye instrucciones sobre cómo cambiar estos valores. Tenga cuidado al cambiar estos valores, ya que una definición incorrecta puede causar la reducción del rendimiento o errores intermitentes. Consulte el archivo léame incluido en el paquete del controlador del dispositivo, firmware o BIOS del adaptador de bus de host para conocer los cambios actualizados de la configuración. Las tablas de Apéndice A, "Host bus adapter settings", en la página 303 muestran los valores necesarios de los ajustes seleccionados para diversos proveedores de HBA.

Conexión de HBA en un entorno de conmutador de canal de fibra

Existen dos esquemas de distribución en zonas primarios que puede utilizar cuando conecta adaptadores de bus de host (HBA) de canal de fibra de servidores de host a puertos de host de subsistemas de almacenamiento en un entorno de conmutador de canal de fibra. En un esquema de distribución en zonas uno a uno, cada puerto HBA se asigna a un puerto de host de controlador. En un esquema de distribución en zonas uno a dos, cada puerto HBA se asigna a dos puertos de host de controlador.

Como regla general, el HBA y las conexiones del puerto de host del subsistema de almacenamiento deben distribuirse en zonas para minimizar las posibles interacciones entre los puertos en un entorno de conexión a SAN. El esquema de distribución en zona uno a uno, aunque no es obligatorio, minimiza las interacciones porque conecta un puerto HBA a un solo puerto de host de servidor. No obstante, el esquema de distribución en zonas a elegir depende de su topología de entorno de conexión a SAN y de las prestaciones de sus conmutadores de canal de fibra.

Dependiendo de su topología de entorno de conexión a SAN y de las prestaciones de sus conmutadores de canal de fibra, puede implementar uno de los dos esquemas de distribución en zonas siguiente en Figura 23 en la página 137 y Figura 24 en la página 138.

Nota: Para obtener más información sobre las mejores prácticas y requisitos de distribución en zonas, consulte la *Guía de referencia sobre hardware de conmutador de canal de fibra* u otra documentación facilitada con el conmutador de canal de fibra. Para enlaces a documentación de conmutador del sitio web de IBM, vaya a

www.ibm.com/servers/storage/support/san/index.html

En este esquema de distribución en zonas (indicado por la barra traslúcida), se asigna un puerto de HBA a un puerto de host de controlador.

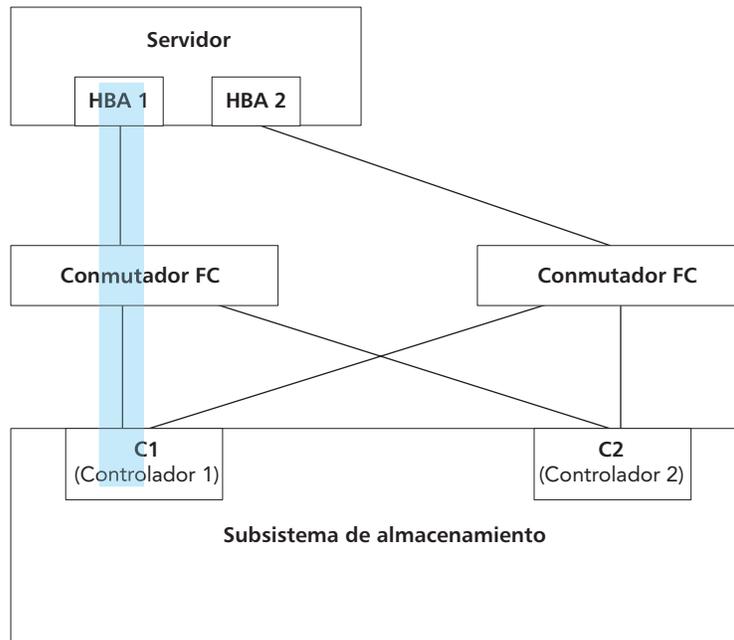


Figura 23. Esquema de distribución en zonas uno a uno

En este esquema de distribución en zonas (indicado por las barras traslúcidas), se asigna un puerto de HBA a dos puertos de host de controlador.

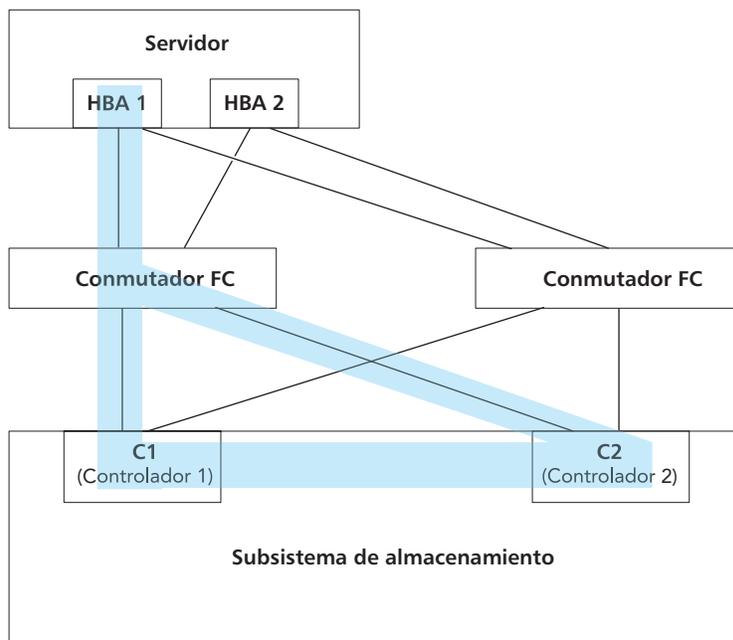


Figura 24. Esquema de distribución en zonas uno a dos

Instalación de un controlador multi-ruta

Debe instalar un controlador multi-ruta en todos los hosts conectados con su subsistema de almacenamiento, independientemente de que estos hosts tengan diversas rutas al subsistema de almacenamiento. Esta sección describe diversos controladores multi-ruta, cómo comprobar el nivel de versión de controlador multi-ruta actual, cómo actualizar el controlador del dispositivo multi-ruta y cómo verificar si se ha completado la actualización multi-ruta.

Controlador multi-ruta MPIO o MPIO/DSM para Windows Descripción general

Este controlador multi-ruta se incluye en el paquete de software host Storage Manager para Windows. MPIO es un kit DDK de Microsoft para desarrollar código para la gestión de dispositivos multi-ruta. El kit DDK contiene un conjunto de controladores binarios que se instalan con el Módulo específico de dispositivos(DSM) del subsistema de almacenamiento; los controladores están diseñados para proporcionar una arquitectura de sistema transparente basado en Microsoft Plug and Play. Estos controladores binarios facilitan funcionalidad multi-ruta LUN y conservan la compatibilidad con las pilas de controlador de dispositivos Microsoft Windows de manera simultánea. En Windows Server 2003, el MPIO se instala con el MPIO DSM. En Windows Server 2008, solo se instala el MPIO DSM porque Windows 2008 tiene ya instalado MPIO.

El controlador de MPIO lleva a cabo las siguientes tareas:

- Detecta y reclama los dispositivos de disco físicos presentados por los subsistemas de almacenamiento (de acuerdo con las cadenas Identificador de producto o Proveedor) y gestiona las rutas lógicas a los dispositivos físicos

- Presenta una instancia única de cada LUN al resto del sistema operativo Windows
- Proporciona una interfaz óptima a través de WMI para uso por parte de aplicaciones de modo de usuario
- Se basa en el Módulo específico de dispositivos (DSM) del proveedor (IBM) para la siguiente información sobre el comportamiento del subsistema de almacenamiento:
 - Información de direccionamiento de E/S
 - Condiciones que requieren que se reintente, falle, migre tras error o suspenda una solicitud; por ejemplo, errores de proveedor único
 - Funciones misceláneas como los comandos de liberación o reserva

Mientras no reclamen el mismo dispositivo de disco, se pueden instalar diversos DSM para diferentes subsistemas de almacenamiento en disco en el mismo servidor de host.

Comandos de Liberación/Reserva SCSI-2 nativos en un entorno multi-ruta

Si existen diversas rutas a un solo controlador y se recibe un comando liberación/reserva (R/R) SCSI-2 para una unidad lógica, el controlador MPIO DSM selecciona una ruta a cada controlador y repite la solicitud (denominada ruta de reserva). Esta función es necesaria porque los controladores no pueden aceptar solicitudes R/R SCSI-2 a través de diversas rutas para una unidad lógica determinada. Una vez establecida la ruta de reserva, las solicitudes de E/S posteriores de las unidades lógicas se restringen en esa ruta hasta que se reciba el comando de liberación SCSI-2. El controlador MPIO DSM distribuye las rutas de reserva si se correlacionan varias unidades lógicas con el host, distribuyendo las cargas en diversas rutas hacia el mismo controlador.

Nota: Este método de reserva SCSI es incompatible con la característica ALUA del controlador. No se debe utilizar cuando dicha característica está habilitada.

Conversión de comandos de Liberación/Reserva SCSI-2 a reservas persistentes SCSI-3

El controlador MPIO DSM también soporta la capacidad de convertir los comandos R/R SCSI-2 en reservas persistentes SCSI-3. Esta función permite a una unidad lógica utilizar una de las políticas de equilibrio de carga mencionadas anteriormente en todas las rutas disponibles del controlador en vez de en una sola. Esta característica requiere el establecimiento de una "clave de reserva" única para cada host por parte del controlador MPIO DSM. Esta clave se almacena en el Registro y se llama S2toS3Key. Si esta clave está presente, las conversiones se realizan o se utiliza el método de "clonación".

Valores de tiempo de espera de E/S por protocolo

El valor asociado con solicitudes de E/S sin traspaso, como las solicitudes de lectura/escritura, se basan en el parámetro **TimeoutValue** del controlador del disco de Microsoft, como se define en el Registro. Una característica del DSM permite aplicar un valor de tiempo de espera personalizado basándose en el protocolo (por ejemplo canal de fibra, SAS o iSCSI) que utiliza una ruta. Los valores de tiempo de espera por protocolo proporcionan los siguientes beneficios:

- Sin valores de tiempo de espera por protocolo, el valor **TimeOutValue** es global y afecta a todo el almacenamiento.
- **TimeOutValue** normalmente se restablece cuando se actualiza un controlador HBA.
- En Windows Server 2003, el valor de tiempo de espera del disco predeterminado se puede ajustar en función del tamaño de la solicitud de E/S. Ajustar el valor de tiempo de espera del disco predeterminado ayuda a soportar dispositivos SCSI de legado.
- La característica de tiempo de espera personalizado de DSM permite definir un valor de tiempo de espera más predecible para entornos Windows Server 2003. Para obtener información sobre los parámetros configurables para la característica de tiempo de espera personalizado, vaya a la sección de Valores de configuración para Windows DSM y Linux RDAC.

La característica de tiempo de espera por protocolo modifica ligeramente el modo en que se evalúa el parámetro **SynchTimeout**. El parámetro **SynchTimeout** determina el tiempo de espera de E/S para las solicitudes síncronas generadas por el controlador de DSM.

Entre los ejemplos se incluyen conversiones de SCSI-2 a SCSI-3 PR y comandos de averiguación utilizados durante el descubrimiento de dispositivos. Es importante que el valor de tiempo de espera de las solicitudes del controlador de DSM sea al menos igual al valor de tiempo de espera de E/S por protocolo. Cuando se arranca un host, el controlador de DSM realiza estas acciones:

- Si el valor del parámetro **SynchTimeout** está definido en la clave de registro del controlador de DSM, registre el valor actual.
- Si el valor del parámetro **TimeOutValue** del controlador del disco Microsoft está definido en el Registro, registre el valor actual.
- Utilice el valor más alto de los dos como valor inicial del parámetro **SynchTimeout**.
- Si no se ha definido ningún valor, utilice el valor predeterminado de 10 segundos.
- Para cada solicitud de E/S síncrona, se utiliza el mayor de los valores de tiempo de espera de E/S por protocolo o parámetro **SynchTimeout**. Por ejemplo:
 - Si el valor del parámetro **SynchTimeout** es 120 segundos y el valor del parámetro **TimeOutValue** es de 60 segundos, se utiliza 120 segundos como valor inicial.
 - Si el valor del parámetro **SynchTimeout** es 120 segundos y el valor del parámetro **TimeOutValue** es de 180 segundos, se utiliza 180 segundos como valor inicial de las solicitudes de E/S síncronas del controlador de DSM.
 - Si el valor de tiempo de espera de E/S para un protocolo diferente (por ejemplo SAS) es 60 segundos y el valor inicial es 120 segundos, la E/S se enviará utilizando un tiempo de espera de 120 segundos.

Transferencia de LUN selectiva

Esta característica limita las condiciones en que el controlador de DSM mueve un LUN al controlador alternativo a tres casos:

1. Cuando un controlador de DSM con una ruta a un único controlador, la ruta no preferida, descubre una ruta al controlador alternativo.
2. Cuando una solicitud de E/S se dirige a un LUN propiedad de la ruta preferida pero el controlador de DSM está asociado solo a la ruta no preferida.

3. Cuando una solicitud de E/S se dirige a un LUN propiedad de la ruta no preferida pero el controlador de DSM está asociado solo a la ruta preferida.

El caso 2 y caso 3 tienen estos parámetros configurables por el usuario que se pueden definir para ajustar el comportamiento de esta característica.

- El número máximo de veces que la transferencia de LUN será emitida. Este valor de parámetro evita que se produzca una condición de hiperpaginación de propiedad continua en los casos en que el alojamiento del controlador o de la unidad del controlador se conecta a otro host que requiere que el LUN sea propiedad del controlador actual.
- Se intenta un tiempo de retardo antes de las transferencias de LUN. Este parámetro se utiliza para evitar errores de enlace de ruta de E/S intermitentes. Durante el retardo de tiempo, las solicitudes de E/S se reintentarán en el controlador actual para aprovechar la posibilidad de que otro host haga la transición del LUN al controlador actual.

Para obtener información sobre estos dos parámetros, vaya a la sección de Valores de configuración para Windows DSM y el RDAC de Linux.

En el caso de que el sistema host esté conectado a ambos controladores y se devuelva una E/S con un estado 94/01, en el que el LUN no tiene propietario pero puede tenerlo, el controlador de DSM modifica sus datos internos sobre el controlador a utilizar para ese LUN y emite de nuevo el comando al otro controlador. Para evitar interferir con otros hosts que pudieran estar conectados con un alojamiento de controlador o de unidades del controlador, el controlador de DSM no emite un comando de transferencia de LUN a dichos alojamientos.

Cuando el DSM detecta que se necesita una operación de transferencia de unidad lógica, no emitirá un comando de migración tras error/abandono inmediatamente. Con los valores predeterminados, esperará tres segundos antes de enviar el comando al subsistema de almacenamiento. Este retardo proporciona tiempo para reunir el mayor número de operaciones de transferencia de unidades lógicas como sea posible. El controlador une las operaciones de transferencia de unidades lógicas y rechaza todos los comandos de transferencia adicional hasta que haya completado la operación en curso. Esto hace que durante un periodo el subsistema de almacenamiento no se haga cargo correctamente de las E/S. Introduciendo un retardo durante el cual se pueden agregar las operaciones de transferencia de unidades lógicas en una operación por lotes, el DSM reduce la probabilidad de que una operación de transferencia de unidades lógicas supere el límite de reintentos. En grandes configuraciones de sistema, quizá deba aumentar el valor de retardo de tres segundos ya que, con más hosts en la configuración, podrían enviarse más comandos de transferencia de unidades lógicas.

El valor de retardo se encuentra en: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\.`

Esta función se habilita cuando se dan estas condiciones:

- El alojamiento del controlador o las unidades del controlador no tiene AVT habilitado.
- El parámetro configurable del controlador de DSM **ClassicModeFailover** está definido en 1.
- El parámetro configurable del controlador de DSM **DisableLunRebalance** está definido en 4.

Clúster de migración tras error de Windows

La agrupación en clúster de Windows Server 2008 OS y Windows Server 2008 R2 OS utiliza las reservas persistentes SCSI-3 de manera nativa. Como resultado, el controlador de DSM no realiza conversiones de comandos R/R SCSI-2 R/R y puede utilizar una de las políticas de equilibrio de carga mencionadas anteriormente en todas las rutas del controlador. Las conversiones se siguen realizando si el controlador de DSM se ejecuta en un entorno basado en el sistema operativo Windows Server 2003. Si opera en un entorno en clúster y no utiliza la característica de Envío de E/S del CFW o la característica de Transferencia de LUN selectiva del DSM, defina el parámetro **DisableLunRebalance** en 3. Para obtener información sobre este parámetro, vaya a la sección Valores de configuración para el DSM de Windows DSM y el RDAC de Linux.

Característica de envío de E/S para Acceso de unidad lógica asimétrico (ALUA)

La característica de envío de E/S soporta el ALUA. Con versiones anteriores del firmware del controlador(CFW), el módulo específico de dispositivos (DSM) tiene que enviar solicitudes de entrada/salida (E/S) para una unidad lógica particular al controlador que posee esa unidad lógica. Los controladores rechazan las solicitudes recibidas para unidades lógicas que no posea. Este comportamiento es necesario para que el subsistema de almacenamiento conserve la consistencia de datos en la unidad lógica. No obstante el mismo comportamiento es responsable de diversas áreas de contienda durante el arranque del sistema y condiciones de error multi-host/ruta.

Con la característica de envío de E/S, un subsistema de almacenamiento puede enviar solicitudes de E/S a través de cualquier controlador en una configuración dúplex. Cuando el controlador no propietario accede a una unidad lógica se produce una penalización de rendimiento. Para conservar el mejor rendimiento del subsistema de E/S, el DSM interactúa con el CFW para asegurar que las solicitudes de E/S se envíen al controlador propietario siempre que esté disponible.

Cuando instala o actualiza el DSM, de forma predeterminada se habilita la característica de Transferencia de LUN selectiva (SLT) para soportar el Envío de E/S. Algunos valores de registro se modifican durante la actualización de DSM si la versión anterior no habilita la SLT. Para evitar que se habilite la SLT para que su subsistema de almacenamiento opere sin la característica de Envío de E/S, edite el registro y observe los siguientes valores:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\

Controlador de dispositivo HBA Storport Miniport

En sistemas operativos Windows, Storage Manager ofrece el controlador de dispositivo MPIO DSM, basado en el modelo de controlador de dispositivo Microsoft Storport Miniport.

El modelo de controlador de dispositivo Storport Miniport se introdujo en Microsoft Windows Server 2003 sustituyendo al modelo SCSIport Miniport. Es el único modelo de controlador de dispositivo soportado por Windows Server 2003 y

Windows Server 2008, con soporte de servidores AMD64 y EM64T. No soporta el parámetro `buschange=0` para eludir el controlador Plug and Play del sistema operativo Microsoft Windows. En vez de esto, trabaja con el controlador Plug and Play para detectar la extracción e inserción de dispositivos en el puerto de adaptador de bus de host de canal de fibra.

Solo los subsistemas de almacenamiento DS4100, DS4200, DS4300 (modelos estándar o turbo), DS4400, DS4500, DS4700 y DS4800 soportan este controlador de dispositivo basado en Storport. Los modelos de subsistema de almacenamiento DS4100, DS4300 (modelos estándar o turbo), DS4400 y DS4500 deben tener el firmware de controlador versión 6.12.27.xx o posterior.

Consulte el archivo léame de Storage Manager para sistemas operativos Microsoft Windows para conocer requisitos adicionales, como los relacionados con las versiones de firmware del controlador o las actualizaciones.

Controlador de dispositivo HBA de minipuerto SCSIport

En entornos de sistema operativo Windows 2000, solo se soportan los controladores de dispositivo basados en el controlador de minipuerto SCSIport (no el modelo Storport).

En versiones anteriores del controlador de dispositivos SCSIport, el parámetro `buschange=0` permite al controlador multi-ruta RDAC controlar y supervisar la inserción y extracción de dispositivos del puerto del HBA impidiendo al controlador de dispositivos Microsoft Plug and Play gestionar el puerto de HBA. Esta nueva versión del controlador de dispositivos SCSIport que se utiliza con MPIO no soporta el parámetro `buschange=0`.

Importante: No todas las versiones de firmware de controlador de DS4000 y DS5000 soportan esta funcionalidad. Solo las versiones de firmware de controlador DS4000 y DS5000 06.12.27.xx (y posteriores) para modelos turbo o estándar DS4300 y subsistemas de almacenamiento DS4500 o versiones 6.16.8x.xx (y posteriores) para subsistemas de almacenamiento DS4200, DS4700 y DS4800 soportan el controlador de dispositivos de minipuerto SCSIport.

Antes de instalar el controlador de dispositivos, compruebe el archivo léame incluido en el archivo del paquete del controlador, así como el archivo léame incluido con el software host Storage Manager para Windows, para conocer los controladores de dispositivos y firmware de controlador soportados para subsistemas de almacenamiento DS3000, DS4000 o DS5000. Consulte “Búsqueda de software, firmware de controlador y archivos léame de Storage Manager” en la página xv para obtener más información acerca de cómo acceder a los archivos léame de Storage Manager en la web. Siga las instrucciones de instalación del controlador de dispositivos del archivo léame asociadas con su sistema operativo.

Nota: Lea el archivo léame del controlador de dispositivos para conocer las modificaciones necesarias en el BIOS del HBA predeterminado y los valores de registro del sistema operativo host para disfrutar de un rendimiento óptimo. Si hace cualquier cambio en los valores del BIOS de HBA, deberá rearrancar el servidor para que estos se apliquen.

Para obtener más información, consulte la documentación facilitada con su HBA de canal de fibra.

Uso de dsmUtil

El programa de utilidad dsmUtil es un programa de utilidad dirigido por la línea de comandos que funciona únicamente con la solución Multipath I/O (MPIO) Device Specific Module (DSM). La utilidad se utiliza principalmente como modo de solicitar al controlador de DSM que realice diversas tareas de mantenimiento, pero también puede servir como herramienta de resolución de problemas en caso de ser necesario.

Para utilizar la utilidad dsmUtil, escriba el siguiente comando y pulse Intro:

```
dsmUtil [[-a target_id]]  
[-c array_name | missing]  
[-d debug_level] [-e error_level] [-g  
virtual_target_id]  
[-o [[feature_action_name=value]] |  
[feature_variable_name=value]][, SaveSettings]] [-M]  
[-P [GetMpioParameters | MpioParameter=value | ...]]  
[-R]  
[-s "failback" | "avt" | "busscan" | "forcerebalance"]  
[-w target_wwn, controller_index]
```

Escriba dsmUtil sin ningún parámetro como muestra la información de uso. Consulte la tabla siguiente para conocer los parámetros de dsmUtil.

Tabla 25. Parámetros de dsmUtil

Parámetro	Descripción
-a <i>target_id</i>	Muestra un resumen de todos los subsistemas de almacenamiento vistos por el DSM. El resumen muestra el <i>target_id</i> , el WWID del subsistema de almacenamiento y el nombre del subsistema de almacenamiento. Si se especifica <i>target_id</i> , aparece información de estado puntual del DSM para el subsistema de almacenamiento. En sistemas operativos UNIX, el HBA virtual especifica identificadores de destino únicos para cada subsistema de almacenamiento. El controlador de HBA virtual de Windows MPIO no utiliza identificadores. El parámetro de esta opción se puede ver como desplazamiento en las estructuras de información del DSM, en donde cada desplazamiento representa un subsistema de almacenamiento diferente. Para uso únicamente por representantes de Soporte técnico y atención al cliente.
-c <i>array_name</i> missing	Borra las entradas del archivo WWN. Este archivo se encuentra en Archivos de programa\DSMDrivers\mppdsm\WWN_FILES con la extensión.wwn. Si se especifica la palabra clave <i>subsystem_name</i> , se borra el archivo WWN del subsistema de almacenamiento específico. Si se utiliza la palabra clave missing, se borran todos los archivos WWN de subsistemas de almacenamiento asociados anteriormente. Si no se utiliza ninguna palabra clave, se borran todos los archivos WWN de subsistemas de almacenamiento asociados actual y anteriormente.

Tabla 25. Parámetros de *dsmUtil* (continuación)

Parámetro	Descripción
-d <i>debug_level</i>	<p>Define el nivel de informe de depuración actual. Esta opción solo funciona si el controlador RDAC se ha compilado con la depuración habilitada. Los informes de depuración están compuestos por dos segmentos. El primer segmento se refiere a un área específica de funcionalidad, el segundo al nivel de realización de informes del área. El <i>debug_level</i> es uno de estos números hexadecimales:</p> <ul style="list-style-type: none"> • 0x20000000 – Muestra mensajes de la rutina de inicialización del controlador RDAC. • 0x10000000 – Muestra mensajes de la rutina de descubrimiento del controlador RDAC. • 0x08000000 – Muestra mensajes de la rutina <i>ioctl()</i> del controlador RDAC. • 0x04000000 – Muestra mensajes de la rutina de apertura de dispositivos del controlador RDAC (solo plataformas Linux). • 0x02000000 – Muestra mensajes de la rutina de lectura de dispositivos del controlador RDAC (solo plataformas Linux). • 0x01000000 – Muestra mensajes relacionados con comandos HBA. • 0x00800000 – Muestra mensajes relacionados con comandos terminado anormalmente. • 0x00400000 – Muestra mensajes relacionados con volcados de pánico. • 0x00200000 – Muestra mensajes relacionados con actividad de E/S síncrona. • 0x00100000 – Muestra mensajes relacionados con actividad de migración tras error. • 0x00080000 – Muestra mensajes relacionados con actividad de restablecimiento. • 0x00040000 – Muestra mensajes adicionales relacionados con actividad de restablecimiento. • 0x00010000 – Muestra mensajes relacionados con extracciones de dispositivos. • 0x00001000 – Muestra mensajes relacionados con actividad de reserva SCSI • 0x00000400 – Muestra mensajes relacionados con actividad de validación de rutas. • 0x00000001 – Nivel de depuración 1. • 0x00000002 – Nivel de depuración 2. • 0x00000004 – Nivel de depuración 3. • 0x00000008 – Nivel de depuración 4. <p>Estas opciones se pueden combinar con el operador lógico <i>or</i> (<i>o</i>) para proporcionar diversas áreas y niveles de informes según sea necesario. Para uso únicamente por representantes de Soporte técnico y atención al cliente.</p>

Tabla 25. Parámetros de *dsmUtil* (continuación)

Parámetro	Descripción
-e <i>error_level</i>	<p>Define el nivel de creación de informes de error actual como <i>error_level</i>, que puede ser uno de estos valores:</p> <ul style="list-style-type: none"> • 0 - Muestra todos los errores • 1 - Muestra la migración tras error de la ruta y el controlador, y los errores recuperados, fatales y repetibles. • 2 - Muestra la migración tras error de la ruta y el controlador, y los errores fatales y repetibles. • 3 - Muestra la migración tras error de la ruta y el controlador, y los errores fatales. Éste es el valor predeterminado. • 4 - Muestra la migración tras error del controlador y los errores fatales. • 5 - Muestra los errores fatales. <p>Para uso únicamente por representantes de Soporte técnico y atención al cliente.</p>
-g <i>target_id</i>	<p>Muestra información detallada sobre el estado de cada controlador, la ruta y los LUN del subsistema de almacenamiento especificado. Puede encontrar el <i>target_id</i> ejecutando el comando <i>dsmUtil -a</i>.</p>
-M	<p>Muestra las correlaciones disco a unidad MPIO del DSM. El resultado es similar al obtenido con el programa de utilidad SMdevices. Para uso únicamente por representantes de Soporte técnico y atención al cliente.</p>
-o [[<i>feature_action_name</i> = <i>value</i>]] [<i>feature_variable_name</i> = <i>value</i>]][, SaveSettings]	<p>Resuelve problemas de una característica o cambia un valor de configuración. Si la palabra clave <i>SaveSettings</i>, los cambios solo afectan al estado en la memoria de las variables. La palabra clave <i>SaveSettings</i> cambia tanto el estado en la memoria como el estado persistente. Algunos ejemplos de comando:</p> <ul style="list-style-type: none"> • <i>dsmUtil -o</i> - Muestra todos los nombres de acción de la característica disponibles. • <i>dsmUtil -o DisableLunRebalance=0x3</i> - Desactiva el reequilibrio de LUN del subsistema de almacenamiento con DSM iniciado (solo afecta al estado en la memoria).
-P [GetMpioParameters MpioParameter= <i>value</i> ...]	<p>Muestra y configura los parámetros MPIO. Para uso únicamente por representantes de Soporte técnico y atención al cliente.</p>
-R	<p>Elimina los valores de política de equilibrio de carga para los dispositivos inactivos.</p>

Tabla 25. Parámetros de dsmUtil (continuación)

Parámetro	Descripción
-s ["failback" "avt" "busscan" "forcerebalance"]	Inicia manualmente una de las tareas de exploración del controlador de DSM. Una exploración "failback" hace que el controlador de DSM reintente las comunicaciones con cualquiera de los controladores que hayan fallado. Una exploración "avt" hace que el controlador DSM compruebe si se ha habilitado o inhabilitado AVT para un subsistema de almacenamiento completo. Una exploración "busscan" hace que el controlador de DSM repase la lista de dispositivos sin configurar para ver si se ha configurado alguno de ellos. Una exploración "forcerebalance" hace que el controlador de DSM mueva unidades lógicas del subsistema de almacenamiento a su controlador preferido e ignore el valor del parámetro de configuración DisableLunRebalance del controlador de DSM.
-w target_wwn, controller_index	Para uso únicamente por representantes de Soporte técnico y atención al cliente.

Controlador de Veritas DMP DSM

Consulte la documentación de Symantec Storage Foundation para Windows para obtener instrucciones para instalar el controlador de Veritas DMP DSM en <http://www.symantec.com/business/support/>.

Controladores multi-ruta AIX

Un sistema host AIX requiere o AIX Redundant Disk Array Controller (RDAC) o el controlador de migración tras error MPIO para redundancia de ruta de canal de fibra. En los entornos Veritas soportados, el RDAC es el controlador de migración tras error compatible.

El controlador de migración tras error supervisa las rutas de E/S. Si se produce un fallo de un componente en una de las rutas de canal de fibra, el controlador de migración tras error dirige todas las E/S a otra ruta.

Nota: AIX soporta tanto el Redundant Disk Array Controller (RDAC) como la ruta múltiple E/S. Estos controladores multi-ruta son parte del sistema operativo AIX nativo. Consulte la documentación de AIX para obtener detalles sobre la instalación de estos controladores.

Controlador Linux Device Mapper Multipath

Device Mapper Multipath (DMMP o DM-MP) es una infraestructura genérica para dispositivos de bloque proporcionados por el sistema operativo Linux. Soporta la concatenación, la escritura en bandas, las instantáneas, la duplicación y la multi-ruta. La función de multi-ruta es una combinación de los módulos de kernel y herramientas del espacio de usuario.

Importante: El host en el que se instala el controlador Linux Device Mapper Multipath debe ser Linux no AVT/no ADR o LinuxCluster (LNXCLUSTER). Puede verificar el estado de ADT o AVT en la información del tipo de host del perfil del subsistema de almacenamiento. El ADT o AVT del host en el que está instalado el controlador Linux Device Mapper Multipath debe estar inhabilitado.

El controlador Device Mapper Multipath:

- Proporciona un nodo de dispositivos de bloque individual para una unidad lógica multi-ruta

- Garantiza la redirección de E/S a rutas disponibles en caso de error de ruta
- Garantiza que las rutas que fallan se revalidarán lo antes posible
- Configura diversas rutas para maximizar el rendimiento
- Vuelve a configurar diversas rutas automáticamente cuando se producen eventos
- Proporciona soporte de DMMP para unidades lógicas recién añadidas
- Proporciona persistencia de nombre para dispositivos DMMP de /dev/mapper/
- Configura diversas rutas automáticamente durante una fase temprana del rearranque para que el sistema operativo se pueda instalar y rearrancar en una unidad lógica multi-ruta

Device Mapper Multipath (DMMP o DM-MP) se soporta en las versiones SLES11, SLES11 SP1, RHEL 6.0, RHEL 6.1 o posteriores.

Instalación del controlador Device Mapper MultiPath

Device Mapper Multipath (DMMP o DM-MP) se soporta en las versiones SLES11, SLES11 SP1, RHEL 6.0, RHEL 6.1 o posteriores.

Consulte <http://www.ibm.com/systems/support/storage/config/ssic> para obtener información sobre los subsistemas DS3000/DS5000 y versiones de firmware de controlador soportados con DMMP.

Instalación de Device Mapper MultiPath en base SLES11

Nota: La funcionalidad ALUA no es compatible con la base SLES 11. Debe actualizar a SLES 11 SP1 o posterior con versión de firmware de controlador 7.8x.xx.xx o posterior.

EL sistema operativo base SLES 11 no dispone de todos los paquetes para soportar el Device Mapper para los subsistemas de almacenamiento IBM DS. Se recomienda utilizar las versiones más recientes de los siguientes componentes, si estuvieran disponibles. Además, debe tener al menos las siguientes versiones de los componentes:

Tabla 26. Versión mínima requerida para cada componente

Componente	Versión mínima	Ubicación de descarga
Kernel	kernel-default-2.6.27.29-0.1.1	http://download.novell.com/patch/finder
scsi_dh_rdac driver	lsi-scsi_dh_rdac-kmp-default-0.0_2.6.27.19_5-1	http://drivers.suse.com/driver-process/pub/update/LSI/sle11/common/x86_64/
Device Mapper library	device-mapper-1.02.27-8.6	http://download.novell.com/patch/finder
Kpartx	kpartx-0.4.8-40.6.1	http://download.novell.com/patch/finder
Multipath_tools	multipath-tools-0.4.8-40.6.1	http://download.novell.com/patch/finder

Asegúrese de instalar todos los paquetes dependientes antes de continuar. Para obtener más detalles, consulte la Guía de administración e instalación de SUSE Linux Enterprise Server 11 en el sitio web de Novel/SuSe.

Para instalar el Device Mapper Multipath en la base SLES11, complete los pasos siguientes:

1. Utilice el soporte facilitado por el proveedor del sistema operativo para completar la instalación de SLES 11.
2. Descargue e instale el kernel de erratas 2.6.27.29-0.1.
3. Rearranque el kernel 2.6.27.29-0.1.
4. Instale `device-mapper-1.02.27-8.6`.
5. Instale `kpartx-tools-0.4.8-40.6.1`.
6. Instale `multipath-tools-0.4.8-40.6.1`.
7. Actualice y configure `/etc/multipath.conf`. Un archivo de muestra se guarda en `/usr/share/doc/packages/multipath-tools/multipath.conf.synthetic`. Copie y renombre este archivo como `/etc/multipath.conf`. Para obtener más detalles, consulte "Trabajo con el archivo `Multipath.conf`" en la página 151.
8. Habilite el servicio multi-ruta utilizando el siguiente comando: **`#chkconfig multipathd on`**.
9. Edite el archivo `/etc/sysconfig/kernel` para añadir `scsi_dh_rdac` a la lista `INITRD_MODULES`. `scsi_dh_rdac` debería añadirse a `initrd`.
10. Instale `lsi-scsi_dh_rdac-kmp-default-0.0_2.6.27.19_5-1`.
11. Rearranque el host.

Instalación de Device Mapper MultiPath en SLES11 sp1 o posterior

Todos los componentes necesarios para DMMP se incluyen en el soporte de instalación de SUSE Linux Enterprise Server (SLES) versión 11.1 sp1. De forma predeterminada, DMMP está inhabilitado en SLES. Complete los pasos siguientes para habilitar los componentes de DMMP en el host:

Nota: El Acceso asimétrico a unidad lógica (ALUA) se soporta con el firmware de controlador 7.83.xx.xx o posterior. SLES sp2 y posteriores tienen los parches necesarios para ALUA como parte de la distribución de kernel.

1. Utilice el soporte facilitado por el proveedor del sistema operativo para completar la instalación de SLES11 sp1.
2. Si ha instalado SLES 11 sp2 o posterior, salte este paso. Además, ejecute `perform rpm -qa | grep <name of the package>` para verificar si se han instalado los siguientes paquetes.
 - `kpartx-0.4.8-40.21.1.1.09.00.0000.0006`
 - `multipath-tools-0.4.8-40.21.1.1.09.00.0000.0000`
 - `scsi_dh_rdac-kmp-default-09.00.0000.0006_2.6.32.12_0.7-sles11.1`

y para habilitar la característica ALUA, instale los paquetes utilizando los siguientes comandos `rpm` -

- `rpm -ivh kpartx-0.4.8-40.21.1.1.00.00.0000.0005.<arch>.rpm --force`
- `rpm -ivh multipath-tools-0.4.8-40.21.1.1.00.00.0000.0005.<arch>.rpm --force`
- `rpm -ivh scsi_dh_rdac-kmp-default-00.00.0000.000<X>_2.6.32.12_0.7-sles11.1.<arch>.rpm --force`

donde `<arch>` se sustituye por la arquitectura adecuada (`x86,x86_x64` , o `PPC64`)

3. Actualice y configure `/etc/multipath.conf`. Un archivo de muestra se guarda en `/usr/share/doc/packages/multipath-tools/multipath.conf.synthetic`.

Copie y renombre este archivo como `/etc/multipath.conf`. Para obtener más detalles, consulte “Trabajo con el archivo Multipath.conf” en la página 151.

4. Habilite el servicio `multipathd` utilizando el siguiente comando: **`#chkconfig multipathd on`**.
5. Edite el archivo `/etc/sysconfig/kernel` para añadir `scsi_dh_rdac` a la lista `INITRD_MODULES`. `scsi_dh_rdac` debería añadirse a `initrd`.
6. Cree la nueva imagen `initrd` utilizando el siguiente comando: **`# mkinitrd -k /boot/vmlinuz-$(uname -r) -i /boot/initrd-$(uname -r)-scsi_dh -M /boot/System.map-$(uname -r)`**
7. Actualice el archivo de configuración del cargador de arranque (`grub.conf`, `lilo.conf`, o `yaboot.conf`) con el nuevo `initrd` creado.
8. Rearranque el host para arrancar la nueva imagen `initrd`.

Instalación de Device Mapper Multi-Path en RHEL 6.0, RHEL 6.1 o posterior

Todos los componentes necesarios para DMMP se incluyen en el soporte de instalación de RHEL 6 y 6.1. De forma predeterminada, DMMP está inhabilitado. Complete los pasos siguientes para habilitar los componentes de DMMP en el host.

Nota: El Acceso asimétrico a unidad lógica (ALUA) no se soporta en RHEL 6.0. Debe actualizar a RHEL 6.1 o posterior, y el firmware de controlador debe ser 7.83.xx.xx o posterior.

1. Utilice el soporte facilitado por el proveedor del sistema operativo para completar la instalación de RHEL 6.0, RHEL 6.1 o posterior.
2. Si ha instalado RHEL 6 actualización 2, salte este paso, ya que RHEL 6 actualización 2 o posterior ya cuenta con los parches necesarios para el soporte de ALUA. Estos parches forman parte de la distribución del kernel. Además, ejecute `perform rpm -qa | grep <name of the package>` para verificar si se han instalado los siguientes paquetes.
 - `kpartx-0.4.8-40.21.1.1.09.00.0000.0006`
 - `multipath-tools-0.4.8-40.21.1.1.09.00.0000.0000`
 - `scsi_dh_rdac-kmp-default-09.00.0000.0006_2.6.32.12_0.7-sles11.1`

y para habilitar la característica ALUA, instale los paquetes utilizando los siguientes comandos `rpm` -

- `rpm -ivh kpartx-0.4.8-40.21.1.1.00.00.0000.0005.<arch>.rpm --force`
- `rpm -ivh device-mapper-multipath-libs-0.4.9-41.1.e16.00.00.0000.0005.<arch>.rpm --force`
- `rpm -ivh device-mapper-multipath-0.4.9-41.1.e16.00.00.0000.000<X>.<arch>.rpm --force`
- `rpm -ivh scsi_dh_rdac-kmod-00.00.0000.0005-e16.<arch>.rpm`

donde `<arch>` se sustituye por la arquitectura adecuada (`x86,x86_x64`, o `PPC64`)

3. Actualice y configure `/etc/multipath.conf`. Un archivo de muestra se guarda en `/usr/share/doc/packages/multipath-tools/multipath.conf.synthetic`. Copie y renombre este archivo como `/etc/multipath.conf`. Para obtener más detalles, consulte “Trabajo con el archivo Multipath.conf” en la página 151.
4. Habilite el servicio `multipathd` utilizando el siguiente comando: **`#chkconfig multipathd on`**.
5. Cree una imagen `initramfs` utilizando el controlador `scsi_dh_rdac`:
 - a. Cree un archivo `scsi_dh_alua.conf` en el directorio `/etc/modprobe.d/`.

- b. En este archivo, añada lo siguiente: **alias scsi_hostadapter99
scsi_dh_rdac**
6. Ejecute el siguiente comando para crear una imagen initramfs:**dracut -f /boot/initrd-\$(uname -r)-scsi_dh \$(uname -r)**
7. Actualice el archivo de configuración del cargador de arranque (grub.conf , lilo.conf, o yaboot.conf) con initramfs.
8. Rearranque el host para arrancar la nueva imagen initramfs.

Trabajo con el archivo Multipath.conf

Multipath.conf es el archivo de configuración del daemon multi-ruta, multipathd. Este archivo sobrescribe la tabla de configuración incorporada para multipathd. Todas las líneas del archivo que comiencen con un carácter que no sea un espacio vacío # son líneas de comentarios. Las líneas vacías se deben ignorar.

De forma predeterminada, DMMP se soporta en determinados modelos ed máquina de los subsistemas IBM DS3000/DS5000. No obstante, IBM recomienda sustituir los valores predeterminados utilizando el archivo multipath.conf para asegurarse de que los valores de DMMP son adecuados:

Para configurar el archivo multipath.conf, complete los siguientes pasos:

1. Copie el ejemplo de multipath.conf del directorio adecuado, dependiendo de si su sistema operativo es Redhat RHEL o Novell SLES, en el directorio /etc.
 - En SLES, el archivo se llama multipath.conf.synthetic y está almacenado en el siguiente directorio: /usr/share/doc/packages/multipath-tools/.
 - En RHEL, el archivo se llama multipath.conf.defaults y está almacenado en el siguiente directorio: /usr/share/doc/device-mapper-multipath-0.4.9/.
2. Renombre el archivo multipath.conf.
3. Haga los cambios de configuración descritos en esta sección en el archivo /etc/multipath.conf. El contenido del archivomultipath.conf varía, dependiendo de si procede de los kernels de SLES o RHEL.

Nota: Todas las entradas de los dispositivos multi-ruta se comentan inicialmente. Para eliminar los comentarios, elimine el primer carácter (#) de esta sección. Debe eliminar los comentarios de las tres secciones - default, blacklist y devices.

El archivo de configuración está dividido en cinco secciones:

defaults

Especifica todos los valores predeterminados.

blacklist

Incluye en la lista negra las nuevas instalaciones. La lista negra predeterminada se incluye en la sección sin comentarios del archivo /etc/multipath.conf. Incluya en la lista negra el Device Mapper Multipath mediante WWID si no desea utilizar esta funcionalidad.

blacklist_exceptions

Especifica todas las excepciones de artículos de la sección blacklist.

devices

Indica todos los dispositivos multi-ruta con su proveedor y valores de producto.

multipaths

Indica todos los dispositivos multi-ruta con sus valores WWID.

Para determinar los atributos de un dispositivo multi-ruta, compruebe la sección multipaths del archivo `/etc/multipath.conf`; después la sección `devices`; y por último la sección `defaults`. Dependiendo de la versión del kernel de Linux, la sección `devices` del archivo `multipath.conf` de ejemplo podría tener valores definidos para el identificador de producto de su modelo de subsistema de almacenamiento. Lo único que debe hacer es verificar si los valores coinciden con los valores recomendados indicados a continuación. De lo contrario, tendrá que especificar los valores de los dispositivos manualmente para el identificador de producto de su modelo de subsistema. Si tiene diversos subsistemas de almacenamiento con diferentes identificadores de producto conectados al host Linux, añada los valores de dispositivo para cada identificador de producto de subsistema de almacenamiento en la sección `devices` del archivo `/etc/multipath.conf`. Los valores de muestra para DS3500 (identificador de producto 1746) y DS5100/DS5300 (identificador de producto 1818) de la sección `devices` del archivo `multipath.conf` en sistemas operativos SLES son los siguientes:

Nota: Si el identificador de producto tiene más de cuatro caracteres, utilice únicamente los cuatro primeros. En el siguiente ejemplo, aunque el identificador de producto es '1746 FAStT', el producto se especifica como '1746'. De forma similar, '1818 FAStT' se especifica como '1818'.

```
Devices {
  device {

        vendor                "IBM"
        product                "1746"
        path_grouping_policy   group_by_prio
        getuid_callout         "/lib/udev/scsi_id -g -u -d /dev/%n"
        path_selector          "round-robin 0"
        path_checker           rdac
        features               "2 pg_init_retries 50"
        hardware_handler       "1 rdac"
        prio                   rdac
        failback               immediate
        no_path_retry          15
        rr_min_io              100
        rr_weight               priorities
    }

  device {

        vendor                "IBM"
        product                "1818"
        path_grouping_policy   group_by_prio
        getuid_callout         "/lib/udev/scsi_id -g -u -d /dev/%n"
        path_selector          "round-robin 0"
        path_checker           rdac
        features               "2 pg_init_retries 50"
        hardware_handler       "1 rdac"
        prio                   rdac
        failback               immediate
        no_path_retry          15
        rr_min_io              100
        rr_weight               priorities
    }
}
```

Los valores de muestra para DS3500 (identificador de producto 1746) y DS5100/DS5300 (identificador de producto 1818) de la sección `devices` del archivo `multipath.conf` en sistemas operativos RHEL son los siguientes:

```
Devices {
  device {

        vendor                "IBM"
```

```

        product                "1746"
        path_grouping_policy    group_by_prio
        getuid_callout          "/lib/udev/scsi_id
                                --whitelisted --device=/dev/%n"

        path_selector           "round-robin 0"
        path_checker            rdac
        features                 "2 pg_init_retries 50"
        hardware_handler        "1 rdac"
        prio                     rdac
        failback                 immediate
        no_path_retry            15
        rr_min_io                100
        rr_weight                priorities
    }

device {

        vendor                  "IBM"
        product                  "1818"
        path_grouping_policy     group_by_prio
        getuid_callout          "/lib/udev/scsi_id
                                --whitelisted --device=/dev/%n"

        path_selector           "round-robin 0"
        path_checker            rdac
        features                 "2 pg_init_retries 50"
        hardware_handler        "1 rdac"
        prio                     rdac
        failback                 immediate
        no_path_retry            15
        rr_min_io                100
        rr_weight                priorities
    }

```

Si tiene LUN de acceso (en ocasiones denominados UTM LUN) correlacionados con las particiones del host, incluya una entrada en la sección blacklist del archivo `/etc/multipath.conf` para que este no sea gestionado por el DMMP. El software host Storage utiliza LUN de acceso para la gestión dentro de banda del subsistema de almacenamiento. Las entradas deben seguir el patrón del siguiente ejemplo:

```

blacklist {
    device {
        vendor "*"
        product "Universal Xport"
    }
}

```

La siguiente tabla describe los atributos y valores de la sección devices del archivo `/etc/multipath.conf`.

Tabla 27. Atributos y valores de parámetros del archivo `multipath.conf`

Atributo	Valor de parámetro	Descripción
<code>path_grouping_policy</code>	<code>group_by_prio</code>	Este atributo determina la política de agrupación de rutas que debe aplicarse a este proveedor y almacenamiento específico.

Tabla 27. Atributos y valores de parámetros del archivo *multipath.conf* (continuación)

Atributo	Valor de parámetro	Descripción
prio	rdac	Este atributo define el programa y argumentos para determinar la rutina de prioridad de rutas. La rutina especificada debe devolver un valor numérico especificando la prioridad relativa de esta ruta. Los miembros más altos tendrán una mayor prioridad.
getuid_callout	Para SLES"/lib/udev/scsi_id -g -u -d /dev/%n" Para RHEL"/lib/udev/scsi_id --whitelisted--device=/dev/%n"	Este atributo determina el programa y argumentos para solicitar y obtener un identificador de ruta único.
polling_interval	5	Este atributo determina el intervalo entre dos comprobaciones de ruta, en segundos.
path_checker	rdac	Este atributo establece el método utilizado para determinar el estado de la ruta.
path_selector	"round-robin 0"	Este atributo determina el algoritmo selector de ruta que debe utilizarse cuando hay más de una ruta en un grupo de rutas.
hardware_handler	"1 rdac"	Este atributo determina el controlador de hardware que se debe utilizar para tratar conocimientos específicos del dispositivo.
failback	inmediato	Este atributo determina cómo funciona gestionar el daemon el restablecimiento de un grupo de rutas. En este ejemplo, el parámetro está definido en 10 segundos, por lo que el restablecimiento se realiza 10 segundos después de que un dispositivo esté en línea. Para inhabilitar el restablecimiento, defina este parámetro como manual. Defínalo como immediate para hacer que el restablecimiento se realice de forma inmediata.

Tabla 27. Atributos y valores de parámetros del archivo `multipath.conf` (continuación)

Atributo	Valor de parámetro	Descripción
features	"2 pg_init_retries 50"	Este atributo habilita funciones. En este ejemplo, el parámetro del kernel <code>pg_init_retries</code> está definido en 50. El parámetro <code>pg_init_retries</code> se utiliza para reintentar los comandos de selección de modo.
no_path_retry	30	Este atributo determina el número de reintentos antes de inhabilitar la puesta en cola. Defina este parámetro como <code>fail</code> para el error inmediato (sin puesta en cola). Cuando este parámetro está definido en <code>queue</code> , la puesta en cola continúa de forma indefinida.
rr_min_io	100	El número de E/S que se direccionan a una ruta antes de cambiar a la siguiente ruta del mismo grupo.
rr_weight	priorities	Si se define como <code>priorities</code> el configurador multi-ruta asignará pesos de ruta como <code>"path prio * rr_min_io"</code>

Uso de dispositivos Device Mapper

Los dispositivos multi-ruta se crean en el directorio `/dev/` con el prefijo `dm-`. Estos dispositivos son iguales a cualquier otro dispositivo de bloque del host. Para ver todos los dispositivos multi-ruta, ejecute el comando **`multipath -ll`**. El siguiente ejemplo muestra el resultado del comando **`multipath -ll`** para uno de los dispositivos multi-ruta en una migración tras error no ALUA.

```
multipath (3600a0b80005ab177000017544a8d6b92) dm-0 IBM, 1746 FASTT
[size=5.0G][features=3 queue_if_no_path pg_init_retries
50][hw_handler=1 rdac][rw]
\_ round-robin 0 [prio=6][active]
\_ 5:0:0:0 sdc 8:32 [active][ready]
\_ round-robin 0 [prio=1][enabled]
\_ 4:0:0:0 sdb 8:16 [active][ghost]
```

El siguiente ejemplo muestra el resultado del comando **`multipath -ll`** para uno de los dispositivos multi-ruta en una migración tras error ALUA.

```
multipath (3600a0b800047516e00006d864f70696c) dm-11 IBM, 1746 FASTT
size=1.0G features='3 queue_if_no_path pg_init_retries 50' hw_handler='1 rdac' wp=rw
| +- policy='round-robin 0' prio=14 status=active
| | ^- 9:0:0:3 sdac 65:192 active ready running
| +- policy='round-robin 0' prio=9 status=enabled
| | ^- 10:0:0:3 sds 65:32 active ready running
```

Mostrará dos rutas listas activas, con prioridades 14 y 9 (si el LUN está en el controlador preferido). Si un controlador alternativo, no preferido, posee el LUN, las prioridades serán 12 y 11, como se indica a continuación:

```

mpathe (3600a0b800029e8320000623d4f70486a) dm-15 IBM, 1746 FAST
size=1.0G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1 rdac' wp=rw
| +- policy='round-robin 0' prio=12 status=active
|   ~- 16:0:0:6 sdah 66:16 active ready running
| +- policy='round-robin 0' prio=11 status=enabled
|   ~- 15:0:0:6 sdat 66:208 active ready running

```

En el ejemplo anterior, el nodo de dispositivo multi-ruta de este dispositivo es `/dev/mapper/mpathp` y `/dev/dm-0`. La siguiente tabla indica algunas opciones y parámetros básicos del comando **multipath**.

Tabla 28. Opciones y parámetros del comando **multipath**

Comando	Descripción
<code>multipath -h</code>	Imprimir información de uso
<code>multipath -ll</code>	Muestra la topología multi-ruta actual de toda la información disponible (sysfs, Device Mapper, comprobadores de rutas, etc.)
<code>multipath -f map</code>	Desecha la correlación de dispositivos multi-ruta especificada por la opción <i>map</i> si la correlación no se utiliza
<code>multipath -F</code>	Desecha todas las correlaciones de dispositivos multi-ruta no utilizadas

Resolución de problemas de Device Mapper

Utilice la información de la siguiente tabla para resolver problemas relacionados con Device Mapper.

Tabla 29. Resolución de problemas de Device Mapper

Situación	Acción
Compruebe si el daemon multi-ruta, <code>multipathd</code> , está en ejecución	En el indicador de comandos, ejecute el comando <code>/etc/init.d/multipathd status</code>
Determine por qué no se indican dispositivos al ejecutar el comando multipath -ll	En el indicador de comandos, ejecute el comando <code>#cat /proc/scsi/scsi</code> . El resultado del sistema mostrará todos los dispositivos ya descubiertos. Compruebe si el archivo <code>multipath.conf</code> se ha actualizado con los valores adecuados.

Problemas y limitaciones conocidos

- Cuando se configura el almacenamiento con el modo ADT/AVT, pueden observarse retrasos en el descubrimiento de dispositivos. Dichos retrasos pueden resultar en largos retardos durante el arranque del sistema operativo.
- En determinadas condiciones de error con la característica `no_path_retry` o `queue_if_no_path` habilitada, las aplicaciones podrían colgarse para siempre. Para solucionar este problema debe especificar el siguiente comando para todos los dispositivos multi-ruta afectados: `dmsetup message device 0 "fail_if_no_path"` donde `device` es el nombre del dispositivo multi-ruta.
- En la E/S los bloqueos podrían producirse cuando una unidad lógica no se correlaciona antes de suprimir el dispositivo DM. Estas limitaciones se producen solo en la base SLES11. En versiones posteriores se ha solucionado.

- En el resultado `multipath -ll` pueden observarse entradas obsoletas si las unidades lógicas no se correlacionan o se suprimen sin antes eliminar el dispositivo DM y sus rutas subyacentes. Estas limitaciones se producen solo en la base SLES11.
- En Device Mapper el comando de selección de modo se emite de manera síncrona para cada LUN. Con grandes configuraciones de LUN, podrían producirse migraciones de dispositivos DM multi-ruta más lentas si se produce algún retraso en la finalización del comando de selección de modo. Estas limitaciones se producen solo en la base SLES11. En versiones posteriores se ha solucionado.
- Si el módulo `scsi_dh_rdac` no se incluye en `initrd`, el descubrimiento de dispositivos podría ser más lento y el `syslog` podría completarse con mensajes de error de E/S de memoria intermedia.
- Si el proveedor y modelo del almacenamiento no se incluyen en el manejador de dispositivo `scsi_dh_rdac`, el descubrimiento de dispositivos podría ser más lento y el `syslog` podría completarse con mensajes de error de E/S de memoria intermedia.
- El uso de las soluciones de migración tras error DMMP y RDAC en conjunto en el mismo host no está permitido. Utilice una solución cada vez.

Controlador Linux RDAC (MPP)

Esta sección describe cómo instalar el controlador RDAC (MPP) para configuraciones Linux. La funcionalidad ALUA es compatible con SLES SP1, RHEL 6.1 o sus versiones posteriores. IBM recomienda utilizar el controlador Linux Device Mapper Multipath para nuevos servidores y configuraciones de subsistema de almacenamiento. El controlador multi-ruta Linux RDAC (MPP) se dejó de mantener con la versión de firmware de controlador 7.8x.xx.xx.

Importante: Antes de instalar MPP, asegúrese de haber configurado y asignado las particiones y LUN y de que se ha instalado el controlador de HBA adecuado.

Para instalar MPP, complete los pasos siguientes:

1. Descargue el paquete de controlador MPP en el portal de soporte de IBM System Storage Disk.
2. Cree un directorio en el host y descargue el paquete de controlador MPP en el directorio.
3. Escriba el siguiente comando para descomprimir el archivo:


```
# tar -zxvf rdac-LINUX-package_version-source.tar.gz
```

 donde `package_version` es el número de versión del paquete SLES o RHEL. Como resultado se creará un directorio llamado `linuxrdac-version#` o `linuxrdac`.
4. Abra el archivo léame incluido en el directorio `linuxrdac-version#`.
5. En el archivo léame, busque las instrucciones para compilar e instalar el controlador y complete todos los pasos.

Nota: Asegúrese de reiniciar el servidor antes de continuar con el siguiente paso.

6. Escriba el siguiente comando para mostrar los módulos instalados:


```
# lsmod
```
7. Compruebe que las entradas del módulo se han incluido en la lista `lsmod` siguiente.

Entradas de módulo para SLES o RHEL:

- scsi_mod
- sd_mod
- sg
- mppVhba
- mppUpper
- lpfc (o qla2xxx para configuraciones de BladeCenter)
- lpfcdfc (si el módulo ioctl está instalado)

Nota: Si no ve el módulo mpp_Vhba, es probable que el servidor se rearrancara antes de asignar los LUN, por lo que el módulo mpp_Vhba no se habrá instalado. Si fuera el caso, asigne los LUN ahora, reinicie el servidor y repita este paso.

8. Escriba el siguiente comando para comprobar la versión del controlador:

```
# mppUtil -V
```

Se mostrará la versión del controlador multi-ruta Linux.

9. Escriba el siguiente comando para comprobar que los dispositivos se han configurado con el controlador RDAC:

```
# ls -lR /proc/mpp
```

Se mostrará un resultado similar al ejemplo siguiente:

```
# ls -lR /proc/mpp
/proc/mpp:
total 0
dr-xr-xr-x  4 root    root           0 Oct 24 02:56 DS4100-sys1
crwxrwxrwx  1 root    root          254, 0 Oct 24 02:56 mppVBusNode

/proc/mpp/ DS4100-sys1:
total 0
dr-xr-xr-x  3 root    root           0 Oct 24 02:56 controllerA
dr-xr-xr-x  3 root    root           0 Oct 24 02:56 controllerB
-rw-r--r--  1 root    root           0 Oct 24 02:56 virtualLun0
-rw-r--r--  1 root    root           0 Oct 24 02:56 virtualLun1
-rw-r--r--  1 root    root           0 Oct 24 02:56 virtualLun2
-rw-r--r--  1 root    root           0 Oct 24 02:56 virtualLun3
-rw-r--r--  1 root    root           0 Oct 24 02:56 virtualLun4
-rw-r--r--  1 root    root           0 Oct 24 02:56 virtualLun5

/proc/mpp/ DS4100-sys1/controllerA:
total 0
dr-xr-xr-x  2 root    root           0 Oct 24 02:56 lpfc_h6c0t2

/proc/mpp/ DS4100-sys1/controllerA/lpfc_h6c0t2:
total 0
-rw-r--r--  1 root    root           0 Oct 24 02:56 LUN0
-rw-r--r--  1 root    root           0 Oct 24 02:56 LUN1
-rw-r--r--  1 root    root           0 Oct 24 02:56 LUN2
-rw-r--r--  1 root    root           0 Oct 24 02:56 LUN3
-rw-r--r--  1 root    root           0 Oct 24 02:56 LUN4
-rw-r--r--  1 root    root           0 Oct 24 02:56 LUN5

/proc/mpp/ DS4100-sys1/controllerB:
total 0
dr-xr-xr-x  2 root    root           0 Oct 24 02:56 lpfc_h5c0t0

/proc/mpp/ DS4100-sys1/controllerB/lpfc_h5c0t0:
total 0
-rw-r--r--  1 root    root           0 Oct 24 02:56 LUN0
-rw-r--r--  1 root    root           0 Oct 24 02:56 LUN1
-rw-r--r--  1 root    root           0 Oct 24 02:56 LUN2
```

```
-rw-r--r-- 1 root root 0 Oct 24 02:56 LUN3
-rw-r--r-- 1 root root 0 Oct 24 02:56 LUN4
-rw-r--r-- 1 root root 0 Oct 24 02:56 LUN5
```

10. Otra forma de asegurarse de que el controlador RDAC ha descubierto las unidades lógicas físicas disponibles y creado unidades lógicas virtuales para ellas es escribiendo en comando `/opt/mpp/1svdev`, y pulsando **Intro**. Ahora puede enviar E/S a las unidades lógicas.
11. Si hace cualquier cambio en el archivo de configuración de RDAC (`/etc/mpp.conf`) o el archivo de enlace persistente (`/var/mpp/devicemapping`), ejecute el comando `mppUpdate` para reconstruir la imagen RAMdisk incluyendo el nuevo archivo. De esta forma, el nuevo archivo de configuración (o archivo de enlace persistente) podrá utilizarse en el siguiente reinicio del sistema.
12. Para volver a cargar dinámicamente la pila del controlador (`mppUpper`, los módulos del controlador de HBA físicos, `mppVhba`) sin reiniciar el sistema, lleve a cabo estos pasos:
 - a. Para descargar el controlador `mppVhba`, escriba el comando `rmmmod mppVhba` y pulse **Intro**.
 - b. Para descargar el controlador de HBA físico, escriba el comando `modprobe -r "physical hba driver modules"` y pulse **Intro**.
 - c. Para descargar el controlador `mppUpper`, escriba el comando `rmmmod mppUpper` y pulse **Intro**.
 - d. Para volver a cargar el controlador `mppUpper`, escriba el comando `modprobe mppUpper` y pulse **Intro**.
 - e. Para volver a cargar el controlador de HBA físico, escriba el comando `modprobe -r "physical hba driver modules"` y pulse **Intro**.
 - f. Para volver a cargar el controlador `mppVhba`, escriba el comando `modprobe mppVhba` y pulse **Intro**.
13. Reinicie el sistema para descargar la pila del controlador.

Nota: Tras instalar el controlador RDAC, estarán disponibles los siguientes comandos y páginas:

- `mppUtil`
- `mppBusRescan`
- `mppUpdate`
- RDAC

Acerca de `mppUtil`

La utilidad `mppUtil` es una utilidad dirigida por la línea de comandos general que funciona solo con soluciones RDAC basadas en MPP. La utilidad instruye a RDAC para realizar diversas tareas de mantenimiento, pero también sirve como herramienta de resolución de problemas si es necesario. Para utilizar la utilidad `mppUtil`, escriba el siguiente comando y pulse **Intro**:

```
mppUtil [-a target_name] [-c wwn_file_name] [-d
debug_level]
[-e error_level] [-g virtual_target_id] [-I host_num]
[-o feature_action_name[=value][, SaveSettings]]
[-s "failback" | "avt" | "busscan" | "forcerebalance"]
[-S] [-U]
[-V] [-w target_wwn,controller_index]
```

Nota: Los parámetros deben ponerse entre comillas.

La utilidad `mppUtil` es una herramienta de plataforma cruzada. A continuación se incluye la descripción de cada parámetro.

Tabla 30. Descripción de los parámetros de *mppUtil*

Parámetro	Descripción
-a <i>target_name</i>	Muestra la información interna del controlador RDAC para el <i>target_name</i> virtual especificado (nombre del subsistema de almacenamiento). Si no se incluye ningún valor <i>target_name</i> , el parámetro -a muestra información sobre todos los subsistemas de almacenamiento actualmente detectados por el host.
-c <i>wnn_file_name</i>	Borra las entradas del archivo WWN. Este archivo se encuentra en <i>/var/mpp</i> con la extensión <i>.wnn</i> .
-d <i>debug_level</i>	<p>Define el nivel de informe de depuración actual. Esta opción solo funciona si el controlador RDAC se ha compilado con la depuración habilitada. Los informes de depuración están compuestos por dos segmentos. El primer segmento se refiere a un área específica de funcionalidad, el segundo al nivel de realización de informes del área. El <i>debug_level</i> es uno de estos números hexadecimales:</p> <ul style="list-style-type: none"> • 0x20000000– Muestra mensajes de la rutina <i>init()</i> del controlador RDAC. • 0x10000000– Muestra mensajes de la rutina <i>attach()</i> del controlador RDAC. • 0x08000000– Muestra mensajes de la rutina <i>ioctl()</i> del controlador RDAC. • 0x04000000– Muestra mensajes de la rutina <i>open()</i> del controlador RDAC. • 0x02000000– Muestra mensajes de la rutina <i>read()</i> del controlador RDAC. • 0x01000000– Muestra mensajes relacionados con comandos de HBA. • 0x00800000– Muestra mensajes relacionados con comandos <i>aborted</i>. • 0x00400000– Muestra mensajes relacionados con volcados de pánico. • 0x00200000– Muestra mensajes relacionados con actividad de E/S asíncrona. • 0x00000001– Nivel de depuración 1. • 0x00000002– Nivel de depuración 2. • 0x00000004– Nivel de depuración 3. • 0x00000008– Nivel de depuración 4. <p>Estas opciones se pueden combinar con el operador lógico Y (AND) para proporcionar diversas áreas y niveles de informes según sea necesario. Para uso únicamente por representantes de Soporte técnico y atención al cliente.</p>

Tabla 30. Descripción de los parámetros de *mppUtil* (continuación)

Parámetro	Descripción
<code>-e error_level</code>	<p>Define el nivel de creación de informes de error actual como <i>error_level</i>, que puede ser uno de estos valores:</p> <ul style="list-style-type: none"> • 0- Muestra todos los errores. • 1- Muestra la migración tras error de la ruta y el controlador, y los errores recuperados, fatales y repetibles. • 2- Muestra la migración tras error de la ruta y el controlador, y los errores fatales y repetibles. • 3- Muestra la migración tras error de la ruta y el controlador, y los errores fatales. Éste es el valor predeterminado. • 4- Muestra la migración tras error del controlador y los errores fatales. • 5- Muestra los errores fatales. <p>Para uso únicamente por representantes de Soporte técnico y atención al cliente.</p>
<code>-g target_id</code>	<p>Muestra información detallada sobre el estado de cada controlador, la ruta y los LUN del subsistema de almacenamiento especificado. Puede encontrar el <i>target_id</i> ejecutando el comando <code>dsmUtil -a</code>.</p>
<code>-M</code>	<p>Muestra las correlaciones disco a unidad MPIO del DSM. El resultado es similar al obtenido con el programa de utilidad <code>SMdevices</code>. Para uso únicamente por representantes de Soporte técnico y atención al cliente.</p>
<code>-o [[feature_action_name[=value]] [feature_variable_name=value]][, SaveSettings]</code>	<p>Resuelve problemas de una característica o cambia un valor de configuración. Si la palabra clave <code>SaveSettings</code>, los cambios solo afectan al estado en la memoria de las variables. La palabra clave <code>SaveSettings</code> cambia tanto el estado en la memoria como el estado persistente. Algunos ejemplos de comando:</p> <ul style="list-style-type: none"> • <code>dsmUtil -o</code> Muestra todos los nombres de acción de la característica disponibles. • <code>dsmUtil -o DisableLunRebalance=0x3</code> Desactiva el reequilibrio de LUN del subsistema de almacenamiento con DSM iniciado (solo afecta al estado en la memoria).
<code>-P [GetMpioParameters MpioParameter=value ...]</code>	<p>Muestra y configura los parámetros MPIO. Para uso únicamente por representantes de Soporte técnico y atención al cliente.</p>
<code>-R</code>	<p>Elimina los valores de política de equilibrio de carga para los dispositivos inactivos.</p>

Tabla 30. Descripción de los parámetros de mppUtil (continuación)

Parámetro	Descripción
-s ["failback" "avt" "busscan" "forcerebalance"]	Inicia manualmente una de las tareas de exploración del controlador de DSM. Una exploración "failback" hace que el controlador de DSM reintente las comunicaciones con cualquiera de los controladores que hayan fallado. Una exploración "avt" hace que el controlador DSM compruebe si se ha habilitado o inhabilitado AVT para un subsistema de almacenamiento completo. Una exploración "busscan" hace que el controlador de DSM repase la lista de dispositivos sin configurar para ver si se ha configurado alguno de ellos. Una exploración "forcerebalance" hace que el controlador de DSM mueva unidades lógicas del subsistema de almacenamiento a su controlador preferido e ignore el valor del parámetro de configuración DisableLunRebalance del controlador de DSM.
-w <i>target_wwn</i> , <i>controller_index</i>	Para uso únicamente por representantes de Soporte técnico y atención al cliente.

Controlador multi-ruta MAC OS

El único controlador multi-ruta MAC OS soportado es el proporcionado por el proveedor del HBA - ATTO Corporation. Para obtener instrucciones sobre el controlador multi-ruta MAC OS, vaya al sitio web de ATTO IBM Solutions. En dicho sitio web, consulte la información sobre la instalación del controlador Celerity HBA y la instalación de la ATTO Configuration Tool en el *ATTO Celerity MultiPaxath Director Installation and Operation Manual*.

Importante: Tras configurar un LUN, debe rearrancar el servidor para que el LUN sea detectado.

Controlador de Veritas DMP

Consulte la documentación de Symantec Storage Foundation para Windows para obtener instrucciones para instalar el controlador de Veritas DMP en <http://www.symantec.com/business/support/>.

Nota: Podría tener que cargar la Array Support Library (ASL) que soporta DMP en el subsistema de almacenamiento. La ASL puede ser un archivo independiente disponible en Symantec, o puede estar integrada con Volume Manager, dependiendo de la versión de Storage Foundation.

Enlaces PV en HP-UX

Si un sistema HP-UX está conectado con dos adaptadores de bus de host al subsistema de almacenamiento, puede establecer acceso redundante al almacenamiento con enlaces de volumen físico (enlaces PV), una característica del sistema operativo HP-UX. Los enlaces PV obtienen redundancia de acceso con dispositivos que tienen una ruta tanto primaria como secundaria al mismo dispositivo.

Importante:

- Hay dos métodos para establecer el acceso redundante al almacenamiento mediante enlaces PV:
 - Si tiene firmware de controlador versión 07.xx.xx.xx, 06.xx.xx.xx o 05.xx.xx.xx, utilice el método descrito en “Uso de enlaces PV: Método 1”.
 - Si tiene firmware de controlador versión 04.xx.xx.xx, utilice el método descrito en “Uso de enlaces PV: Método 2” en la página 164.
- SMutil debe estar instalado en el host para utilizar ambos métodos.

Uso de enlaces PV: Método 1

Con firmware de controlador versión 05.xx.xx.xx o posterior, utilice el siguiente procedimiento para habilitar la E/S multi-ruta con enlaces PV:

1. Ejecute el comando **hot_add** desde el indicador de shell de HP-UX. Este comando actualiza los nuevos dispositivos creados o añadidos. Se genera un volcado. Cuando se ejecuta el comando **hot_add**, cada unidad lógica nueva creada en la ventana Gestión del subsistema representa un dispositivo de disco del sistema operativo.
2. Ejecute el comando **SMdevices**. El sistema proporciona un volcado similar al ejemplo de la tabla siguiente. Tenga en cuenta que cada unidad lógica y unidad de acceso a unidad lógica tiene un número de unidad lógica (LUN) asignado. Cada unidad lógica tiene dos rutas. Cada controlador de subsistema de almacenamiento tiene un acceso a unidad lógica.

```
/dev/rdisk/c166t0d0 [Storage Subsystem DS4000, Logical Drive Accounting, LUN 0,
Logical Drive WWN <600a0b80000f56d00000001e3eaead2b>,
Preferred Path (Controller-B): In Use]
/dev/rdisk/c166t0d1 [Storage Subsystem DS4000, Logical Drive HR, LUN 1,
Logical Drive WWN <600a0b80000f5d6c000000273eaeae30>,
Alternate Path (Controller-B): Not In Use]
/dev/rdisk/c166t0d2 [Storage Subsystem DS4000, Logical Drive Finance,
LUN 2, Logical Drive WWN <600a0b80000f5d6c000000253eaeadf8>,
Alternate Path (Controller-B): Not In Use]
/dev/rdisk/c166t0d3 [Storage Subsystem DS4000, Logical Drive Purchasing,
LUN 3, Logical Drive WWN <600a0b80000f5d6c000000243eaeadbe>,
Alternate Path (Controller-B): Not In Use]
/dev/rdisk/c166t0d4 [Storage Subsystem DS4000, Logical Drive Development,
LUN 4, Logical Drive WWN <600a0b80000f56d00000001d3eaeacef>,
Preferred Path (Controller-B): In Use]
/dev/rdisk/c166t3d7 [Storage Subsystem DS4000, Logical Drive Access, LUN 31,
Logical Drive WWN <600a0b80000f56d00000001b00000000>]
```

```
/dev/rdisk/c172t0d0 [Storage Subsystem DS4000, Logical Drive Accounting, LUN 0,
Alternate Path (Controller-A): Not In Use]
/dev/rdisk/c172t0d1 [Storage Subsystem DS4000, logical Drive HR, LUN 1,
Logical Drive WWN <600a0b80000f5d6c000000273eaeae30>,
Preferred Path (Controller-A): In Use]
/dev/rdisk/c172t0d2 [Storage Subsystem DS4000, Logical Drive Finance, LUN 2,
Logical Drive WWN <600a0b80000f5d6c000000253eaeadf8>,
Preferred Path (Controller-A): In Use]
/dev/rdisk/c172t0d3 [Storage Subsystem DS4000, Logical Drive Purchasing, LUN 3,
Logical Drive WWN <600a0b80000f5d6c000000243eaeadbe>,
Preferred Path (Controller-A): In Use]
/dev/rdisk/c172t0d4 [Storage Subsystem DS4000, Logical Drive Development, LUN 4,
Logical Drive WWN <600a0b80000f56d00000001d3eaeacef>,
Alternate Path (Controller-A): Not In Use]
/dev/rdisk/c172t3d7 [Storage Subsystem DS4000, Logical Drive Access, LUN 31,
Logical Drive WWN <600a0b80000f5d6c0000002200000000>]
```

Nota: Si tras ejecutar los comandos **hot_add** y **SMdevices** no ve las unidad lógicas y accesos a unidad lógica, utilice el comando **reboot** para reiniciar el host HP-UX.

3. Determine las rutas preferida y alternativa para cada unidad lógica examinando el resultado del comando **SMdevices**, como se muestra en el ejemplo anterior. Tenga en cuenta que cada dispositivo se indica dos veces; una instancia hace referencia a la ruta preferida y la otra a la ruta alternativa.

Ruta preferida

En el resultado del siguiente ejemplo, la ruta preferida es
`/dev/rdisk/c166t0d0`.

```
/dev/rdisk/c166t0d0 [Storage Subsystem DS4000, Logical Drive Accounting, LUN 0, Logical Drive WVN <600a0b80000f56d00000001e3eaead2b>, Preferred Path (Controller-B): In Use]
```

Ruta alternativa

En el resultado del siguiente ejemplo, la ruta alternativa es
`/dev/rdisk/c172t0d0`.

```
/dev/rdisk/c172t0d0 [Storage Subsystem DS4000, Logical Drive Accounting, LUN 0, Logical Drive WVN <600a0b80000f56d00000001e3eaead2b>, Alternate Path (Controller-A): NotIn Use]
```

Uso de enlaces PV: Método 2

Con firmware de controlador versión 4.xx.xx.xx, utilice los siguientes procedimientos para habilitar la E/S multi-ruta con enlaces PV:

- Determine las rutas preferida y alternativa
- Cree las unidades lógicas y matrices

Determinación de las rutas preferidas y alternativas

1. Ejecute el comando **hot_add** desde el indicador de shell de HP-UX. Este comando actualiza los nuevos dispositivos creados o añadidos. Se genera un volcado. Cuando se ejecuta el comando **hot_add**, cada unidad lógica nueva creada en la ventana Gestión del subsistema representa un dispositivo de disco del sistema operativo.
2. Ejecute el comando **SMdevices**. El sistema proporciona un volcado similar al ejemplo siguiente. Tenga en cuenta que cada unidad lógica y unidad de acceso a unidad lógica tiene un número de unidad lógica (LUN) asignado. Cada unidad lógica tiene dos rutas. Cada controlador de subsistema de almacenamiento tiene un acceso a unidad lógica.

```
/dev/rdisk/c166t0d0 [Storage Subsystem DS4000, Logical Drive Accounting, LUN 0, Logical Drive WVN <600a0b80000f56d00000001e3eaead2b>]
/dev/rdisk/c166t0d1 [Storage Subsystem DS4000, Logical Drive HR, LUN 1, Logical Drive WVN <600a0b80000f5d6c000000273eaeae30>]
/dev/rdisk/c166t0d2 [Storage Subsystem DS4000, Logical Drive Finance, LUN 2, Logical Drive WVN <600a0b80000f5d6c000000253eaeadf8>]
/dev/rdisk/c166t0d3 [Storage Subsystem DS4000, Logical Drive Purchasing, LUN 3, Logical Drive WVN <600a0b80000f5d6c000000243eaeadbe>]
/dev/rdisk/c166t0d4 [Storage Subsystem DS4000, Logical Drive Development, LUN 4, Logical Drive WVN <600a0b80000f56d00000001d3eaeacef>]
/dev/rdisk/c166t3d7 [Storage Subsystem DS4000, Logical Drive Access, LUN 31, Logical Drive WVN <600a0b80000f56d00000001b0000000>]
```

```
/dev/rdisk/c172t0d0 [Storage Subsystem DS4000, Logical Drive Accounting, LUN 0, Logical Drive WVN <600a0b80000f56d00000001e3eaead2b>]
/dev/rdisk/c172t0d1 [Storage Subsystem DS4000, Logical Drive HR, LUN 1, Logical Drive WVN <600a0b80000f5d6c000000273eaeae30>]
/dev/rdisk/c172t0d2 [Storage Subsystem DS4000, Logical Drive Finance, LUN 2, Logical Drive WVN <600a0b80000f5d6c000000253eaeadf8>]
/dev/rdisk/c172t0d3 [Storage Subsystem DS4000, Logical Drive Purchasing, LUN 3,
```

```

Logical Drive WWN <600a0b80000f5d6c000000243eaeadeb>]
/dev/rdisk/c172t0d4 [Storage Subsystem DS4000, Logical Drive Development, LUN 4,
Logical Drive WWN <600a0b80000f56d00000001d3eaeacef>]
/dev/rdisk/c172t3d7 [Storage Subsystem DS4000, Logical Drive Access, LUN 31,
Logical Drive WWN <600a0b80000f5d6c0000002200000000>]

```

Nota: Si tras ejecutar los comandos **hot_add** y **SMdevices** no ve las unidad lógicas y accesos a unidad lógica, utilice el comando **reboot** para reiniciar el host HP-UX.

3. Determine las rutas preferida y alternativa para cada unidad lógica examinando el resultado del comando **SMdevices**, como se muestra en el ejemplo anterior.

Tenga en cuenta que cada dispositivo se indica dos veces; una instancia hace referencia a la ruta preferida y la otra a la ruta alternativa. Tenga en cuenta también que cada dispositivo tiene un nombre mundial (WWN). Parte del WWN de cada unidad lógica es único para cada controlador del subsistema de almacenamiento. Los WWN para el acceso de unidad lógica del ejemplo anterior solo se diferencian en cinco dígitos, **f56d0** y **f5d6c**.

Los dispositivos del ejemplo anterior se visualizan a través de los controladores **c166** y **c172**. Para determinar la ruta preferida de una unidad lógica específica vista por el sistema operativo, complete los pasos indicados a continuación:

- a. Busque el WWN para el acceso de cada unidad lógica. En este caso, el Acceso de unidad lógica 1 está asociado con **c166** y tiene el WWN **f56d0**.

```

/dev/rdisk/c166t3d7 [Storage Subsystem DS4000, Logical Drive Access, LUN 31,
Logical Drive WWN <600a0b80000f56d00000001b00000000>]

```

El Acceso a unidad lógica 2 está asociado con **c172** y tiene el WWN **f5d6c**.

```

/dev/rdisk/c172t3d7 [Storage Subsystem DS4000, Logical Drive Access, LUN 31,
Logical Drive WWN <600a0b80000f5d6c0000002200000000>]

```

- b. Identifique el nombre de ruta de dispositivo preferido del dispositivo de almacenamiento asociando el WWN de la unidad lógica con un WWN de acceso a unidad lógica. En este caso, el WWN del **LUN 0** está asociado con los controladores **c166** y **c172**. Así, la ruta preferida del **LUN 0** es **/dev/rdisk/c166t0d0**, es decir, el controlador **c166**.

```

/dev/rdisk/c166t0d0 [Storage Subsystem DS4000, Logical Drive
Accounting, LUN 0, Logical Drive g<600a0b80000f56d00000001e3eaead2b>]

```

La ruta alternativa es **/dev/rdisk/c172t0d0**, el controlador **c172**.

```

/dev/rdisk/c172t0d0 [Storage Subsystem DS4000, Logical Drive
Accounting, LUN 0, Logical Drive WWN <600a0b80000f56d00000001e3eaead2b>]

```

- c. Para guardar un registro para futuras referencias, anote esta información de ruta para el LUN 0 en una matriz (similar a la de Tabla 31).

Tabla 31. Registro de muestra de rutas preferida y alternativa de unidad lógica

LUN	Nombre de unidad lógica	Ruta preferida	Ruta alternativa
0	Accounting (contabilidad)	/dev/rdisk/c166t0d0	/dev/rdisk/c172t0d0
1	HR (RRHH)	/dev/rdisk/c172t0d1	/dev/rdisk/c166t0d1
2	Finance (Finanzas)	dev/rdisk/c172t0d2	/dev/rdisk/c166t0d2
3	Purchasing (Compras)	/dev/rdisk/c172t0d3	/dev/rdisk/c166t0d3
4	Development (Desarrollo)	/dev/rdisk/c166t0d4	/dev/rdisk/c172t0d4

- d. Repita los pasos 3.a a 3.c para cada unidad lógica vista por el sistema operativo.

Creación de unidades lógicas y matrices

Tras determinar las rutas preferida y alternativa y haberlas registrado en una matriz para futuras referencias, complete los siguientes pasos para crear unidades lógicas y matrices.

Importante: No utilice la aplicación HP System Administration Management (SAM) para la configuración de almacenamientos DS3000, DS4000 o DS5000; si lo hace, podría observar resultados no deseados.

Nota: Los pasos de este procedimiento se refieren al LUN 0 de la Tabla 31 en la página 165.

1. Cree una unidad lógica física y defina las rutas primarias de los dispositivos de almacenamiento asociados. La ruta primaria es la ruta preferida. Escriba el siguiente comando en el indicador de shell:

```
#pvcreate /dev/rdisk/c166t0d0
```

El sistema confirma la creación de una nueva unidad lógica física.

2. Cree matrices.

Nota: Para obtener más información sobre cómo crear matrices, consulte la documentación de HP-UX omanpages.

- a. Cree un directorio para la matriz escribiendo los siguientes comandos. Este directorio debe estar en el directorio /dev.

```
#cd /dev  
#mkdir /vg1
```

- b. Cree el archivo especial de grupo para la matriz en el directorio /dev escribiendo el siguiente comando:

```
#mknod /dev/vg1/group c 64 0x010000
```

- c. Cree una matriz y defina nombres de las unidades lógicas físicas (enlace primario) para el dispositivo de almacenamiento asociado escribiendo el siguiente comando:

```
#vgcreate /dev/vg1/ /dev/dsk/c166t0d0
```

- d. Defina el nombre de ruta secundario (ruta alternativa) del dispositivo de almacenamiento asociado escribiendo el siguiente comando:

```
#vgextend vg1 /dev/dsk/c172t0d0
```

Nota: También puede utilizar el comando **vgextend** para añadir dispositivos de almacenamiento a la matriz existente. Añada primero la ruta primaria y después la ruta alternativa, como se muestra en el siguiente ejemplo.

- 1) Añada la ruta primaria para el LUN1.

```
#vgextend vg1 /dev/dsk/c172t0d1
```

- 2) Añada la ruta secundaria para el LUN1.

```
#vgextend vg1 /dev/dsk/c166t0d1
```

3. Cree unidades lógicas. Para obtener más información, consulte la documentación de HP-UX.
4. Cree sistemas de archivos para las unidades lógicas.
5. Repita los pasos 1 a 4 para crear matrices adicionales. Para obtener más información, consulte la documentación de HP-UX.
6. Compruebe las rutas primaria (preferida) y secundaria (alternativa) de cada dispositivo escribiendo el siguiente comando:

```
#vgdisplay -v vname
```

donde *vname* es el nombre de la matriz.

Multi-ruta nativa de HP-UX

La multi-ruta es nativa en HP-UX 11i v3. Está incorporada en el subsistema de almacenamiento en masa u está disponible para aplicaciones sin configuración especial.

Para obtener más información sobre la multi-ruta nativa de HP-UX 11iv3, consulte la documentación en <http://docs.hp.com/en/oshpux11iv3.html>.

Controladores de migración tras error en Solaris

El controlador de migración tras error supervisa las rutas de E/S. Si se produce un fallo de un componente en una de las rutas de canal de fibra, el controlador de migración tras error redirige todas las E/S a otra ruta.

Los sistemas host Solaris requieren uno de los siguientes controladores de migración tras error:

- Solaris Multiplexed I/O (MPxIO)
- RDAC
- Veritas VolumeManager con Dynamic Multipathing (DMP)

Nota:

1. RDAC no es compatible con Solaris 10. Debe utilizar Solaris MPxIO o el controlador de migración tras error Veritas DMP.
2. Con Solaris 10, la capacidad MPxIO está incorporada. Si desea utilizar MPxIO con versiones anteriores de Solaris, debe instalar SUN StorEdge SAN Foundation Suite.
3. Para dar soporte al Acceso asimétrico de unidad lógica (ALUA), debe tener Solaris 11 o posterior.

Esta sección incluye los siguientes procedimientos:

- “Instalación del controlador de MPxIO”
- “Instalación del controlador de migración tras error RDAC en Solaris y modificación de los archivos de configuración” en la página 174
- “Planificación y preparación para la instalación del controlador Veritas DMP” en la página 176

Instalación del controlador de MPxIO

la E/S multiplexada (MPxIO) es una arquitectura de controlador multi-ruta de Sun Solaris. Este controlador de migración tras error permite acceder a los subsistemas de almacenamiento a través de diversas interfaces del controlador de host desde una sola instancia del subsistema de almacenamiento. MPxIO ayuda a proteger ante paradas del subsistema de almacenamiento causadas por errores del controlador. Si un controlador falla, MPxIO cambia automáticamente a un controlador alternativo.

MPxIO se integra totalmente en el sistema operativo Solaris 10. Para sistemas operativos Solaris 8 y 9, MPxIO está disponible como parte de la Sun StorEdge SAN Foundation Suite y se debe instalar por separado.

Para conocer las últimas versiones soportadas de Sun StorEdge SAN Foundation Suite, los últimos parches del kernel Solaris y la información más reciente y

actualizaciones de MPxIO, consulte el archivo léame de Storage Manager para Solaris. Consulte “Búsqueda de software, firmware de controlador y archivos léame de Storage Manager” en la página xv para saber cómo encontrar el archivo léame en la web.

Esta sección contiene los siguientes temas:

- “Consideraciones sobre cambio de nombre de dispositivo para MPxIO”
- “Adquisición de la última versión del controlador MPxIO”
- “Habilitación del controlador de migración tras error MPxIO” en la página 169
- “Inhabilitación del controlador multi-ruta MPxIO” en la página 174

Nota: Para obtener más información, consulte la *Sun StorEdge SAN Foundation Software Installation Guide*, *Sun StorEdge SAN Foundation Software Configuration Guide* y *Sun Solaris Fibre Channel and Storage Multipathing Administration Guide* en el sitio web de Sun <http://docs.sun.com>.

Consideraciones sobre cambio de nombre de dispositivo para MPxIO:

En los árboles /dev y /devices, los dispositivos tienen un nombre diferente a su nombre original si MPxIO está habilitado. Consulte los ejemplos siguientes:

Nombre de dispositivo con MPxIO inhabilitado:

```
/dev/dsk/c1t1d0s0
```

Nombre de dispositivo con MPxIO habilitado:

```
/dev/rdisk/c0t600A0B800011121800006B31452CC6A0d0s2
```

Debe configurar las aplicaciones que acuden al dispositivo directamente para utilizar los nuevos nombres cuando MPxIO esté habilitado o inhabilitado.

Además, el archivo /etc/vfstab y la configuración de volcado también contienen referencias a nombres de dispositivo. Cuando utiliza el comando **stmsboot** para habilitar o inhabilitar MPxIO, como se describe en las siguientes secciones, /etc/vfstab y la configuración de volcado se actualizan automáticamente con los nuevos nombres de dispositivo.

Adquisición de la última versión del controlador MPxIO: El método de adquisición de MPxIO depende de la versión de Solaris que tenga instalada:

Solaris 10.

MPxIO está integrado en el sistema operativo Solaris 10 y no requiere una instalación por separado. Utilice parches de Solaris 10 para actualizar MPxIO con Solaris 10. Los parches están disponibles en el sitio web de soporte técnico de Sun <http://sunsolve.sun.com>.

Nota: Debe instalar el parche jumbo kernel regular porque existen dependencias entre varios parches que forman la pila del controlador.

Solaris 8 y 9

Dado que MPxIO no está incluido en Solaris 8 y 9, debe descargar la suite SAN necesaria (Sun StorEdge SAN Foundation Suite) desde el sitio web de soporte técnico de Sun <http://sunsolve.sun.com>. En esta página web, pulse **SAN 4.4 release Software/Firmware Upgrades & Documentation**.

Nota: Utilice el script **install_it.ksh** facilitado para instalar el software.

Habilitación del controlador de migración tras error MPxIO: Esta sección describe cómo habilitar MPxIO utilizando el comando **stmsboot**. Además de habilitar MPxIO, este comando actualiza también los nombres de dispositivos en el archivo `/etc/vfstab` y los archivos de configuración de volcado durante el siguiente rearranque.

Nota: En Solaris 10, el comando **stmsboot** se utiliza para habilitar o deshabilitar MPxIO en todos los dispositivos.

Antes de empezar:

1. Instale el sistema operativo Solaris y los últimos parches.
2. Asegúrese de que el tipo de host Solaris se seleccionó al definir el host.

Habilitación de MPxIO en Solaris 8 y 9

1. Instale la última versión de Sun StorEdge SAN Foundation Suite y los parches necesarios, utilizando el script **Sun StorEdge install_it**. Para más información, consulte la *Guía de instalación de Sun StorEdge SAN Foundation Suite x.xx* (donde *x.xx* es la versión del software StorEdge).
2. Edite el archivo de configuración `/kernel/drv/scsi_vhci.conf` para asegurarse de que el VID/PID no se especifica en este archivo. Asegúrese también de que el archivo presenta las siguientes entradas:

```
mpxio-disable="no";  
load-balance="none";  
auto-failback="enable";
```

Nota: En un entorno de clúster en el que diversos servidores SUN comparten las unidades lógicas (LUN), quizá deba definir el parámetro `auto-failback` como `disable` para evitar el fenómeno siguiente, que puede producirse si uno de los servidores tiene una ruta errónea a uno de los LUN compartidos.

Si un host de una configuración de servidor de clúster pierde una ruta física a un controlador de subsistema de almacenamiento, los LUN correlacionados con el grupo de clúster pueden migrar periódicamente y restablecerse entre nodos de clúster hasta que se restaure la ruta errónea. Este comportamiento es el resultado de la característica de restablecimiento de unidad lógica automático del controlador multi-ruta. El nodo de clúster con una ruta errónea a un controlador de subsistema de almacenamiento emite un comando de migración tras error para todos los LUN correlacionados con el grupo de clúster para el controlador al que puede acceder. Tras un intervalo programado, los nodos sin ruta errónea emiten un comando de restablecimiento para los LUN puesto que estos pueden acceder a los LUN de ambos controladores. El nodo de clúster con la ruta errónea no puede acceder a determinados LUN. Este nodo de clúster emite a continuación un comando de migración tras error para todos los LUN, que repiten el ciclo de migración tras error-restablecimiento de LUN.

Para conocer los servicios de clúster soportados, consulte el System Storage Interoperation Center en www.ibm.com/systems/support/storage/config/ssic

3. Si ha hecho algún cambio en el archivo `/kernel/drv/scsi_vhci.conf` durante el paso anterior, guarde el archivo y utilice el siguiente comando para reiniciar el servidor:

```
# shutdown -g0 -y -i6
```

4. Si fuera necesario, actualice el firmware de HBA de canal de fibra.
5. Cree las unidades lógicas del subsistema de almacenamiento y correlaciónelas con los puertos HBA de canal de fibra en los servidores Sun.

Habilitación de MPxIO en Solaris 10

Tenga en cuenta las siguientes consideraciones para `stmsboot -e [enable] -d [disable]` and `-u [update]`:

- Cuando ejecute el comando **stmsboot**, acepte el valor predeterminado **Rearrancar el sistema ahora**.
- El comando **stmsboot** guarda copias de los archivos `/kernel/drv/fp.conf` y `/etc/vfstab` originales antes de modificarlos para que pueda utilizar las copias guardadas en recuperaciones ante problemas inesperados.
- Asegúrese de que el dispositivo de arranque **eeeprom** está definido para arrancar desde el dispositivo de arranque actual.

Para habilitar MPxIO en todos los dispositivos de canal de fibra, complete estos pasos:

1. ejecute el comando **stmsboot -e** y seleccione el valor predeterminado `[y]` para reiniciar el servidor:

```
# stmsboot -e
```

```
AVISO: Esta operación requerirá el rearranque.  
¿Desea continuar? [s/n] (predeterminado: s) s  
Los cambios se aplicarán tras rearrancar el sistema.  
¿Rearrancar el sistema ahora? [s/n] (predeterminado: s) s
```

Nota: Durante el rearranque, `/etc/vfstab` y la configuración de volcado se actualizarán para reflejar los cambios en el nombre de los dispositivos.

2. Tras el rearranque, configure sus aplicaciones para utilizar los nuevos nombres de dispositivo, como se explica en "Consideraciones sobre cambio de nombre de dispositivo para MPxIO" en la página 168.
3. Si fuera necesario, edite el archivo de configuración `/kernel/drv/fp.conf` para comprobar que los siguientes parámetros están definidos como se indica a continuación:

```
mpxio-disable="no";
```

Edite el archivo de configuración `/kernel/drv/scsi.conf` para comprobar que los siguientes parámetros están definidos como se indica a continuación:

```
load-balance="none";  
auto-failback="enable";
```

4. Si ha hecho algún cambio en el archivo de configuración durante el paso anterior, guarde el archivo y utilice el siguiente comando para reiniciar el servidor:

```
# shutdown -g0 -y -i6
```

5. Si fuera necesario, actualice el firmware de HBA de canal de fibra.
6. Cree las unidades lógicas del subsistema de almacenamiento y correlaciónelas con los puertos HBA de canal de fibra en los servidores Sun.

Verificación de los dispositivos y configuración de ruta de migración tras error/restablecimiento para LUN correlacionados

Para verificar los dispositivos y configurar la ruta de migración tras error para los LUN correlacionados, siga los pasos indicados a continuación:

1. Utilice el comando **cfgadm -al** para verificar los dispositivos. Ejecute el comando **cfgadm -al** para mostrar información sobre los puertos de host y los dispositivos conectados:

```

# cfgadm -al
Ap_Id                               Type      Receptacle  Occupant    Condition
PCI0                                vgs8514/hp  connected   configured  ok
PCI1                                unknown    empty       unconfigured unknown
PCI2                                unknown    empty       unconfigured unknown
PCI3                                mult/hp     connected   configured  ok
PCI4                                unknown    empty       unconfigured unknown
PCI5                                unknown    empty       unconfigured unknown
PCI6                                unknown    empty       unconfigured unknown
PCI7                                mult/hp     connected   configured  ok
PCI8                                mult/hp     connected   configured  ok
c0                                   scsi-bus   connected   configured  unknown
c0::dsk/c0t6d0                      CD-ROM     connected   configured  unknown
c1                                   fc-private  connected   configured  unknown
c1::500000e0106fca91                disk      connected   configured  unknown
c1::500000e0106fcde1                disk      connected   configured  unknown
c1::500000e0106fcf31                disk      connected   configured  unknown
c1::500000e0106fd061                disk      connected   configured  unknown
c1::500000e0106fd7b1                disk      connected   configured  unknown
c1::500000e0106fdaa1                disk      connected   configured  unknown
c1::50800200001d9841                ESI       connected   configured  unknown
c2                                   fc-fabric  connected   configured  unknown
c2::201400a0b811804a                disk      connected   configured  unusable
c2::201400a0b8118098                disk      connected   configured  unusable
c2::201700a0b8111580                disk      connected   configured  unusable
c3                                   fc-fabric  connected   configured  unknown
c3::201500a0b8118098                disk      connected   configured  unusable
c3::201600a0b8111580                disk      connected   configured  unusable
c3::202500a0b811804a                disk      connected   configured  unusable
c4                                   fc-fabric  connected   configured  unknown
c4::200400a0b80f1285                disk      connected   configured  unknown
c4::200400a0b8127a26                disk      connected   configured  unusable
c5                                   fc-fabric  connected   configured  unknown
c5::200400a0b82643f5                disk      connected   unconfigured unknown
c5::200500a0b80f1285                disk      connected   configured  unknown
c5::200500a0b8127a26                disk      connected   configured  unusable
c5::200c00a0b812dc5a                disk      connected   configured  unknown
usb0/1                              usb-kbd    connected   configured  ok
usb0/2                              usb-mouse  connected   configured  ok
usb0/3                              unknown    empty       unconfigured ok
usb0/4                              unknown    empty       unconfigured ok
#

```

2. También puede mostrar información acerca de los puntos de conexión de un servidor. En el ejemplo siguiente, `c0` representa un puerto de host conectado en tejido, y `c1` un puerto de host conectado en bucle. Utilice el comando `cfgadm` para gestionar la configuración de dispositivo en puertos de host conectados en tejido. De forma predeterminada, la configuración de dispositivo en puertos de host conectados en bucle privada es gestionada por el host Solaris.

Nota: El comando `cfgadm -l` muestra información sobre puertos de host de canal de fibra. Utilice el comando `cfgadm -al` también para mostrar información sobre dispositivos de canal de fibra. Las líneas que incluyen un nombre de ámbito mundial (WWN) en el campo `Ap_Id` asociado con `c0` representan un dispositivo de tejido. Utilice los comandos `cfgadm configure` y `cfgadm unconfigure` para gestionar estos dispositivos y hacer que estén disponibles en los hosts Solaris.

```

# cfgadm -l
Ap_Id      Type      Receptacle  Occupant    Condition
c0         fc-fabric  connected   unconfigured unknown
c1         fc-private  connected   configured  unknown

```

3. Configure el dispositivo utilizando el siguiente comando:
`cfgadm -c configure Ap-Id`

El parámetro Ap_ID especifica el identificador del punto de conexión de los dispositivos de canal de fibra configurados. Este identificador puede ser el número de controlador y WWN de un dispositivo (por ejemplo, c3::50020f230000591d).

Consulte el ejemplo de resultado del paso1. Consulte también la página man *cfgadm* para ver una explicación de los puntos de conexión.

Nota: No se puede configurar un Ap_Id con tipo fc-private. Solo se puede configurar y desconfigurar el tipo fc-fabric.

4. Utilice el comando **luxadm probe** para ver una lista de todos los LUN correlacionados:

```
# luxadm probe
luxadm probe
No Network Array enclosures found in /dev/es

Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006ADE452CBC62d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006ADF452CBC6Ed0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006AE0452CBC7Ad0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006AE1452CBC88d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006AE2452CBC94d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006AE3452CBCA0d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006AE4452CBCACd0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006AE5452CBCB8d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006AE6452CBC4d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006AE7452CBCD2d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006AE8452CBCDEd0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006AE9452CBCEA0d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006AEA452CBCF8d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006AEB452CBD04d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006AEC452CBD10d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006AED452CBD1Ed0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006B2A452CC65Cd0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006B2B452CC666d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006B2C452CC670d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006B2D452CC67Ad0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006B31452CC6A0d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c0t600A0B800011121800006B32452CC6ACd0s2
Node WWN:200400a0b8111218 Device Type:Disk device
  Logical Path:/dev/rdisk/c8t201400A0B8111218d7s2
```

5. Puede utilizar el comando **luxadm display logical path** para mostrar más detalles sobre cada LUN correlacionado, incluyendo el número de rutas a cada LUN. El siguiente ejemplo utiliza una ruta lógica del ejemplo anterior.

```
# luxadm display /dev/rdisk/c0t600A0B800011121800006B31452CC6A0d0s2
DEVICE PROPERTIES for disk: /dev/rdisk/c0t600A0B800011121800006B31452CC6A0d0s2
Vendor:                IBM
Product ID:            1742-900
Revision:              0914
Serial Num:            1T51207691
Uninitialized capacity: 1024.000 MBytes
Write Cache:           Enabled
Read Cache:            Enabled
  Minimum prefetch:    0x0
  Maximum prefetch:    0x0
Device Type:           Disk device
Path(s):

/dev/rdisk/c0t600A0B800011121800006B31452CC6A0d0s2
/devices/scsi_vhci/ssd@g600a0b800011121800006b31452cc6a0:c,raw
Controller             /devices/pci07c0/pci00/pci08/SUNW,q1c00,1/fp00,0
  Device Address        201400a0b8111218,1e
  Host controller port WWN 210100e08ba0fca0
  Class                 secondary
  State                 STANDBY
Controller             /devices/pci07c0/pci00/pci08/SUNW,q1c00,1/fp00,0
  Device Address        201500a0b8111218,1e
  Host controller port WWN 210100e08ba0fca0
  Class                 primary
  State                 ONLINE
Controller             /devices/pci07c0/pci00/pci08/SUNW,q1c00/fp00,0
  Device Address        201400a0b8111218,1e
  Host controller port WWN 210000e08b80fca0
  Class                 secondary
  State                 STANDBY
Controller             /devices/pci07c0/pci00/pci08/SUNW,q1c00/fp00,0
  Device Address        201500a0b8111218,1e
  Host controller port WWN 210000e08b80fca0
  Class                 primary
  State                 ONLINE
#
```

Desconfiguración de una ruta de migración tras error/restablecimiento

Para desconfigurar una ruta de migración tras error/restablecimiento, complete estos pasos:

1. Antes de desconfigurar un dispositivo de tejido, detenga toda la actividad del dispositivo y desmonte todos los sistemas de archivos de este (consulte la documentación de administración de Solaris para conocer los procedimientos de desmonte).
2. Ejecute el comando **cfgadm -al** para mostrar información sobre los puertos de host y los dispositivos conectados.
3. Desconfigure el LUN ejecutando el siguiente comando:

```
cfgadm -c unconfigure Ap-Id
```

Ap-Id es el LUN que desea desconfigurar.

4. Ejecute el comando **cfgadm -al** de nuevo para comprobar si el LUN se ha desconfigurado.
5. De ser necesario, defina la estructura de archivo utilizando el comando **newfs**. Añada entradas al archivo `/etc/vfstab`.
6. Escriba el siguiente comando para reiniciar el servidor:

```
shutdown -g0 -y -i6
```

Inhabilitación del controlador multi-ruta MPxIO: Para inhabilitar el controlador multi-ruta MPxIO, realice la acción apropiada para su versión de Solaris:

- En Solaris 10, desconfigure todos los dispositivos utilizando el comando `cfgadm -c unconfigure AP-id Ap-id`. A continuación, ejecute el comando `stmsboot -d` y acepte el valor predeterminado para Reiniciar el sistema ahora.
- En Solaris 8 y 9, desconfigure todos los dispositivos utilizando el comando `cfgadm -c unconfigure AP-id Ap-id` y edite el archivo de configuración `/kernel/drv/scsi_vhci.conf` para definir el valor del parámetro `mpxio-disable` como `sí`. Reinicie el servidor.

Para saber cómo revertir los parches o utilizar el software StorEdge, consulte la *Guía de instalación de Sun StorEdge SAN Foundation* en <http://docs.sun.com>.

Instalación del controlador de migración tras error RDAC en Solaris y modificación de los archivos de configuración

esta sección describe cómo instalar RDAC en un host Solaris.

Antes de empezar:

1. RDAC solo es compatible con Solaris 8 y 9.
2. Dado que no puede ejecutar RDAC y MPxIO, asegúrese de que MPxIO está inhabilitado. Compruebe los archivos de configuración (`/kernel/drv/scsi_vhci.conf`, `/kernel/drv/fp.conf`, o ambos) y asegúrese de que el valor del parámetro `mpxio-disable` está definido como `Yes`.
3. Antes de instalar RDAC, debe instalar un paquete de controlador de HBA. Si tiene una configuración de conexión a SAN, también debe modificar el archivo de configuración de HBA antes de instalar RDAC. Si no sigue los procedimientos en este orden, podrían producirse problemas.
4. Si modifica la configuración de migración tras error en el archivo de configuración de HBA después de instalar RDAC, deberá eliminar RDAC del host.

Importante: En algunas configuraciones, se necesita un parche para que RDAC funcione correctamente. Antes de comenzar con la instalación de RDAC, compruebe el archivo léame de Storage Manager para Solaris para saber qué parche necesita para su configuración concreta. En el archivo léame también puede encontrar las últimas versiones de RDAC y otros datos importantes. Para obtener más información sobre cómo encontrar el archivo léame en Internet, consulte "Búsqueda de software, firmware de controlador y archivos léame de Storage Manager" en la página xv.

Instalación del controlador de migración tras error RDAC

Para instalar el controlador de migración tras error RDAC, complete los pasos siguientes:

1. Inserte el DVD de instalación de Solaris en la unidad de DVD.

Nota: En este procedimiento, el DVD de instalación se monta en `/cdrom/SM91`. Modifique estos comandos según sea necesario para su instalación. Puede ser `'cdrom'` o `'dvdrom'` dependiendo de la forma en que se haya montado el disco.

2. Escriba el siguiente comando para comenzar a instalar el paquete RDAC:

```
# pkgadd -d path/filename.pkg
```

donde *path/filename* es la ruta del directorio y el nombre del paquete que desea instalar.

Se inicia el proceso de instalación.

En la línea de comandos se mostrará información sobre los paquetes que se pueden instalar en el directorio especificado, como indica el siguiente ejemplo:

Los paquetes disponibles son:

```
1 RDAC                               Redundant Disk Array Controller
                                     (sparc) version number
```

```
Select package(s) you wish to process (or 'all' to process all
packages). (default:all) [?,??,q]:
```

3. Escriba el valor del paquete que está instalando y pulse Intro. Se inicia el proceso de instalación.
4. El software comprueba automáticamente si hay conflictos de paquetes. Si se detecta algún conflicto, se muestra un mensaje que indica que algunos archivos ya están instalados y están siendo utilizados por otro paquete. Se muestra la solicitud siguiente:

```
Do you want to install these conflicting files [y, n, ?]
```

Escriba y pulse Intro. Se muestra la siguiente solicitud:

```
This package contains scripts which will be executed with super-user
permission during the process of installing this package.
```

```
Do you want to continue with the installation of <RDAC>
```

```
[y, n, ?]
```

5. Escriba y pulse Intro. El proceso de instalación continuará. Cuando el paquete RDAC se haya instalado correctamente, se mostrará el siguiente mensaje:
Installation of <RDAC> was successful.
6. Asegúrese de que las variables de los archivos de configuración para las tarjetas adaptadoras se han definido con los valores adecuados.
7. Escriba el siguiente comando para reiniciar el host Solaris:

```
# shutdown -g0 -y -i6
```

Modificación de los archivos de configuración

Importante: Cualquier modificación en los enlaces persistentes del archivo de configuración *jnic146x.conf* requiere la eliminación de RDAC. Una vez eliminado RDAC, puede modificar los enlaces persistentes en el archivo *jnic146x.conf* y después volver a instalar RDAC.

Complete los siguientes pasos para modificar el archivo *sd.conf* o *jnic146x.conf*:

1. Escriba el siguiente comando para eliminar RDAC:

```
# pkgrm RDAC_driver_pkg_name
```

donde *RDAC_driver_pkg_name* es el nombre del paquete de controlador de RDAC que desea eliminar.

2. Escriba el siguiente mandato para verificar si se ha eliminado el paquete de controlador de RDAC:

```
# pkginfo RDAC_driver_pkg_name
```

donde *RDAC_driver_pkg_name* es el nombre del paquete de controlador de RDAC eliminado.

3. Escriba el siguiente comando para reiniciar el host Solaris:

```
# shutdown -g0 -y -i6
```
4. Escriba el siguiente comando para modificar los enlaces persistentes del archivo `sd.conf` o editar el archivo `sd.conf`:

```
# vi /kernel/drv/jnic146x.conf o sd.conf
```
5. Cuando haya terminado de hacer sus cambios, escriba el siguiente comando para guardar los cambios:

```
# :wq
```
6. Escriba el siguiente comando para instalar el paquete de controlador de RDAC:

```
# pkgadd -d RDAC_driver_pkg_name
```

donde `RDAC_driver_pkg_name` es el nombre del paquete de controlador de RDAC que desea instalar.
7. Escriba el siguiente mandato para verificar la instalación del paquete:

```
# pkginfo RDAC_driver_pkg_name
```

donde `RDAC_driver_pkg_name` es el nombre del paquete de controlador de RDAC que ha instalado.
8. Escriba el siguiente comando para reiniciar el host Solaris:

```
# shutdown -g0 -y -i6
```

Nota: Tras modificar el archivo `jnic146x.conf`, debe reiniciar el host porque el controlador `jnic146x.conf` es de solo lectura durante el proceso de arranque. Si no reinicia el host algunos dispositivos podrían ser inaccesibles.

Planificación y preparación para la instalación del controlador Veritas DMP

Esta sección describe cómo planificar y preparar la instalación del controlador Veritas Dynamic Multipathing (DMP). El controlador Veritas DMP es un controlador de migración tras error para hosts Solaris. El controlador de migración tras error DMP es una característica de Veritas Volume Manager, componente del producto Storage Foundation de Symantec. Aunque RDAC le permite tener solo 32 LUN, DMP le permite tener hasta 256 LUN.

Importante: Este documento describe cómo instalar el producto Veritas. Para obtener más información, consulte la documentación de Symantec en <http://www.symantec.com/business/support/>.

Requisitos del sistema

Asegúrese de que su servidor cumple los siguientes requisitos antes de instalar Veritas DMP:

- Sistema operativo Solaris
- Veritas Volume Manager 4.0, 4.1, 5.0 o 5.1
- Biblioteca de soporte de matriz (ASL), que permite a Solaris reconocer los sistemas DS3000, DS4000, o DS5000

Nota: La ASL puede ser un archivo independiente disponible en Symantec, o puede estar integrada con Volume Manager, dependiendo de la versión de Storage Foundation.

Visión general de la instalación de Veritas DMP

Asegúrese de que su servidor cumple los siguientes requisitos previos antes de instalar Veritas DMP:

- Los HBA están instalados en el Solaris.
- Se han modificado los ajustes de los parámetros en el archivo de configuración de HBA (por ejemplo, qla2300.conf).
- En un entorno SAN, se han configurado los enlaces.
- Se han creado y habilitado zonas para la partición Solaris.
- El almacenamiento está correlacionado con la partición Solaris.

Para completar la instalación de Veritas DMP realice los procedimientos en el siguiente orden:

1. "Preparación para la instalación de Veritas DMP"
2. "Instalación del paquete ASL" en la página 178

Preparación para la instalación de Veritas DMP

Para preparar el host para la instalación de Veritas DMP, complete los pasos siguientes:

1. Elija el host Solaris en el que quiere instalar DMP.
2. Complete los siguientes pasos para definir manualmente los destinos y LUN en el archivo `/kernel/drv/sd.conf`:

Nota: De manera predeterminada, el archivo `/kernel/drv/sd.conf` define los destinos 0, 1, 2 y 3. El LUN0 también se define para los destinos 0, 1, 2 y 3. Cada destino representa un controlador en un subsistema de almacenamiento, y cada LUN representa una unidad lógica. Si va a añadir definiciones de destino o LUN en el archivo `/kernel/drv/sd.conf` para una configuración de DMP existente, asegúrese de reorganizar el host Solaris.

- a. Escriba el siguiente comando para abrir el archivo `/kernel/drv/sd.conf` con el Editor vi:

```
# vi /kernel/drv/sd.conf
```

El archivo será similar al siguiente ejemplo:

```
#  
# Copyright (c) 1992, Sun Microsystems, Inc.  
#  
# ident "@(#)sd.conf 1.9 98/01/11 SMI"  
  
name="sd" class="scsi" class_prop="atapi"  
target=0 lun=0;  
  
name="sd" class="scsi" class_prop="atapi"  
target=1 lun=0;  
  
name="sd" class="scsi" class_prop="atapi"  
target=2 lun=0;  
  
name="sd" class="scsi" class_prop="atapi"  
target=3 lun=0;
```

- b. Utilice el Editor vi para añadir definiciones de destino y LUN. En el siguiente ejemplo, se supone que el host Solaris está conectado a un subsistema de almacenamiento con tres LUN correlacionados con la

partición del subsistema de almacenamiento. Además, el LUN de acceso debe estar correlacionado con la partición.

```
#
# Copyright (c) 1992, Sun Microsystems, Inc.
#
# ident "@(#)sd.conf 1.9 98/01/11 SMI"

name="sd" class="scsi" class_prop="atapi"
target=0 lun=0;

name="sd" class="scsi" class_prop="atapi"
target=1 lun=0;

name="sd" class="scsi" class_prop="atapi"
target=2 lun=0;

name="sd" class="scsi" class_prop="atapi"
target=3 lun=0;

name="sd" class="scsi" target=0 lun=1;
name="sd" class="scsi" target=0 lun=2;
name="sd" class="scsi" target=0 lun=3;
name="sd" class="scsi" target=0 lun=31;
name="sd" class="scsi" target=1 lun=1;
name="sd" class="scsi" target=1 lun=2;
name="sd" class="scsi" target=1 lun=3;
name="sd" class="scsi" target=1 lun=31;
```

- c. Escriba el siguiente comando para guardar las nuevas entradas en el archivo `/kernel/drv/sd.conf`:

```
# :wq
```

3. Escriba el siguiente comando para verificar que RDAC no está instalado en el host:

```
# pkginfo -l RDAC
```

4. Si RDAC está instalado, escriba el siguiente comando para eliminarlo:

```
# pkgrm RDAC
```

5. Compruebe que se ha creado una partición de host.

Importante: Defina el tipo de host como **Solaris con DMP**. Si no lo hace, no podrá establecer correlaciones para más de los 32 LUN máximos de RDAC y podrían producirse otros resultados indeseados.

6. Asegúrese de que todas las rutas son óptimas y se encuentran en estado de ruta preferida en el SMclient.
7. Instale Veritas Storage Foundation Solaris, incluyendo Veritas Volume Manager con DMP.

Importante: Antes de instalar Veritas Storage Foundation Solaris con Veritas Volume Manager y DMP, asegúrese de que cuenta con las claves de licencia necesarias. Este documento no describe cómo instalar el producto Veritas. Para obtener más información, consulte la documentación de Symantec en <http://www.symantec.com/business/support/>.

8. Escriba el siguiente comando para reiniciar el host Solaris:

```
# shutdown -g0 -y -i6
```

Instalación del paquete ASL

Si fuera necesario, complete los pasos siguientes para instalar el paquete de ASL.

Nota: La versión VxVM 4.x del paquete de ASL se llama SMibmas1 (para obtener más información, consulte <http://seer.entsupport.symantec.com/docs/284913.htm>). En VxVM versión 5.0 y posteriores, muchas ASL están integradas en VxVM y no necesitan ser instaladas. Para VxVM versión 5.0 y posteriores, el paquete de ASL se llama VRTSLSIas1 (consulte <http://seer.entsupport.symantec.com/docs/340469.htm>). En el siguiente ejemplo se supone que está instalado VxVM 4.x.

1. Escriba el siguiente comando para instalar el paquete **SMibmas1**:

Nota: Puede seleccionar el predeterminado (all) o la opción 1.

```
# pkgadd -d SMibmas1_pkg
```

2. Escriba el siguiente comando para reiniciar el host Solaris:

```
# shutdown -g0 -y -i6
```

Consulte la documentación de Symantec Veritas para obtener información sobre cómo completar las tareas siguientes:

- Iniciar Veritas Volume Manager
- Configurar grupos de discos
- Crear volúmenes
- Crear sistemas de archivos
- Montar sistemas de archivos

Identificación de dispositivos

Tras haber instalado el controlador multi-ruta o verificado si este ya está instalado, utilice el programa de utilidad SMdevices para identificar una unidad lógica del subsistema de almacenamiento asociada con un dispositivo del sistema operativo.

Uso del programa de utilidad SMdevices

El software SMutil incluye un programa de utilidad llamado SMdevices que puede utilizar para ver la unidad lógica del subsistema de almacenamiento asociada con un nombre de dispositivo del sistema operativo concreto. Este programa de utilidad es muy útil cuando desea crear letras de unidad o particiones utilizando el administrador de discos.

Uso de SMdevices en sistemas operativos Windows

Tras crear las unidades lógicas en un subsistema de almacenamiento, vaya al host asociado con ese subsistema de almacenamiento y complete los pasos indicados a continuación para utilizar SMdevices en Windows:

1. Desde un indicador de comandos o DOS, cambie al directorio `<installation_directory>\Util`,
donde *installation_directory* es el directorio en el que ha instalado SMutil.
El directorio predeterminado es `c:\Archivos de programa\IBM_DS4000\Util`.
2. Escriba SMdevices y pulse Intro.

Uso de SMdevices en sistemas operativos de tipo UNIX

Puede utilizar SMdevices para correlacionar el nombre de dispositivo asignado por el host para cada LUN con su correspondiente dispositivo de subsistema de almacenamiento. En el resultado de SMdevices, puede ver la información del subsistema de almacenamiento siguiente, como se muestra en SMclient.

Nota: Los ejemplos de la lista hacen referencia al resultado de ejemplo de SMdevices.

- Nombre asignado por el host (/dev/sdh)
- Nombre de subsistema de almacenamiento DS3000, DS4000 o DS5000 (DS4500_Storage_Server-A)
- Nombre de unidad lógica (Raid-5-0A)
- Identificador de LUN (LUN 4)
- Propietario preferido del controlador, y si el controlador controla la unidad lógica

El siguiente ejemplo presenta un resultado de muestra de SMdevices para el subsistema de almacenamiento DS4500_Storage_Server-A:

```
# SMdevices
IBM FAST Storage Manager Devices, Version 09.12.A5.00
Built Fri Jan 14 16:42:15 CST 2005
(C) Copyright International Business Machines Corporation,
2004 Licensed Material - Program Property of IBM. Reservados todos los
derechos.
/dev/sdh (/dev/sg10) [Storage Subsystem DS4500_Storage_Server-A,
Logical Drive Raid-5-0A, LUN 4, Logical Drive ID
<600a0b80000f0fc300000044412e2dbf>, Preferred Path (Controller-A): In Use]
/dev/sdd (/dev/sg6) [Storage Subsystem DS4500_Storage_Server-A,
Logical Drive Raid-5-1A, LUN 0, Logical Drive ID
<600a0b80000f13ec00000016412e2e86>, Preferred Path (Controller-B): In Use]
/dev/sde (/dev/sg7) [Storage Subsystem DS4500_Storage_Server-A,
Logical Drive Raid-0-0A, LUN 1, Logical Drive ID
<600a0b80000f0fc30000003c412e2d59>, Preferred Path (Controller-A): In Use]
/dev/sdf (/dev/sg8) [Storage Subsystem DS4500_Storage_Server-A,
Logical Drive Raid-1-0A, LUN 2, Logical Drive ID
<600a0b80000f0fc30000003e412e2d79>, Preferred Path (Controller-A): In Use]
/dev/sdg (/dev/sg9) [Storage Subsystem DS4500_Storage_Server-A,
Logical Drive Raid-3-0A, LUN 3, Logical Drive ID
<600a0b80000f13ec00000012412e2e4c>, Preferred Path (Controller-A): In Use]
```

Identificación de dispositivos en hostsAIX

La información de esta sección describe el descubrimiento de dispositivos en AIX. Para obtener información sobre resolución de problemas relacionados con errores de la matriz de discos en AIX, consulte “Resolución de errores de matriz de discos en AIX” en la página 296 en Capítulo 7, “Resolución de problemas”, en la página 273.

Comprensión de dispositivos en hosts AIX

el controlador multi-ruta crea los siguientes dispositivos que representan la configuración del subsistema de almacenamiento:

- dar** El dispositivo direccionador de la matriz de discos (dar) representa la matriz entera, incluyendo las rutas actual y aplazadas a todos los LUN (hdisks).
- dac** Los dispositivos controlador de matriz de discos (dac) representan un controlador dentro del subsistema de almacenamiento. En el subsistema de almacenamiento hay dos dacs. Con MPIO, el dispositivo dac se muestra solo si se asigna un dispositivo UTM.
- hdisk** Cada dispositivo hdisk representa un LUN individual de la matriz.
- utm** El dispositivo mecanismo de transporte universal (utm) se utiliza solo con configuraciones de gestión dentro de banda, como canal de comunicación entre el SMagent y el subsistema de almacenamiento.

Nota: El dispositivo utm se puede indicar en el resultado de un comando, independientemente de si tiene una configuración de gestión dentro de banda. Por ejemplo, se podría indicar un utm al ejecutar el comando **lsattr** en un dac.

Realización del descubrimiento de dispositivos inicial

Para realizar el descubrimiento de dispositivo inicial, realice estos pasos:

1. Asegúrese de que el subsistema de almacenamiento se ha configurado, los LUN se han asignado al host y el controlador multi-ruta está instalado.
2. Escriba el siguiente comando para buscar los nuevos dispositivos:

```
# cfmgr -v
```

Nota: En una configuración SAN, los dispositivos no inician sesión en el conmutador SAN hasta que ejecuta el comando **cfmgr**.

3. Escriba el siguiente comando:

```
# lsdev -Cc disk
```

4. Examine el resultado del comando **lsdev -Cc disk** para asegurarse de que el software RDAC reconoce las unidades lógicas del subsistema de almacenamiento, como se muestra en la siguiente lista:

- Each DS4200 logical drive is recognized as an 1814 DS4200 Disk Array Device.
- Each DS4300 logical drive is recognized as an 1722-600 (600) Disk Array Device.
- Each DS4400 logical drive is recognized as an 1742-700 (700) Disk Array Device.
- Each DS4500 logical drive is recognized as an 1742-900 (900) Disk Array Device.
- Each DS4700 logical drive is recognized as an 1814 DS4700 Disk Array Device.
- Each DS4800 logical drive is recognized as an 1815 DS4800 Disk Array Device.

Importante: Podría observar que el proceso de configuración crea dos dacs y dos dars en un subsistema de almacenamiento. Esta situación se puede producir cuando el host utiliza una partición que no tiene LUN asociados. Si esto ocurre, el sistema no puede asociar los dos dacs al dar correcto. Si no hay LUN, el sistema genera dos dacs según lo previsto, pero también genera dos dacs.

En la siguiente lista se indican las causas más habituales:

- Crea una partición y asocia los LUN a la misma, pero no añade puertos de host a la partición. Así, los puertos de host permanecen en la partición predeterminada.
- Sustituye uno o varios HBA pero no actualiza el nombre mundial (WWN) de la partición del HBA.
- Cambia el subsistema de almacenamiento de un conjunto de HBA a otro como parte de una reconfiguración y no actualiza los WWN.

En todos estos casos, resuelva el problema y ejecute **cfmgr** de nuevo. El sistema eliminará el dar adicional o lo cambiará de estado Disponible a estado Definido. (Si el sistema cambia el dar a estado Definido, puede eliminarlo).

Nota: Al realizar la identificación inicial de dispositivos, los atributos de Object Data Manager (ODM) de cada dispositivo se actualizan con los valores predeterminados. En la mayoría de los casos y para la mayoría de configuraciones, los valores predeterminados son adecuados. No obstante, algunos valores se pueden modificar para obtener un mayor rendimiento y disponibilidad. Consulte Apéndice D, “Visualización y definición de atributos de gestor de datos de objeto (ODM) de AIX”, en la página 339 para obtener información sobre el uso del comando `lsattr` para ver los valores de los atributos de un sistema AIX.

Ejemplo de un descubrimiento inicial con MPIO

El siguiente ejemplo muestra un descubrimiento inicial con MPIO.

```
# lsdev -C |grep hdisk10
hdisk10    Available 05-08-02      MPIO Other DS4K Array Disk

# lscfg -vpl hdisk10
hdisk10    U787F.001.DPM0H2M-P1-C3-T1-W200400A0B8112AE4-L9000000000000
MPIO Other DS4K Array Disk
  Manufacturer.....IBM
  Machine Type and Model.....1814      FAStT
  ROS Level and ID.....30393136
  Serial Number.....
  Device Specific.(Z0).....0000053245004032
  Device Specific.(Z1).....

# mpio_get_config -A
Storage Subsystem worldwide name: 60ab8001122ae000045f7fe33
Storage Subsystem Name = 'Kinks-DS-4700'
  hdisk          LUN #
  hdisk2         1
  hdisk3         2
  hdisk4         3
  hdisk5         4
  hdisk6         5
  hdisk7         6
  hdisk8         7
  hdisk9         8
  hdisk10        9
  hdisk11        10
```

Configuración de dispositivos

Para maximizar el rendimiento de su subsistema de almacenamiento, puede definir la profundidad de cola de sus `hdisk`s, deshabilitar la duplicación de la memoria caché, utilizar capacidad dinámica y expansión dinámica de la unidad lógica (DVE) y comprobar el tamaño de sus LUN.

Uso del programa de utilidad `hot_add`

El programa de utilidad `hot_add` permite añadir nuevas unidades lógicas sin tener que reiniciar el sistema. El programa de utilidad registra las nuevas unidades lógicas con el sistema operativo para que pueda utilizar el Administrador de discos para crear particiones y añadir nombres de dispositivo. El programa de utilidad `hot_add` forma parte del paquete de software `SMutil`. Si ejecuta el programa dos veces y las nuevas unidades lógicas no se muestran en la ventana del Administrador de discos, debe ejecutar el diagnóstico de canal de fibra o reiniciar el host.

Tras crear las unidades lógicas en un subsistema de almacenamiento, vaya al host asociado con ese subsistema de almacenamiento y complete los pasos indicados a continuación para utilizar `hot_add`:

1. Desde el DOS o desde un indicador de mandatos, cambie al directorio siguiente:

```
<installation_directory>\Util
```

donde *installation_directory* es el directorio en el que ha instalado SMutil.

Nota: El directorio predeterminado es `c:\Archivos de programa\IBM_DS4000\Util`.

2. Desde el indicador de comandos o DOS, escriba el comando siguiente:
`hot_add`
3. Pulse Intro. Las nuevas unidades lógicas estarán disponibles a través del Administrador de discos.

Uso del programa de utilidad SMrepassist

Utilice el programa de utilidad SMrepassist para desechar datos de la memoria caché de una unidad lógica.

Importante: La unidad FlashCopy no se puede correlacionar o añadir al mismo servidor en el que está la unidad lógica de FlashCopy en un entorno Windows 2000, Windows Server 2003, Windows Server 2008 o NetWare. Debe correlacionar la unidad lógica de FlashCopy con otro servidor.

Para desechar datos de la memoria caché de una unidad lógica, complete los pasos indicados a continuación:

1. Desde el DOS o desde un indicador de mandatos, cambie al directorio

```
<installation_directory>\Util
```

donde *installation_directory* es el directorio en el que ha instalado SMutil.

Nota: El directorio predeterminado es `c:\Archivos de programa\IBM_DS4000\Util`.

2. Escriba el siguiente comando:

```
smrepassist -f logical_drive_letter:
```

donde *logical_drive_letter* es la letra de unidad del sistema operativo asignada a la partición de disco en la unidad lógica.

3. Pulse Intro.

Detención y reinicio del software del agente de host

Debe detener y reiniciar el software del agente de host si añade subsistemas de almacenamiento al dominio de gestión del software del agente de host. Cuando reinicia el servicio, el software del agente de host detecta los nuevos subsistemas de almacenamiento y los añade al dominio de gestión.

Nota: Si no se detecta ninguna unidad lógica de acceso tras el reinicio, el software del agente de host detiene su ejecución automáticamente. Asegúrese de que existe una conexión de canal de fibra entre el host y la SAN a la que está conectada en subsistema de almacenamiento, y reinicie el host o nodo de clúster para que se puedan descubrir los nuevos subsistemas de almacenamiento de gestión de agente de host.

Utilice el procedimiento aplicable para su sistema operativo de esta sección.

Windows 2000

Para detener y reiniciar el software del agente de host en Windows 2000, complete los siguientes pasos:

1. Pulse **Inicio > Programas > Herramientas administrativas > Servicios**. Se abrirá la ventana Servicios.
2. Pulse con el botón derecho en **IBM DS Storage Manager Agent**.
3. Pulse **Reiniciar**. Storage Manager Agent se detendrá e iniciará de nuevo.
4. Cierre la ventana Servicios.

Windows Server 2003 y 2008

Para detener y reiniciar el software del agente de host en Windows Server 2003 y 2008, complete los siguientes pasos:

1. Pulse **Inicio > Herramientas administrativas > Servicios**. Se abrirá la ventana Servicios.
2. Pulse con el botón derecho en **IBM DS Storage Manager Agent**.
3. Pulse **Reiniciar**. Storage Manager Agent se detendrá e iniciará de nuevo.
4. Cierre la ventana Servicios.

Windows Server 2012

Para detener y reiniciar el software del agente de host en Windows Server 2012, complete los siguientes pasos:

1. Pulse **Administración del servidor > Herramientas > Servicios**. Se abrirá la ventana Servicios.
2. Pulse con el botón derecho en **IBM DS Storage Manager Agent**.
3. Pulse **Reiniciar**. Storage Manager Agent se detendrá e iniciará de nuevo.
4. Cierre la ventana Servicios.

Definición de la profundidad de cola para dispositivos hdisk

Definir el atributo `queue_depth` con el valor adecuado es importante para obtener un rendimiento óptimo del sistema. Utilice este valor si tiene una configuración de subsistema de almacenamiento grande con muchas unidades lógicas y hosts conectados.

Esta sección proporciona métodos para calcular la profundidad de cola máxima que puede utilizar como guía para ayudarle a determinar el mejor valor de profundidad de cola para su configuración.

Cálculo de la profundidad de cola máxima

La fórmula para calcular la profundidad de cola máxima de su sistema depende de la versión del firmware instalada en el controlador. Utilice una de las siguientes fórmulas para calcular la profundidad de cola máxima para su sistema.

Importante:

1. Es posible que la profundidad de cola máxima no sea un valor óptimo en todos los casos. Utilice la profundidad de cola máxima como directriz y ajuste el valor, según las necesidades, a su configuración específica.
2. En sistemas con uno o más dispositivos SATA conectados, podría tener que definir el atributo `queue_depth` con un valor inferior a la profundidad de cola máxima.

Fórmulas para controlador con versión de firmware 07.10.xx.xx y posterior

En sistemas de almacenamiento DS4800 y DS4700, o DS4200, que ejecutan la versión de firmware del controlador 07.10.xx.xx o posterior, utilice las siguientes fórmulas para determinar la profundidad de cola máxima:

DS4800: $4096 / (\text{número de hosts} * \text{LUN por host})$. Por ejemplo, un sistema DS4800 con cuatro hosts, cada uno con 32 LUN, tendría una profundidad de cola máxima de 32: $4096 / (4 * 32) = 32$.

DS4700 o DS4200: $2048 / (\text{número de hosts} * \text{LUN por host})$. Por ejemplo, un sistema DS4700 o DS4200 con cuatro hosts, cada uno con 32 LUN, tendría una profundidad de cola máxima de 16: $2048 / (4 * 32) = 16$.

Fórmula para versiones de firmware de controlador 05.4x.xx.xx, o 06.1x.xx.xx a 06.6x.xx.xx

En sistemas de almacenamiento DS4000 o DS5000 con versión de firmware 05.4x.xx.xx o 06.1x.xx.xx a 06.6x.xx.xx, utilice la siguiente fórmula para determinar la profundidad de cola máxima: $2048 / (\text{número de hosts} * \text{LUN por host})$. Por ejemplo, un sistema con cuatro hosts, cada uno con 32 LUN, tendría una profundidad de cola máxima de 16: $2048 / (4 * 32) = 16$.

Fórmula para versiones de firmware de controlador 05.30.xx.xx

En sistemas de almacenamiento DS4000 o DS5000 con versión de firmware 05.30.xx.xx o anterior, utilice la siguiente fórmula para determinar la profundidad de cola máxima: $512 / (\text{número de hosts} * \text{LUN por host})$. Por ejemplo, un sistema con cuatro hosts, cada uno con 32 LUN, tendría una profundidad de cola máxima de 4: $512 / (4 * 32) = 4$.

Cambio de la profundidad de cola para Windows

Puede utilizar el programa QLogic SANsurfer para modificar las preferencias de configuración del adaptador de host y configuración avanzada del adaptador desde el entorno del sistema operativo Windows. No obstante, para que se apliquen los cambios, debe reiniciar los servidores.

De forma alternativa, para cambiar el valor de profundidad de cola para el adaptador QLogic en un entorno de sistema operativo Microsoft Windows, debe seleccionar el menú **Valores de configuración** Fast!UTIL y después **Configuración avanzada del adaptador** para acceder al **Regulador de ejecución**.

Cambio de la profundidad de cola para AIX

Puede cambiar el atributo `queue_depth` para AIX con el comando `chdev -l`, como se muestra en el siguiente ejemplo.

```
# chdev -l hdiskX -a queue_depth=y -P
```

donde *X* es el nombre del hdisk y *y* el el valor de profundidad de cola.

Nota: Utilice el distintivo `-P` para hacer los cambios permanentes en la clase de objeto de dispositivos personalizados.

Inhabilitación de la duplicación de memoria caché

Atención: Antes de inhabilitar la duplicación de la memoria caché, realice una copia de seguridad de todos los datos. Si inhabilita la creación de reflejo de la memoria caché, es posible que se produzcan pérdidas de datos si un controlador falla, se reinicia o se apaga.

Para inhabilitar la duplicación de la memoria caché en Storage Manager, complete estos pasos:

1. En la pestaña **Lógica** o **Física** de la ventana Gestión del subsistema, pulse con el botón derecho en la unidad lógica donde desea inhabilitar la duplicación de la memoria caché y seleccione **Cambiar > Configuración de memoria caché**.
2. En la ventana Cambiar valores de memoria caché, borre el recuadro de selección **Habilitar escritura en memoria caché con duplicación**.
3. Pulse **Aceptar**.

Nota: En sistemas operativos AIX, cuando se abre un LUN que se ejecuta con la escritura en memoria caché habilitada y la duplicación inhabilitada, se muestra un mensaje de aviso sobre matriz FCP. El aviso se vuelve a mostrar cada 24 horas hasta que se habilite de nuevo la duplicación de la memoria caché.

Uso de la expansión de capacidad dinámica y la expansión de unidad lógica dinámica

La expansión de unidad lógica dinámica (DVE) aumenta el tamaño de una unidad lógica. Para realizar una DVE, debe disponer de capacidad libre disponible en la matriz. De no ser así, puede realizar una expansión de capacidad dinámica (DCE) para aumentar la capacidad de la matriz añadiendo unidades. Tras asegurarse de que existe capacidad libre suficiente en la matriz, puede llevar a cabo una operación de DVE.

Realización de una expansión de capacidad dinámica

Si desea aumentar la capacidad de la matriz, complete los pasos siguientes para realizar una DCE.

Nota: Para obtener más información sobre este procedimiento, consulte la ayuda en línea de Storage Manager.

1. En la pestaña **Lógica** o **Física** de la ventana Gestión del subsistema, pulse con el botón derecho en la matriz y seleccione **Añadir capacidad libre (unidades)**.
2. En la ventana Añadir capacidad libre (unidades), seleccione una o dos unidades disponibles y pulse **Añadir**.

Realización de una expansión de unidad lógica dinámica

Antes de llevar a cabo una expansión de unidad lógica dinámica (DVE), asegúrese de que existe capacidad libre disponible en la matriz. Compruebe la pestaña **Lógica** o **Física** de la ventana Gestión del subsistema para verificar la cantidad de capacidad libre disponible. Si no hay capacidad libre suficiente pero hay unidades adicionales disponibles, puede añadir una o varias unidades a la matriz realizando una expansión de capacidad dinámica (DCE) antes de llevar a cabo la operación de DVE.

Nota:

1. No puede redimensionar la unidad lógica mientras la matriz está activada en modo concurrente clásico o mejorado.
2. No puede redimensionar la matriz raíz.

Si desea aumentar la capacidad de una unidad lógica, complete los pasos siguientes para realizar una DVE.

Nota: Para obtener más información sobre este procedimiento, consulte la ayuda en línea de Storage Manager.

1. En la pestaña **Lógica** o **Física** de la ventana Gestión del subsistema, pulse con el botón derecho en la unidad lógica y seleccione **Aumentar capacidad**. Se abrirá la ventana Aumentar capacidad de unidad lógica - Instrucciones adicionales.
2. Lea las instrucciones adicionales y pulse **Aceptar**. Se abrirá la ventana Aumentar capacidad de unidad lógica.
3. Escriba la cantidad en la que desea aumentar la unidad lógica y pulse **Aceptar**. Se mostrará un icono de reloj en cada unidad lógica de la matriz. Debe esperar a que se complete el proceso para poder comenzar cualquier intervención en el host.

Nota: Si el subsistema de almacenamiento está ocupado, el proceso podría tardar varias horas.

4. Escriba los siguientes comandos para volver a explorar la unidad lógica en el host:

```
# cd /sys/block/sdXX/device
# echo 1 > rescan
```

donde *XX* es el nombre del dispositivo.

5. Compruebe el tamaño de la unidad lógica utilizando el procedimiento descrito en "Comprobación del tamaño de LUN" en la página 189.
6. Monte de nuevo la unidad lógica.

Veritas Storage Foundation con SUSE Linux Enterprise Server

A veces el tiempo de arranque aumenta debido a la exploración LVM, pero en el entorno Veritas Storage Foundation no requiere dicha exploración LVM. Por ello, con SLES 10 SP2 o posterior, debe inhabilitar la exploración LVM. Para ello utilice el siguiente procedimiento.

Nota:

- En el entorno Veritas Storage Foundation Linux, el tipo de host predeterminado debe definirse como 13 (LNXCVMWARE o LNXCLUSTER dependiendo de la versión de firmware del controlador).
 - IBM solo soporta DMP A/P-F ASL/APM, no A/P-C ASL.
 - Durante el arranque, antes de que se cargue DMP los analizadores de E/S que van al controlador no propietario generan errores de tiempo de espera. Estos errores de tiempo de arranque no inevitables y no significativos.
1. En el archivo `/etc/lvm/lvm.conf`, cambie el filtro de línea = `["a/*/"]` por el filtro = `["r|/dev/*/by-path/*|", "r|/dev/*/by-id/*|", "r|/dev/sd.*|", "a/*/"]`.
 2. Si la raíz/intercambio es un volumen LVM, complete las tareas siguientes:
 - Añada su dispositivo específico al filtro en el paso 1 para asegurarse de que se exploran los volúmenes adecuados.

- Tras completar el paso 1, ejecute `mkinitrd` y utiliza la nueva imagen `initrd` para futuros arranques.

Veritas Storage Foundation 5.0 con Red Hat Enterprise Linux

El siguiente procedimiento solo es necesario para habilitar el módulo RDAC en RHEL 5.3 para Storage Foundation 5.0. El módulo ya está integrado en Storage Foundation 5.1 y posterior. El módulo `scsi_dh_RDAC` proporciona soporte para los dispositivos RDAC. Elimina el retardo y algunos mensajes de error mostrados durante el proceso de arranque o sondeo.

Nota:

1. En el entorno Veritas Storage Foundation Linux, el tipo de host predeterminado debe definirse como 13 (LNXCLVMWARE o LNXCLUSTER dependiendo de la versión de firmware del controlador).
2. IBM solo soporta DMP A/P-F ASL/APM, no A/P-C ASL.
3. Durante el arranque, antes de que se cargue DMP los analizadores de E/S que van al controlador no propietario generan errores de tiempo de espera. Estos errores de tiempo de arranque no inevitables y no significativos.
4. El siguiente procedimiento trabaja con el IBM NVSRAM porque el módulo `scsi_dh_RDAC` depende de VID/PID.

Habilitación del módulo RDAC en RHEL 5.3 para Storage Foundation 5.0

Para habilitar el módulo RDAC en RHEL 5.3 para Storage Foundation 5.0, complete los pasos siguientes:

1. Inhabilite todos los puertos de almacenamiento del subsistema de almacenamiento para que el HBA no pueda detectarlos.
2. Instale Storage Foundation.
3. Ejecute `mkinitrd` para incluir el módulo `scsi_dh_rdac`:
`mkinitrd $resultant_initrd_image_file $kernel_version --preload=scsi_dh_rdac`

Por ejemplo:

```
mkinitrd /boot/my_image 2.6.18-118.el5 --preload=scsi_dh_rdac
```

Nota: El comando `uname -r` ofrece la versión del kernel.

4. Cambie el cargador de arranque para utilizar la nueva imagen `initrd`. Para servidores IBM i y System p, la imagen `initrd` se llama `boot`. Para servidores System x, el nombre de la imagen es `grub`.
5. Cierre el servidor de host.
6. Habilite el subsistema de almacenamiento para que el HBA reconozca la configuración de almacenamiento.
7. Inicie el servidor de host.

Descarga del módulo RDAC en RHEL 5.3 para Storage Foundation 5.0

Para descargar el módulo tras el sondeo de dispositivos y el proceso de conexión, complete los siguientes pasos durante el proceso de arranque del sistema:

1. Cree un script `/etc/r3.d`, como el del ejemplo siguiente:

```

# vi /etc/init.d/rm_rdac

-----
## this script is used for detaching the scsi_dh_rdac module
## for each LUN
## this script has dependency on lsscsi command and this lsscsi
## should be available for this script to successfully execute.
#!/bin/bash
echo "detaching the scsi_dh_rdac module"
for i in /sys/block/sd*/device/dh_state
do
if [[ "`cat $i`" = "rdac" ]]
then
echo detach > $i
fi
done

modprobe -r scsi_dh_rdac
echo "detached successfully"
-----

```

2. Inserte el script en la ubicación correcta bajo /etc/rc3.d, antes del script de inicio de VCS VxFen Driver (el script de inicio predeterminado de VxFen Driver es /etc/rc2.d/S68vxfen). Si el sistema no ejecuta VCS, inserte el script tras el script /etc/rc3.d/S50vxvm-recover.

```

# ln -s /etc/init.d/rm_rdac /etc/rc.d/rc3.d/S57rm_rdac
# ln -s /etc/init.d/rm_rdac /etc/rc.d/rc5.d/S57rm_rdac

```

Comprobación del tamaño de LUN

Para comprobar el tamaño de un LUN en AIX, siga los pasos indicados a continuación:

1. Especifique los comandos siguientes:

```

#cd /sys/block/sdXX
# cat size

```

donde XX es el nombre del dispositivo. Se mostrará un número, como en el ejemplo siguiente:

```
8388608
```

2. Multiplique este número por 512 (bytes) para calcular el tamaño del LUN, como puede ver en el siguiente ejemplo:

```
8388608 * 512 = 4294967296 (~ 4GB)
```

En este ejemplo, el tamaño del LUN es de 4 GB aproximadamente.

Redistribución de unidades lógicas

En condiciones de migración tras error en las que las unidades lógicas han migrado a la ruta del controlador secundario, algunas configuraciones requieren la intervención manual para volver a mover las unidades una vez resuelto el error. La necesidad de esta intervención depende del controlador multi-ruta del host instalado y de si se ha habilitado ADT (transferencia automática de unidades). De forma predeterminada, ADT está deshabilitada en AIX y Windows, pero sus controladores multi-ruta se pueden recuperar automáticamente. De forma predeterminada, ADT está habilitada en Linux, pero el controlador de MPP puede encargarse de la recuperación automática; debe inhabilitar ADT si utiliza este controlador.

En la ventana Gestión del subsistema, pulse **Avanzada > Recuperación > Redistribuir unidades lógicas** para redistribuir las unidades lógicas a sus rutas preferidas.

Para redistribuir unidades lógicas en AIX, HP-UX o Solaris, complete el procedimiento aplicable de esta sección.

Redistribución de unidades lógicas en AIX

Si ha habilitado la recuperación automática en el host AIX, no tendrá que redistribuir las unidades lógicas manualmente tras la migración tras error del controlador. No obstante, si tiene un entorno de host heterogéneo, quizá deba redistribuir las unidades lógicas de forma manual. Los hosts que no soportan alguna forma de recuperación automática o los hosts AIX en los que la recuperación automática está inhabilitada, no redirigen las unidades lógicas a las rutas preferidas de modo automático.

Para obtener información sobre resolución de problemas relacionados con errores de la matriz de discos en AIX, consulte “Resolución de errores de matriz de discos en AIX” en la página 296 en Capítulo 7, “Resolución de problemas”, en la página 273.

Complete los pasos siguientes para redistribuir manualmente las unidades lógicas en sus rutas:

1. Repare o sustituya los componentes defectuosos que pueda haber. Para obtener más información sobre resolución de problemas, consulte la *Guía de mantenimiento, usuario e instalación* facilitada con su subsistema de almacenamiento.
2. En la ventana Gestión del subsistema, pulse **Avanzada > Recuperación > Redistribuir unidades lógicas** para redistribuir las unidades lógicas a sus rutas preferidas.

Nota: Si se ha configurado un gran número de LUN en el subsistema de almacenamiento, la redistribución de las unidades lógicas podría tardar 60 minutos o más.

3. Ejecute el comando **fget_config** para verificar las rutas activas, como se muestra en el siguiente ejemplo.

```
# fget_config -l dar0
dac0 ACTIVE dac1 ACTIVE
dac0-hdisk1
dac0-hdisk2
dac0-hdisk3
dac1-hdisk4
dac1-hdisk5
dac1-hdisk6
dac1-hdisk7
dac0-hdisk8
```

Redistribución de unidades lógicas en HP-UX

La transferencia automática de unidades (ADT) está habilitada de forma predeterminada en los hosts HP-UX. Si se produce un error que inicia la migración tras error de un controlador, ADT redirige las E/S al controlador disponible. ADT no requiere una redistribución manual.

Importante: Si se produce un error en un entorno de host heterogéneo, el host HP-UX con ADT habilitada redistribuye automáticamente sus LUN una vez que está disponible la ruta. No obstante, en los hosts en los que ADT no esté habilitada deberá redistribuir las unidades lógicas de forma manual. De no hacerlo, el subsistema de almacenamiento pasará al estado Requiere atención porque los hosts no soportan ADT y los hosts en los que ADT está inhabilitada no redirigen

automáticamente las E/S al controlador preferido. En este caso, Storage Manager Recovery Guru indica qué plataforma de host está asociada con el LUN que está en estado de migración tras error.

Nota: Los subsistemas de almacenamiento DS5000 no son compatibles con ALUA. Los subsistemas DS5000 tienen Target Port Group Support (TPGS), similar al protocolo SCSI, que dirige las E/S a los puertos preferidos. Para HP-UX 11.31, debe cambiar el tipo de host HP-UX por el tipo de host TPGS HPXTPGS.

Para activar el soporte TPGS y cambiar el tipo de host, complete los pasos siguientes:

1. Cambie el tipo de sistema operativo del subsistema de almacenamiento DS5000 de HPUX a HPXTPGS.
2. Cambie el equilibrio de carga a **Predeterminado, en rueda**.
3. Compruebe que los cambios son correctos. El siguiente ejemplo muestra uno de los LUN con cuatro rutas activas correctas y cuatro rutas en espera.

```
# scsimgr get_info all_lpt -D /dev/rdisk/asmlai |grep -e STATUS -e 'Open close state'
```

```
STATUS INFORMATION FOR LUN PATH : lunpath306
Open close state                = ACTIVE
STATUS INFORMATION FOR LUN PATH : lunpath344
Open close state                = STANDBY
STATUS INFORMATION FOR LUN PATH : lunpath420
Open close state                = STANDBY
STATUS INFORMATION FOR LUN PATH : lunpath326
Open close state                = ACTIVE
STATUS INFORMATION FOR LUN PATH : lunpath346
Open close state                = ACTIVE
STATUS INFORMATION FOR LUN PATH : lunpath213
Open close state                = ACTIVE
STATUS INFORMATION FOR LUN PATH : lunpath273
Open close state                = STANDBY
STATUS INFORMATION FOR LUN PATH : lunpath179
Open close state                = STANDBY
```

4. Utilice las herramientas de supervisión de conmutador de canal de fibra SAN para comprobar si las cargas de E/S se distribuyen adecuadamente.

Redistribución de unidades lógicas en Solaris

Si selecciona Solaris como tipo de host al definir el host y puerto de host, la Transferencia automática de unidades (ADT) se inhabilita en los hosts Solaris. En este caso, si se produce un error que inicia la migración tras error de un controlador, debe redistribuir las unidades lógicas a sus rutas preferidas de manera manual.

Complete los pasos siguientes para redistribuir manualmente las unidades lógicas a sus rutas preferidas:

1. Repare o sustituya los componentes defectuosos que pueda haber. Para obtener más información, consulte la *Guía de mantenimiento, usuario e instalación* facilitada con su subsistema de almacenamiento.
2. En la ventana Gestión del subsistema, pulse **Avanzada > Recuperación > Redistribuir unidades lógicas** para redistribuir las unidades lógicas a sus rutas preferidas.

Sustitución de HBA en caliente

Atención: Si no sigue este procedimiento como se indica aquí, podría perderse la disponibilidad de datos. Debe leer y comprender todos los pasos de esta sección antes de iniciar el procedimiento de intercambio en caliente del HBA.

Esta sección describe el procedimiento de intercambio en caliente de adaptadores de bus de host (HBA) de canal de fibra en un servidor System p.

La siguiente lista ofrece una descripción general de esta sección:

- “Sustitución de HBA en caliente en AIX”
- “Sustitución de HBA IBM en Linux” en la página 196
- “Sustitución de un HBA de conexión en caliente PCI” en la página 199
- “Correlación del nuevo WWPN con el subsistema de almacenamiento en AIX y Linux” en la página 200
- “Finalización del procedimiento de intercambio en caliente de HBA” en la página 200

Sustitución de HBA en caliente en AIX

Atención: Cualquier cambio en estas notas y procedimientos podría causar una pérdida en la disponibilidad de los datos.

Revise la siguiente lista de problemas y restricciones antes de realizar una operación de intercambio en caliente para AIX.

- El atributo de recuperación automática del dar debe estar definido como no. La recuperación automática es una característica definida de manera dinámica que se puede activar de nuevo una vez completado el procedimiento de intercambio en caliente. Si no inhabilita el modo de recuperación automática durante un procedimiento de intercambio en caliente, podría perder el acceso a datos.
- No redistribuya unidades lógicas a la ruta preferida hasta que verifique que la sustitución de HBA y la posterior configuración se han realizado correctamente. Si redistribuye las unidades lógicas antes de verificar si el intercambio en caliente y la configuración se ha realizado correctamente, podría perder el acceso a datos.
- El único escenario de intercambio en caliente soportado implica la sustitución de un HBA defectuoso por un HBA del mismo modelo y en la misma ranura PCI. No inserte el HBA defectuoso en otro sistema, aunque finalmente no resulte estarlo. Devuelva siempre el HBA a IBM.

Importante: En el momento de crear este documento, no se soportan otros escenarios de sustitución.

- El intercambio en caliente no se soporta en configuraciones de HBA único.

Preparación para el intercambio en caliente de HBA en AIX:

Para prepararse para el intercambio en caliente, complete los siguientes procedimientos:

Recopilación de datos del sistema

Para recopilar datos del sistema, siga estos pasos:

1. Escriba el siguiente comando:

```
# lsdev -C |grep fcs
```

El resultado será similar al ejemplo siguiente:

```
fcs0      Available 17-08      FC Adapter
fcs1      Available 1A-08      FC Adapter
```

2. Escriba el siguiente comando:

```
# lsdev -C |grep dac
```

El resultado será similar al ejemplo siguiente:

```
dac0      Available 17-08-02      1815      DS4800 Disk Array Controller
dac1      Available 1A-08-02      1815      DS4800 Disk Array Controller
```

3. Escriba el siguiente comando para cada dispositivo fcs:

```
# lscfg -vpl fcsX
```

donde *X* es el número de dispositivo fcs. El resultado será similar al ejemplo siguiente:

```
lscfg -vpl fcs0
fcs0      U0.1-P1-I1/Q1  FC Adapter

Part Number.....09P5079
EC Level.....A
Serial Number.....1C21908D10
Manufacturer.....001C
Feature Code/Marketing ID...2765
FRU Number.....09P5080
Network Address.....10000000C92D2981
ROS Level and ID.....02C03951
Device Specific.(Z0).....2002606D
Device Specific.(Z1).....00000000
Device Specific.(Z2).....00000000
Device Specific.(Z3).....03000909
Device Specific.(Z4).....FF401210
Device Specific.(Z5).....02C03951
Device Specific.(Z6).....06433951
Device Specific.(Z7).....07433951
Device Specific.(Z8).....20000000C92D2981
Device Specific.(Z9).....CS3.91A1
Device Specific.(ZA).....C1D3.91A1
Device Specific.(ZB).....C2D3.91A1
Device Specific.(YL).....U0.1-P1-I1/Q1
```

PLATFORM SPECIFIC

```
Name: Fibre Channel
Model: LP9002
Node: Fibre Channel@1
Device Type: fcp
Physical Location: U0.1-P1-I1/Q1
```

4. Escriba el siguiente comando:

```
# lsdev -C |grep dar
```

El resultado será similar al ejemplo siguiente:

```
# dar0      Available      1815      DS4800 Disk Array Router
dar1      Available      1815      DS4800 Disk Array Router
```

5. Escriba el siguiente comando para mostrar los atributos de cada dar encontrado en el sistema:

```
# lsattr -El darX
```

donde *X* es el número del dar. El resultado será similar al ejemplo siguiente:

```

lsattr -El dar0
act_controller  dac0,dac2  Active Controllers                False
all_controller  dac0,dac2  Available Controllers              False
held_in_reset   none        Held-in-reset controller          True
load_balancing  no          Dynamic Load Balancing            True
autorecovery    no          Autorecover after failure is corrected True
hlthchk_freq    600        Health check frequency in seconds  True
aen_freq        600        Polled AEN frequency in seconds   True
balance_freq    600        Dynamic Load Balancing frequency in seconds True
fast_write_ok   yes        Fast Write available               False
cache_size      1024       Cache size for both controllers    False
switch_retries  5          Number of times to retry failed switches True

```

Verificación para saber si la recuperación automática está inhabilitada

Antes de realizar el intercambio en caliente, complete los siguientes pasos para asegurarse de que la recuperación automática está inhabilitada en todos los dar que participan con el HBA que desea sustituir:

1. Escriba el siguiente comando para identificar todos los dacs que participan con el HBA:

```
# lsdev -C|grep 11-08
```

El resultado será similar al ejemplo siguiente:

```

# lsdev -C|grep 11-08
fcs0      Available 11-08      FC Adapter
fscsi0    Available 11-08-01     FC SCSI I/O Controller Protocol Device
dac0      Available 11-08-01     1742 (700) Disk Array Controller
hdisk1    Available 11-08-01     1742 (700) Disk Array Device
hdisk3    Available 11-08-01     1742 (700) Disk Array Device
hdisk5    Available 11-08-01     1742 (700) Disk Array Device
hdisk7    Available 11-08-01     1742 (700) Disk Array Device
hdisk8    Available 11-08-01     1742 (700) Disk Array Device

```

2. Compruebe el resultado del comando **lsattr** obtenido en el paso 5 del procedimiento "Recopilación de datos del sistema" en la página 192. En el resultado de **lsattr**, identifique los dars que indican los dacs identificados en el paso 1 de este procedimiento.
3. Escriba el siguiente comando para cada dar identificado en el paso 2:

```
# lsattr -El darX |grep autorecovery
```

donde X es el número del dar. El resultado será similar al ejemplo siguiente:

```

# lsattr -El dar0 |grep autorecovery
autorecovery  no          Autorecover after failure is corrected    True

```

4. En el resultado del comando **lsattr**, compruebe si la segunda palabra es no. Si la segunda palabra es yes, la recuperación automática estará habilitada.

Importante: Para cada dar en el que esté habilitada la recuperación automática, debe inhabilitarla definiendo el atributo ODM de recuperación automática en no. Consulte "Uso del comando lsattr para ver atributos de ODM" en la página 345 para saber cómo cambiar los valores de los atributos. No continúe con el intercambio en caliente hasta que haya completado este paso y verificado si la recuperación automática está inhabilitada.

Sustitución de HBA en caliente:

Atención: Si no sigue este procedimiento como se indica aquí, podría perderse la disponibilidad de datos. Debe leer y comprender todos los pasos de esta sección antes de iniciar el procedimiento de intercambio en caliente del HBA.

Para realizar un intercambio en caliente de HBA, complete los pasos siguientes:

1. Escriba el siguiente comando para poner el HBA que desea sustituir en estado Definido:

```
# rmdev -Rl fcsX
```

donde *X* es el número del HBA. El resultado será similar al ejemplo siguiente:

```
rmdev -Rl fcs0
  fcnet0 Defined
  dac0 Defined
  fscsi0 Defined
  fcs0 Defined
```

Para sistemas operativos Linux, escriba el siguiente comando para identificar la ranura de conexión en caliente PCI:

```
# drslot_chrp_pci -i -s slot-name
```

donde *slot-name* es el nombre de la ranura del HBA que va a sustituir, por ejemplo, U7879.001.DQD014E-P1-C3.

El LED de la ranura *slot-name* parpadeará y se mostrará el siguiente mensaje.

```
El indicador visual de la ranura PCI especificada
se ha definido en estado
de identificación. Pulse Intro para continuar o
x para salir.
```

2. En el menú smit de AIX, inicie el proceso necesario para el intercambio en caliente de HBA pulsando **smit > Dispositivos > Gestor de conexión en caliente de PC > Sustituir/Eliminar adaptador de conexión en caliente PCI**.
3. En la ventana Sustituir/Eliminar adaptador de conexión en caliente PCI, seleccione el HBA indicado. Se abrirá una ventana en la que se mostrarán instrucciones para sustituir el HBA.
4. Siga las instrucciones smit para sustituir el HBA.

Nota: No vuelva a instalar el cable del canal de fibra ahora.

5. Si los pasos de este procedimiento se han completado correctamente hasta ahora, obtendrá los siguientes resultados:
 - El HBA defectuoso se ha extraído del sistema.
 - El FC HBA de sustitución está encendido.
 - El dispositivo fcsX asociado está en estado Definido.

Antes de continuar, compruebe que ha obtenido estos resultados.

6. Instale el bucle de canal de fibra en el HBA de sustitución.
7. Escriba el siguiente comando para poner el HBA que desea sustituir en estado Activo:

```
# cfgmgr
```

Nota: El nuevo HBA se ubica en el grupo predeterminado. Si se han asignado hdisks al grupo predeterminado, el HBA genera un nuevo dar y un dac, que provocan una división. Emita el comando **rmdev** para eliminar el nuevo dar y dac tras correlacionar el WWPN.

8. Escriba el siguiente comando para comprobar que el dispositivo fcs ya está disponible:

```
# lsdev -C |grep fcs
```
9. Escriba el siguiente comando para comprobar o actualizar el firmware del HBA de sustitución al nivel adecuado:

```
# lscfg -vpl fcsX
```

donde X es el número del fcs.

10. Anote el número de 16 dígitos asociado con la Dirección de red, tal y como se muestra en el resultado del comando utilizado en el paso9. Este número de dirección de red se utilizará en el siguiente procedimiento, "Correlación del nuevo WWPN con el subsistema de almacenamiento en AIX yLinux" en la página 200.

11. Escriba el siguiente comando para devolver el HBA al estado Definido:

```
# rmdev -Rl fcsX
```

Tras completar estos pasos, continúe con "Correlación del nuevo WWPN con el subsistema de almacenamiento en AIX yLinux" en la página 200.

Sustitución de HBA IBM en Linux

Esta sección describe los requisitos y procedimientos para sustituir adaptadores de bus de host IBM en servidores System p, utilizando herramientas de conexión en caliente PCI.

Preparación para en intercambio en caliente de HBA IBM en Linux: Para prepararse para el intercambio en caliente, complete los siguientes procedimientos:

Verificación de las herramientas de conexión en caliente PCI

Asegúrese de que las siguientes herramientas están instaladas en el directorio /usr/sbin:

- lsslot
- drslot_chrp_pci

Si estas herramientas no están instaladas, complete los siguientes pasos para instalarlas:

1. Asegúrese de que `rdist-6.1.5-792.1` y `compat-2004.7.1-1.2` se instalan desde el soporte SLES 9.
2. Para encontrar los archivos rpm de las herramientas de conexión en caliente PCI, vaya a <http://www14.software.ibm.com/webapp/set2/sas/f/lopdiags/>.
3. En el sitio web, seleccione el enlace aplicable para su sistema operativo. Descargue e instale los siguientes archivos rpm:
 - `librtas-1.3.1-0.ppc64.rpm`
 - `rpa-pci-hotplug-1.0-29.ppc64.rpm`
4. Escriba el siguiente comando para instalar cada archivo rpm:

```
# rpm -Uvh <filename>.rpm
```

donde `<filename>` es el nombre del archivo rpm.

Verificación de la instalación del núcleo PCI

El núcleo PCI debe estar instalado en el sistema. Escriba el siguiente comando para verificar si está instalado:

```
# ls -l /sys/bus/pci/slots
```

Si el núcleo PCI está instalado, el resultado será similar al ejemplo siguiente:

```
elm17c224:/usr/sbin # ls -l /sys/bus/pci/slots
total 0
drwxr-xr-x  8 root root 0 Sep  6 04:29 .
drwxr-xr-x  5 root root 0 Sep  6 04:29 ..
drwxr-xr-x  2 root root 0 Sep  6 04:29 0000:00:02.0
```

```

drwxr-xr-x 2 root root 0 Sep 6 04:29 0000:00:02.4
drwxr-xr-x 2 root root 0 Sep 6 04:29 0000:00:02.6
drwxr-xr-x 2 root root 0 Sep 6 04:29 0001:00:02.0
drwxr-xr-x 2 root root 0 Sep 6 04:29 0001:00:02.6
drwxr-xr-x 2 root root 0 Sep 6 04:29 control

```

Si el directorio `/sys/bus/pci/slots` no existe, el núcleo PCI no estará instalado.

Verificación de la instalación del controlador rpaphp

El controlador rpaphp debe estar instalado en el sistema. Escriba el siguiente comando para verificar si está instalado:

```
ls -l /sys/bus/pci/slots/*
```

Si el controlador rpaphp está instalado, el resultado será similar al ejemplo siguiente:

```

e1m17c224:/usr/sbin # ls -l /sys/bus/pci/slots/*
/sys/bus/pci/slots/0000:00:02.0:
total 0
drwxr-xr-x 2 root root 0 Sep 6 04:29 .
drwxr-xr-x 8 root root 0 Sep 6 04:29 ..
-r--r--r-- 1 root root 4096 Sep 6 04:29 adapter
-rw-r--r-- 1 root root 4096 Sep 6 04:29 attention
-r--r--r-- 1 root root 4096 Sep 6 04:29 max_bus_speed
-r--r--r-- 1 root root 4096 Sep 6 04:29 phy_location
-rw-r--r-- 1 root root 4096 Sep 6 04:29 power

```

Uso de la herramienta lsslot para mostrar información de ranuras: Antes de sustituir un HBA utilizando una conexión en caliente PCI, puede utilizar la herramienta lsslot para mostrar la información sobre ranuras de E/S. En esta sección se describe cómo utilizar lsslot y proporciona ejemplos. Utilice la herramienta lsslot de acuerdo a las siguientes directrices.

Sintaxis de la herramienta lsslot

En el siguiente ejemplo se muestra la sintaxis de lsslot.

```
lsslot [ -c slot | -c pci [ -a | -o] ] [ -s drc-name ] [ -F delimiter ]
```

Opciones de la herramienta lsslot

En la siguiente lista se muestran las opciones de lsslot:

Sin opciones

Muestra todas las ranuras de DR

-c slot Muestra todas las ranuras de DR

-c pci Muestra todas las ranuras de conexión en caliente PCI

-c pci -a

Muestra todas las ranuras de conexión en caliente PCI (vacías) disponibles

-c pci -o

Muestra todas las ranuras de conexión en caliente PCI ocupadas

-F Utiliza un delimitador para delimitar las columnas

Lista de ranuras de conexión en caliente PCI con el comando lsslot

Esta sección muestra las líneas de comandos que puede utilizar para mostrar todas las ranuras de conexión en caliente PCI, ranuras de conexión en caliente PCI vacías

o ranuras de conexión en caliente PCI ocupadas. También puede ver información detallada sobre los dispositivos de conexión en caliente PCI.

Nota: En las columnas *Device(s)* del resultado de la línea de comandos, los dispositivos PCI de las ranuras se indican con el siguiente formato: *xxx:yy:zz.t* (por ejemplo, 0001:58:01.1).

Escriba el siguiente comando para mostrar todas las ranuras de conexión en caliente PCI:

```
# lsslot -c pci -a
```

El resultado será similar al ejemplo siguiente.

# Slot	Description	Device(s)
U7879.001.DQD014E-P1-C1	PCI-X capable, 64 bit, 133MHz slot	Empty
U7879.001.DQD014E-P1-C2	PCI-X capable, 64 bit, 133MHz slot	0002:58:01.0
U7879.001.DQD014E-P1-C3	PCI-X capable, 64 bit, 133MHz slot	0001:40:01.0
U7879.001.DQD014E-P1-C4	PCI-X capable, 64 bit, 133MHz slot	Empty
U7879.001.DQD014E-P1-C5	PCI-X capable, 64 bit, 133MHz slot	Empty
U7879.001.DQD014E-P1-C6	PCI-X capable, 64 bit, 133MHz slot	0001:58:01.0

Escriba el siguiente comando para mostrar todas las ranuras de conexión en caliente PCI vacías:

```
# lsslot -c pci -a
```

El resultado será similar al ejemplo siguiente.

# Slot	Description	Device(s)
U7879.001.DQD014E-P1-C1	PCI-X capable, 64 bit, 133MHz slot	Empty
U7879.001.DQD014E-P1-C4	PCI-X capable, 64 bit, 133MHz slot	Empty
U7879.001.DQD014E-P1-C5	PCI-X capable, 64 bit, 133MHz slot	Empty

Escriba el siguiente comando para mostrar todas las ranuras de conexión en caliente PCI ocupadas:

```
# lsslot -c pci -o
```

El resultado será similar al ejemplo siguiente.

# Slot	Description	Device(s)
U7879.001.DQD014E-P1-C2	PCI-X capable, 64 bit, 133MHz slot	0002:58:01.0
U7879.001.DQD014E-P1-C3	PCI-X capable, 64 bit, 133MHz slot	0001:40:01.0
U7879.001.DQD014E-P1-C6	PCI-X capable, 64 bit, 133MHz slot	0001:58:01.0

Para ver información detallada sobre un dispositivo de conexión en caliente PCI, complete los pasos siguientes.

1. Seleccione un número de dispositivo en el resultado de `# lsslot -c pci -o`, como se indica en el ejemplo de resultado anterior.
2. Escriba el siguiente comando para mostrar información detallada sobre el dispositivo:

```
# lspci | grep xxx:yy:zz.t
```

donde *xxx:yy:zz.t* es el número del dispositivo de conexión en caliente PCI. El resultado será similar al ejemplo siguiente.

```
0001:40:01.0 Ethernet controller: Intel Corp. 82545EM Gigabit  
Ethernet Controller (Copper) (rev 01)
```

Sustitución de un HBA de conexión en caliente PCI

Complete los siguientes procedimientos para sustituir un HBA de conexión en caliente PCI utilizando el comando `drslot_chrp_pci`.

Atención: Antes de retirar el HBA, debe desconectar el cable de canal de fibra conectado al mismo. El cable de canal de fibra debe estar desconectado al menos 5 minutos para asegurarse de que toda la actividad de E/S se ha transferido a una ruta alternativa. Si no desconecta el cable de canal de fibra podrá observar resultados indeseados.

Nota: En estos procedimientos, la variable *slot-name* se refiere a la ranura que contiene el HBA que va a sustituir.

1. Escriba el siguiente comando para identificar la ranura de conexión en caliente PCI:

```
# drslot_chrp_pci -i -s slot-name
```

donde *slot-name* es el nombre de la ranura del HBA que va a sustituir, por ejemplo, U7879.001.DQD014E-P1-C3.

El LED de la ranura *slot-name* comenzará a parpadear y se mostrará el siguiente mensaje.

El indicador visual de la ranura PCI especificada se ha definido en estado de identificación. Pulse Intro para continuar o x para salir.

2. Realice la conexión en caliente o retire el HBA de la ranura:
 - a. Desconecte el cable de canal de fibra conectado al HBA y espere a que se complete la migración tras error.
 - b. Una vez finalizada la migración tras error, escriba el siguiente comando:

```
# drslot_chrp_pci -r -s slot-name
```

Se mostrará el siguiente mensaje.

El indicador visual de la ranura PCI especificada se ha definido en estado de identificación. Pulse Intro para continuar o x para salir.

- c. Pulse Intro. Se mostrará el siguiente mensaje.

El indicador visual de la ranura PCI especificada se ha definido en estado de acción.
Extraiga la tarjeta PCI de la ranura identificada y pulse Intro para continuar.
- d. Pulse Intro.
- e. Retire el HBA de la ranura físicamente.
- f. Escriba el siguiente comando para verificar si la ranura está vacía:

```
# lsslot -c pci -s slot-name
```

Si la ranura está vacía, el resultado será similar al ejemplo siguiente.

```
# Slot Description Device(s)
U7879.001.DQD014E-P1-C3 PCI-X capable, 64 bit, 133MHz slot Empty
```

3. Para conectar el HBA en la ranura, complete los pasos siguientes:
 - a. Escriba el siguiente comando:

```
# drslot_chrp_pci -a -s slot-name
```

Se mostrará el siguiente mensaje.

El indicador visual de la ranura PCI especificada se ha definido en estado de identificación. Pulse Intro para continuar o x para salir.

- b. Pulse Intro. Se mostrará el siguiente mensaje.

El indicador visual de la ranura PCI especificada se ha definido en estado de acción. Inserte la tarjeta PCI en la ranura identificada, conecte todos los dispositivos que desee configurar y pulse Intro para continuar. Escriba x para salir.

- c. Inserte el nuevo HBA en la ranura.

- d. Escriba el siguiente comando para verificar si la ranura ha dejado de estar vacía:

```
# lsslot -c pci -s slot-name
```

Si la ranura no está vacía, el resultado será similar al ejemplo siguiente.

```
# Slot Description Device(s)
U7879.001.DQD014E-P1-C3 PCI-X capable, 64 bit, 133MHz slot 0001:40:01.0
```

Correlación del nuevo WWPN con el subsistema de almacenamiento en AIX yLinux

Para cada subsistema de almacenamiento afectado por el intercambio en caliente, complete los pasos indicados a continuación para correlacionar el nombre de puerto de ámbito mundial (WWPN) del HBA con el subsistema de almacenamiento:

1. Inicie Storage Manager y abra la ventana Gestión del subsistema.
2. En la pestaña **Correlaciones** de la ventana Gestión del subsistema, pulse **Correlaciones > Mostrar toda la información de puerto de host**. Se abrirá la ventana Información de puerto de host.
3. Busque la entrada de la ventana Información de puerto de host que se adapta al WWPN del HBA *defectuoso* (el HBA que ha eliminado), y registre el nombre de alias. A continuación, cierre la ventana Información de puerto de host.
4. En la pestaña **Correlaciones**, seleccione el nombre de alias del puerto de host HBA que acaba de registrar.
5. Pulse **Correlaciones > Sustituir puerto de host**. Se abrirá la ventana Sustituir puerto de host.
6. En la ventana Sustituir puerto de host, compruebe si el identificador de puerto de host HBA, indicado en la parte superior de la ventana, coincide con el HBA que ha eliminado.
7. Escriba el WWPN de 16 dígitos, sin los dos puntos (:), del HBA de sustitución en el campo **Nuevo identificador** y pulse **Aceptar**.

Tras completar estos pasos, continúe con “Finalización del procedimiento de intercambio en caliente de HBA”.

Finalización del procedimiento de intercambio en caliente de HBA

Para finalizar el procedimiento de intercambio en caliente de HBA, complete el procedimiento aplicable de esta sección para AIX o Linux.

Finalización del procedimiento de intercambio en caliente de HBA en AIX

1. Elimine el enchufe de bucle de retorno de canal de fibra e inserte el cable de canal de fibra conectado anteriormente al HBA que ha retirado.

Nota: Salte el paso siguiente si el HBA está conectado directamente al subsistema de almacenamiento o si la distribución en zonas de conmutador de canal de fibra se basa en números de puerto en lugar de en WWPN. Si tiene que modificar la distribución en zonas, de no hacerlo correctamente el HBA no podrá acceder al subsistema de almacenamiento.

2. Si un HBA está conectado a un conmutador de canal de fibra y la distribución en zonas se basa en WWPN, modifique la información de distribución en zonas para sustituir el WWPN del anterior HBA por el WWPN del HBA de sustitución.
3. Elimine el enchufe de bucle de retorno de canal de fibra e inserte el cable de canal de fibra conectado anteriormente al HBA que ha retirado.

Nota: Salte el paso siguiente si el HBA está conectado directamente al subsistema de almacenamiento o si la distribución en zonas de conmutador de canal de fibra se basa en números de puerto en lugar de en WWPN. Si tiene que modificar la distribución en zonas, de no hacerlo correctamente el HBA no podrá acceder al subsistema de almacenamiento.

4. Si un HBA está conectado a un conmutador de canal de fibra y la distribución en zonas se basa en WWPN, modifique la información de distribución en zonas para sustituir el WWPN del anterior HBA por el WWPN del HBA de sustitución.
5. Ejecute el comando **cfgmgr** para habilitar el HBA y registrar su WWPN en el conmutador de canal de fibra.

6. Escriba los siguientes comandos para verificar que el dispositivo fcs X sustituido y sus dacs asociados se ponen en estado Disponible:

```
# lsdev -C |grep fcs
lsdev -C |grep dac
```

7. Escriba el siguiente comando para asegurarse de que no se han creado dars nuevos y que los dars previstos están en estado Disponible.

Nota: Con MPIO, el único momento en que tiene un dispositivo dac es cuando se asigna el UTM LUN.

```
# lsdev -C |grep dar
```

Atención: La presencia de dars adicionales en el resultado de `lsdev` indica un problema de configuración. Si esto ocurre, no continúe con este procedimiento hasta que corrija el problema. De lo contrario, podría perderse la disponibilidad de datos.

8. Para cada dar, escriba el comando siguiente con el fin de verificar si los atributos del dar afectado indican la presencia de dos dacs activos:

```
# lsattr -El darX|grep act_controller
```

donde X es el número del dar.

El resultado será similar al ejemplo siguiente:

```
lsattr -El dar0|grep act_controller
act_controller dac0,dac2 Active Controllers False
```

Atención: Si no se indican dos dacs para cada dar afectado, la disponibilidad de datos podría haberse perdido. No continúe con este procedimiento si no se indican dos dacs para cada dar. Soluciones el problema antes de continuar.

9. Redistribuya los volúmenes manualmente a sus rutas preferidas.
10. Compruebe que los discos se mantienen en la ruta preferida con uno o ambos de los métodos siguientes:

Utilizando el sistema AIX

Ejecute el comando `mpio_get_config -Av` y compruebe si las unidades están en la ruta esperada.

Utilizando Storage Manager

En la ventana Gestión empresarial, compruebe si los subsistemas de almacenamiento están en estado Óptimo. Si no se encuentran en estado Óptimo, asegúrese de que las unidades que forman parte de los subsistemas involucrados en el procedimiento de intercambio en caliente no se enumeran en el gurú de recuperación.

11. Si fuera necesario, habilite la recuperación automática de los dars afectados. Consulte Apéndice D, “Visualización y definición de atributos de gestor de datos de objeto (ODM) de AIX”, en la página 339 para saber cómo cambiar la configuración de atributos.

El intercambio en caliente del HBA de canal de fibra se ha completado.

Finalización del procedimiento de intercambio en caliente de HBA en Linux

1. Elimine el enchufe de bucle de retorno de canal de fibra e inserte el cable de canal de fibra conectado anteriormente al HBA que ha retirado.
2. Si un HBA está conectado a un conmutador de canal de fibra y la distribución en zonas se basa en WWPN, modifique la información de distribución en zonas para sustituir el WWPN del anterior HBA por el WWPN del HBA de sustitución.

Nota: Salte este paso si el HBA está conectado directamente al subsistema de almacenamiento o si la distribución en zonas de conmutador de canal de fibra se basa en números de puerto en lugar de en WWPN. Si tiene que modificar la distribución en zonas, de no hacerlo correctamente el HBA no podrá acceder al subsistema de almacenamiento.

3. Si RDAC está instalado, escriba el siguiente comando para reconocer el nuevo HBA:

```
# mppBusRescan
```

El intercambio en caliente del HBA de canal de fibra se ha completado.

Valores del DSM de Windows y el RDAC de Linux

Este tema se aplica a sistemas operativos tanto Windows como Linux. Los valores de configuración de la unidad de migración tras error facilitada con el IBM Storage Manager modifican el controlador.

- Para Linux, los valores de configuración están en el archivo `/etc/mpp.conf`.
- Para Windows, los valores de configuración están en la clave de registro `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\<DSM_Driver>\Parameters`, donde `<DSM_Driver>` es el nombre del controlador específico OEM.

El controlador de migración tras error predeterminado es `mpdsm.sys`. No obstante, para que se apliquen los cambios, debe reanunciar el host. Los valores predeterminados indicados en la siguiente tabla se aplican a sistemas operativos tanto Windows como Linux. Si los valores predeterminados son diferentes para Windows y Linux, se especificará. La mayoría de estos valores son sustituidos por el instalador de migración tras error para Linux o Windows.

Importante: Si cambia los valores configurados, podría perder acceso al subsistema de almacenamiento.

Tabla 32. Parámetros de configuración del controlador de migración tras error

Nombre del parámetro	Valor predeterminado	Descripción
MaxPathsPerController	4	<p>El número máximo de rutas (puntos finales lógicos) soportados por el controlador. El número total de rutas al subsistema de almacenamiento es el valor de MaxPathsPerController multiplicado por el número de controladores. Los valores permitidos van de 0x1 (1) a 0x20 (32) para sistemas operativos Windows y de 0x1 (1) a 0xFF (255) para RDAC Linux. Para uso únicamente por representantes de Soporte técnico y atención al cliente.</p>
ScanInterval	<p>1 (Windows) 60 (Linux)</p>	<p>El intervalo de tiempo, en segundos, que el controlador de migración tras error busca estas condiciones:</p> <ul style="list-style-type: none"> • Un cambio en la propiedad preferida de un LUN • Un intento de reequilibrar LUN a sus rutas preferidas • Un cambio en el estado de habilitación o inhabilitación de AVT <p>Para Windows, los valores permitidos se encuentran entre 0x1 y 0xFFFFFFFF y se deben especificar en minutos. Para Linux, los valores permitidos se encuentran entre 0x1 y 0xFFFFFFFF y se deben especificar en segundos. Para uso únicamente por representantes de Soporte técnico y atención al cliente.</p>

Tabla 32. Parámetros de configuración del controlador de migración tras error (continuación)

Nombre del parámetro	Valor predeterminado	Descripción
ErrorLevel	3	<p>Este valor determina los errores que se deben registrar. Son válidos los valores siguientes:</p> <ul style="list-style-type: none"> • 0 - Muestra todos los errores • 1 - Muestra los errores de migración tras error de ruta, errores de migración tras error de controlador, errores reintentables, errores fatales y errores recuperados • 2 - Muestra los errores de migración tras error de ruta, errores de migración tras error de controlador, errores reintentables y errores fatales • 3 - Muestra los errores de migración tras error de ruta, errores de migración tras error de controlados y errores fatales • 4 - Muestra los errores de migración tras error de controlados y errores fatales <p>Para uso únicamente por representantes de Soporte técnico y atención al cliente.</p>
SelectionTimeoutRetryCount	0	<p>El número de veces que se reintenta un tiempo de espera de selección para una solicitud de E/S antes de que falle la ruta. Si existe otra ruta al mismo controlador, la E/S se reintenta. Si no existe otra ruta al mismo controlador, se produce una migración tras error. Si no existen rutas válidas al controlador alternativo, la E/S falla. Los valores permitidos se encuentran entre 0x0 y 0xFFFFFFFF. Para uso únicamente por representantes de Soporte técnico y atención al cliente.</p>

Tabla 32. Parámetros de configuración del controlador de migración tras error (continuación)

Nombre del parámetro	Valor predeterminado	Descripción
CommandTimeoutRetryCount	1	El número de veces que se reintentará un tiempo de espera de comando para una solicitud de E/S antes de que falle la ruta. Si existe otra ruta al mismo controlador, la E/S se reintentará. Si no existe otra ruta al mismo controlador, se produce una migración tras error. Si no existen rutas válidas al controlador alternativo, la E/S falla. Los valores permitidos se encuentran entre 0x0 y 0xa (10) para Windows, y entre 0x0 y 0xFFFFFFFF para el RDAC de Linux. Para uso únicamente por representantes de Soporte técnico y atención al cliente.
UaRetryCount	10	El número de veces que se reintentará un estado Atención de unidad (UA) de un LUN. Este parámetro no se aplica a condiciones de UA debidas a la Inactividad en curso. Los valores permitidos se encuentran entre 0x0 y 0x64 (100) para Windows, y entre 0x0 y 0xFFFFFFFF para el RDAC de Linux. Para uso únicamente por representantes de Soporte técnico y atención al cliente.
SynchTimeout	120	El tiempo de espera, en segundos, para solicitudes de E/S síncronas generadas internamente por el controlador de migración tras error. Entre los ejemplos de solicitudes internas se incluyen las relacionadas con el reequilibrio, la validación de rutas y la emisión de comandos de migración tras error. Los valores permitidos se encuentran entre 0x1 y 0xFFFFFFFF. Para uso únicamente por representantes de Soporte técnico y atención al cliente.

Tabla 32. Parámetros de configuración del controlador de migración tras error (continuación)

Nombre del parámetro	Valor predeterminado	Descripción
DisableLunRebalance	0	<p>Este parámetro proporciona control sobre el comportamiento de restablecimiento de LUN al reequilibrar LUN a sus rutas preferidas. Son posibles los valores siguientes:</p> <ul style="list-style-type: none"> • 0 – El reequilibrio de LUN está habilitado para el modo AVT y no AVT. • 1 - El reequilibrio de LUN está inhabilitado para el modo AVT y habilitado para el modo no AVT. • 2 - El reequilibrio de LUN está habilitado para el modo AVT e inhabilitado para el modo no AVT. • 3 – El reequilibrio de LUN está inhabilitado para el modo AVT y no AVT. • 4 – La característica de transferencia selectiva de LUN se habilita si el modo AVT está desactivado y ClassicModeFailover está definido como LUN nivel 1.
S2ToS3Key	Clave exclusiva	<p>Este valor es la clave de reserva SCSI-3 generada durante la instalación del controlador de migración tras error. Para uso únicamente por representantes de Soporte técnico y atención al cliente.</p>
LoadBalancePolicy	1	<p>Este parámetro determina la política de equilibrio de carga utilizada por todas las unidades lógicas gestionadas por el controlador de migración tras error del DSM de Windows y el RDAC de Linux. Son válidos los valores siguientes:</p> <ul style="list-style-type: none"> • 0 – En rueda con el subconjunto. • 1 - Menor profundidad de cola con subconjunto. • 2 - Menor peso de ruta con subconjunto (sólo Windows)

Tabla 32. Parámetros de configuración del controlador de migración tras error (continuación)

Nombre del parámetro	Valor predeterminado	Descripción
ClassicModeFailover	0	Este parámetro proporciona control sobre cómo trata el DSM situaciones de migración tras error. Son válidos los valores siguientes: <ul style="list-style-type: none"> • 0 – Realiza la migración tras error a nivel del controlador (todos los LUN se mueven al controlador alternativo). • 1 – Realiza la migración tras error a nivel del LUN (solo se transfieren al controlador alternativo los LUN que indican errores).
SelectiveTransferMaxTransferAttempts	3	Este parámetro define el número máximo de veces que un host transfiere la propiedad de un LUN a un controlador alternativo cuando el modo Transferencia selectiva de LUN está habilitado. Este valor evita que diversos hosts transfieran LUN continuamente entre controladores.
SelectiveTransferMinIOWaitTime	5	Este parámetro define el tiempo de espera mínimo (en segundos) que un DSM espera hasta transferir la propiedad de un LUN a un controlador alternativo cuando el modo Transferencia selectiva de LUN está habilitado. Este parámetro se utiliza para limitar las transferencias de LUN excesivas debido a errores de conexión intermitentes.

Valores de tiempo de espera

Cuando un controlador de migración tras error recibe una solicitud de E/S por primera vez, este registra la información de indicación de fecha y hora de la solicitud. Si una solicitud devuelve un error y el controlador de migración tras error decide reintentar la solicitud, la hora actual se compara con la información de indicación de fecha y hora original. Dependiendo del error y la cantidad de tiempo que haya transcurrido, la solicitud se reintenta en el controlador propietario del LUN actual o se realiza la migración tras error y se envía la solicitud al controlador alternativo. Este proceso se conoce como tiempo de espera. Si el valor de `NotReadyWaitTime`, `BusyWaitTime` y `QuiescenceWaitTime` son superiores al valor de `ControllerIOWaitTime`, no tendrán efecto.

Tabla 33. Parámetros de los valores de tiempo de espera

Nombre del parámetro	Valor predeterminado	Descripción
NotReadyWaitTime	300 (Windows), 270 (Linux)	El tiempo, en segundos, que se permite una condición No listo (SK 0x06, ASC/ASCQ 0x04/0x01) antes de realizar la migración tras error. Los valores permitidos se encuentran entre 0x1 y 0xFFFFFFFF.
BusyWaitTime	600 (Windows) 270 (Linux)	El tiempo, en segundos, que se permite una condición Ocupado antes de realizar la migración tras error. Los valores permitidos se encuentran entre 0x1 y 0xFFFFFFFF.
QuiescenceWaitTime	600 (Windows) 270 (Linux)	La hora, en segundos, se permite una condición de Latencia antes de realizar la migración tras error. Los valores permitidos se encuentran entre 0x1 y 0xFFFFFFFF.
ControllerIoWaitTime	600 (Windows) 120 (Linux)	Proporciona un límite superior, en segundos, de reintento de una solicitud en un controlador independientemente del estado de reintento antes de que se lleve a cabo la migración tras error. Si se supera el límite en el controlador alternativo, la E/S se intenta de nuevo en el controlador original. Este proceso continúa hasta que se alcanza el valor del límite ArrayIoWaitTime. Los valores permitidos se encuentran entre 0x1 y 0xFFFFFFFF.
ArrayIoWaitTime	600	Proporciona un límite superior, en segundos, de reintento de una solicitud en un subsistema de almacenamiento independientemente del controlador en el que se intente la solicitud. Una vez superado este límite, la E/S se devuelve con un estado de error. Los valores permitidos se encuentran entre 0x1 y 0xFFFFFFFF.

Valores de configuración para la detección de congestión de ruta y los estados de ruta en línea/fuera de línea

Los siguientes valores de configuración se aplican utilizando el parámetro `dsMUtil-0`.

Tabla 34. Valores de configuración para la detección de congestión de ruta

Parámetro	Valor predeterminado	Descripción
<code>CongestionDetectionEnabled</code>	0x0	Un valor booleano que indica si la detección de la congestión de ruta está habilitada. Si este parámetro no se define o se establece como 0x0, el valor es falso, la característica de la congestión de ruta se deshabilita y todos los demás parámetros se pasan por alto. Si se define como 0x1, se habilita la característica de congestión de ruta. Los valores válidos son 0x0 o 0x1.
<code>CongestionResponseTime</code>	0x0	Si <code>CongestionIoCount</code> es 0x0 o no se define, este parámetro representa un tiempo de respuesta medio en segundos permitido para una solicitud de E/S. Si el valor del parámetro <code>CongestionIoCount</code> no es cero, será el tiempo absoluto permitido para una solicitud de E/S. Los valores válidos se encuentran entre 0x1 y 0x10000 (aproximadamente 18 horas).
<code>CongestionIoCount</code>	0x0	El número de solicitudes de E/S que ha superado el valor del parámetro <code>CongestionResponseTime</code> dentro del valor del parámetro <code>CongestionTimeFrame</code> . Los valores válidos se encuentran entre 0x0 y 0x10000 (aproximadamente 4000 solicitudes).

Tabla 34. Valores de configuración para la detección de congestión de ruta (continuación)

Parámetro	Valor predeterminado	Descripción
CongestionTimeFrame	0x0	Una ventana deslizante que define el período de tiempo que se evalúa en segundos. Si este parámetro no se define o se establece como 0x0, la característica de congestión de ruta se deshabilita porque no se ha definido ningún marco de tiempo. Los valores válidos se encuentran entre 0x1 y 0x1C20 (aproximadamente dos horas).
CongestionSamplingInterval	0x0	El número de solicitudes de E/S que deben ser enviados a una ruta antes de que la solicitud n se utilice en el cálculo del tiempo de respuesta medio. Por ejemplo, si este parámetro se establece en 100, cada solicitud 100 enviado a una ruta se utiliza en el cálculo del tiempo de respuesta medio. Si este parámetro no se define o se establece como 0x0, la característica de congestión de ruta se deshabilita por motivos de rendimiento y cada solicitud de E/S se incluye en el cálculo. Los valores válidos se encuentran entre 0x1 y 0xFFFFFFFF (aproximadamente 4 billones de solicitudes).
CongestionMinPopulationSize	0x0	El número de solicitudes de E/S de muestra que deben recopilarse para que se calcule el tiempo de respuesta medio. Los valores válidos se encuentran entre 0x1 y 0xFFFFFFFF (aproximadamente 4 billones de solicitudes).

Tabla 34. Valores de configuración para la detección de congestión de ruta (continuación)

Parámetro	Valor predeterminado	Descripción
CongestionTakeLastPathOffline	0x0	Un valor booleano que indica si el controlador de DSM toma la última ruta disponible hacia el subsistema de almacenamiento fuera de línea en caso de que se superen los umbrales de la congestión. Si este parámetro no se define o se establece como 0x0, el valor es falso. Los valores válidos son 0x0 o 0x1. Nota: El establecimiento de una ruta fuera de línea con el programa de utilidad <code>dsmUtil</code> se realiza correctamente independientemente del ajuste de este valor.

Ejemplo de valores de configuración para la detección de congestión de ruta

Aquí aparece una sección breve de ejemplo en un concepto.

Nota: Antes de la detección de la congestión de ruta puede habilitarse, debe definir los parámetros `CongestionResponseTime`, `CongestionTimeFrame`, y `CongestionSamplingInterval` con valores válidos.

Para definir el tiempo de respuesta de ES de congestión de ruta en 10 segundos:
`dsmUtil -o CongestionResponseTime=10,SaveSettings`

Para definir el intervalo de muestreo de congestión de ruta en un minuto: `dsmUtil -o CongestionSamplingInterval=60`

Para habilitar la detección de la congestión de ruta: `dsmUtil -o CongestionDetectionEnabled=0x1,SaveSettings`

Para utilizar el comando `dsmUtil -o` y definir una ruta fuera de línea al administrador: `dsmUtil -o SetPathOffline=0x77070001`

Para utilizar el comando `dsmUtil -o` y definir una ruta en línea: `dsmUtil -o SetPathOnline=0x77070001`

Nota: El identificador de ruta (en este ejemplo 0x77070001) se encuentra utilizando el comando `dsmUtil -g`.

Configuración de detalles en el sistema de almacenamiento DS5000 y el host AIX para soportar T10PI

Debe configurar su sistema de almacenamiento DS5000 y host AIX para soportar la funcionalidad T10PI desde el host AIX hasta las unidades del subsistema de almacenamiento DS5000 utilizando los pasos indicados a continuación.

Configuración del cajón de almacenamiento DS5K

1. Actualiza el sistema de almacenamiento DS5000 con el firmware que soporta T10PI.
2. Cree y exporte número de unidad lógica (LUN) que soporten T10PI.

Nota: Para llevar a cabo este paso, debe tener discos que soporten T10PI. Por lo general estos discos se preinicializan como bloques de 520 bytes. Consulte "Atributos de unidades con capacidad T10PI" en la página 71 para obtener más información.

Configuración del host AIX

Nota: Debe utilizar SSIC para buscar HBA, controladores de HBA y versiones de firmware soportadas, así como su sistema operativo AIX, junto con los parches aplicables.

1. Instale el AIX 61 TL6 SP5 o AIX 71 TL0 SP3. La máquina AIX debe tener al menos un adaptador FC PCIe de 8Gb (código de característica 5735 o 5273) con el firmware más reciente que soporte T10PI. Debe tener al menos la versión df1000f114108a03.200305. Puede utilizar el programa de utilidad AIX diag para descargar el firmware del adaptador FC PCIe de 8Gb (código de característica 5735 o 5273).
 - Debe utilizar el adaptador de canal de fibra PCIe de 8Gb de dos puertos.
 - Se necesita el nivel 200307 o superior de firmware.
 - Código de característica 5735 o código de bajo perfil 5273 necesario.
 - No se soporta en Power Blades.
 - Para descargar el firmware del adaptador, utilice el comando **diag -T download -d fcs#**, donde # es el número de dispositivo fcs
 - Para encontrar la versión de firmware actual en el adaptador Coho, utilice los comandos **lsmcode -cd fcs#** o **lscfg -vl fcs#**
2. Habilite la protección en el adaptador FC PCIe de 8Gb (código de característica 5735 o 5273) (atributo DIF_enabled del dispositivo fcs).
 - Para habilitar la protección en el adaptador de FC, utilice el comando **chdev -l fcs# -a DIF_enabled=yes**.
 - También puede utilizar el comando **smit fcsa** para habilitar/inhabilitar la protección en fcs#

Nota: Para inhabilitar la protección en el adaptador de FC, utilice el comando **chdev -l fcs# -a DIF_enabled=no**.

3. Asegúrese de que actualiza el firmware como se especifica en el paso 1 y lleve a cabo el paso 2 en todos los adaptadores FC PCIe de 8Gb (código de característica 5735 o 5273) para los que el disco tenga rutas.
 - a. Utilice el comando **lspath -l hdisk#** para buscar los adaptadores de FC que se encuentran en las rutas de un disco. Así se mostrarán los dispositivos fcsi# (dispositivos de protocolo FC).

- b. Utilice el comando `lsdev -l fscsi# -F'name parent'` para buscar al padre de un dispositivo fscsi#.
 - c. Habilite la protección.
4. Utilice el comando `chdev -l hdisk# -a DIF_protection=yes` para habilitar la protección T10 en un disco. El disco debe soportar la protección "Type 1" T10.

Nota: También puede utilizar el comando `smit disk` para habilitar/inhabilitar la protección en hdisk#.

Nota: Utilice el comando `chdev -l hdisk# -a DIF_protection=no` para inhabilitar la protección T10 en un disco.

5. Utilice el comando `lsattr -El hdisk#` para comprobar el valor actual de este atributo tras habilitar la protección. Si al menos una ruta no soporta la protección, esta no podrá habilitarse en el disco. Si este atributo tiene valores "unsupported," significa que:
 - alguna de las rutas al disco no soporta la protección O
 - el disco no soporta la protección

hdisk2 tiene tres rutas. Estas tres rutas son fcs0, fcs2 y fcs3. Desea habilitar la protección en estos adaptadores. Para hacerlo:

1. Actualice el firmware de todos los dispositivos fcs mencionados anteriormente. Todos ellos debe ser adaptadores FC PCIe de 8Gb (código de característica 5735 o 5273).
2. Desconfigure los dispositivos hijo (fscsi0, fscsi2 y fscsi3).
3. Habilite la protección en los adaptadores fcs0, fcs2 y fcs3 utilizando el comando `chdev (chdev -l fcs0 -a DIF_enabled=yes)`.
4. Ejecute `cfgmgr` para que todos los dispositivos pasen a estado disponible.
5. Utilice el comando `chdev` en el hdisk2 para habilitar o inhabilitar la protección (`chdev -l hdisk2 -a DIF_protection=yes`). Si el disco y todas las rutas soportan la protección, el valor del atributo será "yes". De lo contrario será "unsupported".

Nota: Si el valor del atributo es "unsupported", compruebe todas las rutas (todos los atributos del adaptador fcs) y verifique si la protección se habilitó en el LUN al crearlo en el almacenamiento DS5000. En algunos casos, el atributo del adaptador fcs puede indicar "yes" pero no estar soportado por contar con un firmware de adaptador FC PCIe de 8Gb (código de característica 5735 o 5273) antiguo que no soporta la protección T10 (característica BlockGuard).

Capítulo 6. Trabajo con el Cifrado de disco completo

Este capítulo describe las prestaciones y ventajas del cifrado de disco completo (FDE) y cómo implementar la seguridad en los subsistemas de almacenamiento compatibles con FDE equipados con discos FDE.

Además de la información de este capítulo, el documento *IBM Full Disk Encryption Best Practices* describe las prácticas más adecuadas para mantener la seguridad en un subsistema de almacenamiento equipado con unidades FDE. Para acceder a este documento, vaya a <http://www-947.ibm.com/support/entry/portal/docdisplay?Indocid=MIGR-5081492&brandind=5000028>, o complete los pasos siguientes:

1. Vaya al Portal de soporte de IBM en <http://www.ibm.com/support/entry/portal>.
2. En el campo **Buscar en todo el soporte y descargas** de la parte inferior de la página, escriba FDE y pulse Intro.
3. En la lista de resultados de la búsqueda, pulse el enlace **IBM Full Disk Encryption Best Practices - IBM System Storage**.
4. Pulse en el enlace del archivo de FDE para abrir o descargar el documento *IBM Full Disk Encryption Best Practices*.

Nota: También puede asegurar una agrupación de discos si cuenta con discos FDE. Consulte “Seguridad de una matriz RAID” en la página 250. El procedimiento es exactamente el mismo.

Nota: Las capturas de pantalla de esta sección son solo ilustrativas y pueden diferir de la interfaz de usuario real dependiendo de la versión de Storage Manager y del firmware del controlador.

En este capítulo se incluyen los temas siguientes:

- “Cifrado de disco completo” en la página 216
 1. “Protección de datos contra infracción” en la página 216
 2. “Elección de la gestión de claves de seguridad externa o local” en la página 217
 3. “Antes de empezar” en la página 234
 4. “Uso de claves de seguridad” en la página 219
 5. “Uso de borrado seguro” en la página 230
 6. “Autorizaciones de seguridad FDE” en la página 231
 7. “Terminología de FDE” en la página 233
- “Instalación y configuración del servidor DS TKLM Proxy Code” en la página 235
 1. “Modificación del archivo de configuración de servidor de código proxy de DS TKLM” en la página 236
 2. “Instalación de DS TKLM Proxy Code” en la página 240
- “Configuración de cifrado de disco con unidades FDE” en la página 242
 1. “Instalación de unidades FDE” en la página 242
 2. “Habilitación de características premium” en la página 242
 3. “Seguridad de una matriz RAID” en la página 250
 4. “Desbloqueo de unidades de disco” en la página 256

5. "Migración de subsistemas de almacenamiento (intercambio de cabezal) con unidades FDE" en la página 259
 6. "Borrado de unidades de disco" en la página 263
 7. "Unidades de disco de reserva activo globales" en la página 266
 8. "Archivos de registro" en la página 267
- "Preguntas frecuentes" en la página 267

Nota: No todos los subsistemas de almacenamiento IBM DS soportan FDE. Consulte la documentación facilitada con su subsistema de almacenamiento para obtener más información sobre compatibilidad de FDE.

Cifrado de disco completo

La información de esta sección ofrece una visión general de cómo funciona el FDE. Las secciones siguientes de este capítulo describen cómo configurar el cifrado de disco utilizando la gestión de claves de seguridad interna y externa.

El uso de cifrado de disco completo (FDE) protege los datos contra amenazas cuando una unidad FDE está fuera del control de su propietario. Las unidades FDE no protegen los datos contra las amenazas que se producen en el centro de datos o en la red. Si un atacante obtiene acceso a un servidor y puede acceder a una unidad desbloqueada, el atacante puede leer el texto simple que proviene de la unidad. Recuerde que la tecnología de cifrado a nivel de unidad no sustituye a los controles de acceso del centro de datos, sino que los complementa.

Las unidades de cifrado de disco completo (FDE) le permiten reducir las vulnerabilidades de seguridad de los datos almacenados. Las unidades de disco FDE que se adhieren a la especificación de clase de subsistema de seguridad empresarial Trusted Storage Group (TCG) están cualificados por la Agencia de Seguridad Nacional y proporcionan seguridad mediante cifrado de nivel gubernamental.

Nota: Ninguna implementación de seguridad individual puede asegurar de manera eficaz todos los niveles de datos de todas las amenazas.

Se requieren tecnologías diferentes para proteger los datos almacenados en unidades de disco duro de las distintas amenazas. Las unidades FDE protegen la seguridad de los datos almacenados a través de los métodos siguientes:

Protección de datos contra infracción

Si un usuario no autorizado se hace con una unidad de disco que contenga datos cifrados, la unidad se retira del centro de datos o se corta la alimentación, los datos permanecerán protegidos.

Uso de borrado seguro

El borrado seguro proporciona un borrado permanente y rápido de los datos de unidades que se van a reutilizar o desechar.

Protección de datos contra infracción

Las unidades con tecnología de cifrado de disco completo tienen capacidad de seguridad. Todas las unidades FDE se entregan de fábrica con el estado Con capacidad de seguridad (seguridad inhabilitada). En este estado, las unidades FDE se comportan exactamente como unidades no FDE. Los datos almacenados en las mismas no están protegidos cuando las unidades se retiran del subsistema de almacenamiento. Puede moverlas de un subsistema de almacenamiento a otro sin

desbloquearlas con un archivo de claves de seguridad. También se pueden utilizar como parte de una matriz RAID compuesta de discos sin cifrado (no FDE). No obstante, una matriz RAID compuesta de unidades no FDE y FDE con capacidad de seguridad no se puede convertir en matriz RAID asegurada más adelante, por lo que los datos de las unidades FDE quedan desprotegidos si estas se retiran del subsistema de almacenamiento.

Los controladores de subsistemas de almacenamiento IBM pueden aplicar seguridad a cualquier unidad FDE de una matriz RAID compuesta totalmente por unidades FDE. Dependiendo del método de gestión de claves de seguridad utilizado (local o externo), el firmware del controlador crea una clave de seguridad u obtiene una clave de seguridad del gestor de claves externo, por ejemplo el software IBM Tivoli Key Lifecycle Manager. Una vez que el firmware tiene la clave de seguridad, activa la función de cifrado de la unidad, que hace que todas las unidades de disco FDE generen una clave de cifrado aleatoria incluida en el disco.

Cuando se habilita la seguridad, la unidad FDE ejecuta automáticamente el cifrado de disco completo para realizar operaciones de lectura y escritura. Cuando se lleva a cabo una operación de escritura, se incluye texto simple en el disco y este se cifra antes de escribirlo en el soporte utilizando la clave de cifrado de disco. Cuando se realiza una operación de lectura, se descifran los datos cifrados que se leen en el soporte antes de que abandonen la unidad.

Durante la operación normal, la unidad FDE está en estado Con capacidad de seguridad o Seguridad habilitada, y se comporta igual que un disco sin cifrado del subsistema de almacenamiento. Las unidades FDE con seguridad habilitada están cifrando datos constantemente. El cifrado de disco no se puede apagar accidentalmente. La propia unidad genera la clave de cifrado de disco, que se almacena en el disco, nunca sale de él y es única para una sola unidad. Para asegurarse de que la seguridad nunca se ve comprometida, solo se guarda una versión cifrada de la clave de cifrado en la unidad de disco. Dado que la clave de cifrado de disco nunca sale del disco, no tendrá que cambiarla periódicamente como debe hacer con las contraseñas de su sistema operativo.

Elección de la gestión de claves de seguridad externa o local

Existen dos métodos para gestionar las claves de seguridad de su subsistema de almacenamiento: la gestión local y la gestión externa.

Gestión local de claves de seguridad

Con la gestión local de las claves de seguridad, la clave se crea y almacena en el controlador del subsistema de almacenamiento. La gestión de claves local no requiere software adicional. Para mover las unidades aseguradas de un subsistema de almacenamiento a otro, debe utilizar el archivo de claves de seguridad guardado desde el subsistema de almacenamiento original con el fin de desbloquear las unidades.

Para habilitar la gestión local de claves de seguridad, complete las tareas siguientes:

1. Siga las instrucciones de activación web de características premium FDE.
2. Utilice Storage Manager para encargar al controlador del subsistema de almacenamiento que cree la clave de seguridad.

Gestión externa de claves de seguridad

En lugar de utilizar la clave de seguridad creada por el controlador del subsistema de almacenamiento, la gestión externa utiliza una ubicación de claves central de su red para gestionar las claves para diferentes subsistemas de almacenamiento. La gestión externa de claves de seguridad se realiza mediante un software de gestión de licencias de claves externo como IBM Tivoli Key Lifecycle Manager (TKLM). Si aún no tiene este software, debe adquirirlo, instalarlo y configurar el servidor proxy.

Con la gestión externa de claves de seguridad, los controladores obtienen la clave de seguridad de un origen de gestión de claves externo. A continuación, esta clave se oculta en la memoria volátil del controlador para su uso en el futuro, durante el tiempo que el subsistema de almacenamiento permanezca encendido. Esta clave se borra de la memoria volátil cuando se apaga el subsistema de almacenamiento. Dado que la clave no se almacena en el subsistema de almacenamiento, este debe tener una unidad no FDE en la configuración para arrancar correctamente; a continuación solicita la clave de seguridad al servidor de gestión de claves externo para desbloquear las unidades FDE.

Este método proporciona una interfaz de gestión de claves común y coherente; el software de gestión de licencias de claves externo también gestiona las claves de seguridad de otros hardware de almacenamiento, como unidades de cintas aseguradas. Para mover unidades de un subsistema de almacenamiento a otro no tiene que acceder al archivo de claves de seguridad guardado. En vez de eso, el software de gestión de licencias de claves proporciona la clave de seguridad que desbloquea las unidades automáticamente si el segundo subsistema de almacenamiento se conecta a dicho software de gestión cuando se insertan las unidades.

Para habilitar la gestión externa de claves de seguridad, complete las tareas siguientes:

1. Instale y configure el software de gestión externa de claves de seguridad. Consulte la documentación facilitada con el software para más información.
2. Instale y configure DS TKLM Proxy Code.
3. Configure el software de gestión externa de claves de seguridad para recibir una solicitud de claves externa.
4. Utilice Storage Manager para encargar al controlador del subsistema de almacenamiento solicitar la clave de seguridad al gestor de licencias de claves externo, en vez de generar una clave de seguridad local.
5. Configure el software de gestión externa de claves de seguridad para aceptar una solicitud de claves externa.

Importante:

1. Tivoli Key Lifecycle Manager es el único software de gestión externa de claves de seguridad soportado en subsistemas de almacenamiento IBM DS.
2. Asegúrese de que al menos una unidad no FDE está instalada en el subsistema de almacenamiento cuando utilice la gestión de claves externa. De lo contrario, si se desconecta y se vuelve a conectar la alimentación del subsistema de almacenamiento, podría tener que facilitar la clave de seguridad del archivo guardado manualmente para desbloquear las unidades FDE aseguradas y completar el proceso de arranque.

Uso de claves de seguridad

Con cifrado de disco completo, el proceso para asegurar una unidad consiste en habilitar la seguridad en el subsistema de almacenamiento y después asegurar las matrices RAID con seguridad donde se almacenan los datos.

El proceso para generar una clave de seguridad depende del tipo de método de gestión de la seguridad de gestión que utilice. Habilitar la seguridad en el subsistema de almacenamiento es un proceso que se realiza una sola vez, a menos que en adelante decida cambiar la clave de seguridad o el método de gestión de claves. No se necesitan claves diferentes para cada unidad, aunque cada unidad FDE tiene su propia clave de cifrado única. Para habilitar la seguridad en un subsistema de almacenamiento, debe adquirir las opciones para unidades FDE una clave para la característica de cifrado de discos IBM DS, además de habilitar la característica en el subsistema de almacenamiento utilizando las instrucciones facilitadas con el kit de titularidad de la misma.

Una vez que los controladores crean la clave de seguridad, o de que obtiene esta con el software de gestión de claves externo, una versión cifrada de la clave de seguridad se creará en el subsistema de almacenamiento y esta no podrá verse directamente.

Tras crear la clave de seguridad en el subsistema de almacenamiento, se le pedirá que guarde la versión cifrada de la clave de seguridad en una copia de un archivo de claves de seguridad en una ubicación específica. Asegúrese de proteger el archivo de claves de seguridad y su frase de contraseña asociada. Además de en la ubicación especificada, el gestor de almacenamiento guardará también una copia del archivo en la ubicación predeterminada `... \IBM_DS\client\data\securityLockKey` para entornos Microsoft Windows o en `/var/opt/SM/securitylockkey` para entornos AIX, Linux, Solaris y HP-UX.

Con el método de gestión de claves de seguridad local, se le pedirá el identificador de clave de seguridad y la frase de contraseña. Este identificador de clave de seguridad se facilita con el identificador mundial del subsistema de almacenamiento para ayudarlo a identificar el subsistema de almacenamiento con el que está asociado la clave de seguridad. Con el método de gestión de claves de seguridad externo, se le pedirá solo la frase de contraseña. El controlador utiliza el identificador mundial del subsistema de almacenamiento para identificar el subsistema de almacenamiento con el que está asociado el archivo de claves de seguridad.

El archivo de claves de seguridad contiene la clave de seguridad cifrada y el identificador de la clave de seguridad. Debe proporcionar la frase de contraseña cuando guarde la clave de seguridad. La frase de contraseña no se almacena en ninguna parte del subsistema de almacenamiento o del archivo de claves de seguridad. El controlador utiliza la frase de contraseña para cifrar la clave de seguridad antes de exportarla al archivo de claves de seguridad. El identificador de claves de seguridad se almacena en el archivo de claves de seguridad para que pueda identificar el subsistema de almacenamiento con el que está asociado el archivo de claves de seguridad. Asegúrese de proteger el archivo de claves de seguridad y su frase de contraseña asociada, ya que podrá utilizarlas para desbloquear unidades FDE aseguradas.>

Para descifrar la clave de seguridad en el archivo de claves, debe facilitar la misma frase de contraseña que se utilizó al generar dicho archivo. A continuación, la

unidad determina si la clave de seguridad y la facilitada por el subsistema de almacenamiento son la misma. De ser así, pueden leerse y escribirse datos en las unidades FDE con seguridad.

Atención: La frase de contraseña solo se utiliza para proteger la clave de seguridad en el archivo de claves de seguridad. Cualquiera que pueda acceder a la ventana Gestión del subsistema, puede guardar una copia del archivo de claves de seguridad con una nueva frase de contraseña. Defina una contraseña para cada subsistema de almacenamiento que requiera la provisión de contraseña cuando se realizan cambios en la configuración, incluyendo la creación y la modificación de claves de seguridad. Consulte “Definición de una contraseña de gestión del subsistema de almacenamiento” en la página 43 para obtener instrucciones sobre la definición de contraseñas de subsistema de almacenamiento.

Si utiliza la gestión local de claves de seguridad, el archivo de claves de seguridad le ofrece protección contra claves corruptas o errores en ambos controladores del subsistema de almacenamiento. El archivo de claves de seguridad también es necesario para desbloquear unidades FDE con seguridad cuando estas se mueven de un subsistema a otro. En estos casos, las unidades FDE con seguridad permanecen bloqueadas hasta que la clave de seguridad almacenada en el archivo de claves desbloquea las unidades. Para descifrar la clave de seguridad en el archivo de claves, debe facilitar la misma frase de contraseña que se utilizó al generar dicho archivo. A continuación, la unidad determina si la clave de seguridad y la facilitada por el subsistema de almacenamiento son la misma. De ser así, pueden leerse y escribirse datos en las unidades FDE con seguridad.

Si utiliza la gestión externa de claves de seguridad, el archivo de claves de seguridad le ofrece protección en las siguientes situaciones:

1. Si se pierde la comunicación con el servidor proxy o los servidores de licencia de claves externos cuando el controlador desbloquea las unidades FDE aseguradas
2. Si las unidades FDE seguras se mueven de un subsistema de almacenamiento a otro no gestionado por el mismo gestor de licencias de claves externo
3. Si tuvieran que desbloquearse unidades tras el ciclo de alimentación de la configuración de un subsistema de almacenamiento que solo tenga unidades FDE con seguridad, ninguna unidad FDE sin seguridad ni unidad no FDE en la configuración

Una vez que el controlador del subsistema de almacenamiento crea la clave de seguridad, las matrices RAID se pueden cambiar del estado Con capacidad de seguridad al estado Seguridad habilitada. El estado Seguridad habilitada requiere el desbloqueo de las unidades FDE de la matriz RAID cuando se activa la alimentación de la unidad utilizando la clave de seguridad para acceder a los datos almacenados en las unidades. Siempre que llega alimentación a las unidades de una matriz RAID, todas las unidades pasan al estado Bloqueo de seguridad. Estas solo se desbloquean durante la inicialización de unidades con la clave de seguridad del subsistema de almacenamiento. El estado Desbloqueo de seguridad hace las unidades accesibles para las actividades de lectura y escritura. Una vez desbloqueadas, las unidades lo están hasta que se corta la alimentación, se retiran las unidades y se reinsertan en las bahías de unidad, o la alimentación del subsistema de almacenamiento cambia de ciclo.

Una vez asegurada una unidad, esta se bloquea si se corta la alimentación o es retirada. La clave de cifrado de la unidad no cifrará ni descifrá datos, por lo que

la unidad no puede leerse hasta ser desbloqueada por los controladores.

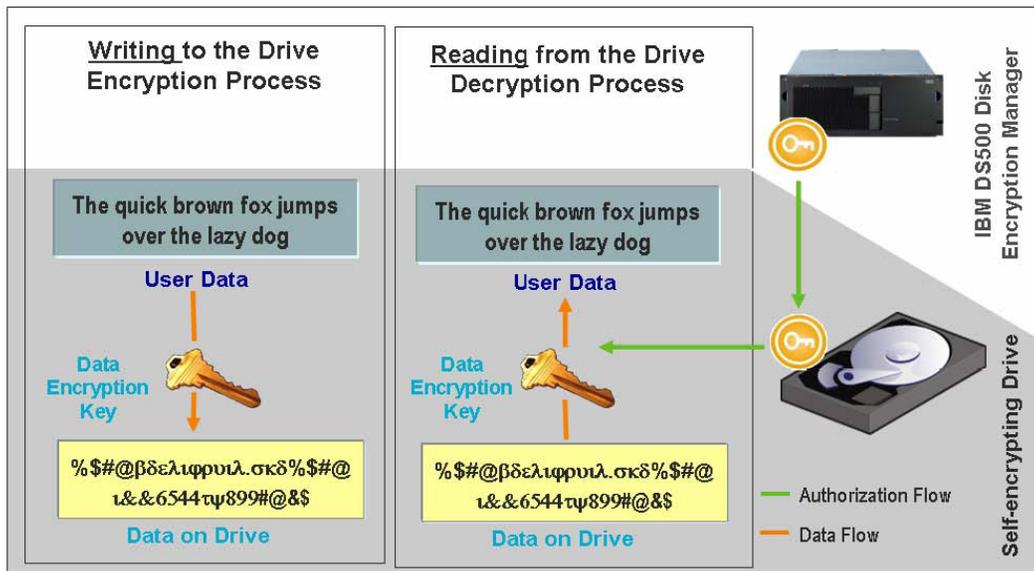


Figura 25. Unidades FDE con seguridad habilitada: Con las autorizaciones adecuadas, la lectura y escritura de datos se produce en estado Desbloqueado

Una vez que se establecen las autenticaciones y se habilita la seguridad en un subsistema de almacenamiento, el cifrado de las operaciones de escritura y descifrado de las operaciones de lectura que tienen lugar en el interior de la unidad FDE no están a la vista del usuario ni de los controladores del subsistema de almacenamiento DS5000. No obstante, si se pierde, elimina o roba una unidad asegurada, esta se bloquea y los datos almacenados en el disco permanecen cifrados e ilegibles. Dado que los usuarios no autorizados no cuentan con el archivo de claves de seguridad ni la frase de contraseña, acceder a los datos almacenados es imposible.

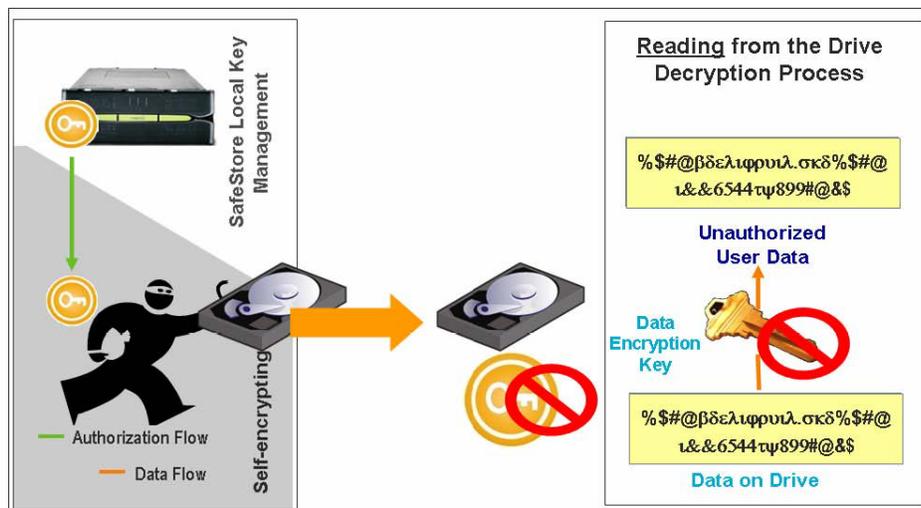


Figura 26. Eliminación de una unidad FDE con seguridad habilitada del subsistema de almacenamiento: Sin las autorizaciones adecuadas, un disco FDE robado no se puede desbloquear y los datos permanecen cifrados

Cambio de una clave de seguridad para la gestión local de claves de seguridad

El proceso para generar una clave de seguridad depende del tipo de método de gestión de la seguridad que utilice. La información de esta sección describe el cambio de una clave de seguridad en una configuración de gestión local de claves de seguridad.

Cuando cambia una clave de seguridad, el firmware de controlador del subsistema de almacenamiento genera una nueva clave de seguridad. La nueva clave de seguridad se oculta en el subsistema de almacenamiento y no podrá verla directamente. La nueva clave de seguridad sustituye a la clave anterior utilizada para desbloquear unidades FDE con seguridad habilitada en el subsistema de almacenamiento. El controlador negocia con todas las unidades FDE con seguridad habilitada la nueva clave.

Cuando cambiar una clave de seguridad, siempre se genera una copia de seguridad del archivo de claves, que debe guardarse también en otro soporte de almacenamiento por si el controlador fallara, o transferirse a otro subsistema de almacenamiento. Al cambiar la clave de seguridad, participa en la creación del identificador de la clave, la frase de contraseña y el nombre y ubicación del archivo de claves. La frase de contraseña no se almacena en ninguna parte del subsistema de almacenamiento o del archivo de claves de seguridad. El controlador utiliza la frase de contraseña para cifrar la clave de seguridad antes de exportarla al archivo de claves de seguridad.

Cambio de una clave de seguridad para la gestión externa de claves de seguridad

La información de esta sección describe el cambio de una clave de seguridad en una configuración de gestión externa de claves de seguridad.

Al cambiar la clave de seguridad, el controlador del subsistema de almacenamiento se pone en contacto con el gestor de licencias de claves externo para obtener una nueva clave de seguridad. A continuación, negocia la nueva clave de seguridad con las unidades de FDE con seguridad habilitada. La nueva clave no se oculta dentro del controlador. Se le pedirá que guarde la clave en un archivo de claves de seguridad. Para realizar una copia de la clave de seguridad se necesitan la frase de contraseña y el nombre y ubicación del archivo de claves de seguridad. La frase de contraseña no se almacena en ninguna parte del subsistema de almacenamiento o del archivo de claves de seguridad. El controlador utiliza la frase de contraseña para cifrar la clave de seguridad antes de exportarla al archivo de claves de seguridad.

Identificación del archivo de claves de seguridad por un subsistema de almacenamiento

Para mayor protección, la clave de seguridad utilizada para desbloquear unidades FDE no está visible para el usuario. El identificador de claves de seguridad le ayuda a identificar el archivo de claves de seguridad asociado con cada subsistema de almacenamiento. Con el método de gestión local de claves de seguridad, podrá proporcionar un valor de hasta 189 caracteres alfanuméricos. Este valor está vinculado con el identificador mundial del subsistema de almacenamiento y un número aleatorio que forman el identificador de claves de seguridad. Con el método de gestión externa de claves de seguridad, no se le pedirá que facilite un valor utilizado como parte del identificador de claves de seguridad. Puede ver el identificador de claves de seguridad durante las operaciones que necesitan el archivo de claves de seguridad de una unidad, como la creación o cambio de una clave de seguridad.

La Figura 27 muestra un ejemplo del campo del identificador de claves de seguridad al realizar una operación de cambio de clave.

Nota: Con la gestión externa de claves de seguridad, el usuario no puede modificar el identificador de claves de seguridad como ocurre con la gestión de claves local.

DS5KTop - Change Security Key

IBM

Security key identifier

The security key identifier is paired with the security key to help you remember which key to use for secured operations. The security key identifier can be left blank or you may type up to 189 alphanumeric characters. The system will add the storage subsystem world-wide identifier and a randomly generated number to what you type in the field. You will have the opportunity to record the final security key identifier later.

Security key identifier:

Passw0rdplus4

File save location

File name:

C:\Program Files\IBM_DS\client\data\securityLockKey\ Browse...

Pass phrase

The pass phrase is required to perform security operations. It must be between eight and thirty-two characters and contain at least one number, one lowercase letter, one uppercase letter, and one non-alphanumeric character (e.g., < > @ +). Spaces are not permitted, and it is case-sensitive.

Pass phrase:

Confirm pass phrase:

Change Key Cancel Help

Figura 27. Cambio de la clave de seguridad

La ventana Cambio de clave de seguridad completo muestra que el identificador de claves de seguridad escrito en el archivo de claves tiene un número aleatorio añadido al identificador que usted especificó en Figura 27 y al identificador

mundial del subsistema de almacenamiento. La Figura 28 muestra un ejemplo de la parte del número aleatoria del identificador de claves de seguridad.



Figura 28. Cambio de la clave de seguridad - Completo

El campo **Identificador de claves de seguridad** de la ventana Propiedades de unidad FDE incluye un número aleatorio generado por el controlador al crear o cambiar la clave de seguridad. La Figura 29 en la página 225 muestra un ejemplo del número aleatorio. El número aleatorio tiene actualmente el prefijo 27000000. Si todas las unidades FDE aseguradas del subsistema de almacenamiento tiene el mismo valor en el campo del identificador de claves de seguridad, podrán desbloquearse con el mismo identificador.

Nota: Los campos **Capacidad de seguridad** y **Asegurada** de la ventana Propiedades de la unidad muestran si la unidad tiene capacidad de seguridad y si está en estado Asegurado (Sí) o No asegurado (No).



Figura 29. Propiedades de la unidad - Unidad FDE asegurada

La Figura 30 en la página 227 muestra un ejemplo del identificador de claves de seguridad indicados en el campo **Información de archivo** al seleccionar una copia del archivo de claves de seguridad para desbloquear las unidades aseguradas del

subsistema de almacenamiento. El identificador de claves de seguridad o LockKeyID, mostrado en el campo Información de archivo, contiene los caracteres especificados en el campo del identificador al crear o cambiar la clave de seguridad unidos al identificador mundial del subsistema de almacenamiento y el número generado aleatoriamente que aparece en el identificador de claves de seguridad de todas las unidades FDE aseguradas. Esta información está delimitada por dos puntos (:). Por ejemplo:

```
Passw0rdplu3:600a0b800029ece6000000004a2d0880:600a0b800029ed8a00001aef4a2e4a73
```

Un LockKeyID contiene la siguiente información:

- El identificador de claves de seguridad especificado, por ejemplo Passw0rdplu3

Nota: Con la gestión externa de claves de seguridad, el usuario no puede modificar el identificador de claves de seguridad como ocurre con la gestión de claves local. Así, esta información no se mostrará.

- El identificador mundial del subsistema de almacenamiento, por ejemplo 600a0b800029ece6000000004a2d0880
- Un número generado aleatoriamente 600a0b800029ed8a00001aef4a2e4a73

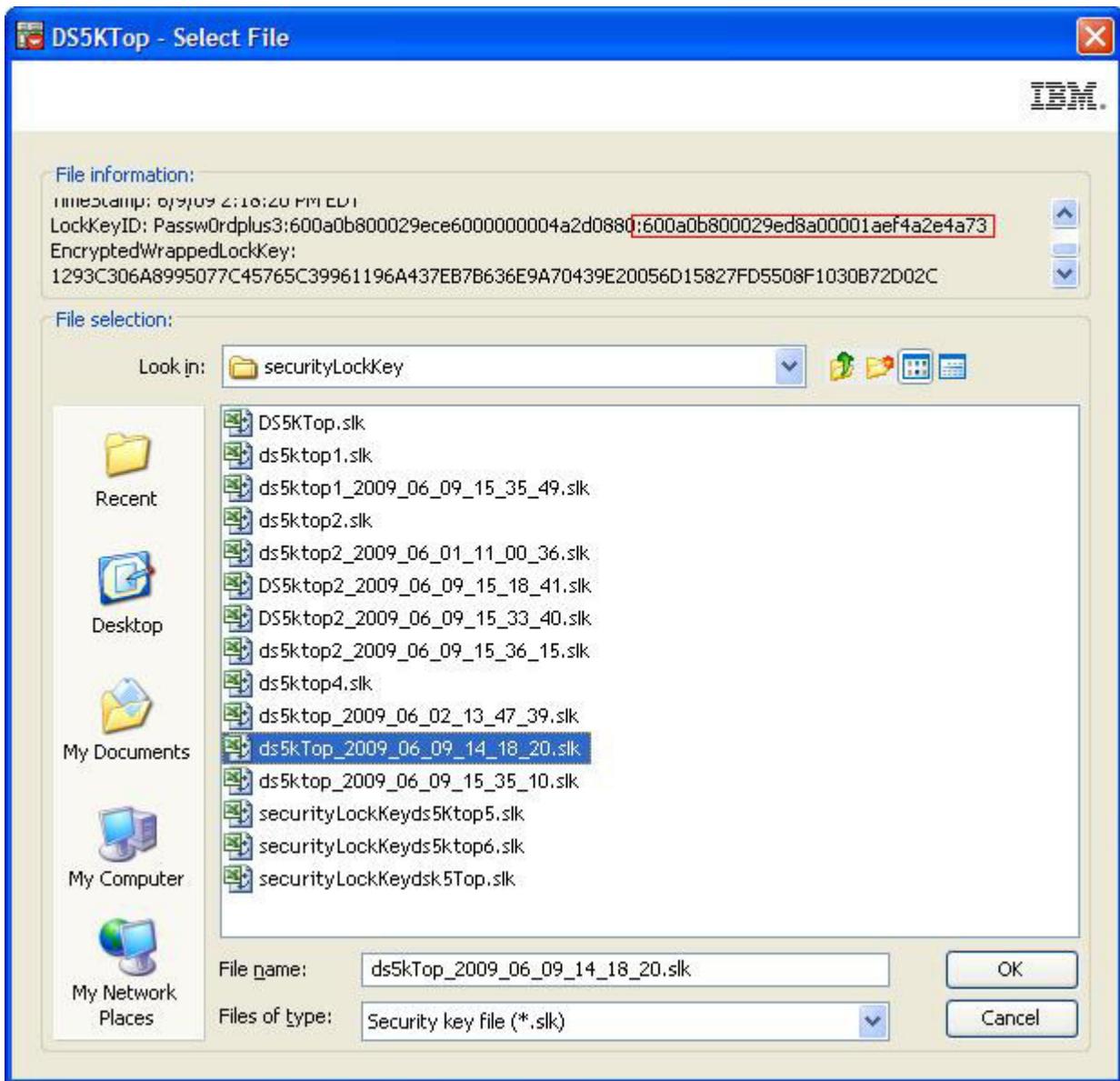


Figura 30. Seleccionar archivo - LockKeyID

La Figura 31 en la página 228 muestra un ejemplo de las propiedades de una unidad FDE no asegurada. Tenga en cuenta que en el campo del identificador de claves de seguridad de una unidad FDE no asegurado se incluyen ceros. Tenga en cuenta también que el valor del campo **Capacidad de seguridad** es sí y el de **Asegurada** es no, lo cual indica que se trata de una unidad FDE con capacidad de seguridad pero sin asegurar.

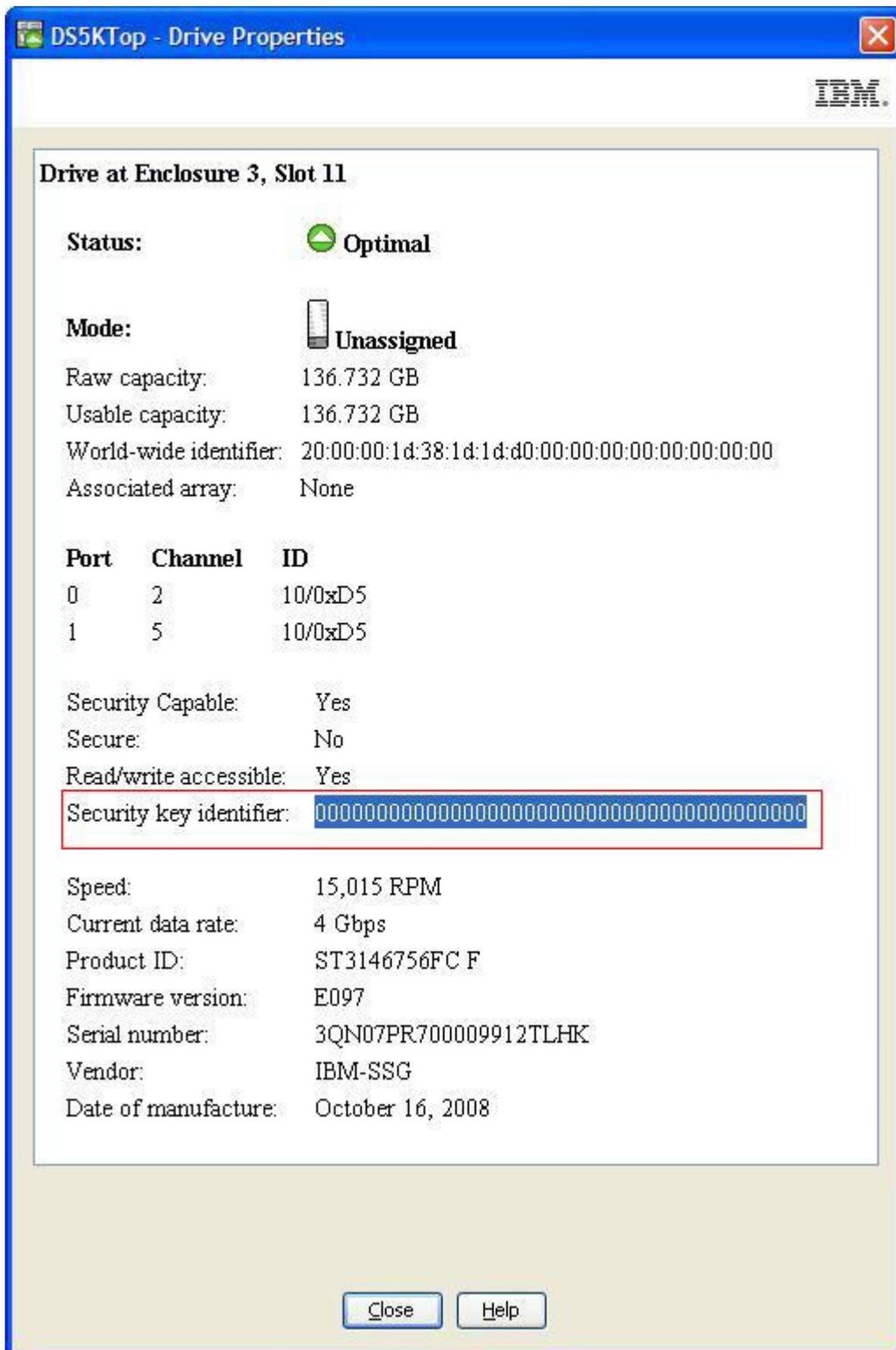


Figura 31. Propiedades de unidad - Unidad FDE no asegurada

Unlocking secure drives in local security key management mode

You can export a RAID array with its security-enabled FDE drives to a different storage subsystem. After you install those drives in the new storage subsystem,

you must unlock the security-enabled FDE drives before data can be read from or written to the drives. The security key on the new storage subsystem will be different and will not unlock the drives. You must supply the security key from a security key file that you saved from the original storage subsystem. In addition, you must provide the pass phrase that was used to encrypt the security key to extract the security key from the security key file. After you unlock the drives with the security key in the security key file, the controller negotiates the existing security key for these drives so that only one version of the security key is used to unlock drives in a storage subsystem.

You do not have to provide the security key file to unlock the security-enabled drives in a storage subsystem every time the storage subsystem power is cycled or the drives are removed and reinserted in the same storage subsystem, because the controllers always keep a copy of the current and previous ($n-1$) values of the security key to unlock these drives. However, if the drives are removed from the storage subsystem and the security key is changed more than two times in the same storage subsystem, the controllers will not have the security key to unlock the drives when they are reinserted in the same storage subsystem.

Atención: Always back up the data in the storage subsystem to secured tape to prevent loss of data due to malicious acts, natural disasters, abnormal hardware failures, or loss of the FDE security key.

Desbloqueo de las unidades seguras en modo de gestión externa de claves de seguridad

Puede exportar una matriz RAID con sus unidades de FDE con seguridad habilitada a un subsistema de almacenamiento diferente. Si las unidades se van a mover a otro subsistema gestionado por el mismo gestor de licencias de claves externo que el subsistema original, no tiene que proporcionar el archivo de claves de seguridad guardado para desbloquear las unidades.

Tras desbloquear las unidades con la clave de seguridad del archivo de claves de seguridad, el controlador negocia la clave de seguridad existente para esas unidades de forma que solo se utilice una versión de dicha clave para desbloquear las unidades de un subsistema de almacenamiento. De lo contrario, debe facilitar la clave de seguridad del archivo de claves de seguridad guardado en el subsistema de almacenamiento original. También debe proporcionar la frase de contraseña utilizada para cifrar la clave de seguridad para poder extraer dicha clave del archivo de claves de seguridad. Tras desbloquear las unidades con la clave de seguridad del archivo de claves de seguridad, el controlador negocia la clave de seguridad existente para esas unidades de forma que solo se utilice una versión de dicha clave para desbloquear las unidades de un subsistema de almacenamiento.

Nota: Debe exportar la matriz del subsistema original antes de mover las unidades de FDE; la matriz es necesaria para configurar las unidades para la supresión y actualizar la configuración del subsistema.

Si la configuración del subsistema no tiene unidades no aseguradas ni unidades no FDE, debe facilitar la clave de seguridad de un archivo de claves guardado en el subsistema de almacenamiento original al activar la alimentación al nuevo subsistema. Si la configuración del subsistema tiene unidades no aseguradas óptimas o unidades no FDE, el subsistema se lanzará y se conectará con el gestor de claves de seguridad externo para obtener la clave que desbloquea las unidades FDE aseguradas.

Atención: Realice siempre una copia de los datos del subsistema de almacenamiento en una cinta asegurada para evitar la pérdida de los mismos debido a actos maliciosos, catástrofes naturales, errores de hardware inusuales o pérdida de la clave de seguridad de FDE.

Uso de borrado seguro

El borrado seguro protege las unidades FDE ante amenazas de seguridad cuando eventualmente se retiran, vuelven a colocar, descartan o redefinen. Cuando se mueven estas unidades del centro de datos o reutilizan, es fundamental que los datos de los discos se borren de forma permanente y no puedan recuperarse. Las unidades descartadas pueden seguir teniendo datos residuales que pueden ser reconstruidos por un usuario no autorizado. El borrado seguro protege ante esta amenaza mediante el borrado criptográfico de los datos.

Los métodos tradicionales utilizados para borrar los datos de forma permanente han demostrado ser caros y lentos, y además pueden no ofrecer el mayor nivel posible de borrado de datos. Asimismo, los métodos tradicionales dejan las unidades fuera de su control por lo que los datos podrían sufrir violaciones. El borrado seguro proporciona las siguientes ventajas en comparación con los métodos tradicionales:

- Borrado de datos criptográfico inmediato
- Costes generales inferiores
- Un alto nivel de saneamiento de soportes, de acuerdo con el National Institute of Standard and Technology (NIST)

Atención: Las operaciones de borrado seguro no son reversibles. Todos los datos del disco se borrarán de manera permanente cuando se complete una acción de borrado seguro. Asegúrese de que los datos de la unidad se han copiado o pueden perderse.

El borrado seguro de unidades FDE permite borrar de forma inmediata datos sin necesidad de retirar la unidad del centro de datos. Con solo unos cuantos clics, podrá reutilizar o descartar una unidad rápidamente. Con el borrado seguro, puede borrar unidades y utilizarlas de nuevo. Esto elimina la necesidad de destruir unidades, sin perder garantías y pudiendo reutilizar las unidades de forma segura. De acuerdo con el NIST, el borrado seguro se considera un tipo de depuración de datos y un nivel más alto de saneamiento de datos que los métodos tradicionales.

El borrado seguro solicita a la unidad FDE que borre permanentemente la clave de cifrado actual y la sustituya con una clave de cifrado nueva generada de manera aleatoria que se guarda dentro de la unidad. La clave de cifrado de la unidad se utiliza para codificar y descodificar todos los datos del disco. Tras cambiar la clave de cifrado, todos los datos escritos anteriormente en el disco pasan a ser ininteligibles. Los datos cifrados con la clave de cifrado anterior son ininteligibles cuando se descifran con la nueva clave. Esto incluye todos los bits, cabeceras y directorios. Los datos pasan a ser completa y permanentemente inaccesibles.

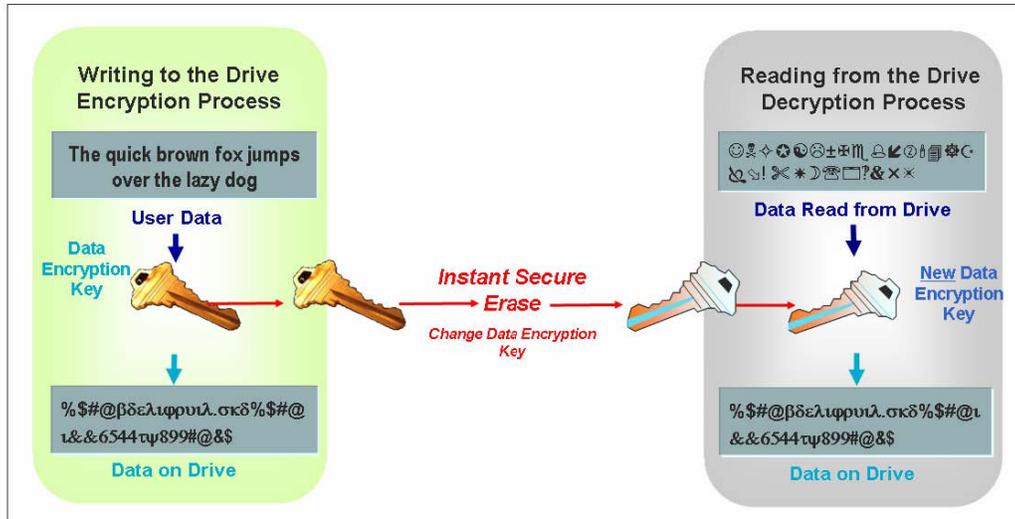


Figura 32. Proceso de borrado seguro

Autorizaciones de seguridad FDE

La siguiente tabla identifica y describe los parámetros de autorización utilizados para implementar la seguridad en subsistemas de almacenamiento compatibles con FDE.

Tabla 35. Autorizaciones de seguridad

Parámetro	Descripción	¿Dónde se ubica y gestionar?	¿Cómo se genera?
Clave de cifrado	La clave de cifrado se utiliza para codificar y descodificar datos en las unidades de disco FDE.	Se almacena y es gestionada por la unidad de disco FDE: <ul style="list-style-type: none"> Nunca se transfiere de la unidad. Cada unidad tiene su propia clave de cifrado. 	La clave de cifrado se genera cuando se fabrica la unidad y se vuelve a generar en la ubicación del cliente (mediante un comando del controlador a la unidad) para asegurarse de que la seguridad de la clave no se ve comprometida antes de su uso.
Clave de seguridad	La clave de seguridad es necesaria para desbloquear la clave de cifrado para cifrar y descifrar datos. Se crea una clave de seguridad para todas las unidades FDE del subsistema de almacenamiento. A la clave de seguridad en ocasiones se le denomina clave de bloqueo.	Se almacena y es gestionada por el controlador. Se sincroniza una clave de seguridad única para todos los controladores del subsistema de almacenamiento.	El subsistema de almacenamiento es el encargado de generar la clave de seguridad y esta se cifra y oculta en el mismo.

Tabla 35. Autorizaciones de seguridad (continuación)

Parámetro	Descripción	¿Dónde se ubica y gestionar?	¿Cómo se genera?
Identificador de clave de seguridad	El identificador de clave de seguridad se empareja con la clave de seguridad para ayudarle a recordar la clave que debe utilizar para operaciones seguras. Solo en el caso de gestión local de claves de seguridad, tiene la opción de proporcionar hasta 189 caracteres alfanuméricos vinculados con el identificador de claves de seguridad generado por el subsistema de almacenamiento.	El identificador de clave de seguridad se almacena en un área especial del disco: <ul style="list-style-type: none"> • Siempre se puede leer en el disco • Puede escribirse en el disco sólo si se ha habilitado la seguridad y la unidad está desbloqueada 	Serie de caracteres alfanuméricos especificada por el usuario (solo para gestión local de claves de seguridad). El subsistema de almacenamiento añade su identificador mundial y un número generado aleatoriamente a los caracteres especificados.
Frase de contraseña	La frase de contraseña se utiliza para cifrar la clave de seguridad y el identificador de claves de seguridad. La frase de contraseña es una serie de caracteres alfanuméricos especificada por el usuario, de un mínimo de 8 caracteres y un máximo de 32. Debe contener al menos un número, una letra minúscula, una letra mayúscula y un carácter alfanumérico (por ejemplo <, >, &, @, +, o -). No se permiten espacios y se diferencia entre mayúsculas y minúsculas.	La serie de caracteres alfanuméricos especificada por el usuario no se almacena en ninguna parte del subsistema de almacenamiento o del archivo de claves de seguridad. La frase de contraseña se utiliza para cifrar la clave de seguridad cuando se exporta al archivo de claves de seguridad. También se utiliza para descifrar la clave en el archivo de claves de seguridad cuando esta se utiliza para importar unidades FDE con seguridad habilitada a un subsistema de almacenamiento.	Serie de caracteres alfanuméricos especificada por el usuario.

Tabla 35. Autorizaciones de seguridad (continuación)

Parámetro	Descripción	¿Dónde se ubica y gestionar?	¿Cómo se genera?
Archivo de claves de seguridad	Archivo en el que se guarda el identificador de claves de seguridad y la clave de seguridad cifrada.	El nombre del archivo y su ubicación los determina el administrador. Además de en la ubicación especificada por el administrador, Storage Manager también guarda una copia del archivo de claves de seguridad en la ubicación predeterminada. Consulte el documento <i>IBM Full Disk Encryption Best Practices</i> para obtener más información.	Generado por el subsistema de almacenamiento una vez que inicia una operación de creación de una clave de seguridad, cambia la clave de seguridad o guarda la clave de seguridad.

Terminología de FDE

La siguiente tabla define la terminología de FDE que se utiliza en este capítulo.

Tabla 36. Terminología de cifrado de disco completo

Término	Descripción
FDE	Cifrado de disco completo, un chip personalizado o ASIC (circuito integrado específico de aplicación) de la unidad de disco que requiere una clave de seguridad para permitir el inicio del cifrado o descifrado. Las unidades de disco FDE cifran todos los datos del disco. La unidad asegurada requiere que se facilita una clave de seguridad antes de realizar operaciones de lectura o escritura. La unidad procesa totalmente el cifrado y descifrado de datos y estos no son aparentes para el subsistema de almacenamiento.
Borrado seguro	Destrucción permanente de los datos mediante la modificación de la clave de cifrado de la unidad. Tras el borrado seguro, los datos grabados anteriormente en el disco pasan a ser ilegibles. Esta característica utiliza las capacidades de seguridad de disco FDE para borrar los datos cambiando la clave de cifrado por un valor generado de forma aleatoria. Dado que la clave de cifrado nunca abandona la unidad, esto proporciona un borrado seguro. Después del borrado seguro, la unidad queda desbloqueada, permitiendo a cualquiera leer o escribir en el disco. El borrado seguro en ocasiones se denomina reaprovisionamiento de unidad.
Gestión de claves local	Método de gestión de claves que utiliza una clave de seguridad creada y contenida en el controlador del subsistema de almacenamiento. Para mover las unidades aseguradas de un subsistema de almacenamiento a otro, debe utilizar el archivo de claves de seguridad guardado desde el subsistema de almacenamiento original con el fin de desbloquear las unidades. La clave de seguridad se oculta y almacena en el subsistema de almacenamiento cuando se desactiva la alimentación.

Tabla 36. Terminología de cifrado de disco completo (continuación)

Término	Descripción
Gestión de claves externa	Método de gestión de claves que utiliza una ubicación de claves central de su red (uno o varios servidores externos a un subsistema de almacenamiento) para gestionar claves de diferentes dispositivos de almacenamiento. Un servidor proxy debe facilitar la solicitud y aceptación de una clave de seguridad. La clave de seguridad no se almacena en el subsistema de almacenamiento cuando se corta la alimentación. Nota: 1. La gestión externa de claves de seguridad requiere software dedicado, como IBM Tivoli Key Lifecycle Manager (TKLM).
Bloqueado	Estado al que cambia una unidad FDE con seguridad habilitada cuando se retira y reinserta en el subsistema de almacenamiento, o cuando se corta la alimentación del subsistema de almacenamiento. Cuando se restaura la alimentación al subsistema de almacenamiento, la unidad permanece en estado Bloqueado. Hasta que el controlador no desbloquea el disco bloqueado utilizando la clave de seguridad, no se pueden escribir o leer datos en el mismo. Si el controlador no tiene la clave de seguridad, se necesitan el archivo de claves de seguridad y frase de contraseña para desbloquear las unidades y realizar operaciones de lectura o escritura.
Reutilización/ reaprovisionamiento	Cambio del estado de una unidad de Asegurada o No asegurada para poder utilizarla de nuevo. El reaprovisionamiento de la unidad se realiza mediante el borrado seguro.
Matriz segura	Una matriz de unidades FDE con seguridad habilitada.
Unidad con capacidad de seguridad	Unidad FDE que puede cifrarse pero está en estado No asegurada (seguridad no habilitada).
Unidad con seguridad habilitada	Unidad FDE con seguridad habilitada. La unidad FDE con seguridad habilitada se debe desbloquear utilizando la clave de seguridad cuando se activa la alimentación para poder realizar operaciones de lectura o escritura.
Desbloqueado	Estado de una unidad FDE con seguridad habilitada en la que se puede acceder a los datos del disco para realizar operaciones de lectura y escritura.

Antes de empezar

Si utiliza la gestión externa de claves de seguridad, debe completar los siguientes procedimientos:

1. Instale y configure el software de gestión externa de licencias de claves IBM Tivoli Key Lifecycle Manager (TKLM). Consulte la documentación facilitada con el software para más información.
2. Descargue DS TKLM Proxy Code del Portal de soporte de IBM en <http://www.ibm.com/support/entry/portal>.
3. Instale y configure DS TKLM Proxy Code. Consulte “Instalación y configuración del servidor DS TKLM Proxy Code” en la página 235.
4. Habilite las características premium Cifrado de disco completo y Gestión de claves externa en Storage Manager. Consulte “Habilitación de características premium” en la página 242.
5. Configure TKLM y los subsistemas de almacenamiento para el proxy DS TKLM y cree las autorizaciones de gestión externa de claves de seguridad. Consulte

“Creación de autorizaciones de seguridad utilizando la gestión externa de claves de seguridad ” en la página 246 en “Habilitación de características premium” en la página 242 para obtener más información.

Si prefiere utilizar la gestión de claves de seguridad local, comience con la información de “Configuración de cifrado de disco con unidades FDE” en la página 242.

Instalación y configuración del servidor DS TKLM Proxy Code

Esta sección describe los procedimientos necesarios para instalar el servidor DS TKLM Proxy Code. DS TKLM Proxy Code soporta los siguientes sistemas operativos:

- AIX 5.x
- AIX 6.x
- Red Hat Enterprise Linux 4.x
- Red Hat Enterprise Linux 5.5
- SUSE Linux Enterprise Server 10.3
- SUSE Linux Enterprise Server 11
- Windows 2008 R2
- Windows 2008 Service Pack 2
- Windows 2008 Standard Edition
- Windows 2008 Enterprise Edition

Importante: Cualquier cambio de entorno o configuración que pudiera afectar al servidor DS TKLM Proxy Code requiere que reinicie el servidor. Por ejemplo, un intercambio de controlador de Storage manager, la emisión del comando **sysWipe** o un cambio en la dirección IP harán que el servidor DS TKLM Proxy Code deba ser configurado de nuevo y reiniciado. Además, cualquier cambio en el identificador de clave de seguridad, como el intercambio del controlador de Storage Manager o la emisión del comando **sysWipe**, requiere la modificación de TKLM para que reconozca el nuevo identificador de clave de seguridad, como se define en “Creación de autorizaciones de seguridad utilizando la gestión externa de claves de seguridad ” en la página 246. Consulte “Inicio, detención y reinicio del servidor DS TKLM Proxy Code” en la página 236 para obtener más información.

El diagrama siguiente ilustra las relaciones entre los componentes de una configuración de gestión externa de claves de seguridad.

Nota:

1. Un servidor proxy puede supervisar un máximo de cuatro controladores de subsistema de almacenamiento.
2. Se pueden conectar un máximo de cuatro servidores TKLM a un servidor proxy.

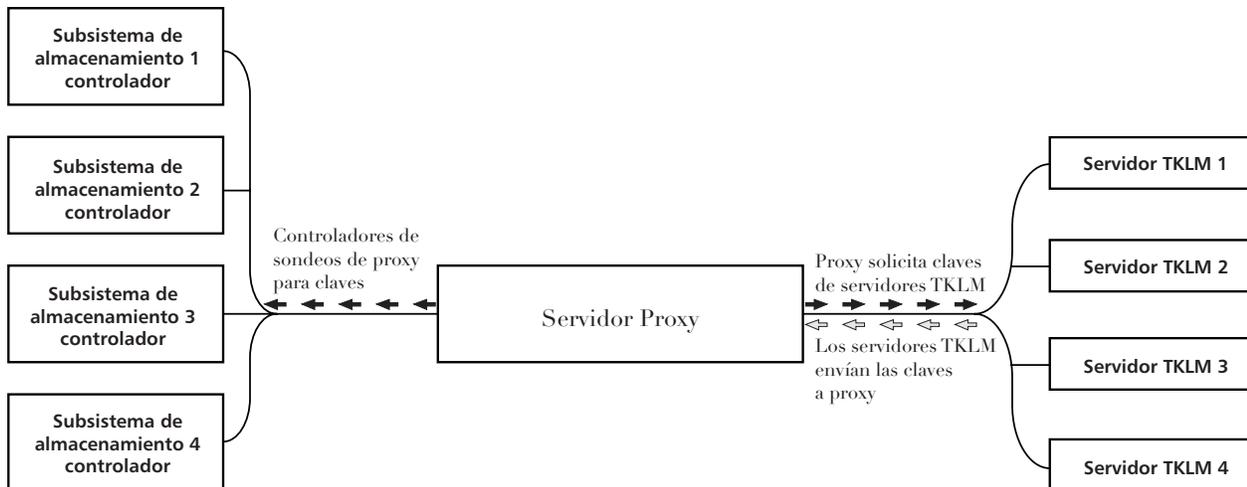


Figura 33. Topología de gestión externa de claves de seguridad

Para establecer una configuración de gestión externa de claves de seguridad, descargue DS TKLM Proxy Code del Portal de soporte de IBM, <http://www.ibm.com/support/entry/portal>, y complete los procedimientos siguientes:

1. "Modificación del archivo de configuración de servidor de código proxy de DS TKLM"
2. "Instalación de DS TKLM Proxy Code" en la página 240

Importante: Debe completar los procedimientos en orden. Asegúrese de que el software IBM Tivoli Key Lifecycle Manager (TKLM) está instalado. Consulte la documentación facilitada con el software para más información.

Inicio, detención y reinicio del servidor DS TKLM Proxy Code

Cualquier cambio relacionado con el entorno o la configuración que pudiera afectar al proxy (por ejemplo cambios de red) requiere que se reinicie el proxy. Están disponibles los siguientes programas de utilidad.

Para AIX:

```
start_DS_TKLM_Proxy_Code_AIX.sh
stop_DS_TKLM_Proxy_Code_AIX.sh
restart_DS_TKLM_Proxy_Code_AIX.sh
```

Para Linux:

```
start_DS_TKLM_Proxy_Code_Linux.sh
stop_DS_TKLM_Proxy_Code_Linux.sh
restart_DS_TKLM_Proxy_Code_Linux.sh
```

El script `stop_DS_TKLM_Proxy_Code_*.sh` eliminará la entrada de `/etc/inittab` y finalizará los procesos.

Modificación del archivo de configuración de servidor de código proxy de DS TKLM

El archivo de configuración para el proxy es `DS_TKLM_Proxy_Code.config`. El nombre del archivo de configuración, así como los parámetros y sus definiciones,

son los mismos para todos los sistemas operativos compatibles (Windows, AIX y Linux). Sin embargo, el formato de algunos de los valores de los parámetros son diferentes en Windows y AIX o Linux.

El método de creación y edición del archivo de configuración en Windows es diferente del método utilizado en AIX o Linux. Con Windows, se debe crear `DS_TKLM_Proxy_Code.config` manualmente, utilizando la plantilla incluida en el archivo `DS_TKLM_Proxy_Code_Windows*.zip`. Las definiciones de los parámetros deben asignarse antes de poder instalar el proxy.

Importante: Si trabaja en un entorno de sistema operativo Windows, debe crear y modificar el archivo de configuración antes de instalar el servidor de código proxy de DS TKLM.

Con AIX y Linux, se crea `DS_TKLM_Proxy_Code.config` y las definiciones de parámetros se asignan durante la instalación. Debe asignar las definiciones de los parámetros del archivo de configuración cuando se le solicite.

La definición de cada parámetro se explica en la siguiente tabla.

Tabla 37. Propiedades del archivo de configuración de proxy

Nombre de propiedad	Descripción	Ejemplo
LogLevel	Esta propiedad especifica uno de los cuatro niveles siguientes para el registro: <ul style="list-style-type: none"> • UserInfo: información básica sobre eventos • UserWarning: información de aviso sobre un problema potencial • UserError: información de error sobre un fallo del sistema, salida del servidor proxy • Debug: información útil para la depuración, como longitud de series y valores de propiedades en diferentes posiciones 	LogLevel = debug
DebugPath	Esta propiedad especifica la ubicación del archivo de depuración. Debe proporcionar una ruta de su sistema de archivos, que puede ser una ruta relativa al directorio <code>/DS_TKLM_Proxy_Code/bin</code> o una ruta absoluta. Nota: Asegúrese de disponer de permisos de lectura y escritura para el directorio de la ruta.	Ejemplo para AIX o Linux: DebugPath = <code>./Log/Debug/debug.log</code> Ejemplo para Windows: DebugPath = <code>.\Log\Debug\debug.log</code>
AuditPath	Esta propiedad especifica la ubicación del archivo de auditoría. Debe proporcionar una ruta de su sistema de archivos, que puede ser una ruta relativa al directorio <code>/DS_TKLM_Proxy_Code/bin</code> o una ruta absoluta. Nota: Asegúrese de disponer de permisos de lectura y escritura para el directorio de la ruta.	Ejemplo para AIX o Linux: AuditPath = <code>./Log/Audit/audit.log</code> Ejemplo para Windows: AuditPath = <code>.\Log\Audit\audit.log</code>

Tabla 37. Propiedades del archivo de configuración de proxy (continuación)

Nombre de propiedad	Descripción	Ejemplo
ThresholdSize	<p>Esta propiedad especifica el tamaño máximo de cada archivo de registro en bytes. Si se alcanza el umbral de tamaño, se crea un nuevo archivo con el mismo nombre que el archivo original y el número 01 añadido al final. Si el nuevo archivo de registro alcanza el umbral de tamaño, se sobrescribe el archivo original.</p> <p>Nota: Si más adelante decide aumentar el límite del umbral, elimine los archivos de registro existentes. De lo contrario, el proxy escribirá información de registro en los archivos antiguos en caso de que el nuevo umbral sea superior al anterior.</p>	Umbral = 100000000000
Keyinformation Path	<p>Esta propiedad especifica la ubicación del archivo de certificados de seguridad (que coincide con el archivo especificado en la propiedad KeyPassword. Proporcione una ruta de su sistema de archivos, que puede ser una ruta relativa al directorio /DS_TKLM_Proxy_Code/bin o una ruta absoluta. Asegúrese de que la ruta se adhiere a las convenciones para la especificación de directorio de Windows o AIX y Linux, y de que el directorio y el archivo que ha especificado existen.</p> <p>Nota: Esta propiedad hace referencia al archivo de certificados de seguridad y a la contraseña que recibió en un correo electrónico tras habilitar la característica premium de gestión externa de claves. Si no recibe el archivo de certificados de seguridad o si ya no tiene dicho archivo, puede solicitar otro archivo y la contraseña mediante el proceso de reactivación de claves del sitio web de características premium de IBM.</p>	<p>Ejemplo para AIX o Linux:</p> <pre>KeyinformationPath = ./CertFile/ibmproxycert.p12</pre> <p>Ejemplo para Windows:</p> <pre>KeyinformationPath = .\CertFile\ibmproxycert.p12</pre>
KeyPassword	<p>Esta propiedad especifica la contraseña para el certificado de seguridad (coincide con el archivo especificado en la propiedad KeyinformationPath), y se ocultará una vez que se lea. Si necesita cambiar la contraseña una vez que esta se haya ocultado, antes debe suprimir el valor de la propiedad KeyPasswordHex y reiniciar el servidor proxy. De lo contrario, se ignorará la nueva contraseña.</p> <p>Nota: Esta propiedad hace referencia al archivo de certificados de seguridad y a la contraseña que recibió en un correo electrónico tras habilitar la característica premium de gestión externa de claves. Si no recibe el archivo de certificados de seguridad o si ya no tiene dicho archivo, puede solicitar otro archivo y la contraseña mediante el proceso de reactivación de claves del sitio web de características premium de IBM.</p>	<p>Ejemplo de la propiedad KeyPassword antes de que se realice la primera lectura:</p> <pre>KeyPassword = password</pre> <p>Ejemplo de la propiedad KeyPassword tras la primera lectura y una vez ocultada la contraseña:</p> <pre>KeyPasswordHex = 47558BADDI3321FC</pre> <pre>KeyPassword = *****</pre>

Tabla 37. Propiedades del archivo de configuración de proxy (continuación)

Nombre de propiedad	Descripción	Ejemplo
SYMServer.x	<p>El término <i>SYMServer</i> se refiere a un subsistema de almacenamiento y sus controladores.</p> <p>Nota: Un servidor proxy puede supervisar un máximo de cuatro controladores de subsistema de almacenamiento. Esta propiedad especifica información sobre cada subsistema de almacenamiento, o símbolo-servidor (<i>SYMServer. 1 - SYMServer. n</i>) de su configuración. Cada <i>SYMServer</i> requiere dos direcciones IP de controlador, dos puertos (2463), un SSID, un indicador de contraseña y una contraseña. Así, cada valor de la propiedad <i>SYMServer</i> debe coincidir con el patrón en el siguiente formato. Las variables aparecen en cursiva:</p> <p><i>SYMSEVER.x = Dirección IP Controlador A , Dirección IP Controlador B , número de puerto , número de puerto , SSID , indicador de contraseña , contraseña</i></p> <p>El indicador de contraseña debe definirse como falso si la contraseña se facilita en texto simple y como verdadero si la contraseña se oculta. La contraseña se utiliza para gestionar el subsistema de almacenamiento. La contraseña se ocultará de forma automática y se almacenará en un formato cifrado por el proxy tras la lectura.</p> <p>En esta propiedad, puede utilizar espacios entre cada parte del valor. El SSID debe ser un valor hexadecimal. El proxy compara el SSID del archivo <i>DS_TKLM_Proxy_Code.config</i> con el SSID que recupera del subsistema de almacenamiento. Si no son iguales, el proxy detendrá la supervisión del subsistema de almacenamiento.</p> <p>Nota: Debe obtener el SSID para el subsistema de almacenamiento en la ventana Perfil del subsistema de almacenamiento de Storage Manager.</p>	<p>Ejemplo antes de que se lea por primera vez el archivo de configuración:</p> <pre>SYMServer.1 = 9.37.117.35 , 9.37.117.36 , 2463 , 2463 ,600A0B8000339848000000004B72851F, false, SymPasswd</pre> <p>Ejemplo una vez leído por primera vez el archivo de configuración:</p> <pre>SYMServer.1 = 9.37.117.35 , 9.37.117.36 , 2463 , 2463 , 600A0B8000339848000000004B72851F, true , 6408D5D0C596979894AA8F</pre>
TKLMServer.x	<p>Esta propiedad especifica información sobre cada servidor TKLM de su configuración.</p> <p>Nota: Se pueden conectar un máximo de cuatro servidores TKLM a un servidor proxy. Cada servidor TKLM tiene una dirección IP y un puerto, por lo que cada valor de propiedad del servidor TKLM debe coincidir con el patrón respetando el siguiente formato. Las variables aparecen en cursiva:</p> <p><i>TKLMServer.x = dirección IP , número de puerto</i></p> <p>En esta propiedad, puede utilizar espacios entre cada parte del valor. Si no se introduce un valor para esta propiedad, el servidor proxy utiliza el valor predeterminado (localhost, 3801). El número de puerto se encuentra en la ventana Puertos de servicio de claves del software Tivoli Lifecycle Key Manager.</p>	<p><i>TKLMServer.1 = 9.41.18.161 , 3801</i></p>
TcpTimeout	<p>Esta propiedad especifica la duración del período de tiempo de espera para una conexión TCP a los servidores, en segundos.</p>	<p>TcpTimeout = 1000</p>

Tabla 37. Propiedades del archivo de configuración de proxy (continuación)

Nombre de propiedad	Descripción	Ejemplo
RpcTimeout	Esta propiedad especifica la duración del período de tiempo de espera para llamadas a procedimiento remoto, en segundos.	RpcTimeout = 10
TimeBetween-SymbolServer-Queries	Esta propiedad especifica un período de espera entre las comprobaciones del servidor proxy del estado de atención, en segundos.	TimeBetweenSymbolServerQueries = 10

Instalación de DS TKLM Proxy Code

Para instalar DS TKLM Proxy Code y utilizarlo para la gestión externa de claves de seguridad, complete uno de los procedimientos siguientes. Para entornos Windows, consulte “Instalación del servidor DS TKLM Proxy Code en un entorno Windows”. Para entornos AIX o Linux, consulte “Instalación del servidor DS TKLM Proxy Code en un entorno AIX o Linux” en la página 241.

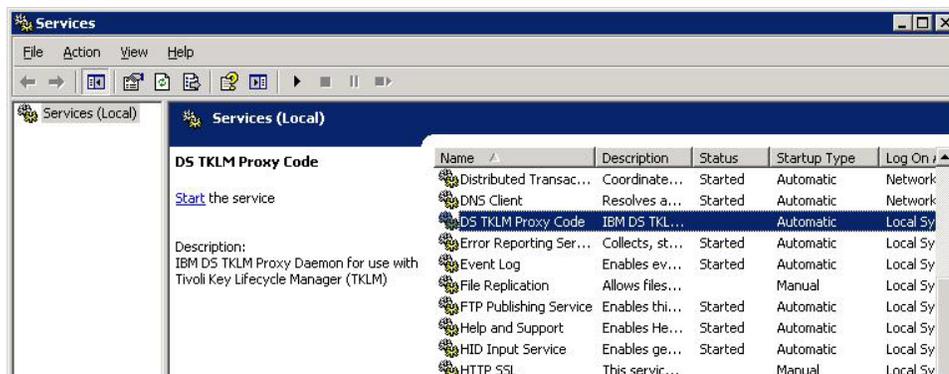
Instalación del servidor DS TKLM Proxy Code en un entorno Windows

Para instalar el servidor proxy en un entorno Windows, complete los pasos siguientes:

1. Vaya al Portal de soporte de IBM en <http://www.ibm.com/support/entry/portal> y descargue el archivo aplicable para su versión de Windows en la zona de Descargas y arreglos del portal. El nombre de archivo será similar a DS_TKLM_Proxy_Code-Windows-V*.zip.
2. Extraiga los archivos comprimidos en un directorio local (por ejemplo c:\DS_TKLM_Proxy_Code).
3. Asegúrese de que se ha modificado el archivo DS_TKLM_Proxy_Code.config (consulte “Modificación del archivo de configuración de servidor de código proxy de DS TKLM” en la página 236 para saber qué propiedades se deben modificar).
4. Asegúrese de que el archivo de certificado, proporcionado por IBM y especificado en la propiedad KeyInformationPath del archivo de configuración, existe antes de iniciar el servidor proxy.

Nota: Si se muestra el mensaje “DS_TKLM_Proxy_Code_WinService.exe - Error de aplicación”, deberá descargar e instalar el paquete Microsoft Visual C++ Redistributable Package. Para conocer qué paquete es compatible con Windows 2008, vaya a <http://www.microsoft.com/downloads/details.aspx?familyid=A5C84275-3B97-4AB7-A40D-3802B2AF5FC2&displaylang=en>.

5. En una ventana de indicador del DOS, escriba el comando: DS_TKLM_Proxy_Code_WinService.exe -i. El proxy se añadirá a la ventana Servicios. Para iniciar el proxy, pulse **Inicio** en la ventana Servicios.



Nota: Para desinstalar el proxy, abra una ventana de indicador del DOS y escriba y ejecute el siguiente comando: `DS_TKLM_Proxy_Code_WinService.exe -u`. Reinicie Windows.

Instalación del servidor DS TKLM Proxy Code en un entorno AIX o Linux

DS TKLM Proxy Code se facilita en formato RPM para AIX o Linux (RedHat y SUSE). Para instalar el servidor proxy en un entorno AIX o Linux, complete los pasos siguientes:

1. Vaya al Portal de soporte de IBM en <http://www.ibm.com/support/entry/portal> y descargue el archivo aplicable para su versión de sistema operativo en la zona de Descargas y arreglos del portal. Por ejemplo, el nombre de archivo para AIX podría estar en `DS_TKLM_Proxy_Code-AIX-V2.01_90.70.60.04.ppc.rpm`, y el de Linux en `DS_TKLM_Proxy_Code-Linux-V2.01_90.70.60.04.i386.rpm`.

Nota: Asegúrese de descargar el archivo correcto para su sistema operativo. El sistema operativo es una parte del nombre de archivo RPM.

2. Utilice comandos `rpm` para extraer el archivo descargado y comenzar con el proceso de instalación. Por ejemplo:

```
rpm -ivh --nodeps DS_TKLM_Proxy_Code-AIX-V1_.ppc.rpm
```

Nota: La parte `-nodeps` del comando es necesaria solo para instalaciones en AIX.

Al ejecutar el comando RPM, cree enlaces simbólicos, especifique la ubicación del archivo de certificado facilitado por IBM, cree una copia de seguridad de `/etc/inittab` y proporcione la ruta a utilizar al ejecutar el script de instalación.

3. Tras ejecutar el comando RPM, ejecute el script de instalación (`/DS_TKLM_Proxy_Code/bin/install.sh`).
4. Cuando se le pida, introduzca todas las propiedades del archivo de configuración. Consulte "Modificación del archivo de configuración de servidor de código proxy de DS TKLM" en la página 236 para ver una descripción de la propiedades y sus valores.

Para configurar TKLM y subsistemas de almacenamiento para el proxy, y crear autorizaciones de seguridad de gestión externa ed claves, continúa con "Creación de autorizaciones de seguridad utilizando la gestión externa de claves de seguridad " en la página 246 in "Habilitación de características premium" en la página 242.

Configuración de cifrado de disco con unidades FDE

Esta sección indica los procedimientos para habilitar FDE y crear matrices seguras en el subsistema de almacenamiento. Para configurar el cifrado de disco con discos FDE, realice las siguientes tareas:

1. Instale las unidades FDE (consulte “Instalación de unidades FDE”).
2. Habilite la característica premium de cifrado de disco completo (consulte “Habilitación de características premium”).
3. Cree una matriz y habilite la seguridad de matriz (consulte “Seguridad de una matriz RAID” en la página 250). También puede habilitar la seguridad para una agrupación de discos. El procedimiento es exactamente el mismo que el utilizado para una matriz.

Nota: Las capturas de pantalla de esta sección son ilustrativas y pueden diferir de la interfaz de usuario real en función de la versión de Storage Manager y del firmware del controlador.

Las unidades FDE con seguridad habilitada se bloquean cuando se corta la alimentación o cuando se retira del subsistema de almacenamiento. Para desbloquear una unidad bloqueada, consulte “Desbloqueo de unidades de disco” en la página 256.

En algunos subsistemas de almacenamiento, las unidades se pueden migrar como una matriz completa a otro subsistema de almacenamiento. Para migrar una unidad bloqueada, consulte “Migración de subsistemas de almacenamiento (intercambio de cabezal) con unidades FDE” en la página 259.

Instalación de unidades FDE

En esta sección se indican las unidades de disco FDE que soportan los subsistemas de almacenamiento IBM DS compatibles con FDE a fecha del documento. Consulte la *Guía de migración e instalación de alojamiento de expansión de almacenamiento y discos duros IBM System Storage DS3000, DS4000 o DS5000* y la *Guía de interoperabilidad de DS5000* para conocer los procedimientos de instalación y la información de soporte más actualizada.

Las unidades FDE soportadas por los subsistemas de almacenamiento IBM DS se especifican en la carta de anuncio de cada subsistema de almacenamiento particular. También puede ponerse en contacto con su distribuidor de IBM o representante de marketing de IBM para obtener más información sobre las unidades FDE compatibles con su subsistema de almacenamiento.

Nota: Si la unidad FDE está en estado Seguridad habilitada y no desea conservar los datos de la unidad, realice un borrado seguro en todas las unidades antes de utilizarlas como parte de una nueva matriz RAID. El borrado seguro obliga a las unidades a generar una nueva clave de cifrado, pone las unidades en estado Sin seguridad y garantiza que los datos almacenados previamente en el disco se borrarán. Consulte “Uso de borrado seguro” en la página 230 para obtener más información.

Habilitación de características premium

La característica premium de FDE debe habilitarse en el subsistema de almacenamiento utilizando las instrucciones facilitadas con el kit de titularidad de la característica premium de cifrado de disco de IBM DS. Para verificar si el cifrado de disco completo está habilitado, en la página Configuración, seleccione

Ver/habilitar características premium. En la ventana Características premium e información sobre paquete de características, Cifrado de disco completo: Habilitado y Gestión de claves externa: Habilitada indican que la característica premium de FDE está habilitada.

Importante: La gestión de claves externa requiere un archivo de certificado de seguridad y su contraseña. El archivo y contraseña se le envían por correo electrónico tras habilitar la característica premium Gestión de claves externa. Al habilitar la característica premium Gestión de claves externa en el sitio web de características premium de IBM, debe proporcionar una dirección de correo electrónico válida en los campos mostrados en la imagen siguiente. De lo contrario, se le pedirá que escriba su dirección de correo electrónico tras pulsar **Continuar**.

Your activation key file will be provided via a link once the information above is verified and submitted. In addition, if you would like the activation key file sent to you, please provide your email address below:

Email address

Verify email address

E-mail: Stay informed about IBM products, services, and other offerings! If you want to stay informed by e-mail, please let us know by checking the box below.

e-mail: Yes, please have IBM or an affiliate send me e-mail.

Other communications: IBM or an affiliate or selected organizations may keep you informed about IBM related products, services and other offerings through ways other than e-mail, for example, by telephone or postal mail. If you do not want us to use the information you provided here to keep you informed through other ways, please indicate in the box below.

Other communications: Please do not use the information I have provided here.

By clicking "Continue", you agree that IBM may process your data in the manner indicated above and as described in our Privacy policy.

Podría tardar hasta un día en recibir el archivo de certificado de seguridad y la contraseña. Si no recibe el archivo, o si ya no tiene el correo electrónico con el mismo, puede solicitar otro archivo y contraseña utilizando el proceso de reactivación de claves del sitio web de características premium de IBM. Para obtener más información sobre el archivo de certificado de seguridad y la configuración de las propiedades KeyInformationPath y KeyPassword (solo sistemas operativos Windows), consulte "Modificación del archivo de configuración de servidor de código proxy de DS TKLM" en la página 236.

Si ha habilitado la característica de FDE después de noviembre de 2010 para un subsistema de almacenamiento con firmware de controlador 7.70.xx.xx o posterior, External Key Management: Enabled y Full Disk Encryption: Enabled se mostrarán en la ventana Características premium y e información sobre paquete de características.



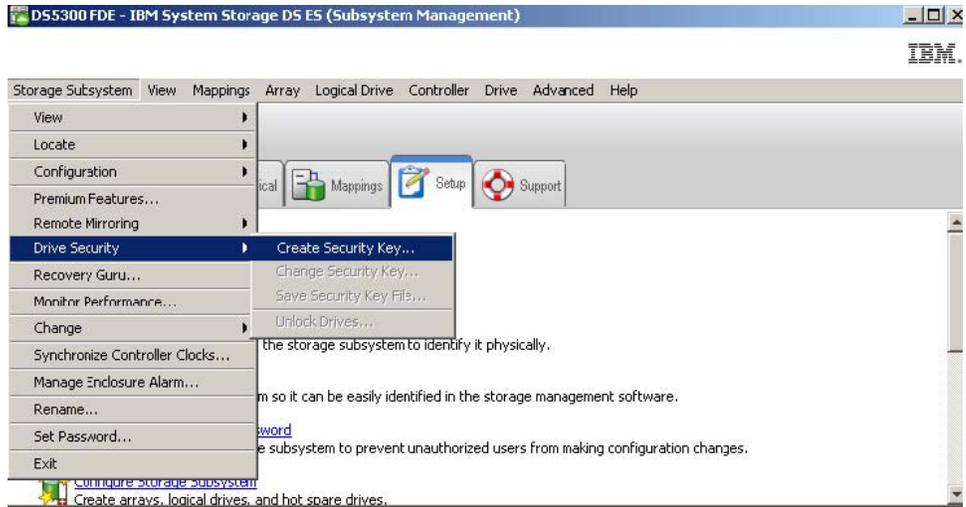
La habilitación del cifrado de disco completo incluye la creación de autorizaciones de seguridad que necesitará más adelante para desbloquear unidades de FDE aseguradas que se hayan apagado o retirado del subsistema de almacenamiento. Estas autorizaciones incluyen el identificador de claves de seguridad, una frase de contraseña y el archivo de claves de seguridad. Las autorizaciones de seguridad se aplican a todas las unidades de FDE del subsistema de almacenamiento y son fundamentales si tiene que desbloquear una unidad una vez conectada la alimentación.

El proceso de creación de autorizaciones de seguridad depende del método de gestión de claves utilizado. Consulte la sección aplicable para la gestión de claves de seguridad externa o local.

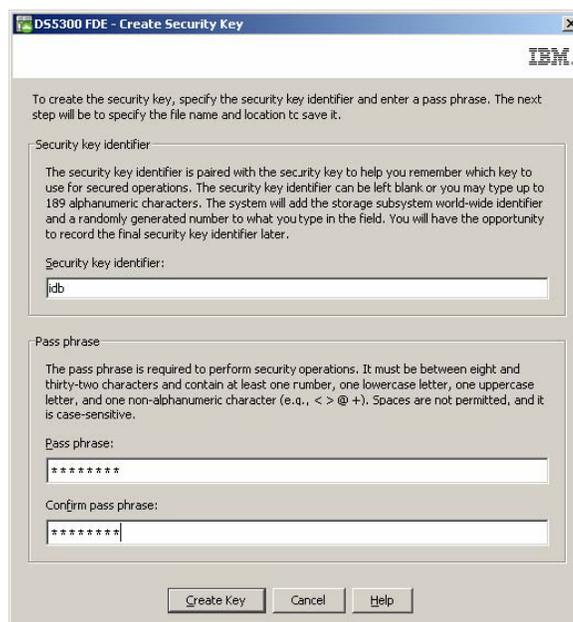
Creación de claves de seguridad utilizando la gestión de claves de seguridad local

Para crear las autorizaciones de seguridad para el cifrado de disco completo utilizando la gestión de claves local, siga los pasos indicados a continuación. Para las autorizaciones de seguridad de gestión de claves externa, consulte “Creación de autorizaciones de seguridad utilizando la gestión externa de claves de seguridad ” en la página 246.

1. En la ventana Gestión del subsistema de Storage Manager, pulse **Subsistema de almacenamiento, Seguridad de unidad y Crear clave de seguridad**.



2. Introduzca un identificador de clave de seguridad, el nombre y ubicación del archivo de claves de seguridad y una frase de contraseña en la ventana Crear clave de seguridad:
 - **Identificador de clave de seguridad:** El identificador de clave de seguridad está asociado con el identificador mundial del subsistema de almacenamiento y un número generado aleatoriamente, y se utiliza para identificar de manera única el archivo de claves de seguridad. El identificador de clave de seguridad se puede dejar en blanco o estar formado por un máximo de 189 caracteres.
 - **Frase de contraseña:** La frase de contraseña se utiliza para descifrar la clave de seguridad cuando esta se lee en el archivo de claves de seguridad. Introduzca y registre la frase de contraseña en este momento. Confirme la frase de contraseña.
 - **Archivo de copia de seguridad de la clave de seguridad:** Pulse **Examinar** junto al nombre del archivo para seleccionar el nombre y ubicación del archivo de claves de seguridad o introduzca directamente el valor en el campo. Pulse en **Crear clave**.



Nota: Guarde el archivo de claves de seguridad en una ubicación segura. Lo mejor es guardar su archivo de claves de seguridad con sus políticas de gestión de claves. Es importante registrar y recordar dónde ha almacenado el archivo porque será necesario cuando se mueva una unidad de un subsistema de almacenamiento a otro o cuando se sustituyan ambos controladores de un subsistema de almacenamiento a la vez.

3. En la ventana Creación de clave de seguridad completada, registre el identificador de clave de seguridad y el nombre del archivo de claves y pulse **Aceptar**. Las autorizaciones necesarias para habilitar la seguridad en la unidad de FDE del subsistema de almacenamiento ya están listas. Estas autorizaciones se sincronizan en ambos controladores del subsistema de almacenamiento. Con estas autorizaciones establecidas, las matrices de las unidades de FDE del subsistema de almacenamiento están seguras.

Atención: Para mayor seguridad, almacene más de una copia de la frase de contraseña y el archivo de claves de seguridad. No especifique el directorio del archivo de seguridad como ubicación para almacenar su copia del archivo de claves de seguridad. Si especifica el directorio predeterminado como ubicación para guardar el archivo de claves de seguridad, solo se guardará una copia del archivo de claves. No almacene el archivo de claves de seguridad en una unidad lógica correlacionada del mismo subsistema de almacenamiento. Consulte el documento *IBM Full Disk Encryption Best Practices* para mayor información.



Creación de autorizaciones de seguridad utilizando la gestión externa de claves de seguridad

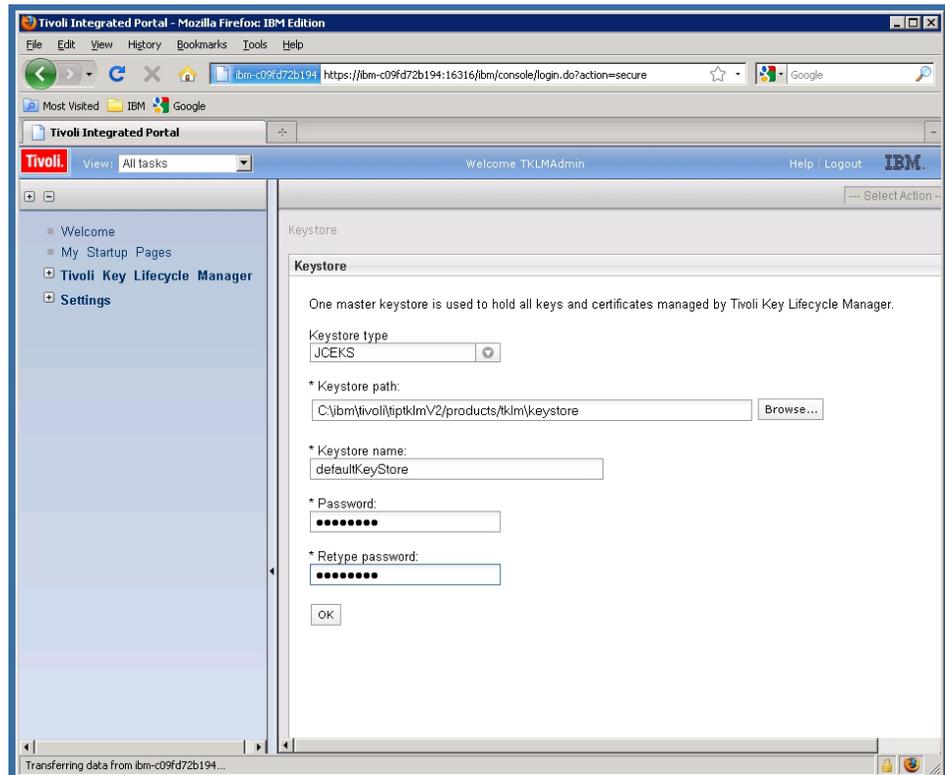
Importante:

Antes de crear las autorizaciones de seguridad para el cifrado de disco completo con gestión externa de claves, debe completar los procedimientos de "Instalación y configuración del servidor DS TKLM Proxy Code" en la página 235.

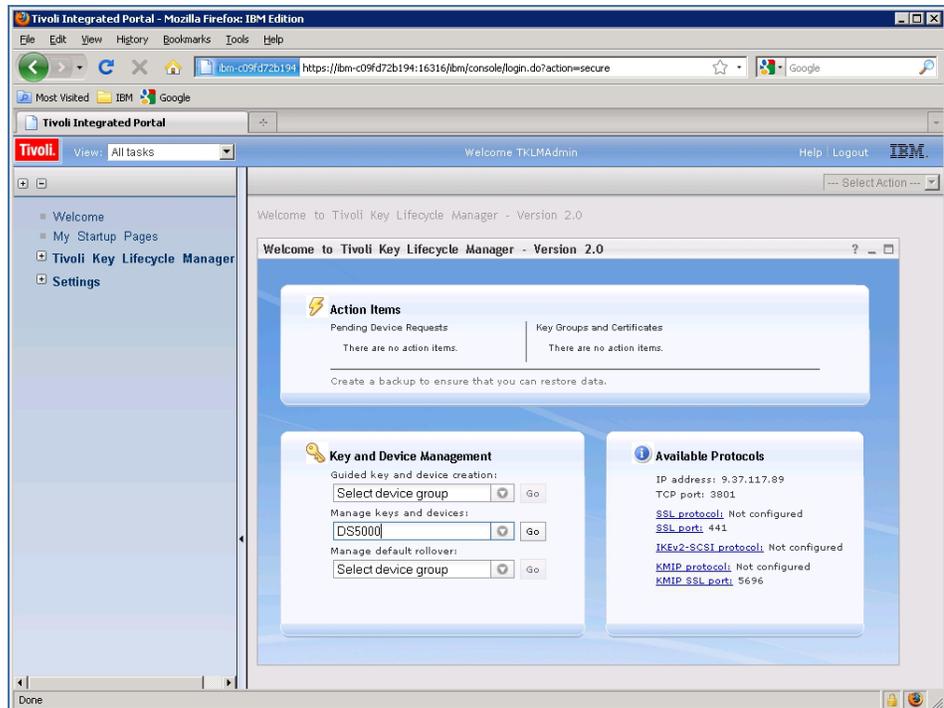
Una vez instalado Tivoli Key Lifecycle Manager (TKLM), se debe configurar para servir solicitudes de claves del servidor DS TKLM Proxy Code. Para configurar TKLM, complete los pasos siguientes:

1. Abra TKLM e inicie sesión con el identificador TKLAdmin.
2. Pulse **pulsar aquí para crear almacén de claves maestro**. Se abrirá la ventana Configuración de almacén de claves.

3. Escriba y vuelva a escribir la contraseña del almacén de claves. Mantenga los valores predeterminados para el resto de la configuración del almacén de claves y pulse **Aceptar**.

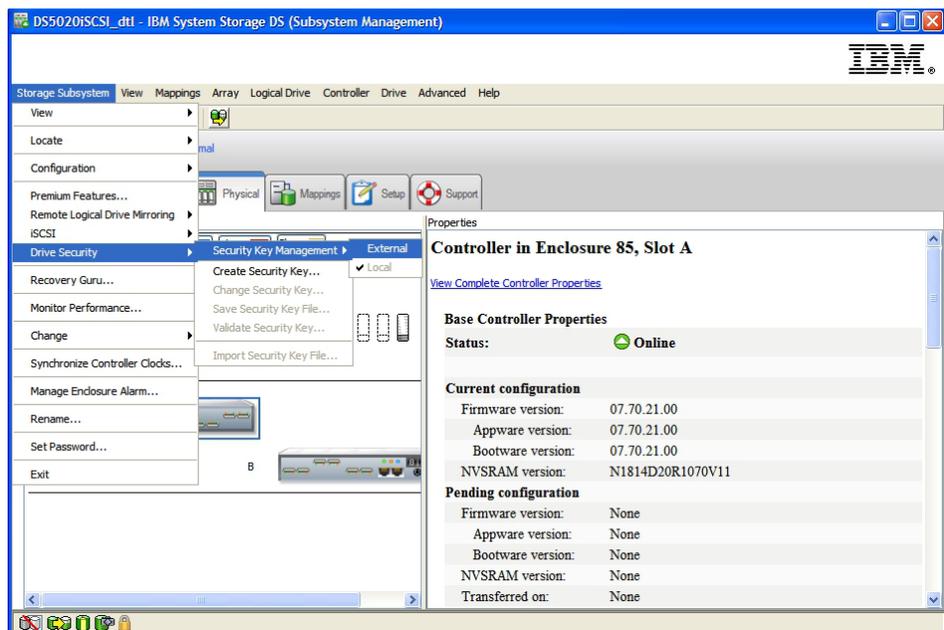


4. Pulse el enlace **Bienvenido** de la parte izquierda de la ventana. Se abrirá la ventana Bienvenido.
5. En el cuadro **Gestión de claves y dispositivos**, seleccione **DS5000** del menú **Gestionar claves y dispositivos**, y pulse **Ir**. Se abrirá la ventana Gestión de claves y dispositivos.



6. Cuando se muestre el mensaje de confirmación, pulse **Cancelar**.
7. En el menú desplegable de la parte inferior de la ventana, seleccione **Nuevas solicitudes de dispositivo pendientes de mi aprobación**.
8. Abra Storage Manager, inicie sesión y abra la ventana Gestión del subsistema del subsistema de almacenamiento que desee configurar.
9. Pulse **Subsistema de almacenamiento > Seguridad de unidad > Gestión de claves de seguridad > Externa**.

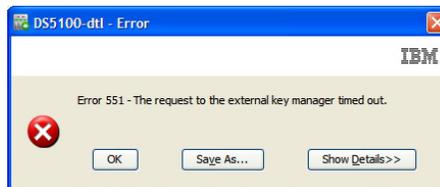
Nota: Si la característica premium Gestión de claves externa no está habilitada, la opción de menú **Gestión de claves de seguridad** no se mostrará al pulsar **Subsistema de almacenamiento > Seguridad de unidad**.



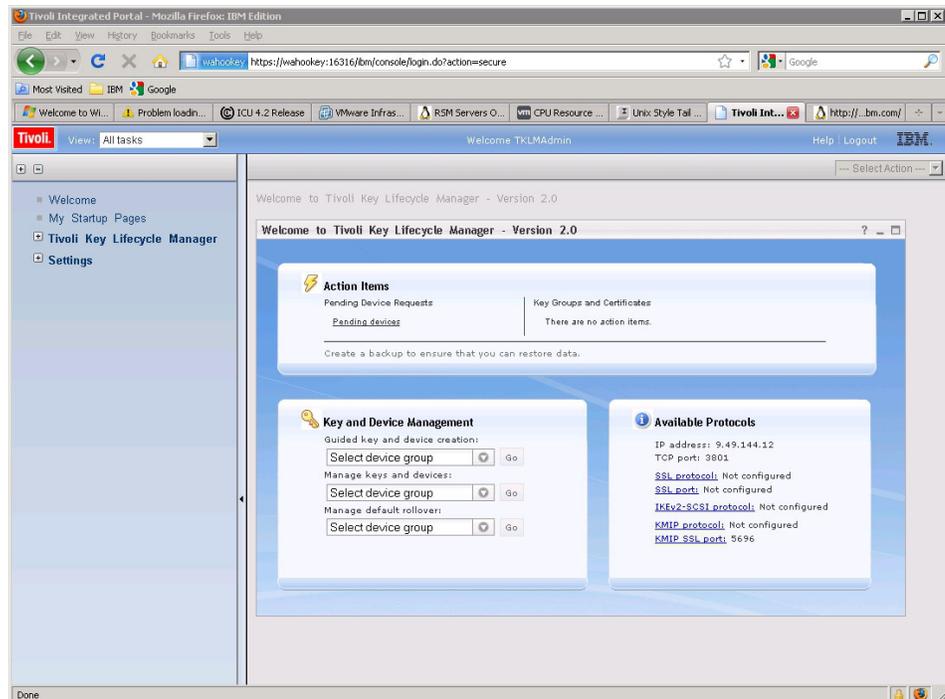
10. Cuando aparezca la ventana Confirmar gestión de claves de seguridad, escriba sí y pulse **Aceptar**.



11. Cuando se le pida, guarde una copia de la clave de seguridad. Introduzca la frase de contraseña, el nombre y ubicación del archivo, y pulse **Aceptar**. El controlador intentará conectar con el gestor de claves externo para solicitar la clave de seguridad. Si no lo consigue, se mostrará el mensaje siguiente:

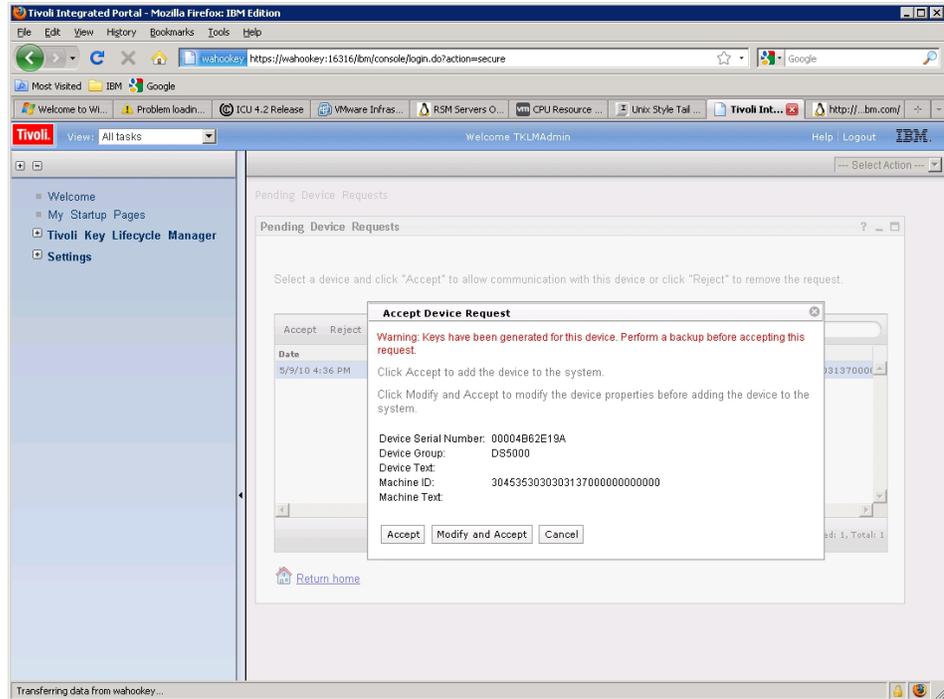


12. Vuelva a la aplicación TKLM y pulse el enlace **Dispositivos pendientes** en el cuadro **Elementos de acción**.



Se abrirá la ventana Solicitud de dispositivos pendientes.

13. Seleccione el dispositivo de la lista y pulse **Aceptar**. Se abrirá la ventana Aceptar solicitud de dispositivo.
14. Pulse **Aceptar** en la ventana Aceptar solicitud de dispositivo.



El servidor TKLM está listo para enviar claves al servidor DS TKLM Proxy Code.

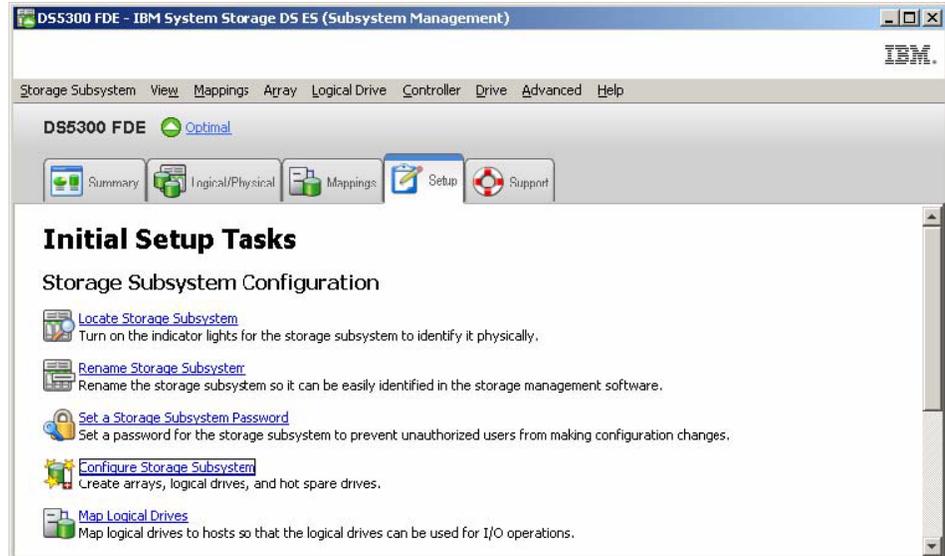
Seguridad de una matriz RAID

Cuando las unidades FDE de una matriz tiene la seguridad habilitada, dicha matriz está asegurada. Las unidades FDE de una matriz asegurada se bloquean si se corta su alimentación o se retiran del subsistema de almacenamiento.

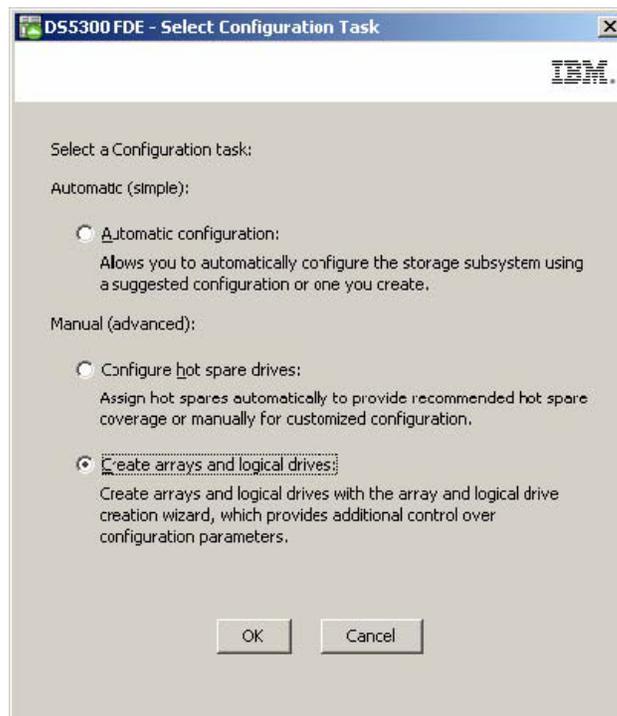
Todas las unidades de la matriz deben ser unidades FDE con capacidad de seguridad sin la seguridad habilitada. La matriz no debe contener ningún disco lógico de base FlashCopy o disco lógico de repositorioFlashCopy. Los discos lógicos de base y discos lógicos FlashCopy solo se pueden escribir en los discos una vez habilitada la seguridad.

Para crear una matriz RAID y asegurarla, siga los pasos indicados a continuación:

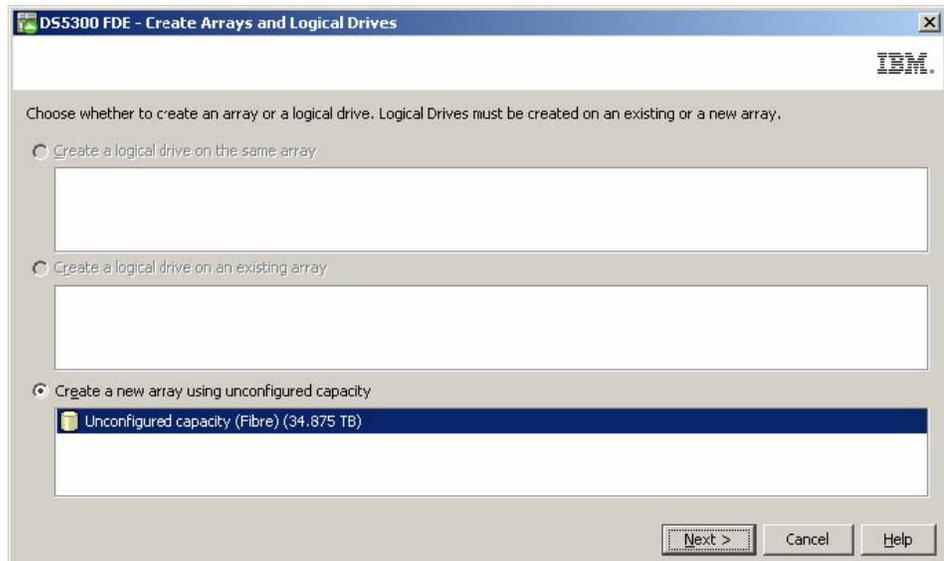
1. Cree una matriz RAID a partir de las unidades FDE disponibles en el subsistema de almacenamiento y asegúrela. En la página Configuración, pulse **Configurar subsistema de almacenamiento**.



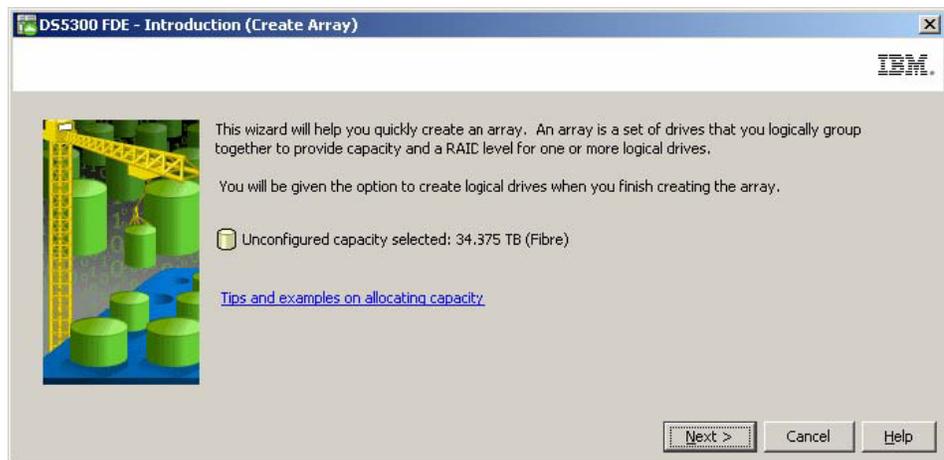
2. En la ventana Seleccionar tarea de configuración, pulse **Manual (avanzada)**, **Crear matrices y unidades lógicas** y **Aceptar**.



3. En la ventana Crear matrices y unidades lógicas, seleccione **Crear una nueva matriz con capacidad sin configurar**. Si hay otros tipos de unidades (no FDE) instalados en el DS5000, asegúrese de seleccionar solo unidades FDE de canal de fibra. Pulse **Siguiente** para continuar.

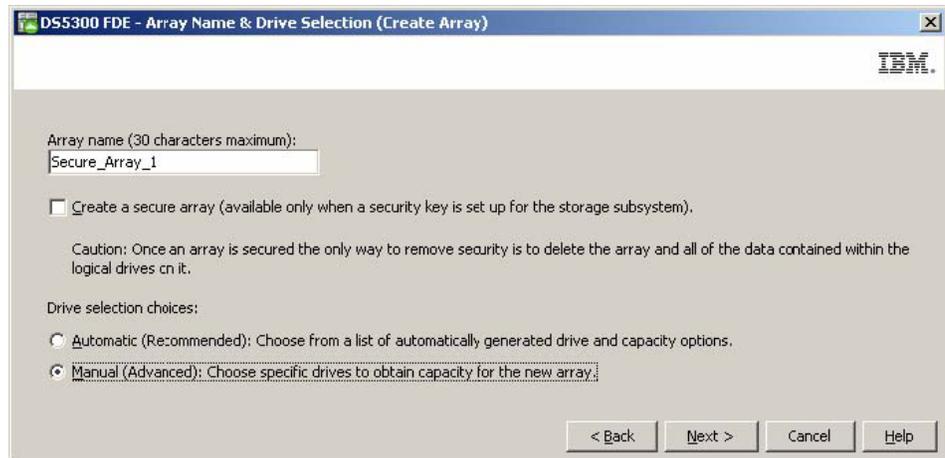


- Utilice el asistente Crear matriz para crear la matriz. Pulse **Siguiente** para continuar.



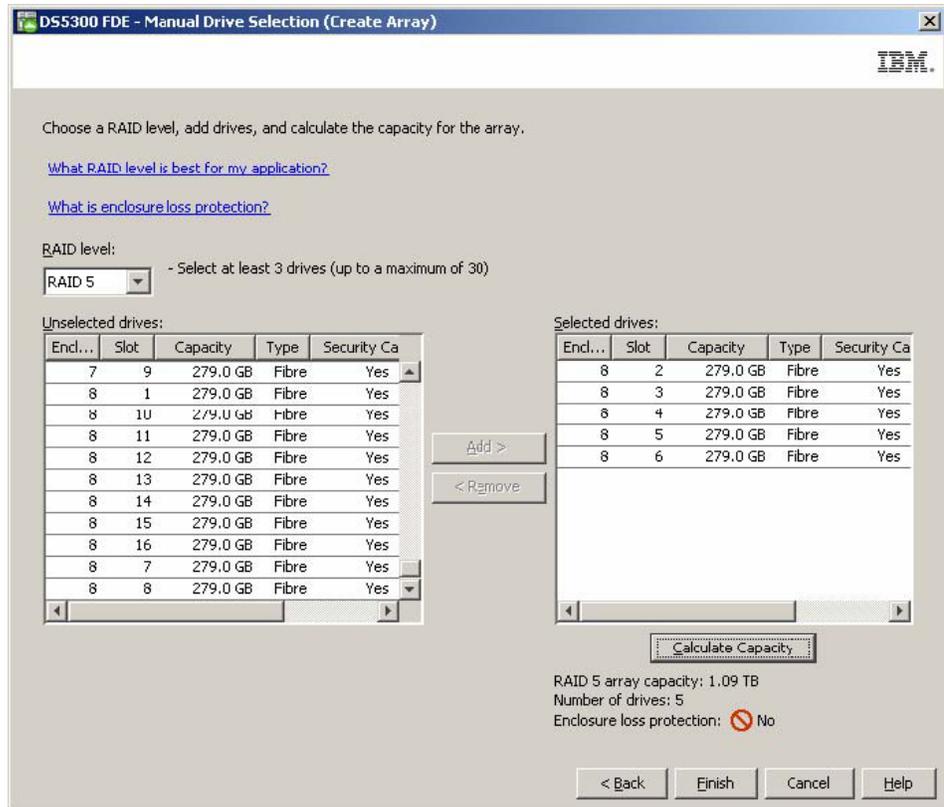
- En la ventana Nombre de matriz y selección de unidad, escriba un nombre para la matriz, (por ejemplo, Secure_Array_1). Tenga en cuenta que el recuadro de selección **Crear una matriz segura** se ha preseleccionado en esta ventana. Borre el recuadro de selección **Crear una matriz segura** y seleccione **Manual (avanzada)** en **Opciones de selección de disco**. Pulse **Siguiente** para continuar.

Nota: El recuadro de selección **Crear una matriz segura** se mostrará y seleccionará *solo* si la característica premium de cifrado de disco completo está habilitada. Si selecciona este recuadro de selección al crear una matriz, la matriz creada se asegurará y la opción **Manual (avanzada)** no será necesaria para asegurar la matriz.



6. Configurar las unidades de la matriz en la ventana Selección manual de unidades:
 - a. Seleccionar un nivel de RAID (por ejemplo, RAID 5).
 - b. En la lista **Unidades no seleccionadas**, seleccionar las unidades con capacidad de seguridad que desea utilizar y pulsar **Añadir** para añadirlas a la lista **Unidades seleccionadas** (por ejemplo, seleccionar las unidades de disco de las ranuras 2 a 6 del alojamiento de expansión del almacenamiento 8).
 - c. Pulsar **Calcular capacidad** para calcular la capacidad total de las unidades seleccionadas.
 - d. Pulsar **Finalizar** para completar la matriz.

Nota: Estas unidades aún no estarán aseguradas. Se asegurarán durante el proceso restante.

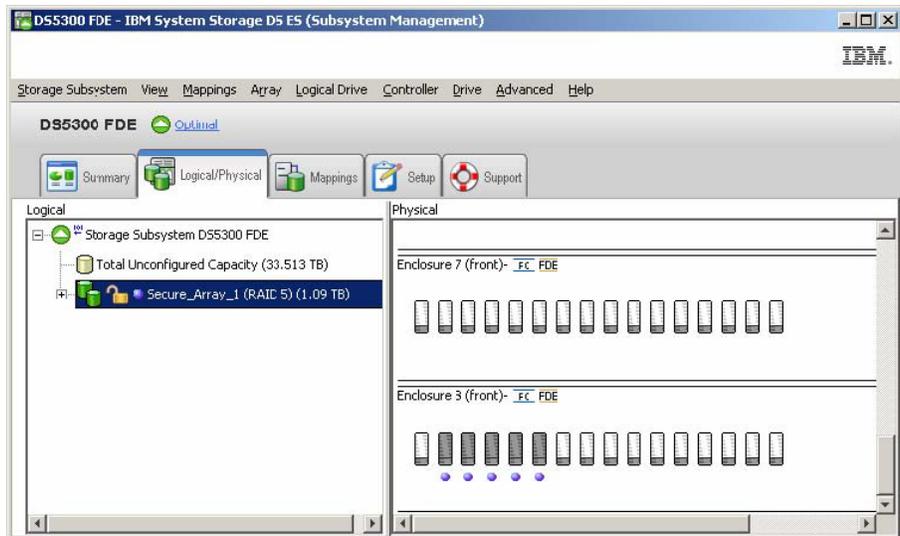


7. En la ventana Matriz creada, pulse **Aceptar** para reconocer la creación correcta de la matriz.

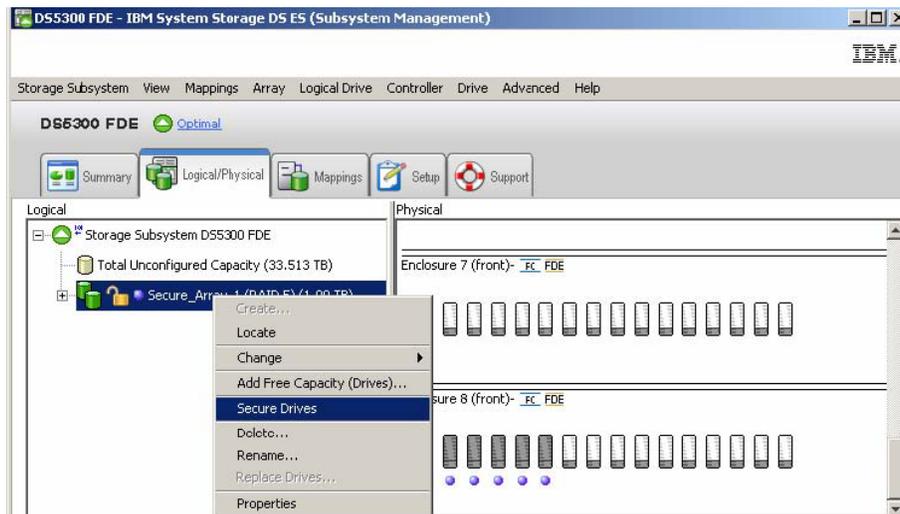


8. Cuando el asistente le pida que cree unidades lógicas en la matriz, utilice el asistente para crear las unidades lógicas. Una vez creadas las unidades lógicas, continúe al paso siguiente. Consulte Capítulo 4, "Configuración del almacenamiento", en la página 65 para obtener más información sobre la creación de unidades lógicas.
9. Asegure la matriz que ha creado:
 - a. En la ventana Gestión del subsistema, pulse la pestaña **Lógica/Física**.

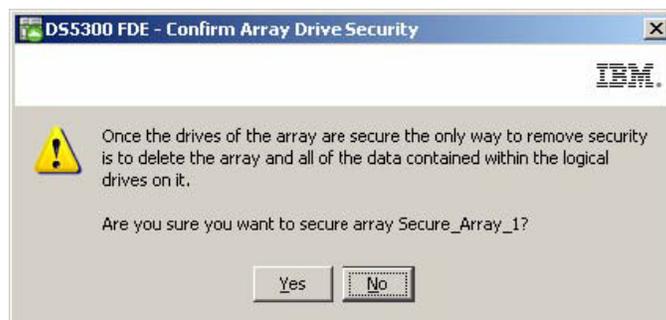
Nota: Los puntos azules bajo los iconos de disco del lado derecho de la ventana indican que discos componen la matriz.



- b. Para habilitar la seguridad en la matriz, pulse con el botón derecho en el nombre de la matriz; a continuación, pulse **Asegurar unidades**.



- c. En la ventana Confirmar seguridad de unidades de matriz, pulse **Sí** para asegurar la matriz.

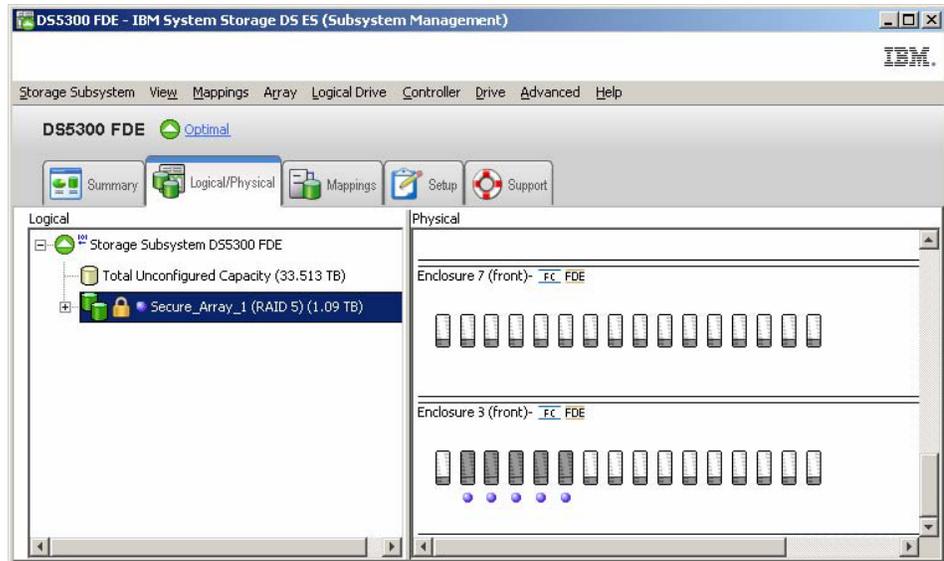


Nota:

- 1) Si mueve una unidad a un subsistema de almacenamiento distinto o si cambia la clave de seguridad más de dos veces en el subsistema de almacenamiento actual mientras la unidad no se encuentra en el

mismo, deberá facilitar la frase de contraseña, la clave de seguridad y el archivo de claves de seguridad para desbloquear la unidad y hacer que los datos sean legibles.

- 2) Una vez asegurada una matriz, la única forma de eliminar la seguridad es suprimiendo dicha matriz. Puede realizar un VolumeCopy de la matriz y guardarlo en otros discos para poder seguir accediendo a los datos.
10. En la ventana Gestión del subsistema, pulse la pestaña **Lógica/Física** y observe que la matriz está asegurada, como indica el símbolo del candado situado a la izquierda del nombre de la matriz.



Desbloqueo de unidades de disco

Las unidades FDE con seguridad habilitada se bloquean cuando se corta la alimentación o cuando se retiran del subsistema de almacenamiento. Esta es una característica importante del cifrado de disco de los subsistemas de almacenamiento y las unidades FDE; el estado bloqueado hace que los usuarios no autorizados no puedan leer los datos.

Importante: Si el subsistema de almacenamiento está en modo de gestión de claves externa y no hay una unidad no FDE óptima o unidad FDE no asegurada en la configuración del subsistema, debe proporcionar el archivo de seguridad y su frase de contraseña asociada para desbloquear las unidades con el fin de que el subsistema de almacenamiento se reinicie correctamente.

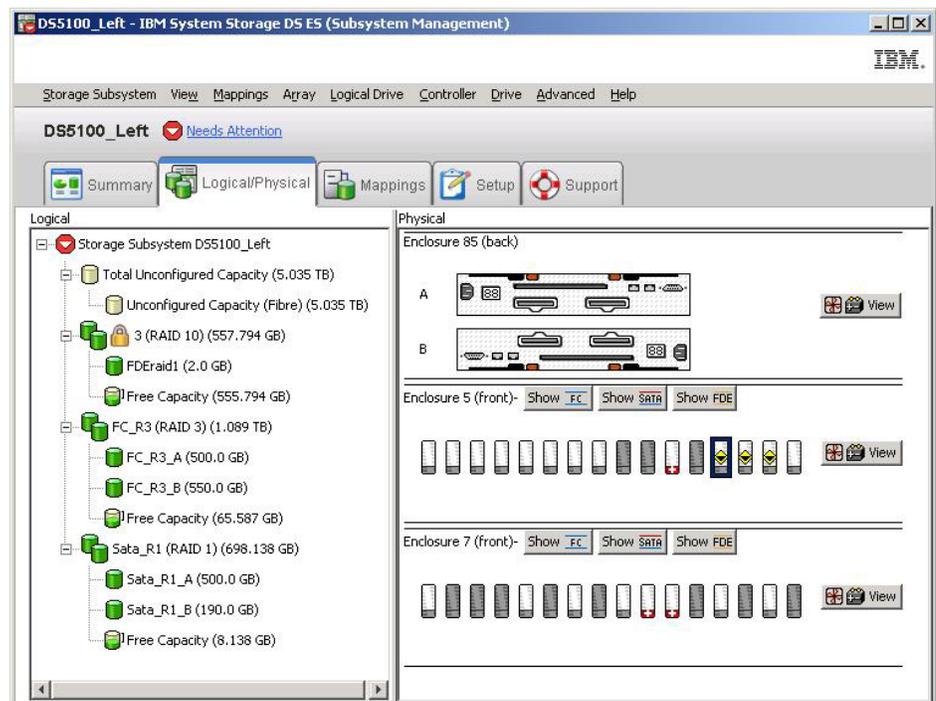
Las condiciones que hacen que una unidad FDE se bloquee varían dependiendo del tipo de gestión de claves de seguridad que utilice. Con la gestión de claves de seguridad local, las claves se almacenan dentro del controlador. Dado que los controladores siempre guardan una copia de las claves de seguridad anteriores y la actual, el archivo de claves de seguridad no es necesario cada vez que se conecte la alimentación del subsistema de almacenamiento o se retire una unidad y se reinserte en el mismo subsistema de almacenamiento. No obstante, si mueve una unidad a otro subsistema de almacenamiento o si cambia la clave de seguridad más de dos veces en el subsistema de almacenamiento actual mientras la unidad no se encuentra en el mismo, deberá facilitar la frase de contraseña y el archivo de claves de seguridad para desbloquear la unidad.

Nota: Las unidades FDE con seguridad habilitada permanecen desbloqueadas hasta que se actualiza el firmware o mientras se sustituyen componentes. El único caso en que estas unidades están bloqueadas es cuando se apagan o retiran del subsistema de almacenamiento.

Con la gestión de claves de seguridad externa, la aplicación de gestión de claves externa proporciona la clave de seguridad para desbloquear una unidad que se haya movido de un subsistema original a un subsistema nuevo, siempre que dicha aplicación pueda acceder al subsistema nuevo. Para desbloquear la unidad movida, el nuevo subsistema debe estar conectado a la aplicación de gestión de claves externa. Si se interrumpe la comunicación entre la aplicación de gestión de claves externa y el subsistema de almacenamiento, las unidades no se podrán desbloquear hasta que dicha comunicación se restablezca o hasta que las unidades se desbloqueen con la copia del archivo de claves de seguridad.

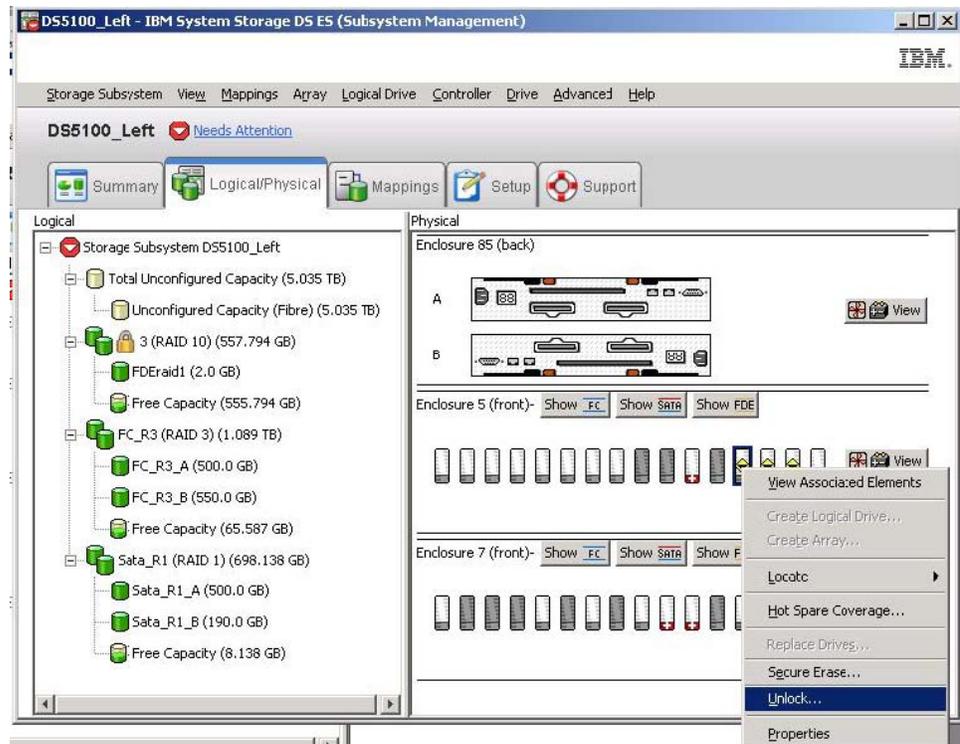
Para desbloquear una unidad FDE bloqueada con la copia del archivo de claves de seguridad, complete los pasos siguientes:

1. En la ventana de Gestión del subsistema, pulse en la pestaña **Lógica/Física**.



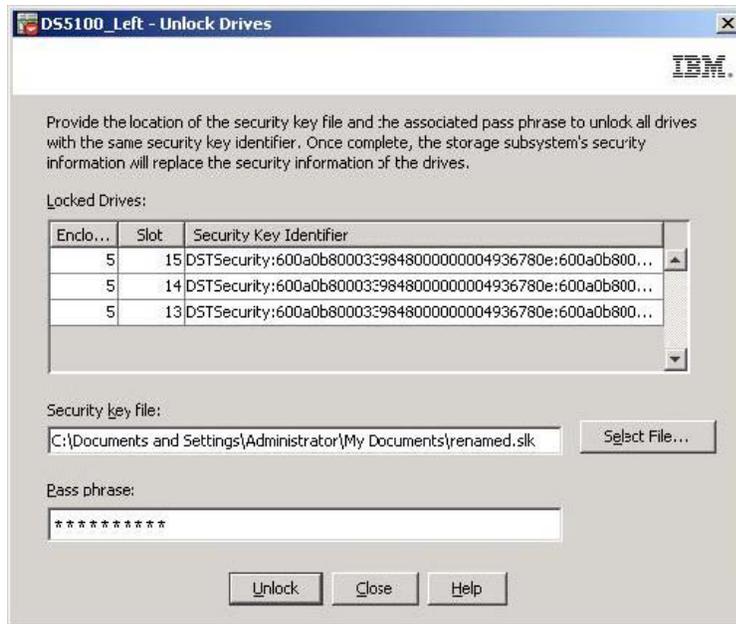
2. Pulse con el botón derecho en las unidades que desea desbloquear y después pulse **Desbloquear**.

Nota: Si desea desbloquear varias unidades, sólo tiene que seleccionar una unidad. Storage Manager mostrará automáticamente todas las unidades bloqueadas en el subsistema de almacenamiento y comprobará cada unidad contra el archivo de claves de seguridad proporcionado para determinar si puede utilizar la clave de dicho archivo.



3. En la ventana Desbloquear unidades, se mostrarán las unidades bloqueadas seleccionadas. Para desbloquear estas unidades, seleccione el archivo de claves de seguridad, especifique la frase de contraseña y pulse **Desbloquear**. El subsistema de almacenamiento utiliza la frase de contraseña para descifrar la clave de seguridad del archivo de claves de seguridad. A continuación, el subsistema de almacenamiento compara la clave de seguridad descifrada con la clave de seguridad de la unidad y desbloquea todas las unidades cuya contraseña coincida.

Nota: El proceso de autenticación solo se realiza cuando una unidad está en estado Bloqueado porque la unidad se ha encendido tras un evento de falta de alimentación. No se repite con cada operación de lectura y escritura.



4. En la ventana Desbloqueo de unidades completo, pulse **Aceptar** para confirmar el desbloqueo de las unidades. Las unidades desbloqueadas ahora están listas para importarse.



Migración de subsistemas de almacenamiento (intercambio de cabezal) con unidades FDE

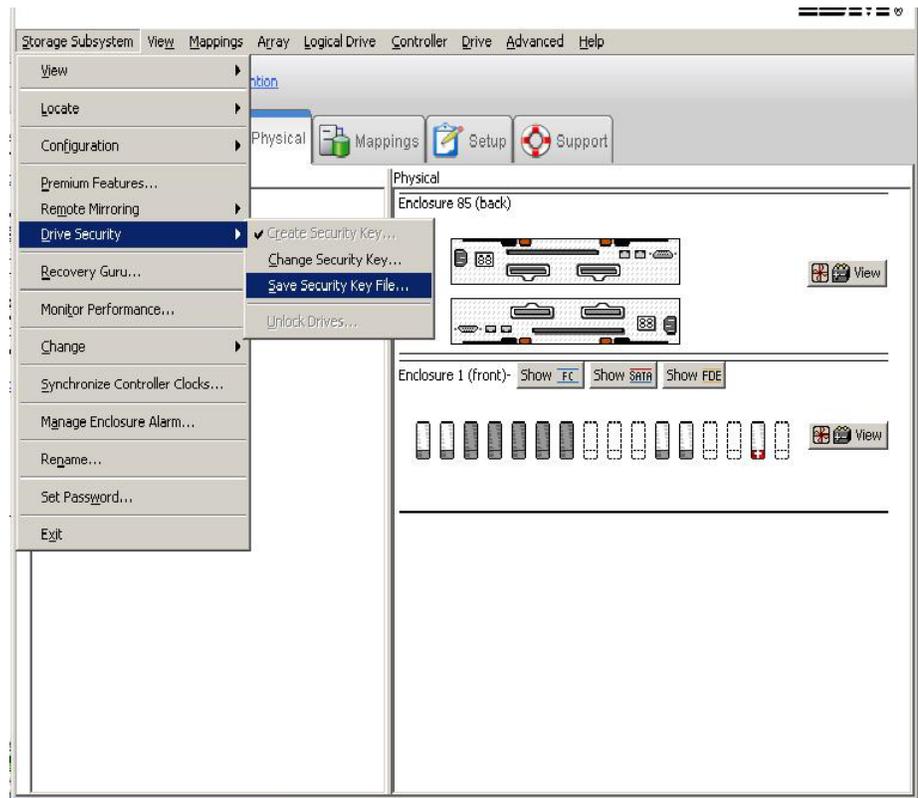
Con los subsistemas de almacenamiento compatibles con FDE, puede migrar unidades como un subsistema de almacenamiento completo a otro subsistema de almacenamiento compatible con FDE utilizando las técnicas de migración de grupos de discos existentes. Los datos del usuario permanecen intactos en los discos ya que los metadatos de configuración se almacenan en todas las unidades del subsistema de almacenamiento. Las unidades FDE con seguridad habilitada también se pueden migrar y pueden permanecer protegidas llevando a cabo algunos pasos adicionales, que se describen en esta sección.

Nota:

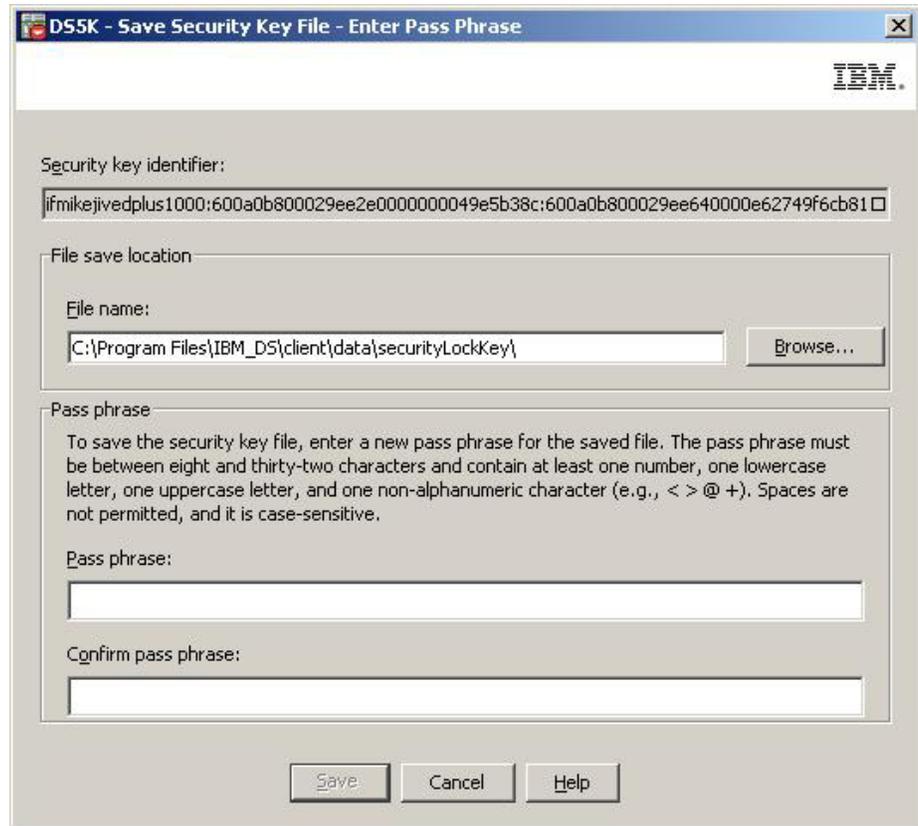
1. El siguiente procedimiento describe solo los pasos de migración de datos adicionales necesarios para las matrices aseguradas. Para conocer la información y procedimientos completos, consulte la *IBM System Storage DS3000, DS4000, or DS5000 Hard Drive and Storage Expansion Enclosure Installation and Migration Guide*.
2. Los siguientes pasos de migración de datos también se aplican cuando sustituye ambos controladores en un subsistema de almacenamiento. Se debe

incluir todas las unidades del subsistema de almacenamiento. Cuando sustituye ambos controladores, no puede realizar migraciones parciales. En este caso es necesario un archivo de seguridad; si se deben sustituir ambos controladores puede no tener acceso de gestión al subsistema de almacenamiento para exportar la clave de seguridad actual.

1. Guarde la clave de seguridad utilizada para desbloquear las unidades del subsistema de almacenamiento existente en un archivo de claves de seguridad antes de retirar las unidades del subsistema de almacenamiento. Tras exportar la clave de seguridad, frase de contraseña y archivo de claves de seguridad, dicho archivo se puede transferir de un subsistema de almacenamiento a otro.
 - a. En la ventana de Gestión del subsistema, pulse en **Subsistema de almacenamiento**, pulse en **Seguridad de unidad** y pulse en **Guardar archivo de clave de seguridad**.

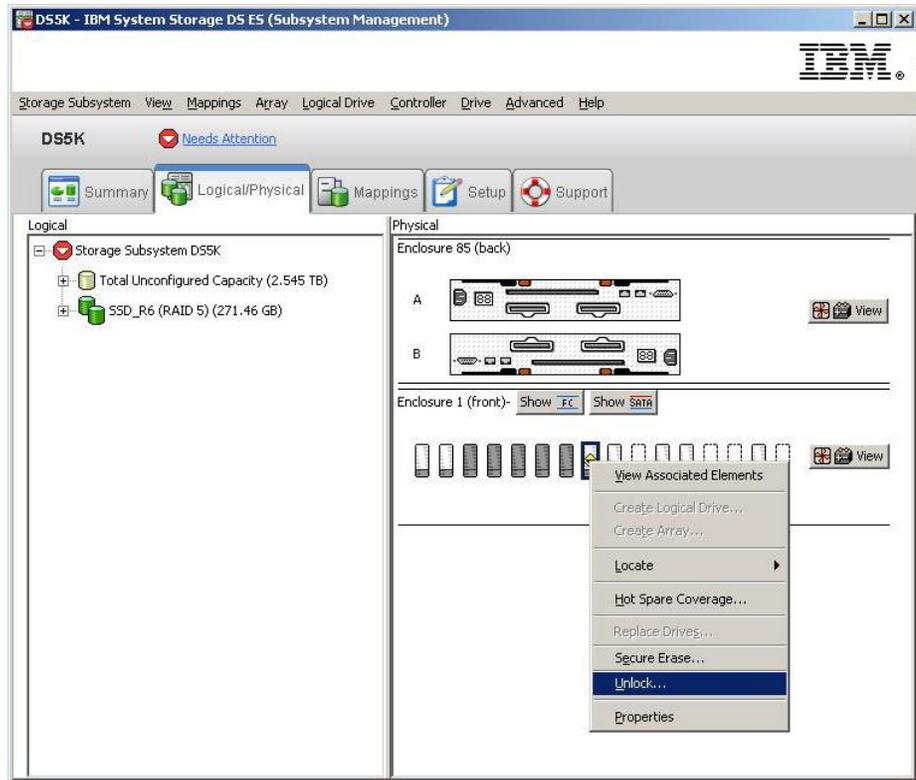


- b. En Guardar archivo de claves de seguridad - Entre en la ventana frase de contraseña, seleccione una ubicación para guardar el archivo y escriba y confirme la frase de contraseña, después pulse en **Guardar**.

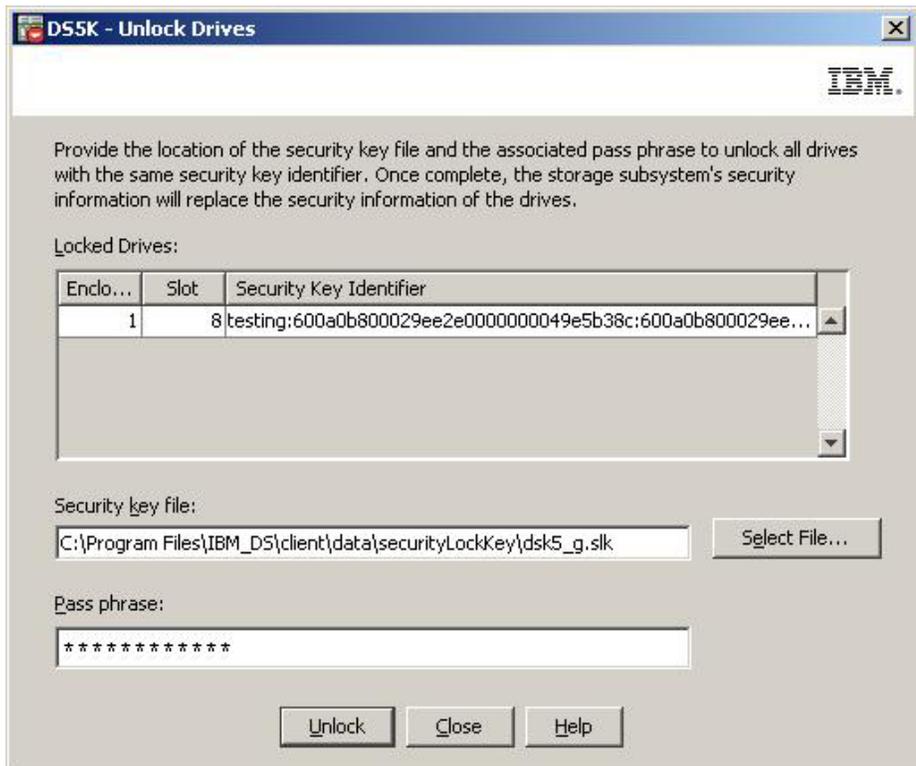


- c. Exporte las matrices definidas en el subsistema de almacenamiento original.
 - d. Apague el subsistema y sustituya el antiguo alojamiento del controlador del subsistema de almacenamiento por el alojamiento del controlador.
 - e. Encienda en nuevo subsistema de almacenamiento.
2. Tras sustituir el alojamiento del controlador del subsistema de almacenamiento existente por un nuevo alojamiento de controlador, desbloquee las unidades FDE con seguridad habilitada antes de importar las matrices RAID:
- a. Pulse la pestaña **Lógica/Física** en la ventana Gestión del subsistema.
 - b. Pulse con el botón derecho en las unidades que desea desbloquear y después pulse **Desbloquear**.

Nota: La característica premium Cifrado de disco completo podría no funcionar. Genere el nuevo archivo de claves de características premium FDE para habilitar la funcionalidad FDE del subsistema de almacenamiento.



- c. Seleccione el archivo de claves de seguridad para las unidades seleccionada, escriba la frase de contraseña que escribió cuando guardó el archivo de copia de seguridad de la clave de seguridad; después, pulse en **Desbloquear**.



Borrado de unidades de disco

Atención: Todos los datos del disco se borrarán de manera permanente cuando se complete la operación de borrado seguro en una unidad de FDE con seguridad habilitada. No lleve a cabo esta acción a menos que esté seguro de que desea eliminar los datos.

El borrado seguro proporciona un nivel de borrado de datos más alto que otros métodos tradicionales. Cuando inicia el borrado seguro con Storage Manager, se envía un comando a la unidad de FDE para que realice un borrado criptográfico. El borrado criptográfico borra la clave de cifrado de datos existente y genera una nueva clave de cifrado en la unidad, haciendo imposible descifrar los datos. Una vez que haya cambiado la clave de cifrado, todos los datos grabados en el disco y cifrados con la clave de cifrado anterior pasarán a ser ilegibles. Esto incluye todos los bits, cabeceras y directorios.

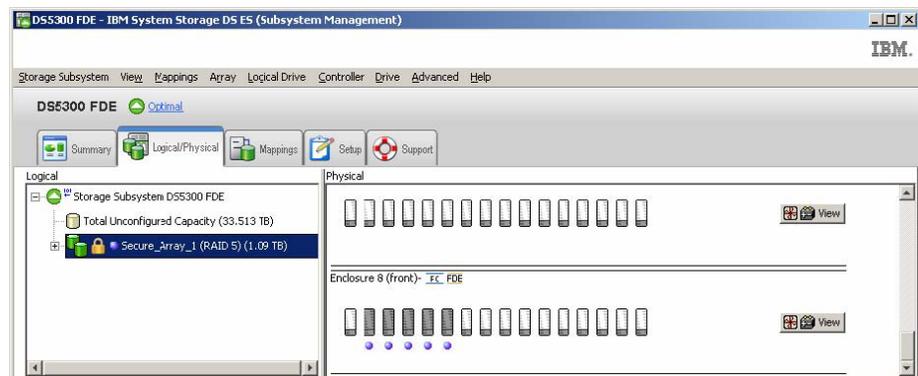
Tras el borrado de datos en la unidad, se producen las siguientes acciones:

- Los datos pasan a ser completa y permanentemente inaccesibles y la unidad vuelve al estado original de fábrica.
- La seguridad de la unidad se deshabilita y debe ser rehabilitada si fuera necesario.

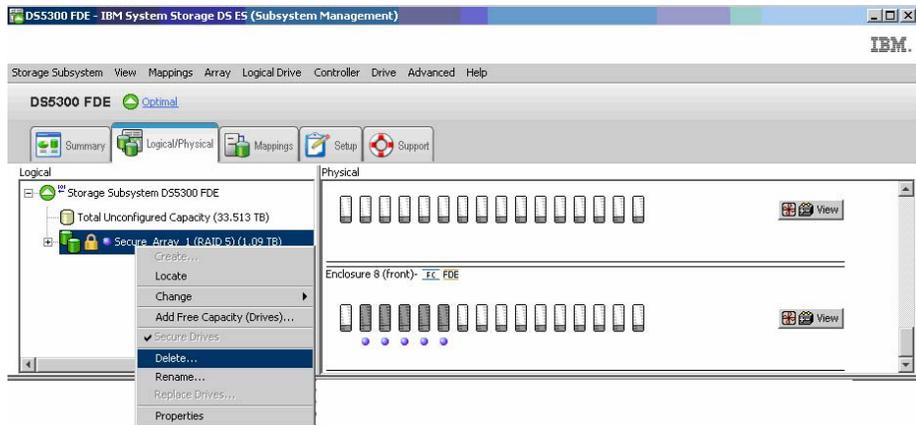
Antes de iniciar un borrado seguro, debe desbloquear la unidad de FDE con seguridad habilitada y debe suprimirse la matriz a la que está asignada.

Atención: Si desea acceder a los datos más adelante, debe realizar una copia de seguridad de los datos de las unidades de FDE con seguridad habilitada en otras unidades o cintas antes de realizar el borrado seguro de las mismas. Todos los datos del disco se borrarán de manera permanente cuando se complete la operación de borrado seguro en una unidad de FDE con seguridad habilitada. No lleve a cabo esta acción a menos que esté seguro de que desea eliminar los datos. El uso indebido del borrado seguro resultará en la pérdida de datos.

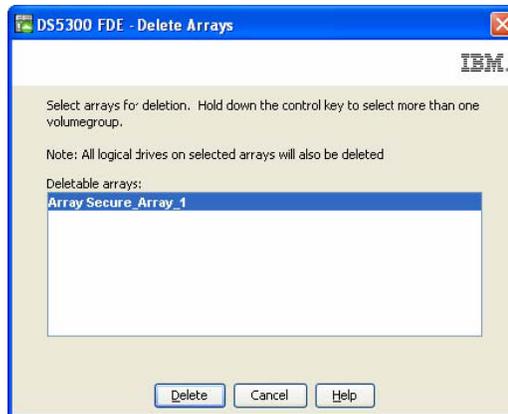
1. Antes de poder realizar el borrado seguro de las unidades, debe suprimir la matriz RAID con la que están asociadas las unidades y devolver dichas unidades a estado Sin asignar:
 - a. Pulse en la pestaña **Lógica/física** en la ventana de Gestión del Subsistema.



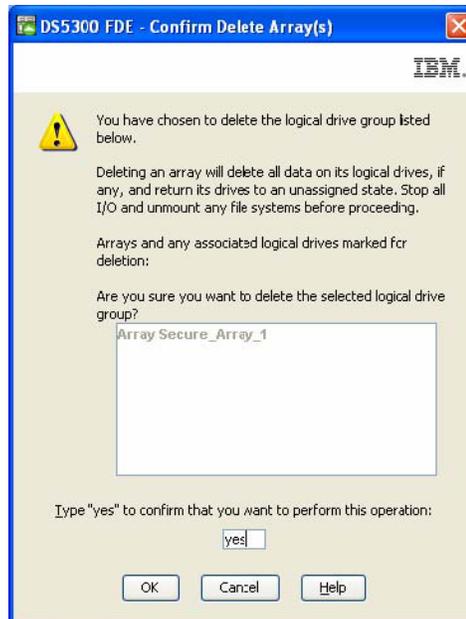
- b. Pulse con el botón derecho en el nombre de matriz, después pulse en **Eliminar**.



- c. Cuando se le solicite, seleccione la matriz que quiere suprimir, pulse en el nombre de matriz y pulse en **Suprimir**.

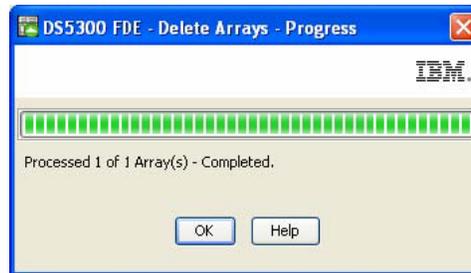


- d. Para confirmar que desea suprimir la matriz, introduzca sí en el campo y pulse **Aceptar**.

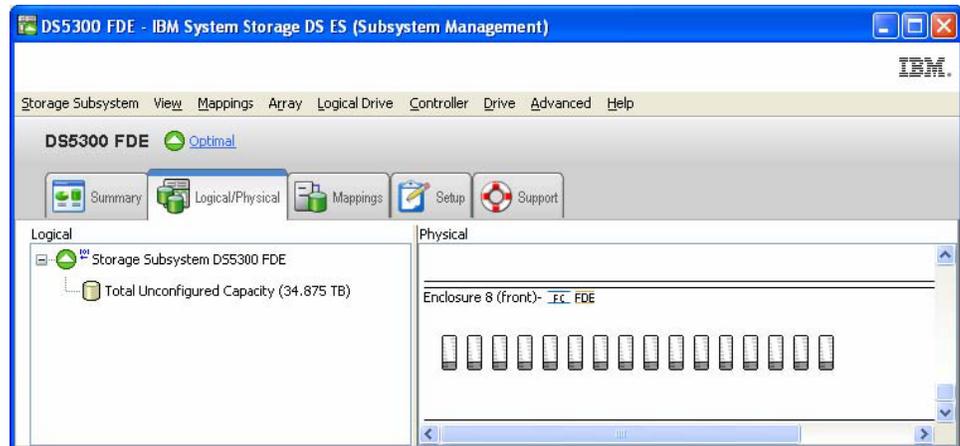


- e. Espere hasta que se haya completado el proceso de supresión de la matriz. Cuando reciba la confirmación Processed 1 of array(s) – Complete, pulse

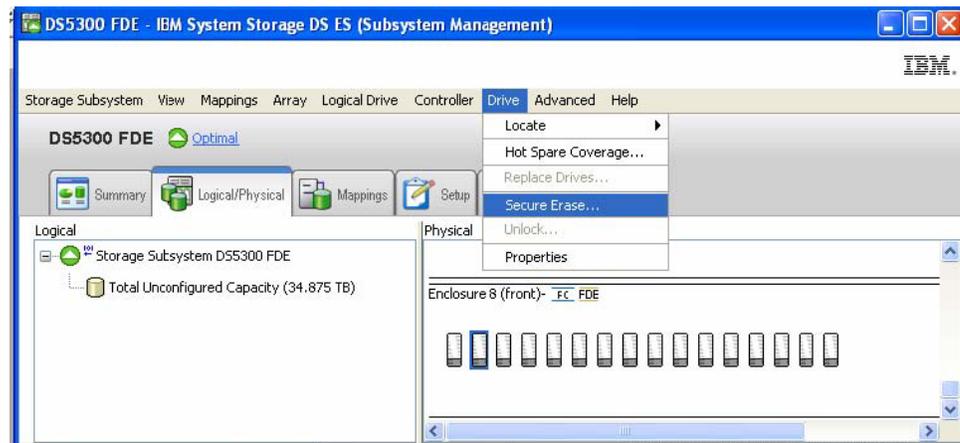
en **Aceptar**.



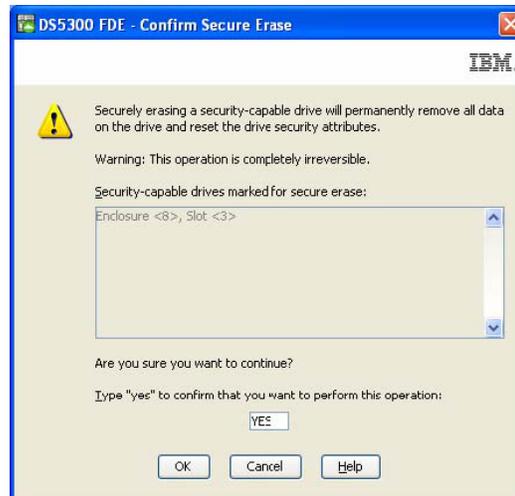
2. Pulse en la pestaña **Lógica/física** en la ventana de Gestión del Subsistema.



3. Seleccione la unidad en la que desea realizar el borrado seguro. Puede seleccionar más de una unidad manteniendo pulsada la tecla Ctrl. En la barra de menú superior, pulse **Unidad**; después pulse **Borrado seguro**.



4. Para confirmar que desea suprimir la matriz, introduzca **sí** en el campo y pulse **Aceptar**. Estas unidades se pueden utilizar para otros fines o descartarse.



Unidades de disco de reserva activo globales

Si una unidad de disco falla en un subsistema de almacenamiento compatible con FDE, el controlador utiliza datos redundantes para reconstruir los datos de la unidad que ha fallado en una unidad de reserva activa global. La unidad de reserva activa global se sustituye automáticamente por la unidad que ha fallado sin intervención. Cuando la unidad que ha fallado se sustituye, los datos de la unidad de reserva se copian en la unidad de sustitución.

Las unidades de reserva activa debe cumplir los requisitos de reserva de la matriz. Cuando se configuran matrices con capacidad de seguridad, se requieren los siguientes tipos de unidad como unidad de reserva. Si una unidad falla, Storage Manager determina automáticamente qué unidad de reserva debe sustituirla de acuerdo con el tipo de la unidad que ha fallado.

- Para matrices con unidades FDE aseguradas, las unidades de reserva deben ser unidades FDE no aseguradas con la misma o mayor capacidad. Una vez que la unidad de reserva FDE no asegurada se utiliza como reserva de una unidad fallida de la matriz RAID asegurada, se le habilitará su seguridad.
- Para matrices con unidades FDE no aseguradas, las unidades de reserva pueden ser unidades FDE no aseguradas o unidades no FDE.

Nota: Si una unidad de reserva FDE no asegurada se ha utilizado como reserva de una matriz FDE no asegurada y la matriz se ha asegurado una vez copiados los datos, la unidad de reserva FDE no asegurada sigue sin asegurar, dejando los datos expuestos en caso de ser retirada del subsistema de almacenamiento.

Una unidad FDE asegurada sin configurar no puede utilizarse como unidad de reserva global. Si una unidad de reserva global es una unidad FDE asegurada, se puede utilizar como unidad de reserva solo en matrices aseguradas. Si una unidad de reserva global es una unidad FDE no asegurada, se puede utilizar como unidad de reserva en matrices aseguradas o no aseguradas con unidades FDE o no FDE. Debe realizar el borrado seguro de la unidad FDE para cambiarla a estado No asegurado antes de poder utilizarla como unidad de reserva global. Si asigna una unidad FDE asegurada sin configurar como unidad de reserva global, se generará el siguiente mensaje de error.

Código de retorno: Error 2 - La operación no se puede completar porque (1) el estado actual de un componente no permite que se complete la operación,

(2) la operación se ha inhabilitado en NVSRAM (por ejemplo, está modificando los parámetros de exploración de medios cuando esa opción (desplazamiento 0x31, bit 5) está inhabilitada), o (3) existe un problema con el subsistema de almacenamiento. Por favor, compruebe el subsistema de almacenamiento y sus diversos componentes en busca de posibles problemas y reintente la operación. Operación al producirse el error:
PROC_assignSpecificDrivesAsHotSpares

Cuando se utiliza una unidad de reserva global como reserva de una unidad fallida de una matriz asegurada, esta pasa a ser una unidad FDE asegurada y sigue estándolo siempre que sea reserva en la matriz asegurada. Tras sustituir una unidad fallida de la matriz asegurada y copiar los datos de la unidad de reserva global en la unidad de sustitución, los controladores reaprovisionan automáticamente la unidad de reserva global para que se convierta en unidad de reserva global FDE no asegurada .

La práctica más adecuada en entornos de disco mixtos que incluyan unidades SATA y de canal de fibra sin capacidad de seguridad, y unidades de canal de fibra FDE (con seguridad habilitada o no habilitada), es utilizar al menos un tipo de unidad de reserva global (unidad SATA y canal de fibra FDE) con la mayor capacidad de la matriz. Si se incluye una unidad de reserva SATA y de canal de fibra FDE con capacidad de seguridad, todas las matrices estarán protegidas.

Siga las directrices de configuración de unidades de reserva estándar indicadas en “Configuración de unidades de repuesto en caliente globales” en la página 92). Las directrices de configuración de unidades de reserva estándar son las mismas para las unidades FDE.

Archivos de registro

El registro de eventos principal (MEL) de Storage Manager incluye mensajes que describen los cambios de seguridad realizados en el subsistema de almacenamiento.

Preguntas frecuentes

Esta sección incluye las preguntas más frecuentes sobre FDE. Las preguntas y respuestas se organizan en las siguientes categorías:

- “Seguridad de matrices”
- “Borrado seguro” en la página 268
- “Gestión local de claves de seguridad” en la página 269
- “Gestión externa de claves de seguridad” en la página 269
- “Características premium” en la página 269
- “Unidades de repuesto en caliente globales” en la página 270
- “Soporte de arranque” en la página 270
- “Estados bloqueado y desbloqueado” en la página 270
- “Copia de seguridad y recuperación” en la página 271
- “Otras” en la página 271

Seguridad de matrices

- ¿Puedo convertir una matriz no asegurada con unidades FDE en una matriz asegurada?

- Sí. Los pasos para completar este proceso se describen en “Seguridad de una matriz RAID” en la página 250. La característica de cifrado de DS5000 debe estar habilitada y se han debido establecer el archivo de claves de seguridad y la frase de contraseña. Consulte “Habilitación de características premium” en la página 242 para obtener más información.
- Al habilitar la seguridad en una matriz, ¿perderé o se borrarán los datos grabados anteriormente en esa matriz?
 - No. A menos que realice un borrado seguro de las unidades de disco de la matriz los datos permanecerán intactos.
- ¿Puedo convertir una matriz asegurada con unidades FDE en una matriz no asegurada?
 - No. No es una opción soportada. Cuando convierte una matriz no asegurada en matriz asegurada, no puede convertirla de nuevo en no asegurada sin destruir los datos de las unidades FDE con seguridad habilitada. Utilice VolumeCopy para copiar los datos asegurados en una matriz no asegurada o realice una copia de seguridad de los datos en una cinta segura. Si utiliza VolumeCopy para copiar los datos asegurados en una matriz no asegurada, debe asegurar las unidades físicamente. A continuación, debe suprimir la matriz original y realizar un borrado seguro de las unidades de la matriz. Cree una nueva matriz no asegurada con estas unidades y utilice VolumeCopy para copiar los datos de nuevo en las unidades originales, o restaure los datos de la cinta segura.
- Si tengo una matriz con unidades FDE asegurada, ¿puedo crear otra matriz que utilice las mismas unidades y no habilitar la seguridad? ¿El subsistema de almacenamiento tiene control para que esto no ocurra?
 - No. No son funciones compatibles. Todas las unidades lógicas que formen parte de una matriz deben estar aseguradas porque las unidades en las que están almacenadas están aseguradas.
- Cuando se suprime una matriz, ¿la seguridad del disco permanece habilitada?
 - Sí. La única forma de inhabilitar la seguridad es realizar un borrado seguro o reaprovisionar las unidades.
- Si creo una nueva matriz en un conjunto de discos FDE con seguridad habilitada sin asignar/sin configurar, ¿pasarán a ser seguros automáticamente?
 - Sí.

Borrado seguro

- ¿Qué puedo borrar con el borrado seguro, una unidad individual o una matriz?
 - El borrado seguro se lleva a cabo en una unidad individual. No puede borrar una unidad asegurada que forme parte de una matriz; antes debe suprimir la matriz. Una vez suprimida la matriz, las unidades pasan a no tener asignación y puede borrar diversos discos con la misma operación manteniendo pulsada la tecla Ctrl mientras selecciona las unidades en las que desea realizar el borrado seguro.
- Si solo quiero utilizar la característica de borrado seguro, ¿tengo que configurar un identificador de clave de seguridad y una frase de contraseña?
 - Sí. La característica de cifrado de disco completo debe habilitarse para poder utilizar el borrado seguro.
- Una vez realizado el borrado seguro en una unidad, ¿la seguridad de esa unidad está habilitada o inhabilitada?
 - Tras el borrado seguro la unidad vuelve al estado Con capacidad de seguridad (no asegurada). La seguridad de la unidad se inhabilita.

- Si realizo el borrado seguro en una unidad sin darme cuenta, ¿es posible recuperar los datos de la unidad?
 - No. Cuando se realiza el borrado seguro, los datos de la unidad no se pueden recuperar. Debe recuperar los datos perdidos de una copia de seguridad. Realice una copia de seguridad en unidades aseguradas antes de realizar el borrado seguro de unidades.

Gestión local de claves de seguridad

- ¿Puedo hacerme con las claves de seguridad a través de Storage Manager o del controlador?
 - No. Las claves de seguridad se ocultan en el subsistema de almacenamiento. Solo se puede exportar una versión cifrada de la clave a un archivo de claves de seguridad utilizando la operación para guardar dichas claves. La clave de seguridad real no está disponible para ser vista. Implemente características de seguridad prudentes para el subsistema de almacenamiento. Storage Manager obliga a tener una contraseña sólida, pero el acceso del administrador debe tener controles rigurosos.
- Si pierdo una unidad desbloqueada o con la seguridad inhabilitada, ¿se puede acceder a los datos aunque estén cifrados?
 - Sí. Dado que no se ha habilitado la seguridad en la unidad, esta permanece desbloqueada y se puede acceder a los datos.
- Si mi clave de seguridad cae en las manos equivocadas, ¿puedo cambiarla sin perder mis datos?
 - Sí. Puede cambiar la clave de la unidad utilizando el procedimiento de cambio de claves de seguridad.

Gestión externa de claves de seguridad

- ¿En qué se diferencia la gestión externa de claves de seguridad de la gestión local?
 - En lugar de utilizar la clave de seguridad almacenada y oculta en un controlador del subsistema de almacenamiento, la gestión externa utiliza una ubicación de claves central de su red para gestionar las claves de diferentes subsistemas de almacenamiento. La gestión externa de claves de seguridad se realiza mediante un software de gestión de licencias de claves externo como IBM Tivoli Key Lifecycle Manager (TKLM). Si aún no tiene este software, debe adquirirlo, instalarlo y configurar el servidor proxy para configurar la gestión externa de claves de seguridad.
- ¿Necesito acceso al archivo de seguridad guardado cuando cambio unidades aseguradas de un subsistema de almacenamiento a otro?
 - No. Si el nuevo subsistema de almacenamiento está conectado y es reconocido por el servidor proxy y el software de gestión externa de claves de seguridad, el software proporciona la clave de seguridad para desbloquear la unidad automáticamente.
- ¿Por qué el subsistema de almacenamiento requiere la provisión manual de la clave de seguridad desde el archivo de claves tras un ciclo de alimentación del subsistema?
 - El subsistema no tiene al menos una unidad no FDE instalada.

Características premium

- ¿Cómo puedo estar seguro de que los datos duplicados están seguros? ¿Cuál es la mejor forma de proteger los datos en mi sitio remoto?

- Asegure sus datos con unidades FDE con seguridad habilitada tanto en el sitio primario como en el secundario. Además, debe asegurarse de que los datos están protegidos mientras se transfieren entre el sitio primario y secundario.
- ¿Puedo utilizar VolumeCopy para copiar un número de unidad lógica asegurado a uno no asegurado? De ser así, ¿qué evita que se haga esto primero y después se robe la copia no asegurada?
 - Sí. Para evitar que alguien robe sus datos con este método, implemente características de seguridad prudentes para el subsistema de almacenamiento DS5000. Storage Manager obliga a tener una contraseña sólida, pero el acceso del administrador debe tener controles rigurosos.
- ¿Se pueden asegurar datos de FlashCopy y VolumeCopy?
 - Sí. Para FlashCopy, la unidad lógica de repositorio FlashCopy se debe asegurar si los datos FlashCopy de destino están asegurados. Storage Manager impone esta regla. De forma similar, si la matriz de origen de VolumeCopy está asegurada, la matriz de destino de VolumeCopy también deberá estarlo.

Unidades de repuesto en caliente globales

- ¿Puedo utilizar una unidad FDE como unidad de repuesto en caliente global?
 - Sí, pero solo si la unidad no está asegurada (seguridad no habilitada). Compruebe el estado de la unidad FDE sin configurar. Si la unidad está asegurada, debe realizar el borrado seguro o reaprovisionamiento antes de poder utilizarla como unidad de repuesto en caliente global.
- Si la unidad de repuesto en caliente de una matriz asegurada es una unidad FDE no asegurada, ¿esta unidad pasa a estar asegurada automáticamente cuando falla una unidad FDE y los datos se escriben en la unidad de repuesto en caliente?
 - Sí. Cuando la unidad errónea se retira del grupo RAID, automáticamente se inicia una reconstrucción en la unidad de repuesto en caliente. Antes de iniciar la reconstrucción, se habilita la seguridad en la unidad de repuesto en caliente. En una unidad no FDE no se puede iniciar una reconstrucción de una matriz asegurada. Una vez sustituida la unidad errónea de una matriz asegurada y cuando se han copiado los datos de la unidad de repuesto en caliente global en la unidad de sustitución, los controladores reaprovisionan automáticamente dicha unidad de repuesto para convertirla en una unidad de repuesto en caliente global FDE asegurada.

Soporte de arranque

- ¿Existe algún proceso especial para arrancar desde una unidad con seguridad habilitada?
 - No. El único requisito es que el subsistema de almacenamiento debe estar en ejecución (necesario en cualquier proceso de arranque).
- ¿Las unidades FDE son susceptibles de ataques de arranque en frío?
 - No. Este problema afecta más al lado servidor, ya que un individuo puede crear una imagen de arranque para obtener acceso al servidor. Esto no ocurre con las unidades FDE. Las unidades FDE no utilizan un tipo de memoria susceptible al ataque de arranque en frío.

Estados bloqueado y desbloqueado

- ¿Cuándo pasa una unidad con seguridad habilitada al estado Bloqueado?

- La unidad pasa a estar bloqueada cuando se apaga el disco. Si se apaga o desconecta una unidad FDE, esta bloquea automáticamente los datos del disco.

Copia de seguridad y recuperación

- ¿Cómo puedo estar seguro de que los datos archivados están seguros?
 - La seguridad de los datos archivados no entra dentro de los temas de este documento. Consulte las directrices de la Storage Networking Interface Association (SNIA) para saber cómo realizar copias de seguridad de cintas. Para conocer referencias específicas, consulte el documento *IBM Full Disk Encryption Best Practices*. Para acceder a este documento desde el sitio web de IBM, vaya a <http://www-947.ibm.com/support/entry/portal/docdisplay?indocid=MIGR-5081492&brandind=5000028>, o complete los pasos siguientes:
 1. Vaya al Portal de soporte de IBM en <http://www.ibm.com/support/entry/portal>.
 2. En el campo **Search within all of support & downloads** de la parte inferior de la página, escriba FDE y pulse Intro.
 3. En la lista de resultados de la búsqueda, pulse el enlace **IBM Full Disk Encryption Best Practices - IBM System Storage**.
 4. Pulse en el enlace del archivo de FDE para abrir o descargar el documento *IBM Full Disk Encryption Best Practices*.

Otras

- ¿La información DACstore se sigue escribiendo en el disco?
 - Sí.No obstante, si la unidad está asegurada, debe ser desbloqueada por el controlador para poder leer la información DACstore. En el extraño caso de que la clave de seguridad del controlador esté corrupta o se sustituyan ambos controladores, debe utilizar un archivo de claves de seguridad para desbloquear la unidad.
- ¿Los datos de la memoria caché de los controladores están seguros con FDE y el cifrado de disco de IBM? De no ser así, ¿existen otras prácticas mejores al respecto?
 - No. Se trata de una cuestión de seguridad del acceso físico al hardware. El administrador debe tener control físico y garantizar la seguridad del propio subsistema de almacenamiento.
- Si tengo discos con capacidad de seguridad pero no he adquirido la clave de la característica premium de cifrado de disco de IBM, ¿puedo reconocer discos con capacidad de seguridad desde la interfaz de usuario?
 - Sí.Esta información está disponible en diversas ventanas de la interfaz de Storage Manager.
- ¿Qué ocurre con la clasificación de datos?
 - Consulte las prácticas recomendadas de la SNIA para obtener información sobre la clasificación de datos. Para conocer referencias específicas, consulte el documento *IBM Full Disk Encryption Best Practices*. Para acceder a este documento desde el sitio web de IBM, vaya a <http://www-947.ibm.com/support/entry/portal/docdisplay?indocid=MIGR-5081492&brandind=5000028>, o complete los pasos siguientes:
 1. Vaya al Portal de soporte de IBM en <http://www.ibm.com/support/entry/portal>.

2. En el campo **Search within all of support & downloads** de la parte inferior de la página, escriba FDE y pulse Intro.
 3. En la lista de resultados de la búsqueda, pulse el enlace **IBM Full Disk Encryption Best Practices - IBM System Storage**.
 4. Pulse en el enlace del archivo de FDE para abrir o descargar el documento *IBM Full Disk Encryption Best Practices*.
- ¿Puedo utilizar tanto unidades FDE como no FDE si no aseguro las unidades?
 - Sí.No obstante, utilizar unidades tanto FDE como no FDE no supone un uso rentable de las unidades FDE. Una matriz con unidades tanto FDE como no FDE no se puede convertir en una matriz segura más adelante.
 - ¿Las unidades de disco FDE tienen menos capacidad utilizable porque los datos están cifrados o porque la capacidad se necesita para el motor y las claves de cifrado?
 - No. No existe diferencia de capacidad entre las unidades de disco FDE y no FDE (1 GB sin cifrar = 1 GB cifrado).

Capítulo 7. Resolución de problemas

Utilice la información de este capítulo para diagnosticar y solucionar problemas relacionados con Storage Manager. Para obtener información sobre la obtención de ayuda, servicios y otra asistencia técnica, consulte “Obtención de información, ayuda y servicios” en la página xvii.

En este capítulo se tratan estos temas:

- “Resolución de problemas de eventos críticos”
-
- “Captura de datos de diagnóstico (DCC) de DS” en la página 293
- “Resolución de errores de matriz de discos en AIX” en la página 296

Resolución de problemas de eventos críticos

Cuando se produce un evento crítico, se registra en el registro de eventos y se envía a todas las direcciones de correo electrónico y destinos de interrupción SNMP configurados. El tipo de evento crítico y la clave de detección, ASC y datos ASCQ se muestran en los detalles del registro de eventos.

Si se produce un evento crítico y planea llamar al soporte de IBM, puede utilizar la característica Paquete de soporte del cliente para recopilar y empaquetar los diversos fragmentos de datos, que pueden ser útiles en la resolución de problemas. Para utilizar la característica Paquete de soporte del cliente, complete los pasos siguientes:

1. En la ventana Gestión del subsistema de la unidad lógica que presenta problemas pulse **Avanzada > Resolución de problemas > Avanzada > Recopilar todos los datos de soporte**. Se abrirá la ventana Recopilar todos los datos de soporte.
2. Escriba el nombre del archivo en el que desea guardar todos los datos recopilados o examine para seleccionar el archivo. Pulse **Inicio**.

Nota: La creación del archivo comprimido puede tardar varios minutos, dependiendo de la cantidad de datos que deba recopilarse.

3. Cuando el proceso se haya completado, puede enviar el archivo comprimido de forma electrónica al soporte de IBM para la resolución de problemas.

Tabla 38 en la página 274 proporciona más información sobre eventos con prioridad crítica, como se muestra en el registro de eventos de la ventana Gestión del subsistema.

Tabla 38. Eventos críticos

Número de evento crítico	Clave de detección/ASC/ASCQ	Descripción del evento crítico y acción requerida
Evento 1001 - Fallo de canal	6/3F/C3	<p>Descripción: El controlador ha fallado un canal y ya no puede acceder a las unidades de este canal. El calificador de grupo FRU (byte 26) de los datos de detección indica el número de canal relativo del canal que ha fallado. Normalmente, esta condición está causada por una unidad que ignora el protocolo SCSI de uno de los canales de destino del controlador. El controlador falla un canal si emite un restablecimiento en un canal y continúa viendo a las unidades ignorar el restablecimiento de bus SCSI en este canal.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Canal SCSI de unidad fallado. Póngase en contacto con el soporte IBM para completar este procedimiento.</p>
Evento 1010 - Error de unidad inminente (PFA) detectado	6/5D/80	<p>Descripción: Una unidad ha informado de que se ha superado un umbral de predicción de errores. Esto indica que la unidad podría fallar en 24 horas.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Error de unidad inminente. Siga las instrucciones para corregir el error.</p>
Evento 1015 - Parámetros de modo incorrectos definidos en la unidad	6/3F/BD	<p>Descripción: El controlador no puede consultar a la unidad sus valores de página de modo crítico actuales o no puede cambiar estos valores por los valores adecuados. Esto indica que el bit Qerr está definido de manera incorrecta en la unidad especificada en el campo FRU de los datos de Solicitud de detección.</p> <p>Acción: El controlador aún no ha fallado. Póngase en contacto con el soporte de IBM para conocer las instrucciones para recuperarse de este evento crítico.</p>
Evento 1207 - Errores de enlace de canal de fibra - umbral superado	Ninguno	<p>Descripción: Se han detectado caracteres no válidos en la señal de canal de fibra. Entre las posibles causas del error se encuentran un láser degradado en un conversor de interfaz gigabit (GBIC) o adaptador de interfaz de soporte, cables de canal de fibra dañados o defectuosos, o conexiones de cables inadecuadas entre los componentes del bucle.</p> <p>Acción: En la ventana Gestión del subsistema, pulse Ayuda → Procedimientos de recuperación. Pulse Umbral de errores de enlace de canal de fibra superado para obtener más información sobre la recuperación de este error.</p>
Evento 1208 - Negociación de velocidad de datos fallida	Ninguno	<p>Descripción: El controlador no puede negociar automáticamente las velocidades de enlace de transferencia. El controlador considera el enlace caído hasta que se intenta la negociación durante el inicio de la jornada del controlador o cuando se detecta una señal tras la pérdida de señal.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Negociación de velocidad de datos fallida y siga las instrucciones para corregir el error.</p>

Tabla 38. Eventos críticos (continuación)

Número de evento crítico	Clave de detección/ASC/ASCQ	Descripción del evento crítico y acción requerida
Evento 1209 - Canal de unidad definido como Degradado	Ninguno	<p>Descripción: El estado de un canal de unidad se ha definido como Degradado debido a un número de errores de E/S excesivo o porque un representante de soporte técnico ha solicitado al administrador de matriz definir manualmente el estado del canal de unidad por motivos relacionados con el diagnóstico u otros motivos de soporte.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Canal de unidad degradado y siga las instrucciones para corregir el error.</p>
Evento 150E - Diagnóstico de bucle de retorno de controlador fallido	Ninguno	<p>Descripción: El controlador no puede inicializar los bucles de canal de fibra del lado unidad. Se ha ejecutado una rutina de diagnóstico y se ha identificado un problema en el controlador, y este se ha puesto fuera de línea. Este evento se produce solo en determinados modelos de controlador.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Controlador fuera de línea y siga las instrucciones para sustituir el controlador.</p>
Evento 150F - Cableado incorrecto de canal	Ninguno	<p>Descripción: Dos o más canales de unidad están conectados al mismo bucle de canal de fibra. Esto puede hacer que el subsistema de almacenamiento se comporte de manera imprevista.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Cableado incorrecto de canal y siga las instrucciones para corregir el error.</p>
Evento 1510 - Cableado incorrecto de blade de ESM	Ninguno	<p>Descripción: Dos blades de ESM del mismo alojamiento de expansión de almacenamiento están conectados al mismo bucle de canal de fibra. Se ha perdido un nivel de redundancia y el rendimiento de E/S de este alojamiento de expansión de almacenamiento se ha reducido.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Cableado incorrecto de blade de ESM y siga las instrucciones para corregir el error.</p>
Evento 1513 - Unidad individual - Ruta degradada	Ninguno	<p>Descripción: El canal de unidad especificado está experimentando errores intermitentes en la ruta hacia una o varias unidades.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Unidad individual - Ruta degradada y siga las instrucciones para corregir el error.</p>
Evento 1600 - Unidad sin certificar detectada	Ninguno	<p>Descripción: Se ha insertado una unidad sin certificar en el subsistema de almacenamiento.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Unidad sin certificar y siga las instrucciones para corregir el error.</p>

Tabla 38. Eventos críticos (continuación)

Número de evento crítico	Clave de detección/ASC/ASCQ	Descripción del evento crítico y acción requerida
Evento 1601 - No se pueden descubrir bloques reservados en unidades ATA	Ninguno	<p>Descripción: No se han reconocido los bloques reservados en unidades ATA.</p> <p>Acción: Póngase en contacto con el soporte de IBM para obtener instrucciones para la recuperación de este evento.</p>
Evento 200A - Falta de coincidencia de paridad/datos detectada en unidad lógica	Ninguno	<p>Descripción: Una operación de exploración de soportes ha detectado inconsistencias entre una porción de bloques de datos de la unidad lógica y los bloques de paridad asociados. Se podrían haber perdido datos del usuario de esta porción de la unidad lógica.</p> <p>Acción: Seleccione una herramienta específica de la aplicación (si está disponible) para verificar si los datos se encuentran en la unidad lógica. Si no estuviera disponible dicha herramienta, o si se observaran errores con los datos del usuario, restaure el contenido de la unidad lógica completa con la copia de seguridad más reciente, en caso de que los datos fueran fundamentales.</p>
Evento 202E - Error de lectura de unidad durante escritura interrumpida	3/11/8A	<p>Descripción: Se ha producido un error en la operación de lectura durante el procesamiento de escritura interrumpido.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Escritura interrumpida no recuperada. Póngase en contacto con el soporte IBM para completar este procedimiento.</p>
Evento 2109 - Memoria caché del controlador no habilitada - Los tamaños de memoria caché no coinciden	6/A1/00	<p>Descripción: El controlador no puede habilitar la duplicación si el tamaño de memoria caché de este y el controlador alternativo no es el mismo. Compruebe si el tamaño de la memoria caché de los dos controladores es igual.</p> <p>Acción: Póngase en contacto con el soporte de IBM para obtener instrucciones para la recuperación de este error.</p>
Evento 210C - Error en la batería de la memoria caché del controlador	6/0C/80	<p>Descripción: El controlador ha detectado que la batería no está físicamente presente, está totalmente descargada o ha llegado a su fecha de caducidad.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Error de CRU de batería y siga las instrucciones para corregir el error.</p>
Evento 210E - Error de recuperación de la memoria caché del controlador tras el ciclo de alimentación o restablecimiento	6/0C/81	<p>Descripción: La recuperación de un error de de la memoria caché de datos no se ha realizado correctamente. Se podrían haber perdido los datos de usuario.</p> <p>Acción: Póngase en contacto con el soporte de IBM para obtener instrucciones para la recuperación de este error.</p>

Tabla 38. Eventos críticos (continuación)

Número de evento crítico	Clave de detección/ASC/ASCQ	Descripción del evento crítico y acción requerida
Evento 2110 - Error de inicialización de la memoria caché del controlador	6/40/81	<p>Descripción: El controlador ha detectado un error en un componente interno del controlador (búfer RAID). El error del componente interno del controlador podría haberse detectado durante la operación o durante una rutina de diagnóstico.</p> <p>Acción: Póngase en contacto con el soporte de IBM para obtener instrucciones para la recuperación de este error.</p>
Evento 2113 - Vencimiento cercano de la batería de la memoria caché del controlador	6/3F/D9	<p>Descripción: Faltan seis semanas para el vencimiento de la batería de la memoria caché.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Proximidad de vencimiento de batería y siga las instrucciones para corregir el error.</p>
Evento 211B - Baterías presentes pero NVSRAM configurado para no tener baterías	Ninguno	<p>Descripción: Una batería está presente en el subsistema de almacenamiento, pero NVSRAM está configurado para no incluir baterías.</p> <p>Acción: Póngase en contacto con su representante de soporte técnico de IBM para obtener instrucciones para recuperarse de este error.</p>
Evento 2229 - Unidad fallada por el controlador	Ninguno	<p>Descripción: El controlador ha fallado una unidad debido a un problema con la misma.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento Unidad fallada por el controlador y siga las instrucciones para corregir el error.</p>
Evento 222D - Unidad fallada manualmente	6/3F/87	<p>Descripción: La unidad ha sido fallada manualmente por un usuario.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento Unidad fallada manualmente y siga las instrucciones para corregir el error.</p>
Evento 2247 - Pérdida de datos en la unidad lógica durante escritura interrumpida sin recuperar	6/3F/EB	<p>Descripción: Se produjo un error durante el proceso de escritura interrumpida en la rutina de inicio de jornada que ha hecho que la unidad lógica esté en estado de error.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Escritura interrumpida sin recuperar y siga las instrucciones para corregir el error. Póngase en contacto con el soporte IBM para completar este procedimiento.</p>
Evento 2248 - Error de unidad - Error de escritura	6/3F/80	<p>Descripción: La unidad ha fallado durante un comando de escritura. La unidad se ha marcado como Errónea.</p> <p>Acción: Inicie Recovery Guru y siga las instrucciones para corregir el error.</p>
Evento 2249 - Capacidad de unidad inferior a la mínima	6/3F/8B	<p>Descripción: Durante la sustitución de una unidad, la capacidad de la nueva unidad no es suficiente para dar soporte a todas las unidades lógicas que se deben reconstruir en la misma.</p> <p>Acción: Sustituya la unidad por una de mayor capacidad.</p>

Tabla 38. Eventos críticos (continuación)

Número de evento crítico	Clave de detección/ASC/ASCQ	Descripción del evento crítico y acción requerida
Evento 224A - Unidad con tamaño de bloque erróneo	6/3F/8C	<p>Descripción: El tamaño de bloque de la unidad no coincide con el del resto de unidades de la unidad lógica. La unidad se ha marcado como Errónea.</p> <p>Acción: Inicie Recovery Guru y siga las instrucciones para corregir el error.</p>
Evento 224B - Error de unidad - Error de inicialización	6/3F/86	<p>Descripción: La unidad ha fallado durante un comando de Format Unit o una operación de Write (emitido al inicializar una unidad lógica). La unidad se ha marcado como Errónea.</p> <p>Acción: Inicie Recovery Guru y siga las instrucciones para corregir el error.</p>
Evento 224D - Error de la unidad - Falta de respuesta al iniciar el día	6/3F/85	<p>Descripción: La unidad ha fallado un comando Read Capacity o Read durante la rutina de inicio de jornada. El controlador no puede leer la información de configuración almacenada en la unidad. La unidad se ha marcado como Errónea.</p> <p>Acción: Inicie Recovery Guru y siga las instrucciones para corregir el error.</p>
Evento 224E - Error de unidad - Error de inicialización/reconstrucción	6/3F/82	<p>Descripción: La unidad que falló anteriormente se ha marcado como Fallada por una de las razones siguientes:</p> <ul style="list-style-type: none"> • La unidad ha fallado un comando Format Unit emitido en la misma • La reconstrucción de la unidad ha fallado porque el controlador no ha podido restaurarla (por ejemplo, debido a un error en otra unidad necesaria para la reconstrucción). <p>Acción: Inicie Recovery Guru y siga las instrucciones para corregir el error.</p>
Evento 2250 - Error de unidad lógica	6/3F/E0	<p>Descripción: El controlador ha marcado la unidad lógica como Errónea. Ya no se pueden mantener los datos de usuario y la redundancia (paridad). La causa más probable es el fallo de una unidad individual de configuraciones sin redundancia o una segunda unidad no redundante en una configuración protegida por una unidad.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Error de unidad lógica errónea y siga las instrucciones para corregir el error.</p>
Evento 2251 - Error de unidad - Error de reconstrucción	6/3F/8E	<p>Descripción: Una unidad ha fallado debido a un error de reconstrucción durante la rutina de inicio de jornada.</p> <p>Acción: Inicie Recovery Guru y siga las instrucciones para corregir el error.</p>

Tabla 38. Eventos críticos (continuación)

Número de evento crítico	Clave de detección/ASC/ASCQ	Descripción del evento crítico y acción requerida
Evento 2252 - Unidad marcada como fuera de línea durante escritura interrumpida	6/3F/98	<p>Descripción: Se ha producido un error durante el proceso de escritura interrumpida que ha hecho que la unidad lógica se marque como Errónea. Las unidades de la matriz que no han experimentado el error de lectura pasan a estado Fuera de línea y registran este error.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Escritura interrumpida no recuperada. Póngase en contacto con el soporte IBM para completar este procedimiento.</p>
Evento 2254 - Falta de coincidencia de datos y redundancia (paridad) detectado	6/8E/01	<p>Descripción: El controlador detectó incoherencias de redundancia (paridad) o datos durante la verificación de la paridad.</p> <p>Acción: Póngase en contacto con el soporte de IBM para obtener instrucciones para la recuperación de este error.</p>
Evento 2255 - Definición de unidad lógica incompatible con modo ALT - ALT inhabilitado Nota: Este evento no es aplicable para el DS4800.	6/91/3B	<p>Descripción: La Transferencia automática de LUN (ALT) solo funciona con matrices en las que se ha definido una unidad lógica. Actualmente, hay matrices del subsistema de almacenamiento con más de una unidad lógica definida; por eso se ha inhabilitado el modo ALT. El controlador opera en modo redundante normal y si se produce un problema, transfiere todas las unidades lógicas de una matriz en vez de una sola unidad lógica.</p> <p>Acción: Póngase en contacto con el soporte de IBM para obtener instrucciones para la recuperación de este error.</p>
Evento 2260 - Unidad sin certificar	ASC/ASCQ: Ninguno	<p>Descripción: Una unidad del subsistema de almacenamiento no está certificada.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Unidad sin certificar.</p>
Evento 2602 - Error de sincronización automática de firmware de controlador	02/04/81	<p>Descripción: Las versiones de firmware de los controladores redundantes no son iguales porque la sincronización automática del firmware ha fallado. Los controladores con versiones de firmware incompatibles podrían causar resultados inesperados.</p> <p>Acción: Intente descargar el firmware de nuevo. Si el problema persiste, póngase en contacto con el soporte de IBM.</p>
Evento 2801 - Subsistema de almacenamiento en ejecución en batería de sistema de alimentación ininterrumpible	6/3F/C8	<p>Descripción: El sistema de alimentación ininterrumpible ha indicado que la alimentación de CA ya no está presente y ha cambiado a modo en espera. No existe motivo inmediato de preocupación, pero debe guardar sus datos con frecuencia por si la batería se agotara de manera repentina.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Pérdida de alimentación de CA. Siga las instrucciones para corregir el error.</p>

Tabla 38. Eventos críticos (continuación)

Número de evento crítico	Clave de detección/ASC/ASCQ	Descripción del evento crítico y acción requerida
Evento 2803 - Batería de sistema de alimentación ininterrumpible - Dos minutos de error	6/3F/C9	<p>Descripción: El sistema de alimentación ininterrumpible ha indicado que la fuente de alimentación en espera está prácticamente agotada.</p> <p>Acción: Adopte medidas para detener la actividad de E/S en el controlador. Normalmente, el controlador cambia de modo de almacenamiento en caché de rescritura a modo de escritura directa.</p>
Evento 2804 - Error en la batería del sistema de alimentación ininterrumpible	Ninguno	<p>Descripción: La batería del sistema de alimentación ininterrumpible ha fallado.</p> <p>Acción: Póngase en contacto con el soporte de IBM para obtener instrucciones para la recuperación de este error.</p>
Evento 2807 - Error de módulo de servicio de entorno	Ninguno	<p>Descripción: Un ESM ha fallado.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Error de CRU de módulo de servicio de entorno. Siga las instrucciones para corregir el error.</p>
Evento 2808 - Identificador de alojamiento de expansión no único	6/98/01	<p>Descripción: El controlador ha determinado que hay diversos alojamiento de expansión de almacenamientos con el mismo identificador seleccionados. Compruebe si cada alojamiento de expansión de almacenamiento tiene su valor de identificador exclusivo.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Conflicto de identificadores de alojamiento. Siga las instrucciones para corregir el error.</p>
Evento 280A - Ausencia de componente de alojamiento de controlador	6/3F/C7	<p>Descripción: Falta un componente distinto al controlador en el alojamiento del controlador (por ejemplo un ventilador, fuente de alimentación o batería). Los códigos FRU indican el componente que falta.</p> <p>Acción: Inicie Recovery Guru y siga las instrucciones para corregir el error.</p>
Evento 280B - Error de componente de alojamiento de controlador	6/3F/C7	<p>Descripción: Ha fallado un componente distinto al controlador en el alojamiento del controlador (por ejemplo un ventilador, fuente de alimentación o batería) o se ha producido una condición de exceso de temperatura. Los códigos FRU indican el componente erróneo.</p> <p>Acción: Inicie Recovery Guru y siga las instrucciones para corregir el error.</p>
Evento 280B - Error de componente de alojamiento de expansión de almacenamiento de unidad	6/3F/C7	<p>Descripción: Ha fallado un componente distinto a una unidad en el alojamiento de expansión de almacenamiento (por ejemplo un ventilador, fuente de alimentación o batería) o se ha producido una condición de exceso de temperatura. Los códigos FRU indican el componente que ha fallado.</p> <p>Acción: Inicie Recovery Guru y siga las instrucciones para corregir el error.</p>

Tabla 38. Eventos críticos (continuación)

Número de evento crítico	Clave de detección/ASC/ASCQ	Descripción del evento crítico y acción requerida
Evento 280E - Fuente de alimentación en espera no cargada totalmente	6/3F/CA	<p>Descripción: El sistema de alimentación ininterrumpible ha indicado que la fuente de alimentación en espera no ha alcanzado su capacidad máxima.</p> <p>Acción: Revise el sistema de alimentación ininterrumpida para asegurarse de que la fuente de energía en espera (batería) está en funcionamiento.</p>
Evento 280F - Módulo de servicio de entorno - Pérdida de comunicación	6/E0/20	<p>Descripción: Se ha perdido la comunicación con una de las CRU de ESM dual en un alojamiento de expansión de almacenamiento. El alojamiento de expansión de almacenamiento solo tiene una ruta de E/S disponible.</p> <p>Acción: Inicie Recovery Guru y siga las instrucciones para corregir el error.</p>
Evento 2813 - Error de CRU de miniconcentrador	6/3F/C7	<p>Descripción: Se ha perdido la comunicación con la CRU del miniconcentrador. Esto podría deberse a un error de la CRU del miniconcentrador, un error del controlador o un error interno de la placa de comunicaciones de la placa posterior. Si solo se produce un error en el miniconcentrador, el subsistema de almacenamiento sigue en funcionamiento, si se produce un segundo error los alojamientos afectados fallarán.</p> <p>Acción: Inicie Recovery Guru y siga las instrucciones para corregir el error.</p>
Evento 2815 - Error de GBIC	Ninguno	<p>Descripción: Ha fallado un convertor de interfaz gigabit (GBIC) del alojamiento del controlador o alojamiento de expansión de almacenamiento. Si solo se produce un error en el GBIC, el subsistema de almacenamiento sigue en funcionamiento, si se produce un segundo error los alojamientos afectados fallarán.</p> <p>Acción: Inicie Recovery Guru y siga las instrucciones para corregir el error.</p>
Evento 2816 - Conflicto de identificadores de alojamiento de expansión del almacenamiento - Identificadores duplicados en alojamiento de expansión de almacenamientos	6/98/01	<p>Descripción: Dos o más alojamiento de expansión de almacenamientos utilizan el mismo número de identificación de alojamiento.</p> <p>Acción: Inicie Recovery Guru y siga las instrucciones para corregir el error.</p>
Evento 2818 - No coincidencia de identificadores de alojamiento de expansión del almacenamiento - Identificadores duplicados en el mismo alojamiento de expansión de almacenamiento	6/98/02	<p>Descripción: Un alojamiento de expansión de almacenamiento del subsistema de almacenamiento contiene ESM con diferentes números de identificación de alojamiento.</p> <p>Acción: Inicie Recovery Guru y siga las instrucciones para corregir el error.</p>

Tabla 38. Eventos críticos (continuación)

Número de evento crítico	Clave de detección/ASC/ASCQ	Descripción del evento crítico y acción requerida
Evento 281B - Temperatura nominal superada	6/98/03	<p>Descripción: La temperatura nominal del alojamiento se ha superado. O bien ha fallado un ventilador, o la temperatura de la sala es demasiado alta. Si la temperatura del alojamiento continúa aumentando, el alojamiento afectado podría detenerse automáticamente. Solucione el problema de inmediato, antes de que sea más grave. Las condiciones de detención automática dependen del modelo del alojamiento.</p> <p>Acción: Inicie Recovery Guru y siga las instrucciones para corregir el error.</p>
Evento 281C- - Temperatura máxima superada	6/3F/C6	<p>Descripción: Se ha superado la temperatura máxima del alojamiento. O bien ha fallado un ventilador, o la temperatura de la sala es demasiado alta. Esta condición es crítica y puede hacer que el alojamiento se detenga si no soluciona el problema de inmediato. Las condiciones de detención automática dependen del modelo del alojamiento.</p> <p>Acción: Inicie Recovery Guru y siga las instrucciones para corregir el error.</p>
Evento 281D - Sensor de temperatura retirado	6/98/03	<p>Descripción:Se ha retirado del subsistema de almacenamiento una CRU de ventilador que contiene un sensor de temperatura.</p> <p>Acción: Sustituya la CRU lo antes posible.Inicie Recovery Guru, pulse el procedimiento de recuperación CRU de ventilador errónea o retirada, y siga las instrucciones para corregir el error.</p>
Evento 281E - Falta de coincidencia de firmware de módulo de servicio de entorno	6/98/03	<p>Descripción: Un alojamiento de expansión de almacenamiento del subsistema de almacenamiento contiene ESM con diferentes versiones de firmware. Los ESM del mismo alojamiento de expansión de almacenamiento deben tener la misma versión de firmware. Si no dispone de un supervisor de servicio de sustitución, llame al soporte de IBM para llevar a cabo la descarga del firmware.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Falta de coincidencia de firmware de módulo de servicio de entorno. Siga las instrucciones para corregir el error.</p>
Evento 2821 - Miniconcentrador incompatible	Ninguno	<p>Descripción: Se ha detectado un blade miniconcentrador incompatible en el alojamiento del controlador.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Blade miniconcentrador incompatible. Siga las instrucciones para corregir el error.</p>
Evento 2823 - Unidad eludida	Ninguno	<p>Descripción: El ESM ha informado de que la unidad se ha eludido para mantener la integridad del bucle de canal de fibra.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Unidad eludida y siga las instrucciones para corregir el error.</p>

Tabla 38. Eventos críticos (continuación)

Número de evento crítico	Clave de detección/ASC/ASCQ	Descripción del evento crítico y acción requerida
Evento 2827 - Controlador sustituido inadvertidamente con un ESM	Ninguno	<p>Descripción: Un blade del controlador se ha sustituido inadvertidamente con un blade de ESM.</p> <p>Acción: Sustituya el blade de ESM por un blade de controlador lo antes posible.</p>
Evento 2828 - alojamiento de expansión de almacenamiento seleccionado no soportado	Ninguno	<p>Descripción: El subsistema de almacenamiento contiene uno o varios alojamientos de expansión de almacenamiento incompatibles. Si se detectan como incompatibles todos sus alojamientos de expansión del almacenamiento, podría tener un problema con un archivo de configuración NVSRAM o una versión de firmware inadecuada. Esta condición de error hará que las unidades de los alojamientos de expansión del almacenamiento incompatibles se desconecten por seguridad, lo cual puede provocar el fallo de las matrices o unidades lógicas definidas.</p> <p>Acción: Si se producen errores en la matriz o unidades lógicas, llame al soporte de IBM para conocer el procedimiento de recuperación. De lo contrario, inicie Recovery Guru para acceder al procedimiento de recuperación Alojamiento de unidad incompatible y siga las instrucciones para corregir el error.</p>
Evento 2829 - Redundancia de controlador perdida	6/E0/20	<p>Descripción: Se ha perdido la comunicación entre los dos controladores a través de uno de los bucles de unidad (canales).</p> <p>Acción: Inicie Recovery Guru y determine si se han producido otros problemas de pérdida de redundancia. De ser así, antes de nada soluciónelos. Si se siguen registrando problemas de redundancia, póngase en contacto con el soporte de IBM.</p>
Evento 282B - Pérdida de redundancia de ruta de alojamiento de expansión de almacenamiento	6/E0/20	<p>Descripción: Un alojamiento de expansión de almacenamiento con bucles de unidad redundantes (canales) ha perdido la comunicación a través de uno de sus bucles. El alojamiento de expansión del almacenamiento solo tiene un bucle disponible para E/S. Corrija este error lo antes posible. Aunque el subsistema de almacenamiento sigue en funcionamiento, podría perderse un nivel de redundancia de ruta. Si fallase el bucle de unidad restante, todas las E/S al alojamiento de expansión del almacenamiento fallarían.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Unidad - Pérdida de redundancia de ruta. Siga las instrucciones para corregir el error.</p>
Evento 282D - Pérdida de redundancia de ruta de unidad	6/E0/20	<p>Descripción: Se ha perdido una ruta de comunicación con una unidad. Corrija este error lo antes posible. Aunque la unidad siga en funcionamiento, podría haberse perdido un nivel de redundancia de ruta. Si el otro puerto de la unidad o cualquier otro componente fallase en el canal de trabajo, la unidad fallaría.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Unidad - Pérdida de redundancia de ruta. Siga las instrucciones para corregir el error.</p>

Tabla 38. Eventos críticos (continuación)

Número de evento crítico	Clave de detección/ASC/ASCQ	Descripción del evento crítico y acción requerida
Evento 282F - Versión incompatible de firmware de ESM detectada	Ninguno	<p>Descripción: Un alojamiento de expansión de almacenamiento del subsistema de almacenamiento contiene blades ESM con diferentes versiones de firmware. Este error también se podría dar si un alojamiento de expansión de almacenamiento del subsistema de almacenamiento contiene blades ESM con hardware diferente.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación No coincidencia de versión de firmware de blade ESM y siga las instrucciones para corregir el error.</p>
Evento 2830 - Combinación de tipos de unidad no soportada	Ninguno	<p>Descripción: Actualmente el subsistema de almacenamiento contiene diferentes tecnologías de unidad, como canal de fibra (FC) y Serial ATA (SATA). En este subsistema de almacenamiento no se permite combinar diferentes tecnologías de unidad.</p> <p>Acción: Seleccione Recovery Guru para acceder al procedimiento de recuperación Combinación de tipos de unidad no soportada y siga las instrucciones para corregir el error.</p>
Evento 2835 - Alojamientos de expansión del almacenamiento de unidad no cableados juntos	ASC/ASCQ: Ninguno	<p>Descripción: En el subsistema de almacenamiento hay alojamientos de expansión del almacenamiento de unidad no cableados correctamente; tiene blades ESM que deben cablearse juntas de manera secuencial.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Alojamientos de unidad no cableados juntos y siga las instrucciones para corregir el error.</p>
Evento 3019 - Cambio de propiedad de unidad lógica debido a migración tras error	Ninguno	<p>Descripción: El software del controlador multi-ruta ha cambiado la propiedad de las unidades lógicas al otro controlador porque no ha podido acceder a las mismas en una ruta concreta.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Unidad lógica fuera de ruta preferida. Siga las instrucciones para corregir el error.</p>
Evento 4011 - Unidad lógica fuera de ruta preferida	Ninguno	<p>Descripción: No se puede acceder al controlador que se muestra en la zona de Recovery Guru. Todas las unidades lógicas para las que este controlador se asigna como ruta preferida se moverán a la ruta no preferida (controlador alternativo).</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Unidad lógica fuera de ruta preferida. Siga las instrucciones para corregir el error.</p>

Tabla 38. Eventos críticos (continuación)

Número de evento crítico	Clave de detección/ASC/ASCQ	Descripción del evento crítico y acción requerida
Evento 5005 - Controlador fuera de línea	Ninguno	<p>Descripción: El controlador está fuera de línea. Esto podría deberse a que el controlador haya fallado una prueba de diagnóstico. (Los diagnósticos se inician internamente a través del controlador o de la opción de menú Controlador → Ejecutar diagnóstico). Además, el controlador se puede establecer fuera de línea con la opción de menú Controlador → Establecer fuera de línea.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Controlador fuera de línea. Siga las instrucciones para sustituir el controlador.</p>
Evento 502F - Unidades lógicas suprimidas	Ninguno	<p>Descripción: El subsistema de almacenamiento ha detectado que las unidades asociadas con una unidad lógica ya no están disponibles. Esto puede deberse a la eliminación de todas las unidades asociadas con una matriz o a la pérdida de alimentación en uno o varios alojamientos de expansión de almacenamientos.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Falta de unidad lógica. Siga las instrucciones para corregir el error.</p>
Evento 5038 - Controlador en modo de bloqueo	Ninguno	<p>Descripción: Ambos controladores se han establecido en modo de bloqueo durante 10 minutos porque se han superado los 10 intentos de autenticación de contraseña en un periodo de 10 minutos. Durante el periodo de bloqueo, ambos controladores denegarán todas las solicitudes de autenticación. Cuando finalice el bloqueo de 10 minutos, el controlador restablecerá el contador de errores de autenticación totales y se desbloqueará.</p> <p>Acción: Espere 10 minutos e intente indicar la contraseña de nuevo.</p>
Evento 5040 - Establezca el controlador en modo de servicio	Ninguno	<p>Descripción: El controlador se ha establecido manualmente en modo de servicio por motivos de diagnóstico o recuperación.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Controlador en modo de servicio. Utilice este procedimiento para establecer el controlador en línea de nuevo.</p>
Evento 5405 - Gold Key - Valores no coincidentes	ASC/ASCQ: Ninguno	<p>Descripción: Cada controlador del par de controladores tiene un valor de bit NVSRAM diferente que determina si el controlador está sujeto a restricciones Gold Key.</p> <p>Acción: Este evento se podría generar si unidades o controladores de un subsistema de almacenamiento IBM se cambian inadvertidamente por unidades o controladores no IBM. Este evento crítico no se aplica a la configuración de subsistemas de almacenamiento IBM DS3000, DS4000 o DS5000. Póngase en contacto con el soporte IBM para conocer el procedimiento de recuperación.</p>

Tabla 38. Eventos críticos (continuación)

Número de evento crítico	Clave de detección/ASC/ASCQ	Descripción del evento crítico y acción requerida
Evento 5406 - Combinación de tipos de unidad - Valores no coincidentes	ASC/ASCQ: Ninguno	<p>Descripción: Cada controlador del par de controladores tiene un valor de bit NVSRAM diferente que controla si la Combinación de tipos de unidad es una característica premium.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Combinación de tipos de unidad - Valores no coincidentes y siga las instrucciones para corregir esta condición del controlador.</p>
Evento 5602 - Error del controlador alternativo - Tiempo de espera para resultados	Ninguno	<p>Descripción: Este controlador inició diagnósticos en el controlador alternativo pero no ha recibido una respuesta que indique que el diagnóstico se ha completado. El controlador alternativo de este par se ha establecido fuera de línea.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Controlador fuera de línea. Siga las instrucciones para sustituir el controlador.</p>
Evento 560B - La tarea CtlrDiag no puede obtener el bloque Selección de modo	Ninguno	<p>Descripción: Este controlador está intentando ejecutar diagnósticos y no ha podido asegurar la zona de prueba de otras operaciones del subsistema de almacenamiento. Los diagnósticos se han cancelado.</p> <p>Acción: Póngase en contacto con el soporte de IBM para obtener instrucciones para la recuperación de este error.</p>
Evento 560C - La tarea CtlrDiag del controlador alternativo no ha podido obtener el Modo	Ninguno	<p>Descripción: El controlador alternativo de este par está intentando ejecutar diagnósticos y no ha podido asegurar la zona de prueba de otras operaciones del subsistema de almacenamiento. Los diagnósticos se han cancelado.</p> <p>Acción: Póngase en contacto con el soporte de IBM para obtener instrucciones para la recuperación de este error.</p>
Evento 560D - Error de prueba de lectura de diagnósticos en el controlador	Ninguno	<p>Descripción: Mientras el controlador ejecutaba diagnósticos, ha detectado que la información recibida no coincide con la devolución esperada de la prueba. Esto podría indicar que la E/S no se ha completado o que existe una falta de coincidencia en los datos leídos. Como resultado de este error, el controlador se establecerá fuera de línea.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Controlador fuera de línea. Siga las instrucciones para sustituir el controlador.</p>
Evento 560E - Error de lectura de diagnóstico del controlador alternativo	Ninguno	<p>Descripción: Mientras el controlador alternativo ejecutaba diagnósticos, ha detectado que la información recibida no coincide con la devolución esperada de la prueba. Esto podría indicar que la E/S no se ha completado o que existe una falta de coincidencia en los datos leídos. El controlador alternativo de este par se ha establecido fuera de línea.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Controlador fuera de línea. Siga las instrucciones para sustituir el controlador.</p>

Tabla 38. Eventos críticos (continuación)

Número de evento crítico	Clave de detección/ASC/ASCQ	Descripción del evento crítico y acción requerida
Evento 560F - Error de prueba de lectura de diagnósticos en el controlador	Ninguno	<p>Descripción: Mientras el controlador alternativo ejecutaba diagnósticos, no pudo escribir datos en la zona de prueba. Esto podría indicar que la E/S no se ha completado o que existe una falta de coincidencia en los datos que se están escribiendo. El controlador se ha establecido fuera de línea.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Controlador fuera de línea. Siga las instrucciones para sustituir el controlador.</p>
Evento 5610 - Error de escritura de diagnóstico del controlador alternativo	Ninguno	<p>Descripción: Mientras el controlador alternativo ejecutaba diagnósticos, no pudo escribir datos en la zona de prueba. Esto podría indicar que la E/S no se ha completado o que existe una falta de coincidencia en los datos que se están escribiendo. El controlador alternativo de este par se ha establecido fuera de línea.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Controlador fuera de línea. Siga las instrucciones para sustituir el controlador.</p>
Evento 5616 - Diagnóstico rechazado - Error de configuración en el controlador	Ninguno	<p>Descripción: El controlador alternativo de este par está intentando ejecutar diagnósticos y no ha podido crear la zona de prueba necesaria para la realización de las pruebas. El diagnóstico se ha cancelado.</p> <p>Acción: Póngase en contacto con el soporte de IBM para obtener instrucciones para la recuperación de este error.</p>
Evento 5617 - Diagnóstico rechazado - Error de configuración en el controlador alternativo	Ninguno	<p>Descripción: El controlador alternativo de este par está intentando ejecutar diagnósticos y no ha podido crear la zona de prueba necesaria para la realización de las pruebas. El diagnóstico se ha cancelado.</p> <p>Acción: Póngase en contacto con el soporte de IBM para obtener instrucciones para la recuperación de este error.</p>
Evento 6101 - Base de datos de configuración interna llena	Ninguno	<p>Descripción: Debido a la cantidad de datos necesarios para almacenar determinados datos de configuración, se ha subestimado el número máximo de unidades lógicas. Uno o los dos tipos de datos siguientes podrían haber hecho que se llene la base de datos de configuración interna:</p> <ul style="list-style-type: none"> • Datos de configuración de unidades lógicas FlashCopy • Datos de configuración remota globales/Metro mirror <p>Acción: Para recuperarse de este evento, puede suprimir una o varias unidades lógicas FlashCopy de su subsistema de almacenamiento o eliminar una o varias relaciones de duplicación remota.</p>

Tabla 38. Eventos críticos (continuación)

Número de evento crítico	Clave de detección/ASC/ASCQ	Descripción del evento crítico y acción requerida
Evento 6107 - El controlador alternativo no funciona y se está restableciendo	Ninguno	<p>Descripción: Un controlador del subsistema de almacenamiento ha detectado que su controlador alternativo no funciona debido a problemas de hardware y debe ser sustituido.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Controlador fuera de línea y siga las instrucciones para corregir el error.</p>
Evento 6200 - Umbral de unidad lógica de repositorio FlashCopy superado	Ninguno	<p>Descripción: La capacidad de unidad lógica de repositorio FlashCopy ha superado un nivel de umbral de aviso. Si se llena la capacidad de unidad lógica de repositorio FlashCopy, su unidad lógica FlashCopy podría fallar. Este es el último aviso que recibirá antes de que la unidad lógica de repositorio FlashCopy se llene.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Umbral de unidad lógica de repositorio FlashCopy superado. Siga las instrucciones para corregir el error.</p>
Evento 6201 - Unidad lógica de repositorio FlashCopy llena	Ninguno	<p>Descripción: Se ha utilizado toda la capacidad disponible de la unidad lógica de repositorio FlashCopy. La política de error de la unidad lógica de repositorio FlashCopy determina qué sucede cuando se llena la unidad lógica de repositorio FlashCopy. La política de error se puede definir para que la unidad lógica FlashCopy falle (valor predeterminado) o para que fallen las E/S entrantes a la unidad lógica de base.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Capacidad de unidad lógica de repositorio FlashCopy - Llena. Siga las instrucciones para corregir el error.</p>
Evento 6202 - Unidad lógica FlashCopy errónea	Ninguno	<p>Descripción: La unidad lógica de repositorio FlashCopy asociada con la unidad lógica FlashCopy está llena o las unidades lógicas de repositorio FlashCopy han fallado debido a uno o varios errores en sus matrices.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Unidad lógica FlashCopy errónea. Siga las instrucciones para corregir el error.</p>
Evento 6400 - Unidad lógica primaria dual	Ninguno	<p>Descripción: Ambas unidades lógicas se han ascendido a unidades lógicas primarias tras un cambio de papel forzado. Esto puede darse cuando se restablece el controlador o se reinserta un cable de una matriz en un conmutador de canal de fibra después de haberlo retirado y de que otra unidad lógica haya pasado a ser la unidad lógica primaria.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Conflicto de unidad lógica primaria dual. Siga las instrucciones para corregir el error.</p>

Tabla 38. Eventos críticos (continuación)

Número de evento crítico	Clave de detección/ASC/ASCQ	Descripción del evento crítico y acción requerida
Evento 6401 - Unidad lógica secundaria dual	Ninguno	<p>Descripción: Ambas unidades lógicas del reflejo remoto se han descendido a unidades lógicas secundarias tras un cambio de papel forzado. Esto puede darse cuando se restablece el controlador o se reinserta un cable de una matriz en un conmutador de canal de fibra después de haberlo retirado y de que otra unidad lógica haya pasado a ser una unidad lógica secundaria.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Conflicto de unidad lógica secundaria dual. Siga las instrucciones para corregir el error.</p>
Evento 6402 - Datos duplicados no sincronizados	Sin registrar con evento	<p>Descripción: Esto podría ocurrir debido a errores de E/S, pero otros eventos pueden estar asociados con este problema. Un icono Requiere atención se muestra en los subsistemas de almacenamiento primario y secundario del reflejo remoto.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Datos duplicados ni sincronizados. Siga las instrucciones para corregir el error.</p>
Evento 6503 - Caída de enlace de unidad lógica remota	Ninguno	<p>Descripción: Este evento se desencadena cuando se desconecta un cable entre una matriz y su igual, falla el conmutador de canal de fibra o se restablece la matriz igual. Este error podría provocar un Evento 6402, Datos duplicados no sincronizados. La unidad lógica remota afectada muestra un icono Sin respuesta, y este estado se selecciona en la ayuda contextual al pasar el cursor sobre la unidad lógica.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Error de comunicación con reflejo - No se puede contactar con la unidad lógica. Siga las instrucciones para corregir el error.</p>
Evento 6505 - Error de cambio de WWN	Ninguno	<p>Descripción: La duplicación hace que se comunique un cambio de WWN entre matrices. Los errores en el cambio de WWN se producen debido a errores de comunicación no E/S entre una matriz, en la que se ha cambiado el WWN, y una matriz igual. (El WWN de la matriz es el nombre exclusivo utilizado para ubicar una matriz en una red de fibra. Cuando se sustituyen ambos controladores de una matriz, el WWN de la matriz cambia). La unidad lógica remota afectada muestra un icono Sin respuesta, y este estado se selecciona en la ayuda contextual al pasar el cursor sobre la unidad lógica.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación No se puede actualizar la duplicación remota. Siga las instrucciones para corregir el error. La única solución a este problema es suprimir la duplicación remota y establecer una nueva.</p>

Tabla 38. Eventos críticos (continuación)

Número de evento crítico	Clave de detección/ASC/ASCQ	Descripción del evento crítico y acción requerida
Evento 6600 - Error de operación de copia de unidad lógica	Ninguno	<p>Descripción: Una operación de copia de unidad lógica con estado En curso ha fallado. Este error puede estar provocado por un error de lectura en la unidad lógica de origen, un error de escritura en la unidad lógica de destino o un error del subsistema de almacenamiento que afecte a la unidad lógica de origen o de destino.</p> <p>Acción: Inicie Recovery Guru y pulse el procedimiento de recuperación Error de operación de copia de unidad lógica. Siga las instrucciones para corregir el error.</p>
Evento 6700 - Sector(es) ilegible(s) detectado(s) - pérdida de datos	Ninguno	<p>Descripción: Se han detectado sectores ilegibles en una o varias unidades lógicas y se ha perdido datos.</p> <p>Acción: Inicie Recovery Guru para acceder al procedimiento de recuperación Sectores ilegibles detectados y siga las instrucciones para corregir el error.</p>
Evento 6703 - Desbordamiento en base de datos de sector ilegible	Ninguno	<p>Descripción: El registro de sectores ilegibles ha alcanzado su capacidad máxima.</p> <p>Acción: Seleccione Recovery Guru para acceder al procedimiento de recuperación Registro de sectores ilegibles lleno y siga las instrucciones para corregir el error.</p>

Recuperación de almacenamientos intermedios de rastreo

Los almacenamientos intermedios de rastreo binario proporcionan datos durante un periodo de tiempo mayor que el texto dqprint anterior `destateCaptureData.txt`.

Los datos de soporte y resolución de problemas avanzados se recopilar en formato binario y deben ser analizados por el Soporte de IBM. Estos forman parte del paquete de soporte Collect All Support Data (CASD) (`traceBuffers.zip`).

Uso en el CLi:

```
start controller [both] trace dataType=all forceFlush=FALSE file="C:\TBTest2.zip";
```



Validación de la base de datos de configuración

La versión 10.77 incluye una nueva característica de diagnóstico de la base de datos de configuración.

Para llevar a cabo la validación manual, seleccione un controlador en la pestaña Físico, a continuación seleccione **Avanzado > Resolución de problemas > Ejecutar diagnósticos > Base de datos de configuración**.

Una comprobación de la base de datos automática se llevará a cabo antes de que comience la descarga del firmware del controlador a través del EMW, la ventana Gestión del subsistema o la CLI.

Si la validación falla, se crea un archivo zip con un archivo de texto que contiene una descripción del error y un archivo DQ para la resolución de problemas.

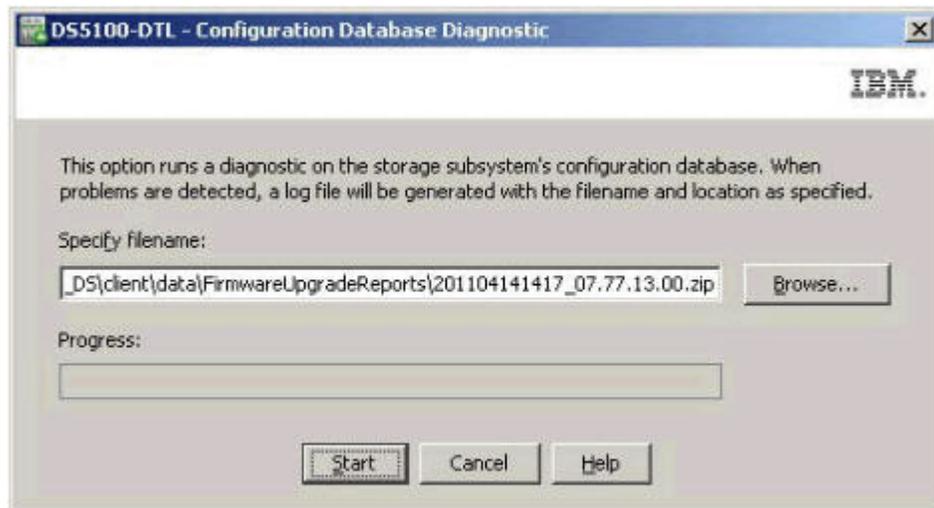
Evento de fallo de validación MEL:

Nombre del evento: Inconsistencia de estructura de recuperación de datos en bruto detectada

Tipo: 3408

Tipo de componente: Controlador

Nuevo comando CLI:**start storageSubsystem configDbDiagnostic;**



Guardar/restaurar la base de datos

Storage Monitor Service guarda automáticamente la base de datos de configuración de un subsistema y esta puede restaurarse.

Guardar

Storage Monitor Service guarda automáticamente la base de datos de configuración de un subsistema y guarda el archivo en "...client\data\monitor\dbcapture" si se realiza algún cambio en la base de datos y han pasado 125 minutos desde la anterior captura.

Cuando se añade un subsistema a un HSW recién instalador, se captura la primera base de datos.

Todos los archivos de base de datos capturados se comprimen y nombran del siguiente modo: RetrievedRecords_SSID_Fecha_Hora.dbm.

Ejemplo:

RetrievedRecords_60080e500017b8de000000004be47b12_2010_08_20_14_48_27.dbm

La CLI se puede usar para guardar una base de datos manualmente utilizando el comando **save storageSubsystem dbmDatabase file="C:\path\filename.zip"**

Restauración

Una base de datos de configuración existente se puede restaurar para recuperar sistemas que han perdido su configuración o cuya configuración se ha eliminado para recuperarse de la anomalía.

Se restauran las porciones de la base de datos que contiene:

- El Lun y la configuración de la matriz
- Los WWN del Lun
- Los WWN del controlador
- Las características premium

- Las correlaciones

Se excluyen:

- El MEL
- El UTM
- La memoria caché

Duración: hasta 45 minutos

El usuario debe tener una cadena de validación para restaurar la base de datos de configuración. Para obtener el validador, envíe el archivo zip de la base de datos de configuración y el perfil del sistema al soporte de IBM. El soporte de IBM genera la cadena de validación en base a la información que usted facilite.

Cargar base de datos de configuración

Para cargar la base de datos de configuración, haga lo siguiente:

1. Abra el archivo *.key enviado a través de correo electrónico en un editor de texto.
2. Registre la cadena. Ejemplo: 8bbaadfa7375cb4dfcc81c15bde30ad32d814c09
3. Detenga la E/S al subsistema
4. Defina uno de los controladores fuera de línea a través de la interfaz gráfica de usuario
5. La restauración se habrá realizado utilizando el comando CLI **load storageSubsystem dbmDatabase file="C:\path\filename.zip" validator="8bbaadfa7375cb4dfcc81c15bde30ad32d814c09"**;

Captura de datos de diagnóstico (DCC) de DS

La función DDC se implementó para asistir al soporte de IBM en la recopilación de datos para la resolución de problemas relacionados con eventos de firmware de controlador inusuales.

Nota: Esta función no se implementa con versiones de código de firmware de controlador anteriores al nivel 06.12.27.xx.

En circunstancias excepcionales, un error interno del controlador puede hacer que una rutina ejecute la función de captura de datos de diagnóstico (DDC). Cuando esto ocurre, en la ventana Gestión empresarial se muestra un signo de detención rojo junto al nombre del subsistema de almacenamiento que tiene el error (está en estado no óptimo). Tras abrir la ventana Gestión del subsistema de este subsistema de almacenamiento, puede pulsar en el Recovery Guru. El Recovery Guru muestra el problema, al igual que el MEL (registro de sucesos principal de Storage Manager). Consulte "Eventos DDC MEL" en la página 295 para obtener más información sobre el MEL.

Cuando se implementa la función de DDC, el estado del subsistema de almacenamiento cambia de Óptimo a Necesita atención debido a la DDC. Esto sucede bajo las condiciones siguientes:

- Los controladores del subsistema de almacenamiento detectan eventos inusuales como una terminación anormal maestra (el chip de canal de fibra accede a una dirección errónea, lo cual resulta en un error de bus PCI).

- El controlador no consigue procesar las solicitudes de E/S del host durante un periodo prolongado de tiempo (varios minutos).
- El registro de número de dispositivo de destino está corrupto.
- Las unidades de disco devuelven un EDC (código de detección de error).
- Se ha producido un error de inactividad en la unidad lógica propiedad del controlador alternativo.
- Los registros relacionados con la gestión de las particiones de almacenamiento están corruptos.

Cuando se define un distintivo **Necesita atención debido a la DDC**, este persiste al ciclo de alimentación y arranque del controlador, siempre que las baterías de la memoria caché del controlador estén lo suficientemente cargadas. Además, se recopilan y guardan hasta que los recupere, los datos que reflejan el estado de los controladores del subsistema de almacenamiento en el momento en que se produjo el evento inusual. Para borrar el distintivo **Necesita atención debido a la DDC** y recuperar los datos de diagnóstico guardados, consulte "Pasos de recuperación".

Dado que la función de DCC actual mantiene los datos de DCC solo para un evento inusual hasta que estos se guardan, debe llevar a cabo los comandos **SMc1i** lo antes posible cuando se produzca un error Necesita atención debido a la DDC para que los controladores estén listos para capturar datos de otros eventos inusuales. Hasta que no se guarden los datos de diagnóstico y se borre el distintivo **Necesita atención debido a la DDC**, ningún otro evento inusual hará que el controlador capture datos de diagnóstico para los mismos. Un evento inusual invoca un activador de DDC si un activador de DDC anterior ha recuperado información de DDC al menos 48 antes. Además, la información de DDC sólo está disponible si el controlador está en línea. Los controladores en modalidad de servicio o bloqueados no desencadenan eventos de DDC. Tras recopilar los datos de DDC, póngase en contacto con el soporte de IBM para informar sobre el problema y obtener ayuda para resolver el problema.

Pasos de recuperación

Para llevar a cabo el proceso de recuperación de DCC, complete los pasos siguientes:

1. Abra el editor de scripts desde la ventana Gestión empresarial o la interfaz de línea de comandos (CLI).

Nota: Consulte la ayuda en línea en la ventana Gestión empresarial para obtener más información sobre la sintaxis de estos comandos.

2. Siga las instrucciones de la página siguiente, dependiendo de si desea o no guardar los datos de diagnóstico.

Tabla 39. Paso de recuperación 2

Si...	Entonces...
Desea guardar los datos de diagnóstico	Vaya al paso 3.
No desea guardar los datos de diagnóstico	Vaya al paso 5.

3. Escriba

```
save storageSubsystem diagnosticData file="filename ";
```

donde *filename* es la ubicación y nombre del archivo que va a guardar. El archivo se inicializa como archivo .zip.

Nota: El parámetro `esm` de la sintaxis del comando no se soporta.

4. Siga las instrucciones de la tabla incluida a continuación para trabajar con los datos de diagnóstico.

Tabla 40. Paso de recuperación 4

Si...	Entonces...	
No se devuelve ningún error	Vaya al paso6.	
Se devuelve algún error	Si...	Entonces...
	El mensaje de error indica que se ha producido un error al guardar los datos.	Espere 2 minutos y reinicie el paso3.
	El mensaje de error indica que se ha producido un error al restablecer los datos.	Espere 2 minutos y vaya al paso5.

5. Escriba

```
reset storageSubsystem diagnosticData;
```

Tabla 41. Paso de recuperación 5

Si...	Entonces...
No se devuelve ningún error	Vaya al paso 6.
Se devuelve algún error	Espere dos minutos y ejecute el comando de nuevo. Los controladores podrían necesitar tiempo adicional para actualizar su estado. Nota: Si el estado de los datos de diagnóstico ya se ha restablecido, podría producirse otro error. Vaya al paso6.

6. Pulse **Comprobar de nuevo** para ejecutar el Recovery Guru de nuevo. El error ya no se muestra en el área **Resumen**.

Una vez completado este proceso, el mensaje de DDC se eliminará automáticamente y la nueva comprobación del Recovery Guru no mostrará entradas de captura de DDC. Si por alguna razón los datos no se eliminan, el Recovery Guru proporciona un ejemplo de cómo borrar la información de DDC sin guardar los datos. Para completar el procedimiento anterior, en el editor de scripts escriba

```
reset storageSubsystem diagnosticData;
```

Eventos DDC MEL

Cuando un evento inusual desencadena la acción de captura datos de diagnóstico, uno o varios de los eventos siguientes se publican en los registros de sucesos del subsistema de almacenamiento, dependiendo de las acciones del usuario.

Tabla 42. Eventos DDC MEL

Número de evento	Descripción	Prioridad	Descripción
0x6900	Los datos de diagnóstico están disponibles.	Crítico	Se registra cuando un evento del controlador inusual desencadena la función DDC para almacenar datos de diagnóstico.

Tabla 42. Eventos DDC MEL (continuación)

Número de evento	Descripción	Prioridad	Descripción
0x6901	La operación de recuperación de datos de diagnóstico ha comenzado.	Informativo	Se registra cuando el usuario ejecuta un comando SMcli para recuperar y guardar los datos de diagnóstico, como se describe en el paso 3 de "Pasos de recuperación" en la página 294.
0x6902	La operación de recuperación de datos de diagnóstico se ha completado.	Informativo	Se registra cuando la recuperación de datos de diagnóstico se ha completado y guardado.
0x6903	Los datos de diagnóstico requieren que se borre el estado/distintivo Atención.	Informativo	Se registra cuando el usuario restablece el distintivo <i>Requiere atención debido a DDC</i> con el comando SMcli , o cuando la recuperación de los datos de diagnóstico se completa y guarda correctamente tras ser iniciada por el usuario con el comando SMcli save storageSubsystem diagnosticData .

Resolución de errores de matriz de discos en AIX

Esta sección describe los errores de la matriz de discos que pueden observarse en el registro de errores de AIX. Puede ver el registro de errores de AIX utilizando el comando **errpt -a**. También puede consultar el registro de Storage Manager Major Event (MEL) para saber si existe alguna correlación entre el host, la SAN y el subsistema de almacenamiento.

Puede que tenga que validar su configuración o sustituir hardware defectuoso para resolver la situación.

Nota: Para obtener más información sobre resolución de problemas, consulte la *Guía de mantenimiento usuario e instalación* facilitada con su subsistema de almacenamiento.

Tabla 43. Errores de matriz de discos

Número de error	Nombre de error	Tipo de error	Descripción del error
1	FCP_ARRAY_ERR1	ERROR OPERACIÓN MATRIZ DE DISCOS	Se ha producido un error de hardware permanente en el que se está implicado el soporte de la matriz de discos.
2	FCP_ARRAY_ERR2	ERROR OPERACIÓN MATRIZ DE DISCOS	Se ha producido un error de hardware permanente.
3	FCP_ARRAY_ERR3	ERROR OPERACIÓN MATRIZ DE DISCOS	el adaptador de matriz ha detectado un error permanente.
4	FCP_ARRAY_ERR4	ERROR OPERACIÓN MATRIZ DE DISCOS	Se ha producido un error temporal en la matriz, comunicaciones o adaptador.

Tabla 43. Errores de matriz de discos (continuación)

Número de error	Nombre de error	Tipo de error	Descripción del error
5	FCP_ARRAY_ERR5	ERROR NO DETERMINADO	Se ha producido un error no determinado.
6	FCP_ARRAY_ERR6	ANOMALÍA DE COMPONENTE DE SUBSISTEMA	Se ha producido una condición de degradación distinta a la unidad de disco.
7	FCP_ARRAY_ERR7	ANOMALÍA COMPROB. ESTADO CONTROLADOR	Ha fallado una comprobación de estado en el controlador pasivo.
8	FCP_ARRAY_ERR8	CONMUTADOR CONTROLADOR MATRIZ	Un controlador de la matriz dejó de estar disponible, de modo de E/S se trasladó a otro controlador.
9	FCP_ARRAY_ERR9	ANOMALÍA DE CONMUTADOR DE CONTROLADOR DE MATRIZ DE DISCOS	Un conmutador de controlador de discos ha fallado.
10	FCP_ARRAY_ERR10	CAMBIADA CONFIGURACIÓN MATRIZ DISCOS	Una unidad lógica se ha movido de un controlador a otro (probablemente por la acción de un host alternativo).
11	FCP_ARRAY_ERR11	TIPO UNIDAD IMPROPIA PARA MOD. ACT. DUAL	Este error no es posible en la matriz 2102 y solo existe para fines históricos. FCP_ARRAY_ERR11 se podría reutilizar para un error distinto en el futuro.
12	FCP_ARRAY_ERR12	FALLO AEN SONDEO	Una notificación de error automática ha fallado.
13	FCP_ARRAY_ERR13	FALLO COMUNICACIÓN INTER-CONTROLADOR MATRIZ	Los controladores no pueden comunicarse entre sí. Este error puede ocurrir si uno de los controladores se reinicia mientras se está generando el registro de errores. Sin embargo, también puede indicar un problema con las conexiones de canal de fibra.
14	FCP_ARRAY_ERR14	ANOMALÍA UNIDAD MATRIZ DISCOS	Se ha detectado un error grave o irreparable se detectó en un disco físico del subsistema de almacenamiento. Un ingeniero de sistemas podría ser capaz de obtener la causa exacta con un análisis de los datos de detección.
15	FCP_ARRAY_ERR15	POSIBLE PÉRDIDA DE DATOS/BATERÍA DE CACHÉ BAJA	Si se sustituye una tarjeta controladora, las baterías de la caché podrían drenarse. Las baterías de la caché pueden tardar dos días en recargarse. Durante este tiempo, los errores se registran en el registro de errores. No sustituya el controlador.

Tabla 43. Errores de matriz de discos (continuación)

Número de error	Nombre de error	Tipo de error	Descripción del error
16	FCP_ARRAY_ERR16	CARGA DE BATERÍA DE CACHÉ POR DEBAJO DE 87,5%	Si se sustituye una tarjeta controladora, las baterías de la caché podrían drenarse. Las baterías de la caché pueden tardar dos días en recargarse. Durante este tiempo, los errores se registran en el registro de errores. No sustituya el controlador.
17	FCP_ARRAY_ERR17	NOMBRE MUNDIAL MODIFICADO	Un controlador ha cambiado nombres mundiales. Este error puede producirse si reemplaza el controlador sin antes ponerlo en estado de restablecimiento o si cambia el cableado y hay un controlador diferente con el mismo ID SCSI en el bucle.
18	FCP_ARRAY_ERR18	CONFLICTO DE RESERVA	Una operación ha fallado porque la unidad lógica de la matriz de discos (LUN) ha sido reservada por otro host.
19	FCP_ARRAY_ERR19	REPOSITORIO DE VOLUMEN DE INSTANTÁNEAS COMPLETO	Se ha alcanzado el límite de capacidad del repositorio. Para resolver este error, aumente la capacidad de dicho repositorio.
20	FCP_ARRAY_ERR20	OPERACIÓN DE INSTANTÁNEA DETENIDA POR ADMIN	La operación de FlashCopy (instantánea) ha sido deshabilitada o detenida. Para resolver este error, recree FlashCopy.
21	FCP_ARRAY_ERR21	ERROR DE METADATOS REPOSITORIO INSTANTÁNEAS	Se ha producido un problema con los metadatos del repositorio de FlashCopy (instantánea) durante la operación de FlashCopy. Para resolver este error, recree FlashCopy.
22	FCP_ARRAY_ERR22	DUPLICACIÓN VOLUMEN REMOTO: ORIGEN E/S ILEGAL	La unidad lógica primaria ha recibido E/S de una matriz remota o la unidad lógica secundaria ha recibido E/S de un origen distinto a la unidad lógica primaria. Para resolver este error, repita la operación.
23	FCP_ARRAY_ERR23	OPERACIÓN DE INSTANTÁNEA NO PERMITIDA	Se ha alcanzado el límite de capacidad del repositorio, la operación de FlashCopy (instantánea) ha fallado. Para resolver este error, suprima o recree FlashCopy.
24	FCP_ARRAY_ERR24	REPOSITORIO DE VOLUMEN DE INSTANTÁNEAS COMPLETO	Se ha alcanzado el límite de capacidad del repositorio. Para resolver este error, suprima o recree FlashCopy (instantánea).

Tabla 43. Errores de matriz de discos (continuación)

Número de error	Nombre de error	Tipo de error	Descripción del error
25	FCP_ARRAY_ERR25	LOS DATOS DE CACHÉ SE PERDERÁN SI EL CONTROLADOR FALLA	<p>Este mensaje avisa de que una unidad lógica de matriz de discos (LUN) se está ejecutando con la caché de escritura habilitada y la duplicación de caché deshabilitada. El aviso se muestra cuando el LUN se abre y vuelve a aparecer cada 24 horas hasta que se habilita de nuevo la duplicación de caché.</p> <p>Si un controlador falla o si la alimentación del controlador está apagada mientras el LUN se ejecuta en este modo, los datos que están en la caché de escritura (pero no escritos en el soporte de disco físico) podrían perderse. Esto puede causar daños en los archivos, sistemas de archivos o bases de datos.</p>
26	FCP_ARRAY_ERR26	VOLUMEN LÓGICO PROTEGIDO CONTRA ESCRITURA	<p>El estado de la unidad lógica es de sólo lectura. La razón probable es que sea una unidad lógica secundaria de un FlashCopy, VolumeCopy o par de duplicación remota. Determine qué relación se aplica a la unidad lógica.</p> <ul style="list-style-type: none"> • Para FlashCopy, un estado de sólo lectura en la unidad lógica secundaria por lo general indica que el repositorio está lleno. • Para VolumeCopy, ambas unidades lógicas, primaria y secundaria, son de sólo lectura durante la operación de copia. La unidad lógica secundaria es de sólo lectura cuando la operación de copia se detiene y el par de copia no se ha eliminado. • Para duplicación remota, la unidad lógica secundaria es de sólo lectura siempre que la duplicación esté activa.

Tabla 43. Errores de matriz de discos (continuación)

Número de error	Nombre de error	Tipo de error	Descripción del error
27	FCP_ARRAY_ERR27	CONTROLADOR INDIVIDUAL REINICIADO	<p>El subsistema de almacenamiento está operando como controlador único y se ha reparado un error. El error puede estar causado por un problema de comunicación o hardware, o puede producirse debido a que un LUN se ha trasladado a un controlador que no tiene una ruta al host actual.</p> <p>Si se trata de un subsistema de almacenamiento de controlador dual, encuentre la razón por la que el subsistema de almacenamiento está funcionando en modo de controlador único y resuelva el problema. Entre las posibles razones se encuentran las siguientes:</p> <ul style="list-style-type: none"> • Un HBA, puerto de conmutador, conmutador, subsistema de almacenamiento o controlador de subsistema de almacenamiento no estaba disponible durante el último reinicio del sistema o la última vez que se ejecutó el comando cfgmgr. • Ha eliminado una ruta (dac) como parte de una operación de intercambio en caliente del adaptador de canal de fibra.

Tabla 43. Errores de matriz de discos (continuación)

Número de error	Nombre de error	Tipo de error	Descripción del error
28	FCP_ARRAY_ERR28	FALLO REINICIO CONTROLADOR INDIVIDUAL	<p>El subsistema de almacenamiento está operando como controlador único y no se ha reparado un error. Existe un problema con la ruta entre este host y el subsistema de almacenamiento o con el subsistema de almacenamiento en sí. El host ha intentado comunicarse con el subsistema de almacenamiento y la comunicación ha fallado.</p> <p>Si se ha alcanzado el número de reintentos que se especifica en el atributo ODM switch_retries, el E/S se devuelve al usuario.</p> <p>Repáre el error. A continuación, si se trata de un subsistema de almacenamiento de controlador dual, encuentre la razón por la que el subsistema de almacenamiento está funcionando en modo de controlador único y resuelva el problema. Entre las posibles razones se encuentran las siguientes:</p> <ul style="list-style-type: none"> • Un HBA, puerto de conmutador, conmutador, subsistema de almacenamiento o controlador de subsistema de almacenamiento no estaba disponible durante el último reinicio del sistema o la última vez que se ejecutó el comando cfgmgr. • Ha eliminado una ruta (dac) como parte de una operación de intercambio en caliente del adaptador de canal de fibra.

Se ha creado un nuevo registro de errores DISK_ERR7 para notificar que se ha designado una ruta como fallida debido a un número predeterminado de errores de ES. Esto normalmente está precedido por otros registros de errores que representan el error real que se produce en la ruta.

IBM DS Storage Manager - Restablecer contraseña

Si ha olvidado la contraseña y no puede iniciar sesión en IBM DS Storage Manager, pulse **Restablecer contraseña** en el panel de control y acceda al subsistema.

Para saber dónde está el botón **Restablecer contraseña**, consulte la *Guía de instalación del usuario y de mantenimiento* de su subsistema de almacenamiento.

Apéndice A. Host bus adapter settings

This chapter covers the default settings for a variety of host bus adapters (HBAs) suitable for use with DS3000, DS4000, and DS5000 storage subsystems for Windows, Linux on Intel, VMware ESX, and NetWare operating systems. All other operating systems and platforms must use the default values. See the applicable product documentation for more information.

See the readme file that is included in the Fibre Channel host bus adapter BIOS or device driver package for any up-to-date changes to the settings.

An HBA is used to connect servers to Fibre Channel topologies. Its function is similar to that provided by network adapters to access LAN resources. The device driver for an HBA is typically responsible for providing support for a Fibre Channel topology, whether point-to-point, loop, or fabric.

Important: IBM supports the coexistence of DS3000, DS4000, and DS5000 storage subsystems in the same server, using the same HBAs, only if the application can accommodate the common set of device and multipath driver time-out settings. The common set of time-out settings consists of the longest settings that are published in this section for the DS3000, DS4000, and DS5000 storage subsystems. If this is not possible, and if the multipath driver allows for it, the use of mixed DS3000, DS4000, and DS5000 storage subsystems can still be achieved if the HBAs that you use for DS3000 subsystems are different than the ones that you use for DS4000 or DS5000 storage subsystems. Otherwise, the coexistence of DS3000, DS4000, and DS5000 storage subsystems in the same server is not possible.

See the latest IBM DS controller firmware and Storage Manager readme files for any restrictions on the coexistence of DS3000, DS4000, and DS5000 storage subsystems in the same server. For detailed HBA support information, see www.ibm.com/systems/support/storage/config/ssic.

Ajuste de la configuración de HBA

A menudo es necesario ajustar la configuración de su HBA para que coincida con las prestaciones de su dispositivo. En esta sección se describe cómo acceder a esta configuración para hacer los ajustes necesarios.

Acceso a la configuración de HBA a través de Fast!UTIL

La característica Fast!UTIL proporciona acceso a la configuración del adaptador de bus de host. Para acceder a esta característica, pulse Alt+Q o Ctrl+Q durante la inicialización de BIOS. Puede que el menú de Fast!UTIL tarde unos segundos en aparecer. Si se ha instalado más de un adaptador, Fast!UTIL le pedirá que seleccione el adaptador que desea configurar. Tras cambiar la configuración del adaptador, Fast!UTIL reiniciará el servidor para cargar los nuevos parámetros. Después de entrar a Fast!UTIL, podrá realizar las siguientes selecciones en el menú **Opciones de Fast!UTIL:**

- Valores de configuración
- Prueba de bucle de retorno
- Selección de puerto de adaptador de host

También puede acceder a la configuración del adaptador de bus de host a través del menú **Valores de configuración** de Fast!UTIL; a continuación, seleccione **Configuración del adaptador** o **Configuración avanzada del adaptador**.

Nota: Como alternativa, también puede utilizar el programa QLogic SANsurfer para modificar la **configuración del puerto de adaptador de host** y las preferencias de **Configuración avanzada del adaptador** para en entorno del sistema operativo Microsoft Windows. Para que se apliquen los cambios, debe reiniciar los servidores.

Configuración predeterminada del adaptador de bus de host

Acceda a la configuración del adaptador de bus de host a través del menú **Valores de configuración** de Fast!UTIL y seleccione **Configuración del adaptador**. Los valores del adaptador de bus de host predeterminados de FC2-133 HBA son los siguientes:

Adaptador de host BIOS

Cuando este valor está **Deshabilitado**, el ROM BIOS de FC2-133 HBA está deshabilitado y el espacio pasa a estar disponible en la memoria superior. Este valor debe estar **Habilitado** si va a arrancar desde una unidad de disco de canal ed fibra asociada al adaptador FC2-133. El valor predeterminado es **Deshabilitado**.

Tamaño de marco

este valor especifica la longitud máxima de marco soportada por el FC2-133 HBA. El tamaño predeterminado es 2048, que proporciona el máximo rendimiento para conexiones F-Port (punto a punto).

Retardo desde restablecimiento de bucle

Tras restablecer el bucle, el firmware evita iniciar actividad del bucle alguna durante el número de segundos especificado en este valor. El valor predeterminado es 5 segundos.

ID de bucle de adaptador

Este valor obliga al adaptador a intentar utilizar el identificador especificado en el valor de ID de bucle. El valor predeterminado es **Habilitado**.

ID de bucle

Si el ID de bucle del adaptador está **Habilitado**, el adaptador intentará utilizar el identificador especificado en este valor. El valor predeterminado es 125. Defina este identificador con un valor único de 0 a 125 si hay más de un adaptador conectado a un bucle FC-AL y el valor del ID de bucle del adaptador está **Habilitado**.

Retardo de giro

Cuando este bit está definido, el BIOS espera hasta 5 minutos para buscar la primera unidad. El valor predeterminado es **Deshabilitado**.

Opciones de conexión

Este valor define el tipo de conexión (bucle o de punto a punto) o la preferencia de conexión. El valor predeterminado es 2, es decir bucle a menos que se establezca punto a punto.

Soporte de cinta de canal de fibra

Este valor habilita la recuperación FCP-2. El valor predeterminado es **Habilitado**. Cambie este valor por **Deshabilitado** si el HBA no está conectado a un dispositivo de cinta.

Velocidad de datos

Este valor determina la velocidad de datos. Cuando es 0, el FC2-133 HBA

se ejecuta a 1 Gbps. Cuando es 1, el FC2-133 HBA se ejecuta a 2 Gbps. Cuando este valor es 2, Fast!UTIL determina qué velocidad puede utilizar su sistema y define la misma en consecuencia. El valor predeterminado es 2 (configuración automática).

Configuración avanzada de HBA

Acceda a la configuración del adaptador de bus de host a través del menú **Valores de configuración** de Fast!UTIL y seleccione **Configuración avanzada del adaptador**. Los valores predeterminados de FC2-133 HBA son los siguientes:

Regulador de ejecución

Este valor especifica el número máximo de comandos que se ejecutan en cualquier puerto. Cuando se alcanza un regulador de ejecución del puerto, no se ejecutan nuevos comandos hasta que el comando actual ha terminado. Las opciones válidas para este valor son 1-256. El valor predeterminado es 255.

LUN por destino

Este valor especifica el número de LUN por destino. El soporte de varios LUN normalmente se utiliza para sistemas de matriz redundante de discos independientes (RAID) que utilizan LUN para correlacionar unidades. El valor predeterminado es 0. Para sistemas operativos de host distintos a Microsoft Windows, quizá desee cambiar este ajuste a un valor distinto a 0 para que el host vea más de una unidad lógica desde el subsistema de almacenamiento.

Habilitar restablecimiento de LIP

Este valor determina el tipo de restablecimiento de proceso de inicialización de bucle (LIP) que se utiliza cuando el sistema operativo inicia una rutina de restablecimiento del bus. Si este valor es Sí, el controlador inicia un restablecimiento de LIP global para borrar las reservas de dispositivo de destino. Si este valor es No, el controlador inicia un restablecimiento de LIP global con un inicio de sesión completo. El valor predeterminado es No.

Habilitar Inicio de sesión completo de LIP

Este valor indica al chip ISP que inicie sesión, de nuevo, en todos los puestos tras cualquier LIP. El valor predeterminado es Sí.

Habilitar restablecimiento de destino

Este valor habilita los controladores para que emitan un comando de restablecimiento de destino a todos los dispositivos del bucle cuando se emita un comando de restablecimiento del bus SCSI. El valor predeterminado es Sí.

Recuento de intentos de inicio de sesión

Este valor especifica el número de veces que el software intenta iniciar sesión en un dispositivo. El valor predeterminado es 30 intentos.

Recuento de intentos de caída de puerto

Este valor especifica el número de segundos que transcurren antes de que el software vuelva a intentar un comando a un puerto que indique estado de puerto caído. El valor predeterminado es 30 segundos. Para servidores Microsoft Windows con configuración MSCS, el parámetro BIOS de recuento de intentos de caída de puerto debe cambiar del valor predeterminado, 30, a 70.

Tiempo de espera de enlace caído

Este valor especifica el número de segundos que el software espera para que vuelva a activarse un enlace caído. El valor predeterminado es de 60 segundos.

Registro de errores ampliado

Este valor proporciona información adicional sobre errores y depuración al sistema operativo. Cuando está habilitado, los eventos se registran en el visor de sucesos Windows NT Event Viewer. El valor predeterminado es Deshabilitado.

Modalidad de operación RIO

Este valor especifica las modalidades de operación de interrupción reducida (RIO), si estos son compatibles con el controlador de software. Las modalidades RIO permiten realizar diversas terminaciones de comando en una sola interrupción. El valor predeterminado es 0.

Temporizador de retardo de interrupción

Este ajuste contiene el valor (en incrementos de 100 microsegundos) que utiliza un temporizador para definir el tiempo de espera entre el acceso (DMA) a un conjunto de descriptores y la generación de una interrupción. El valor predeterminado es 0.

QLogic host bus adapter settings

Important: IBM supports the coexistence of DS3000, DS4000, and DS5000 storage subsystems in the same server, using the same HBAs, only if the application can accommodate the common set of device and multipath driver time-out settings. The common set of time-out settings consists of the longest settings that are published in this section for the DS3000, DS4000, and DS5000 storage subsystems. If this is not possible, and if the multipath driver allows for it, the use of mixed DS3000, DS4000, and DS5000 storage subsystems can still be achieved if the HBAs that you use for DS3000 subsystems are different than the ones that you use for DS4000 or DS5000 storage subsystems. Otherwise, the coexistence of DS3000, DS4000, and DS5000 storage subsystems in the same server is not possible.

See the latest IBM DS controller firmware and Storage Manager readme files for any restrictions on the coexistence of DS3000, DS4000, and DS5000 storage subsystems in the same server. For detailed HBA support information, see www.ibm.com/systems/support/storage/config/ssic.

Nota: The BIOS settings in the Windows column are the default values that are set when the adapters are ordered from IBM as IBM FC-2 (QLA2310), FC2-133 (QLA2340) and single-port and dual-port 4 Gbps (QLx2460 and QLx2462) Fibre Channel host bus adapters. If the adapters are not from IBM, the default BIOS might not be the same as those defined in the Microsoft Windows column. There is one exception: the default setting for Fibre Channel tape support is enabled.

Tabla 44 en la página 307 shows the default settings for IBM Fibre Channel FC-2 and FC2-133 (QLogic adapter models QLA2310 and QLA2340) host bus adapter settings (for BIOS V1.35 and later) by operating system as well as the default registry settings for Microsoft Windows operating systems. DS3000, DS4000, or DS5000 products require BIOS V1.43 or later for these adapters. In addition, these settings are also the default BIOS settings for the newer DS3000, DS4000, or DS5000 4 Gbps single and dual-port host bus adapters (QLogic adapter models

QLx2460 and QLx2462). The 4 Gbps host bus adapter BIOS version is 1.12 or later. See the applicable readme file for the latest updates to these values.

Tabla 44. QLogic model QLA234x, QLA24xx, QLE2462, QLE2460, QLE2560, QLE2562, QMI2572, QMI3572, QMI2582

Item	Default	VMware	Windows 2000	Windows 2003 and Windows 2008	Solaris	LINUX MPP	LINUX DMMP	NetWare
BIOS settings								
Host Adapter settings								
Host Adapter BIOS	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Frame Size	2048	2048	2048	2048	2048	2048	2048	2048
Loop Reset Delay	5	5	8	8	8	8	8	8
Adapter Hard Loop ID – (only for arbitrated loop topology).	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
Hard Loop ID (must be unique for each HBA) – (only for arbitrated loop topology).	0	125 ¹	125 ¹	125 ¹	125 ¹	125 ¹	125 ¹	125 ¹
Spin-up Delay	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Connect Options	2	2	2	2	2	2	2	2
Fibre Channel Tape Support	Disabled	Disabled ³	Disabled ³	Disabled ³	Disabled ³	Disabled ³	Disabled ³	Disabled ³
Data Rate	2	2 (Auto)	2 (Auto)	2 (Auto)	2 (Auto)	2 (Auto)	2 (Auto)	2 (Auto)
Advance Adapter Settings								
Execution Throttle	16	256	256	256	256	256	256	256
LUNs per Target	8	0	0	0	0	0	0	32
Enable LIP Reset	No	No	No	No	No	No	No	No
Enable LIP Full Login	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enable Target Reset	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Login Retry Count	8	30	30	30	30	30	30	30
Port Down Retry Count (5.30 controller firmware and earlier)	8	30	30	30	30	12	12	70
Port Down Retry Count	8	70	DS3K: 144 DS4K/5K: 70 ²	DS3K: 144 DS4K/5K: 70 ²	70	DS3K: 70 DS4K5K: 35	10	70
Link Down Timeout	30	60	DS3K:144 DS4K/5K: 60	DS3K:144 DS4K/5K: 60	60	DS3K:144 DS4K/5K: 60	NA	60
Extended Error Logging	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
RIO Operation Mode	0	0	0	0	0	0	0	0
Interrupt Delay Timer	0	0	0	0	0	0	0	0
IOCB Allocation	256	256	256	256	256	256	256	256

Tabla 44. QLogic model QLA234x, QLA24xx, QLE2462, QLE2460, QLE2560, QLE2562, QMI2572, QMI3572, QMI2582 (continuación)

Item	Default	VMware	Windows 2000	Windows 2003 and Windows 2008	Solaris	LINUX MPP	LINUX DMMP	NetWare
>4 GB Addressing	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Drivers Load RISC Code	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
Enable Database Updates	No	No	No	No	No	No	No	No
Disable Database Load	No	No	No	No	No	No	No	No
Fast Command Posting	Disabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
Extended Firmware Settings (1.34 and Earlier)								
Extended Control Block	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
RIO Operation Mode	0	0	0	0	0	0	0	0
Connection Options	2	2	2	2	2	2	2	2
Class 2 Service	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
ACK0	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Fibre Channel Tape Support	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Fibre Channel Confirm	Enabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Command Reference Number	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Read Transfer Ready	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled
Response Timer	0	0	0	0	0	0	0	0
Interrupt Delay Timer	0	0	0	0	0	0	0	0
Data Rate	2	2 (Auto)	2 (Auto)	2 (Auto)	2 (Auto)	2 (Auto)	2 (Auto)	2 (Auto)

REGISTRY SETTINGS⁵

(HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\QL2300\Parameters\Device)

LargeLuns	1	1	N/A	N/A	N/A	N/A	N/A	N/A
MaximumSGList	0x21	0xff	0xff	0xff	N/A	N/A	N/A	N/A

O/S REGISTRY SETTINGS⁵

(HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\QL2300\Parameters\Device) under DriverParameter variable.

Nota:

1. Prior to QLogic driver versions 9.1.x.x, the variable name used was DriverParameters instead of DriverParameter.
2. DriverParameter is of type REG_SZ and the following parameters are added to the DriverParameters string. Do not create a separate key for each of the parameters.

UseSameNN	1	1	1	1	N/A	N/A	N/A	N/A
BusChange (SCSI Port Miniport 9.0.1.60 and earlier – does not apply to 9.1.1.11 and newer)	2	N/A	0	0	N/A	N/A	N/A	N/A

Tabla 44. QLogic model QLA234x, QLA24xx, QLE2462, QLE2460, QLE2560, QLE2562, QMI2572, QMI3572, QMI2582 (continuación)

Item	Default	VMware	Windows 2000	Windows 2003 and Windows 2008	Solaris	LINUX MPP	LINUX DMMP	NetWare
TimeOutValue 4 (REG_DWORD)	0x3C	N/A	DS3K: xA0 DS4K/5K: x78	DS3K: xA0 DS4K/5K: x78	N/A	N/A	N/A	N/A

REGISTRY SETTINGS⁵

(HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<FAILOVER>\parameters: Where <FAILOVER>=Rdacdisk for MPP or RDAC installations or <FAILOVER>=mppdsm, ds4dsm, md3dsm, sx3dsm, csmdsm, or tpsdsm for MPIO installations. Mppdsm is for the generic version, your installation could be different.)

SynchTimeOut (REG_DWORD)	0x78	N/A	DS3K: xA0 DS4K/5K: x78	DS3K: xA0 DS4K/5K: x78				
DisableLunRebalance (Only applies to cluster configurations. Firmware version 6.xx.xx.xx and later.)	0x00	N/A	0x03	0x03				

SuSE 7.3 specific modifications:

- Offset 0x11 in the Linux region (6) of the array controller NVSRAM must be changed from the default of 0x20 to 0x7f. The following command can be run from the script engine:
 - Set controller[a] HOSTNVSRAMByte[6,0x11]=0x7f;
 - Set controller[b] HOSTNVSRAMByte[6,0x11]=0x7f;
- The QLogic driver source must be modified to reflect the symbolic link used by SuSE.
 - vi makefile
 - find OSVER and change it from OSVER=linux-2.4 to OSVER=linux
 - Save and quit

Red Hat Linux Advanced Server 2.1 / SuSE Linux Enterprise Server 8.0 (6.x series failover driver [with no RDAC] only). Append the following to the HBA driver option string in the /etc/modules.conf file: ql2xretrycount=60 ql2xsuspendcount=40

If you are running the QLogic Inbox driver, the string options qla2xxx qlport_down_retry=144 (PB1-3) or options qla2xxx qlport_down_retry=70 (PB4-6) must be added in /etc/modprobe.conf (for RHEL) or /etc/modprobe.conf.local (for SLES). For all prior (RH3/4 SLES8/9) Linux versions (and out-of-box drivers), the string options qla2xxx qlport_down_retry=72 (PB1-3) or options qla2xxx qlport_down_retry=35 (PB4-6) must be added instead.

Tabla 44. QLogic model QLA234x, QLA24xx, QLE2462, QLE2460, QLE2560, QLE2562, QMI2572, QMI3572, QMI2582 (continuación)

Item	Default	VMware	Windows 2000	Windows 2003 and Windows 2008	Solaris	LINUX MPP	LINUX DMMP	NetWare
------	---------	--------	--------------	-------------------------------	---------	-----------	------------	---------

Nota:

1. This setting must be changed to a unique AL-PA value if there is more than one Fibre Channel device in the FC-AL loop.
2. For larger configurations with heavy I/O loads or in a Microsoft cluster service (MSCS) environment, this value might be increased.
3. Change this setting to Enabled or Supported when the HBA is connected to a tape device only. Set it to Disabled when you connect to a DS3000, DS4000, or DS5000 storage subsystem.
4. In certain storage subsystem maximum configuration installations, you might have to set the TimeOutValue to 120 (decimal). Changing this value to a higher value might affect your application especially when it requires the disk I/O completion acknowledgement within a certain amount of time.
5. You can access registry settings by clicking **Start**, select **Run...**, type regedit into the **Open:** field, and then click **OK**.

Atención: Exercise caution when you change the Windows registry. If you change the wrong registry entry or make an incorrect entry for a setting, you can cause an error that prevents your server from booting or operating correctly.

Nota: The BIOS settings under the Windows column are the default values that are set when the adapters are ordered from IBM as IBM Fibre Channel host bus adapters. If the adapters are not from IBM, the default BIOS might not be the same as the ones that are defined in the Microsoft Windows column. There is one exception: the default setting for Fibre Channel tape support is enabled.

Tabla 45 shows the default settings for various IBM DS3000, DS4000, or DS5000 Fibre Channel host bus adapters (QLogic adapter QL220x) models (for BIOS V1.81) by operating system. See the applicable readme file for the latest updates to these values.

Tabla 45. QLogic model QL220x (for BIOS V1.81) host bus adapter settings by operating system

Item	Windows		Linux	NetWare
	NT	2000 / Server 2003		
BIOS settings				
Host Adapter settings				
Host Adapter BIOS	Disabled	Disabled	Disabled	Disabled
Frame Size	2048	2048	2048	2048
Loop Reset Delay	5	5	8	5
Adapter Hard Loop ID	Enabled	Enabled	Enabled	Enabled
Hard Loop ID (must be unique for each HBA)	125 ¹	125 ¹	125 ¹	125 ¹
Spin Up Delay	Disabled	Disabled	Disabled	Disabled
Advanced adapter settings				
Execution Throttle	256	256	256	256
>4 Gbyte Addressing	Disabled	Disabled	Disabled	Disabled
LUNs per Target	0	0	0	32

Tabla 45. QLogic model QL220x (for BIOS V1.81) host bus adapter settings by operating system (continuación)

Enable LIP Reset	No	No	No	No
Enable LIP Full Login	Yes	Yes	Yes	Yes
Enable Target Reset	Yes	Yes	Yes	Yes
Login Retry Count	30	30	30	30
Port Down Retry Count	30	30	12	30 ²
IOCB Allocation	256	256	256	256
Extended Error Logging	Disabled	Disabled	Disabled	Disabled
Extended Firmware Settings				
Extended Control Block	Enabled	Enabled	Enabled	Enabled
RIO Operation Mode	0	0	0	0
Connection Options	3	3	3	3
Class 2 Service	Disabled	Disabled	Disabled	Disabled
ACK0	Disabled	Disabled	Disabled	Disabled
Fibre Channel Tape Support	Supported ³	Supported ³	Supported ³	Supported ³
Fibre Channel Confirm	Disabled	Disabled	Disabled	Disabled
Command Reference Number	Disabled	Disabled	Disabled	Disabled
Read Transfer Ready	Disabled	Disabled	Disabled	Disabled
Response Timer	0	0	0	0
Interrupt Delay Time	0	0	0	0
Registry settings ⁴ (HKEY_LOCAL_MACHINE → System → CurrentControlSet → Services → QL2200 → Parameters → Device)				
LargeLuns		1		
MaximumSGList	0x21	0x21		
Registry settings ⁴ (HKEY_LOCAL_MACHINE → System → CurrentControlSet → Services → Disk)				
TimeOutValue ⁴ (REG_DWORD)	0x3C	0x3C		
Registry settings ⁴ (HKEY_LOCAL_MACHINE → System → CurrentControlSet → Services → QL2200 → Parameters → Device) under the DriverParameter variable				
BusChange		0		

Nota:

1. This setting must be changed to a unique AL-PA value if there is more than one Fibre Channel device in the FC-AL loop.
2. For larger configurations with heavy I/O loads, change this value to 70.
3. Change this setting to Enable or Supported when the HBA is connected to a tape device only. Set it to Disabled when you connect to DS3000, DS4000, or DS5000 Storage Subsystem.
4. To access registry settings, click **Start**, select **Run**, type regedit into the **Open** field, and then click **OK**.
Atención: Exercise caution when you change the Windows registry. If you change the wrong registry entry or make an incorrect entry for a setting, you can cause an error that prevents your server from booting or operating correctly.

Configuración de adaptador de bus de host JNI y QLogic

Las siguientes tablas detallan los valores de diferentes adaptadores de bus de host (HBA) para Sun Solaris.

Nota: Los adaptadores de bus de host JNI solo se soportan en Solaris 8 y 9. No son compatibles con Solaris 10.

Configuración de tarjeta JNI HBA

Las tarjetas JNI no son dispositivos Conectar y listo con configuración automática. Tendrá que cambiar la configuración o enlaces.

Valores de configuración para FCE-1473/FCE-6460/FCX2-6562/FCC2-6562

Los modelos de adaptador de bus de host JNI FCE-1473, FCE-6460, FCX2-6562 y FCC2-6562 son compatibles con todos los niveles actualmente soportados de firmware de controlador de subsistema de almacenamiento.

Importante: Para cada valor indicado en la Tabla 46, debe eliminar los comentarios de la línea. Esto ocurre tanto con los valores predeterminados como con los valores que debe modificar.

Tabla 46. Valores de configuración para FCE-1473/FCE-6460/FCX2-6562/FCC2-6562

Valor original	Valor nuevo
FcLoopEnabled = 1	FcLoopEnabled = 0 (para no bucle; topología automática) FcLoopEnabled = 1 (para bucle)
FcFabricEnabled = 0	FcFabricEnabled = 0 (para no tejido; topología automática) FcFabricEnabled = 1 (para tejido)
FcEngHeartbeatInterval = 5	Igual que valor original (en segundos)
FcLinkUpRecoveryTime = 1000	Igual que valor original (en milisegundos)
BusRetryDelay = 5000	Igual que valor original (en milisegundos)
TargetOfflineEnable = 1	TargetOfflineEnable = 0 (Inhabilitar) TargetOfflineEnable = 1 (Habilitar)
FailoverDelay = 30;	FailoverDelay = 60 (en segundos)
FailoverDelayFcTape = 300	Igual que valor original (segundos)
TimeoutResetEnable = 0	Igual que valor original
QfullRetryCount = 5	Igual que valor original
QfullRetryDelay = 5000	Igual que valor original (en milisegundos)
LunRecoveryInterval = 50	Igual que valor original (en milisegundos)
FcLinkSpeed = 3	Igual que valor original
JNICreationDelay = 1	JNICreationDelay = 10 (en segundos)
FlogiRetryCount = 3	Igual que valor original
FcFlogiTimeout = 10	Igual que valor original (en segundos)
PlogiRetryCount = 3	Igual que valor original
PlogiControlSeconds = 30	Igual que valor original (en segundos)
LunDiscoveryMethod = 1	Igual que valor original (informe de LUN)
CmdTaskAttr = 0	CmdTaskAttr = 0 (cola simple) CmdTaskAttr = 1 (sin etiqueta)
automap = 0	automap = 1 (Habilitar)

Tabla 46. Valores de configuración para FCE-1473/FCE-6460/FCX2-6562/FCC2-6562 (continuación)

Valor original	Valor nuevo
FclpEnable = 1	FclpEnable = 0 (Inhabilitar)
OverrunFailoverCount = 0	Igual que valor original
PlogiRetryTime = 50	Igual que valor original
SwitchGidPtSyncEnable = 0	Igual que valor original
target_throttle = 256	Igual que valor original
lun_throttle = 64	Igual que valor original
Añada estos valores.	target0_hba = "jnic146x0";
	target0_wwpn = "<controller wwpn>"
	target1_hba = "jnic146x1";
	target1_wwpn = "<controller wwpn>"

Nota: Quizá deba ejecutar el script de reconfiguración /etc/raid/bin/genjnicnf desde el shell Solaris:

```
# /etc/raid/bin/genjnicnf
```

Valores de configuración para FCE-1063/FCE2-1063/FCE-6410/FCE2-6410

Los modelos de adaptador de bus de host JNI FCE-1063, FCE2-1063, FCE-6410 y FCE2-6410 son compatibles con todos los niveles actualmente soportados de firmware de controlador de subsistema de almacenamiento.

Nota: Para cada valor indicado en la Tabla 47, debe eliminar los comentarios de la línea. Esto ocurre tanto con los valores predeterminados como con los valores que debe modificar.

Tabla 47. Valores de configuración para FCE-1063/FCE2-1063/FCE-6410/FCE2-6410

Valor original	Valor nuevo
FcLoopEnabled = 1	FcLoopEnabled = 0 (para no bucle) FcLoopEnabled = 1 (para bucle)
FcFabricEnabled = 0	FcFabricEnabled = 0 (para no tejido) FcFabricEnabled = 1 (para tejido)
FcPortCfgEnable = 1	FcPortCfgEnable = 0 (configuración de puerto no necesaria) FcPortCfgEnable = 1 (configuración de puerto necesaria)
FcEngHeartbeatInterval = 5	Igual que valor original (en segundos)
FcLrrTimeout = 100	Igual que valor original (en milisegundos)
FcLinkUpRecoverTime = 1000	Igual que valor original (en milisegundos)
BusyRetryDelay = 5000	Igual que valor original (en milisegundos)
FailoverDelay = 30;	FailoverDelay = 60;
TimeoutResetEnable = 0	Igual que valor original
QfullRetryCount = 5	Igual que valor original
QfullRetryDelay = 5000	Igual que valor original (en milisegundos)

Tabla 47. Valores de configuración para FCE-1063/FCE2-1063/FCE-6410/FCE2-6410 (continuación)

Valor original	Valor nuevo
loRecoveryDelay = 50	Igual que valor original (en milisegundos)
JniCreationDelay = 5;	JniCreationDelay = 10;
FlogiRetryCount = 3	Igual que valor original
PlogiRetryCount = 5	Igual que valor original
FcEmIdEndTcbTimeCount = 1533	Igual que valor original
target_throttle = 256	Igual que valor original (regulador predeterminado para todos los destinos)
lun_throttle = 64	Igual que valor original (regulador predeterminado para todos los LUN)
automap = 0	automap = 0 (enlace de persistencia) automap = 1 (correlación automática)
Añada estos valores.	target0_hba = "jnic146x0"; target0_wwpn = "controller_wwpn" target1_hba = "jnic146x1"; target1_wwpn = "controller_wwpn"

- Quizá deba ejecutar el script de reconfiguración /etc/raid/bin/genjnicnf desde el shell Solaris:
/etc/raid/bin/genjnicnf
- Defina portEnabled = 1; solo cuando vea tarjetas JNI que accedan al modo no participativo en el archivo /var/adm/messages. En estas condiciones, siga estos pasos:
 1. Defina FcPortCfgEnabled = 1;
 2. Reinicie el host.
 3. Defina FcPortCfgEnabled = 0;
 4. Reinicie el host de nuevo.

Cuando lo haya hecho, compruebe /var/adm/messages para asegurarse de que define las tarjetas JNI en modo tejido o bucle.

Valores de configuración para FCI-1063

El adaptador de bus de host JNI modelo FCI-1063 *solo* se soporta en configuraciones de subsistema de almacenamiento con versión de firmware de controlador 05.4x.xx.xx o anterior.

Nota: Para cada valor indicado en la Tabla 48, debe eliminar los comentarios de la línea. Esto ocurre tanto con los valores predeterminados como con los valores que debe modificar.

Tabla 48. Valores de configuración para FCI-1063

Valor original	Valor nuevo
scsi_initiator_id = 0x7d	Igual que valor original
fca_nport = 0;	fca_nport = 1 (para tejido) / fca_nport = 0 (para bucle)
public_loop = 0	Igual que valor original

Tabla 48. Valores de configuración para FCI-1063 (continuación)

Valor original	Valor nuevo
target_controllers = 126	Igual que valor original
ip_disable = 1;	Igual que valor original
ip_compliant = 0	Igual que valor original
qfull_retry_interval = 0	Igual que valor original
qfull_retry_interval = 1000	Igual que valor original (en milisegundos)
failover = 30;	failover = 60 (en segundos)
failover_extension = 0	Igual que valor original
recovery_attempts - 5	Igual que valor original
class2_enable = 0	Igual que valor original
fca_heartbeat = 0	Igual que valor original
reset_glm = 0	Igual que valor original
timeout_reset_enable = 0	Igual que valor original
busy_retry_delay= 100;	Igual que valor original (en milisegundos)
link_recovery_delay = 1000;	Igual que valor original (en milisegundos)
scsi_probe_delay = 500;	scsi_probe_delay = 5000 (en milisegundos; 10 resolución milisegundos)
def_hba_binding = "fca-pci*";	def_hba_binding = "nonjni"; (para enlace) def_hba_binding = "fcaw"; (para no enlace)
def_wwnn_binding = "\$xxxxxx"	def_wwnn_binding = "xxxxxx"
def_wwpn_binding = "\$xxxxxx"	Igual que la entrada original
fca_verbose = 1	Igual que la entrada original
Será añadido por el script de reconfiguración	name="fca-pci" parent="physical path" unit-address="#"
Será añadido por el script de reconfiguración	target0_hba="fca-pci0" target0_wwpn="controller wwpn";
Será añadido por el script de reconfiguración	name="fca-pci" parent="physical path" unit-address="#"
Será añadido por el script de reconfiguración	target0_hba="fca-pci1" target0_wwpn= "controller wwpn";

Nota: Quizá deba ejecutar el script de reconfiguración /etc/raid/bin/genjnicnf desde el shell Solaris:

```
# /etc/raid/bin/genjnicnf
```

Valores de configuración para FC64-1063

El adaptador de bus de host JNI modelo FC64-1063 *solo* se soporta en configuraciones de subsistema de almacenamiento con versión de firmware de controlador 05.4x.xx.xx o anterior.

Importante: Para cada valor indicado en la Tabla 49 en la página 316, debe eliminar los comentarios de la línea. Esto ocurre tanto con los valores predeterminados como con los valores que debe modificar.

Tabla 49. Valores de configuración para FC64-1063

Valor original	Valor nuevo
fca_nport = 0;	fca_nport =1;
ip_disable = 0;	ip_disable=1;
failover = 0;	failover =30;
busy_retry_delay = 5000;	busy_retry_delay = 5000;
link_recovery_delay = 1000;	link_recovery_delay = 1000;
scsi_probe_delay = 5000;	scsi_probe_delay = 5000;
def_hba_binding = "fcaw*";	Configuraciones de conexión directa: def_hba_binding = "fcaw*"; Configuraciones asociadas con SAN: def_hba_binding = "nonJNI";
def_wwnn_binding = "\$xxxxxx"	def_wwnn_bindindef_hba_ binding = "nonjni"; g = "xxxxxx"
def_wwnn_binding = "\$xxxxxx"	Igual que la entrada original
Será añadido por el script de reconfiguración	name="fcaw" parent="<physical path>"unit-address="<#>"
Será añadido por el script de reconfiguración	target0_hba="fcaw0" target0_wwpn="<controller_wwpn>";
Será añadido por el script de reconfiguración	name="fcaw" parent="<physical path>"unit-address="<#>"
Será añadido por el script de reconfiguración	target0_hba="fcaw0" target0_wwpn= "<controller_wwpn>";

Nota: Quizá deba ejecutar el script de reconfiguración /etc/raid/bin/genscsiconf desde el indicador de shell:

```
# /etc/raid/bin/genscsiconf
```

Valores de HBA de QLogic

Los HBA de QLogic no son elementos Conectar y listo con configuración automática. Deberá cambiar los valores o enlaces, como se describe en Tabla 50 en la página 317.

Nota: En Tabla 50 en la página 317, el HBA se identifica como hba0. No obstante, puede modificar los valores de ambos HBA de QLogic: hba0 y hba1.

Al modificar los valores de hba1, utilice los mismos valores que se indican en la tabla, pero cambie todas las instancias de hba0 por hba1, como se muestra en el ejemplo siguiente.

HBA	Valor original	Valor nuevo
hba0	hba0-execution-throttle=16;	hba0-execution-throttle=255;
hba1	hba1-execution-throttle=16;	hba1-execution-throttle=255;

En el Editor vi, elimine los comentarios y modifique los atributos de bucle de cada HBA de QLogic utilizando los valores especificados en Tabla 50 en la página 317.

Tabla 50. Valores de configuración para QL2342

Valor original	Valor nuevo	Comentarios
max-frame-length=2048;	max-frame-length=2048	Utilice el valor predeterminado
execution-throttle=16;	execution-throttle=255;	Cambiar
login-retry-count=8;	login-retry-count=30;	Cambiar
enable-adapter-hard-loop-ID=0;	enable-adapter-hard-loop-ID=1;	Cambiar
adapter-hard-loop-ID=0;	adapter-hard-loop-ID=0;	Debe ser un número único
enable-LIP-reset=0;	enable-LIP-reset=0;	Utilice el valor predeterminado
hba0-enable-LIP-full-login=1;	hba0-enable-LIP-full-login=1;	Utilice el valor predeterminado
enable-target-reset=0;	enable-target-reset=0;	Utilice el valor predeterminado
reset-delay=5	reset-delay=8	Cambiar
port-down-retry-count=8;	port-down-retry-count=70;	Cambiar
maximum-luns-per-target=8;	maximum-luns-per-target=0;	Cambiar
connection-options=2;	connection-options=2;	Utilice el valor predeterminado
fc-tape=1;	fc-tape=0;	Cambiar
loop-reset-delay = 5;	loop-reset-delay = 8;	Cambiar
> gbyte-addressing = disabled;	> gbyte-addressing = enabled;	Cambiar
link-down-timeout = 30;	link-down-timeout = 60;	Cambiar

Apéndice B. Uso de un subsistema de almacenamiento con una configuración de VMware ESX Server

El software Storage Manager actualmente no está disponible para sistemas operativos VMware ESX Server. Así, para gestionar subsistemas de almacenamiento DS3000, DS4000 y DS5000 con su host VMware ESX Server, debe instalar el software cliente Storage Manager (SMclient) en una estación de gestión Windows o Linux. Puede tratarse de la misma estación de trabajo que utiliza para la Interfaz de gestión de VMware ESX Server basada en navegador. Además, para habilitar el Acceso asimétrico a unidad lógica (ALUA) debe tener el sistema operativo VMware ESX Server versión 4.1 u2 o posterior y 5.0 u1 o posterior.

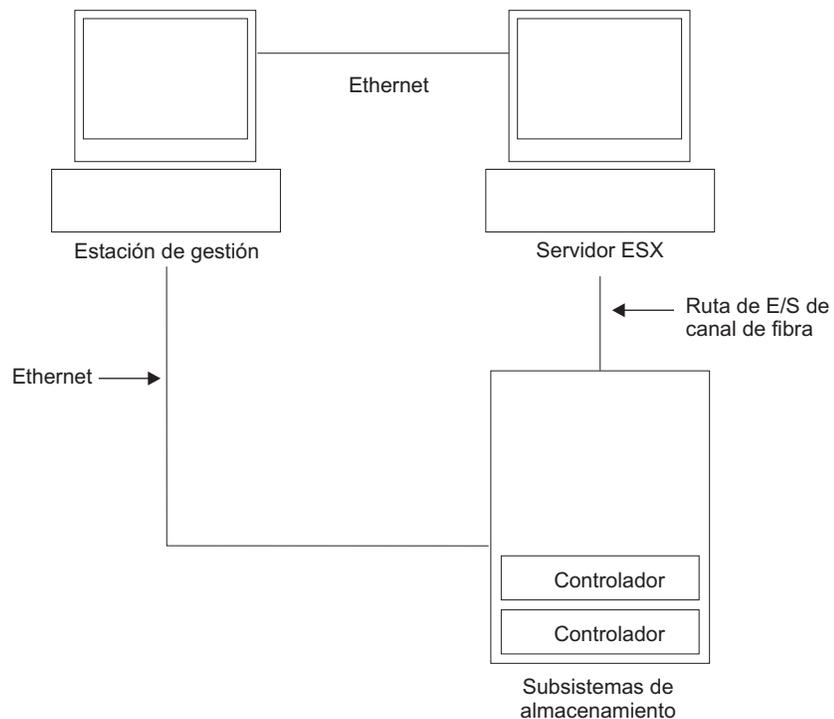
Para obtener información adicional sobre el uso de un subsistema de almacenamiento DS3000, DS4000 o DS5000 con un host VMware ESX Server, consulte "Restricciones de VMware ESX Server" en la página 321.

También puede visitar el System Storage Interoperation Center en el siguiente sitio web:

www.ibm.com/systems/support/storage/config/ssic

Configuración de ejemplo

Figura 34 en la página 320 muestra un ejemplo de configuración del servidor de VMware ESX.



SJ001150

Requisitos de Software

Esta sección describe el software necesario para utilizar un sistema operativo VMware ESX Server con un subsistema de almacenamiento DS3000, DS4000 o DS5000.

Estación de gestión

Para la estación de gestión Windows o Linux se requiere el software siguiente:

1. SM Runtime (solo Linux)
2. SMclient (Linux y Windows)

Host (VMware ESX Server)

Para VMware ESX Server se necesita el siguiente software:

- VMware ESX Server (con DS3000, DS4000 o DS5000 versión de firmware de controlador 07.1x.xx.xx)
- Controlador de VMware ESX Server para HBA de canal de fibra
- Controlador de VMware ESX Server para configuración de migración tras error de controlador QLogic
- VMware ESX Server Tools (instalado en todas las máquinas virtuales que utilicen unidades lógicas DS3000, DS4000 o DS5000)

Versiones anteriores de VMware ESX Server:

1. VMware ESX Server 2.1 soportado solo con DS4000 y DS5000 con firmware de controlador versión 06.12.xx.xx.
2. VMware ESX Server 2.0 soportado solo con DS4000 y DS5000 con firmware de controlador versión 05.xx.xx.xx.

Agrupación en clúster de SO invitado: Si quiere crear una configuración de clúster de SO invitado, debe utilizar el software Microsoft Cluster Services, además de seguir los requisitos de software host indicados en esta sección.

Agrupación en clúster host VMWare: VMware ESX Server 2.5 y superior se facilita con un planificador de recursos distribuidos y alta disponibilidad para la agrupación en clúster, lo cual le permite agregar diversos recursos de host en una agrupación de recursos. (Un clúster DRS es de manera implícita una agrupación de recursos).

Para obtener información sobre la agrupación en clúster de Windows con VMware ESX Server, consulte la Guía de instalación de ESX Server 2.5 en el siguiente sitio web: <http://www.vmware.com/support/pubs/>.

Requisitos de hardware

Puede utilizar servidores host VMware ESX Server con los siguientes tipos de subsistemas de almacenamiento y alojamientos de expansión del almacenamiento. Para obtener información adicional, consulte el Centro de interoperación de System Storage en el siguiente sitio web:

<http://www.ibm.com/systems/support/storage/config/ssic>

Nota: Para conocer los requisitos generales del subsistema de almacenamiento, consulte Capítulo 1, "Preparación de la instalación", en la página 1.

Subsistemas de almacenamiento DS5000

- DS5300
- DS5100

Subsistemas de almacenamiento DS4000

- DS4100 (solo unidades con controlador dual)
- DS4200
- DS4300 (solo unidades con controlador dual)
- DS4400
- DS4500
- DS4700
- DS4800

Alojamientos de expansión del almacenamiento DS5000

- EXP5000

Alojamientos de expansión del almacenamiento DS4000

- EXP100
- EXP420 (solo con DS4200)
- EXP500
- EXP700
- EXP710
- EXP810

Restricciones de VMware ESX Server

Restricciones de SAN y conectividad:

- Los hosts VMware ESX Server solo soportan configuraciones de subsistema de almacenamiento gestionado por el agente de host (fuera de banda). Las configuraciones de gestión de conexión directa (dentro de banda) no son compatibles.
- Los hosts VMware ESX Server pueden soportar diversos adaptadores de bus de host (HBA) y dispositivos DS3000, DS4000 y DS5000. No obstante existen limitaciones sobre el número de HBA que se pueden conectar a un mismo subsistema de almacenamiento. Puede configurar hasta dos HBA por partición y hasta dos particiones por subsistema de almacenamiento. Se pueden añadir HBA adicionales para subsistemas de almacenamiento adicionales y otros dispositivos SAN, hasta alcanzar el límite de su plataforma de subsistema de almacenamiento específica.
- Cuando utiliza dos HBA en un VMware ESX Server, los números de LUN deben ser los mismos para cada HBA conectado al subsistema de almacenamiento.
- Se permiten configuraciones de HBA único, pero cada una de ellas requiere que ambos controladores del subsistema de almacenamiento estén conectados a un HBA a través de un conmutador. Si están conectados a través de un conmutador, ambos controladores deben estar en la misma zona SAN que el HBA.

Atención: Una configuración de un solo HBA puede provocar la pérdida de acceso a datos en caso de error en la ruta.

- Se aceptan configuraciones de conmutador único, pero cada combinación de HBA y controlador de subsistema de almacenamiento debe estar en una zona SAN.
- Otros dispositivos de almacenamiento como, por ejemplo dispositivos de cinta y demás almacenamientos en disco, han de estar conectados a través de zonas HBA y SAN distintas.

Restricciones de partición:

- El número máximo de particiones por host VMware ESX Server y subsistema de almacenamiento es dos.
- Todas las unidades lógicas configuradas para VMware ESX Server deben correlacionarse en un grupo de host VMware ESX Server.

Nota: El tipo de host específico VMware ESX Server no está disponible para subsistemas de almacenamiento DS3000, DS4000, o DS5000 si la versión de firmware de controlador es anterior a la versión 7.70.xx.xx. Utilice el tipo de host LNXCLVMWARE para sus hosts y grupos de hosts VMware. Si utiliza el grupo de host predeterminado, asegúrese de que este es LNXCLVMWARE. Los subsistemas de almacenamiento DS con firmware de controlador 7.70.xx.xx o posterior tienen un tipo de host específico VMware ESX Server definido, llamado VMWARE. VMWARE se debe utilizar como tipo de host de los host y grupos de host VMWare.

- En una configuración de subsistema de almacenamiento DS4100, debe asignar inicialmente los LUN al controlador A en el HBA con menor número. Una vez inicializados los LUN, puede cambiar la ruta al controlador B. (Esta restricción se corregirá en una versión futura de ESX Server).
- Asigne LUN al ESX Server empezando por el LUN número 0.
- No correlacione un LUN de acceso (UTM) a ningún host o grupo de host ESX Server. Los LUN de acceso(UTM) solo se utilizan con configuraciones de subsistemas de almacenamiento gestionados dentro de banda, que VMware ESX Server no soporta actualmente.

Restricciones de la migración tras error:

- Debe utilizar el controlador de migración tras error VMware ESX Server para configuraciones multi-ruta. Otros controladores de migración tras error (como RDAC) no se soportan en configuraciones de VMware ESX Server.
- La política de migración tras error predeterminada para todos los subsistemas de almacenamiento ahora es MRU (utilizada más recientemente).
- Utilice el tipo de host LNXCLVMWARE (si el firmware de controlador es anterior a la versión 7.70.xx.xx) o VMWARE (si el firmware de controlador es 7.70.xx.xx o posterior) en configuraciones VMware ESX Server (2.0 y superior). El tipo de host LNXCLVMWARE o VMWARE inhabilita automáticamente la Transferencia automática de unidad (ADT).

Restricciones de interoperabilidad:

- Los subsistemas de almacenamiento DS4100 y DS4300 *de controlador único* no se soportan con hosts VMware ESX Server. (Los subsistemas de almacenamiento DS4100 y DS4300 *de controlador dual* sí se soportan).

- Los alojamientos de expansión de almacenamiento EXP700 no están soportados con subsistemas de almacenamiento DS4800. Debe actualizar a alojamientos de expansión del almacenamiento EXP710.

Otras restricciones:

- La Expansión dinámica de unidad lógica (DVE) no se soporta para LUN con formato VMFS en sistemas operativos VMware ESX Server anteriores a la versión 2.5.x. Para obtener información sobre la disponibilidad de características de Servicio de copia de DS soportadas en configuraciones de VMware ESX Server 2.5 Server y superiores, póngase en contacto con su representante de soporte de IBM.
- No arranque su sistema desde un dispositivo SATA.

Otra información sobre host VMware ESX Server

Para obtener más información sobre la configuración de su host VMware ESX Server, consulte la documentación y archivos léame disponibles en el siguiente sitio web:

www.vmware.com/support/pubs/

Para obtener más información sobre la instalación del sistema operativo VMware ESX Server en un servidor IBM, consulte el sitio web de soporte de IBM en:

www-03.ibm.com/systems/i/advantages/integratedserver/vmware/

Configuración de subsistemas de almacenamiento para VMware ESX Server

Para poder configurar un subsistema de almacenamiento, debe configurar físicamente el servidor host, tejido SAN y controladores del subsistema de almacenamiento, asignar direcciones IP iniciales a los controladores e instalar SMclient en la estación de gestión Windows o Linux. Consulte Capítulo 4, "Configuración del almacenamiento", en la página 65 para conocer los procedimientos de configuración del subsistema de almacenamiento.

Configuración de conexiones cruzadas para conexiones VMware

Cuando los hosts VMware están conectados a un subsistema de almacenamiento DS3000, DS4000 o DS5000, se necesita una configuración de red de área de almacenamiento (SAN) de conexión cruzada. Cada adaptador de bus de host (HBA) de un host VMware debe tener una ruta a cada uno de los controladores del subsistema de almacenamiento. Figura 35 en la página 324 muestra las conexiones cruzadas para configuraciones de VMware Server.

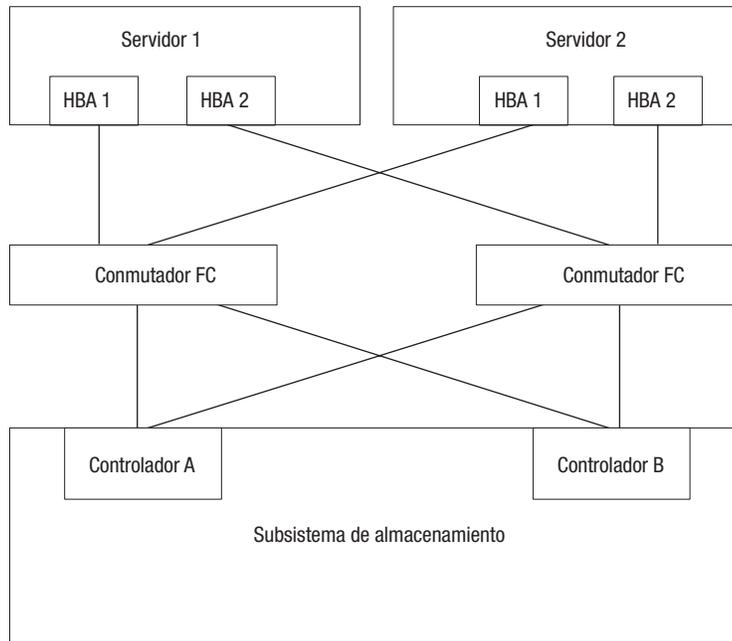


Figura 35. Configuración de conexiones cruzadas para conexiones VMware

Correlación de LUN con una partición de almacenamiento en VMware ESX Server

Consulte “Correlación de LUN” en la página 97 para conocer los procedimientos sobre cómo correlacionar LUN con una partición. Esta sección contiene notas sobre la correlación de LUN específicas para VMware ESX Servers.

Cuando correlacione LUN en VMware ESX Server, tenga en cuenta lo siguiente:

- Correlacione los LUN utilizando números consecutivos, empezando por LUN 0. Por ejemplo, correlacione los LUN con los números 0; 1; 2; 3; 4; 5; etc., sin saltar ningún número.
- En cada partición, debe correlacionar un LUN 0.
- Si su configuración no requiere la compartición de LUN (servidores ESX independientes únicos o múltiples, clúster virtual local), cada unidad lógica se debe correlacionar directamente con un host o con un grupo de host con un host individual como miembro.
- El compartimiento de LUNs entre varios servidores ESX sólo está soportado cuando está configurando hosts habilitados para VMotion o nodos de clúster Microsoft. En LUNs que se correlacionan con varios servidores ESX, debe cambiar la modalidad de acceso a compartido (Shared).

Puede correlacionar los LUN con un grupo de host para servidores ESX de forma que estén disponibles para todos los miembros del grupo de host. Para obtener información adicional sobre la agrupación en clúster de Windows con ESX Server, consulte la *Guía de instalación de ESX* en el siguiente sitio web:

www.vmware.com/support/pubs/

Verificación de la configuración de almacenamiento para VMware

Complete los siguientes pasos para verificar si su subsistema de almacenamiento está configurado correctamente y si puede ver su subsistema de almacenamiento:

1. Inicie el servidor.
2. Tras la inicialización del BIOS de QLogic, pulse Ctrl+Q para entrar al programa de configuración Fast!UTIL.
3. Seleccione el primer adaptador de bus de host mostrado en la pantalla de Fast!UTIL.
4. Seleccione **Configuración de adaptador de host** y pulse Intro.
5. Seleccione **Explorar dispositivos de fibra** y pulse Intro. El resultado será similar al siguiente:

```
Scan Fibre Channel Loop
ID      Vendor      Product      Rev      Port Name      Port ID
128     No device present 0520
129     IBM      1742      0520      200400A0b00F0A16 610C00
130     No device present
131     No device present
132     No device present
133     No device present
134     No device present
135     No device present
```

Nota: Dependiendo de cómo esté cableada la configuración, es posible que vea varias instancias.

Si no ve un controlador de subsistema de almacenamiento, verifique el cableado, la zona de conmutador y la correlación de LUN.

Apéndice C. Uso de Storage Manager con servicios de clúster de alta disponibilidad

Los servicios de agrupación en clúster de alta disponibilidad proporcionados por Storage Manager permiten a los servicios de aplicaciones continuar cuando se produce un error de hardware o software. Este sistema le protege de errores de software, así como de errores de un componente de una CPU, disco o LAN. Si falla un componente, el componente colaborador redundante se encarga de los servicios en clúster y coordina la transferencia entre componentes.

Información general

Este documento no describe cómo instalar o configurar los servicios de clúster. Consulte la documentación proporcionada con sus productos de servicios de clúster para obtener esta información.

Importante: La información de este documento podría no incluir niveles de versiones de software de clúster actualizadas.

Para conocer los requisitos e información de usuario más reciente sobre el uso de Storage Manager con servicios de clúster, consulte el archivo léame incluido en el DVD de Storage Manager para su sistema operativo host o consulte los últimos archivos léame en línea.

Consulte “Búsqueda de software, firmware de controlador y archivos léame de Storage Manager” en la página xv para conocer instrucciones sobre cómo buscar el archivo léame en línea.

También puede encontrar información en el System Storage Interoperation Center, situado en el siguiente sitio web:

www.ibm.com/systems/support/storage/config/ssic

Uso de servicios de clúster en sistemas AIX

Las secciones siguientes contienen requisitos de hardware generales e información adicional sobre servicios de clúster.

Importante: La información de este documento podría no indicar niveles de versiones de software de clúster actualizadas. Consulte el archivo léame de Storage Manager para AIX para conocer la información más reciente sobre los requisitos de la agrupación en clúster. Consulte “Búsqueda de software, firmware de controlador y archivos léame de Storage Manager” en la página xv para conocer instrucciones sobre cómo buscar el archivo léame en la web.

También puede visitar los siguientes sitios web para consultar la información más reciente sobre AIX y la agrupación en clúster:

www.ibm.com/systems/support/storage/config/ssic

publib.boulder.ibm.com/infocenter/clresctr/index.jsp

Multiproceso de clúster de alta disponibilidad

Esta sección contiene los requisitos generales y notas de uso para el soporte del multiproceso de clúster de alta disponibilidad (HACMP) con Storage Manager.

Requisitos de Software

Para las últimas versiones de HACMP soportadas, consulte el Centro de interoperación de System Storage en el siguiente sitio web:

www.ibm.com/systems/support/storage/config/ssic

Limitaciones de configuración

Las siguientes limitaciones se aplican a configuraciones HACMP:

- HACMP C-SPOC no se puede utilizar para añadir un disco DS3000, DS4000 o DS5000 a AIX utilizando el recurso *Añadir un disco al clúster*.
- HACMP C-SPOC no soporta matrices de modo concurrente mejorado.
- Se permiten configuraciones de HBA único, pero cada una de ellas requiere que ambos controladores del subsistema de almacenamiento estén conectados a un conmutador en la misma zona SAN que el HBA.

Atención: Aunque se aceptan configuraciones de HBA único, no las utilice en entornos HACMP porque introducen un punto único de anomalía a la ruta de E/S del almacenamiento.

- Utilice conexiones de tejido conmutado entre los nodos de host y el subsistema de almacenamiento. La asociación directa de nodos de host y subsistemas de almacenamiento en un entorno HACMP se soporta *solo* si se respetan todas las restricciones y limitaciones siguientes:
 - Para la asociación directa en una configuración de alta disponibilidad solo se soportan las versiones de subsistema de almacenamiento DS3000, DS4000 o DS5000 de controlador dual.
 - La versión del sistema operativo AIX debe ser 05.2 o posterior.
 - La versión del software de clúster HACMP debe ser 05.1 o posterior.
 - Todos los nodos de host directamente asociados con el subsistema de almacenamiento deben formar parte del mismo clúster HACMP.
 - Todas las unidades lógicas (LUN) cubiertas por el subsistema de almacenamiento forman parte de una o más matrices de modo concurrente mejorado.
 - La matriz **varyon** está en estado activo *solo* en el nodo de host que posee el grupo de recursos n o concurrentes HACMP (que contiene la matriz o matrices de modo concurrente mejorado). En el resto de nodos de host del clúster HACMP, la matriz de modo concurrente mejorado **varyon** está en estado pasivo.
 - No se pueden realizar operaciones directas en las unidades lógicas de las matrices de modo concurrente mejorado, desde ninguno de los nodos de host del clúster HACMP si las operaciones eluden la capa Logical VolumeManager (LVM) del sistema operativo AIX. Por ejemplo, no puede utilizar un comando DD si ha iniciado sesión como usuario root.
 - Cada nodo de host del clúster HACMP debe tener conexiones de canal de fibra al subsistema de almacenamiento. Debe realizarse una conexión de canal de fibra directa con el controlado A del subsistema de almacenamiento y la otra con el controlador B de este.

- Puede asociar directamente un máximo de dos nodos de host de un clúster HACMP con una versión de controlador dual de un subsistema de almacenamiento DS4100 o DS4300.
- Puede asociar directamente un máximo de dos nodos de host de un clúster HACMP con un subsistema de almacenamiento. Cada nodo de host debe tener dos conexiones de canal de fibra directas al subsistema de almacenamiento.

Nota: En subsistemas de almacenamiento DS3000, DS4000 o DS5000, las dos conexiones directas de canal de fibra de cada host deben realizarse con minihub independientes. Por tanto, esta configuración requiere la instalación de cuatro minihub principales (código de característica 3507) en el subsistema de almacenamiento DS3000, DS4000 o DS5000 — dos minihubs principales para cada nodo de host del clúster HACMP.

Otras notas de uso de HACMP

Las siguientes notaciones son específicas para entornos HACMP:

- Los clúster HACMP soportan de 2 a 32 servidores en cada partición de un subsistema de almacenamiento DS3000, DS4000 y DS5000. Si ejecuta este tipo de entorno, asegúrese de leer y comprende los valores de profundidad de cola de los controladores de dispositivos AIX descritos en “Definición de la profundidad de cola para dispositivos hdisk” en la página 184.
- Puede adjuntar hosts AIX sin clúster a un subsistema de almacenamiento que ejecute Storage Manager y esté asociado a un clúster HACMP. No obstante, debe configurar los hosts AIX sin clúster en particiones de hosts independientes de un subsistema de almacenamiento.

Parallel System Support Programs y General Parallel File System

Esta sección contiene requisitos generales y notas de uso sobre soporte de Parallel System Support Programs (PSSP) y General Parallel File System (GPFS) con Storage Manager.

Requisitos de Software

Para conocer las últimas versiones de PSSP y GPFS soportadas, consulte el Centro de interoperación de System Storage en el siguiente sitio web:

www.ibm.com/systems/support/storage/config/ssic

Limitaciones de configuración

Las siguientes limitaciones se aplican a las configuraciones de PSSP y GPFS:

- No se permite la conexión directa entre un nodo de host y un subsistema de almacenamiento DS3000, DS4000 o DS5000. Solo se permiten conexiones de tejido conmutado.
- Los clústers RVSD pueden soportar hasta dos servidores IBM Virtual Shared Disk y RVSD para cada partición del subsistema de almacenamiento.
- El quórum de nodo único no se soporta en clústers GPFS de nodo dual con discos DS3000, DS4000 o DS5000 en la configuración.
- No se soportan configuraciones heterogéneas.

Otras notas de uso de PSSP y GPFS

En sistemas de archivos GPFS, se admiten los siguientes valores de memoria caché de subsistemas de almacenamiento DS3000, DS4000 y DS5000:

- Lectura de memoria caché habilitada o inhabilitada
- Escritura de memoria caché habilitada o inhabilitada
- Duplicación de memoria caché habilitada o inhabilitada (dependiendo del valor de duplicación de escritura de memoria caché)

Los beneficios de rendimiento de la lectura o escritura de la memoria caché dependen de la aplicación.

Diagramas de configuración de clúster GPFS, PSSP y HACMP

Los diagramas de esta sección muestran la ruta preferida y la ruta de migración tras error de un par HBA a una unidad lógica determinada o conjunto de unidades lógicas.

La ruta preferida a una unidad lógica se determina cuando se crea la unidad lógica y se distribuye en un controlador de subsistema de almacenamiento. El controlador al que se asigna determina la ruta preferida o activa para la transferencia de E/S. Las unidades lógicas pueden, y en la mayoría de los casos deben, asignarse a ambos controladores, equilibrando la carga de E/S en los HBA y controladores del subsistema de almacenamiento.

Figura 36 muestra una configuración de clúster que contiene un subsistema de almacenamiento DS individual con entre una y cuatro particiones.

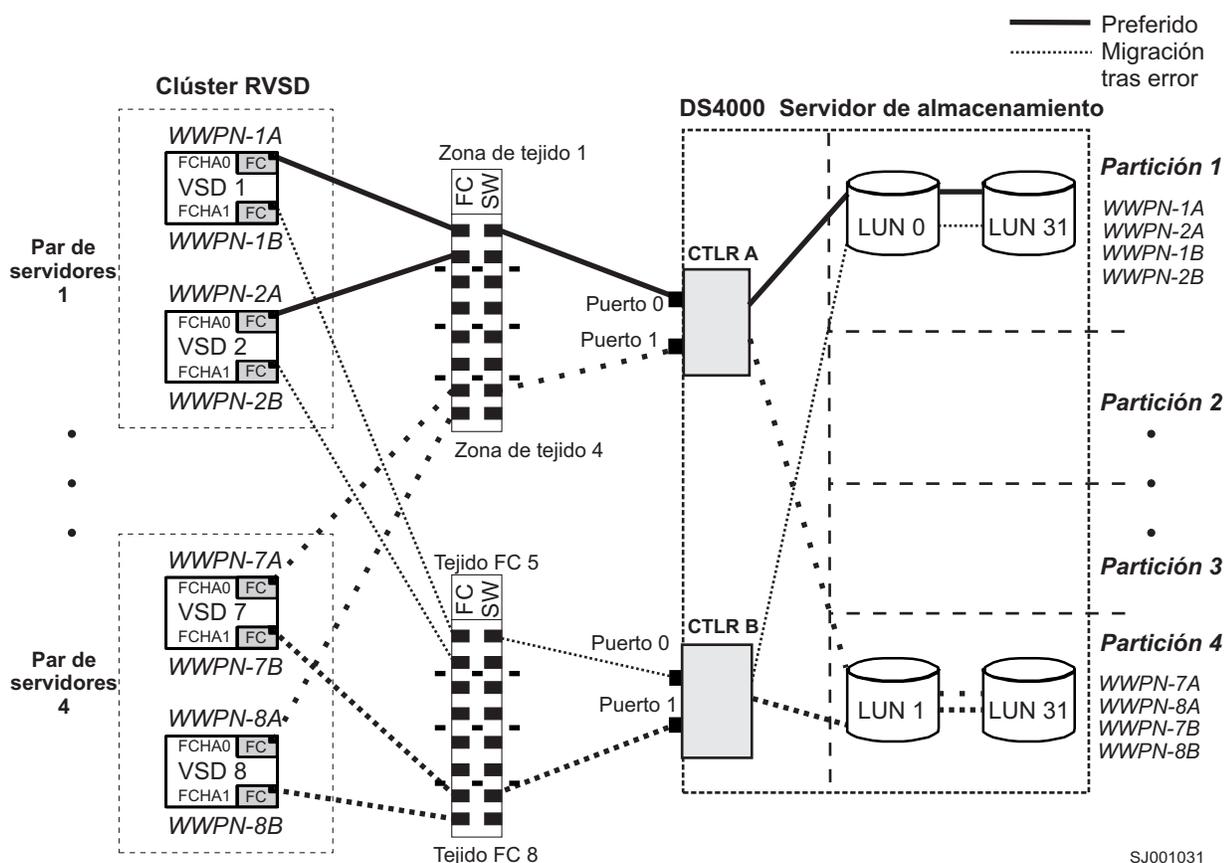


Figura 36. Configuración de clúster con un subsistema de almacenamiento individual - una a cuatro particiones

Figura 37 muestra una configuración de clúster que contiene tres subsistemas de almacenamiento DS con una partición en cada uno de ellos.

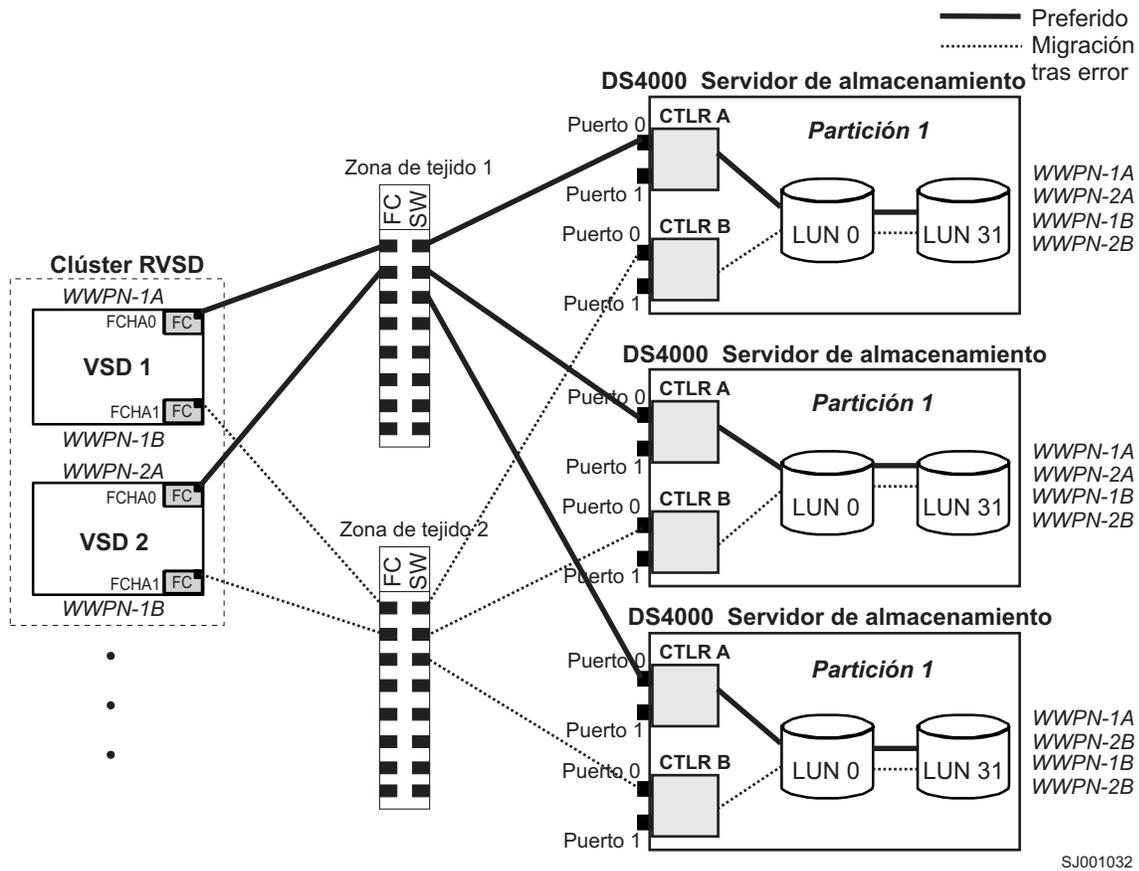


Figura 37. Configuración de clúster con tres subsistemas de almacenamiento - una partición por subsistema

Figura 38 en la página 332 muestra una configuración de clúster que contiene cuatro subsistemas de almacenamiento DS, con una partición en cada subsistema de almacenamiento.

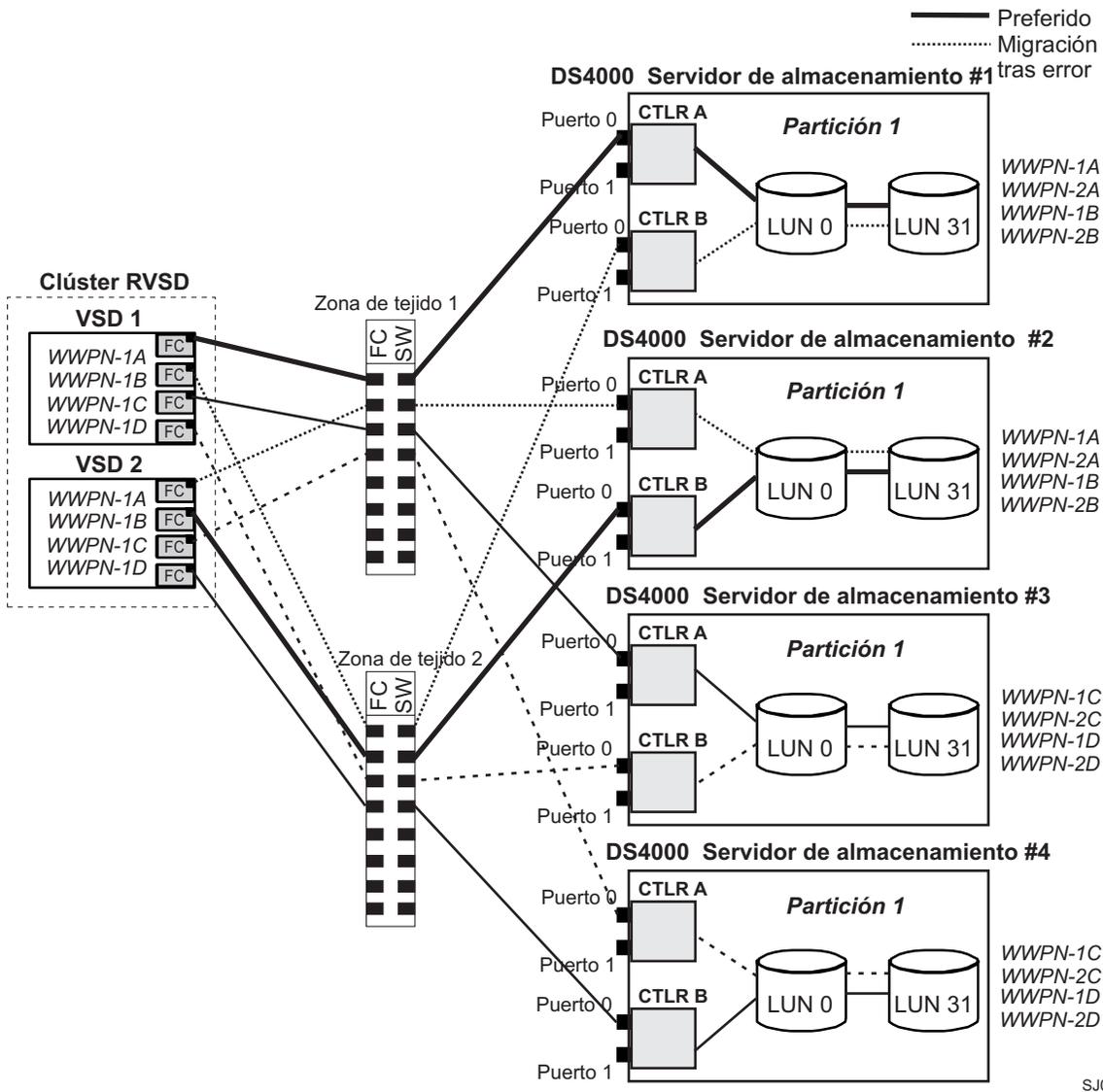
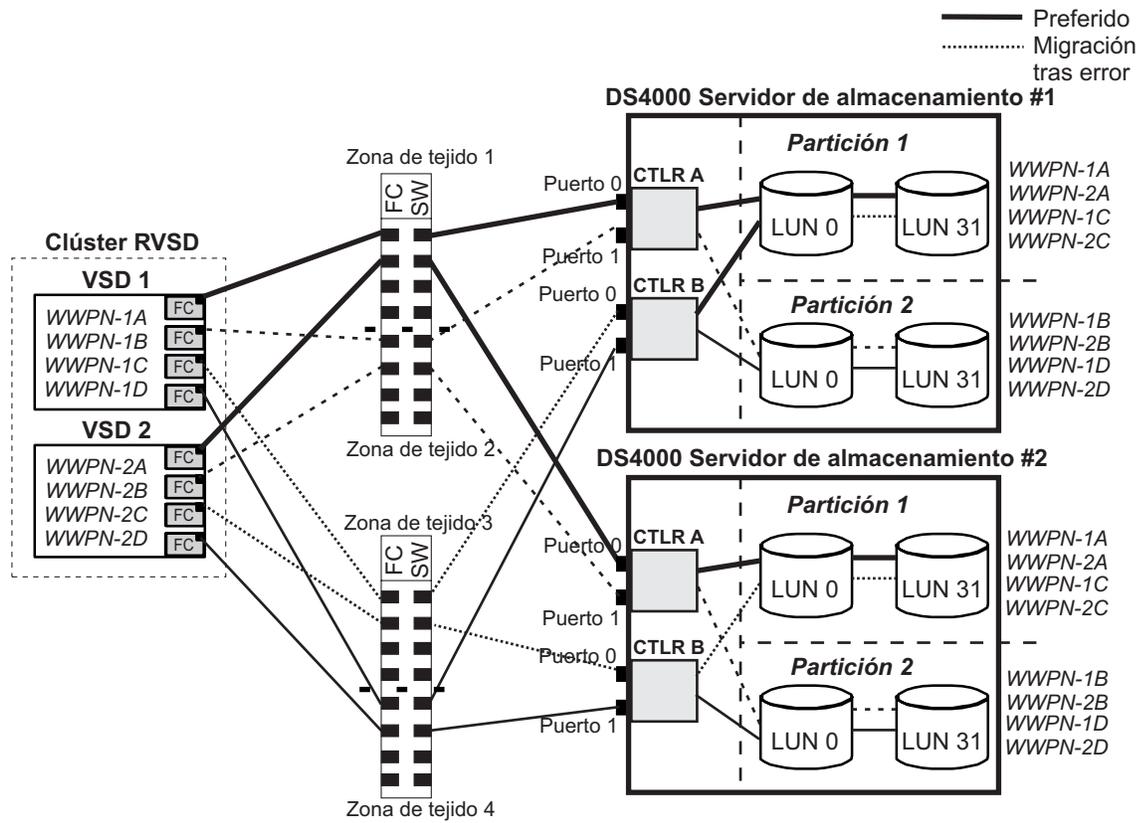


Figura 38. Configuración de clúster con cuatro subsistemas de almacenamiento - una partición por subsistema

Figura 39 en la página 333 muestra una configuración de clúster que contiene dos subsistemas de almacenamiento DS con dos particiones en cada uno de ellos.



SJ001034

Figura 39. Configuración de clúster RVSD con dos subsistemas de almacenamiento - dos particiones por subsistema

Figura 40 en la página 334 muestra una configuración de clúster HACMP/GPFS que contiene un subsistema de almacenamiento DS individual con una partición.

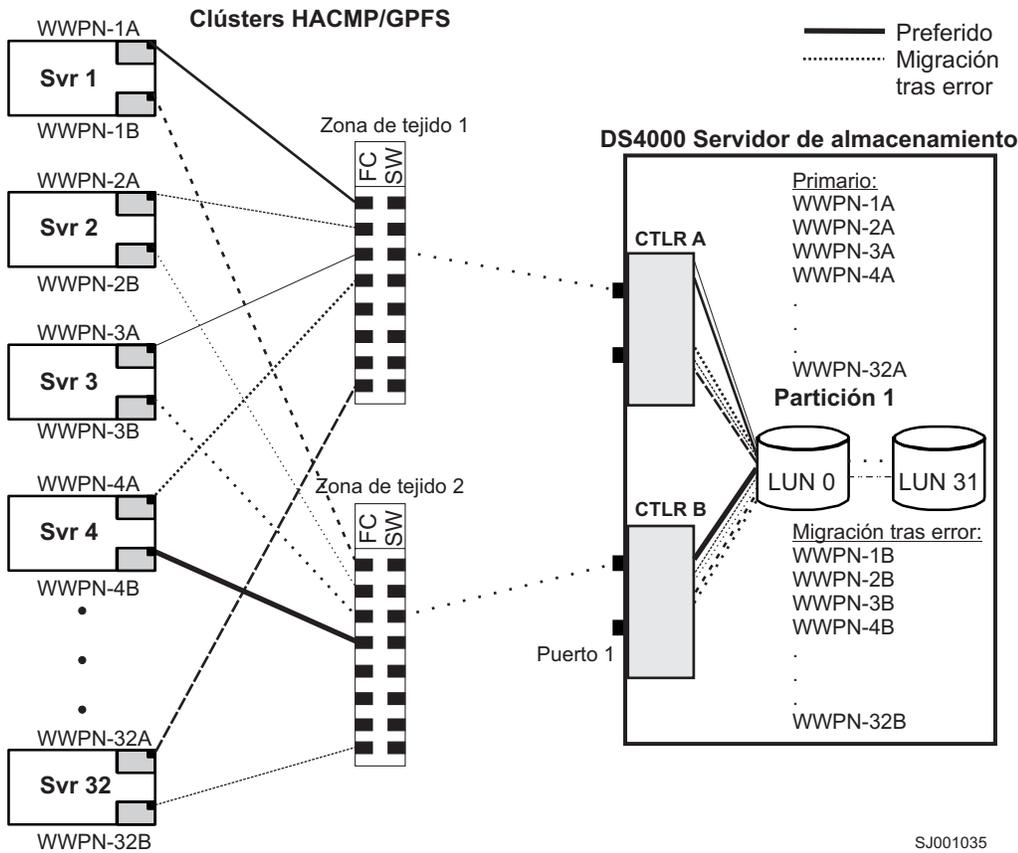


Figura 40. Configuración de clúster HACMP/GPFS con un subsistema de almacenamiento - una partición

Figura 41 en la página 335 muestra una configuración de clúster HACMP/GPFS que contiene dos subsistemas de almacenamiento DS con dos particiones en cada uno de ellos.

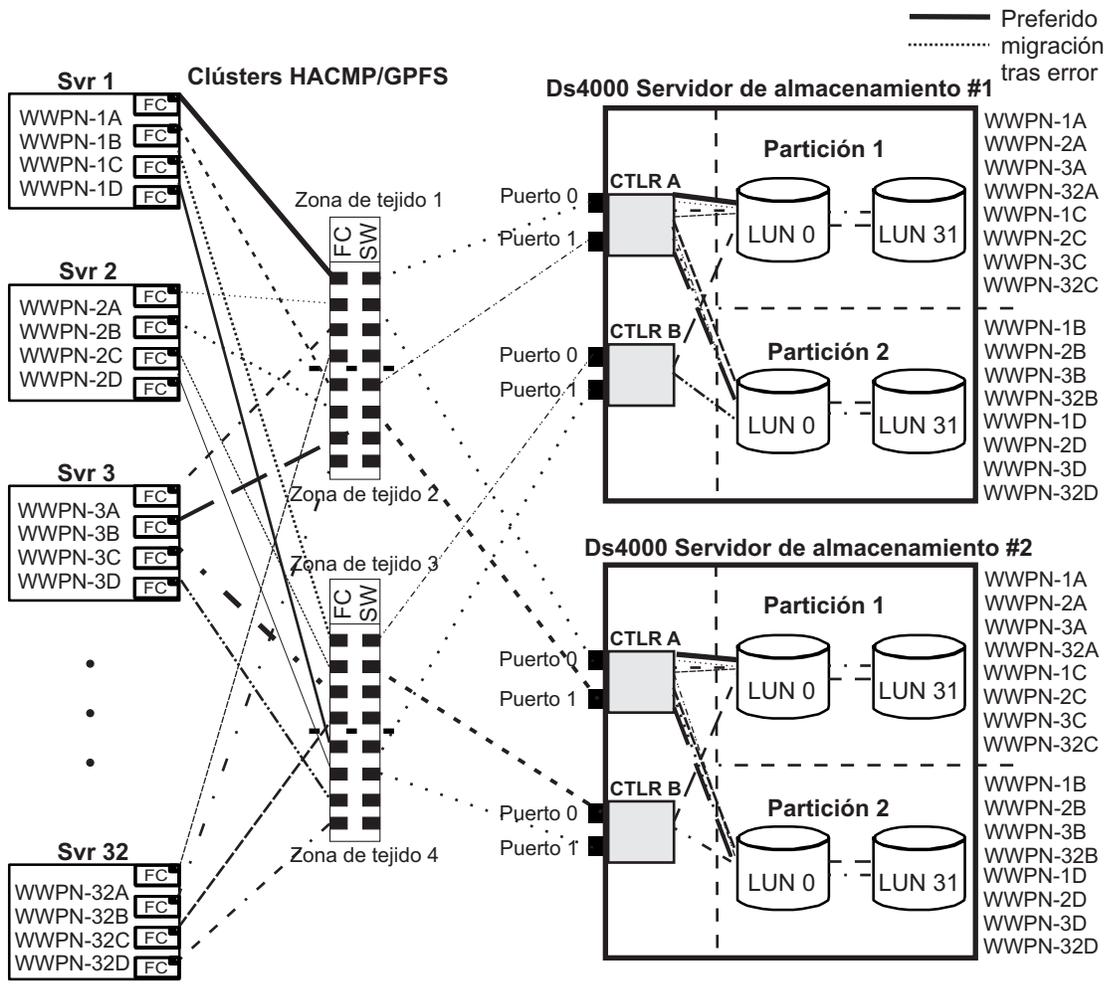


Figura 41. Configuración de clúster HACMP/GPFS con dos subsistemas de almacenamiento - dos particiones por subsistema

Uso de servicios de clúster en sistemas HP-UX

La información de este documento podría no indicar niveles de versiones de software de clúster actualizadas. Consulte el archivo léame de Storage Manager para HP-UX para conocer la información más reciente sobre los requisitos de la agrupación en clúster. Consulte "Búsqueda de software, firmware de controlador y archivos léame de Storage Manager" en la página xv para conocer instrucciones sobre cómo buscar el archivo léame en línea.

También puede visitar el System Storage Interoperation Center en el siguiente sitio web:

www.ibm.com/systems/support/storage/config/ssic

Al configurar la agrupación en clúster en un sistema HP-UX puede elegir muchas configuraciones. La configuración mínima está formada por dos servidores, ambos configurados con una LAN primaria y dos LAN en espera para establecer una LAN de pulsación.

Proporciona al subsistema de almacenamiento conexiones de canal de fibra a través de dos conmutadores que faciliten la ruta necesaria a los datos redundantes a los hosts. Asegúrese de que cada servidor tiene dos adaptadores de bus de host HP Tachyon.

Uso de servicios de clúster en sistemas Solaris

Las secciones siguientes contienen requisitos de hardware generales e información adicional sobre servicios de clúster.

Importante: La información de este documento podría no indicar niveles de versiones de software de clúster actualizadas. Consulte el archivo léame de Storage Manager para Solaris para conocer información actualizada sobre los requisitos de la agrupación en clúster, incluyendo las últimas versiones soportadas de Veritas Cluster Server. Consulte “Búsqueda de software, firmware de controlador y archivos léame de Storage Manager” en la página xv para conocer instrucciones sobre cómo buscar el archivo léame en línea.

También puede visitar el System Storage Interoperation Center en el siguiente sitio web:

www.ibm.com/systems/support/storage/config/ssic

Requisitos generales de Solaris

Cada sistema Solaris del clúster requiere el siguiente hardware:

- Al menos tres puertos Ethernet:
 - Dos para las conexiones de red privadas
 - Al menos uno para la conexión de red pública
- Dos adaptadores de bus de host de canal de fibra para conexión con el subsistema de almacenamiento
- Una conexión SCSI para los discos del sistema operativo
- Cada sistema Veritas Cluster Server requiere al menos 128 MB de RAM y 35 MB de espacio de disco libre

Dependencias del sistema

Esta sección proporciona información acerca de los identificadores RDAC y los puntos únicos de anomalía.

Adición de IDs de RDAC

Puede añadir hasta ocho identificadores adicionales al archivo `/etc/symsm/rmparams`. Para añadirlos, siga estos pasos:

1. Abra el archivo `/etc/symsm/rmparams` en el vi Editor escribiendo el siguiente comando:

```
# vi /etc/symsm/rmparams
```
2. Modifique la línea `Rdac_HotAddIDs` como se indica a continuación:

```
Rdac_HotAddIDs:0:1:2:3:4:5:6:7:8
```
3. Guarde y cierre el archivo `/etc/symsm/rmparams`.

Puntos únicos de anomalía

Al configurar servicios de clúster, es importante eliminar los puntos únicos de anomalía porque estos hacen que los clústers tengan solo la resistencia de su componente más débil. Configure el subsistema de almacenamiento para el

almacenamiento compartido; por ejemplo, todos los nodos del clúster deben reconocer el mismo almacenamiento y los tipos de host se deben definir correctamente.

Apéndice D. Visualización y definición de atributos de gestor de datos de objeto (ODM) de AIX

Algunos de los atributos de ODM solo tiene fines informativos. Estos atributos informativos muestran cómo se configura el subsistema de almacenamiento y su estado actual. Puede modificar otros atributos utilizando SMIT o con el comando UNIX `chdev -p`.

Definiciones de atributo

Las siguientes tablas muestran las definiciones y valores de los atributos ODM para `dars`, `dacs` y `hdisks`:

- Tabla 51: *Atributos para dispositivos dar*
- Tabla 52 en la página 341: *Atributos para dispositivos dac*
- Tabla 53 en la página 342: *Atributos para dispositivos hdisk*

Nota:

1. El valor predeterminado de los atributos con True (Verdadero) en la columna Modificable puede modificarse.
2. Los atributos con False (Falso) en la columna Modificable solo tienen fines informativos o de estado. No obstante, algunos atributos con False en la columna Modificable se pueden modificar con Storage Manager.
3. El comando `lsattr -El` (E mayúscula, L minúscula) es otra forma de determinar qué atributos se pueden modificar. Los atributos que pueden modificarse indican True en la última columna del resultado de `lsattr -El`. También puede mostrar los valores predeterminados con el comando `lsattr -Dl`.

Tabla 51. *Atributos para dispositivos dar*

atributo	Definición	Modificable(T/F)	Valor posible
<i>act_controller</i>	Lista de controladores en estado activo durante la configuración.	False	Definida durante la configuración por el software RDAC.
<i>all_controller</i>	Lista de controladores que incluyen esta matriz; normalmente hay dos dispositivos <code>dac</code> .	False	Definida durante la configuración por el software RDAC.
<i>held_in_reset</i>	Nombre del controlador que estaba en estado <code>held_in_reset</code> durante la configuración o ninguno si no había ningún controlador en ese estado.	True	Definida durante la configuración por el software RDAC.No debe modificarse.

Tabla 51. Atributos para dispositivos dar (continuación)

atributo	Definición	Modificable(T/F)	Valor posible
<i>load_balancing</i>	Indicador que especifica si el equilibrio de carga está habilitado (sí) o inhabilitado (no); vea la definición del atributo <i>balance_freq</i> para más información.	True	Sí o No. Atención: Sólo se debe definir el atributo <i>load_balancing</i> como sí en configuraciones de un solo host.
<i>autorecovery</i>	Indicador que especifica si el dispositivo devuelve la matriz a la modalidad dual-activa si detecta una operación adecuada de rutas y controladores (sí) o no (no).	True	Sí o No. Ver restricciones de uso.
<i>hlthchk_freq</i>	Número que especifica con qué frecuencia se realizan comprobaciones de estado en segundos.	True	1 - 9999. No debe modificarse.
<i>aen_freq</i>	Número que especifica con qué frecuencia se realizan comprobaciones de AEN de sondeo en segundos.	True	1 - 9999. No debe modificarse.
<i>balance_freq</i>	Si <i>load_balancing</i> está habilitado, número que especifica con qué frecuencia, en segundos, se realiza el equilibrio de carga en la matriz.	True	1 - 9999 - No debe modificarse.
<i>fast_write_ok</i>	Indicador que muestra si la escritura-rápida o la caché-rápida estaban disponibles para este sistema (sí) o no (no).	False	Sí o No. Estado de la configuración del subsistema de almacenamiento.
<i>cache_size</i>	Tamaño de la caché de ambos controladores, en megabytes; 0 si los tamaños no coinciden.	False	512 o 1024. Definido por el subsistema de almacenamiento.

Tabla 51. Atributos para dispositivos dar (continuación)

atributo	Definición	Modificable(T/F)	Valor posible
<i>switch_retries</i>	Número que especifica cuántas veces se reintentan los conmutadores fallidos, en enteros.	True	0 - 255. Predeterminado: 5 Para la mayoría de configuraciones, el valor predeterminado es el mejor valor. Si está utilizando HACMP, puede ser útil para establecer el valor a 0. Atención: No se puede utilizar una descarga de firmware simultánea si se cambia el valor predeterminado.

Tabla 52. Atributos para dispositivos dac

atributo	Definición	Modificable(T/F)	Valor posible
<i>passive_control</i>	Indicador que especifica si este controlador estaba en estado pasivo durante la configuración (sí) o no (no).	False	Sí o No. Estado de la configuración del subsistema de almacenamiento.
<i>alt_held_reset</i>	Indicador que muestra si el controlador alternativo estaba en estado held-in-reset durante la configuración (sí) o no (no).	False	Sí o No. Estado de la configuración del subsistema de almacenamiento.
<i>controller_SN</i>	Número de serie de este controlador.	False	Definido por el subsistema de almacenamiento.
<i>ctrl_type</i>	Tipo de matriz a la que pertenece este controlador.	False	1742, 1722, 1742-900. Definido por el subsistema de almacenamiento.
<i>cache_size</i>	Tamaño de la memoria caché de este controlador, en megabytes.	False	512, 1024. Definido por el subsistema de almacenamiento.
<i>scsi_id</i>	Identificador SCSI de este controlador.	False	Definido por SAN, informe por AIX.
<i>lun_id</i>	Número de unidad lógica de este controlador.	False	Definido por el subsistema de almacenamiento.

Tabla 52. Atributos para dispositivos dac (continuación)

atributo	Definición	Modificable(T/F)	Valor posible
<i>utm_lun_id</i>	Número de unidad lógica de este controlador, o ninguno si las UTM (unidades lógicas de acceso) no está habilitadas.	False	0 - 31. Definido por Storage Manager.
<i>node_name</i>	Nombre del nodo de canal de fibra.	False	Definido por el subsistema de almacenamiento.
<i>location</i>	Etiqueta de ubicación definida por el usuario para este controlador; el sistema no utiliza este valor.	True	Definida por Storage Manager.
<i>ww_name</i>	Nombre de ámbito mundial de canal de fibra de este controlador.	False	Definido por el subsistema de almacenamiento.
<i>GLM_type</i>	Tipo de GLM utilizado para este controlador.	False	Alto o Bajo. Definido por el subsistema de almacenamiento.

Tabla 53. Atributos para dispositivos hdisk

atributo	Definición	Modificable(T/F)	Valor posible
<i>pvid</i>	Identificador de volumen AIX físico o ninguno si no está definido.	False	Definido por AIX.
<i>q_type</i>	Tipo de colas para este dispositivo, se debe establecer en simple .	False	Definido por AIX.Debe ser "simple".
<i>queue_depth</i>	Número que especifica la profundidad de la cola en base a la configuración del sistema; reduzca este número si la matriz devuelve un estado BUSY de manera continuada.	True	1 - 64 Nota: Consulte "Definición de la profundidad de cola para dispositivos hdisk" en la página 184 para conocer información importante sobre la definición de este atributo.
<i>PR_key_value</i>	Sólo es necesario si el dispositivo soporta alguna de las políticas de reserva permanentes. Este atributo se utiliza para distinguir ente distintos hosts.	True	1-64 o Ninguno. Nota: Se ha de establecer un valor que no sea cero para este atributo antes de definir el atributo <i>reserve_policy</i> .

Tabla 53. Atributos para dispositivos hdisk (continuación)

atributo	Definición	Modificable(T/F)	Valor posible
<i>reserve_policy</i>	Política de reserva permanente, que indica si se emplea una metodología de reserva cuando se abre el dispositivo.	True	no_reserve PR_shared, PR_exclusive o single_path
<i>max_transfer</i>	El tamaño máximo de transferencia es el tamaño de transferencia más grande que se puede utilizar en el envío de E/S.	True	Valor numérico: Predeterminado = 1 MB Nota: Normalmente, no es necesario cambiar el valor predeterminado, a menos que operaciones de E/S muy grandes requieran aumentar este valor.
<i>write_cache</i>	Indicador que especifica si está habilitada la escritura en memoria caché en este dispositivo (sí) o no (no); vea la definición del atributo <i>cache_method</i> para más información.	False	Sí o No.
<i>size</i>	Tamaño de esta unidad lógica.	False	Definido por el subsistema de almacenamiento.
<i>raid_level</i>	Número que especifica el nivel de RAID de este dispositivo.	False	0, 1, 3, 5. Definido por Storage Manager.
<i>rw_timeout</i>	Número que especifica el valor de tiempo de espera lectura/escritura de cada mandato de lectura/escritura para esta matriz, en segundos; normalmente se establece en 30.	True	30 - 180. El valor predeterminado no debe modificarse.
<i>reassign_to</i>	Número que especifica el valor de tiempo de espera para operaciones de reasignación de FC, en segundos; normalmente se establece en 120.	True	0 - 1000. El valor predeterminado no debe modificarse.

Tabla 53. Atributos para dispositivos *hdisk* (continuación)

atributo	Definición	Modificable(T/F)	Valor posible
<i>scsi_id</i>	Identificador SCSI durante la configuración.	False	Definido por SAN, informe por AIX.
<i>lun_id</i>	Número de unidad lógica de este dispositivo.	False	0 - 255. Definido por Storage Manager.
<i>cache_method</i>	<p>Si <i>write_cache</i> está habilitado, el método de escritura en memoria caché de esta matriz; establecido con uno de los siguientes valores:</p> <ul style="list-style-type: none"> • default. Modalidad predeterminada; "default" no se visualiza si <i>write_cache</i> se ha establecido en Sí. • fast_write. Modalidad de escritura rápida (con batería de reserva, memoria caché de escritura duplicada). • fw_unavail. Se ha especificado la modalidad de escritura rápida pero no se ha podido habilitar: la escritura en memoria caché no se está utilizando. • fast_load. Modalidad de carga rápida (sin batería de reserva, sin memoria caché de escritura duplicada). • fl_unavail. Se ha especificado la modalidad de carga rápida pero no se ha podido habilitar. 	False	Default, <i>fast_write</i> , <i>fast_load</i> , <i>fw_unavail</i> , <i>fl_unavail</i> .
<i>prefetch_mult</i>	Número de bloques que se han de captar previamente en la memoria caché de lectura para cada lectura de bloque.	False	0 - 100.

Tabla 53. Atributos para dispositivos hdisk (continuación)

atributo	Definición	Modificable(T/F)	Valor posible
<i>ieee_volname</i>	Identificador IEEE exclusivo de nombre de unidad lógica para esta unidad lógica.	False	Definido por el subsistema de almacenamiento.

Uso del comando lsattr para ver atributos de ODM

Para ver la configuración de atributos de Object Data Manager (ODM) para dars, dacs y hdisks, utilice el comando **lsattr** del modo siguiente:

- Para ver la configuración predeterminada, escriba **lsattr -DI**.
- Para ver los atributos definidos actualmente en el sistema, escriba **lsattr -EI**.

Los ejemplos del resultado de **lsattr -EI** mostrados en la Tabla 54, Tabla 55 y Tabla 56 en la página 346, especifican la configuración de atributos de ODM para un dar, un dac y un hdisk.

Tabla 54. Ejemplo 1: Visualización de la configuración de atributos para un dar

```
# lsattr -EI dar0
act_controller dac0,dac1 Active Controllers           False
aen_freq      600      Polled AEN frequency in seconds           True
all_controller dac0,dac1 Available Controllers           False
autorecovery  no        Autorecover after failure is corrected      True
balance_freq  600      Dynamic Load Balancing frequency in seconds True
cache_size    128      Cache size for both controllers            False
fast_write_ok yes      Fast Write available                         False
held_in_reset none     Held-in-reset controller                   True
hlthchk_freq  600      Health check frequency in seconds          True
load_balancing no       Dynamic Load Balancing                     True
switch_retries 5       Number of times to retry failed switches   True
```

Tabla 55. Ejemplo 2: Visualización de la configuración de atributos para un dac

```
# lsattr -EI dac0
GLM_type      low      GLM type                               False
alt_held_reset no       Alternate held in reset                 False
cache_size    128      Cache Size in MBytes                    False
controller_SN 1T24594458 Controller serial number                False
ctrl_type     1722-600 Controller Type                          False
location      Location Label                           True
lun_id        0x0      Logical Unit Number                     False
node_name     0x200200a0b80f14af FC Node Name                             False
passive_control no       Passive controller                       False
scsi_id       0x11000  SCSI ID                                  False
utm_lun_id    0x001f000000000000 Logical Unit Number                       False
ww_name       0x200200a0b80f14b0 World Wide Name                          False
```

Nota: Al ejecutar el comando `# lsattr -RI <device> -a <attribute>`, se mostrarán los valores permitidos para el atributo especificado, una lista de atributos de hdisk al utilizar MPIO.

Nota: En Tabla 56 en la página 346, los valores de atributo **ieee_volname** y **lun_id** aparecen abreviados. Un resultado real mostraría los valor en su totalidad.

Tabla 56. **Ejemplo 3:** Visualización de la configuración de atributos para un hdisk

lsattr -El hdisk174			
cache_method	fast_write	Write Caching method	False
ieee_volname	600A0B8...1063F7076A7	IEEE Unique volume name	False
lun_id	0x0069...000000	Logical Unit Number	False
prefetch_mult	12	Multiple of blocks to prefetch on read	False
pvid	none	Physical volume identifier	False
q_type	simple	Queuing Type	False
queue_depth	2	Queue Depth	True
raid_level	5	RAID Level	False
reassign_to	120	Reassign Timeout value	True
reserve_lock	yes	RESERVE device on open	True
rw_timeout	30	Read/Write Timeout value	True
scsi_id	0x11f00	SCSI ID	False
size	2048	Size in Mbytes	False
write_cache	yes	Write Caching enabled	False

Apéndice E. Acerca del proveedor VDS/VSS

Microsoft Virtual Disk Service (VDS) y Microsoft Volume Shadow-copy Service (VSS) son interfaces IBM DS Storage Manager para Microsoft Windows Server 2003 y Microsoft Windows Server 2008. VDS y VSS permiten al subsistema de almacenamiento interactuar con aplicaciones de terceros que utilicen la interfaz de programación de aplicaciones (API) de VDS o VSS. Microsoft VDS/VSS se incluye en las instalaciones Windows Server 2003 y Windows Server 2008. Microsoft VSS se incluye y tiene soporte en Windows Server 2012, pero Microsoft VDS está obsoleto a partir de Windows Server 2012.

Nota: El proveedor de hardware IBM VDS/VSS no tiene soporte para versiones de cliente de Windows Server 2012.

El proveedor de hardware IBM VDS/VSS no tiene soporte para versiones de cliente de Windows Server 2012. El proveedor de hardware IBM DS Storage Manager VDS es una biblioteca Dynamic Link Library (DLL) de Windows que carga VDS, y se utiliza como canal de comunicación para el subsistema de almacenamiento. Con el proveedor de hardware IBM DS Storage Manager VDS instalado, las aplicaciones de terceros pueden enviar mandatos de gestión al subsistema de almacenamiento. Tiene soporte para comandos como - creación de unidades lógicas, supresión de unidades lógicas y desenmascaramiento de unidades lógicas. Las aplicaciones de terceros puede obtener información de configuración y estado del subsistema de almacenamiento. El proveedor de hardware de IBM DS Storage Manager VSS es un servicio de Windows (.exe). VSS de Microsoft se conecta al servicio y lo utiliza para coordinar la creación de las unidades lógicas FlashCopy en el subsistema de almacenamiento. Las FlashCopies de unidad lógica iniciadas por VSS se pueden desencadenar por medio de herramientas de copia de seguridad de terceros conocidas como 'solicitantes'.

Descargue el proveedor VDS/VSS y las instrucciones de instalación del sitio web siguiente. En primer lugar, registre una cuenta y obtenga las credenciales de inicio de sesión; a continuación, descargue el programa de instalación.

[http://support.netapp.com/NOW/apbu/oemcp/protcd/.](http://support.netapp.com/NOW/apbu/oemcp/protcd/)

Apéndice F. Instalación del proveedor SMI-S

La SMIS-S (Especificación de iniciativa de gestión de almacenamiento) define un método para la gestión interoperativa de una red de área de almacenamiento (SAN) y describe la información disponible para un cliente WBEM desde un servidor CIM compatible con SMI-S y una interfaz basada en XML, en mensajería y orientada a objetos. Esta interfaz está diseñada para dar soporte a requisitos específicos de gestión de dispositivos en y a través de redes SAN, IBM SAN Volume Controller, Tivoli Storage Productivity Center, y subsistemas de almacenamiento DS3000, DS4000 y DS5000 con soporte por parte de Director. Para obtener detalles, consulte la matriz de interoperatividad de software de IBM.

Descargue el proveedor SMI-S y las instrucciones de instalación del sitio web siguiente. En primer lugar, registre una cuenta y obtenga las credenciales de inicio de sesión; a continuación, descargue el programa de instalación.

<http://support.netapp.com/NOW/apbu/oemcp/protcd/>.

Apéndice G. Accesibilidad

La información de este apéndice describe las características de accesibilidad y accesibilidad a la documentación de Storage Manager.

Formato de documento

Las publicaciones de este producto están en Adobe Portable Document Format (PDF) y deben cumplir los estándares de accesibilidad. Si experimenta dificultades al utilizar los archivos PDF y quiere solicitar un formato basado en la web o un documento PDF accesible para una documentación, dirija el correo electrónico a la siguiente dirección:

*Information Development
IBM Corporation
205/A015
3039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
EE.UU.*

En la solicitud, asegúrese de incluir el número y el título de la publicación.

Cuando envía información a IBM, otorga a IBM un derecho no exclusivo a utilizar o distribuir dicha información en la forma en que IBM considere adecuada, sin contraer por ello ninguna obligación con el remitente.

Características de accesibilidad de Storage Manager

Esta sección proporciona información sobre navegación de teclado alternativa, una característica de accesibilidad de Storage Manager. Las funciones de accesibilidad ayudan a los usuarios que tienen alguna discapacidad física, como una limitación de los movimientos o de la visión, a utilizar satisfactoriamente los productos de software.

Con las operaciones de teclado alternativas descritas en esta sección, puede utilizar teclas o combinaciones de teclas para llevar a cabo tareas de Storage Manager e iniciar numerosas acciones de menú que también pueden realizarse con el ratón.

Nota: Además de las operaciones de teclado descritas en esta sección, los paquetes de instalación de Storage Manager versión 9.14 - 10.10 (y posteriores) para Windows incluyen una interfaz de software de lectura de pantalla.

Para habilitar el lector de pantalla, seleccione **Instalación personalizada** al utilizar el asistente de instalación para instalar Storage Manager 9.14 - 10.10 (o posterior) en una estación de gestión/host Windows. A continuación, en la ventana Seleccionar características de producto, seleccione **Java Access Bridge**, además del resto de componentes del software host necesarios.

En la Tabla 57 en la página 352 se definen las operaciones de teclado que le permitirán desplazarse por los componentes de la interfaz de usuario, seleccionarlos y activarlos. En la tabla se utilizan los términos siguientes:

- *Navegar* significa mover el foco de entrada de un componente de la interfaz de usuario a otro, dirigirse al componente deseado.

- *Seleccionar* significa elegir uno o más componentes, por lo general, para realizar una acción posterior.
- *Activar* significa llevar a cabo la acción de un componente en particular.

Nota: En general, el desplazamiento de un componente a otro se realiza con las teclas siguientes:

- **Tabulador:** mueve el foco al siguiente componente o al primer miembro del siguiente grupo de componentes.
- **Despl-tabulador:** mueve el foco al componente anterior o al primer componente del grupo de componentes anterior.
- **Teclas de flecha:** mueve el foco de un componente a otro dentro de un grupo de componentes.

Tabla 57. Operaciones de teclado alternativas de Storage Manager

Tecla de atajo	Acción
F1	Abre la ayuda.
F10	Desplaza el foco del teclado a la barra de menús principal y resalta el primer menú; para desplazarse por las opciones disponibles se utilizan las teclas de flecha.
Alt+F4	Cierra la ventana de gestión.
Alt+F6	Mueve el foco de un diálogo (no modal) a otro y de una ventana de gestión a otra.
Alt + letra subrayada	<p>Acceda a los elementos de menú, botones y otros componentes de interfaz con las teclas asociadas con las letras subrayadas.</p> <p>En el caso de las opciones de menú, seleccione la combinación Alt + letra subrayada para acceder a un menú principal y, a continuación, seleccione la letra subrayada para acceder a un elemento concreto del menú.</p> <p>Para los demás componentes, utilice la combinación Alt + letra subrayada.</p>
Ctrl+F1	Muestra u oculta la ayuda flotante cuando el foco del teclado se encuentra en la barra de herramientas.
Barra espaciadora	Selecciona un elemento o activa un hipervínculo.
Control+barra espaciadora (Contiguo/no contiguo) Vista física/lógica AMW)	<p>Selecciona varias unidades en la vista física.</p> <p>Para seleccionar varias unidades, seleccione una unidad con la barra espaciadora y después pulse el tabulador para trasladar el foco a la siguiente unidad que desea seleccionar; pulse Control+barra espaciadora para seleccionar la unidad.</p> <p>Si pulsa la barra espaciadora solamente cuando hay varias unidades seleccionadas, se eliminan todas las selecciones.</p> <p>Utilice la combinación Control+barra espaciadora para deselegionar una unidad cuando haya varias seleccionadas.</p> <p>Este comportamiento es el mismo tanto si se seleccionan unidades adyacentes como si no son adyacentes.</p>

Tabla 57. Operaciones de teclado alternativas de Storage Manager (continuación)

Tecla de atajo	Acción
Fin, Av Pág	Desplaza el foco del teclado al último elemento de la lista.
Esc	Cierra el diálogo actual.No requiere el foco del teclado.
Inicio, Re Pág	Desplaza el foco del teclado al primer elemento de la lista.
Despl+tabulador	Desplaza el foco del teclado de un componente a otro en la dirección contraria en la que se produce el desplazamiento si se pulsa la tecla Tabulador.
Control+Tabulador	Desplaza el foco del teclado de una tabla al siguiente componente de la interfaz de usuario.
Tabulador	Desplaza el foco del teclado de un componente a otro o selecciona un hiperenlace.
Flecha hacia abajo	Mueve el foco al elemento siguiente de la lista.
Flecha hacia la izquierda	Desplaza el foco del teclado a la izquierda.
Flecha hacia la derecha	Desplaza el foco del teclado a la derecha.
Flecha hacia arriba	Desplaza el foco del teclado al elemento anterior de la lista.

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en Estados Unidos.

Es posible que en otros países IBM no ofrezca los productos, los servicios o las características que se describen en este documento. Consulte con el representante local de IBM para obtener información sobre los productos y servicios actualmente disponibles en su zona. Cualquier referencia a un producto, programa o servicio de IBM no implica que solo se pueda utilizar dicho producto, programa o servicio de IBM. Puede utilizarse en su lugar cualquier producto, programa o servicio funcionalmente equivalente que no infrinja ningún derecho de la propiedad intelectual de IBM. Sin embargo, la evaluación y la verificación del funcionamiento de cualquier producto, programa o servicio no IBM son responsabilidad del usuario.

IBM puede tener patentes o solicitudes de patentes pendientes que cubran el tema principal descrito en este documento. La posesión de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar consultas sobre licencias, por escrito, a la siguiente dirección:

*IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
EE.UU.*

Para consultas sobre licencias relativas a información de juego de caracteres de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM de su país, o envíe las consultas, por escrito, a:

*Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japón, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japón*

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país donde estas disposiciones sean incompatibles con la legislación vigente:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUYENDO PERO NO LIMITÁNDOSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN, COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO. Algunos países no permiten la renuncia a garantías explícitas o implícitas en determinadas transacciones, por lo que puede que esta declaración no sea aplicable en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí contenida; dichos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede realizar mejoras o cambios en los productos o programas descritos en esta publicación en cualquier momento y sin previo aviso.

Las referencias en este documento a sitios web que no sean de IBM se proporcionan únicamente como ayuda y no se consideran en modo alguno como una recomendación por parte de IBM de dichos sitios web. Los materiales de dichos sitios web no forman parte de este producto de IBM y la utilización de los mismos será por cuenta y riesgo del usuario.

IBM puede utilizar o distribuir la información que proporcione el usuario de cualquier manera que considere adecuada sin incurrir por ello en ninguna obligación con el usuario.

Los licenciatarios de este programa que deseen obtener información acerca del mismo con el fin de: (i) intercambiar la información entre programas creados independientemente y otros programas (incluido este) y (ii) utilizar mutuamente la información que se ha intercambiado, deben ponerse en contacto con:

*IBM Corporation
Almaden Research
650 Harry Road
Bldg 80, D3-304, Department 277
San José, CA 95120-6099
EE.UU.*

Puede que esta información esté disponible, sujeta a los términos y condiciones adecuados, y puede incluir en algunos casos, el pago de una tasa.

IBM proporciona el programa bajo licencia que se describe en este documento y todo el material bajo licencia disponible para el mismo bajo los términos del Acuerdo de cliente de IBM, el Acuerdo internacional de licencias de programas de IBM o cualquier acuerdo equivalente entre las partes.

Los datos de rendimiento contenidos en este documento se obtuvieron en un entorno controlado. Por lo tanto, los resultados que se obtengan en otros entornos operativos pueden variar significativamente. Pueden haberse realizado algunas mediciones en sistemas a nivel de desarrollo y no existe ninguna garantía de que estas mediciones vayan a ser equivalentes en sistemas disponibles generalmente. Además, es posible que algunas mediciones se hayan calculado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a su entorno específico.

La información relacionada con los productos que no son de IBM se ha obtenido de los proveedores de tales productos, de los anuncios que han publicado o de otras fuentes de disponibilidad pública. IBM no ha comprobado estos productos y no puede confirmar la precisión de su rendimiento, compatibilidad ni contemplar ninguna otra reclamación relacionada con los productos que no son de IBM. Las preguntas relativas a las prestaciones de productos que no son de IBM deben dirigirse a los proveedores de dichos productos.

Todas las declaraciones de intenciones de IBM están sujetas a cambio o cancelación sin previo aviso, y sólo representan objetivos.

Todos los precios de IBM que se muestran son precios actuales de venta al por menor sugeridos por IBM y están sujetos a modificaciones sin previo aviso. Los precios de los proveedores pueden variar.

Esta información está pensada únicamente a efectos de planificación. La información aquí contenida está sujeta a cambios antes de que los productos descritos estén disponibles.

Esta información contiene ejemplos de datos e informes utilizados en operaciones empresariales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos incluyen los nombres de personas, compañías, marcas y productos. Todos ellos son ficticios y cualquier parecido con los nombres y direcciones utilizados por una empresa real son mera coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicaciones de ejemplo en código fuente, que ilustran técnicas de programación en las distintas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo como desee, sin pago alguno a IBM, con la intención de desarrollar, utilizar, comercializar o distribuir programas de aplicación de acuerdo con la interfaz de programación de aplicaciones correspondiente a la plataforma operativa para la que están escritos los programas de ejemplo. Estos ejemplos no se han probado exhaustivamente bajo todas las condiciones. Por consiguiente, IBM, no puede garantizar ni presuponer la fiabilidad, capacidad de servicio o funcionamiento de dichos programas. Los programas de ejemplo se proporcionan "TAL CUAL", sin ningún tipo de garantía. IBM no se responsabilizará de los daños que puedan producirse por el uso de los programas de ejemplo.

Cada copia o parte de estos programas de ejemplo o cualquier trabajo derivado debe incluir un aviso de copyright como el siguiente:

© (nombre de la empresa) (año). Partes de este código proceden de programas de ejemplo de IBM Corp.

© Copyright IBM Corp. _especifique el año o los años_.

Si ve esta información en copia software, es posible que no aparezcan las fotografías y las ilustraciones en color.

Marcas registradas

IBM, el logotipo de IBM e [ibm.com](http://www.ibm.com) son marcas registradas de International Business Machines Corporation en Estados Unidos y/o en otros países. Si estos y otros términos con marca registrada de IBM contienen en su primera aparición en esta información un símbolo de marca registrada (® o ™), estos símbolos indican marcas registradas o de ley común de Estados Unidos propiedad de IBM en el momento de la publicación de esta información. Estas marcas también pueden estar registradas en otros países.

Encontrará una lista actualizada de las marcas registradas de IBM en <http://www.ibm.com/legal/copytrade.shtml>.

Los términos siguientes son marcas registradas de International Business Machines Corporation en los Estados Unidos y/o en otros países:

IBM
AIX
eServer
FlashCopy

Netfinity
POWER
Series p
RS/6000
TotalStorage

Adobe y PostScript son marcas registradas de Adobe Systems Incorporated en EE.UU. y/o en otros países.

Intel, Intel Xeon, Itanium y Pentium son marcas comerciales o marcas registradas de Intel Corporation o sus filiales en los Estados Unidos y otros países.

Java y todas las marcas registradas de Java son marcas registradas de Sun Microsystems, Inc. en EE.UU. y/o en otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos o en otros países.

Microsoft, Windows y Windows NT son marcas registradas de Microsoft Corporation en los Estados Unidos y/o en otros países.

UNIX es una marca registrada de The Open Group en Estados Unidos y en otros países.

Otros nombres de servicio, producto o empresa pueden ser marcas registradas de terceros.

Notas importantes

La velocidad del procesador indica la velocidad del reloj interno del microprocesador; otros factores también afectan al rendimiento de la aplicación.

Este producto no está pensado para conectarse directa o indirectamente por ningún medio a las interfaces de las redes de telecomunicaciones públicas.

La velocidad de las unidades de CD o DVD indica la velocidad de lectura variable. Las velocidades reales varían y, a menudo, son inferiores al máximo posible.

Cuando se hace referencia al almacenamiento de procesador, el almacenamiento real y virtual, o el volumen de canales, 1 KB equivale a 1024 bytes, 1 MB equivale a 1.048.576 bytes y 1 GB equivale a 1.073.741.824 bytes.

Cuando se hace referencia a la capacidad de la unidad de disco duro o al volumen de comunicaciones, 1 MB equivale a 1.000.000 bytes y 1 GB equivale a 1.000.000.000 bytes. La capacidad total a la que puede acceder el usuario puede variar dependiendo del entorno operativo.

En las capacidades máximas de las unidades de disco duro internas se da por supuesta la sustitución de cualquiera de las unidades de disco duro estándar y la utilización, en todas las bahías de unidad de disco duro, de las unidades de mayor capacidad soportadas actualmente de las que dispone IBM.

Para obtener la memoria máxima puede ser necesario sustituir la memoria estándar por un módulo de memoria opcional.

IBM no se hace responsable ni garantiza los productos que no sean de IBM ni los servicios que sean ServerProven, incluyendo, entre otros, las garantías implícitas de mercantibilidad y ajustes para un fin específico. Estos productos sólo los ofrecen y garantizan terceros.

IBM no representa ni ofrece ninguna garantía relacionada con productos que no son de IBM. El soporte para productos que no son IBM (si existe) lo proporcionará el tercero y no IBM.

Algún software puede diferir de la versión comercial (si está disponible) y puede no incluir manuales de usuario o todas las funciones del programa.

Glosario

Este glosario proporciona definiciones de la terminología y abreviaturas utilizadas en las publicaciones sobre IBM System Storage.

Si no encuentra el término que busca, consulte el *IBM Glossary of Computing Terms* ubicado en el siguiente sitio Web:

<http://www.ibm.com/ibm/terminology>

Este glosario también incluye términos y definiciones de:

- *Information Technology Vocabulary* del Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Las definiciones se identifican con el símbolo (I) situado tras la definición; las definiciones extraídas del borrador de los estándares internacionales, borradores del comité y trabajos de ISO/IEC JTC1/SC1 se identifican con el símbolo (T) situado tras la definición, lo cual indica que los organismos nacionales de SC1 aún no han establecido un acuerdo final.
- *IBM Glossary of Computing Terms*. Nueva York: McGraw-Hill, 1994.

En este glosario se utilizan los siguientes convenios de referencias cruzadas:

Consulte

Remite a (a) un término que corresponde a la expresión completa de una abreviatura o acrónimo, o (b) un sinónimo o término de uso preferente.

Consulte también

Le remite a un término relacionado.

AL_PA

Consulte *dirección física de bucle arbitrado*.

arreglo temporal de programa (PTF)

Para productos de System i, System p y System z, arreglo que prueba IBM y que se pone a disposición de todos los clientes.

AT Consulte también *arquitectura de bus de tecnología avanzada (AT)*.

adaptador de bus de host (HBA)

Tarjeta de interfaz que conecta un bus de host, como un bus PCI (interconexión de componentes periféricos), a la red de área de almacenamiento.

almacenamiento no volátil (NVS)

Dispositivo de almacenamiento cuyo contenido no se pierde en caso de producirse una interrupción en la alimentación.

arquitectura Micro Channel (MCA)

Reglas que definen la manera en que los subsistemas y adaptadores utilizan el bus de Micro Channel en un sistema. MCA define los servicios que cada subsistema puede o debe proporcionar.

AGP Consulte *puerto de gráficos acelerados*.

ATA Consulte *conexión AT*.

Arquitectura de almacenamiento serie (SSA)

Estándar del American National Standards Institute (ANSI), implementado por IBM para una interfaz en serie de alta velocidad que proporciona una conexión punto a punto para periféricos con subsistemas de almacenamiento. La SSA, que es compatible con los dispositivos de interfaz para pequeños sistemas (SCSI), admite transferencias de datos serie multiplexados de paquetes dúplex a velocidades de 20 Mbps en cada dirección.

arquitectura estándar de la industria (ISA)

Nombre no oficial que recibe la arquitectura de bus del sistema personal IBM PC/XT. Este diseño de bus incluía ranuras de expansión para conectar varias placas de adaptador. En las versiones anteriores tenía una vía de datos de 8 bits, que más tarde se amplió a 16 bits. La "Arquitectura estándar de la industria" (EISA) ha seguido ampliando la vía de datos hasta los 32 bits. Consulte también *arquitectura estándar de la industria ampliada*.

ADT Consulte *Transferencia automática de unidad*.

Abstract Windowing Toolkit (AWT)

En programación Java, una colección de

componentes de GUI implementados mediante versiones de plataforma nativa de los componentes. Estos componentes proporcionan el subconjunto de funciones común a todos los entornos de sistema operativo.

alojamiento de expansión de almacenamiento (EXP), o alojamiento de almacenamiento

Dispositivo que puede conectarse con una unidad del sistema para proporcionar capacidad de proceso y de almacenamiento adicionales.

adaptador

Conjunto de circuitos impresos que transmite la entrada/salida (E/S) de los datos de usuario entre el bus interno del sistema principal y el enlace de Canal de fibra (FC) externo y viceversa. También denominado adaptador de E/S, adaptador del sistema principal o adaptador de canal de fibra.

arquitectura estándar de la industria ampliada (EISA)

Estándar de bus de PC que amplía el bus AT (bus ISA) a 32 bits y proporciona soporte para el bus master. Se presentó en 1988 como una alternativa de 32 bits para el microcanal que mantendría la inversión en las placas existentes. Los adaptadores de PC y AT (adaptadores ISA) se pueden conectar en el bus EISA. Consulte también *arquitectura estándar de la industria*.

arquitectura de bus de tecnología avanzada (AT)

Estándar de bus para sistemas compatibles con IBM. Amplía la arquitectura de bus XT a 16 bits y también da soporte a la función de control maestro de bus, aunque sólo están disponibles para el acceso directo los 16 primeros MB de la memoria principal.

agente Programa servidor que recibe conexiones virtuales del gestor de red (el programa cliente) en un entorno de gestión de red SNMP-TCP/IP (Protocolo simple de gestión de red-Protocolo de control de la transmisión/Protocolo Internet).

acceso directo a la memoria (DMA)

Transferencia de datos entre la memoria y un dispositivo de entrada/salida (E/S) sin la intervención del procesador.

AWT Consulte *Abstract Windowing Toolkit*.

ámbito

Define un grupo de controladores por sus direcciones IP (Protocolo Internet). Para poder asignar direcciones IP dinámicas a los controladores de la red, debe crearse y definirse un ámbito.

bus local PCI

Consulte *bus local de interconexión de componentes periféricos*.

bucle arbitrado de canal de fibra (FC-AL)

Consulte *bucle arbitrado*.

BOOTP

Consulte *protocolo de arranque*.

Base de información de gestión (MIB)

En el protocolo simple de gestión de red (SNMP), base de datos de objetos que un sistema de gestión de red puede consultar o establecer.

Definición para la información de gestión que especifica la información que hay disponible en un sistema principal o en una pasarela y las operaciones permitidas.

bucles de unidad

Un bucle de unidad consta de un canal de cada director que se combina para formar un par de canales de unidad redundantes o un bucle de unidad redundante. Cada bucle de unidad se asocia a dos puertos. (Existen dos canales de unidad y cuatro puertos asociados por controlador.) En el DS4800, es muy común que se haga referencia a los bucles de unidad como canales de unidad. Consulte *canales de unidad*.

bucle privado

Bucle arbitrado de canal de fibra (FC-AL) sin accesorio de tejido. Consulte también *bucle arbitrado*.

bus local Peripheral Component Interconnect (bus local PCI)

Bus local para los sistemas personales, de Intel, que proporciona una vía de datos de alta velocidad entre la CPU y un máximo de 10 periféricos (vídeo, disco, red, etc.). El bus PCI coexiste en el PC con el bus de Arquitectura estándar de la industria (ISA) o el bus de Arquitectura estándar de la industria ampliada (EISA). Las placas ISA y EISA se conectan a una ranura IA o EISA, mientras que los controladores PCI de alta velocidad se conectan a una ranura PCI. Consulte

también *arquitectura estándar de la industria, arquitectura estándar de la industria ampliada.*

BIOS Consulte *sistema básico de entrada/salida.*

bucle arbitrado

Una de las tres topologías de canal de fibra existentes en la que los puertos 2 - 126 se interconectan en serie en un circuito de bucle individual. El acceso al bucle arbitrado de canal de fibra (FC-AL) se controla mediante un esquema de arbitraje. La topología de FC-AL da soporte a todas las clases de servicio y garantiza la entrega ordenada de las tramas de canal de fibra cuando el originador y el que responde se encuentran en la misma FC-AL. La topología por omisión para la matriz de discos es el bucle arbitrado. A veces, también se hace referencia al bucle arbitrado como Modalidad oculta.

con conexión AT

Dispositivos periféricos compatibles con el estándar para sistemas IBM AT original en el que las señales de un cable de cinta plano con conexión AT (ATA) de 40 patillas han seguido los patrones temporales y las restricciones del bus de sistema ISA (arquitectura estándar de la industria) en el sistema IBM PC AT. Equivale a electrónica de unidad integrada (IDE).

copia global

Hace referencia a un par de duplicación de unidades lógicas remotas que se ha configurado mediante la utilización de la modalidad de grabación asíncrona sin la opción de grupo de coherencia de grabación. También se denomina "duplicación asíncrona sin grupo de coherencia". La copia global no garantiza que las solicitudes de escritura a diversas unidades lógicas primarias se realicen en el mismo orden que están en estas en las unidades lógicas secundarias. Si es fundamental que la escritura de las unidades lógicas primarias se realice en el mismo orden en las unidades lógicas secundarias adecuadas, debe utilizar la duplicación global en vez de la copia global. Consulte también *modalidad de grabación asíncrona, duplicación global, duplicación remota, duplicación Metro Mirror.*

clave de característica premium

Archivo que el controlador de subsistema de almacenamiento utiliza para habilitar una característica premium autorizada. Este archivo contiene el identificador de habilitación de característica del subsistema de almacenamiento para el que la característica adicional está autorizada, así como datos acerca de dicha característica premium. Consulte también *identificador de característica premium.*

canales de unidad

Los subsistemas DS4200, DS4700 y DS4800 utilizan canales de unidad de puerto dual que, desde el punto de vista físico, se conectan del mismo modo que dos bucles de unidad. Sin embargo, desde el punto de vista del número de unidades y alojamientos, se tratan como si fueran un único bucle de unidad en lugar de dos bucles de unidad distintos. Los alojamientos de expansión de un grupo de almacenamiento se conectan a los subsistemas de almacenamiento DS3000 o DS4000 utilizando un canal de unidad para cada controlador. A este par de canales de unidad se hace referencia como par de canales de unidad redundantes.

concentrador

En una red, punto en el que se conectan o se conmutan los circuitos. Por ejemplo, en una red en estrella, el concentrador es el nodo central; en una red en estrella/anillo, es la ubicación de los concentradores de cables.

conversor de interfaz gigabit (GBIC)

Dispositivo de codificación/descodificación formado por un conjunto de componentes láser de clase 1 con receptáculos de transmisión y recepción que se conecta a cables de fibra óptica. Los GBIC realizan conversiones óptica a eléctrica y eléctrica a óptica en serie de la señal. Los GBIC de conmutadores se pueden sustituir en caliente. Consulte también *conectable de formato pequeño.*

conjunto RAID

Consulte *matriz.*

conectable de formato pequeño (SFP)

Transceptor óptico que se utiliza para convertir las señales entre los cables de fibra óptica y los conmutadores. Un SFP

es más pequeño que un conversor de interfaz gigabit (GBIC). Consulte también *conversor de interfaz gigabit*.

controlador IBMSAN

Controlador de dispositivo que se utiliza en un entorno Novell NetWare para proporcionar al controlador de almacenamiento soporte de entrada salida (E/S) de varias vías.

conmutador

Dispositivo de canal de fibra que proporciona ancho de banda completo por puerto y direccionamiento de datos de alta velocidad con direccionamiento de nivel de enlace.

comprobación de redundancia cíclica (CRC)

(1) Comprobación de la redundancia en la que un algoritmo cíclico genera la clave de comprobación. (2) Técnica de detección de errores que tiene lugar en las estaciones de envío y de recepción.

canal de fibra (FC)

Una tecnología para transmitir datos entre dispositivos informáticos. Es particularmente adecuada cuando se desea conectar servidores de sistemas a dispositivos de almacenamiento compartido o interconectar unidades y controladores de almacenamiento. FC da soporte a topologías punto a punto, bucle arbitrado y conmutadas.

controlador de matriz de discos (dac)

El dispositivo, como la matriz redundante de discos independientes (RAID), que gestiona una o varias matrices de discos y proporciona funciones. Consulte también *direccionador de matriz de discos*.

cartucho de ESM

Consulte *cartucho de módulo de servicios medioambientales*.

CRU Consulte *unidad sustituible por el cliente*.

codificación de corrección de errores (ECC)

Código añadido a un bloque de datos con capacidad para detectar y corregir errores de bits múltiples dentro del bloque. La mayor parte de los códigos ECC se caracterizan por el número máximo de errores que pueden detectar y corregir.

carga del programa inicial (IPL)

Proceso que carga los programas del sistema desde el almacenamiento auxiliar

del sistema, comprueba el hardware del sistema y prepara el sistema para las operaciones del usuario. También se denomina reinicio del sistema, arranque del sistema y arranque.

circuito integrado (IC)

Dispositivo semiconductor microelectrónico que consta de numerosos transistores interconectados y de otros componentes. Los circuitos integrados se elaboran a partir de un pequeño rectángulo de cristal de silicio u otro material semiconductor. El reducido tamaño de estos circuitos permite obtener una alta velocidad, una escasa disipación del calor y un bajo coste de fabricación en comparación con la integración en la placa. También se denomina *chip*.

cartucho de módulo de servicios de entorno (ESM)

Componente de un alojamiento de expansión del almacenamiento que supervisa las condiciones del entorno de los componentes que se encuentran en ese alojamiento. No todos los subsistemas de almacenamiento disponen de cartuchos de ESM.

control de acceso a soportes (MAC)

En sistemas de red, las dos subcapas inferiores de la capa de enlace de datos del modelo Open Systems Interconnection. La subcapa MAC maneja el acceso al soporte compartido, como por ejemplo si se utiliza el paso de señales o la contención.

controlador de matriz de discos redundante (RDAC)

En hardware, un conjunto redundante de controladores (activo/pasivo o activo/activo).

En software, una capa que gestiona la entrada/salida (E/S) a través del controlador activo durante la operación normal y redirecciona de manera transparente las E/S al otro controlador del conjunto redundante su falla un controlador o ruta de E/S.

CRT Consulte *tubo de rayos catódicos*.

CRC Consulte *comprobación de redundancia cíclica*.

comando

Una sentencia utilizada para iniciar una acción o un servicio. Un comando se

compone de la abreviatura del nombre del comando y, si se aplica, de sus parámetros y distintivos. Una comando se emite escribiendo éste en una línea de comandos o bien seleccionando el comando deseado en un menú.

cliente

Programa de software o sistema que solicita servicios de un servidor. Varios clientes pueden compartir el acceso a un servidor común.

comprobación de paridad

Prueba para determinar si el número de unos (o de ceros) de una matriz de dígitos binarios es par o impar.

Operación matemática para la representación numérica de la información que se transmite entre dos componentes. Por ejemplo, si la paridad es impar, se añadirá un bit a cualquier carácter representado por un número par, con lo que se transformará en impar, y el receptor de la información comprobará que cada unidad de información tenga un valor impar.

dirección de bucle

ID exclusivo de un nodo en la topología de bucle de canal de fibra al que, a veces, se hace referencia como ID de bucle.

descarga simultánea

Método para bajar e instalar firmware en el que no es necesario que el usuario detenga la actividad de E/S de los controladores durante el proceso.

difusión

Transmisión simultánea de datos a más de un destino.

direccionador

Sistema que determina la vía de acceso del flujo del tráfico de la red. La selección de la vía de acceso se realiza a partir de varias vías de acceso, basándose en la información obtenida de protocolos específicos, algoritmos que intentan identificar cuál es la vía de acceso más corta o mejor y otros criterios, como, por ejemplo, la métrica o las direcciones de destino específicas del protocolo.

dirección de bloque lógico (LBA)

Dirección de un bloque lógico. Las direcciones de bloque lógico se utilizan normalmente en comandos de E/S del

host. Por ejemplo, el protocolo de mandatos de discos SCSI utiliza direcciones de bloques lógicos.

duplicación remota

Duplicación de datos en línea y en tiempo real entre los subsistemas de almacenamiento que se mantienen en medios separados. La opción de duplicación remota mejorada es una característica premium que proporciona soporte para la duplicación remota. Consulte también *duplicación global*, *duplicación de Metro Mirror*.

datos de detección

Datos enviados con una respuesta negativa, indicando la razón de la respuesta.

Datos que describen un error de E/S. Los datos de detección se envían a un sistema principal como respuesta a un mandato de petición de detección.

destinatario de interrupción

Receptor de un mensaje de condición de excepción de Protocolo simple de gestión de red (SNMP) que se ha reenviado. Específicamente, un receptor de mensaje de condición de excepción se define por medio de una dirección IP (Protocolo Internet) y un puerto al que se envían los mensajes de condición de excepción. Se supone que el destinatario real es una aplicación de software que se ejecuta en la dirección IP y que está a la escucha en el puerto.

disco compartido virtual recuperable (RVSD)

Disco compartido virtual en un nodo de servidor que se ha configurado para proporcionar acceso continuado a los datos y a los sistemas de archivos en un clúster.

dirección de Protocolo de Internet (IP)

Dirección exclusiva de un dispositivo o una unidad lógica en una red que utiliza el estándar IP. Por ejemplo, 9.67.97.103 es una dirección IP.

dentro de banda

Transmisión del protocolo de gestión a través del transporte de canal de fibra.

DRAM

Consulte *memoria dinámica de acceso aleatorio*.

distribución en zonas de los conmutadores

Consulte *distribución en zonas*.

dispositivo de almacenamiento de acceso directo (DASD)

Dispositivo en el que el tiempo de acceso es realmente independiente de la ubicación de los datos. La información se entra y se recupera sin consultar los datos a los que se ha accedido anteriormente. Por ejemplo, una unidad de disco es un DASD, y no lo es una unidad de cintas, que almacena los datos en secuencia lineal. Los DASD incluyen dispositivos de almacenamiento fijos y extraíbles.

duplicación

Técnica de tolerancia de errores mediante la cual la información de un disco duro se duplica en otros discos duros. Consulte también *duplicación remota*.

dac Consulte *controlador de matriz de discos*.

direccionador de matriz de discos (dar)

Un direccionador que representa una matriz completa, incluyendo las rutas actual y aplazadas a todos los números de unidad lógica (LUN) (hdisks en AIX). Consulte también *controlador de matriz de discos*.

DHCP Consulte *Protocolo de configuración dinámica de sistemas principales*.

dominio

Byte más significativo del identificador de puerto de nodo (puerto_N) del dispositivo de Canal de fibra (FC). No se utiliza en el ID de vía de acceso de hardware de canal de fibra-interfaz para pequeños sistemas (FC-SCSI). Debe ser el mismo para todos los destinos SCSI conectados lógicamente a un adaptador FC.

dirección física de bucle arbitrado (AL_PA)

Un valor de 8 bits utilizado para identificar un dispositivo participante en un bucle arbitrado. Un bucle puede tener uno o más AL_PA.

DMA Consulte *acceso directo a la memoria*.

descarga electrostática (ESD)

Flujo de corriente que se genera cuando los objetos que tienen carga estática se aproximan lo suficiente para que se produzca una descarga.

dar Consulte *direccionador de matriz de discos*.

distribución en zonas

En entornos de canal de fibra, la agrupación de varios puertos para formar una red de almacenamiento virtual y privada. Los puertos miembros de una zona pueden comunicarse entre sí, pero están aislados de puertos de otras zonas.

Función que permite la segmentación de los nodos por la dirección, el nombre o el puerto físico y que se proporciona por medio de concentradores o de conmutadores de tejido.

DASD

Consulte *dispositivo de almacenamiento de acceso directo*.

duplicación global

Una capacidad opcional de la característica de copia y duplicación remotos que proporciona una copia remota de distancia ampliada en dos sitios. Los datos que graba el sistema principal en la unidad de almacenamiento en el emplazamiento local se mantienen de forma automática en el emplazamiento remoto. Consulte también *modalidad de grabación asíncrona, copia global, duplicación remota y duplicación Metro Mirror*.

eventos servidor/dispositivo

Eventos que se producen en el servidor o un dispositivo designado que cumplen los criterios establecidos por el usuario.

eventos de acciones de usuario

Acciones que el usuario realiza, como por ejemplo la realización de cambios en la red de área de almacenamiento (SAN), en los valores, etc.

ECC Consulte *código de corrección de error*.

etiqueta

Valor de propiedad descubierto o facilitado por el usuario que se muestra bajo cada dispositivo de las correlaciones Física y Ruta de datos.

EEPROM

Consulte *memoria de sólo lectura programable que puede borrarse eléctricamente*.

estación de gestión

Sistema empleado para gestionar el subsistema de almacenamiento. Estación de gestión que no necesita estar conectada a un subsistema de almacenamiento a

través de una ruta de entrada/salida (E/S) de canal de fibra.

EISA Consulte *arquitectura estándar de la industria ampliada*.

E_port Consulte *puerto de expansión*.

ESD Consulte *descarga electrostática*.

EXP consulte *alojamiento de expansión de almacenamiento*.

Entorno de tiempo de ejecución Java (JRE)
Un subconjunto de un kit de desarrollador Java que contiene los principales programas ejecutables y archivos que constituyen la plataforma Java estándar. El JRE incluye la máquina virtual Java (JVM), las clases principales (core) y los archivos de soporte.

Exploración de medios
Una exploración de medios es un proceso de fondo que se ejecuta en todas las unidades lógicas del subsistema de almacenamiento para el que se ha habilitado y que proporciona detección de errores en los medios de la unidad. El proceso de la exploración de medios explora todos los datos de la unidad lógica para verificar si puede accederse a éstos y, opcionalmente, también explora la información de redundancia de la unidad lógica.

electrónica de unidad integrada (IDE)
Interfaz de unidad de disco basada en la Arquitectura estándar de la industria (ISA) de sistemas personales de IBM de 16 bits en la que la electrónica del controlador reside en la propia unidad, con lo que se elimina la necesidad de disponer de una tarjeta de adaptador por separado. También se denomina interfaz de conexión de tecnología avanzada (ATA).

entorno de host heterogéneo
Un sistema host en el que diversos servidores de host, que utilizan diferentes sistemas operativos con su propia configuración de subsistema de almacenamiento de disco único se conectan al mismo subsistema de almacenamiento a la vez. Consulte también *host*.

escritura en bandas
Consulte *escritura en bandas de datos*.

estación de gestión de la red (NMS)
En el Protocolo simple de gestión de red (SNMP), estación que ejecuta programas de aplicación de gestión que supervisan y controlan los elementos de la red.

FRU Consulte *unidad sustituible localmente*.

fuera de banda
Transmisión de protocolos de gestión que tiene lugar fuera de la red de Canal de fibra, por lo general, a través de Ethernet.

F_port Consulte *puerto de tejido*.

FC Consulte *canal de fibra*.

FlashCopy
Característica opcional de la familia Storage System DS que puede realizar copias instantáneas de los datos, es decir, copias puntuales de una unidad lógica.

FC-AL Consulte *bucle arbitrado*.

fragmentación de datos
Proceso de almacenamiento en el que la información se divide en bloques (una cantidad fija de datos) y los bloques se graban en (o se leen de) una serie de discos en paralelo.

grupo de puentes
Un puente y el conjunto de dispositivos conectados al mismo.

grupo de host
Entidad de la topología de partición del almacenamiento que define un conjunto lógico de hosts que necesitan disponer de acceso compartido a una o más unidades lógicas.

grupo de host predeterminado
Grupo lógico de puertos de host detectados, hosts definidos y grupos de host definidos en la topología de partición del almacenamiento que cumplen los requisitos siguientes:

- No están presentes en correlaciones de unidad lógica y LUN específicas.
- Comparten el acceso a las unidades lógicas con correlaciones de unidad lógica y LUN predeterminadas.

GUI Consulte *interfaz gráfica de usuario*.

gestor de datos de objeto (ODM)
Mecanismo de almacenamiento patentado por AIX para los archivos de secciones

ASCII que se editan como parte de la configuración de una unidad en el kernel.

GBIC Consulte *conversor de interfaz gigabit*

grupo de conmutador

Se trata de un conmutador y de una colección de dispositivos conectados con éste que no están en otros grupos.

grabar una vez leer varias (WORM)

Cualquier tipo de soporte de almacenamiento en el que los datos sólo pueden grabarse una vez, pero donde los datos pueden leerse cualquier número de veces. Una vez grabados los datos, no pueden modificarse.

grupo de bucle

Conjunto de dispositivos de red de área de almacenamiento (SAN) que están interconectados en serie en un único circuito de bucle.

hdisk Término de AIX que representa un número de unidad lógica (LUN) en una matriz.

host Sistema que se conecta directamente con el subsistema de almacenamiento por medio de una ruta de E/S de canal de fibra. Este sistema se utiliza para servir datos (normalmente en forma de archivos) del subsistema de almacenamiento. Un sistema puede ser una estación de gestión y un host de forma simultánea.

HBA Consulte *adaptador de bus de host*.

identificador de habilitación de de característica

Identificador exclusivo del subsistema de almacenamiento que se utiliza en el proceso para generar una clave de característica premium. Consulte también *clave de característica premium*.

IC Consulte *circuito integrado*.

interfaz gráfica de usuario (GUI)

Tipo de interfaz de sistema que presenta una metáfora visual de una escena real, a menudo de un escritorio, combinando gráficos de alta resolución, dispositivos de puntero, barras de menús y otros menús, ventanas superpuestas, iconos y la relación objeto-acción.

interfaz para pequeños sistemas (SCSI)

Interfaz electrónica de estándar ANSI que permite a los ordenadores personales

comunicarse con hardware periférico como unidades de disco, unidades de cintas, unidades de CD-ROM o DVD-ROM, impresoras y escáneres más rápido y con mayor flexibilidad que las interfaces anteriores.

Interfaz de hardware estándar que permite que gran diversidad de dispositivos periféricos puedan comunicarse entre sí.

intercambio en caliente

Relativo a un dispositivo que se puede sustituir mientras el sistema está encendido.

interrupción

En el Protocolo simple de gestión de red (SNMP), mensaje que envía un nodo gestionado (función de agente) a una estación de gestión para informar acerca de una condición de excepción.

identificador de subsistema de almacenamiento (SAI o identificador SA)

El identificador de subsistema de almacenamiento es el valor de identificación utilizado por el software host de Storage Manager (SMClient) para identificar de manera única cada servidor de almacenamiento gestionado. El programa SMClient de Storage Manager conserva registros del identificador del subsistema de almacenamiento de servidores de almacenamiento descubiertos con anterioridad en el archivo residente de host, lo cual permite conservar información de descubrimiento de manera persistente.

Identificador SA

Consulte *identificador de subsistema de almacenamiento*.

IDE Consulte *electrónica de unidad integrada*.

interrupción no enmascarable (NMI)

Interrupción de hardware sobre la que otra petición de servicio no puede prevalecer (enmascarar). Una NMI elude, y tiene prioridad sobre, las solicitudes de interrupción que genera el sistema, el teclado y otros dispositivos de este tipo, y se envía al microprocesador sólo en circunstancias muy graves, como, por ejemplo, cuando se han producido errores

de memoria muy graves o van a producirse inminentes anomalías en la alimentación.

- ISA** Consulte *arquitectura estándar de la industria*.
- IRQ** Consulte *petición de interrupción*.
- IPL** Consulte *carga del programa inicial*.
- IP** Consulte *Protocolo de Internet*.
- JRE** Consulte *Java Runtime Environment*.
- LPAR** Consulte *partición lógica*.
- LUN** Consulte *número de unidad lógica*.
- LBA** Consulte *dirección de bloque lógico*.
- LAN** Consulte *red de área local*.
- MIB** Consulte *base de información de gestión*.

memoria dinámica de acceso aleatorio (DRAM)

Almacenamiento en el que las células requieren la aplicación repetitiva de señales de control para retener datos almacenados.

memoria de sólo lectura programable que puede borrarse eléctricamente (EEPROM)

Tipo de chip de memoria que puede retener su contenido sin recibir alimentación eléctrica constante. A diferencia de la memoria PROM, que sólo puede programarse una vez, la memoria EEPROM puede borrarse electrónicamente. Puesto que sólo puede programarse un número limitado de tiempo antes de que se quede inservible, es adecuada para almacenar pequeñas cantidades de datos que no cambian con frecuencia.

modalidad de grabación síncrona

En la duplicación remota, opción que obliga al controlador primario a esperar un acuse de recibo de una operación de grabación del controlador secundario antes de devolver una indicación de finalización de petición de E/S al host. Consulte también *modalidad de grabación asíncrona, duplicación remota, duplicación Metro Mirror*.

Metro Mirror

Función de la característica de copia y duplicación remota que actualiza constantemente una copia secundaria de una unidad lógica para adaptarla a los cambios realizados en una unidad lógica

de origen. Consulte también *duplicación remota, duplicación global*.

miniconcentrador

Tarjeta de interfaz o dispositivo de puerto que recibe GBIC o SFP de canal de fibra de onda corta. Estos dispositivos habilitan conexiones de canal de fibra redundantes desde sistemas principales, tanto directamente como a través de un conmutador de canal de fibra o concentrador gestionado, por los cables de fibra óptica de los controladores DS3000 y DS4000 Storage Server. Cada controlador DS3000 y DS4000 es responsable de dos miniconcentradores. Cada miniconcentrador está asociado con dos puertos. Cuatro puertos de host (dos en cada controlador) proporcionan una solución de clúster sin el uso de un conmutador. En general, se facilitan dos miniconcentradores de lado host. Consulte también *puerto de host, conversor de interfaz gigabit (GBIC), conectable de formato pequeño(SFP)*.

modalidad de grabación asíncrona

En la duplicación remota, opción que permite al controlador primario devolver una indicación de finalización de petición de E/S de grabación al servidor de host antes de que el controlador secundario haya grabado correctamente los datos. Consulte también *modalidad de grabación asíncrona, duplicación remota, copia global, duplicación global*.

memoria de sólo lectura (ROM)

Memoria en la que el usuario no puede cambiar los datos almacenados, excepto cuando se dan condiciones especiales.

método de barrido

Método para enviar peticiones de Protocolo simple de gestión de red (SNMP) solicitando información a todos los dispositivos de un subred mediante el envío de la petición a cada dispositivo de la red.

memoria de acceso aleatorio (RAM)

Memoria de sistema en la que se puede acceder a cualquier ubicación de almacenamiento directamente. Compárese con *DASD*.

matriz Una colección de discos duros de canal de fibra o SATA agrupados de manera lógica. A todas las unidades de la matriz se les

ha asignado el mismo nivel de RAID. A veces, también se hace referencia a una matriz como "conjunto RAID". Véase *matriz redundante de discos independientes (RAID), nivel de RAID*.

memoria estática de acceso aleatorio (SRAM)

Memoria de acceso aleatorio basada en el circuito lógico que se conoce como circuito biestable o flip-flop. Se denomina estática porque retiene un valor mientras existe suministro de alimentación, a diferencia de la memoria dinámica de acceso aleatorio (DRAM), que debe renovarse regularmente. Sin embargo, sigue siendo volátil en tanto que puede perder su contenido cuando se apaga la alimentación.

MCA Consulte *arquitectura Micro Channel*.

Microsoft Cluster Server (MSCS)

Tecnología que proporciona una alta disponibilidad al agrupar sistemas en clústeres de MSCS. Si uno de los sistemas del clúster tiene algún problema de una gama, MSCS cierra de forma ordenada la aplicación interrumpida, transfiere sus datos de estado a otro sistema del clúster y reinicia la aplicación en ese punto.

MSCS Consulte *Microsoft Cluster Server*.

matriz redundante de discos independientes (RAID)

Colección de dos o más unidades de disco físicas (o una *matriz*) que presentan al host una imagen de una o más unidades de disco lógicas. Si se produce una anomalía en un dispositivo físico, los datos se pueden leer o volver a generar desde las otras unidades de disco de la matriz mediante la redundancia de datos. Consulte también *matriz, comprobación de paridad, duplicación, nivel RAID, escritura en bandas*.

MAC Consulte *control de acceso a soportes*.

modelo

Identificación de modelo que el fabricante asigna a un dispositivo.

nombre de ámbito mundial (WWN)

Identificador de nombre único, sin firma, de 64 bits asignado a cada puerto de canal de fibra.

NVSRAM

Memoria de acceso aleatorio de

almacenamiento no volátil. Consulte *almacenamiento no volátil*.

Nivel RAID

Los niveles de matriz RAID son un número que hace referencia al método utilizado para lograr la redundancia y la tolerancia al error en la matriz. Consulte también *matriz, matriz redundante de discos independientes (RAID)*.

NVS Consulte *almacenamiento no volátil*.

N_port

Consulte *puerto de nodo*.

NMI Consulte *interrupción no enmascarable*.

NMS Consulte *estación de gestión de red*.

nombre de puerto de ámbito mundial (WWPN)

Identificador de 64 bits único asociado con un conmutador. El WWPN se asigna de forma independiente en relación con la implementación y el protocolo.

nombre del sistema

Nombre de dispositivo asignado por el software de otros proveedores.

nodo Dispositivo físico que permite la transmisión de datos dentro de una red.

número de unidad lógica (LUN)

En el estándar SCSI (interfaz para pequeños sistemas), se utiliza un identificador exclusivo para diferenciar dispositivos, cada uno de los cuales es una unidad lógica (LU).

ODM Consulte *gestor de datos de objetos*.

Protocolo de Internet (IP)

Protocolo que direcciona los datos por medio de una red o de redes interconectadas. El Protocolo Internet (IP) actúa de intermediario entre las capas de protocolo más altas y la red física.

puerto de nodo (N_port)

Entidad de hardware definida del Canal de fibra que lleva a cabo las comunicaciones de datos a través de un enlace de Canal de fibra. Puede identificarse por medio de un nombre universal exclusivo. Puede actuar como elemento originador o de respuesta.

puerto de tejido (F_port)

En un tejido, punto de acceso para la conexión del puerto_N de un usuario. Un puerto de tejido (F_port) facilita

conexiones de N_port al tejido desde los nodos conectados al tejido. Un puerto_F se direcciona por medio del puerto_N que está conectado con éste. Consulte también *tejido*.

protocolo de canal de fibra (FCP) para interfaz para pequeños sistemas (SCSI)

Capa de correlación de canal de fibra de alto nivel (FC-4) que utiliza servicios de canal de fibra de menor nivel (FC-PH) para transmitir comandos, datos, e información de estado SCSI entre un iniciador SCSI y un destino SCSI a través del enlace de FC con formatos de secuencia y marco FC.

programa que termina y permanece residente (programa TSR)

Programa que instala parte de sí mismo como una extensión de DOS al ejecutarse.

puerto de host

Puertos que residen físicamente en los adaptadores de host y son descubiertos automáticamente por el software Storage Manager. Para que un host pueda disponer de acceso a una partición, deben definirse sus puertos de host asociados.

Portable Document Format (PDF)

Un estándar especificado por Adobe Systems, Incorporated, para la distribución electrónica de documentos. Los archivos PDF son compactos; se pueden distribuir a nivel global a través de correo electrónico, Internet, intranets, CD-ROM o DVD-ROM; y se pueden visualizar con Acrobat Reader.

puerto de gráficos acelerados (AGP)

Especificación de bus que proporciona a las tarjetas gráficas de 3D de bajo coste un acceso más rápido a la memoria principal de los PC que el bus de interconexión de componentes periféricos (PCI). Los AGP reducen el coste global de la creación de subsistemas de gráficos de alta gama subsistemas con la memoria del sistema existente.

puerto de bucle convertido (TL_port)

Puerto que se conecta con un bucle privado y que permite la conectividad entre los dispositivos de bucle privado y los dispositivos de bucle externo (dispositivos no conectados con ese puerto_TL en particular).

página man

En sistemas UNIX, una página de documentación en línea. Cada mandato UNIX, programa de utilidad y función de biblioteca tiene asociada una página man.

protocolo de control de transmisión (TCP)

Protocolo de comunicaciones que se utiliza en Internet y en cualquier red que siga los estándares de la Internet Engineering Task Force (IETF) para el protocolo de interconexión de redes. TCP proporciona un protocolo fiable de host a host en redes de comunicaciones conmutadas mediante paquetes y en sistemas interconectados mediante tales redes.

puerto de bucle segmentado (SL_port)

Puerto que permite la división de un bucle privado de canal de fibra en diversos segmentos. Cada segmento puede pasar tramas como un bucle independiente y puede conectarse por medio del tejido con otros segmentos del mismo bucle.

protocolo de control de transmisión/Protocolo Internet (TCP/IP)

Conjunto de protocolos de comunicaciones que proporcionan funciones de conectividad de igual a igual para las redes de área local y de área amplia.

puerto de bucle

Puerto utilizado para conectar un nodo a un bucle arbitrado de canal de fibra (FC-AL).

protocolo simple de gestión de red (SNMP)

Conjunto de protocolos para sistemas y dispositivos de supervisión en redes complejas. La información sobre dispositivos gestionados se define y almacena en una Base de información de gestión (MIB).

partición de almacenamiento

Unidades lógicas del subsistema de almacenamiento que son visibles para un sistema principal o que se comparten entre los sistemas principales que forman parte de un grupo de sistemas principales.

puente

Dispositivo SAN (red de área de almacenamiento) que proporciona

conversión física y de transporte, como, por ejemplo, el puente de Canal de fibra a SCSI (interfaz para pequeños sistemas).

partición

Consulte *partición de almacenamiento*.

Protocolo de arranque (BOOTP)

Un protocolo que permite a un cliente encontrar su dirección de Protocolo Internet (IP) y el nombre de un archivo de un servidor en la red.

Protocolo de configuración dinámica de hosts (DHCP)

Protocolo de comunicaciones utilizado para gestionar centralmente la información de configuración. Por ejemplo, DHCP asigna automáticamente direcciones IP a los sistemas en una red.

programa TSR

Consulte *programa que termina y permanece residente*.

puerto Parte de la unidad del sistema o del controlador remoto a los que se conectan los cables de dispositivos externos (estaciones de visualización, terminales, impresoras, conmutadores o unidades de almacenamiento externo). El puerto es un punto de acceso para la entrada o la salida de datos. Un dispositivo puede contener uno o más puertos.

puerto de expansión (E_port)

En la compilación de un tejido de conmutador más grande, puerto utilizado como puerto de expansión inter-conmutador para conectar con el E_port de otro conmutador.

partición lógica (LPAR)

Subconjunto de un único sistema que contiene recursos (procesadores, memoria y dispositivos de entrada/salida). Una partición lógica opera como sistema independiente. Si se satisfacen los requisitos de hardware, dentro de un sistema pueden existir varias particiones lógicas.

Porción de tamaño fijo de una unidad lógica. Una partición lógica tiene el mismo tamaño que las particiones físicas de su matriz. A menos que se duplique la unidad lógica de la que forma parte, cada partición lógica pertenece a una partición física individual, y sus contenidos están almacenados en esta.

Entre una y tres particiones físicas (copias). El número de particiones lógicas dentro de una unidad lógica es variable.

PTF Consulte *arreglo temporal de programa*.

PDF Consulte *Portable Document Format*.

RVSD Consulte *disco compartido virtual recuperable*.

RDAC Consulte *controlador de matriz de discos redundante*.

RAM Consulte *memoria de acceso aleatorio*.

RAID Consulte *matriz redundante de discos independientes (RAID)*.

red de área de almacenamiento(SAN)

Red de almacenamiento dedicada adaptada a un entorno específico, que combina servidores, productos de almacenamiento, productos de red, software y servicios. Consulte también *tejido*.

retardo de sondeo

Tiempo, expresado en segundos, que ha de transcurrir entre procesos de detección sucesivos durante los cuales la detección está inactiva.

red de área local (LAN)

Red que conecta varios dispositivos en un área limitada (como un único edificio o campus) y que se puede conectar con una red más grande.

ROM Consulte *memoria de sólo lectura*.

sistema principal
Consulte *host*.

subred

Red dividida en subgrupos independientes más pequeños, que continúan conectados entre sí.

SSA Consulte *arquitectura de almacenamiento en serie*.

sistema de alimentación ininterrumpible

Una fuente de alimentación proveniente de una batería situada entre la alimentación comercial y el sistema que mantiene el sistema en funcionamiento, en caso de interrumpirse la alimentación comercial, hasta que el procesamiento del sistema finaliza de manera ordenada.

suceso de rendimiento

Evento relacionado con los umbrales de rendimiento definidos en la red de área de almacenamiento (SAN).

solicitud de interrupción (IRQ)

Entrada en un procesador que hace que se suspenda temporalmente la ejecución de instrucción normal y se inicie la ejecución de una rutina de manejador de interrupción.

sincronización de firmware de ESM automática

Cuando instala un nuevo ESM en un alojamiento de almacenamiento existente de un subsistema de almacenamiento DS3000 o DS4000 que soporta la sincronización de firmware de ESM automática, el firmware del nuevo ESM se sincroniza automáticamente con el firmware del ESM existente.

SAI Consulte *identificador de subsistema de almacenamiento*.

serie de caracteres de comunidad

Nombre de una comunidad contenido en cada uno de los mensajes de Protocolo simple de gestión de red (SNMP).

SAN Consulte *red de área de almacenamiento*.

SATA Consulte *Serial ATA*.

SRAM

Consulte *memoria estática de acceso aleatorio*.

SCSI Consulte *interfaz para pequeños sistemas*.

Serial ATA

Estándar de una alternativa de alta velocidad a las unidades de disco duro de interfaz para pequeños sistemas (SCSI). El rendimiento del estándar SATA-1 equivale al rendimiento de una unidad SCSI a 10.000 RPM.

servidor

Programa de software o sistema que proporciona servicios a otros programas de software o sistemas.

SFP Consulte *conectable de formato pequeño*.

SL_port

Consulte *puerto de bucle segmentado*.

SMagent

El software agente de host basado en Java opcional de Storage Manager, que se puede utilizar en Microsoft Windows, Novell NetWare, AIX, HP-UX, Solaris y

Linux en sistemas host POWER para gestionar subsistemas de almacenamiento a través de la canal de fibra host.

Sistema básico de entrada/salida (BIOS)

Código que controla las operaciones de hardware básicas, por ejemplo las interacciones con las unidades de disquete, las unidades de disco duro y el teclado.

SMclient

El software cliente de Storage Manager, con interfaz gráfica de usuario (GUI) basada en Java utilizado para configurar, gestionar, y solucionar problemas relacionados con los servidores de almacenamiento y los alojamientos de expansión del almacenamiento de un subsistema de almacenamiento. SMclient se puede utilizar en un sistema host o en una estación de gestión.

SMruntime

Compilador Java para SMclient.

SNMPv1

Actualmente, el estándar original de SNMP se denomina SNMPv1 para diferenciarlo de SNMPv2, que es una revisión de SNMP. Consulte también *protocolo simple de gestión de red*.

SMutil

Programa de utilidad de Storage Manager utilizado en Microsoft Windows, AIX, HP-UX, Solaris y Linux en sistemas host POWER para registrar y correlacionar nuevas unidades lógicas con el sistema operativo. En Microsoft Windows, también contiene un programa de utilidad para desechar los datos de la memoria caché del sistema operativo de una unidad concreta antes de crear una FlashCopy.

SNMP

Consulte *protocolo simple de gestión de red y SNMPv1*.

suceso de condición de excepción de SNMP

Notificación de suceso que envía el agente SNMP y que identifica condiciones, como por ejemplo los umbrales, que han excedido un valor predeterminado. Consulte también *protocolo simple de gestión de red*.

Transferencia automática de unidad (ADT)

Función que proporciona sustitución por anomalía automática en caso de producirse una anomalía de controlador en un subsistema de almacenamiento.

tubo de rayos catódicos (CRT)

Dispositivo de visualización en el que se utilizan haces de electrones controlados para visualizar datos alfanuméricos o datos gráficos en una pantalla electroluminiscente.

tejido Entidad de canal de fibra que interconecta y facilita conexiones de los puertos de nodo (N_port) conectados a ella. El tejido se ocupa del direccionamiento de tramas entre N_ports de origen y de destino utilizando la información de dirección de la cabecera de la trama. Un tejido puede ser tan simple como un canal de punto a punto entre dos puertos de nodos (N-port), o tal complejo como un conmutador de direccionamiento de tramas que proporciona varias vías internas redundantes dentro del tejido entre los puertos de tejido (F_port).

tipo de dispositivo

Identificador que se utiliza para situar los dispositivos en la correlación física, como por ejemplo, el conmutador, el concentrador o el almacenamiento.

topología de partición del almacenamiento

En el cliente de Storage Manager, la vista Topología de la ventana Correlaciones muestra el grupo de host predeterminado, el grupo de host definido, el sistema principal y los nodos de puerto de host. Para poder otorgar acceso a los sistemas principales o a los grupos de sistemas principales utilizando correlaciones de unidades lógicas y LUN, deben definirse los elementos topológicos del puerto del sistema principal, del sistema principal y del grupo de sistemas principales.

transmisor/receptor

En comunicaciones, el dispositivo que conecta el cable de transmisor/receptor al cable coaxial Ethernet. El transmisor/receptor se utiliza para transmitir y recibir datos. Transmisor/receptor.

TCP Consulte *protocolo de control de transmisiones*.

TCP/IP

Consulte *protocolo de control de transmisiones/protocolo Internet*.

topología

La correlación física o lógica de la ubicación de componentes de red o nodos dentro de una red. Las topologías de redes comunes son de tipo bus, anillo, estrella y árbol. Las tres topologías de Canal de fibra son el tejido, el bucle arbitrado y el punto a punto. La topología por omisión para la matriz de discos es el bucle arbitrado.

TL_port

Véase *puerto de bucle convertido*.

unidad sustituible localmente (FRU)

Un conjunto que se sustituye totalmente cuando uno de sus componentes no se ejecuta correctamente. En algunos casos, una unidad sustituible localmente puede contener otras unidades sustituibles localmente. Compárese con *unidad sustituible por el cliente (CRU)*.

unidad sustituible por el cliente (CRU)

Conjunto o componente que puede ser sustituido por el cliente. Compárese con *unidad sustituible localmente (FRU)*.

unidad lógica de acceso

Una unidad lógica que permite que el agente de host se comunique con los controladores del subsistema de almacenamiento.

WWN Consulte *nombre de ámbito mundial*.

WORM

Consulte *grabar una vez leer varias*.

Índice

A

- accesibilidad
 - características de Storage Manager 351
 - documento 351
- acceso a disco, minimizar 114
- actividad de E/S, supervisión 133
- actualizaciones
 - recepción xix
- actualizaciones (actualizaciones de productos) xix
- adaptadores de bus de host
 - Véase también* HBA
 - HBA
 - definición de puertos de hosts 65
 - Solaris
 - valores de QLogic 317
- adapter
 - Véase* HBAs
- ADT 190, 191
- agrupación de discos
 - creación 84
- agrupación en clúster
 - Configuración de VMware ESX Server 320
- AIX 147
 - atributos de gestor de datos de objeto (ODM)
 - visualización y definición 339
 - atributos de Object Data Manager (ODM)
 - comando lsattr 345
 - definiciones 339
 - dispositivos dac 339
 - dispositivos dar 339
 - dispositivos hdisk 339
- correlación del nuevo WWPN con subsistemas de almacenamiento 200
- errores de matriz de discos FCP 296
- intercambio en caliente de HBA, sustitución 194
- intercambio en caliente HBA, finalización 200
- intercambio en caliente HBA, preparación 192
- registro de errores 296
- servicios de clúster 327
- unidades lógicas, redistribución 190

- aplicaciones de imágenes médicas 87
- aplicaciones multimedia 87
- archivo de claves de característica 61
- archivos, desfragmentación 114
- archivos de registro 273
- cambios en la seguridad 267
- registro de eventos principal 267
- arranque remoto
- Véase* arranque SAN
- arranque SAN
- configuración de hosts 119
- requisitos 119

- Asistente de tareas
 - atajos 66
 - descripción 66
- atributo load_balancing 340
- atributos
 - dac 345
 - dar 345
 - hdisk 184, 345
 - LUN 184, 345
- atributos de Object Data Manager (ODM)
 - definiciones 339
 - identificación de dispositivos inicial 181
- autenticación de destino, cambio para iSCSI 47
- autorizaciones de seguridad, FDE 231
- avisos xviii
 - general 355
- avisos importantes 358
- ayuda
 - obtención xvii, xviii
 - sitios web xvi
- ayuda, en línea xiv

B

- BIOS
 - settings 303
- borrado seguro, FDE 230

C

- campo de datos E/S 110, 111
- canal de fibra
 - HBA en un entorno de conmutador 136
- Captura de datos de diagnóstico
 - Editor de scripts 293
 - eventos MEL 295
 - Gurú de recuperación 295
 - pasos de recuperación 294
 - Recovery Guru 293
- característica premium 102
- característica premium FC/SATA Intermix 58
- características
 - Fast!UTIL 303
- características, premium
 - Véase* características premium
- características premium 58
 - archivo de claves de característica 61
 - Cifrado de disco completo
 - Véase* FDE
 - clave 101, 102
 - configuración 99
 - descripciones de 58
 - FDE 215
 - FDE, habilitación 242
 - FDE y FlashCopy 269
 - FDE y VolumeCopy 269
- características premium 58
 - (*continuación*)
 - FlashCopy 100
 - habilitación 61
 - identificador de habilitación de característica 60
 - inhabilitación 62
 - Opción Duplicación remota 101
 - partición de almacenamiento 95, 96
 - uso 99
 - VolumeCopy 101
- CHAP 47
- cifrado de disco completo
 - Véase* FDE
- claves, seguridad (FDE)
 - Véase* FDE
- claves de seguridad
 - cambio (externo) 222
 - cambio (local) 222
 - creación 219
 - identificador 222
 - uso para desbloquear unidades FDE 256
- claves de seguridad, FDE
 - Véase* FDE
- coincidencia de memoria caché
 - optimización 113
 - porcentaje 113
- comentarios, Editor de scripts 115
- componentes, software Storage Manager 2, 38
- conexión en caliente PCI 197
- conexiones cruzadas
 - VMware ESX Server 323
- configuración 5, 6, 236, 246
 - Clústers GPFS, PSCP y HACMP 330
 - conexión a SAN 3, 7
 - conexión directa 3
 - conexión directamente 7
 - configuración iSCSI 46
 - contraseñas del subsistema de almacenamiento 43
 - controlador de dispositivos, controlador Linux DM-Multipath 147
 - dispositivos 182
 - DS TKLM Proxy Code, para gestión externa de claves de seguridad 235
 - ejemplo de red 4
 - exploración de soportes 108
 - HBA avanzada 305
 - HBA por defecto 304
 - hosts 119
 - IBM i 98
 - MTU 50
 - prioridad de modificación 114
 - puertos de hosts iSCSI 47
 - recuperación 78
 - red 3
 - servidor DS TKLM Proxy Code, inicio, detención y reinicio 236

- configuración (*continuación*)
 - subsistemas de almacenamiento 7
 - tipos 3
 - unidades de repuesto en caliente 92
 - unidades FDE 242
 - valores de red para conexión de host iSCSI 49
 - configuración con conexión a SAN
 - configuración 7
 - configuración de conexión directa
 - configuración de direcciones IP 8
 - configuración de gestión de agente de host 6
 - configuración de gestión en red 5
 - configuración dentro de banda
 - Véase* configuración de gestión de agente de host
 - configuración fuera de banda
 - Véase* configuración de gestión en red
 - configuraciones de conexión directa
 - configuración 7
 - configuration
 - HBA 303
 - conmutadores
 - distribución en zonas 7
 - en una configuración de conexión a SAN 7
 - conmutadores de distribución en zonas 7
 - contraseñas, definición 43
 - controlador de matriz de discos
 - Véase* dac
 - controlador de migración tras error
 - descripción 133
 - MPxIO 169
 - controlador DMP DSM 147
 - controlador Linux DM-Multipath 147
 - controlador multi-ruta 162
 - descripción 133
 - controlador RDAC
 - descripción 133
 - controladores
 - dar 180
 - direcciones 8
 - direcciones IP 8
 - matriz de discos 180
 - rpaphp 196
 - tasa de transferencia, optimización 112
 - controladores de dispositivo con clúster HACMP 329
 - controlador de migración tras error
 - RDAC en Solaris 174
 - controlador Linux DM-Multipath 147
 - descripción 133
 - DMP, instalación 176
 - HBA 142, 143
 - migración tras error 133
 - minipuerto SCSIport 143
 - multi-ruta 133
 - instalación 138
 - RDAC 133, 167
 - Storport Miniport 142
 - Veritas DMP DSM 147
 - controladores de Veritas DMP 162
 - controladores DMP 162
 - controladores Linux MPP 157
 - controladores MPP 157
 - controladores multi-ruta 121, 147, 157, 179
 - instalación 138
 - migración tras error 121
 - controladores multi-ruta AIX 147
 - controladores RDAC
 - archivos de configuración, modificación 174
 - descripción 167
 - Solaris, instalación en 174
 - Controller Firmware Upgrade Tool
 - visión general 54
- ## D
- dac
 - atributos 345
 - y RDAC 180
 - dar
 - atributos 345
 - y RDAC 180
 - datos
 - archivos, desfragmentación 114
 - protección con FDE 216
 - recopilación anterior al intercambio en caliente de HBA en AIX 192
 - redundancia 86
 - tamaño de segmento óptimo, elección 114
 - DCE 186
 - DDC
 - Véase* Captura de datos de diagnóstico
 - declaraciones xviii
 - descarga de firmware simultánea 50, 57
 - descubrimiento, subsistema de
 - almacenamiento automático 41
 - descubrimiento automático de subsistemas de almacenamiento 41
 - descubrimiento de destino, cambio para iSCSI 47
 - descubrimiento de host automático 41
 - descubrimiento manual 42
 - desinstalación
 - DS TKLM Proxy Code en Windows, para gestión externa de claves de seguridad 241
 - Storage Manager 40
 - DHCP, uso 48
 - dirección de Control de acceso a soportes (MAC)
 - Véase* direcciones MAC
 - dirección IP
 - IPv6 49
 - direccionador de matriz de discos
 - Véase* dar
 - direcciones IP 8
 - direcciones MAC
 - identificación 10
 - direcciones MAC Ethernet
 - Véase* direcciones MAC
 - direcciones TCP/IP , estáticas
 - asignación a subsistemas de almacenamiento 11
 - disco de reserva
 - unidades de disco FDE 266
 - disk drives
 - FDE, unlocking (local) 228
 - dispositivo UTM 180
 - dispositivos
 - adición 42
 - configuración 182
 - configuración de notificaciones de alerta 44
 - identificación 179, 181
 - distribución en zonas 136
 - distribución en zonas de conmutador de canal de fibra 136
 - DMP 167
 - planificación de la instalación 176
 - preparación para la instalación 176
 - documentación
 - accesibilidad 351
 - acerca de xi
 - avisos xviii
 - declaraciones xviii
 - prácticas recomendadas FDE 271
 - recursos de documentación
 - relacionada xiii
 - sitios web xiv, xvi
 - Storage Manager xiv
 - Sun Solaris 167
 - Sun StorEdge 174
 - Symantec 147, 176
 - uso xvii
 - Veritas 147, 176
 - VMware 323
 - DS TKLM Proxy Code, configuración para gestión externa de claves de seguridad 246
 - DS TKLM Proxy Code, para gestión externa de claves de seguridad 240
 - DS TKLM Proxy Code, reinicio 236
 - DSM 138
 - duplicación de caché 299
 - duplicación de la memoria caché, inhabilitación 186
 - duplicación de memoria caché 330
 - Duplicación global mejorada (Enhanced Global Mirroring)
 - Uso de 102
 - DVE 186
 - Dynamic Multipathing (DMP)
 - Véase también* DMP
 - descripción 167
- ## E
- E/S
 - escritura en memoria caché 113
 - optimización de la tasa de solicitud 112
 - patrón de acceso 112
 - tamaño 112
 - E/S canal de fibra
 - equilibrio de carga 111
 - porcentaje de coincidencia de memoria caché 113
 - E/S multiplexada (MPxIO)
 - Véase* MPxIO
 - Editor de scripts
 - Captura de datos de diagnóstico 293
 - uso 115

- Editor de scripts (*continuación*)
 - ventana 115
- enlaces PV
 - Véase* HP-UX
- entorno de conmutador 136
- entorno heterogéneo 96
- entorno multi-usuario 88
- entornos de conmutador de tejido 136
- equilibrio de carga 340
- errores
 - matriz de discos FCP 296
- errores, exploración de soportes 107
- errores de matriz de discos FCP 296
- escritura en memoria caché
 - habilitación 113
- estaciones de gestión
 - descripción 5
 - tipos compatibles de configuración 3
 - VMware ESX Server 320
- estadísticas, iSCSI 48
- Ethernet
 - requisitos Solaris, servicios de clúster 336
- eventos
 - DDC MEL 295
- eventos, críticos
 - acciones necesarias 273
 - descripciones 273
 - números 273
 - resolución de problemas 273
- Expansión de capacidad dinámica
 - Véase* DCE
- Expansión de unidad lógica dinámica
 - Véase* DVE
- exploración de soportes 105
 - configuración 108
 - duración 109
 - errores indicados 107
 - impacto sobre el rendimiento 106
 - modificación de valores 105
 - visión general 105
- exploración de soportes en segundo plano 105

F

- Fast!UTIL 303
- FDE 102, 215
 - archivos de registro 267
 - autorizaciones de seguridad 231
 - borrado seguro 268
 - borrado seguro, uso 230
 - claves de seguridad
 - creación 219
 - obtención 218, 219
 - uso 219
 - claves de seguridad, cambio (externo) 222
 - claves de seguridad, cambio (local) 222
 - claves de seguridad, creación 219
 - claves de seguridad, obtención 218
 - comprensión 216
 - copia de seguridad y recuperación 271
 - estados, bloqueado y desbloqueado 270

- FDE (*continuación*)
 - gestión de claves de seguridad, FDE 217
 - gestión externa de claves de seguridad 217, 269
 - gestión local de claves de seguridad 217, 269
 - habilitación 242
 - identificador de claves de seguridad 222
 - matrices, seguridad 267
 - matrices RAID, seguridad 250
 - método de gestión de claves, elección 217
 - prácticas recomendadas 271
 - preguntas más frecuentes 267
 - protección de datos contra infracción 216
 - secure drives, unlocking (local) 228
 - soporte de arranque 270
 - terminología 233
 - unidades de disco 216
 - unidades de disco, borrado 263
 - unidades de disco, configuración 242
 - unidades de disco, desbloqueo (local y externo) 256
 - unidades de disco, instalación 242
 - unidades de disco, migración 259
 - unidades de disco de reserva activo 266
 - unidades de repuesto en caliente 270
 - unidades seguras, desbloqueo (externo) 229
 - uso con otras características premium 269
- firmware
 - controlador xv
 - descarga 50, 56
 - descarga con E/S 57
 - niveles, determinación 51, 52
 - obtención xv
 - soportados por Storage Manager 2
 - versiones 2
 - firmware de controlador
 - descarga 50, 53
 - firmware
 - descarga 53
 - firmware de ESM
 - descarga 50, 56
 - descarga de firmware de ESM automática 56
 - niveles, determinación 51, 52
 - sincronización de firmware de ESM automática 56
 - firmware de NVSRAM
 - descarga 50, 53
 - firmware de unidad
 - descarga 57
 - niveles, determinación 51, 52
 - FlashCopy 100
 - Enhanced 99
 - mensajes de error de matriz de discos (AIX) 298
 - funciones premium
 - partición de almacenamiento 65

G

- General Parallel File System (GPFS) 329
- gestión agente de host, configuración 6
- gestión en red, configuración 5
- gestión externa de claves de seguridad 218, 222, 229, 235, 236, 240, 246
 - configuración 246
 - servidor DS TKLM Proxy Code 240, 241
- gestión local de claves de seguridad 219, 222
- glosario 361
- GPFS 329
- grupos de hosts
 - definición 65, 95

H

- HACMP 328
 - uso 329
- hardware
 - dirección Ethernet 6
 - requisitos de VMware ESX Server 320
 - servicio y soporte xviii
- HBA
 - conexión en caliente PCI, sustitución 199
 - conexión en un entorno de conmutador de canal de fibra 136
 - configuración avanzada 305
 - configuración de JNI 311
 - configuración de JNI en Solaris 312
 - controladores de dispositivo 142, 143
 - distribución en zonas de conmutador de canal de fibra 136
 - en Linux, sustitución 196
 - en una configuración de conexión a SAN 7
 - en una configuración de conexión directa 7
 - intercambio en caliente, finalización 200
 - intercambio en caliente, sustitución 192
 - intercambio en caliente, sustitución en AIX 192
 - intercambio en caliente, sustitución en AIX y Linux 194
 - intercambio en caliente en Linux, preparación 196
 - uso 136
 - valores de QLogic 316
 - valores predeterminados 304
 - visión general 136
- HBA conexión en caliente PCI 199
- HBAs
 - QLogic settings 306
 - settings 303
- hdisk
 - atributos 184, 345
 - profundidad de cola, definición 184
- hdisks
 - verificación 181

- Herramienta de actualización del firmware de controlador
 - apertura 55
 - archivo de registro, visualización 56
 - estado de dispositivos, comprobación 54
 - firmware, descarga 55
 - subsistemas de almacenamiento, adición 55
 - uso 55
- herramienta lsslot 197
- herramientas
 - conexión en caliente PCI 196
 - lsslot 197
- herramientas de conexión en caliente PCI 196
- host bus adapters
 - Véase* HBAs
- hosts
 - AIX, dispositivos en 180
 - configuración 119
 - definición 96
 - descubrimiento automático 41
 - descubrimiento manual 42
 - heterogéneos 96
 - IBM i 98, 99
 - iSCSI 49
 - tareas previas a la instalación 6
 - VMware ESX Server 320
- HP-UX
 - E/S multi-ruta con enlaces PV 163, 164
 - enlaces PV 162, 163, 164
 - multi-ruta E/S con enlaces PV 162
 - multi-ruta nativa 167
 - servicios de clúster, requisitos de alta disponibilidad 335
 - unidades lógicas, redistribución 190

I

- IBM i
 - configuración 98
 - definición como tipo de host 99
 - identificador de puerto 98
- IBM Power systems 98
- IBM System Storage Controller Firmware Upgrade Tool
 - Véase* Controller Firmware Upgrade Tool
- IBM System Storage Productivity Center xv
- IBM Tivoli Key Lifecycle Manager 217, 246
 - archivo de configuración de servidor de código proxy de DS TKLM, modificación 236
 - DS TKLM Proxy Code, configuración 246
 - DS TKLM Proxy Code, instalación 240
 - para gestión externa de claves de seguridad, configuración 235
- identificación de destino, cambio para iSCSI 47
- identificador de habilitación de característica 60

- información de ranuras PCI 197
- iniciadores de hardware, iSCSI 48
- instalación 240
 - configuración de redes 3
 - configuración de VMware ESX Server 319
 - controladores multi-ruta 138
 - DS TKLM Proxy Code en Windows, para gestión externa de claves de seguridad 240
 - procedimientos de finalización 40
 - proxy en AIX o Linux, gestión externa de claves de seguridad 241
 - secuencia 38
 - Storage Manager 33
 - Storage Manager, automáticamente 34
 - Storage Manager, manual 38, 39
 - Support Monitor 33
 - tipos de configuración 3
 - unidades FDE 242
 - ventana de consola 37
- instalación de red, preparación 3
- instalar
 - prepararse para 1
- intercambio de cabezal, subsistemas de almacenamiento FDE 259
- intercambio de HBA en caliente
 - Véase* HBA, intercambio en caliente
- interfaz de línea de mandatos (CLI) 115
- interrupciones SNMP 44
- introducción
 - Storage Manager 1
- IPv6 49
- iSCSI
 - autenticación de destino, cambio 47
 - configuración, gestión 46
 - consideraciones software initiator, Microsoft 50
 - descubrimiento de destino, cambio 47
 - estadísticas, visualización 48
 - identificación de destino, cambio 47
 - iniciadores de hardware soportados, uso 48
 - permisos de autenticación mutua, especificación 47
 - puertos de host 46
 - puertos de host, configuración 47
 - servidor iSNS, uso 48
 - sesión, visualización o finalización 48
 - valores de red 49

J

- JNI
 - configuración de HBA en Solaris 312
 - configuración HBA 311

L

- léame
 - obtención de archivos xv
- lectura anticipada de memoria caché, elección de un multiplicador 112

- Línea de soporte de IBM xviii
- Linux
 - correlación del nuevo WWPN con subsistemas de almacenamiento 200
 - DCE 186
 - DVE 186
 - HBA, preparación para intercambio en caliente 196
 - intercambio en caliente de HBA, sustitución 194
 - intercambio en caliente HBA, finalización 200
 - RHEL 5.3, con Veritas Storage Foundation 5.0 188
 - SUSE, con Veritas Storage Foundation 187
 - sustitución de HBA 196
- local security key management 228
- LockKeyID, FDE 222
- LUN
 - adición a una partición existente 97
 - atributos 184, 345
 - comprobación el tamaño 189
 - correlación con una nueva partición 97
 - correlación con una partición en VMware ESX Server 324

M

- MAC OS 162
- management stations
 - description 1
- marcas registradas 357
- matrices 86
 - creación 78
 - definición 78
- MC/Service Guard 335
- mecanismo de transporte universal
 - Véase* dispositivo UTM
- MEL
 - cambios en la seguridad 267
- Memoria caché de lectura de rendimiento
 - Uso de 102
- memoria caché del controlador 103
- método de gestión host-agente
 - dispositivo UTM 180
- Mi soporte xix
- Microsoft iSCSI Software Initiator 50
- Microsoft Windows MPIO 138
- Microsoft Windows MPIO/DSM 138
- Minihubs 7
- minipuerto SCSIport 143, 147
- Modalidades de migración tras error
 - Acceso asimétrico a unidad lógica 121
 - Migración tras error de RDAC 121
 - Transferencia automática de volúmenes 121
- modificación del archivo de configuración de proxy para la gestión externa de claves de seguridad 236
- Módulo específico de dispositivos
 - Véase* DSM
- MPIO 182
- MPxIO 167

MPxIO (*continuación*)
controlador, inhabilitación 174
controlador de migración tras error,
habilitación 169
dispositivos, verificación 169
nombres de dispositivo, cambio 168
ruta de migración tras error,
configuración 169
ruta de migración tras error,
desconfiguración 169
última versión del controlador,
adquisición 168

MTU
configuración 50
multi-ruta 50, 138, 167
controlador de migración tras error
RDAC en Solaris 174
DMP, instalación en Solaris 176
enlaces PV, uso en HP-UX 162, 163,
164
MPxIO, uso con Solaris 167
nativa, en HP-UX 167
redistribución de unidades lógicas en
AIX 190
redistribución de unidades lógicas en
HP-UX 190
redistribución de unidades lógicas en
Solaris 191

Multiproceso de clúster de alta
disponibilidad
Véase HACMP

N

Nivel RAID
comportamiento de las
aplicaciones 88
configuraciones 87
elección 88
nombre de puerto de ámbito mundial
Véase WWPN
nombres, subsistema de
almacenamiento 43
notas, importantes 358
notificaciones
a buscapersonas alfanuméricos 44
a correo electrónico 44
uso de interrupciones SNMP 44
notificaciones de alerta,
configuración 44
notificaciones de soporte xix
recepción xix
núcleo PCI 196

O

Opción Duplicación remota 101
otras preguntas más frecuentes 271

P

paquetes, software Storage Manager 2,
38
Parallel System Support Programs
(PSSP) 329
paridad 86

partición 65
partición de almacenamiento 58, 96
y grupos de host 65
patrón de acceso de E/S y tamaño de
E/S 112
perfil, subsistema de almacenamiento 63
permisos de autenticación mutua,
especificación para iSCSI 47
pestaña Almacenamiento y servicios de
copia
Véase ventana Gestión del subsistema
pestaña Configuración
ventana Gestión del subsistema 30
ventana Gestión empresarial 22
pestaña Correlaciones de host
Véase ventana Gestión del subsistema
pestaña Dispositivos
Véase ventana Gestión empresarial
pestaña hardware
Véase ventana Gestión del subsistema
pestaña Resumen
Véase ventana Gestión del subsistema
política de menor peso de ruta 110
política de menor profundidad de
cola 110
política round robin 110
políticas, equilibrio de carga
política de menor peso de ruta 110
política de menor profundidad de
cola 110
política round robin 110
Preguntas más frecuentes, otras 271
problemas, resolución 273
productos, desarrollados 355
profundidad de cola
cambio para AIX 185
cambio para Windows 185
máxima, calculo 184
profundidad de cola, definición 184
programa de utilidad hot_add 182
programa de utilidad SMdevices
en sistemas operativos de tipo
Unix 179
en Windows 179
uso 179
programa de utilidad SMrepassist 183
programas de utilidad
hot_add 182
SMdevices 179
SMrepassist 183
progreso de operaciones
visualización 91
Proveedor VDS/VSS 347
proxy, desinstalación en Windows 241
proxy, instalación en AIX o Linux 241
proxy, instalación en Windows 240
PSSP 329
puertos de host
definición 96
puertos de host, iSCSI 47
puertos host
definición 96

Q

QLogic
configuración 317

QLogic (*continuación*)
configuración HBA 311, 316
HBA settings 303, 306
QLogic SANsurfer xiv

R

red de área de almacenamiento(SAN)
configuración 7
RAID
comportamiento de la aplicación, por
nivel 113
elección de niveles 113
niveles 86
redundancia de datos 86
seguridad de matrices con FDE 250
RAID-0
consecuencias de error de unidad 87
descripción 87
RAID-1
consecuencias de error de unidad 87
descripción 87
RAID-3
consecuencias de error de unidad 87
descripción 87
RAID-5
consecuencias de error de unidad 88
descripción 88
RAID-6
paridad dual distribuida 88
RDAC
identificadores, servicios de
clúster 336
IDs, adición 336
Recovery Guru
Captura de datos de diagnóstico 293
recuperación automática
verificación de estado inhabilitado
antes de intercambio en caliente de
HBA en AIX 192
redes
configuración general 3
configuración iSCSI 49
ejemplo de configuración 4
rendimiento
definición de atributos de ODM
y 184
requisitos
HP-UX
servicios de clúster, alta
disponibilidad 335
sistema operativo 34
software cliente Storage Manager 39
requisitos previos
HP-UX
servicios de clúster, alta
disponibilidad 335
requisitos previos, software cliente
Storage Manager 39
reservas persistentes 104
resolución de problemas 273
Captura de datos de diagnóstico 293
eventos críticos 273
resolución de problemas, eventos
críticos 273

S

- servicio
 - solicitud xvii
- servicios de clúster
 - HACMP ES y ESCRM 328
 - Requisitos de AIX 329
- servicios de clúster, alta disponibilidad
 - AIX 327
 - Dependencias del sistema 327
 - MC/Service Guard 335
 - PSSP con GPFS 329
 - requisitos de AIX 328
 - requisitos de HP-UX 335
 - requisitos de Solaris 336
 - Requisitos de Solaris 336
 - Solaris 336
- servicios de copia 58
- servicios ofrecidos en EE.UU. 355
- Servidor DHCP/BOOTP 9
- servidor DS TKLM Proxy Code, sistemas operativos compatibles 235
- servidor iSNS, uso 48
- sesión, iSCSI 48
- settings
 - HBA 303
- sincronización de firmware de ESM automática
 - definido 56
 - Requisito del supervisor de sucesos 56
- sistema operativo
 - requisitos 34
- sistemas operativos
 - arrancar con arranque SAN 119
 - DS TKLM Proxy Code 235
 - Solaris 169
 - soportados con Storage Manager 1
- sitios web
 - controlador de migración tras error
 - Solaris 176
 - documentación xiv
 - lista xvi
 - notificación xix
 - prácticas recomendadas FDE 271
 - servicios xviii
 - soporte xviii, xix
 - VMware 323
- SMagent
 - secuencia de instalación del software 38
- SMclient
 - secuencia de instalación del software 38
- SMruntime
 - secuencia de instalación del software 38
- SMutil
 - secuencia de instalación del software 38
- software
 - componentes Storage Manager 2, 38
 - configuración de direcciones de controlador 8
 - controladores multi-ruta 133
 - gestión de licencias de claves 217
 - paquete RDAC 167

- software (*continuación*)
 - requisitos de VMware ESX Server 320
 - servicio y soporte xviii
- software agente de host
 - detención y reinicio 183
- Solaris
 - requisitos de servicios de clúster 336
 - servicios de clúster, alta disponibilidad 336
 - unidades lógicas, redistribución 191
 - Veritas 176
- soporte
 - controlador multi-ruta 133
 - notificaciones xix
 - obtención xvii, xviii
 - sitios web xvi, xix
- soporte de anomalías
 - controlador DMP 167
 - controlador RDAC 167
 - MPxIO 167
 - redistribución de unidades lógicas 190, 191
 - servicios de clúster 327
- SSPC (System Storage Productivity Center) xv
- Storage Manager 103, 104, 105
 - accesibilidad 351
 - asistente de instalación 34
 - Asistente de tareas 66
 - características premium 58, 99
 - componentes de software 2, 38
 - configuración de direcciones de controlador 8
 - Controller Firmware Upgrade Tool
 - uso de la herramienta 54
 - descarga de firmware de unidad
 - versión 10.5x 57
 - description 1
 - desinstalación 40
 - desinstalación en Linux, AIX o Solaris 40
 - desinstalación en Windows 40
 - editor de scripts 115
 - elementos de la interfaz 15
 - elementos de la interfaz, Storage Manager 15
 - instalación 40
 - instalación manual 38, 39
 - instalación para uso con IBM System Storage Productivity Center xv
 - interfaz de línea de comandos 115
 - obtención de software xv
 - otras características 103
 - problemas, resolución 273
 - registro de eventos 273
 - resolución de problemas 273
 - secuencia de instalación 38
 - sistemas operativos soportados 1
 - Ventana Gestión del subsistema 22
 - ventana Gestión empresarial 15
 - versiones 2
- storage subsystems
 - introduction 1
- Storport Miniport 142
- subsistema de almacenamiento
 - adición 183

- subsistema de almacenamiento (*continuación*)
 - configuración de VMware ESX Server 319
 - niveles de firmware, determinación 51, 52
 - perfil, guardar 63
- subsistema de almacenamiento, gestión externa de claves de seguridad 246
- subsistemas de almacenamiento
 - ajustar 110, 111, 112, 113, 114
 - ajuste 109
 - ajuste de opciones disponibles 109
 - configuración para gestión externa de claves de seguridad 246
 - correlación del nuevo WWPN en AIX y Linux 200
 - definición de contraseñas 43
 - denominación 43
 - descubrimiento automático inicial 41
 - descubrimiento manual 42
 - direcciones IP 8
 - direcciones TCP/IP estáticas 11
 - para gestión externa de claves de seguridad, configuración 235
 - servicios de clúster 327
- Supervisor de rendimiento 109
- System Storage Productivity Center xv

T

- tasa de solicitud de E/S
 - optimización 112
- tasa de transferencia de E/S, optimización 112
- TCP/IP
 - IPv6 49
- terminología, FDE 233
- tipos de configuración
 - instalación de Storage Manager 3
- tipos de host
 - definición de valores predeterminados 94
 - verificación 94
- tipos de host predeterminados, definición y verificación 94
- Tivoli Key Lifecycle Manager
 - Véase IBM Tivoli Key Lifecycle Manager
- TKLM
 - Véase IBM Tivoli Key Lifecycle Manager

U

- Unidad de transmisión máxima
 - Véase MTU
- unidades
 - Véase unidades de disco
- unidades de disco
 - FDE 216
 - FDE, borrado 263
 - FDE, borrado seguro 230
 - FDE, configuración 242
 - FDE, desbloqueo (externo) 229

- unidades de disco (*continuación*)
 - FDE, desbloqueo (local y externo) 256
 - FDE, instalación 242
 - FDE, migración 259
 - repuesto en caliente, asignación 92
 - repuesto en caliente, configuración 92
 - repuesto en caliente, restauración de datos 92
 - reserva FDE 266
- unidades de repuesto en caliente 92
- unidades lógicas 7, 342
 - configuración 89
 - creación 78, 89, 90
 - creación a partir de capacidad libre o no configurada 85
 - definición 78
 - identificación 179
 - redistribución 189, 190, 191
 - uso esperado 90
 - valor de prioridad de modificación 114
- Veritas Storage Foundation 5.0 (*continuación*)
 - módulo RDAC, habilitación 188
- versiones de software, múltiples
 - Véase* ventana Gestión del subsistema
- VMware ESX Server 319
 - conexiones cruzadas 323
 - correlación de LUN con una partición 324
- VolumeCopy 101
- volúmenes de acceso 7, 342

W

- WWPN
 - correlación con el subsistema de almacenamiento en AIX y Linux 200

V

- velocidad de transferencia 109
- ventana
 - Editor de scripts 115
- ventana Gestión del subsistema
 - apertura 23
 - ayuda en línea xiv
 - elementos 23
 - múltiples versiones de software 30
 - pestaña Almacenamiento y servicios de copia 24
 - pestaña Configuración 30
 - pestaña Correlaciones de host 28
 - pestaña hardware 29
 - pestaña Resumen 24
 - registro de eventos 273
- Ventana Gestión del subsistema
 - elementos 22
- ventana Gestión empresarial
 - adición de dispositivos 42
 - ayuda en línea xiv
 - descripción de vista de árbol 18
 - descripción de vista de tabla 18
 - elementos 15
 - notificaciones de alerta 44
 - pestaña Configuración 22
 - pestaña Dispositivos 18
- Veritas 147
 - DMP 176
 - Dynamic Multipathing (DMP) 167
 - Sistemas de archivos 176
 - Storage Foundation 187
 - Storage Foundation 5.0 188
 - VolumeManager 167, 176
- Veritas DMP DSM 147
- Veritas Storage Foundation
 - exploración LVM, inhabilitación para SUSE Linux Enterprise Server 187
 - módulo RDAC, habilitación en RHEL para Storage Foundation 5.0 188
- Veritas Storage Foundation 5.0
 - módulo RDAC, descarga 188



Número Pieza: 00Y8830

Impreso en España

GA10-5522-04



(1P) P/N: 00Y8830

