

Almacenamiento de vSphere

Actualización 1

Modificado el 19 de abril de 2022

VMware vSphere 6.0

VMware ESXi 6.0

vCenter Server 6.0

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

<https://docs.vmware.com/es/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Copyright © 2009-2022 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Acerca del almacenamiento de vSphere 13

Información actualizada 14

1 Introducción al almacenamiento 15

Virtualización de almacenamiento 15

Tipos de almacenamiento físico 16

Almacenamiento local 16

Almacenamiento en red 17

Representar dispositivos y destinos 21

Características de los dispositivos de almacenamiento 22

Mostrar dispositivos de almacenamiento de un host 23

Mostrar dispositivos de almacenamiento para un adaptador 24

Adaptadores de almacenamiento compatibles 24

Características del adaptador de almacenamiento 25

Ver información sobre adaptadores de almacenamiento 25

Características de los almacenes de datos 26

Mostrar la información del almacén de datos 28

Listado de almacenes de datos para un objeto de infraestructura 29

Acceden al almacenamiento las máquinas virtuales 30

Comparar tipos de almacenamiento 31

2 Descripción general de la utilización de ESXi con una SAN 33

Casos de uso de ESXi y SAN 34

Detalles de la utilización de almacenamiento SAN con ESXi 35

Hosts ESXi y varias matrices de almacenamiento 35

Toma de decisiones relacionadas con el LUN 36

Usar el esquema predictivo para tomar decisiones sobre LUN 36

Usar el esquema adaptativo para tomar decisiones de LUN 37

Seleccionar la ubicación de las máquinas virtuales 37

Aplicaciones en capas 38

Solución (de terceros) basada en matrices 39

Solución basada en archivos (VMFS) 39

Aplicaciones de administración de terceros 39

Consideraciones sobre copias de seguridad de almacenamiento SAN 40

Usar paquetes de copia de seguridad de terceros 41

3 Usar ESXi con SAN de canal de fibra 42

Conceptos de SAN de canal de fibra	42
Puertos en SAN de canal de fibra	43
Tipos de matrices de almacenamiento de canal de fibra	43
Usar la división en zonas con las SAN de canal de fibra	44
Cómo acceden las máquinas virtuales a los datos en una SAN de canal de fibra	45

4 Configurar almacenamiento de canal de fibra 46

ESXi	46
Restricciones de SAN de canal de fibra de ESXi	47
Establecer asignaciones de LUN	47
Establecer los HBA de canal de fibra	48
Pasos de instalación y configuración	48
Virtualizar identificador de puerto N	49
Funcionamiento del acceso al LUN basado en NPIV	49
Requisitos para utilizar NPIV	49
Funcionalidades y limitaciones de NPIV	50
Asignar WWN a máquinas virtuales	51
Modificar asignaciones de WWN	51

5 Configurar el canal de fibra en Ethernet 53

Adaptadores de canal de fibra en Ethernet	53
Instrucciones de configuración para FCoE de software	54
Configurar redes para FCoE de software	55
Agregar adaptadores de FCoE de software	56

6 Arrancar ESXi desde una SAN de canal de fibra 57

Beneficios del arranque desde SAN	57
Requisitos y consideraciones sobre el arranque desde SAN de canal de fibra	58
Prepararse para el arranque desde SAN	58
Configurar los componentes de la SAN y del sistema de almacenamiento	59
Configurar adaptador de almacenamiento para arrancar desde SAN	60
Configurar sistema para arrancar desde los medios de instalación	60
Configurar HBA de Emulex para arrancar desde SAN	61
Habilitar el símbolo de BootBIOS	61
Habilitar el BIOS	61
Configurar HBA de QLogic para arrancar desde SAN	62

7 Arrancar ESXi con FCoE de software 64

Requisitos y consideraciones sobre el arranque de FCoE de software	64
Prácticas recomendadas para el arranque de FCoE de software	65
Configurar arranque de FCoE de software	65

- Configurar parámetros de arranque de FCoE de software 66
- Instalación y arranque de ESXi desde LUN FCoE de software 66
- Solucionar problemas de instalación y arranque desde FCoE de software 67

8 Prácticas recomendadas para el almacenamiento de canal de fibra 69

- Evitar problemas de SAN de canal de fibra 69
- Deshabilitar el registro automático de hosts 70
- Optimizar el rendimiento del almacenamiento de SAN de canal de fibra 71
 - Rendimiento de matrices de almacenamiento 71
 - Rendimiento de servidores con canal de fibra 71

9 Usar ESXi con una SAN iSCSI 73

- Conceptos de SAN iSCSI 73
 - Puertos en la SAN iSCSI 74
 - Convenciones de nomenclatura de iSCSI 74
 - Iniciadores iSCSI 75
 - Establecer conexiones iSCSI 76
 - Tipos de sistema de almacenamiento iSCSI 77
 - Detectar, autenticar y controlar el acceso 78
 - Corregir errores 79
- Cómo acceden las máquinas virtuales a los datos en una SAN iSCSI 80

10 Configurar adaptadores y almacenamiento iSCSI 81

- Requisitos de SAN iSCSI de ESXi 82
- Restricciones de SAN iSCSI ESXi 82
- Establecer asignaciones de LUN para iSCSI 83
- Configurar y autenticar red 83
- Configurar adaptadores de iSCSI de hardware independientes 84
 - Ver adaptadores de iSCSI de hardware independientes 85
 - Modificar propiedades generales de los adaptadores de iSCSI 85
 - Editar la configuración de red para iSCSI de hardware 86
 - Configurar la detección dinámica o estática de iSCSI 87
- Acerca de los adaptadores de iSCSI de hardware dependiente 88
 - Consideraciones sobre iSCSI de hardware dependiente 89
 - Configurar los adaptadores de iSCSI de hardware dependiente 89
- Acerca del adaptador de iSCSI de software 97
 - Configurar adaptador de iSCSI de software 98
 - Deshabilitar el adaptador de iSCSI de software 105
- Modificar propiedades generales de los adaptadores de iSCSI 106
- Configurar la red de iSCSI 107
 - Instrucciones de utilización de enlace de puertos iSCSI en ESXi 110

Crear conexiones de red para iSCSI	110
Administrar una red iSCSI	115
Solucionar problemas de red de iSCSI	116
Usar tramas gigantes con iSCSI	116
Habilitar tramas gigantes para iSCSI de hardware dependiente y de software	117
Habilitar tramas gigantes para iSCSI de hardware independiente	118
Configurar direcciones de detección para adaptadores de iSCSI	118
Configurar la detección dinámica o estática de iSCSI	119
Quitar destinos iSCSI dinámicos o estáticos	119
Configurar parámetros CHAP para adaptadores de iSCSI	120
Seleccionar el método de autenticación de CHAP	120
Configurar CHAP para un adaptador de iSCSI	122
Configurar CHAP para un destino	123
Deshabilitar CHAP	124
Configurar los parámetros avanzados de iSCSI	125
Configurar los parámetros avanzados de iSCSI	126
Administrar sesiones de iSCSI	127
Revisar las sesiones iSCSI	128
Agregar sesiones iSCSI	128
Quitar sesiones iSCSI	129

11 Arrancar desde SAN iSCSI 131

Recomendaciones generales de arranque desde SAN iSCSI	131
Preparar SAN iSCSI	132
Configurar adaptador de iSCSI de hardware independiente para el arranque de SAN	133
Configurar las opciones de arranque de iSCSI	134
Descripción general del arranque de iBFT de iSCSI	135
Consideraciones sobre el arranque de iBFT de iSCSI	136
Configurar arranque de iBFT desde SAN	136
Prácticas recomendadas para redes	139
Cambiar la configuración de arranque de iSCSI iBFT	140
Solucionar problemas de arranque de iSCSI de iBFT	140

12 Prácticas recomendadas de almacenamiento iSCSI 142

Evitar problemas en una SAN iSCSI	142
Optimización del rendimiento del almacenamiento SAN iSCSI	143
Rendimiento del sistema de almacenamiento	143
Rendimiento del servidor con iSCSI	144
Rendimiento de la red	145
Comprobar estadísticas del conmutador Ethernet	148

13 Administrar dispositivos de almacenamiento 149

- Características de los dispositivos de almacenamiento 149
 - Mostrar dispositivos de almacenamiento de un host 150
 - Mostrar dispositivos de almacenamiento para un adaptador 151
- Descripción de la nomenclatura de dispositivos de almacenamiento 151
 - Cambiar nombre de los dispositivos de almacenamiento 153
- Operaciones para actualizar y volver a examinar el almacenamiento 153
 - Realizar la operación para volver a examinar el almacenamiento 154
 - Realizar la operación para volver a examinar el adaptador 155
 - Cambiar la cantidad de dispositivos de almacenamiento examinados 155
- Identificar problemas de conectividad del dispositivo 156
 - Detectar condiciones de PDL 156
 - Eliminar dispositivo de almacenamiento planificada 158
 - Recuperar condiciones de PDL 159
 - Manejar condiciones de APD transitorias 160
 - Comprobar el estado de conexión de un dispositivo de almacenamiento 162
 - Alta disponibilidad y problemas de conectividad del dispositivo 163
- Habilitar o deshabilitar el LED localizador en dispositivos de almacenamiento 163

14 Trabajar con dispositivos flash 165

- Usar dispositivos flash con vSphere 165
 - Identificar discos virtuales flash 166
- Marcado de dispositivos de almacenamiento 167
 - Marcar dispositivos de almacenamiento como flash 167
 - Marcar dispositivos de almacenamiento como locales 168
- Supervisar dispositivos flash 168
- Prácticas recomendadas para dispositivos flash 169
 - Vida útil estimada para dispositivos flash 169
- Acerca del recurso flash virtual 170
 - Consideraciones sobre el recurso flash virtual 171
 - Configurar un recurso flash virtual 171
 - Quitar el recurso flash virtual 172
 - Configuración avanzada de flash virtual 172
- Configurar la memoria caché de intercambio del host 173
 - Configurar la memoria caché del host con un almacén de datos de VMFS 173
 - Configurar la memoria caché de intercambio del host con un recurso flash virtual 174

15 Acerca de VMware vSphere Flash Read Cache 176

- Compatibilidad con DRS para Flash Read Cache 177
- Compatibilidad de vSphere High Availability con Flash Read Cache 177
- Configurar Flash Read Cache para una máquina virtual 177

Migrar máquinas virtuales con Flash Read Cache 179

16 Trabajar con almacenes de datos 181

Descripción de los almacenes de datos de VMFS 182

Características de los almacenes de datos VMFS5 183

Almacenes de datos de VMFS y formatos de disco de almacenamiento 184

Almacenes de datos de VMFS como repositorios 184

Compartir un almacén de datos de VMFS entre hosts 185

Actualizaciones de metadatos de VMFS 186

Mecanismos de bloqueo de VMFS 187

Descripción de los almacenes de datos de Network File System 191

Instrucciones y requisitos de almacenamiento NFS 192

Protocolos NFS y ESXi 194

Configuraciones de firewall para almacenamiento NFS 196

Usar las conexiones enrutadas de Capa 3 para acceder al almacenamiento NFS 198

Configurar entorno de almacenamiento NFS 198

Usar credenciales Kerberos para NFS 4.1 199

Crear almacenes de datos 202

Crear un almacén de datos de VMFS 203

Crear un almacén de datos de NFS 204

Crear un almacén de datos virtual 205

Administrar almacenes de datos de VMFS duplicados 206

Conservar la firma de almacén de datos existente 206

Volver a firmar una copia de un almacén de datos de VMFS 207

Actualizar los almacenes de datos de VMFS 208

Actualizar un almacén de datos a VMFS5 209

Aumentar la capacidad de un almacén de datos de VMFS 210

Aumentar la capacidad de un almacén de datos de VMFS 210

Operaciones administrativas para almacenes de datos 212

Cambiar nombre del almacén de datos 213

Desmontar almacenes de datos 213

Montar almacenes de datos 214

Quitar almacenes de datos de VMFS 215

Usar el explorador del almacén de datos 215

Desactivar los filtros de almacenamiento 220

Configurar reflejo de discos dinámico 222

Recopilar información de diagnóstico para hosts ESXi en un dispositivo de almacenamiento 223

Configurar una partición de dispositivo como ubicación de volcado de núcleo 224

Configurar un archivo como ubicación de volcado de núcleo 225

Comprobar la coherencia de los metadatos con VOMA 227

Configurar la memoria caché de bloque de puntero de VMFS 230

- Establecer atributos de host avanzados 231
- Obtener información para la memoria caché de bloque del puntero de VMFS 231

17 Descripción de múltiples rutas y conmutación por error 233

- Conmutación por error con canal de fibra 234
- Conmutación por error basada en host con iSCSI 234
- Conmutación por error basada en matrices con iSCSI 236
- Conmutación por error de rutas de acceso y máquinas virtuales 237
 - Establecer el tiempo de espera en un sistema operativo invitado Windows 238
- Administrar varias rutas de acceso 238
- Módulo de múltiples rutas de VMware 240
 - SATP de VMware 241
 - PSP de VMware 241
 - Flujo NMP de E/S de VMware 242
- Explorar y notificar rutas de acceso 243
 - Ver información de rutas de acceso 244
 - Ver las rutas de acceso de los almacenes de datos 244
 - Ver rutas de acceso de dispositivos de almacenamiento 245
 - Establecer una directiva de selección de rutas de acceso 245
 - Cambiar la directiva de selección de rutas de acceso 246
 - Deshabilitar rutas de acceso de almacenamiento 247
- Administrar rutas de acceso de almacenamiento y complementos de múltiples rutas 247
 - Consideraciones sobre múltiples rutas 248
 - Lista de reglas de notificación de múltiples rutas para el host 248
 - Mostrar módulos de múltiples rutas 250
 - Mostrar SATP para el host 250
 - Mostrar dispositivos de almacenamiento NMP 251
 - Agregar reglas de notificación de múltiples rutas 252
 - Eliminar reglas de notificación de múltiples rutas 254
 - Enmascarar rutas de acceso 255
 - Desenmascarar rutas de acceso 256
 - Definir reglas de SATP de NMP 257
- Colas de programación de E/S de máquinas virtuales 259
 - Editar programación de E/S por archivo 259
 - Utilizar comandos esxcli para habilitar o deshabilitar la programación de E/S por archivo 260

18 Asignación de dispositivos sin formato 262

- Acerca de la asignación de dispositivos sin formato 262
 - Beneficios de la asignación de dispositivos sin formato 264
 - Consideraciones y limitaciones de RDM 266
- Características de la asignación de dispositivos sin formato 266

Modos de compatibilidad virtual y física de RDM	267
Resolución de nombres dinámica	267
Asignación de dispositivos sin formato con clústeres de máquinas virtuales	267
Comparar modos de acceso de dispositivos SCSI disponibles	268
Crear máquinas virtuales con RDM	269
Administrar rutas de acceso para un LUN asignado	270

19 Trabajar con Virtual Volumes 272

Conceptos de Virtual Volumes	273
Virtual Volumes	274
Virtual Volumes y proveedores de almacenamiento	275
Contenedores de almacenamiento	276
Extremos de protocolo	276
Almacenes de datos virtuales	277
Virtual Volumes y directivas de almacenamiento de máquina virtual	278
Instrucciones sobre el uso de Virtual Volumes	278
Virtual Volumes y protocolos de almacenamiento	279
Arquitectura de Virtual Volumes	280
Virtual Volumes y VMware Certificate Authority	281
Antes de habilitar Virtual Volumes	282
Sincronizar el entorno de almacenamiento de vSphere con un servidor horario de red	283
Configurar Virtual Volumes	283
Registrar proveedores de almacenamiento de Virtual Volumes	284
Crear un almacén de datos virtual	285
Revisar y administrar extremos de protocolo	286
Cambiar la directiva de selección de rutas de acceso para un extremo de protocolo	287
Aprovisionar máquinas virtuales en almacenes de datos virtuales	288
Definir una directiva de almacenamiento de máquina virtual para Virtual Volumes	288
Asignar la directiva de almacenamiento de Virtual Volumes a máquinas virtuales	289
Cambiar la directiva de almacenamiento predeterminada de un almacén de datos virtual	290

20 Directivas de almacenamiento de máquinas virtuales 292

Actualizar perfiles de almacenamiento heredados	292
Descripción de las directivas de almacenamiento de máquinas virtuales	293
Directivas y reglas de almacenamiento	294
Acerca de los conjuntos de reglas específicos y comunes de los almacenes de datos	296
Trabajar con directivas de almacenamiento de máquinas virtuales	297
Crear y administrar directivas de almacenamiento de máquina virtual	298
Asignar etiquetas a almacenes de datos	298
Definir una directiva de almacenamiento para una máquina virtual	299
Eliminar una directiva de almacenamiento de una máquina virtual	303

Editar o clonar una directiva de almacenamiento de máquina virtual	304
Directivas de almacenamiento y máquinas virtuales	304
Directivas de almacenamiento predeterminadas	305
Asignar directivas de almacenamiento a máquinas virtuales	307
Cambiar la asignación de directivas de almacenamiento para archivos y discos de máquinas virtuales	308
Supervisar cumplimiento del almacenamiento en máquinas virtuales	309
Comprobar el cumplimiento de una directiva de almacenamiento de máquina virtual	310
Encontrar un recurso de almacenamiento compatible para máquinas virtuales no compatibles	311
Volver a aplicar una directiva de almacenamiento de máquinas virtuales	312
21 Filtrar E/S de máquinas virtuales	314
Acerca de los filtros de E/S	314
Tipos de filtros de E/S	315
Componentes de los filtros de E/S	315
Proveedores de almacenamiento para filtros VAIO	317
Utilizar dispositivos de almacenamiento flash con filtros de E/S de memoria caché	317
Implementar y configurar filtros de E/S en el entorno de vSphere	318
Instalar filtros de E/S en un clúster	319
Ver proveedores de almacenamiento para filtros de E/S	320
Revisar las capacidades de los filtros de E/S	320
Configurar el recurso flash virtual para almacenar en caché los filtros de E/S	321
Habilitar servicios de datos de filtros de E/S en discos virtuales	321
Administrar filtros de E/S	325
Desinstalar filtros de E/S de un clúster	325
Actualizar filtros de E/S en un clúster	326
Directrices y prácticas recomendadas para los filtros de E/S	326
Migrar máquinas virtuales con filtros de E/S	327
22 VMkernel y almacenamiento	329
Storage APIs	330
23 Aceleración de hardware de almacenamiento	332
Beneficios de la aceleración de hardware	332
Requisitos de aceleración de hardware	333
Estado de compatibilidad con la aceleración de hardware	333
Aceleración de hardware para dispositivos de almacenamiento en bloque	333
Deshabilitar la aceleración de hardware para dispositivos de almacenamiento en bloque	334
Administrar aceleración de hardware en dispositivos de almacenamiento en bloque	335
Aceleración de hardware en dispositivos NAS	340
Instalar el complemento de NAS	341

- Desinstalar los complementos de NAS 342
- Actualizar los complementos de NAS 342
- Comprobar el estado de aceleración de hardware para NAS 343
- Consideraciones sobre la aceleración de hardware 343

24 Aprovisionamiento fino y grueso de almacenamiento 345

- Sobresuscripción del almacenamiento 345
- Aprovisionamiento fino de discos virtuales 345
 - Acerca de las directivas de aprovisionamiento de discos virtuales 346
 - Crear discos virtuales con aprovisionamiento fino 347
 - Ver los recursos de almacenamiento de una máquina virtual 348
 - Determinar el formato de disco de una máquina virtual 349
 - Expandir discos virtuales finos 349
 - Manejar la sobresuscripción del almacén de datos 350
- Aprovisionamiento fino de matrices y almacenes de datos de VMFS 350
 - Supervisar la utilización del espacio 351
 - Identificar dispositivos de almacenamiento de aprovisionamiento fino 352
 - Recuperar espacio de almacenamiento acumulado 353

25 Usar proveedores de almacenamiento 355

- Proveedores de almacenamiento y representación de datos de almacenamiento 356
- Consideraciones y requisitos del proveedor de almacenamiento 356
- Informe de estado de almacenamiento 357
- Registrar proveedores de almacenamiento 358
- Proteger la comunicación con proveedores de almacenamiento 359
- Ver información sobre el proveedor de almacenamiento 359
- Cancelar el registro de proveedores de almacenamiento 360
- Actualizar proveedores de almacenamiento 360

26 Usar vmkfstools 362

- Sintaxis del comando vmkfstools 362
- Opciones de vmkfstools 363
 - Subopción -v 364
 - Opciones del sistema de archivos 364
 - Opciones de discos virtuales 367
 - Opciones de dispositivos de almacenamiento 374

Acerca del almacenamiento de vSphere

El almacenamiento de *vSphere* describe las opciones de almacenamiento disponibles para VMware[®] ESXi y explica cómo configurar el sistema ESXi para que pueda utilizar y administrar diferentes tipos de almacenamiento. Además, el almacenamiento de *vSphere* se concentra explícitamente en redes de área de almacenamiento (SAN) de canal de fibra[®] e iSCSI como opciones de almacenamiento y analiza los aspectos específicos de usar ESXi en entornos de canal de fibra e iSCSI.

Audiencia prevista

Esta información está dirigida a administradores de sistemas con experiencia y familiarizados con la tecnología de máquinas virtuales, las operaciones de centros de datos y los conceptos de almacenamiento SAN.

Información actualizada

Esta documentación sobre *Almacenamiento de vSphere* se actualiza con cada versión del producto o cuando sea necesario.

En esta tabla se muestra el historial de actualizaciones de *Almacenamiento de vSphere*.

Revisión	Descripción
19 de abril de 2022	Revisiones menores.
15 de agosto de 2020	En VMware, valoramos la inclusión. Para fomentar este principio entre nuestros clientes, nuestros partners y nuestra comunidad interna, estamos reemplazando parte de la terminología en nuestro contenido. Hemos actualizado esta guía para eliminar el lenguaje no inclusivo.
27 de junio de 2019	Revisiones menores.
27 de noviembre 2018	Revisiones menores.
12 de julio de 2018	Revisiones menores.
18 de abril de 2018	Revisiones menores.
20 de marzo de 2018	Revisiones menores.
14 de febrero de 2018	Revisiones menores.
ES-001799-07	Copiar archivos o carpetas de almacenes de datos ahora incluye una instrucción que indica que el explorador de almacenes de datos no admite la copia de archivos de máquina virtual de un vCenter Server a otro.
ES-001799-06	Usar el explorador del almacén de datos se actualizó para que incluya otros detalles.
ES-001799-05	<ul style="list-style-type: none">■ Directrices y prácticas recomendadas para los filtros de E/S se actualizó para que incluya una instrucción sobre los filtros de E/S y los árboles de instantáneas.■ Filtrado de almacenamiento se actualizó para corregir el valor del filtro para los mismos hosts y transportes. El valor correcto es <code>config.vpxd.filter.sameHostsAndTransportsFilter</code>.
ES-001799-04	Vida útil estimada para dispositivos flash se actualizó para que incluya otros detalles.
ES-001799-03	Migrar máquinas virtuales con Flash Read Cache se corrigió para que coincida con las opciones disponibles en vSphere Web Client.
ES-001799-02	Obtener información para la memoria caché de bloque del puntero de VMFS ahora incluye el comando <code>esxcli storage vmfs pbcache</code> .
ES-001799-01	Revisiones menores.
ES-001799-00	Versión inicial.

Introducción al almacenamiento

1

Esta introducción describe las opciones de almacenamiento disponibles en vSphere y explica cómo configurar el host para usar y administrar distintos tipos de almacenamiento.

Este capítulo incluye los siguientes temas:

- [Virtualización de almacenamiento](#)
- [Tipos de almacenamiento físico](#)
- [Representar dispositivos y destinos](#)
- [Características de los dispositivos de almacenamiento](#)
- [Adaptadores de almacenamiento compatibles](#)
- [Características de los almacenes de datos](#)
- [Acceden al almacenamiento las máquinas virtuales](#)
- [Comparar tipos de almacenamiento](#)

Virtualización de almacenamiento

La virtualización de almacenamiento de vSphere admite funcionalidades como máquinas virtuales, Virtual SAN, Virtual Volumes, administración de almacenamiento basada en directivas, entre otras.

ESXi ofrece virtualización de almacenamiento en el nivel del host, que abstrae lógicamente la capa de almacenamiento físico de las máquinas virtuales. Una máquina virtual de ESXi utiliza un disco virtual para almacenar su sistema operativo, archivos de programa y otros datos relacionados con sus actividades. Un disco virtual es un archivo físico de gran tamaño o un conjunto de archivos que pueden copiarse, transferirse, archivarse y respaldarse en una copia de seguridad con la misma facilidad que cualquier otro archivo. Es posible configurar máquinas virtuales con varios discos virtuales.

Para acceder a discos virtuales, una máquina virtual utiliza controladoras SCSI virtuales. Entre estas controladoras virtuales se encuentran BusLogic Parallel, LSI Logic Parallel, LSI Logic SAS y VMware Paravirtual. Estas controladoras son los únicos tipos de controladoras SCSI que puede ver y a las que puede acceder una máquina virtual.

Cada disco virtual reside en un almacén de datos que está implementado en almacenamiento físico. Desde el punto de vista de la máquina virtual, cada disco virtual aparece como si fuera una unidad SCSI conectada a una controladora SCSI. El acceso al almacenamiento físico real a través de adaptadores de almacenamiento o de la red en el host es generalmente transparente para el sistema operativo invitado y las aplicaciones que se ejecutan en la máquina virtual.

Además de discos virtuales, vSphere ofrece un mecanismo que se conoce como asignación de dispositivos sin formato (RDM). RDM es útil para los casos donde un sistema operativo invitado dentro de una máquina virtual requiere acceso directo a un dispositivo de almacenamiento. Para obtener información sobre RDM, consulte [Capítulo 18 Asignación de dispositivos sin formato](#).

Entre otras capacidades de virtualización que ofrece vSphere se encuentran Virtual SAN, Virtual Flash, Virtual Volumes y administración de almacenamiento basada en directivas. Para obtener información sobre Virtual SAN, consulte *Administración de VMware Virtual SAN*.

Tipos de almacenamiento físico

El proceso de administración de almacenamiento de ESXi comienza con el espacio de almacenamiento que el administrador de almacenamiento asigna previamente en los diferentes sistemas de almacenamiento.

ESXi admite los siguientes tipos de almacenamiento:

Almacenamiento local

Almacena archivos de máquina virtual en discos de almacenamiento internos o externos de conexión directa.

Almacenamiento en red

Almacena archivos de máquina virtual en discos de almacenamiento externos o matrices asociadas al host directamente o a través de una red de alta velocidad.

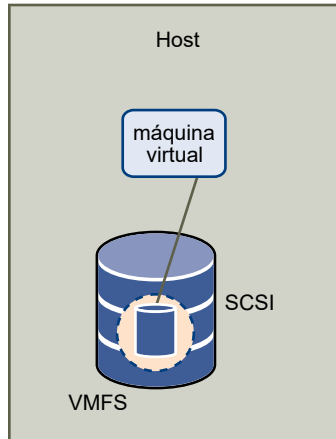
Almacenamiento local

El almacenamiento local puede constar de discos duros internos ubicados dentro del host ESXi, o bien sistemas de almacenamiento externos ubicados fuera y conectados directamente al host a través de protocolos como SAS o SATA.

El almacenamiento local no requiere una red de almacenamiento para comunicarse con el host. Necesita un cable conectado a la unidad de almacenamiento y, cuando se requiere, un HBA compatible en el host.

En la siguiente ilustración se muestra una máquina virtual que utiliza almacenamiento SCSI local.

Figura 1-1. Almacenamiento local



En este ejemplo de una topología de almacenamiento local, el host utiliza una sola conexión a un disco de almacenamiento. En ese disco, puede crear un almacén de datos de VMFS, que puede usar para almacenar archivos de disco de máquinas virtuales.

Aunque esta configuración de almacenamiento es posible, no es una topología recomendada. Con conexiones individuales entre matrices de almacenamiento y hosts, se crean únicos puntos de error (SPOF) que pueden causar interrupciones cuando una conexión se vuelve poco confiable o tiene errores. Sin embargo, debido a que la mayoría de dispositivos de almacenamiento local no admiten varias conexiones, no puede usar varias rutas de acceso para acceder al almacenamiento local.

ESXi admite distintos dispositivos de almacenamiento local, entre ellos SCSI, IDE, SATA, USB y sistemas de almacenamiento SAS. Más allá del tipo de almacenamiento que use, el host oculta una capa de almacenamiento físico de las máquinas virtuales.

Nota No pueden usar unidades IDE/ATA o USB para almacenar máquinas virtuales.

El almacenamiento local no admite el uso de recursos compartidos entre varios hosts. Solo un host tiene acceso a un almacén de datos en un dispositivo de almacenamiento local. En consecuencia, aunque puede usar almacenamiento local para crear máquinas virtuales, esto no permite usar las funciones de VMware que requieren almacenamiento compartido, como HA y vMotion.

Sin embargo, si usa un clúster de hosts que tienen únicamente dispositivos de almacenamiento locales, puede implementar Virtual SAN. Virtual SAN transforma los recursos de almacenamiento locales en almacenamiento compartido definido por software, y permite usar funciones que requieren almacenamiento compartido. Para obtener información detallada, consulte la documentación de *Administración de VMware Virtual SAN*.

Almacenamiento en red

El almacenamiento en red consiste en sistemas de almacenamiento externos que usa el host ESXi para almacenar archivos de máquina virtual de forma remota. Generalmente, el host accede a estos sistemas por medio de una red de almacenamiento de alta velocidad.

Los dispositivos de almacenamiento en red son compartidos. Varios hosts pueden acceder simultáneamente a los almacenes de datos en dispositivos de almacenamiento en red. ESXi admite varias tecnologías de almacenamiento en red.

Además del almacenamiento en red tradicional que abarca este tema, VMware admite almacenamiento compartido virtualizado, como Virtual SAN. Virtual SAN transforma los recursos de almacenamiento internos de los hosts ESXi en un almacenamiento compartido que brinda capacidades como High Availability y vMotion para las máquinas virtuales. Para obtener información detallada, consulte la documentación de *Administración de VMware Virtual SAN*.

Nota No se puede presentar el mismo LUN a un host ESXi o a varios hosts a través de distintos protocolos de almacenamiento. Para acceder al LUN, los hosts deben usar siempre un solo protocolo, por ejemplo, solo canal de fibra o solo iSCSI.

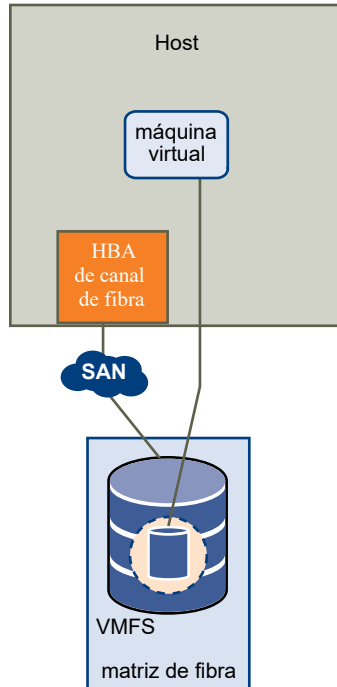
Canal de fibra (FC)

Almacena archivos de máquina virtual de forma remota en una red de área de almacenamiento (SAN) de FC. SAN de FC es una red especializada de alta velocidad que conecta los hosts a dispositivos de almacenamiento de alto rendimiento. La red usa el protocolo Fibre Channel para transportar el tráfico SCSI desde las máquinas virtuales hasta los dispositivos SAN de FC.

Para conectarse a la SAN de FC, el host debe tener adaptadores de bus host (HBA) de canal de fibra. A menos que use el almacenamiento de conexión directa de canal de fibra, necesitará conmutadores de canal de fibra para enrutar el tráfico de almacenamiento. Si el host contiene adaptadores de canal de fibra en Ethernet (FCoE), solo puede conectarse a los dispositivos de canal de fibra compartidos con una red Ethernet.

El almacenamiento de canal de fibra muestra las máquinas virtuales que usan almacenamiento de canal de fibra.

Figura 1-2. Almacenamiento de canal de fibra



En esta configuración, un host se conecta a un tejido de SAN, que consiste en conmutadores de canal de fibra y matrices de almacenamiento, con un adaptador de canal de fibra. Los LUN de una matriz de almacenamiento pasan a estar disponibles para el host. Puede acceder a los LUN y crear almacenes de datos para satisfacer sus necesidades de almacenamiento. Los almacenes de datos usan el formato VMFS.

Para obtener información específica sobre la configuración de la SAN de canal de fibra, consulte [Capítulo 3 Usar ESXi con SAN de canal de fibra](#).

Internet SCSI (iSCSI)

Almacena archivos de máquina virtual en dispositivos de almacenamiento iSCSI. iSCSI empaqueta el tráfico de almacenamiento SCSI en el protocolo TCP/IP para que pueda viajar por redes TCP/IP estándar en lugar de una red de FC especializada. Con una conexión iSCSI, el host actúa como el iniciador que se comunica con un destino, ubicado en sistemas de almacenamiento iSCSI remotos.

ESXi ofrece los tipos siguientes de conexiones iSCSI:

iSCSI de hardware

El host se conecta al almacenamiento a través de un adaptador de terceros capaz de descargar el procesamiento de red e iSCSI. Los adaptadores de hardware pueden ser dependientes e independientes.

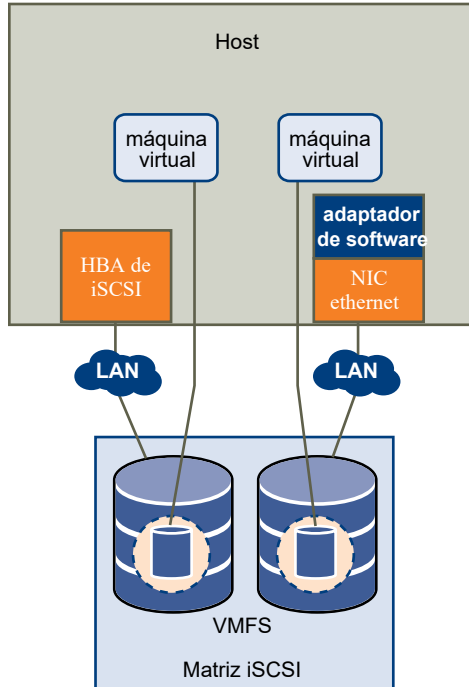
iSCSI de software

El host usa un iniciador iSCSI basado en software en VMkernel para conectarse al almacenamiento. Con este tipo de conexión iSCSI, el host necesita solo un adaptador de red estándar para la conectividad de red.

Debe configurar iniciadores iSCSI para que el host acceda y muestre los dispositivos de almacenamiento iSCSI.

El almacenamiento iSCSI muestra distintos tipos de iniciadores iSCSI.

Figura 1-3. Almacenamiento iSCSI



En el ejemplo de la izquierda, el host usa el adaptador de iSCSI de hardware para conectarse al sistema de almacenamiento iSCSI.

En el ejemplo de la derecha, el host usa un adaptador de iSCSI de software y una NIC Ethernet para conectarse al almacenamiento iSCSI.

Los dispositivos de almacenamiento iSCSI del sistema de almacenamiento pasan a estar disponibles para el host. Puede acceder a los dispositivos de almacenamiento y crear almacenes de datos de VMFS para sus necesidades de almacenamiento.

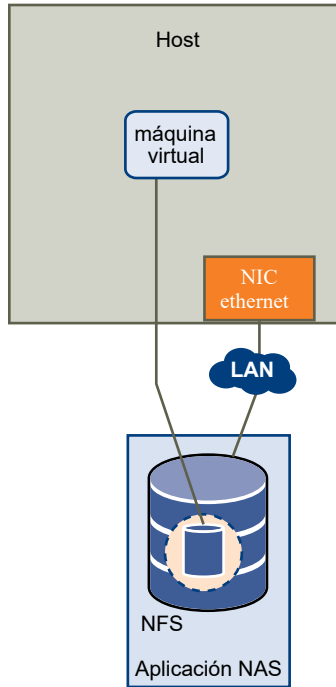
Para obtener información específica sobre la configuración de la SAN iSCSI, consulte [Capítulo 9 Usar ESXi con una SAN iSCSI](#).

Almacenamiento conectado a la red (NAS)

Almacena los archivos de máquina virtual en servidores de archivos remotos a los que se accede a través de una red TCP/IP estándar. El cliente NFS incorporado en ESXi usa las versiones 3 y 4.1 del protocolo Network File System (NFS) para comunicarse con los servidores NAS/NFS. Para la conectividad de red, el host requiere un adaptador de red estándar.

El almacenamiento NFS muestra una máquina virtual que usa el volumen NFS para almacenar sus archivos. En esta configuración, el host se conecta al servidor NFS, que almacena los archivos de disco virtual, a través de un adaptador de red normal.

Figura 1-4. Almacenamiento NFS



Para obtener información específica sobre la configuración del almacenamiento NFS, consulte [Descripción de los almacenes de datos de Network File System](#).

Shared Serial Attached SCSI (SAS)

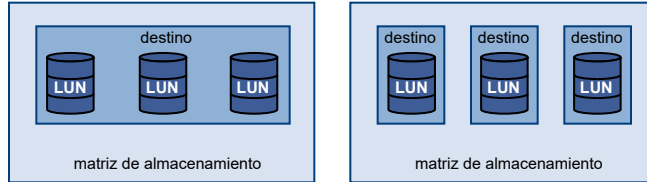
Almacena máquinas virtuales en sistemas de almacenamiento SAS directamente conectados que ofrecen acceso compartido a varios hosts. Este tipo de acceso permite que varios hosts accedan al mismo almacén de datos de VMFS en un LUN.

Representar dispositivos y destinos

En el contexto de ESXi, el término destino identifica a una sola unidad de almacenamiento a la que puede acceder el host. Los términos dispositivo y LUN describen un volumen lógico que representa el espacio de almacenamiento en un destino. Por lo general, los términos dispositivo y LUN en el contexto de ESXi significan un volumen de almacenamiento presentado al host desde un destino de almacenamiento y disponible para formateo.

Los distintos proveedores de almacenamiento presentan los sistemas de almacenamiento a los hosts ESXi de distintas formas. Algunos proveedores presentan un solo destino con varios dispositivos de almacenamiento o LUN, mientras que otros presentan varios destinos con un LUN cada uno.

Figura 1-5. Representar LUN y destinos



En esta ilustración, hay disponibles tres LUN en cada configuración. En uno de los casos, el host ve un destino, pero ese destino tiene tres LUN que se pueden utilizar. Cada LUN representa un volumen de almacenamiento individual. En el otro ejemplo, el host ve tres destinos distintos, cada uno con un LUN.

Los destinos a los que se accede a través de la red tienen nombres únicos proporcionados por los sistemas de almacenamiento. Los destinos iSCSI utilizan nombres de iSCSI, mientras que los destinos de canal de fibra utilizan los nombres World Wide Names (WWN).

Nota ESXi no admite el acceso al mismo LUN a través de distintos protocolos de transporte, como iSCSI y canal de fibra.

Un dispositivo, o LUN, se identifica por su nombre de UUID. Si varios hosts comparten un LUN, debe presentarse a todos los hosts con el mismo UUID.

Características de los dispositivos de almacenamiento

Se pueden ver todos los dispositivos de almacenamiento o los LUN disponibles para el host, incluidos todos los dispositivos en red y locales. Si se usan complementos de múltiples rutas de terceros, los dispositivos de almacenamiento disponibles por medio de los complementos también aparecen en la lista.

Se puede ver una lista independiente de los dispositivos de almacenamiento disponibles para un adaptador en particular.

Generalmente, al consultar los dispositivos de almacenamiento, se ve la siguiente información.

Tabla 1-1. Información de dispositivos de almacenamiento

Información de dispositivos de almacenamiento	Descripción
Name (Nombre)	También llamado Nombre para mostrar. Es un nombre que el host ESXi asigna al dispositivo según el tipo de almacenamiento y el fabricante. Puede cambiar este nombre por el nombre que desee.
Identificador	Un identificador universalmente único que es intrínseco al dispositivo.
Estado operativo	Indica si el dispositivo está montado o desmontado. Para obtener información detallada, consulte Separar dispositivos de almacenamiento .
LUN	Número de unidad lógica (LUN) en el destino SCSI. El número LUN se obtiene del sistema de almacenamiento. Si un destino tiene un solo LUN, el número LUN siempre es cero (0).

Tabla 1-1. Información de dispositivos de almacenamiento (continuación)

Información de dispositivos de almacenamiento	Descripción
Tipo	Tipo de dispositivo, por ejemplo, disco o CD-ROM.
Tipo de unidad	Información que especifica si el dispositivo es una unidad flash o una unidad HDD regular. Para obtener información sobre las unidades flash, consulte Capítulo 14 Trabajar con dispositivos flash .
Transporte	Protocolo de transporte que usa el host para acceder al dispositivo. El protocolo depende del tipo de almacenamiento que se usa. Consulte Tipos de almacenamiento físico .
Capacity (Capacidad)	Capacidad total del dispositivo de almacenamiento.
Propietario	El complemento, como NMP o el complemento de un tercero, que el host usa para administrar las rutas de acceso al dispositivo de almacenamiento. Para obtener información detallada, consulte Administrar varias rutas de acceso .
Aceleración de hardware	Información sobre si el dispositivo de almacenamiento asiste al host en las operaciones de administración de máquinas virtuales. El estado puede ser Supported (Compatible), Not Supported (No compatible) o Unknown (Desconocido). Para obtener información detallada, consulte Capítulo 23 Aceleración de hardware de almacenamiento .
Ubicación	Una ruta de acceso al dispositivo de almacenamiento en el directorio <code>/vmfs/devices/</code> .
Formato de partición	Un esquema de particiones que usa el dispositivo de almacenamiento. Puede ser un formato de registro de arranque maestro (MBR) o de tabla de particiones GUID (GPT). Los dispositivos GPT pueden admitir almacenes de datos mayores a 2 TB. Para obtener más información, consulte Almacenes de datos de VMFS y formatos de disco de almacenamiento .
Particiones	Particiones principales y lógicas, incluido un almacén de datos de VMFS, si está configurado.
Directivas de múltiples rutas (almacenes de datos de VMFS)	Directiva de selección de rutas de acceso y directiva de tipo de matriz de almacenamiento que usa el host para administrar las rutas de acceso al almacenamiento. Para obtener más información, consulte Capítulo 17 Descripción de múltiples rutas y conmutación por error .
Rutas de acceso (almacenes de datos de VMFS)	Rutas de acceso que se utilizan para acceder al almacenamiento y a su estado.

Mostrar dispositivos de almacenamiento de un host

Muestre todos los dispositivos de almacenamiento disponibles para un host. Si se utiliza algún complemento de múltiples rutas de terceros, los dispositivos de almacenamiento disponibles por medio de los complementos también aparecen en la lista.

La vista Storage Devices (Dispositivos de almacenamiento) permite enumerar los dispositivos de almacenamiento de los hosts, analizar la información y modificar las propiedades.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento**.

Todos los dispositivos de almacenamiento disponibles para el host aparecen enumerados en Storage Devices (Dispositivos de almacenamiento).

4 Para ver los detalles de un dispositivo específico, seleccione el dispositivo en la lista.

5 Utilice las pestañas en Device Details (Detalles del dispositivo) para acceder a la información adicional y modificar las propiedades del dispositivo seleccionado.

Pestaña	Descripción
Properties (Propiedades)	Vea las propiedades y características del dispositivo. Vea y modifique las directivas de múltiples rutas para el dispositivo.
Rutas de acceso	Muestre las rutas de acceso disponibles para el dispositivo. Permite deshabilitar o habilitar una ruta de acceso seleccionada.

Mostrar dispositivos de almacenamiento para un adaptador

Muestre una lista de dispositivos de almacenamiento a los que se pueda acceder a través de un adaptador de almacenamiento específico en el host.

Procedimiento

1 Diríjase al host en el navegador de vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 Haga clic en Storage Adapters (Adaptadores de almacenamiento).

Todos los adaptadores de almacenamiento instalados en el host aparecen en el listado de Storage Adapters (Adaptadores de almacenamiento).

4 Seleccione el adaptador en la lista y haga clic en la pestaña **Devices** (Dispositivos).

Aparecen los dispositivos de almacenamiento a los que puede acceder el host a través del adaptador.

Adaptadores de almacenamiento compatibles

Los adaptadores de almacenamiento brindan conectividad al host ESXi a una red o una unidad de almacenamiento específicas.

ESXi es compatible con distintas clases de adaptadores, entre ellos, SCSI, iSCSI, RAID, canal de fibra, canal de fibra en Ethernet (FCoE) y Ethernet. ESXi accede a los adaptadores directamente a través de los controladores de dispositivos en el VMkernel.

Según el tipo de almacenamiento que se utilice, es posible que se deba habilitar y configurar un adaptador de almacenamiento en el host.

Para obtener información sobre cómo configurar adaptadores de FCoE de software, consulte [Capítulo 5 Configurar el canal de fibra en Ethernet](#).

Para obtener información sobre cómo configurar distintos tipos de adaptadores de iSCSI, consulte [Capítulo 10 Configurar adaptadores y almacenamiento iSCSI](#).

Características del adaptador de almacenamiento

El host utiliza adaptadores de almacenamiento para acceder a los diferentes dispositivos de almacenamiento. Es posible mostrar detalles de los adaptadores de almacenamiento disponibles y revisar su información.

Debe habilitar ciertos adaptadores, por ejemplo, iSCSI o FCoE de software, antes de poder ver su información.

Tabla 1-2. Información del adaptador de almacenamiento

Información del adaptador	Descripción
Modelo	Modelo del adaptador.
Destinos (canal de fibra y SCSI)	Cantidad de destinos a los que se accede a través del adaptador.
Destinos conectados (iSCSI)	Cantidad de destinos conectados en un adaptador de iSCSI.
WWN (canal de fibra)	Nombre World Wide Name formado según los estándares de canal de fibra que brindan una identificación única del adaptador de canal de fibra.
Nombre iSCSI (iSCSI)	Nombre único formado según los estándares de iSCSI que identifica al adaptador de iSCSI.
Alias iSCSI (iSCSI)	Nombre alternativo que se utiliza en lugar del nombre iSCSI.
Dirección IP (iSCSI de hardware independiente)	Dirección asignada al HBA de iSCSI.
Dispositivos	Todos los dispositivos de almacenamiento o LUN a los que puede acceder el adaptador.
Rutas de acceso	Todas las rutas de acceso que utiliza el adaptador para acceder a dispositivos de almacenamiento.
Propiedades (Propiedades)	Vínculo que indica que el adaptador requiere configuración adicional. Los adaptadores de iSCSI y FCoE muestran este vínculo.

Ver información sobre adaptadores de almacenamiento

Muestre los adaptadores de almacenamiento que usa el host y revise la información.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento**.
- 4 Para ver los detalles de un adaptador específico, seleccione el adaptador en la lista.

Características de los almacenes de datos

Los almacenes de datos son contenedores lógicos, de manera análoga a los sistemas de archivos, que ocultan aspectos específicos de cada dispositivo de almacenamiento y ofrecen un modelo uniforme para almacenar archivos de máquinas virtuales. Puede visualizar todos los almacenes de datos disponibles para los hosts y analizar sus propiedades.

Los almacenes de datos se agregan a vCenter Server mediante los siguientes métodos:

- Puede crear un almacén de datos VMFS5, un almacén de datos de NFS versión 3 o 4.1 o un almacén de datos virtual mediante el asistente New Datastore (Nuevo almacén de datos). Al habilitar Virtual SAN, se crea un almacén de datos de Virtual SAN de forma automática.
- Al agregar un host a vCenter Server, todos los almacenes de datos del host se agregan a vCenter Server.

En la siguiente tabla se describen los detalles de los almacenes de datos que puede consultar mediante vSphere Web Client. Es posible que ciertas características no estén disponibles o no sean aplicables para todos los tipos de almacenes de datos.

Tabla 1-3. Información de almacén de datos

Información de almacén de datos	Tipo de almacén de datos aplicable	Descripción
Name (Nombre)	VMFS NFS Virtual SAN VVOL	Nombre editable que se asigna a un almacén de datos. Para obtener información sobre el cambio de nombre de un almacén de datos, consulte Cambiar nombre del almacén de datos .
Tipo de sistema de archivos	VMFS NFS Virtual SAN VVOL	El sistema de archivos que usa el almacén de datos. Para obtener información sobre los almacenes de datos de VMFS y NFS, y el modo de administrarlos, consulte Capítulo 16 Trabajar con almacenes de datos . Para obtener información sobre los almacenes de datos Virtual SAN, consulte la documentación de <i>Administración de VMware Virtual SAN</i> . Para obtener información sobre Virtual Volumes, consulte Capítulo 19 Trabajar con Virtual Volumes .
Copia de seguridad de los dispositivos	VMFS NFS Virtual SAN	Información sobre el almacenamiento subyacente, como un dispositivo de almacenamiento en el que se implementan el almacén de datos (VMFS), el servidor y la carpeta (NFS), o los grupos de discos (Virtual SAN).
Extremos de protocolo	VVOL	Información sobre los extremos de protocolo correspondientes. Consulte Extremos de protocolo .
Extensiones	VMFS	Extensiones individuales que expanden el almacén de datos y su capacidad.
Tipo de unidad	VMFS	Tipo de dispositivo de almacenamiento subyacente, una unidad flash o una unidad HDD regular. Para obtener información detallada, consulte Capítulo 14 Trabajar con dispositivos flash .

Tabla 1-3. Información de almacén de datos (continuación)

Información de almacén de datos	Tipo de almacén de datos aplicable	Descripción
Capacity (Capacidad)	VMFS NFS Virtual SAN VVOL	Incluye capacidad total, espacio aprovisionado y espacio libre.
Punto de montaje	VMFS NFS Virtual SAN VVOL	Una ruta de acceso al almacén de datos del directorio / <code>vmfs/volumes/</code> del host.
Conjunto de funcionalidades	VMFS <hr/> Nota Un almacén de datos de VMFS de varias extensiones asume las funcionalidades de solo una de sus extensiones. <hr/> NFS Virtual SAN	Información sobre los servicios de datos de almacenamiento que proporciona la entidad de almacenamiento subyacente. No se pueden modificar.
Storage I/O Control	VMFS NFS	Información sobre el estado de la priorización de E/S de almacenamiento en todo el clúster, para saber si está habilitada o no. Consulte la documentación de <i>Administración de recursos de vSphere</i> .
Aceleración de hardware	VMFS NFS Virtual SAN VVOL	Información sobre la compatibilidad de la entidad de almacenamiento subyacente con la aceleración de hardware. El estado puede ser Supported (Compatible), Not Supported (No compatible) o Unknown (Desconocido). Para obtener información detallada, consulte Capítulo 23 Aceleración de hardware de almacenamiento . <hr/> Nota NFS 4.1 no admite la aceleración de hardware.
Tags	VMFS NFS Virtual SAN VVOL	Las funcionalidades de bases de datos que el usuario define y asocia con almacenes de datos en forma de etiquetas. Para obtener información, consulte Directivas y reglas de almacenamiento .
Conectividad con hosts	VMFS NFS VVOL	Hosts en los que está montado el almacén de datos.
Múltiples rutas	VMFS VVOL	Directiva de selección de rutas de acceso que usa el host para acceder al almacenamiento. Para obtener más información, consulte Capítulo 17 Descripción de múltiples rutas y conmutación por error .

Mostrar la información del almacén de datos

Acceda a la vista Datastores (Almacenes de datos) con el navegador de vSphere Web Client. La vista Datastores (Almacenes de datos) que se muestra en el navegador permite enumerar todos los almacenes de datos disponibles en el inventario de infraestructura de vSphere, analizar la información y modificar las propiedades. También puede utilizar la vista para crear almacenes de datos.

Para enumerar los almacenes de datos de un objeto primario específico, como un centro de datos, un clúster o un host, consulte [Listado de almacenes de datos para un objeto de infraestructura](#).

Procedimiento

- 1 En el navegador de vSphere Web Client, seleccione **Listas de inventario global > Almacenes de datos**.

Los almacenes de datos que están disponibles en el inventario aparecen en el panel central Datastores (Almacenes de datos).

- 2 Utilice los iconos para crear un almacén de datos o para realizar tareas básicas para un almacén de datos seleccionado.

Icono	Descripción
	Crea un almacén de datos.
	Aumenta la capacidad del almacén de datos.
	Monta un almacén de datos a ciertos hosts.
	Quita un almacén de datos.
	Desmonta un almacén de datos de ciertos hosts.

- 3 Para ver detalles específicos del almacén de datos, haga clic en el almacén de datos seleccionado.
- 4 Utilice las pestañas para acceder a la información adicional y modificar las propiedades del almacén de datos.

Pestaña	Descripción
Getting Started (Introducción)	Vea la información introductoria y acceda a las acciones básicas.
Summary	Vea las estadísticas y la configuración de los almacenes de datos seleccionados.
Monitor (Supervisar)	Vea la información sobre alarmas, datos de rendimiento, asignación de recursos, eventos y otra información de estado del almacén de datos.

Pestaña	Descripción
Manage (Administrar)	Vea y modifique permisos, etiquetas, definiciones de alarma y propiedades del almacén de datos. Utilice esta pestaña para acceder a los dispositivos de almacenamiento que respaldan el almacén de datos y para ver y editar detalles de múltiples rutas para los dispositivos del almacén de datos.
Related Objects (Objetos relacionados)	Vea los objetos relacionados con el almacén de datos. Los objetos incluyen máquinas virtuales que residen en el almacén de datos y los hosts donde está montado el almacén de datos.

Listado de almacenes de datos para un objeto de infraestructura






Muestra los almacenes de datos de un objeto primario en particular, como un centro de datos, un clúster o un host.

Procedimiento

- 1 Utilice el navegador de objetos de vSphere Web Client para desplazarse hasta un objeto que sea un objeto primario válido de un almacén de datos, como un centro de datos, un clúster o un host.
- 2 Haga clic en la pestaña **Related Objects** (Objetos relacionados) y haga clic en **Datastores** (Almacenes de datos).

Si hay algún almacén de datos configurado para este objeto, aparece en el panel Datastores (Almacenes de datos) ubicado en el centro.

- 3 Utilice los iconos para crear un almacén de datos o para realizar tareas básicas para un almacén de datos seleccionado.

Icono	Descripción
	Crea un almacén de datos.
	Aumenta la capacidad del almacén de datos.
	Monta un almacén de datos a ciertos hosts.
	Quita un almacén de datos.
	Desmonta un almacén de datos de ciertos hosts.

- 4 Utilice las pestañas para acceder a la información adicional y modificar las propiedades del almacén de datos.

Pestaña	Descripción
Getting Started (Introducción)	Vea la información introductoria y acceda a las acciones básicas.
Summary	Vea las estadísticas y la configuración de los almacenes de datos seleccionados.
Monitor (Supervisar)	Vea la información sobre alarmas, datos de rendimiento, asignación de recursos, eventos y otra información de estado del almacén de datos.

Pestaña	Descripción
Manage (Administrar)	Vea y modifique permisos, etiquetas, definiciones de alarma y propiedades del almacén de datos. Utilice esta pestaña para acceder a los dispositivos de almacenamiento que respaldan el almacén de datos y para ver y editar detalles de múltiples rutas para los dispositivos del almacén de datos.
Related Objects (Objetos relacionados)	Vea los objetos relacionados con el almacén de datos. Los objetos incluyen máquinas virtuales que residen en el almacén de datos y los hosts donde está montado el almacén de datos.

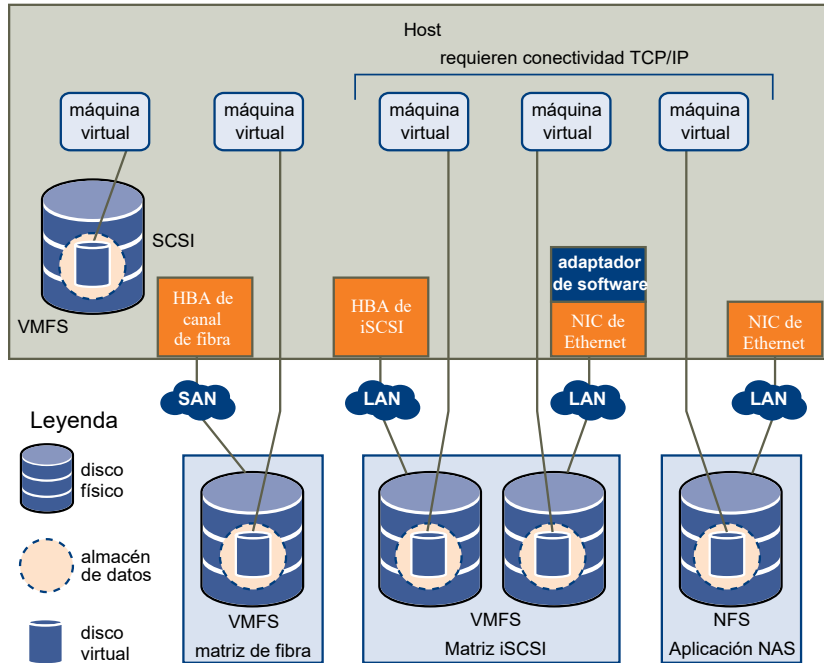
Acceden al almacenamiento las máquinas virtuales

Cuando una máquina virtual se comunica con su disco virtual almacenado en un almacén de datos, emite comandos SCSI. Debido a que los almacenes de datos pueden existir en distintos tipos de almacenamiento físico, estos comandos se encapsulan en otras formas, según el protocolo que el host ESXi usa para conectarse a un dispositivo de almacenamiento.

ESXi admite los protocolos Fibre Channel (FC), Internet SCSI (iSCSI), Fibre Channel over Ethernet (FCoE) y NFS. Más allá del tipo de dispositivo de almacenamiento que utilice el host, el disco virtual siempre aparece como un dispositivo SCSI montado para la máquina virtual. El disco virtual oculta una capa de almacenamiento físico desde el sistema operativo de la máquina virtual. Esto permite ejecutar sistemas operativos que no estén certificados para equipos de almacenamiento específicos, como SAN, dentro de la máquina virtual.

En el siguiente gráfico se incluyen cinco máquinas virtuales que usan diferentes tipos de almacenamiento para ilustrar las diferencias entre cada uno de ellos.

Figura 1-6. Acceso de máquinas virtuales a diferentes tipos de almacenamiento



Nota Este diagrama tiene fines exclusivamente conceptuales. No se trata de una configuración recomendada.

Comparar tipos de almacenamiento

La compatibilidad con ciertas funcionalidades de vSphere puede depender de la tecnología de almacenamiento utilizada.

En la siguiente tabla se comparan las tecnologías de almacenamiento en red compatibles con ESXi.

Tabla 1-4. Almacenamiento en red compatible con ESXi

Tecnología	Protocolo	Transferencias	Interfaz
Canal de fibra	FC/SCSI	Acceso en bloque a datos/LUN	HBA de FC
Canal de fibra en Ethernet	FCoE/SCSI	Acceso en bloque a datos/LUN	<ul style="list-style-type: none"> ■ Adaptador de red convergente (FCoE de hardware) ■ NIC compatible con FCoE (FCoE de software)
iSCSI	IP/SCSI	Acceso en bloque a datos/LUN	<ul style="list-style-type: none"> ■ HBA de iSCSI o NIC habilitada para iSCSI (iSCSI de hardware) ■ Adaptador de red (iSCSI de software)
NAS	IP/NFS	Archivo (sin acceso directo al LUN)	Adaptador de red

En la siguiente tabla se comparan las características de vSphere y los diferentes tipos de almacenamiento compatibles.

Tabla 1-5. Características de vSphere compatibles con el almacenamiento

Tipo de almacenamiento	Máquina virtual de arranque	vMotion	Almacén de datos	RDM	Clúster de máquina virtual	VMware HA y DRS	Storage APIs - Data Protection
Almacenamiento local	Sí	No	VMFS	No	Sí	No	Sí
Canal de fibra	Sí	Sí	VMFS	Sí	Sí	Sí	Sí
iSCSI	Sí	Sí	VMFS	Sí	Sí	Sí	Sí
NAS en NFS	Sí	Sí	NFS 3 y NFS 4.1	No	No	Sí	Sí

Nota El almacenamiento local es compatible con un clúster de máquinas virtuales en un solo host (denominado sistema Cluster-in-a-box). Se requiere un disco virtual compartido. Para obtener más información sobre esta configuración, consulte la documentación de *Administración de recursos de vSphere*.

Descripción general de la utilización de ESXi con una SAN

2

Utilizar ESXi con una SAN mejora la flexibilidad, la eficiencia y la confiabilidad. El uso de ESXi con una SAN también es compatible con las tecnologías de equilibrio de la carga, conmutación por error y administración centralizada.

A continuación, se mencionan los beneficios de utilizar ESXi con una SAN:

- Puede almacenar datos de forma segura y configurar varias rutas de acceso al almacenamiento, y eliminar así un único punto de error.
- Utilizar una SAN con sistemas ESXi amplía la resistencia a errores al servidor. Cuando se utiliza el almacenamiento de SAN, todas las aplicaciones pueden reiniciarse instantáneamente en otro host después de un error del host original.
- Puede realizar una migración en vivo de máquinas virtuales con VMware vMotion.
- Utilice VMware High Availability (HA) junto con una SAN para reiniciar las máquinas virtuales en su último estado conocido en un servidor distinto si hay un error en su host.
- Utilice VMware Fault Tolerance (FT) para replicar máquinas virtuales protegidas en dos hosts distintos. Las máquinas virtuales siguen funcionando sin interrupción en el host secundario si ocurre un error en el principal.
- Utilice VMware Distributed Resource Scheduler (DRS) para migrar máquinas virtuales de un host a otro para el equilibrio de la carga. Como el almacenamiento está en una matriz SAN compartida, las aplicaciones continúan ejecutándose sin problemas.
- Si utiliza clústeres de VMware DRS, ponga un host ESXi en modo de mantenimiento para que el sistema migre todas las máquinas virtuales en ejecución a otros hosts ESXi. A continuación, podrá realizar actualizaciones u otras operaciones de mantenimiento en el host original.

La portabilidad y la encapsulación de máquinas virtuales de VMware complementan la naturaleza de uso compartido de este almacenamiento. Cuando las máquinas virtuales se encuentran en un almacenamiento basado en SAN, puede apagar rápidamente una máquina virtual en un servidor y prenderla en otro, o suspenderla en uno y reanudar la operación en otro servidor en la misma red. Esta capacidad permite migrar los recursos informáticos y mantener un acceso compartido coherente.

Este capítulo incluye los siguientes temas:

- [Casos de uso de ESXi y SAN](#)

- Detalles de la utilización de almacenamiento SAN con ESXi
- Hosts ESXi y varias matrices de almacenamiento
- Toma de decisiones relacionadas con el LUN
- Seleccionar la ubicación de las máquinas virtuales
- Aplicaciones en capas
- Aplicaciones de administración de terceros
- Consideraciones sobre copias de seguridad de almacenamiento SAN

Casos de uso de ESXi y SAN

Cuando se utiliza con una SAN, ESXi puede aprovechar varias características de vSphere, incluidas Storage vMotion, Distributed Resource Scheduler (DRS), High Availability, etc.

La utilización de ESXi junto con una SAN es eficaz para las tareas siguientes:

Consolidación del almacenamiento y simplificación del diseño de almacenamiento

Si trabaja con varios hosts y cada uno ejecuta varias máquinas virtuales, el almacenamiento de los hosts deja de ser suficiente y se requiere un almacenamiento externo. Elija una SAN para el almacenamiento externo a fin de proporcionar una arquitectura de sistema más simple junto con otros beneficios.

Mantenimiento con cero tiempo de inactividad

Cuando realice mantenimiento de infraestructura o host ESXi, utilice vMotion para migrar las máquinas virtuales a otro host. Si el almacenamiento compartido está en la SAN, puede realizar el mantenimiento sin interrupciones para los usuarios de las máquinas virtuales. Los procesos en funcionamiento de la máquina virtual continúan durante toda una migración.

Load balancing (Equilibrio de carga)

Puede agregar un host a un clúster DRS y los recursos del host se vuelven parte de los recursos del clúster. La distribución y la utilización de los recursos de memoria y de CPU de todos los hosts y las máquinas virtuales en el clúster se supervisan continuamente. DRS compara estas métricas con una utilización de recursos ideal. La utilización ideal toma en cuenta los atributos de las máquinas virtuales y los grupos de recursos del clúster, la demanda actual y el destino de desequilibrio. A continuación, realiza (o recomienda) migraciones de máquina virtual, de manera acorde.

Recuperación ante desastres

VMware High Availability se puede utilizar para configurar varios hosts ESXi como clúster a fin de proporcionar una recuperación rápida de las interrupciones y una alta disponibilidad rentable para las aplicaciones que se ejecutan en máquinas virtuales.

Migraciones de matrices simplificadas y actualizaciones de almacenamiento

Cuando compre nuevos sistemas o matrices de almacenamiento, utilice Storage vMotion para realizar migraciones automáticas en vivo de archivos de disco de máquina virtual de un almacenamiento existente a su destino nuevo sin interrupciones para los usuarios de las máquinas virtuales.

Detalles de la utilización de almacenamiento SAN con ESXi

La utilización de una SAN junto con un host ESXi es diferente a la utilización tradicional de una SAN en varias maneras.

Cuando utiliza almacenamiento SAN con ESXi, tenga en cuenta las siguientes consideraciones:

- No puede utilizar las herramientas de administración de SAN para acceder directamente a todos los sistemas operativos de las máquinas virtuales que utilizan ese almacenamiento. Con herramientas tradicionales, puede supervisar solo el sistema operativo de VMware ESXi. Puede utilizar vSphere Web Client para supervisar máquinas virtuales.
- El HBA visible para las herramientas de administración de SAN forma parte del sistema ESXi, no de la máquina virtual.
- Por lo general, el sistema ESXi se encarga de las múltiples rutas.

Hosts ESXi y varias matrices de almacenamiento

Un host ESXi puede acceder a dispositivos de almacenamiento presentados desde varias matrices de almacenamiento, incluidas matrices de distintos proveedores.

Cuando se utilizan varias matrices de distintos proveedores, se deben tener en cuenta las siguientes consideraciones:

- Si el host utiliza el mismo complemento de tipo de matriz de almacenamiento (SATP) para varias matrices, se debe tener cuidado al cambiar la directiva de selección de ruta de acceso (PSP) predeterminada para ese SATP. El cambio se aplicará a todas las matrices. Para obtener información sobre SATP y PSP, consulte [Capítulo 17 Descripción de múltiples rutas y conmutación por error](#).
- Algunas matrices de almacenamiento ofrecen recomendaciones sobre la profundidad de la cola y otras opciones. Por lo general, estas opciones se configuran de manera global en el nivel del host ESXi. Un cambio en una matriz afecta a otras matrices que presentan LUN al host. Para obtener información sobre cómo cambiar la profundidad de la cola, consulte el artículo de la base de conocimientos de VMware en <http://kb.vmware.com/kb/1267>.
- Utilice la división en zonas de un solo destino y un solo iniciador cuando divida en zonas los hosts ESXi en matrices de canal de fibra. Con este tipo de configuración, los eventos relacionados con el tejido que ocurren en una matriz no afectan otras matrices. Para obtener más información sobre la división en zonas, consulte [Usar la división en zonas con las SAN de canal de fibra](#).

Toma de decisiones relacionadas con el LUN

Debe planificar de qué forma se realizará la configuración del almacenamiento para los sistemas ESXi antes de formatear los LUN con almacenes de datos de VMFS.

Al tomar decisiones relacionadas con el LUN, tenga en cuenta las siguientes consideraciones:

- Cada LUN debe tener el nivel de RAID y la característica de almacenamiento correctos para las aplicaciones que se ejecutan en las máquinas virtuales que utilizan el LUN.
- Cada LUN debe contener un solo almacén de datos de VMFS.
- Si varias máquinas virtuales acceden al mismo VMFS, utilice discos compartidos para priorizarlas.

Es conveniente tener menos LUN de mayor tamaño por los siguientes motivos:

- Más flexibilidad para crear máquinas virtuales sin solicitar más espacio al administrador de almacenamiento.
- Más flexibilidad para redimensionar los discos virtuales, realizar las instantáneas, etc.
- Menos almacenes de datos de VMFS para administrar.

Es conveniente tener más LUN de menor tamaño por los siguientes motivos:

- Menos espacio de almacenamiento desperdiciado.
- Diferentes aplicaciones pueden necesitar diferentes características de RAID.
- Más flexibilidad, ya que la directiva de múltiples rutas y los discos compartidos se establecen por LUN.
- La utilización del Servicio de clúster de Microsoft requiere que cada recurso de disco de clúster esté en su propio LUN.
- Mejor rendimiento, ya que hay menos contención para un solo volumen.

Cuando la caracterización del almacenamiento de una máquina virtual no está disponible, con frecuencia no hay un método simple para determinar la cantidad y el tamaño de los LUN que se debe aprovisionar. Puede experimentar con un esquema predictivo o adaptativo.

Usar el esquema predictivo para tomar decisiones sobre LUN

Cuando configura el almacenamiento de sistemas ESXi, antes de crear almacenes de datos de VMFS, debe decidir el tamaño y la cantidad de LUN que aprovisionará. Puede experimentar con el esquema predictivo.

Procedimiento

- 1 Aprovechone varios LUN con distintas características de almacenamiento.
- 2 Cree un almacén de datos de VMFS en cada LUN, etiquete cada almacén de datos según sus características.

- 3 Cree discos virtuales para contener los datos de las aplicaciones de máquina virtual en los almacenes de datos de VMFS creados en LUN con el nivel RAID adecuado para los requisitos de las aplicaciones.
- 4 Utilice los discos compartidos para distinguir las máquinas virtuales con prioridad alta de aquellas con prioridad baja.

Nota Los discos compartidos solo son pertinentes dentro de un host determinado. Los recursos compartidos asignados a las máquinas virtuales de un host no afectan a las máquinas virtuales de los demás hosts.

- 5 Ejecute las aplicaciones para determinar si el rendimiento de una máquina virtual es aceptable.

Usar el esquema adaptativo para tomar decisiones de LUN

Al configurar el almacenamiento para hosts ESXi, antes de crear almacenes de datos de VMFS, debe decidir el tamaño y la cantidad de LUN que aprovisionará. Puede experimentar con el esquema adaptativo.

Procedimiento

- 1 Aprovisione un LUN de gran tamaño (RAID 1+0 o RAID 5) con la escritura de almacenamiento en caché habilitada.
- 2 Cree un VMFS en ese LUN.
- 3 Cree cuatro o cinco discos virtuales en el VMFS.
- 4 Ejecute las aplicaciones para determinar si el rendimiento de un disco es aceptable.

Resultados

Si el rendimiento es aceptable, puede colocar discos virtuales adicionales en el VMFS. Si el rendimiento no es aceptable, cree un nuevo LUN de gran tamaño, posiblemente con un nivel de RAID diferente, y repita el proceso. Utilice la migración para no perder datos de máquinas virtuales al volver a crear el LUN.

Seleccionar la ubicación de las máquinas virtuales

Cuando se trabaja para optimizar el rendimiento de las máquinas virtuales, la ubicación del almacenamiento es un factor importante. Siempre existen ventajas y desventajas al comparar un almacenamiento costoso que ofrece alto rendimiento y alta disponibilidad con un almacenamiento de menor costo y menor rendimiento.

El almacenamiento puede dividirse en diferentes niveles de acuerdo con una serie de factores:

- Nivel alto. Ofrece alto rendimiento y alta disponibilidad. Puede ofrecer instantáneas integradas para facilitar la creación de copias de seguridad y las restauraciones en un punto en el tiempo (PiT). Admite replicación, redundancia completa del procesador de almacenamiento y unidades SAS. Utiliza cabezales de alto costo.

- Nivel medio. Ofrece rendimiento medio, menor disponibilidad, redundancia parcial del procesador de almacenamiento y unidades SCSI o SAS. Puede ofrecer instantáneas. Utiliza cabezales de costo intermedio.
- Nivel inferior. Ofrece bajo rendimiento y poca redundancia de almacenamiento interno. Utiliza unidades SCSI de nivel inferior o SATA (cabezales en serie de bajo costo).

No todas las aplicaciones necesitan estar en el almacenamiento de mayor rendimiento y disponibilidad, al menos no durante toda su vida útil.

Nota Si necesita parte de la funcionalidad del nivel alto, como las instantáneas, pero no desea pagar por ello, quizás pueda acceder a algunas de las características de alto rendimiento mediante software. Por ejemplo, puede crear instantáneas en software.

Cuando decida dónde colocar una máquina virtual, hágase estas preguntas:

- ¿Qué nivel de importancia tiene la máquina virtual?
- ¿Cuáles son sus requisitos de rendimiento y disponibilidad?
- ¿Cuáles son sus requisitos de restauración PiT?
- ¿Cuáles son sus requisitos de copia de seguridad?
- ¿Cuáles son sus requisitos de replicación?

Una máquina virtual puede cambiar de nivel durante su vida útil debido a cambios en su nivel de importancia o a cambios tecnológicos que permiten ofrecer características de niveles superiores en un nivel más bajo. El nivel de importancia es relativo y puede cambiar por distintos motivos, entre ellos por cambios en la organización, procesos operativos, requisitos normativos, planificación ante desastres, etc.

Aplicaciones en capas

Los administradores de SAN usan habitualmente software basado en matriz para copias de seguridad, recuperación ante desastres, minería de datos, análisis y prueba de configuración.

Los proveedores de almacenamiento generalmente proporcionan dos tipos de servicios avanzados para sus LUN: creación de instantáneas y replicación.

- La creación de instantáneas genera espacio con copias eficaces de los LUN que comparten bloques comunes de datos. En general, la creación de instantáneas se usa de forma local en los mismos sistemas de almacenamiento que el LUN principal para tareas rápidas de minería de datos, análisis, pruebas de aplicación y copias de seguridad.
- La replicación crea copias completas de los LUN. Las réplicas generalmente se hacen en sistemas de almacenamiento distintos, posiblemente en sitios distintos, como forma de protección contra interrupciones importantes que incapacitan o destruyen una matriz o un sitio en su totalidad.

Cuando utiliza un sistema ESXi junto con una SAN, debe decidir si las herramientas basadas en host o en matriz son las más adecuadas para su situación en especial.

Solución (de terceros) basada en matrices

Al utilizar un sistema ESXi junto con una SAN, se debe decidir si las herramientas basadas en matrices son más adecuadas para una situación en particular.

Cuando considere una solución basada en matrices, tenga en cuenta lo siguiente:

- Las soluciones basadas en matrices por lo general resultan en estadísticas más amplias. Con los RDM, los datos siempre toman la misma ruta de acceso, lo que resulta en una administración de rendimiento más sencilla.
- La seguridad es más transparente para el administrador de almacenamiento cuando utiliza un RDM y una solución basada en matrices porque con los RDM, las máquinas virtuales se asemejan más a las máquinas físicas.
- Si utiliza una solución basada en matrices, los RDM con compatibilidad física por lo general se utilizan para el almacenamiento de máquinas virtuales. Si no tiene intenciones de utilizar RDM, revise la documentación del proveedor de almacenamiento para ver si las operaciones en los LUN con volúmenes VMFS son compatibles. Si utiliza operaciones de matriz en LUN de VMFS, lea con atención la sección sobre volver a firmar.

Solución basada en archivos (VMFS)

Al utilizar un sistema ESXi junto con una SAN, se debe decidir si las herramientas basadas en archivos son más adecuadas para una situación en particular.

Al considerar una solución basada en archivos que utilice VMware Tools y VMFS en lugar de las herramientas de matriz, tenga en cuenta los siguientes puntos:

- El uso de VMware Tools y VMFS es mejor para el aprovisionamiento. Se asigna un LUN de gran tamaño y pueden colocarse varios archivos .vmdk en ese LUN. Con el RDM, se requiere un LUN nuevo para cada máquina virtual.
- Se incluye sin ningún costo adicional la creación de instantáneas con el host ESXi.
- El uso de VMFS es más sencillo para los administradores de ESXi.
- Los administradores de ESXi que utilizan la solución basada en archivos son más independientes del administrador de SAN.

Aplicaciones de administración de terceros

Puede usar aplicaciones de administración de terceros en combinación con su host ESXi.

La mayor parte del hardware de SAN incluye el software de administración de almacenamiento. En la mayoría de los casos, el software es una aplicación web que puede usarse con un explorador web conectado a la red. En otros casos, este software se suele ejecutar en el sistema de almacenamiento o en un servidor individual independiente de los servidores que utilizan SAN para fines de almacenamiento.

Puede usar el software de administración de terceros para las siguientes tareas:

- Administración de matrices de almacenamiento, como creación de LUN, administración de memorias caché de matriz, asignación de LUN y seguridad de LUN.
- Configurar replicación, puntos de control, instantáneas o creación de reflejo.

Si decide ejecutar el software de administración de SAN en una máquina virtual, obtiene el beneficio de ejecutar una máquina virtual, que incluye la conmutación por error mediante vMotion y VMware HA. Sin embargo, debido al nivel adicional de direccionamiento indirecto, es posible que el software de administración no pueda detectar la SAN. En este caso, se puede usar un RDM.

Nota Según el sistema de almacenamiento específico, una máquina virtual puede o no ejecutar el software de administración.

Consideraciones sobre copias de seguridad de almacenamiento SAN

Contar con una estrategia de copias de seguridad adecuada es uno de los aspectos más importantes de la administración de SAN. En el entorno de SAN, las copias de seguridad tienen dos objetivos. El primer objetivo es archivar los datos en línea en un soporte físico sin conexión. Este proceso se repite periódicamente para todos los datos en línea en una programación cronológica. El segundo objetivo es proporcionar acceso a los datos sin conexión para la recuperación frente a un problema. Por ejemplo, la recuperación de la base de datos, por lo general, requiere la recuperación de archivos de registro archivados que actualmente no están en línea.

La programación de una copia de seguridad depende de varios factores:

- La identificación de aplicaciones críticas que requieren ciclos de copia de seguridad más frecuentes dentro de un período de tiempo dado.
- Los objetivos de punto de recuperación y tiempo de recuperación. Evalúe qué tan preciso debe ser el punto de recuperación y cuánto tiempo está dispuesto a esperar por él.
- La tasa de cambio (RoC) asociada con los datos. Por ejemplo, si utiliza la replicación sincrónica/asincrónica, la RoC afecta la cantidad de ancho de banda necesaria entre los dispositivos de almacenamiento principales y secundarios.
- El impacto general en un entorno de SAN, el rendimiento del almacenamiento (durante la realización de la copia de seguridad) y otras aplicaciones.
- La identificación de períodos de tráfico pico en la SAN (las copias de seguridad programadas durante esos períodos pico pueden ralentizar las aplicaciones y el proceso de copia de seguridad).
- El tiempo para programar todas las copias de seguridad en el centro de datos.
- El tiempo que demora realizar una copia de seguridad de una aplicación individual.

- La disponibilidad de recursos para el archivo de datos; generalmente, acceso a soporte físico sin conexión (cinta).

Incluya un objetivo de tiempo de recuperación para cada aplicación cuando diseñe la estrategia de copia de seguridad. Es decir, tenga en cuenta el tiempo y los recursos necesarios para realizar una copia de seguridad. Por ejemplo, si una copia de seguridad programada almacena tantos datos que la recuperación requiere una cantidad de tiempo considerable, examine la copia de seguridad programada. Realice la copia de seguridad con más frecuencia, para que la copia de seguridad que se haga incluya menos datos por vez y disminuya así el tiempo de recuperación.

Si una aplicación en especial requiere la recuperación dentro de un marco de tiempo determinado, el proceso de copia de seguridad debe proporcionar una programación cronológica y un procesamiento de datos específicos para cumplir con este requisito. La recuperación rápida puede requerir el uso de volúmenes de recuperación que residen en el almacenamiento en línea para minimizar o eliminar la necesidad de acceder a un soporte físico sin conexión lento en busca de componentes de datos faltantes.

Usar paquetes de copia de seguridad de terceros

Es posible utilizar soluciones de copia de seguridad de terceros para proteger los datos del sistema, de las aplicaciones y de los usuarios en las máquinas virtuales.

VMware ofrece Storage APIs - Data Protection para trabajar junto con los productos de terceros. Cuando utiliza las API, el software de terceros puede realizar copias de seguridad sin cargar los hosts ESXi con el procesamiento de tareas de copia de seguridad.

Los productos de terceros que utilizan Storage APIs - Data Protection pueden realizar las tareas de copia de seguridad siguientes:

- Realizar una copia de seguridad de imagen incremental, diferencial y completa, y restauración de las máquinas virtuales.
- Realizar una copia de seguridad en el nivel de los archivos de las máquinas virtuales que utilizan sistemas operativos Windows y Linux compatibles.
- Garantizar la consistencia de los datos con servicios de instantáneas de volumen (VVS) de Microsoft para máquinas virtuales que ejecutan sistemas operativos Microsoft Windows.

Dado que Storage APIs - Data Protection aprovecha las capacidades de instantánea de VMFS, las copias de seguridad que se pueden realizar no requieren tiempo de inactividad de las máquinas virtuales. Estas copias de seguridad se realizan sin interrupciones, pueden llevarse a cabo en cualquier momento y no necesitan ventanas de copia de seguridad extendidas.

Para obtener información sobre Storage APIs - Data Protection y la integración con los productos de copia de seguridad, consulte el sitio web de VMware o póngase en contacto con el proveedor de copias de seguridad.

Usar ESXi con SAN de canal de fibra

3

Al configurar hosts ESXi para que usen matrices de almacenamiento SAN de canal de fibra, se deben tener en cuenta algunas consideraciones especiales. En esta sección se incluye información introductoria sobre la forma de usar ESXi con una matriz SAN de canal de fibra.

Este capítulo incluye los siguientes temas:

- [Conceptos de SAN de canal de fibra](#)
- [Usar la división en zonas con las SAN de canal de fibra](#)
- [Cómo acceden las máquinas virtuales a los datos en una SAN de canal de fibra](#)

Conceptos de SAN de canal de fibra

Si es un administrador de ESXi que planifica configurar hosts para que trabajen junto con SAN, debe tener un conocimiento práctico de los conceptos de SAN. Puede encontrar información sobre SAN impresa y en Internet. Debido a que esta industria está en permanente cambio, es conveniente consultar estos recursos con frecuencia.

Si hace poco tiempo que conoce la tecnología SAN, recomendamos que se familiarice con la terminología básica.

Una red de área de almacenamiento (SAN) es una red de alta velocidad especializada que conecta sistemas informáticos o servidores de hosts con subsistemas de almacenamiento de alto rendimiento. Entre los componentes de SAN se encuentran adaptadores de bus de host (HBA) en los servidores del host, conmutadores que ayudan a enrutar el tráfico de almacenamiento, cables, procesadores de almacenamiento (SP) y matrices de discos de almacenamiento.

Una topología SAN con al menos un conmutador presente en la red forma un tejido SAN.

Para transferir tráfico de los servidores de host al almacenamiento compartido, la SAN utiliza el protocolo de canal de fibra (FC), que empaqueta comandos SCSI en tramas de canal de fibra.

Para restringir el acceso del servidor a las matrices de almacenamiento no asignadas a ese servidor, la SAN utiliza la división en zonas. Por lo general, se crean zonas para cada grupo de servidores que accede a un grupo compartido de dispositivos de almacenamiento y LUN. Las zonas definen cuáles HBA pueden conectarse a cuáles SP. Los dispositivos fuera de una zona no son visibles para los dispositivos incluidos en ella.

La división en zonas es similar al enmascaramiento de LUN que, por lo general, se utiliza para la administración de permisos. El enmascaramiento de LUN es un proceso mediante el cual se permite que un LUN esté disponible para ciertos hosts y no lo esté para otros.

Al transferir datos entre el almacenamiento y el servidor del host, la SAN utiliza una técnica denominada múltiples rutas. La función de múltiples rutas permite contar con más de una ruta de acceso física desde el host ESXi hasta el LUN de un sistema de almacenamiento.

Por lo general, una sola ruta de acceso de un host a un LUN está compuesta por un HBA, puertos de conmutación, cables de conexión y el puerto de la controladora de almacenamiento. Si cualquier componente de la ruta de acceso presenta errores, el host selecciona otra ruta disponible para E/S. El proceso de detección de una ruta de acceso con errores se denomina conmutación por error de la ruta de acceso.

Puertos en SAN de canal de fibra

En el contexto de este documento, un puerto es la conexión de un dispositivo a la SAN. Cada nodo de la SAN, como un host, un dispositivo de almacenamiento o un componente del tejido, tiene uno o más puertos que lo conectan a la SAN. Los puertos se identifican de varias formas.

WWPN (World Wide Port Name)

Un identificador único global de un puerto que permite que ciertas aplicaciones accedan al puerto. Los conmutadores de FC detectan el WWPN de un dispositivo o un host y asignan una dirección de puerto al dispositivo.

Port_ID (o dirección de puerto)

Dentro de una SAN, cada puerto tiene un identificador de puerto único que actúa como la dirección de FC del puerto. Este identificador único permite el enrutamiento de datos a través de la SAN a ese puerto. Los conmutadores de FC asignan el identificador de puerto cuando el dispositivo inicia sesión en el tejido. El identificador de puerto es válido solo mientras el dispositivo esté conectado.

Cuando se utiliza la virtualización de identificador de puerto N (NPIV), un único puerto de HBA de FC (N-port) puede registrarse en el tejido con varios WWPN. Este método permite que un puerto N reclame varias direcciones de tejido, cada una de las cuales aparece como una entidad única. Cuando los hosts ESXi utilizan una SAN, estos identificadores varios y únicos permiten la asignación de WWN a máquinas virtuales individuales como parte de la configuración.

Tipos de matrices de almacenamiento de canal de fibra

ESXi admite diferentes tipos de sistemas y matrices de almacenamiento.

Entre los tipos de almacenamiento que admite un host se encuentran activo-activo, activo-pasivo y compatible con ALUA.

Sistema de almacenamiento activo-activo

Permite acceder simultáneamente a los LUN en todos los puertos de almacenamiento que están disponibles sin una degradación significativa del rendimiento. Todas las rutas de acceso están activas en todo momento, a menos que una de ellas falle.

Sistema de almacenamiento activo-pasivo

Un sistema en el cual un procesador de almacenamiento proporciona acceso de forma activa a un LUN determinado. Los otros procesadores actúan como copia de seguridad del LUN y pueden proporcionar acceso activamente a otras operaciones de E/S del LUN. Las operaciones de E/S pueden enviarse correctamente solo a un puerto activo de un LUN determinado. Si el acceso a través del puerto de almacenamiento activo genera errores, uno de los procesadores de almacenamiento pasivos puede activarse mediante los servidores que acceden a él.

Sistema de almacenamiento asimétrico

Admite acceso asimétrico a unidades lógicas (ALUA). Los sistemas de almacenamiento compatibles con ALUA ofrecen diferentes niveles de acceso por puerto. ALUA permite que los hosts determinen los estados de los puertos de destino y prioricen rutas de acceso. El host utiliza algunas de las rutas de acceso activas como principales y otras como secundarias.

Usar la división en zonas con las SAN de canal de fibra

La división en zonas proporciona control de acceso en la topología de la SAN. La división en zonas define qué HBA pueden conectarse a cuáles destinos. Cuando configura una SAN con la división en zonas, los dispositivos fuera de una zona no son visibles para los dispositivos dentro de la zona.

La división en zonas tiene los efectos siguientes:

- Disminuye la cantidad de destinos y LUN que se presentan a un host.
- Controla y aísla las rutas en un tejido.
- Puede evitar que otros sistemas que no sean ESXi accedan a un sistema de almacenamiento en especial y que, posiblemente, destruyan los datos de VMFS.
- Se puede usar para separar distintos entornos, por ejemplo, uno de prueba de uno de producción.

Con hosts ESXi, use una división en zonas de un solo iniciador o una división en zonas de un solo destino y un solo iniciador. La última opción es una de las divisiones en zonas preferidas. El uso de una división en zonas más restrictiva evita problemas y errores de configuración que pueden suceder en la SAN.

Para obtener instrucciones detalladas y las mejores prácticas de la división en zonas, póngase en contacto con los proveedores del conmutador o de las matrices de almacenamiento.

Cómo acceden las máquinas virtuales a los datos en una SAN de canal de fibra

ESXi almacena los archivos del disco de una máquina virtual en un almacén de datos de VMFS que reside en un dispositivo de almacenamiento SAN. Cuando los sistemas operativos invitados de la máquina virtual emiten comandos SCSI a sus discos virtuales, la capa de virtualización SCSI traduce esos comandos a operaciones de archivos VMFS.

Cuando una máquina virtual interactúa con su disco virtual almacenado en una SAN, se llevan a cabo los siguientes procesos:

- 1 Cuando el sistema operativo invitado en una máquina virtual lee o escribe en un disco SCSI, emite comandos SCSI al disco virtual.
- 2 Los controladores de dispositivos en el sistema operativo de la máquina virtual se comunican con las controladoras SCSI virtuales.
- 3 La controladora SCSI virtual reenvía el comando al VMkernel.
- 4 El VMkernel realiza las siguientes tareas.
 - a Ubica el archivo en el volumen que corresponde al disco de la máquina virtual invitada.
 - b Asigna las solicitudes de los bloques en el disco virtual en bloques del dispositivo físico apropiado.
 - c Envía la solicitud de E/S modificada del controlador del dispositivo en el VMkernel al HBA físico.
- 5 El HBA físico realiza las siguientes tareas.
 - a Empaqueta la solicitud de E/S según las reglas del protocolo de FC.
 - b Transmite la solicitud a la SAN.
- 6 Según el puerto que utilice el HBA para conectarse con el tejido, uno de los conmutadores de la SAN recibe la solicitud y la enruta al dispositivo de almacenamiento al que desea acceder el host.

Configurar almacenamiento de canal de fibra

4

Cuando se utilizan sistemas ESXi con almacenamiento SAN, existen requisitos de hardware y de sistema específicos.

Este capítulo incluye los siguientes temas:

- [ESXi](#)
- [Pasos de instalación y configuración](#)
- [Virtualizar identificador de puerto N](#)

ESXi

Como preparación para configurar la SAN y el sistema ESXi para que utilice almacenamiento SAN, repase los requisitos y las recomendaciones.

- Asegúrese de que las combinaciones de hardware y firmware de almacenamiento SAN que utiliza sean compatibles junto con los sistemas ESXi. Para acceder a una lista actualizada, consulte *Guía de compatibilidad de VMware*.
- Configure el sistema para que tenga un solo volumen VMFS por LUN.
- A menos que esté utilizando servidores sin discos, no configure la partición de diagnóstico en un LUN de SAN.

En el caso de servidores sin discos que arranquen desde una SAN, es apropiado usar una partición de diagnóstico compartida.

- Use RDM para acceder a discos sin formato. Para obtener información, consulte [Capítulo 18 Asignación de dispositivos sin formato](#).
- Para que la funcionalidad de múltiples rutas funcione adecuadamente, cada LUN debe presentar el mismo número de identificador de LUN para todos los hosts ESXi.
- Asegúrese de que el controlador del dispositivo de almacenamiento especifique una cola lo suficientemente extensa. Puede establecer la profundidad de la cola del HBA físico durante la configuración del sistema. Para obtener información sobre la forma de cambiar la profundidad de la cola de HBA y máquinas virtuales, consulte la documentación de *Solución de problemas de vSphere*.

- En máquinas virtuales con Microsoft Windows, aumente el valor del parámetro `TimeoutValue` de SCSI a 60. Este aumento permite que Windows tolere mejor las E/S retrasadas que son consecuencia de la conmutación por error de las rutas de acceso. Para obtener información, consulte [Establecer el tiempo de espera en un sistema operativo invitado Windows](#).

Restricciones de SAN de canal de fibra de ESXi

Cuando se utiliza ESXi con una SAN, aplican ciertas restricciones.

- ESXi no es compatible con dispositivos de cinta conectados a FC.
- No se puede utilizar software de múltiples rutas dentro de una máquina virtual para realizar el equilibrio de carga de E/S de un único LUN físico. Sin embargo, cuando la máquina virtual de Microsoft Windows utiliza discos dinámicos, esta restricción no aplica. Para obtener información sobre la configuración de discos dinámicos, consulte [Configurar reflejo de discos dinámico](#).

Establecer asignaciones de LUN

Este tema brinda información general sobre cómo asignar LUN cuando ESXi trabaja junto con SAN.

Cuando configura asignaciones de LUN, tenga en cuenta lo siguiente:

Aprovisionamiento de almacenamiento

Para garantizar que el sistema ESXi reconozca los LUN en el momento del inicio, provisione todos los LUN en los HBA adecuados antes de conectar la SAN al sistema ESXi.

VMware recomienda que provisione todos los LUN a todos los HBA de ESXi al mismo tiempo. La conmutación por error de HBA funciona solo si todos los HBA ven los mismos LUN.

En el caso de los LUN que se compartirán entre varios hosts, asegúrese de que los identificadores de LUN sean coherentes en todos los hosts. Por ejemplo, el LUN 5 debe estar asignado al host 1, host 2 y host 3 como LUN 5.

vMotion y DRS de VMware

Cuando usa vCenter Server y vMotion o DRS, asegúrese de que los LUN de las máquinas virtuales se provisionen en todos los hosts ESXi. Esto proporciona la mayor habilidad para mover máquinas virtuales.

Matrices activa-activa en comparación con activa-pasiva

Cuando use vMotion o DRS con un dispositivo de almacenamiento SAN activo-pasivo, asegúrese de que todos los sistemas ESXi tengan rutas de acceso coherentes con todos procesadores de almacenamiento. Si no lo hace, puede provocar la destrucción de las rutas de acceso cuando se produzca una migración de vMotion.

En el caso de las matrices de almacenamiento activo-pasivo que no figuran en Compatibilidad con almacenamiento/SAN, VMware no admite la conmutación por error de puerto de almacenamiento. En esos casos, debe conectar el servidor al puerto activo en la matriz de almacenamiento. Esta configuración garantiza que los LUN se presenten al host ESXi.

Establecer los HBA de canal de fibra

Por lo general, los HBA de canal de fibra que se utilizan en el host ESXi funcionan correctamente con las opciones de configuración predeterminadas.

Debe seguir las instrucciones de configuración proporcionadas por el proveedor de la matriz de almacenamiento. Durante la configuración del HBA de canal de fibra, tenga en cuenta lo siguiente.

- No combine HBA de canal de fibra de diferentes proveedores en un solo host. Se admiten diferentes modelos del mismo HBA, pero no se puede acceder a un solo LUN con dos tipos de HBA diferentes; eso solo es posible a través del mismo tipo de HBA.
- Asegúrese de que el nivel de firmware en cada HBA sea el mismo.
- Establezca el valor de tiempo de espera para detectar la conmutación por error. Para garantizar un rendimiento óptimo, no cambie el valor predeterminado.
- ESXi admite 16 GB de conectividad de canal de fibra de extremo a extremo.

Pasos de instalación y configuración

En este tema se ofrece una descripción general de los pasos de instalación y configuración que se deben seguir al configurar el entorno de SAN para que funcione con ESXi.

Siga estos pasos para configurar el entorno de SAN de ESXi.

- 1 Si aún no está configurada, debe diseñar la SAN. La mayoría de las SAN existentes requieren solo modificaciones menores para funcionar con ESXi.
- 2 Compruebe que todos los componentes de la SAN cumplan con los requisitos.
- 3 Realice todas las modificaciones necesarias en la matriz de almacenamiento.

La mayoría de los proveedores poseen documentación específica para configurar una SAN de modo que funcione junto con VMware ESXi.
- 4 Configure los HBA para los hosts que conectó a la SAN.
- 5 Instale ESXi en los hosts.
- 6 Cree máquinas virtuales e instale sistemas operativos invitados.
- 7 (Opcional) Configure el sistema para la conmutación por error de VMware HA o para utilizar Microsoft Clustering Services.
- 8 Actualice o modifique el entorno según sea necesario.

Virtualizar identificador de puerto N

La virtualización de identificador de puerto N (NPIV) es un estándar ANSI T11 que describe cómo un puerto HBA de canal de fibra único puede registrarse con el tejido usando varios nombres de puertos universales (WWPN). Esto permite que un puerto N ligado a un tejido reclame varias direcciones de tejido. Cada dirección aparece como entidad única en el tejido de canal de fibra.

Funcionamiento del acceso al LUN basado en NPIV

NPIV permite que un solo puerto HBA de FC registre varias WWN únicas en el tejido y cada una de ellas puede asignarse a una máquina virtual individual.

Se pueden asignar identificadores World Wide Name (WWN) a objetos SAN, como conmutadores, HBA, dispositivos de almacenamiento o máquinas virtuales. Los WWN son una identificación única para estos objetos en el tejido del canal de fibra. Cuando las máquinas virtuales tienen asignaciones de WWN, las utilizan para todo el tráfico de RDM, de forma tal que los LUN a los que apuntan cualquiera de los RDM en la máquina virtual no puedan enmascarse contra sus WWN. Cuando las máquinas virtuales no tienen asignaciones de WWN, acceden a los LUN de almacenamiento con los WWN de los HBA físicos del host. Sin embargo, al utilizar NPIV, el administrador de SAN puede supervisar y enrutar el acceso de almacenamiento por máquina virtual. En la siguiente sección se describe cómo funciona este procedimiento.

Cuando se le asigna un WWN a una máquina virtual, el archivo de configuración (.vmx) de la máquina virtual se actualiza para incluir un par de WWN, que consta de un nombre de puerto World Wide Port Name (WWPN) y un nombre de nodo World Wide Node Name (WWNN). Cuando se enciende esa máquina virtual, el VMkernel crea una instancia de puerto virtual (VPORT) en el HBA físico que se utiliza para acceder al LUN. El VPORT es un HBA virtual que aparece ante el tejido de FC como un HBA físico, es decir, tiene su propio identificador único: el par de WWN que se asignó a la máquina virtual. Cada VPORT es específico de la máquina virtual. Los VPORT se destruyen en el host y ya no aparecen en el tejido de FC cuando se apaga la máquina virtual. Cuando se migra una máquina virtual de un host a otro, el VPORT se cierra en el primer host y se abre en el host de destino.

Si NPIV está habilitado, se especifican los pares de WWN (WWPN y WWNN) para cada máquina virtual en el momento de su creación. Cuando se enciende una máquina virtual con NPIV, la máquina utiliza cada uno de estos pares de WWN en secuencia para intentar detectar una ruta de acceso al almacenamiento. La cantidad de VPORT de los que se crea una instancia equivale a la cantidad de HBA físicos presentes en el host. Se crea un VPORT en cada HBA físico donde se encuentra una ruta de acceso física. Se usa cada ruta de acceso física para determinar la ruta de acceso virtual que se utilizará para acceder al LUN. Tenga en cuenta que los HBA que no tienen reconocimiento de NPIV se omiten en este proceso de detección, ya que no pueden crearse instancias de VPORT en ellos.

Requisitos para utilizar NPIV

Si planea habilitar NPIV en las máquinas virtuales, debe conocer ciertos requisitos.

Existen los requisitos siguientes:

- NPIV puede usarse solo con las máquinas virtuales que tienen RDM. Las máquinas virtuales que tienen discos virtuales normales usan los WWN de los HBA físicos del host.
- Los HBA del host deben ser compatibles con NPIV.

Para obtener información, consulte la *Guía de compatibilidad de VMware* y la documentación del proveedor.

- Use HBA del mismo tipo, todos QLogic o todos Emulex. VMware no admite que HBA heterogéneos en el mismo host accedan a los mismos LUN.
- Si un host usa varios HBA físicos como rutas al almacenamiento, divida en zonas todas las rutas físicas a la máquina virtual. Esto es necesario para admitir múltiples rutas, a pesar de que solo habrá una ruta de acceso activa a la vez.
- Asegúrese de que los HBA físicos en el host tengan acceso a todos los LUN a los que deben acceder las máquinas virtuales que admiten NPIV que se ejecutan en ese host.
- Los conmutadores en el tejido deben tener reconocimiento de NPIV.
- Cuando configure un LUN para el acceso de NPIV en el nivel del almacenamiento, asegúrese de que el número LUN de NPIV y el identificador de destino de NPIV coincidan con el LUN y el identificadores de destino físicos.

Funcionalidades y limitaciones de NPIV

Obtenga información sobre las capacidades y las limitaciones de la utilización de NPIV con ESXi.

ESXi con NPIV es compatible con:

- NPIV es compatible con vMotion. Cuando se utiliza vMotion para migrar una máquina virtual, se retiene el WWN asignado.

Si migra una máquina virtual basada en NPIV a un host que no es compatible con NPIV, el VMkernel vuelve a utilizar un HBA físico para enrutar las operaciones de E/S.
- Si el entorno de SAN de canal de fibra admite E/S simultáneas en los discos de una matriz activa-activa, también se admiten operaciones de E/S simultáneas en dos puertos de NPIV diferentes.

Cuando se utiliza ESXi con NPIV, se aplican las siguientes limitaciones:

- Debido a que la tecnología NPIV es una extensión del protocolo de FC, requiere un conmutador de canal de fibra y no funciona en los discos de canal de fibra de conexión directa.
- Cuando se clonan una máquina virtual o una plantilla con un WWN asignado, los clones no retienen el WWN.
- NPIV no es compatible con Storage vMotion.

- Deshabilitar y volver a habilitar la funcionalidad de NPIV en un conmutador de canal de fibra con máquinas virtuales en ejecución puede provocar errores en un vínculo de canal de fibra y la interrupción de las operaciones de E/S.

Asignar WWN a máquinas virtuales

Asigne la configuración de WWN a máquinas virtuales con un disco RDM.

Puede crear entre 1 y 16 pares de WWN, que pueden asignarse a los primeros 1 a 16 HBA de FC físicos en el host.

Requisitos previos

Cree una máquina virtual con un disco RDM. Consulte [Crear máquinas virtuales con RDM](#).

Procedimiento

- 1 En vSphere Web Client, desplácese hasta la máquina virtual.
- 2 Haga clic con el botón derecho en la máquina virtual y seleccione **Edit Settings** (Editar configuración).
- 3 Haga clic en **VM Options** (Opciones de máquina virtual).
- 4 Haga clic en el triángulo de NPIV de canal de fibra para expandir las opciones de NPIV.
- 5 Desactive la casilla **Temporarily Disable NPIV for this virtual machine** (Deshabilitar NPIV temporalmente para esta máquina virtual).
- 6 Seleccione **Generate new WWNs** (Generar WWN nuevos).
- 7 Especifique la cantidad de WWNN y WWPN.

Se necesita un mínimo de 2 WWPN para admitir la conmutación por error con NPIV. Por lo general, se crea 1 solo WWNN para cada máquina virtual.

Resultados

El host crea asignaciones de WWN para la máquina virtual.

Pasos siguientes

Registre los WWN recientemente creados en el tejido para que la máquina virtual pueda iniciar sesión en el conmutador y asignar LUN de almacenamiento a los WWN.

Modificar asignaciones de WWN

Se pueden modificar las asignaciones de WWN de una máquina virtual con un RDM.

En general, no es necesario cambiar las asignaciones de WWN existentes en la máquina virtual. En determinadas circunstancias, por ejemplo, cuando los WWN asignados manualmente provocan conflictos en la SAN, es posible que deba cambiar o quitar los WWN.

Requisitos previos

Asegúrese de apagar la máquina virtual si desea editar los WWN existentes.

Antes de comenzar, asegúrese de que el administrador de SAN haya aprovisionado la ACL del LUN de almacenamiento para permitir que el host ESXi de la máquina virtual pueda acceder a él.

Procedimiento

- 1 Para abrir el cuadro de diálogo Virtual Machine Properties (Propiedades de la máquina virtual), haga clic en el vínculo **Edit Settings** (Editar configuración) de la máquina virtual seleccionada.
- 2 Haga clic en la pestaña **Options** (Opciones) y seleccione **Fibre Channel NPIV** (NPIV de canal de fibra).

Se abre el cuadro de diálogo Virtual Machine Properties (Propiedades de la máquina virtual).

- 3 Para editar las asignaciones de WWN, seleccione una de las siguientes opciones:

Opción	Descripción
Temporarily disable NPIV for this virtual machine (Deshabilitar NPIV temporalmente para esta máquina virtual)	Se deshabilitan las asignaciones de WWN para la máquina virtual.
Leave unchanged (Dejar sin modificaciones)	Se conservan las asignaciones de WWN existentes. En este cuadro de diálogo, la sección WWN Assignments (Asignaciones de WWN) de solo lectura muestra los valores de puerto y nodo de las asignaciones de WWN existentes.
Generate new WWNs (Generar nuevos WWN)	Se generan nuevos WWN y se asignan a la máquina virtual; por lo tanto, se anulan los WWN existentes (los del HBA no se ven afectados).
Remove WWN assignment (Quitar la asignación de WWN)	Los WWN asignados a la máquina virtual son eliminados y se utilizan los WWN del HBA para acceder al LUN de almacenamiento. Esta opción no está disponible al crear una máquina virtual.

- 4 Haga clic en **OK** (Aceptar) para guardar los cambios.

Configurar el canal de fibra en Ethernet

5

Para acceder al almacenamiento de canal de fibra, un host ESXi puede utilizar el protocolo de canal de fibra en Ethernet (FCoE).

El protocolo FCoE encapsula las tramas de canal de fibra en tramas Ethernet. Como resultado, el host no necesita vínculos de canal de fibra especiales para conectarse al almacenamiento de canal de fibra, pero puede utilizar Ethernet sin pérdida de 10 Gbit para entregar el tráfico del canal de fibra.

Este capítulo incluye los siguientes temas:

- [Adaptadores de canal de fibra en Ethernet](#)
- [Instrucciones de configuración para FCoE de software](#)
- [Configurar redes para FCoE de software](#)
- [Agregar adaptadores de FCoE de software](#)

Adaptadores de canal de fibra en Ethernet

Para usar canal de fibra en Ethernet (FCoE), debe instalar adaptadores de FCoE en el host.

Los adaptadores que VMware admite generalmente corresponden a dos categorías, adaptadores de FCoE de hardware y adaptadores de FCoE de software que usan la pila de FCoE nativa en ESXi.

Adaptadores de FCoE de hardware

Esta categoría incluye adaptadores de red convergentes (CNA) especializados y completamente descargados que contienen funcionalidades de red y canal de fibra en la misma tarjeta.

Cuando se instala este tipo de adaptadores, el host detecta y puede usar ambos componentes del CNA. En el cliente, el componente de red aparece como un adaptador de red estándar (vmnic) y el componente de canal de fibra como un adaptador de FCoE (vmhba). No es necesario que configure el adaptador de FCoE de hardware para poder usarlo.

Adaptadores de FCoE de software

Un adaptador de FCoE de software usa la pila de protocolo de FCoE nativa en ESXi para el procesamiento del protocolo. El adaptador de FCoE de software se usa con una NIC que ofrece capacidades de descarga de E/S y de protocolo Data Center Bridging (DCB). Intel X520 es un ejemplo de este tipo de NIC. Para obtener información sobre las NIC que admiten FCoE de software, consulte la *Guía de compatibilidad de VMware*.

En el caso del adaptador de FCoE de software, debe configurar correctamente la red y, a continuación, activar el adaptador.

Nota La cantidad de adaptadores de FCoE de software que activa corresponden a la cantidad de puertos de NIC físicos. ESXi admite un máximo de cuatro adaptadores de FCoE de software en un host.

Instrucciones de configuración para FCoE de software

Al configurar el entorno de red para que funcione con FCoE de software de ESXi, siga las instrucciones y las prácticas recomendadas que ofrece VMware.

Instrucciones para conmutadores de red

Siga estas instrucciones al configurar un conmutador de red para el entorno de FCoE de software:

- En los puertos que se comunican con el host ESXi, deshabilite el protocolo de árbol de expansión (Spanning Tree Protocol, STP). Habilitar el STP puede retrasar la respuesta del protocolo de inicialización (FCoE Initialization Protocol, FIP) en el conmutador y provocar una condición en la que todas las rutas de acceso quedan inactivas (All Paths Down, APD).

FIP es un protocolo que usa FCoE para detectar e inicializar entidades FCoE en Ethernet.
- Active el control de flujo basado en prioridades (Priority-based Flow Control, PFC) y establézcalo en AUTO (Automático).
- Asegúrese de tener una versión de firmware compatible en el conmutador FCoE.

Prácticas recomendadas del adaptador de red

Si planea habilitar los adaptadores FCoE de software para que funcionen con adaptadores de red, debe tener en cuenta algunas consideraciones especiales.

- Compruebe que esté instalado el microcódigo más reciente en el adaptador de red FCoE.
- Al configurar las redes, debe agregar cada puerto a un conmutador virtual distinto si el adaptador de red tiene varios puertos. Esta práctica ayuda a evitar una condición APD en caso de que se produzca un evento disruptivo, como un cambio de MTU.
- No mueva un puerto de adaptador de red de un conmutador virtual a otro cuando hay tráfico FCoE activo. Si debe realizar este cambio, vuelva a arrancar el host posteriormente.

- Si cambió el conmutador virtual por un puerto de adaptador de red y provocó un error, vuelva a colocar el puerto en el conmutador virtual original para resolver el problema.

Configurar redes para FCoE de software

Antes de activar los adaptadores FCoE de software, se deben crear adaptadores de red VMkernel para todas las NIC de FCoE instaladas en el host.

Este procedimiento explica cómo crear un solo adaptador de red VMkernel conectado a un solo adaptador de red físico FCoE a través de un conmutador estándar de vSphere. Si el host tiene varios adaptadores de red o varios puertos en el adaptador, conecte cada NIC de FCoE a un conmutador estándar distinto. Para obtener más información, consulte la documentación de *Redes de vSphere*.

Nota ESXi admite el uso de hasta cuatro puertos de adaptador de red para FCoE de software.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en **Acciones > Agregar redes**.
- 3 Seleccione **Adaptador de red de VMkernel** y haga clic en **Siguiente**.
- 4 Seleccione **Nuevo conmutador estándar** para crear un conmutador estándar de vSphere.
- 5 En Unclaimed Adapters (Adaptadores sin reclamar), seleccione el adaptador de red (vmnic#) compatible con FCoE y haga clic en **Assign** (Asignar).

Asegúrese de asignar el adaptador a Active Adapters (Adaptadores activos).

- 6 Introduzca una etiqueta de red.

La etiqueta de red es un nombre simple que identifica el adaptador de VMkernel que se está creando, por ejemplo, FCoE.

- 7 Especifique un identificador de VLAN y haga clic en **Next** (Siguiente).

Dado que el tráfico FCoE requiere una red aislada, asegúrese de que el identificador de VLAN que especifica sea diferente del que se usa para el tráfico de redes común del host. Para obtener más información, consulte la documentación de *Redes de vSphere*.

- 8 Después de completar la configuración, revise la información y haga clic en **Finish** (Finalizar).

Resultados

Creó el adaptador de VMkernel virtual para el adaptador de red de FCoE físico instalado en el host.

Nota Para evitar las interrupciones del tráfico de FCoE, no quite el adaptador de red de FCoE (vmnic#) del conmutador estándar de vSphere después de configurar las redes de FCoE.

Agregar adaptadores de FCoE de software

Es necesario activar los adaptadores de FCoE de software para que el host pueda utilizarlos para acceder al almacenamiento de canal de fibra.

La cantidad de adaptadores de FCoE de software que se puede activar corresponde a la cantidad de puertos de NIC de FCoE físicos en el host. ESXi admite un máximo de cuatro adaptadores de FCoE de software en un host.

Requisitos previos

Configure las redes del adaptador de FCoE de software.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y, a continuación, en el icono **Agregar** (+).
- 4 Seleccione **Software FCoE Adapter** (Adaptador de FCoE de software).
- 5 En el cuadro de diálogo Add Software FCoE Adapter (Agregar adaptador de FCoE de software), seleccione una vmnic en la lista desplegable de adaptadores de red físicos.

Solo aparecen los adaptadores que aún no se utilizan para el tráfico de FCoE.
- 6 Haga clic en **OK** (Aceptar).

El adaptador de FCoE de software aparece en la lista de adaptadores de almacenamiento.

Resultados

Una vez activado el adaptador de FCoE de software, es posible ver sus propiedades. Si no utiliza el adaptador, puede eliminarlo de la lista de adaptadores.

Arrancar ESXi desde una SAN de canal de fibra

6

Cuando se configura el host para arrancar desde una SAN, la imagen de arranque del host se almacena en uno o más LUN en el sistema de almacenamiento SAN. Cuando el host arranca, lo hace desde el LUN en la SAN, no desde su disco local.

ESXi admite el arranque a través de un adaptador de bus host (HBA) de canal de fibra o un adaptador de red convergente (CNA) de canal de fibra en Ethernet (FCoE).

Este capítulo incluye los siguientes temas:

- [Beneficios del arranque desde SAN](#)
- [Requisitos y consideraciones sobre el arranque desde SAN de canal de fibra](#)
- [Prepararse para el arranque desde SAN](#)
- [Configurar HBA de Emulex para arrancar desde SAN](#)
- [Configurar HBA de QLogic para arrancar desde SAN](#)

Beneficios del arranque desde SAN

El arranque desde SAN puede ofrecer numerosos beneficios para el entorno. No obstante, en ciertos casos no debe utilizar el arranque desde SAN para hosts ESXi. Antes de configurar el sistema para el arranque desde SAN, decida si es apropiado para el entorno.

Precaución Cuando utiliza el arranque desde SAN con varios hosts ESXi, cada host debe tener su propio LUN de arranque. Si configura varios hosts para que compartan el mismo LUN de arranque, es probable que se produzcan daños en la imagen de ESXi.

Si utiliza el arranque desde SAN, algunos de los beneficios para el entorno son los siguientes:

- **Servidores más económicos.** Los servidores pueden ser más densos y funcionar con menos temperatura sin almacenamiento interno.
- **Reemplazo más sencillo de los servidores.** Cuando reemplaza servidores, el nuevo servidor puede apuntar a la ubicación de arranque anterior.
- **Menos espacio desperdiciado.** Con frecuencia, los servidores sin discos locales ocupan menos espacio.

- Procesos más sencillos de copia de seguridad. Puede realizar copias de seguridad de imágenes de arranque del sistema en la SAN como parte de los procedimientos generales de copia de seguridad de la SAN. Además, puede utilizar características avanzadas de la matriz, como instantáneas en la imagen de arranque.
- Administración mejorada. Crear y administrar la imagen del sistema operativo es más sencillo y eficiente.
- Mayor confiabilidad. Puede acceder al disco de arranque a través de múltiples rutas, lo que protege al disco y evita que sea un único punto de error.

Requisitos y consideraciones sobre el arranque desde SAN de canal de fibra

La configuración de arranque de ESXi debe cumplir requisitos específicos.

Tabla 6-1. Requisitos para arranque desde SAN

Requisito	Descripción
Requisitos del sistema ESXi	Siga la recomendación del proveedor sobre el arranque del servidor desde una SAN.
Requisitos del adaptador	Habilite y configure correctamente el adaptador, para que pueda acceder al LUN de arranque. Consulte la documentación del proveedor.
Control de acceso	<ul style="list-style-type: none"> ■ Cada host debe tener acceso solo a su propio LUN de arranque, no a los LUN de arranque de otros hosts. Utilice el software del sistema de almacenamiento para asegurarse de que el host acceda solo a los LUN designados. ■ Varios servidores pueden compartir una partición de diagnóstico. Se puede utilizar el enmascaramiento de LUN específico de matriz para lograr esto.
Compatibilidad con múltiples rutas	No se pueden habilitar múltiples rutas para un LUN de arranque en matrices activas-pasivas porque el BIOS no admite múltiples rutas y no puede activar una ruta de acceso en espera.
Consideraciones sobre SAN	Las conexiones de SAN deben realizarse a través de una topología con conmutadores si la matriz no está certificada para la topología de conexión directa. Si la matriz está certificada para la topología de conexión directa, las conexiones de SAN pueden realizarse directamente a esa matriz. El arranque desde SAN se admite tanto en la topología con conmutadores como en la de conexión directa, si estas topologías están certificadas para la matriz específica.
Consideraciones específicas sobre hardware	Si ejecuta un IBM eServer BladeCenter y utiliza el arranque desde una SAN, debe deshabilitar las unidades IDE en los blades.

Prepararse para el arranque desde SAN

Cuando se configura el arranque desde un entorno de SAN, se deben realizar varias tareas.

Esta sección describe el proceso de habilitación genérico de arranque desde SAN en los servidores montados en bastidores. Para obtener información sobre cómo habilitar el arranque desde SAN en servidores blade FCoE Cisco Unified Computing System, consulte la documentación de Cisco.

Procedimiento

1 Configurar los componentes de la SAN y del sistema de almacenamiento

Antes de configurar el host ESXi para arrancar desde un LUN de SAN, configure los componentes de la SAN y un sistema de almacenamiento.

2 Configurar adaptador de almacenamiento para arrancar desde SAN

Cuando el host se configura para arrancar desde la SAN, se habilita el adaptador de arranque en el BIOS del host. A continuación, se debe configurar el adaptador de arranque para que inicie una conexión primitiva con el LUN de arranque de destino.

3 Configurar sistema para arrancar desde los medios de instalación

Al configurar el host para arrancar desde SAN, primero se debe arrancar el host desde el medio de instalación de VMware. Para lograrlo, se debe cambiar la secuencia de arranque del sistema en la configuración del BIOS.

Configurar los componentes de la SAN y del sistema de almacenamiento

Antes de configurar el host ESXi para arrancar desde un LUN de SAN, configure los componentes de la SAN y un sistema de almacenamiento.

Debido a que la configuración de componentes de la SAN es específica del proveedor, debe consultar la documentación del producto para cada elemento.

Procedimiento

1 Conecte el cable de red, consultando cualquier guía de cableado que se aplique a la instalación.

Revise el cableado del conmutador, si lo hubiera.

2 Configure la matriz de almacenamiento.

- a Desde la matriz de almacenamiento SAN, haga que el host ESXi sea visible para la SAN. Con frecuencia, este proceso se conoce como crear un objeto.
- b Desde la matriz de almacenamiento SAN, configure el host para que tenga los WWPN de los adaptadores del host como nombres de puerto o nombres de nodo.
- c Cree los LUN.
- d Asigne los LUN.

- e Registre las direcciones IP de los conmutadores y las matrices de almacenamiento.
- f Registre el WWPN de cada SP.

Precaución Si utilizó una instalación generada por script para que ESXi arranque en modo de SAN, debe seguir pasos especiales para evitar la pérdida no deseada de datos.

Configurar adaptador de almacenamiento para arrancar desde SAN

Cuando el host se configura para arrancar desde la SAN, se habilita el adaptador de arranque en el BIOS del host. A continuación, se debe configurar el adaptador de arranque para que inicie una conexión primitiva con el LUN de arranque de destino.

Requisitos previos

Determine el WWPN para el adaptador de almacenamiento.

Procedimiento

- ◆ Configure el adaptador de almacenamiento para que arranque desde la SAN.
Dado que la configuración de los adaptadores de arranque depende de cada distribuidor, se debe consultar la documentación del proveedor.

Configurar sistema para arrancar desde los medios de instalación

Al configurar el host para arrancar desde SAN, primero se debe arrancar el host desde el medio de instalación de VMware. Para lograrlo, se debe cambiar la secuencia de arranque del sistema en la configuración del BIOS.

Debido a que el procedimiento de cambio de la secuencia de arranque en el BIOS es específico de cada proveedor, consulte la documentación del proveedor para obtener instrucciones. A continuación, se explica cómo cambiar la secuencia de arranque en un host de IBM.

Procedimiento

- 1 Durante el encendido del sistema, entre a la utilidad de configuración/instalación del BIOS del sistema.
- 2 Seleccione **Startup Options** (Opciones de inicio) y presione Entrar.
- 3 Seleccione **Startup Sequence Options** (Opciones de la secuencia de inicio) y presione Entrar.
- 4 Cambie la opción **First Startup Device** (Primer dispositivo de inicio) a **[CD-ROM]**.

Resultados

Ahora ya puede instalar ESXi.

Configurar HBA de Emulex para arrancar desde SAN

La configuración del BIOS del HBA de Emulex para arrancar desde SAN incluye la habilitación del símbolo de BootBIOS y del BIOS.

Procedimiento

1 Habilitar el símbolo de BootBIOS

Al configurar el BIOS de HBA Emulex para que arranque ESXi desde SAN, se debe habilitar el símbolo de BootBIOS.

2 Habilitar el BIOS

Cuando configura el BIOS del HBA Emulex para que arranque ESXi desde SAN, debe habilitar el BIOS.

Habilitar el símbolo de BootBIOS

Al configurar el BIOS de HBA Emulex para que arranque ESXi desde SAN, se debe habilitar el símbolo de BootBIOS.

Procedimiento

- 1 Ejecute `lputil`.
- 2 Seleccione **3. Firmware Maintenance** (3. Mantenimiento de firmware).
- 3 Seleccione un adaptador.
- 4 Seleccione **6. BootBIOS Maintenance** (6. Mantenimiento de BootBIOS).
- 5 Seleccione **1. Enable BootBIOS** (1. Habilitar BootBIOS).

Habilitar el BIOS

Cuando configura el BIOS del HBA Emulex para que arranque ESXi desde SAN, debe habilitar el BIOS.

Procedimiento

- 1 Reinicie el host.
- 2 Para configurar los parámetros del adaptador, presione ALT+E en el símbolo de Emulex y siga estos pasos.
 - a Seleccione un adaptador (compatible con BIOS).
 - b Seleccione **2. Configure This Adapter's Parameters** (2. Configurar los parámetros de este adaptador).
 - c Seleccione **1. Enable or Disable BIOS** (1. Habilitar o deshabilitar el BIOS).
 - d Seleccione **1** para habilitar el BIOS.
 - e Seleccione **x** para salir y **Esc** para regresar al menú anterior.

- 3 Para configurar el dispositivo de arranque, siga estos pasos en el menú principal de Emulex.
 - a Seleccione el mismo adaptador.
 - b Seleccione **1. Configure Boot Devices** (1. Configurar dispositivos de arranque).
 - c Seleccione la ubicación de la entrada de arranque.
 - d Introduzca el dispositivo de arranque de dos dígitos.
 - e Introduzca el LUN de inicio de dos dígitos hexadecimales (por ejemplo, **08**).
 - f Seleccione el LUN de arranque.
 - g Seleccione **1. WWPN**. (Arranque este dispositivo con WWPN, no DID).
 - h Seleccione **x** para salir e **Y** para reiniciar.
- 4 Arranque en el BIOS del sistema y mueva Emulex al primer lugar en la secuencia de la controladora de arranque.
- 5 Reinícielo e instálelo en un LUN de SAN.

Configurar HBA de QLogic para arrancar desde SAN

Este procedimiento de muestra explica cómo configurar el HBA QLogic para arrancar ESXi desde SAN. El procedimiento implica habilitar el BIOS del HBA QLogic, habilitar el arranque seleccionable y seleccionar el LUN de arranque.

Procedimiento

- 1 Mientras arranca el servidor, presione **Ctrl+Q** para entrar a la utilidad de configuración Fast!UTIL.
- 2 Realice la acción adecuada según la cantidad de HBA.

Opción	Descripción
One HBA (Un HBA)	Si tiene un solo adaptador de bus host (HBA), aparece la página Fast!UTIL Options (Opciones de Fast!UTIL). Salte al Paso 3 .
Multiple HBAs (Varios HBA)	Si tiene más de un HBA, seleccione el HBA manualmente. <ol style="list-style-type: none"> a En la página Select Host Adapter (Seleccionar adaptador de host), utilice las teclas de flecha para ubicar el cursor en el HBA adecuado. b Presione Entrar.

- 3 En la página Fast!UTIL Options (Opciones de Fast!UTIL), seleccione **Configuration Settings** (Opciones de configuración) y presione **Entrar**.
- 4 En la página Configuration Settings (Opciones de configuración), seleccione **Adapter Settings** (Configuración del adaptador) y presione **Entrar**.

- 5 Establezca el BIOS para que busque dispositivos SCSI.
 - a En la página Host Adapter Settings (Configuración del adaptador de host), seleccione **Host Adapter BIOS** (BIOS del adaptador de host).
 - b Presione **Entrar** para alternar el valor a Enabled (Habilitado).
 - c Presione **Esc** para salir.
- 6 Habilite el arranque seleccionable.
 - a Seleccione **Selectable Boot Settings** (Configuración del arranque seleccionable) y presione **Entrar**.
 - b En la página Selectable Boot Settings (Configuración del arranque seleccionable), seleccione **Selectable Boot** (Arranque seleccionable).
 - c Presione **Entrar** para alternar el valor a **Enabled** (Habilitado).
- 7 Utilice las teclas de dirección para seleccionar la entrada de Boot Port Name (Nombre de puerto de arranque) en la lista de procesadores de almacenamiento (SP) y, a continuación, presione **Entrar** para abrir la pantalla Select Fibre Channel Device (Seleccionar dispositivo de canal de fibra).
- 8 Utilice las teclas de dirección para seleccionar el SP específico y presione **Entrar**.

Si va a utilizar una matriz de almacenamiento de tipo activo-pasivo, el SP seleccionado debe estar en la ruta de acceso (activa) preferida al LUN de arranque. Si no está seguro respecto de qué SP está en la ruta de acceso activa, utilice el software de administración de matriz de almacenamiento para encontrarlo. El BIOS crea los identificadores de destino, y estos pueden cambiar con cada reinicio.
- 9 Realice la acción adecuada según la cantidad de LUN asociados al SP.

Opción	Descripción
One LUN (Un LUN)	Se selecciona el LUN como LUN de arranque. No es necesario entrar a la pantalla Select LUN (Seleccionar LUN).
Multiple LUNs (Varios LUN)	Se abre la pantalla Select LUN (Seleccionar LUN). Utilice el cursor para seleccionar el LUN de arranque y, a continuación, presione Entrar .

- 10 Si aparece algún otro procesador de almacenamiento restante en la lista, presione **C** para eliminar los datos.
- 11 Presione **Esc** dos veces para salir y, a continuación, presione **Entrar** para guardar la configuración.

Arrancar ESXi con FCoE de software

7

ESXi admite el arranque desde adaptadores de red compatibles con FCoE.

Cuando se instala y se arranca ESXi desde un LUN de FCoE, el host puede utilizar un adaptador FCoE de software de VMware y un adaptador de red con capacidades de FCoE. El host no requiere un HBA FCoE dedicado.

La mayoría de las configuraciones se realiza a través de la opción ROM del adaptador de red. Los adaptadores de red deben admitir uno de los formatos siguientes, que comunican parámetros sobre un dispositivo de arranque FCoE al VMkernel.

- Tabla de firmware de arranque de FCoE (FBFT). FBFT es propiedad de Intel.
- Tabla de parámetros de arranque de FCoE (FBPT). VMware define FBPT para que los proveedores de terceros implementen el arranque de FCoE de software.

Los parámetros de configuración se establecen en la opción ROM del adaptador. Durante la instalación o el arranque posterior de ESXi, estos parámetros se exportan a la memoria del sistema en formato FBFT o FBPT. El VMkernel puede leer las opciones de configuración y utilizarlas para acceder al LUN de arranque.

Este capítulo incluye los siguientes temas:

- [Requisitos y consideraciones sobre el arranque de FCoE de software](#)
- [Prácticas recomendadas para el arranque de FCoE de software](#)
- [Configurar arranque de FCoE de software](#)
- [Solucionar problemas de instalación y arranque desde FCoE de software](#)

Requisitos y consideraciones sobre el arranque de FCoE de software

Cuando el host ESXi se arranca desde una SAN con FCoE de software, aplican ciertos requisitos y consideraciones.

Requisitos

- ESXi 5.1 o versiones posteriores.

- El adaptador de red debe tener las capacidades siguientes:
 - Ser compatible con FCoE.
 - Admitir una pila de FCoE abierta de ESXi.
 - Contener un firmware de arranque de FCoE que pueda exportar información de arranque en formato FBFT o FBPT.

Consideraciones

- No se puede cambiar la configuración de arranque de FCoE de software desde ESXi.
- No se admite el volcado de núcleos en ningún LUN de FCoE de software, incluido el LUN de arranque.
- No se admite la función de múltiples rutas antes del arranque.
- El LUN de arranque no puede compartirse con otros host, incluso en un almacenamiento compartido.

Prácticas recomendadas para el arranque de FCoE de software

VMware recomienda varias prácticas recomendadas cuando arranca el sistema desde un LUN FCoE de software.

- Asegúrese de que el host tenga acceso al LUN de arranque completo. El LUN de arranque no puede compartirse con otros hosts, incluso en un almacenamiento compartido.
- Si utiliza una controladora de Ethernet Intel de 10 Gigabit (Niantec) con un conmutador de Cisco, configure el puerto del conmutador de la siguiente manera:
 - Habilite el protocolo de árbol de expansión (Spanning Tree Protocol, STP).
 - Desactive `switchport trunk native vlan` en la VLAN que se utiliza para FCoE.

Configurar arranque de FCoE de software

El host ESXi puede arrancar desde un LUN de FCoE con el adaptador FCoE de software o un adaptador de red.

Al configurar el host para una arranque de FCoE de software, debe realizar una serie de tareas.

Requisitos previos

El adaptador de red tiene las siguientes capacidades:

- Compatibilidad parcial con descarga de FCoE (FCoE de software).
- Contiene una tabla de firmware de arranque de FCoE (FBFT) o una tabla de parámetros de arranque de FCoE (FBPT).

Para obtener información sobre los adaptadores de red compatibles con el arranque de FCoE de software, consulte la *Guía de compatibilidad de VMware*.

Procedimiento

1 Configurar parámetros de arranque de FCoE de software

Para complementar un proceso de arranque de FCoE de software, un adaptador de red en el host debe tener un firmware de arranque de FCoE especialmente configurado. Al configurar el firmware, habilita el adaptador para el arranque de FCoE de software y especifica los parámetros del LUN de arranque.

2 Instalación y arranque de ESXi desde LUN FCoE de software

Cuando se configura el sistema para que arranque desde un LUN FCoE de software, se instala la imagen de ESXi en el LUN de destino. Posteriormente, es posible arrancar el host desde ese LUN.

Configurar parámetros de arranque de FCoE de software

Para complementar un proceso de arranque de FCoE de software, un adaptador de red en el host debe tener un firmware de arranque de FCoE especialmente configurado. Al configurar el firmware, habilita el adaptador para el arranque de FCoE de software y especifica los parámetros del LUN de arranque.

Procedimiento

- ◆ En la opción ROM del adaptador de red, especifique los parámetros de arranque de FCoE de software.

Entre estos parámetros se encuentran destino de arranque, LUN de arranque, identificador de VLAN, etc.

Debido a que la configuración del adaptador de red depende del proveedor, es necesario consultar la documentación del proveedor para obtener instrucciones.

Instalación y arranque de ESXi desde LUN FCoE de software

Cuando se configura el sistema para que arranque desde un LUN FCoE de software, se instala la imagen de ESXi en el LUN de destino. Posteriormente, es posible arrancar el host desde ese LUN.

Requisitos previos

- Configure la opción ROM del adaptador de red para que apunte a un LUN de destino que desea utilizar como el LUN de arranque. Asegúrese de tener información acerca del LUN de arranque.
- Cambie el orden de arranque en el BIOS del sistema a la secuencia siguiente:
 - a El adaptador de red que utiliza para el arranque de FCoE de software.
 - b Los medios de instalación de ESXi.

Consulte la documentación del proveedor de su sistema.

Procedimiento

- 1 Inicie una instalación interactiva desde el CD/DVD de instalación de ESXi.

El instalador de ESXi comprueba que el arranque de FCoE esté habilitado en el BIOS y, de ser necesario, crea un conmutador virtual estándar para el adaptador de red compatible con FCoE. El nombre del vSwitch es VMware_FCoE_vSwitch. El instalador utiliza, a continuación, parámetros de arranque de FCoE preconfigurados para detectar y mostrar todos los LUN FCoE disponibles.

- 2 En la pantalla **Select a Disk** (Seleccionar un disco), seleccione el LUN FCoE de software que especificó en la configuración de parámetros de arranque.

Si el LUN de arranque no aparece en este menú, asegúrese de haber configurado los parámetros de arranque correctamente en la opción ROM del adaptador de red.

- 3 Siga las indicaciones para completar la instalación.

- 4 Reinicie el host.

- 5 Cambie el orden de arranque en el BIOS del sistema para que el LUN de arranque de FCoE sea el primer dispositivo de arranque.

ESXi continúa arrancando desde el LUN FCoE de software hasta que está listo para ser utilizado.

Pasos siguientes

De ser necesario, puede cambiar el nombre y modificar la instancia de VMware_FCoE_vSwitch que creó automáticamente el instalador. Asegúrese de que el modo Cisco Discovery Protocol (CDP) esté establecido en Listen (Escucha) o Both (Ambos).

Solucionar problemas de instalación y arranque desde FCoE de software

Si la instalación o el arranque de ESXi desde un LUN de FCoE de software produce errores, puede usar varios métodos de solución de problemas.

Problema

Cuando instala o arranca ESXi desde el almacenamiento de FCoE con un adaptador de FCoE de software de VMware y un adaptador de red con capacidades de descarga de FCoE parciales, el proceso de instalación o de arranque produce errores.

Solución

- Asegúrese de haber configurado correctamente los parámetros de arranque en la opción ROM del adaptador de red de FCoE.
- Durante la instalación, supervise el BIOS del adaptador de red de FCoE en busca de cualquier error.

- De ser posible, compruebe el registro del VMkernel en busca de errores.
- Use el comando `esxcli` para comprobar que el LUN de arranque esté presente.

```
esxcli conn_options hardware bootdevice list
```

Prácticas recomendadas para el almacenamiento de canal de fibra

8

Cuando use ESXi con SAN de canal de fibra, siga las prácticas recomendadas que ofrece VMware para evitar problemas de rendimiento.

vSphere Web Client ofrece varias opciones para recopilar información de rendimiento. La información se muestra de forma gráfica y se actualiza con frecuencia.

También puede usar las utilidades de línea de comandos `resxtop` o `esxtop`. Estas utilidades proporcionan una vista detallada en tiempo real del modo en que ESXi usa los recursos. Para obtener más información, consulte la documentación de *Administración de recursos de vSphere*.

Consulte a su representante de almacenamiento si su sistema de almacenamiento admite las características de aceleración de hardware de Storage API - Array Integration. Si las admite, consulte la documentación del proveedor para obtener información sobre cómo habilitar la compatibilidad con la aceleración de hardware en el sistema de almacenamiento. Para obtener más información, consulte [Capítulo 23 Aceleración de hardware de almacenamiento](#).

Este capítulo incluye los siguientes temas:

- [Evitar problemas de SAN de canal de fibra](#)
- [Deshabilitar el registro automático de hosts](#)
- [Optimizar el rendimiento del almacenamiento de SAN de canal de fibra](#)

Evitar problemas de SAN de canal de fibra

Al utilizar ESXi junto con una SAN de canal de fibra, se deben seguir instrucciones específicas para evitar problemas en la SAN.

Debe observar estos consejos para evitar problemas en la configuración de la SAN:

- Coloque un solo almacén de datos de VMFS en cada LUN.
- No cambie la directiva de rutas de acceso que el sistema establece a menos que comprenda las consecuencias de realizar esa modificación.
- Documente todo. Incluya información sobre la división en zonas, el control de acceso, el almacenamiento, el conmutador, el servidor y la configuración del HBA de FC.

- Planificación en caso de errores:
 - Haga varias copias de los mapas de topología. Para cada elemento, tenga en cuenta lo que sucede con la SAN si el elemento presenta errores.
 - Verifique diferentes vínculos, conmutadores, HBA y otros elementos para asegurarse de no haber omitido ningún punto de error crítico en el diseño.
- Asegúrese de que los HBA de canal de fibra estén instalados en las ranuras correctas en el host, según la velocidad del bus y de la ranura. Equilibre la carga del bus PCI entre los buses disponibles del servidor.
- Familiarícese con los distintos puntos de supervisión en la red de almacenamiento, en todos los puntos de visibilidad, incluidos los gráficos de rendimiento, las estadísticas de conmutador de FC y las estadísticas de rendimiento del almacenamiento del host.
- Tenga cuidado cuando cambie los identificadores de los LUN que tienen almacenes de datos de VMFS utilizados por el host ESXi. Si cambia el identificador, el almacén de datos se vuelve inactivo y las máquinas virtuales generan errores. Puede volver a firmar el almacén de datos para activarlo nuevamente. Consulte [Administrar almacenes de datos de VMFS duplicados](#).

Si no hay máquinas virtuales en ejecución en el almacén de datos de VMFS, después de cambiar el identificador del LUN, debe volver a examinar para restablecer el identificador en el host. Para obtener información sobre cómo volver a examinar, consulte [Operaciones para actualizar y volver a examinar el almacenamiento](#).

Deshabilitar el registro automático de hosts

Ciertas matrices de almacenamiento requieren que los hosts ESXi se registren en ellas. ESXi realiza el registro automático de los hosts al enviar el nombre y la dirección IP de los hosts a la matriz. Si prefiere el registro manual mediante el software de administración de almacenamiento, deshabilite la característica de registro automático de ESXi.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Sistema**, haga clic en **Configuración avanzada del sistema**.
- 4 En Advanced System Settings (Configuración avanzada del sistema), seleccione el parámetro **Disk.EnableNaviReg** y haga clic en el icono **Edit** (Editar).
- 5 Cambie el valor a 0.

Resultados

De este modo, se deshabilitará el registro automático de hosts habilitado de forma predeterminada.

Optimizar el rendimiento del almacenamiento de SAN de canal de fibra

Hay varios factores que contribuyen a la optimización del entorno típico de SAN.

Si el entorno está configurado apropiadamente, los componentes del tejido de SAN (particularmente, los conmutadores de la SAN) son solo contribuyentes menores debido a sus latencias bajas relativas en servidores y matrices de almacenamiento. Asegúrese de que las rutas de acceso por el tejido de conmutadores no estén saturadas; es decir, que el tejido de conmutadores funcione con la máxima capacidad de proceso.

Rendimiento de matrices de almacenamiento

El rendimiento de la matriz de almacenamiento es uno de los principales factores que contribuye al rendimiento de todo el entorno SAN.

Si existen problemas con el rendimiento de la matriz de almacenamiento, asegúrese de consultar la documentación del proveedor de la matriz de almacenamiento para acceder a toda la información relevante.

Siga estas instrucciones generales para mejorar el rendimiento de la matriz en el entorno de vSphere:

- Al asignar LUN, recuerde que se accede a cada LUN a través de una determinada cantidad de hosts y que puede ejecutarse determinada cantidad de máquinas virtuales en cada host. Un LUN utilizado por un host puede prestar servicios de E/S de varias aplicaciones diferentes ejecutadas en distintos sistemas operativos. Debido a esta carga de trabajo diversa, el grupo RAID que contiene los LUN de ESXi no debe incluir LUN utilizados por otros servidores que no ejecuten ESXi.
- Asegúrese de que el almacenamiento en caché de lectura/escritura esté habilitado.
- Las matrices de almacenamiento SAN requieren un rediseño y un ajuste continuo para garantizar que la E/S tenga una carga equilibrada en todas las rutas de acceso de las matrices de almacenamiento. Para cumplir con este requisito, distribuya las rutas de acceso a los LUN entre todos los SP. De esa manera, se podrá proporcionar un equilibrio de carga óptimo. Mediante una supervisión minuciosa, se puede determinar cuándo es necesario volver a equilibrar la distribución de LUN.

El ajuste de las matrices de almacenamiento equilibradas estadísticamente consiste en supervisar las estadísticas de rendimiento específicas (como las operaciones de E/S por segundo, los bloques por segundo y el tiempo de respuesta) y distribuir la carga de trabajo de LUN para diseminar la carga de trabajo entre todos los SP.

Nota Actualmente, ESXi no admite el equilibrio de carga dinámico.

Rendimiento de servidores con canal de fibra

Se deben tener en cuenta varios factores para garantizar un rendimiento óptimo del servidor.

Cada aplicación del servidor debe tener acceso a su almacenamiento designado con las condiciones siguientes:

- Velocidad de E/S alta (cantidad de operaciones de E/S por segundo)
- Alta capacidad de proceso (megabytes por segundo)
- Latencia mínima (tiempos de respuesta)

Dado que cada aplicación tiene distintos requisitos, puede cumplir estos objetivos eligiendo un grupo RAID adecuado en la matriz de almacenamiento. Para alcanzar los objetivos de rendimiento:

- Coloque cada LUN en un grupo RAID que proporcione los niveles de rendimiento necesarios. Preste atención a las actividades y la utilización de recursos de otros LUN en el grupo RAID asignado. Es posible que un grupo RAID de alto rendimiento que tiene demasiadas aplicaciones que realizan operaciones de E/S en él no cumpla con los objetivos de rendimiento requeridos por una aplicación que se ejecuta en el host ESXi.
- Asegúrese de que cada servidor tenga una cantidad suficiente de HBA para permitir la mayor capacidad de proceso de todas las aplicaciones alojadas en el servidor durante el período pico. La propagación de E/S en varios HBA proporciona mayor capacidad de proceso y menor latencia para cada aplicación.
- Para proporcionar redundancia en caso de errores del HBA, asegúrese de que el servidor esté conectado a un tejido redundante dual.
- Cuando se asignan LUN o grupos RAID a sistemas ESXi, varios sistemas operativos utilizan y comparten ese recurso. Como resultado, el rendimiento requerido de cada LUN en el subsistema de almacenamiento puede ser mucho mayor si se trabaja con sistemas ESXi que si se utilizan máquinas físicas. Por ejemplo, si espera ejecutar cuatro aplicaciones de uso intensivo de E/S, asigne el cuádruple de capacidad de rendimiento al LUN de ESXi.
- Cuando se utilizan varios sistemas ESXi junto con vCenter Server, el rendimiento que se necesita del subsistema de almacenamiento aumenta en consecuencia.
- La cantidad de E/S pendientes requerida por las aplicaciones que se ejecutan en un sistema ESXi debe coincidir con la cantidad de E/S que pueden controlar el HBA y la matriz de almacenamiento.

Usar ESXi con una SAN iSCSI

9

Es posible utilizar ESXi junto con una red de área de almacenamiento (SAN), una red de alta velocidad especializada que conecte los sistemas de los equipos a subsistemas de almacenamiento de alto rendimiento. La utilización de ESXi junto con una SAN proporciona consolidación del almacenamiento, mejora la confiabilidad y ayuda en la recuperación ante desastres.

Para utilizar ESXi de forma eficaz con una SAN, es necesario tener un conocimiento práctico de los sistemas ESXi y los conceptos de SAN. Además, cuando se configuran hosts ESXi para utilizar sistemas de almacenamiento SAN de Internet SCSI (iSCSI), se debe estar al tanto de ciertas consideraciones especiales que existen.

Este capítulo incluye los siguientes temas:

- [Conceptos de SAN iSCSI](#)
- [Cómo acceden las máquinas virtuales a los datos en una SAN iSCSI](#)

Conceptos de SAN iSCSI

Si es administrador y planifica configurar hosts ESXi para que trabajen junto con SAN iSCSI, debe tener un conocimiento práctico de los conceptos de iSCSI.

Las SAN iSCSI utilizan conexiones Ethernet entre sistemas informáticos o servidores hosts, además de subsistemas de almacenamiento de alto rendimiento. Entre los componentes de SAN se encuentran adaptadores de bus de host (HBA) o tarjetas de interfaz de red (NIC) en los servidores del host, conmutadores y enrutadores que transportan el tráfico de almacenamiento, cables, procesadores de almacenamiento (SP) y sistemas de discos de almacenamiento.

Las SAN iSCSI utilizan una arquitectura de cliente-servidor. El cliente, denominado iniciador iSCSI, funciona en el host. Inicia las sesiones iSCSI mediante la emisión y transmisión a un servidor de comandos de SCSI encapsulados en el protocolo iSCSI. El servidor se denomina destino iSCSI. El destino iSCSI representa un sistema de almacenamiento físico típico en la red. Esto también puede ser ofrecido por una SAN iSCSI virtual; por ejemplo, un emulador de destinos iSCSI que se ejecuta en una máquina virtual. El destino iSCSI responde a los comandos del iniciador transmitiendo los datos iSCSI requeridos.

Múltiples rutas iSCSI

Al transferir datos entre el almacenamiento y el servidor del host, la SAN utiliza una técnica denominada múltiples rutas. La función de múltiples rutas permite contar con más de una ruta de acceso física desde el host ESXi hasta el LUN de un sistema de almacenamiento.

Por lo general, una ruta de acceso individual de un host a un LUN consiste en un adaptador de iSCSI o una NIC, puertos de conmutadores, cables de conexión y el puerto de la controladora de almacenamiento. Si cualquier componente de la ruta de acceso presenta errores, el host selecciona otra ruta disponible para E/S. El proceso de detección de una ruta de acceso con errores se denomina conmutación por error de la ruta de acceso.

Para obtener más información sobre las múltiples rutas, consulte [Capítulo 17 Descripción de múltiples rutas y conmutación por error](#).

Puertos en la SAN iSCSI

Una entidad detectable individual en la SAN iSCSI, como un iniciador o un destino, representa un nodo iSCSI. Cada nodo tiene uno o varios puertos que lo conectan a la SAN.

Los puertos iSCSI son extremos de una sesión iSCSI. Cada nodo puede identificarse de distintas maneras.

Dirección IP

Cada nodo iSCSI puede tener una dirección IP asociada a él, para que los equipos de enrutamiento y conmutación de la red puedan establecer la conexión entre el servidor y el almacenamiento. Esta dirección es igual a la dirección IP que se asigna a un equipo para acceder a la red de la empresa o a Internet.

Nombre iSCSI

Un nombre universal único para identificar el nodo. iSCSI utiliza el nombre calificado iSCSI (IQN) y el identificador único extendido (EUI).

De manera predeterminada, ESXi genera nombres iSCSI únicos para los iniciadores iSCSI, por ejemplo, `iqn.1998-01.com.vmware:iscsitestox-68158ef2`. Por lo general, no se debe cambiar el valor predeterminado; caso contrario, el nombre iSCSI nuevo que se introduzca debe ser único.

Alias iSCSI

Un nombre más manejable para un dispositivo o puerto iSCSI utilizado en lugar del nombre iSCSI. Los alias iSCSI no son únicos, y su objetivo es ser un nombre fácil de recordar que se asocia con un puerto.

Convenciones de nomenclatura de iSCSI

iSCSI utiliza un nombre único para identificar un nodo de iSCSI, se trate de destino o iniciador. Este nombre es similar al nombre WorldWide Name (WWN) asociado con dispositivos de canal de fibra, y se usa como modo de identificación universal del nodo.

Los nombres de iSCSI se formatean de dos maneras diferentes. El formato más común es IQN.

Para obtener más detalles sobre los requisitos de nomenclatura y los perfiles de cadenas de iSCSI, consulte RFC 3721 y RFC 3722 en el sitio web de IETF.

Formato de nombre calificado de iSCSI (IQN)

El formato IQN adopta la forma `iqn.yyyy-mm.naming-authority:unique name`, donde:

- `yyyy-mm` es el año y el mes en que se estableció la autoridad de asignación de nombres.
- Por lo general, *naming-authority* es la sintaxis inversa del nombre de dominio de Internet de la autoridad de asignación de nombres. Por ejemplo, la autoridad de asignación de nombres de `iscsi.vmware.com` podría tener la forma `iqn.1998-01.com.vmware.iscsi` de nombre calificado de iSCSI. El nombre indica que el nombre de dominio `vmware.com` se registró en enero de 1998, mientras que `iscsi` es un subdominio mantenido por `vmware.com`.
- *unique name* es cualquier nombre que desee usar; por ejemplo, el nombre del host. La autoridad de asignación de nombres debe asegurarse de que todos los nombres asignados después de los dos puntos sean únicos, por ejemplo:
 - `iqn.1998-01.com.vmware.iscsi:name1`
 - `iqn.1998-01.com.vmware.iscsi:name2`
 - `iqn.1998-01.com.vmware.iscsi:name999`

Formato identificador único empresarial (EUI)

El formato EUI adopta la forma `eui.16 hex digits`.

Por ejemplo, `eui.0123456789ABCDEF`.

Los dígitos de 16 hexadecimales son representaciones en texto de números de 64 bits en formato IEEE EUI (identificador único extendido). Los 24 bits superiores son un identificador de empresa que IEEE registra con una empresa determinada. La entidad titular de ese identificador de empresa asigna los 40 bits inferiores, que deben ser únicos.

Iniciadores iSCSI

Para acceder a destinos iSCSI, el host utiliza iniciadores iSCSI. Los iniciadores transportan solicitudes y respuestas SCSI, encapsuladas en el protocolo iSCSI, entre el host y el destino iSCSI.

El host admite diferentes tipos de iniciadores.

Para obtener información sobre cómo configurar y utilizar adaptadores de iSCSI, consulte [Capítulo 10 Configurar adaptadores y almacenamiento iSCSI](#).

Adaptador de iSCSI de software

Un adaptador de iSCSI de software es un código de VMware integrado en el VMkernel. Permite que el host se conecte al dispositivo de almacenamiento iSCSI a través de adaptadores de red estándar. El adaptador de iSCSI de software controla el procesamiento de iSCSI mientras se comunica con el adaptador de red. Con el adaptador de iSCSI de software, se puede utilizar tecnología iSCSI sin adquirir hardware especializado.

Adaptador de iSCSI de hardware

Un adaptador de iSCSI de hardware es un adaptador de terceros que asigna procesamiento de iSCSI y de red desde el host. Los adaptadores de iSCSI de hardware se dividen en categorías.

Adaptador de iSCSI de hardware dependiente

Depende de las redes de VMware y de las interfaces de configuración y administración de iSCSI proporcionadas por VMware.

Este tipo de adaptador puede ser una tarjeta que presenta un adaptador de red estándar y una funcionalidad de asignación de iSCSI para el mismo puerto. La funcionalidad de asignación de iSCSI depende de la configuración de red del host para obtener la IP, la dirección MAC y otros parámetros utilizados para sesiones iSCSI. Un ejemplo de un adaptador dependiente es Broadcom 5709 NIC con licencia iSCSI.

Adaptador de iSCSI de hardware independiente

Implementa su propia configuración de redes y de iSCSI, además de sus propias interfaces de administración.

Un ejemplo de un adaptador de iSCSI de hardware independiente es una tarjeta que presenta solo funcionalidad de asignación de iSCSI o funcionalidad de asignación de iSCSI y funcionalidad de NIC estándar. La funcionalidad de asignación de iSCSI posee una administración de configuración independiente que asigna la IP, la dirección MAC y otros parámetros utilizados para las sesiones iSCSI. Un ejemplo de un adaptador independiente es QLogic QLA4052.

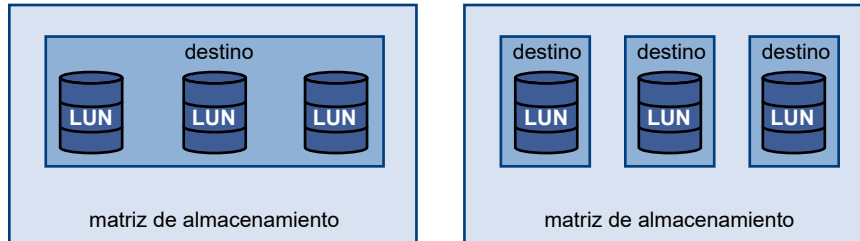
Es posible que deba obtenerse una licencia para los adaptadores de iSCSI de hardware. En caso contrario, los adaptadores no aparecen en la CLI del cliente o de vSphere. Para obtener información sobre licencias, póngase en contacto con el proveedor.

Establecer conexiones iSCSI

En el contexto de ESXi, el término destino identifica a una sola unidad de almacenamiento a la que puede acceder el host. Los términos dispositivo de almacenamiento y LUN describen un volumen lógico que representa espacio de almacenamiento en un destino. Por lo general, los términos dispositivo y LUN, en el contexto de ESXi, significan un volumen SCSI presentado al host desde un destino de almacenamiento y disponible para dar formato.

Los distintos proveedores de almacenamiento iSCSI presentan el almacenamiento a los servidores de distintas formas. Algunos proveedores presentan varios LUN en un solo destino, mientras que otros presentan varios destinos con un LUN cada uno. Si bien la forma en que ESXi usa el almacenamiento es similar, la forma en que se presenta la información a través de herramientas administrativas es diferente.

Figura 9-1. Destino en comparación con representaciones de LUN



Hay tres LUN disponibles en cada una de estas configuraciones. En el primer caso, el host detecta un destino, pero ese destino tiene tres LUN que se pueden utilizar. Cada uno de los LUN representa un volumen de almacenamiento individual. En el segundo caso, el host detecta tres destinos diferentes, cada uno con un LUN.

Los iniciadores iSCSI basados en host establecen conexiones a cada destino. Los sistemas de almacenamiento con un solo destino con varios LUN tienen tráfico a todos los LUN en una sola conexión. Con un sistema que tiene tres destinos con un LUN cada uno, un host utiliza conexiones distintas a los tres LUN. Esta información es útil cuando se intenta combinar tráfico de almacenamiento en varias conexiones desde el host con varios HBA de iSCSI, donde el tráfico de un destino puede establecerse en un HBA en especial, mientras que el tráfico de otro destino puede utilizar un HBA distinto.

Tipos de sistema de almacenamiento iSCSI

ESXi admite distintas matrices y sistemas de almacenamiento.

Entre los tipos de almacenamiento que admite un host se encuentran activo-activo, activo-pasivo y compatible con ALUA.

Sistema de almacenamiento activo-activo

Permite acceder simultáneamente a los LUN en todos los puertos de almacenamiento que están disponibles sin una degradación significativa del rendimiento. Todas las rutas de acceso están activas en todo momento, a menos que una de ellas falle.

Sistema de almacenamiento activo-pasivo

Un sistema en el cual un procesador de almacenamiento proporciona acceso de forma activa a un LUN determinado. Los otros procesadores actúan como copia de seguridad del LUN y pueden proporcionar acceso activamente a otras operaciones de E/S del LUN. Las operaciones de E/S pueden enviarse correctamente solo a un puerto activo de un LUN determinado. Si el acceso a través del puerto de almacenamiento activo genera errores, uno

de los procesadores de almacenamiento pasivos puede activarse mediante los servidores que acceden a él.

Sistema de almacenamiento asimétrico

Admite acceso asimétrico a unidades lógicas (ALUA). Los sistemas de almacenamiento compatibles con ALUA ofrecen diferentes niveles de acceso por puerto. ALUA permite que los hosts determinen los estados de los puertos de destino y prioricen rutas de acceso. El host utiliza algunas de las rutas de acceso activas como principales y otras como secundarias.

Sistema de almacenamiento de puerto virtual

Permite el acceso a todos los LUN disponibles a través de un solo puerto virtual. Son dispositivos de almacenamiento activo-activo, pero ocultan sus distintas conexiones a través de un solo puerto. La habilitación de múltiples rutas de ESXi no convierte varias conexiones de un puerto específico al almacenamiento de forma predeterminada. Algunos proveedores de almacenamiento suministran administradores de sesión para establecer y administrar varias conexiones al almacenamiento. Estos sistemas de almacenamiento controlan la conmutación por error de puertos y el equilibrio de la conexión de forma transparente. Por lo general, esto se denomina conmutación por error transparente.

Detectar, autenticar y controlar el acceso

Se pueden utilizar distintos mecanismos para detectar el almacenamiento y limitar el acceso a él.

El host y el sistema de almacenamiento iSCSI se deben configurar para que admitan la directiva de control de acceso al almacenamiento del usuario.

Detección

Una sesión de detección es parte del protocolo iSCSI y devuelve el conjunto de destinos al que se puede acceder en un sistema de almacenamiento iSCSI. Los dos tipos de detección disponibles en ESXi son dinámica y estática. La detección dinámica obtiene una lista de destinos a los que se puede acceder desde el sistema de almacenamiento iSCSI, mientras que la detección estática solo puede intentar acceder a un destino específico por nombre y dirección de destino.

Para obtener más información, consulte [Configurar direcciones de detección para adaptadores de iSCSI](#).

Authentication (Autenticación)

Los sistemas de almacenamiento iSCSI autentican un iniciador mediante un par de nombre y clave. ESXi es compatible con el protocolo CHAP, que VMware recomienda para la implementación de la SAN. Para utilizar la autenticación de CHAP, el host ESXi y el sistema de almacenamiento iSCSI deben tener CHAP habilitado y disponer de credenciales comunes.

Para obtener más información sobre cómo habilitar CHAP, consulte [Configurar parámetros CHAP para adaptadores de iSCSI](#).

Control de acceso

Control de acceso es una directiva configurada en el sistema de almacenamiento iSCSI. La mayoría de las implementaciones admiten uno o más de tres tipos de control de acceso:

- Por nombre de iniciador
- Por dirección IP
- Por el protocolo CHAP

Solo los iniciadores que cumplen con todas las reglas pueden acceder al volumen iSCSI.

Utilizar solo CHAP para el control de acceso puede desacelerar el proceso de volver a examinar debido a que el host ESXi puede detectar todos los destinos, pero en el paso de autenticación. El proceso de volver a examinar de iSCSI funciona más rápido si el host detecta solo los destinos que puede autenticar.

Corregir errores

Para proteger la integridad de los datos y encabezados iSCSI, el protocolo iSCSI define los métodos de corrección de errores conocidos como resúmenes de encabezados y resúmenes de datos.

Ambos parámetros están deshabilitados de forma predeterminada, pero es posible habilitarlos. Estos resúmenes pertenecen, respectivamente, al encabezado y a los datos de SCSI que se transfieren entre los iniciadores iSCSI y los destinos, en ambas direcciones.

Los resúmenes de encabezado y datos comprueban la integridad de los datos no criptográficos, de extremo a extremo, más allá de las comprobaciones de integridad que proporcionan otras capas de redes, como TCP y Ethernet. Comprueban la ruta de acceso de comunicación completa, incluidos todos los elementos que pueden cambiar el tráfico en el nivel de la red, como los enrutadores, los conmutadores y los proxy.

La existencia y el tipo de los resúmenes se negocian cuando se establece una conexión iSCSI. Cuando el iniciador y el destino acuerdan una configuración de resumen, este resumen debe utilizarse para todo el tráfico entre ellos.

Habilitar los resúmenes de encabezado y datos requiere un procesamiento adicional tanto para el iniciador como para el destino, y puede afectar la capacidad de proceso y el rendimiento de la CPU.

Nota Los sistemas que utilizan procesadores Intel Nehalem descargan los cálculos del resumen de iSCSI, lo que reduce el impacto sobre el rendimiento.

Para obtener información sobre cómo habilitar los resúmenes de datos y encabezado, consulte [Configurar los parámetros avanzados de iSCSI](#).

Cómo acceden las máquinas virtuales a los datos en una SAN iSCSI

ESXi almacena los archivos del disco de una máquina virtual en un almacén de datos de VMFS que reside en un dispositivo de almacenamiento SAN. Cuando los sistemas operativos invitados de la máquina virtual emiten comandos SCSI a sus discos virtuales, la capa de virtualización SCSI traduce esos comandos a operaciones de archivos VMFS.

Cuando una máquina virtual interactúa con su disco virtual almacenado en una SAN, se llevan a cabo los siguientes procesos:

- 1 Cuando el sistema operativo invitado en una máquina virtual lee o escribe en el disco SCSI, emite comandos SCSI al disco virtual.
- 2 Los controladores de dispositivos en el sistema operativo de la máquina virtual se comunican con las controladoras SCSI virtuales.
- 3 La controladora SCSI virtual reenvía el comando al VMkernel.
- 4 El VMkernel realiza las siguientes tareas.
 - a Coloca el archivo, que corresponde al disco de la máquina virtual invitada, en el volumen VMFS.
 - b Asigna las solicitudes de los bloques en el disco virtual en bloques del dispositivo físico apropiado.
 - c Envía la solicitud de E/S modificada desde el controlador del dispositivo en el VMkernel al iniciador iSCSI (hardware o software).
- 5 Si el iniciador iSCSI es un adaptador de iSCSI de hardware (sea independiente o dependiente), el adaptador realiza las tareas siguientes.
 - a Encapsula las solicitudes de E/S en unidades de datos de protocolo (PDU) de iSCSI.
 - b Encapsula PDU de iSCSI en paquetes TCP/IP.
 - c Envía paquetes IP por Ethernet al sistema de almacenamiento iSCSI.
- 6 Si el iniciador iSCSI es un adaptador de iSCSI del software, ocurre lo siguiente.
 - a El iniciador iSCSI encapsula las solicitudes de E/S en PDU de iSCSI.
 - b El iniciador envía PDU de iSCSI a través de conexiones TCP/IP.
 - c La pila de TCP/IP del VMkernel retransmite los paquetes TCP/IP a la NIC física.
 - d La NIC física envía paquetes IP por Ethernet al sistema de almacenamiento iSCSI.
- 7 Según cuál puerto utilice el iniciador iSCSI para conectarse a la red, los enrutadores y conmutadores Ethernet llevan la solicitud al dispositivo de almacenamiento al que desea acceder el host.

Configurar adaptadores y almacenamiento iSCSI

10

Para que ESXi pueda funcionar con una SAN, debe configurar el almacenamiento y los adaptadores de iSCSI.

Para ello, primero debe tener en cuenta ciertos requisitos básicos y, a continuación, seguir las prácticas recomendadas para instalar y configurar los adaptadores de iSCSI de software o hardware para acceder a la SAN.

La tabla siguiente enumera los adaptadores de iSCSI (vmhbases) compatibles con ESXi e indica si es necesaria una configuración de redes VMkernel.

Tabla 10-1. Adaptadores iSCSI compatibles

Adaptador de iSCSI (vmhba)	Descripción	Redes VMkernel
Software	Utiliza NIC estándar para conectar el host a un destino iSCSI remoto en la red IP.	Obligatorio
Hardware independiente	Adaptador de terceros que descarga la administración y el procesamiento de red e iSCSI del host.	No son obligatorias
Hardware dependiente	Adaptador de terceros que depende de las interfaces de administración y configuración de iSCSI y de las redes de VMware.	Obligatorio

Después de configurar los adaptadores de iSCSI, puede crear un almacén de datos en el almacenamiento iSCSI. Para obtener detalles sobre cómo crear y administrar almacenes de datos, consulte [Crear almacenes de datos](#).

Este capítulo incluye los siguientes temas:

- [Requisitos de SAN iSCSI de ESXi](#)
- [Restricciones de SAN iSCSI ESXi](#)
- [Establecer asignaciones de LUN para iSCSI](#)
- [Configurar y autenticar red](#)
- [Configurar adaptadores de iSCSI de hardware independientes](#)
- [Acerca de los adaptadores de iSCSI de hardware dependiente](#)

- [Acerca del adaptador de iSCSI de software](#)
- [Modificar propiedades generales de los adaptadores de iSCSI](#)
- [Configurar la red de iSCSI](#)
- [Usar tramas gigantes con iSCSI](#)
- [Configurar direcciones de detección para adaptadores de iSCSI](#)
- [Configurar parámetros CHAP para adaptadores de iSCSI](#)
- [Configurar los parámetros avanzados de iSCSI](#)
- [Administrar sesiones de iSCSI](#)

Requisitos de SAN iSCSI de ESXi

Se deben cumplir varios requisitos para que el host ESXi funcione correctamente con una SAN.

- Compruebe que las combinaciones de hardware y firmware de almacenamiento SAN sean compatibles junto con los sistemas ESXi. Para acceder a una lista actualizada, consulte la *Guía de compatibilidad de VMware*.
- Configure el sistema para que tenga un solo almacén de datos de VMFS por cada LUN.
- A menos que utilice servidores sin disco, configure una partición de diagnóstico en un almacenamiento local. Si tiene servidores sin disco que arrancan desde una SAN iSCSI, consulte [Recomendaciones generales de arranque desde SAN iSCSI](#) para obtener información sobre las particiones de diagnóstico con iSCSI.
- Utilice los RDM para acceder a cualquier disco sin formato. Para obtener información, consulte [Capítulo 18 Asignación de dispositivos sin formato](#).
- Establezca el controlador de la controladora SCSI en el sistema operativo invitado con una cola lo suficientemente grande. Para obtener información sobre cómo cambiar la profundidad de la cola para adaptadores de iSCSI y máquinas virtuales, consulte *Solución de problemas de vSphere*.
- En máquinas virtuales con Microsoft Windows, aumente el valor del parámetro `TimeoutValue` de SCSI para permitir que Windows tolere mejor las E/S retrasadas que son consecuencia de la conmutación por error de las rutas de acceso. Para obtener información, consulte [Establecer el tiempo de espera en un sistema operativo invitado Windows](#).

Restricciones de SAN iSCSI ESXi

Existen ciertas restricciones cuando se usa ESXi con una SAN iSCSI.

- ESXi no es compatible con dispositivos de cinta conectados a iSCSI.
- No se puede usar un software de múltiples rutas de máquina virtual para realizar el equilibrio de carga de E/S de un único LUN físico.

- ESXi no admite múltiples rutas cuando se combinan adaptadores de hardware independiente con adaptadores de hardware dependiente o de software.

Establecer asignaciones de LUN para iSCSI

Al preparar el sistema ESXi para usar almacenamiento de SAN iSCSI, debe establecer las asignaciones de LUN.

Tenga en cuenta los siguientes puntos:

- Aprovisionamiento de almacenamiento. Para asegurarse de que el host reconozca los LUN durante el inicio, configure todos los destinos de almacenamiento iSCSI de forma tal que el host pueda acceder a ellos y usarlos. Además, configure el host de forma tal que pueda detectar todos los destinos iSCSI disponibles.
- vMotion y VMware DRS. Cuando usa vCenter Server y vMotion o DRS, asegúrese de que los LUN de las máquinas virtuales estén aprovisionados en todos los hosts. Esta configuración ofrece la mayor libertad para mover máquinas virtuales.
- Matrices activas-activas frente a activas-pasivas. Cuando use vMotion o DRS con un dispositivo de almacenamiento SAN activo-pasivo, asegúrese de que todos los hosts tengan rutas de acceso coherentes hacia todos los procesadores de almacenamiento. Si no lo hace, puede provocar la destrucción de las rutas de acceso cuando se produzca una migración de vMotion.

En el caso de las matrices de almacenamiento activas-pasivas no incluidas en la lista de compatibilidad de almacenamiento/SAN, VMware no admite la conmutación por error de puerto de almacenamiento. Debe conectar el servidor al puerto activo en el sistema de almacenamiento. Esta configuración garantiza que los LUN se presenten ante el host.

Configurar y autenticar red

Para que el host ESXi pueda detectar el almacenamiento iSCSI, los iniciadores iSCSI deben estar configurados y posiblemente se deba configurar la autenticación.

- En el caso de iSCSI de software e iSCSI de hardware dependiente, se deben configurar las redes del VMkernel. Puede comprobar la configuración de red con la utilidad `vmkping`. Con iSCSI de software e iSCSI dependiente, se admiten los protocolos IPv4 e IPv6.
- Para iSCSI de hardware independiente, se deben configurar en el HBA los parámetros de red, como la dirección IP, la máscara de red y la puerta de enlace predeterminada. También se puede especificar un protocolo de red, IPv4 o IPv6, para el adaptador.
- Revise y cambie el nombre del iniciador predeterminado, de ser necesario.
- Se deben configurar la dirección de detección dinámica o la dirección de detección estática y el nombre de destino del sistema de almacenamiento. Para iSCSI de software e iSCSI de hardware dependiente, se debe poder hacer ping en la dirección con `vmkping`.

- Para la autenticación de CHAP, habilítela del lado del sistema de almacenamiento y en el iniciador. Una vez habilitada la autenticación, esta se aplica para todos los destinos que aún no se detectaron, pero no para los destinos que ya se descubrieron. Una vez configurada la dirección de detección, los nuevos destinos detectados se exponen y pueden utilizarse en esa instancia.

Para obtener detalles sobre cómo usar el comando `vmkping`, busque en la base de conocimientos de VMware.

Configurar adaptadores de iSCSI de hardware independientes

Un adaptador de iSCSI de hardware independiente es un adaptador de terceros especializado capaz de acceder al almacenamiento iSCSI mediante TCP/IP. Este adaptador de iSCSI controla todo el procesamiento y la administración de red e iSCSI para el sistema ESXi.

Requisitos previos

- Compruebe si el adaptador requiere una licencia.
- Instale el adaptador.

Para obtener información sobre las licencias, la instalación y las actualizaciones de firmware, consulte la documentación del proveedor.

Procedimiento

1 [Ver adaptadores de iSCSI de hardware independientes](#)

Vea un adaptador de iSCSI de hardware independiente para comprobar que esté instalado correctamente y listo para ser configurado.

2 [Modificar propiedades generales de los adaptadores de iSCSI](#)

Es posible modificar el alias y el nombre iSCSI predeterminados asignados a los adaptadores de iSCSI. En el caso de los adaptadores de iSCSI de hardware independientes, también se puede cambiar la configuración IP predeterminada.

3 [Editar la configuración de red para iSCSI de hardware](#)

Después de instalar un adaptador de iSCSI de hardware independiente, es posible que deba cambiar la configuración de red predeterminada para configurarlo correctamente para la SAN iSCSI.

4 [Configurar la detección dinámica o estática de iSCSI](#)

Con la detección dinámica, cada vez que el iniciador se contacte con el sistema de almacenamiento iSCSI especificado, le enviará una solicitud de `SendTargets`. El sistema iSCSI le responde al iniciador y le suministra una lista de destinos disponibles. Además del método de detección dinámica, se puede utilizar una detección estática e introducir manualmente la información de los destinos.

Pasos siguientes

Si es necesario, configure los parámetros de CHAP y las tramas gigantes.

Ver adaptadores de iSCSI de hardware independientes

Vea un adaptador de iSCSI de hardware independiente para comprobar que esté instalado correctamente y listo para ser configurado.

Después de instalar un adaptador de iSCSI de hardware independiente en un host, aparecerá en el listado de adaptadores de almacenamiento disponibles para configuración. Es posible ver sus propiedades.

Requisitos previos

Privilegios necesarios: **Host.Configuración.Configuración de la partición de almacenamiento**

Procedimiento

1 Diríjase al host en el navegador de vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento**.

Si está instalado, el adaptador de iSCSI de hardware aparecerá en la lista de adaptadores de almacenamiento.

4 Seleccione el adaptador que desea ver.

Aparecen los detalles predeterminados del adaptador, incluidos el modelo, el nombre iSCSI, el alias iSCSI, la dirección IP y la información sobre el destino y las rutas de acceso.

Modificar propiedades generales de los adaptadores de iSCSI

Es posible modificar el alias y el nombre iSCSI predeterminados asignados a los adaptadores de iSCSI. En el caso de los adaptadores de iSCSI de hardware independientes, también se puede cambiar la configuración IP predeterminada.

Importante Cuando modifique cualquier propiedad predeterminada de los adaptadores de iSCSI, asegúrese de darle el formato correcto a los nombres y las direcciones IP.

Requisitos previos

Privilegios necesarios: **Host .Configuración.Configuración de la partición de almacenamiento**

Procedimiento

1 Diríjase al host en el navegador de vSphere Web Client.

2 Haga clic en la pestaña **Configurar**.

3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador (vmhba#) que desea configurar.

- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Properties** (Propiedades) y en **Edit** (Editar) en el panel General.
- 5 Para cambiar el nombre iSCSI predeterminado del adaptador, escriba el nuevo nombre.
Asegúrese de que el nombre que ingrese sea un nombre universal único y tenga el formato adecuado; de lo contrario, es posible que algunos dispositivos de almacenamiento no reconozcan el adaptador de iSCSI.
- 6 (opcional) Introduzca el alias iSCSI.
El alias es un nombre que se utiliza para identificar el adaptador de iSCSI.

Resultados

Si cambia el nombre iSCSI, este se utilizará en las nuevas sesiones de iSCSI. Para las sesiones existentes, no se utilizará la nueva configuración hasta que la sesión se cierre y se vuelva a iniciar.

Editar la configuración de red para iSCSI de hardware

Después de instalar un adaptador de iSCSI de hardware independiente, es posible que deba cambiar la configuración de red predeterminada para configurarlo correctamente para la SAN iSCSI.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador (vmhba#) que desea configurar.
- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Network Settings** (Configuración de red) y en **Edit** (Editar).
- 5 En la sección de configuración de IPv4, deshabilite IPv6 o seleccione el método utilizado para obtener las direcciones IP.

Nota Las opciones de DHCP automático y estático son mutuamente exclusivas.

Opción	Descripción
No IPv4 settings (Sin configuración de IPv4)	Deshabilite IPv4.
Obtain IPv4 settings automatically (Obtener configuración de IPv4 automáticamente)	Use DHCP para obtener la configuración de IP.
Use static IPv4 settings (Usar configuración de IPv4 estática)	Escriba la dirección IP, la máscara de subred y la puerta de enlace predeterminada IPv4 para el adaptador de iSCSI.

- 6 En la sección de configuración de IPv6, deshabilite IPv6 o seleccione una opción adecuada para obtener las direcciones IPv6.

Nota Las opciones automática y estática son mutuamente exclusivas.

Opción	Descripción
No IPv6 settings (Sin configuración IPv6)	Deshabilite IPv6.
Enable IPv6 (Habilitar IPv6)	Seleccione una opción para obtener las direcciones IPv6.
Obtain IPv6 addresses automatically through DHCP (Obtener las direcciones IPv6 automáticamente por medio de DHCP)	Use DHCP para obtener las direcciones IPv6.
Obtain IPv6 addresses automatically through Router Advertisement (Obtener las direcciones IPv6 automáticamente por medio del anuncio de enrutador)	Use el anuncio de enrutador para obtener las direcciones IPv6.
Override Link-local address for IPv6 (Anular dirección local de vínculo para IPv6)	Anule la dirección IP local de vínculo con la configuración de una dirección IP estática.
Static IPv6 addresses (Direcciones IPv6 estáticas)	a Haga clic en Add (Agregar) para agregar una nueva dirección IPv6. b Introduzca la dirección IPv6 y la longitud del prefijo de subred, y haga clic en OK (Aceptar).

- 7 En la sección de configuración de DNS, proporcione las direcciones IP de un servidor DNS preferido y un servidor DNS alternativo.

Debe proporcionar ambos valores.

Configurar la detección dinámica o estática de iSCSI

Con la detección dinámica, cada vez que el iniciador se contacte con el sistema de almacenamiento iSCSI especificado, le enviará una solicitud de SendTargets. El sistema iSCSI le responde al iniciador y le suministra una lista de destinos disponibles. Además del método de detección dinámica, se puede utilizar una detección estática e introducir manualmente la información de los destinos.

Al configurar la detección estática o dinámica, solo se pueden agregar destinos iSCSI nuevos. No se puede cambiar ningún parámetro de un destino existente. Para hacer cambios, quite el destino existente y agregue uno nuevo.

Requisitos previos

Privilegios necesarios: **Host.Configuración.Configuración de la partición de almacenamiento**

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.

- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Storage Adapters** (Adaptadores de almacenamiento) y seleccione el adaptador de iSCSI que desea configurar en la lista.
- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Targets** (Destinos).
- 5 Configure el método de detección.

Opción	Descripción
Detección dinámica	<ol style="list-style-type: none"> a Haga clic en Dynamic Discovery (Detección dinámica) y, a continuación, en Add (Agregar). b Escriba la dirección IP o el nombre DNS del sistema de almacenamiento y haga clic en OK (Aceptar). c Vuelva a examinar el adaptador de iSCSI. <p>Después de establecer la sesión de SendTargets con el sistema iSCSI, el host completa la lista de detección estática con todos los destinos recién detectados.</p>
Detección estática	<ol style="list-style-type: none"> a Haga clic en Static Discovery (Detección estática) y, a continuación, en Add (Agregar). b Introduzca la información del destino y haga clic en OK (Aceptar). c Vuelva a examinar el adaptador de iSCSI.

Acerca de los adaptadores de iSCSI de hardware dependiente

Un adaptador de iSCSI de hardware dependiente es un adaptador de terceros que depende de las redes de VMware, así como de las interfaces de administración y configuración de iSCSI que proporciona VMware.

Un ejemplo de adaptador de iSCSI dependiente es una NIC Broadcom 5709. Cuando está instalado en un host, presenta sus dos componentes, un adaptador de red estándar y un motor iSCSI, en el mismo puerto. El motor iSCSI aparece en la lista de adaptadores de almacenamiento como un adaptador de iSCSI (vmhba). Aunque el adaptador de iSCSI está habilitado de forma predeterminada, para que sea funcional, primero debe conectarlo mediante un adaptador VMkernel virtual (vmk) a un adaptador de red físico (vmnic) asociado con él. A continuación, puede configurar el adaptador de iSCSI.

Después de configurar el adaptador de iSCSI de hardware dependiente, los datos de detección y autenticación pasan por la conexión de red, mientras que el tráfico iSCSI pasa por el motor iSCSI y omite la red.

Consideraciones sobre iSCSI de hardware dependiente

Cuando se utilizan adaptadores de iSCSI de hardware dependiente con ESXi, aplican ciertas consideraciones.

- Cuando se utiliza cualquier adaptador de iSCSI de hardware dependiente, los informes de rendimiento de una NIC asociada con el adaptador pueden mostrar poca o ninguna actividad, incluso cuando hay demasiado tráfico iSCSI. Este comportamiento ocurre porque el tráfico iSCSI omite la pila de redes normal.
- Si utiliza un conmutador virtual de terceros, por ejemplo, Cisco Nexus 1000V DVS, deshabilite la fijación automática. En su lugar, utilice la fijación manual, y asegúrese de conectar un adaptador VMkernel (vmk) a una NIC física (vmnic) adecuada. Para obtener información, consulte la documentación del proveedor del conmutador virtual.
- El adaptador Broadcom iSCSI realiza el reensamblaje de datos en el hardware, el cual tiene espacio de búfer limitado. Cuando utilice el adaptador Broadcom iSCSI en una red congestionada o con una carga pesada, habilite el control de flujo para evitar la degradación del rendimiento.

El control de flujo administra la tasa de transmisión de datos entre dos nodos para evitar que un remitente rápido sature a un receptor lento. Para obtener los mejores resultados, habilite el control de flujo en los extremos de la ruta de acceso de E/S, en los hosts y en los sistemas de almacenamiento iSCSI.

Para habilitar el control de flujo para el host, utilice el comando `esxcli system module parameters`. Para obtener detalles, consulte el artículo de la base de conocimientos de VMware en <http://kb.vmware.com/kb/1013413>

- Los adaptadores de hardware dependiente son compatibles con IPv4 e IPv6.

Configurar los adaptadores de iSCSI de hardware dependiente

El proceso completo de instalación y configuración de los adaptadores de iSCSI de hardware dependiente involucran varios pasos. Después de instalar el adaptador, es posible que necesite configurar los parámetros CHAP y las tramas gigantes.

Procedimiento

1 Ver adaptadores de iSCSI de hardware dependiente

Se puede ver un adaptador de iSCSI de hardware dependiente para comprobar que esté correctamente cargado.

2 Modificar propiedades generales de los adaptadores de iSCSI

Es posible modificar el alias y el nombre iSCSI predeterminados asignados a los adaptadores de iSCSI. En el caso de los adaptadores de iSCSI de hardware independientes, también se puede cambiar la configuración IP predeterminada.

3 Determinar la asociación entre iSCSI y los adaptadores de red

Puede crear conexiones de red para vincular adaptadores de red dependientes de iSCSI y físicos. Para crear las conexiones correctamente, se debe determinar el nombre de la NIC física con la que está asociado el adaptador de iSCSI de hardware dependiente.

4 Crear conexiones de red para iSCSI

Configure conexiones para el tráfico entre los adaptadores de iSCSI de hardware dependiente o de software y los adaptadores de red física.

5 Configurar la detección dinámica o estática de iSCSI

Con la detección dinámica, cada vez que el iniciador se contacte con el sistema de almacenamiento iSCSI especificado, le enviará una solicitud de SendTargets. El sistema iSCSI le responde al iniciador y le suministra una lista de destinos disponibles. Además del método de detección dinámica, se puede utilizar una detección estática e introducir manualmente la información de los destinos.

Pasos siguientes

Si es necesario, configure los parámetros de CHAP y las tramas gigantes.

Ver adaptadores de iSCSI de hardware dependiente

Se puede ver un adaptador de iSCSI de hardware dependiente para comprobar que esté correctamente cargado.

Si hay un adaptador de iSCSI de hardware dependiente (vmhba#) instalado, aparece en la lista de adaptadores de almacenamiento en una categoría, por ejemplo, Broadcom iSCSI Adapter (Adaptador de iSCSI Broadcom). Si el adaptador de hardware dependiente no aparece en la lista de adaptadores de almacenamiento, compruebe si necesita una licencia. Consulte la documentación del proveedor.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento**.
- 4 Seleccione el adaptador (vmhba#) para verlo.

Aparecen los detalles predeterminados del adaptador, incluidos el nombre iSCSI, alias iSCSI y el estado.

Pasos siguientes

Aunque el adaptador de iSCSI dependiente esté habilitado de forma predeterminada, para que funcione, se debe configurar la red para el tráfico iSCSI y enlazar el adaptador al puerto VMkernel de iSCSI correspondiente. A continuación, se configuran las direcciones de detección y los parámetros CHAP.

Modificar propiedades generales de los adaptadores de iSCSI

Es posible modificar el alias y el nombre iSCSI predeterminados asignados a los adaptadores de iSCSI. En el caso de los adaptadores de iSCSI de hardware independientes, también se puede cambiar la configuración IP predeterminada.

Importante Cuando modifique cualquier propiedad predeterminada de los adaptadores de iSCSI, asegúrese de darle el formato correcto a los nombres y las direcciones IP.

Requisitos previos

Privilegios necesarios: **Host .Configuración.Configuración de la partición de almacenamiento**

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador (vmhba#) que desea configurar.
- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Properties** (Propiedades) y en **Edit** (Editar) en el panel General.
- 5 Para cambiar el nombre iSCSI predeterminado del adaptador, escriba el nuevo nombre.
Asegúrese de que el nombre que ingrese sea un nombre universal único y tenga el formato adecuado; de lo contrario, es posible que algunos dispositivos de almacenamiento no reconozcan el adaptador de iSCSI.
- 6 (opcional) Introduzca el alias iSCSI.
El alias es un nombre que se utiliza para identificar el adaptador de iSCSI.

Resultados

Si cambia el nombre iSCSI, este se utilizará en las nuevas sesiones de iSCSI. Para las sesiones existentes, no se utilizará la nueva configuración hasta que la sesión se cierre y se vuelva a iniciar.

Determinar la asociación entre iSCSI y los adaptadores de red

Puede crear conexiones de red para vincular adaptadores de red dependientes de iSCSI y físicos. Para crear las conexiones correctamente, se debe determinar el nombre de la NIC física con la que está asociado el adaptador de iSCSI de hardware dependiente.

Requisitos previos

En vSphere Web Client, desplácese hasta el adaptador de iSCSI de hardware dependiente (vmhba#). Consulte [Ver adaptadores de iSCSI de hardware dependiente](#).

Procedimiento

- 1 Seleccione el adaptador vmhba# y haga clic en la pestaña **Enlace de puertos de red** en Detalles de adaptador.
- 2 Haga clic en **Add** (Agregar).

El adaptador de red (vmnic#) que corresponde al adaptador de iSCSI dependiente aparece en la columna Physical Network Adapter (Adaptador de red físico).

Pasos siguientes

Si la columna VMkernel Adapter (Adaptador VMkernel) está vacía, cree un adaptador VMkernel (vmk#) para el adaptador de red físico (vmnic#) y vincúlelo con el iSCSI de hardware dependiente asociado. Consulte [Configurar la red de iSCSI](#).

Crear conexiones de red para iSCSI

Configure conexiones para el tráfico entre los adaptadores de iSCSI de hardware dependiente o de software y los adaptadores de red física.

En las siguientes tareas se analiza la configuración de la red iSCSI con un conmutador estándar de vSphere.

Si se utiliza un conmutador distribuido de vSphere con varios puertos de vínculo superior, para el enlace de puertos se debe crear un grupo de puertos distribuidos por separado por cada NIC física. A continuación, establezca la directiva de formación de equipos de forma tal que cada grupo de puertos distribuidos tenga un solo puerto de vínculo superior activo. Para obtener información detallada sobre los conmutadores distribuidos de vSphere, consulte la documentación de *Redes de vSphere*.

Procedimiento

- 1 [Crear un adaptador VMkernel único para iSCSI](#)

Conecte el VMkernel, que ejecuta servicios para almacenamiento iSCSI, a un adaptador de red física.

- 2 [Crear adaptadores VMkernel adicionales para iSCSI](#)

Utilice esta tarea si tiene dos o más adaptadores de red físicos para iSCSI y desea conectar todos los adaptadores físicos a un solo conmutador estándar de vSphere. En esta tarea, se agregan los adaptadores físicos y los adaptadores VMkernel a un conmutador estándar de vSphere.

- 3 [Cambiar directiva de red para iSCSI](#)

Si utiliza un solo conmutador estándar de vSphere para conectar varios adaptadores VMkernel a varios adaptadores de red, configure la directiva de red de forma que solo un adaptador de red físico esté activo para cada adaptador VMkernel.

- 4 [Vincular adaptadores VMkernel e iSCSI](#)

Vincule un adaptador de iSCSI con un adaptador VMkernel.

5 Revisar detalles de enlace de puertos

Revise los detalles de redes del adaptador VMkernel enlazado al adaptador de iSCSI.

Crear un adaptador VMkernel único para iSCSI

Conecte el VMkernel, que ejecuta servicios para almacenamiento iSCSI, a un adaptador de red física.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en **Acciones > Agregar redes**.
- 3 Seleccione **Adaptador de red de VMkernel** y haga clic en **Siguiente**.
- 4 Seleccione **Nuevo conmutador estándar** para crear un conmutador estándar de vSphere.
- 5 Haga clic en el icono **Add adapters** (Agregar adaptadores) y seleccione el adaptador de red (vmnic#) para utilizarlo en iSCSI.

Asegúrese de asignar el adaptador a Active Adapters (Adaptadores activos).

Importante Si crea un adaptador VMkernel para de iSCSI hardware dependiente, seleccione el adaptador de red que corresponda al componente iSCSI. Consulte [Determinar la asociación entre iSCSI y los adaptadores de red](#).

- 6 Introduzca una etiqueta de red.

Una etiqueta de red es un nombre descriptivo que identifica al adaptador VMkernel que se está creando, por ejemplo, iSCSI.

- 7 Especifique la configuración IP.
- 8 Revise la información y haga clic en **Finish** (Finalizar).

Resultados

Creó el adaptador VMkernel virtual (vmk#) para un adaptador de red física (vmnic#) en el host.

Pasos siguientes

Si el host tiene un adaptador de red físico para tráfico iSCSI, debe enlazar el adaptador virtual que creó con el adaptador de iSCSI.

Si tiene varios adaptadores de red, cree adaptadores VMkernel adicionales y, a continuación, realice el enlace de iSCSI. La cantidad de adaptadores virtuales debe ser igual a la cantidad de adaptadores físicos del host.

Crear adaptadores VMkernel adicionales para iSCSI

Utilice esta tarea si tiene dos o más adaptadores de red físicos para iSCSI y desea conectar todos los adaptadores físicos a un solo conmutador estándar de vSphere. En esta tarea, se agregan los adaptadores físicos y los adaptadores VMkernel a un conmutador estándar de vSphere.

Requisitos previos

Cree un conmutador estándar de vSphere que asigne un adaptador VMkernel de iSCSI a un solo adaptador de red físico designado para el tráfico iSCSI.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar** y en **Redes**.
- 3 Haga clic en **Conmutadores virtuales** y, desde la lista, seleccione el conmutador de vSphere que desea modificar.
- 4 Conecte los adaptadores de red adicionales al conmutador.
 - a Haga clic en el icono **Add host networking** (Agregar redes de host).
 - b Seleccione **Physical Network Adapters** (Adaptadores de red físicos) y haga clic en **Next** (Siguiente).
 - c Asegúrese de estar utilizando el conmutador existente y haga clic en **Next** (Siguiente).
 - d Haga clic en el icono **Add adapters** (Agregar adaptadores) y seleccione uno o más adaptadores (vmnic#) para utilizar con iSCSI.

Con adaptadores de iSCSI por hardware dependiente, seleccione solo las NIC que tienen un componente iSCSI correspondiente.
 - e Complete la configuración y haga clic en **Finish** (Finalizar).
- 5 Cree los adaptadores VMkernel de iSCSI para todos los adaptadores de red físicos que agregó.

La cantidad de interfaces VMkernel debe corresponderse con la cantidad de adaptadores de red físicos en el conmutador estándar de vSphere.
 - a Haga clic en el icono **Add host networking** (Agregar redes de host).
 - b Seleccione **Adaptador de red de VMkernel** y haga clic en **Siguiente**.
 - c Asegúrese de estar utilizando el conmutador existente y haga clic en **Next** (Siguiente).
 - d Complete la configuración y haga clic en **Finish** (Finalizar).

Pasos siguientes

Cambie la directiva de red de todos los adaptadores VMkernel para que solo un adaptador de red físico esté activo para cada adaptador VMkernel. A continuación, puede enlazar los adaptadores VMkernel iSCSI con el software iSCSI o los adaptadores de iSCSI de hardware dependiente.

Cambiar directiva de red para iSCSI

Si utiliza un solo conmutador estándar de vSphere para conectar varios adaptadores VMkernel a varios adaptadores de red, configure la directiva de red de forma que solo un adaptador de red físico esté activo para cada adaptador VMkernel.

De forma predeterminada, para cada adaptador VMkernel del conmutador estándar de vSphere, todos los adaptadores de red aparecen como activos. Debe anular esta configuración para que cada adaptador VMkernel se asigne a un solo físico activo correspondiente. Por ejemplo, vmk1 se asigna a vmnic1, vmk2 se asigna a vmnic2 y así sucesivamente.

Requisitos previos

Cree un conmutador estándar de vSphere que conecte el VMkernel con adaptadores de red físicos diseñados para el tráfico iSCSI. La cantidad de adaptadores VMkernel debe ser igual a la cantidad de adaptadores físicos en el conmutador estándar de vSphere.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar** y en **Redes**.
- 3 Haga clic en **Conmutadores virtuales** y, desde la lista, seleccione el conmutador de vSphere que desea modificar.
- 4 En el diagrama de vSwitch, seleccione el adaptador VMkernel y haga clic en el icono **Edit Settings** (Editar configuración).
- 5 En el asistente **Edit Settings** (Editar configuración), haga clic en **Teaming and Failover** (Formación de equipos y conmutación por error) y haga clic en **Override** (Anular) en Failover Order (Orden de conmutación por error).
- 6 Designe como activo solo un adaptador físico y mueva los demás adaptadores a la categoría **Unused Adapters** (Adaptadores sin utilizar).
- 7 Repita del [Paso 4](#) al [Paso 6](#) para cada interfaz VMkernel iSCSI en el conmutador estándar de vSphere.

Ejemplo: Directiva de red de iSCSI

La tabla siguiente muestra la asignación de iSCSI adecuada en la que solo un adaptador de red físico está activo para cada adaptador VMkernel.

Adaptador VMkernel (vmk#)	Adaptador de red físico (vmnic#)
vmk1	Active Adapters (Adaptadores activos) vmnic1
	Unused Adapters (Adaptadores sin utilizar) vmnic2
vmk2	Active Adapters (Adaptadores activos) vmnic2
	Unused Adapters (Adaptadores sin utilizar) vmnic1

Pasos siguientes

Después de realizar esta tarea, enlace los adaptadores virtuales VMkernel al software iSCSI o a los adaptadores de iSCSI de hardware dependiente.

Vincular adaptadores VMkernel e iSCSI

Vincule un adaptador de iSCSI con un adaptador VMkernel.

Requisitos previos

Cree un adaptador VMkernel virtual para cada adaptador de red físico del host. Si utiliza varios adaptadores VMkernel, configure la directiva de red correcta.

Privilegios necesarios: **Host.Configuración.Configuración de la partición de almacenamiento**

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Storage Adapters** (Adaptadores de almacenamiento) y seleccione en la lista el adaptador de iSCSI dependiente o de software para configurar.
- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Network Port Binding** (Enlace de puertos de red) y en **Add** (Agregar).
- 5 Seleccione un adaptador VMkernel para unir al adaptador de iSCSI.

Nota Asegúrese de que la directiva de red del adaptador VMkernel cumpla con los requisitos de unión.

Se puede vincular el adaptador de iSCSI de software con uno o más adaptadores VMkernel. En el caso de un adaptador de iSCSI de hardware dependiente, solo hay disponible un adaptador VMkernel asociado con la NIC física correcta.

- 6 Haga clic en **OK** (Aceptar).

Resultados

La conexión de red aparece en la lista de enlaces de puertos VMkernel para el adaptador de iSCSI.

Revisar detalles de enlace de puertos

Revise los detalles de redes del adaptador VMkernel enlazado al adaptador de iSCSI.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Storage Adapters** (Adaptadores de almacenamiento) y seleccione el adaptador de iSCSI de software o dependiente en la lista.
- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Network Port Binding** (Enlace de puertos de red) y en **View Details** (Ver detalles).
- 5 Revise la información sobre el adaptador VMkernel alternando entre las pestañas disponibles.

Configurar la detección dinámica o estática de iSCSI

Con la detección dinámica, cada vez que el iniciador se contacte con el sistema de almacenamiento iSCSI especificado, le enviará una solicitud de SendTargets. El sistema iSCSI le responde al iniciador y le suministra una lista de destinos disponibles. Además del método de detección dinámica, se puede utilizar una detección estática e introducir manualmente la información de los destinos.

Al configurar la detección estática o dinámica, solo se pueden agregar destinos iSCSI nuevos. No se puede cambiar ningún parámetro de un destino existente. Para hacer cambios, quite el destino existente y agregue uno nuevo.

Requisitos previos

Privilegios necesarios: **Host.Configuración.Configuración de la partición de almacenamiento**

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Storage Adapters** (Adaptadores de almacenamiento) y seleccione el adaptador de iSCSI que desea configurar en la lista.
- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Targets** (Destinos).
- 5 Configure el método de detección.

Opción	Descripción
Detección dinámica	<ol style="list-style-type: none"> a Haga clic en Dynamic Discovery (Detección dinámica) y, a continuación, en Add (Agregar). b Escriba la dirección IP o el nombre DNS del sistema de almacenamiento y haga clic en OK (Aceptar). c Vuelva a examinar el adaptador de iSCSI. <p>Después de establecer la sesión de SendTargets con el sistema iSCSI, el host completa la lista de detección estática con todos los destinos recién detectados.</p>
Detección estática	<ol style="list-style-type: none"> a Haga clic en Static Discovery (Detección estática) y, a continuación, en Add (Agregar). b Introduzca la información del destino y haga clic en OK (Aceptar). c Vuelva a examinar el adaptador de iSCSI.

Acerca del adaptador de iSCSI de software

La implementación de iSCSI basado en software permite utilizar NIC estándar para conectar el host a un destino iSCSI remoto en la red IP. El adaptador de iSCSI de software incorporado en ESXi facilita esta conexión gracias a la comunicación con la NIC física a través de la pila de red.

Para poder utilizar el adaptador de iSCSI de software, debe configurar las redes, activar el adaptador y configurar parámetros como las direcciones de detección y CHAP.

Nota Diseñe un adaptador de red independiente para iSCSI. No utilice iSCSI para adaptadores de 100 Mbps o más lentos.

Configurar adaptador de iSCSI de software

El flujo de trabajo de configuración del adaptador de iSCSI de software incluye estos pasos.

Procedimiento

1 Activar el adaptador de iSCSI de software

Se debe activar el adaptador de iSCSI de software para que el host puede utilizarlo para acceder al almacenamiento iSCSI.

2 Modificar propiedades generales de los adaptadores de iSCSI

Es posible modificar el alias y el nombre iSCSI predeterminados asignados a los adaptadores de iSCSI. En el caso de los adaptadores de iSCSI de hardware independientes, también se puede cambiar la configuración IP predeterminada.

3 Crear conexiones de red para iSCSI

Configure conexiones para el tráfico entre los adaptadores de iSCSI de hardware dependiente o de software y los adaptadores de red física.

4 Configurar la detección dinámica o estática de iSCSI

Con la detección dinámica, cada vez que el iniciador se contacte con el sistema de almacenamiento iSCSI especificado, le enviará una solicitud de SendTargets. El sistema iSCSI le responde al iniciador y le suministra una lista de destinos disponibles. Además del método de detección dinámica, se puede utilizar una detección estática e introducir manualmente la información de los destinos.

Pasos siguientes

Si es necesario, configure los parámetros de CHAP y las tramas gigantes.

Activar el adaptador de iSCSI de software

Se debe activar el adaptador de iSCSI de software para que el host puede utilizarlo para acceder al almacenamiento iSCSI.

Se puede activar un solo adaptador de iSCSI de software únicamente.

Requisitos previos

Privilegios necesarios: **Host.Configuración.Configuración de la partición de almacenamiento**

Nota Si se arranca desde iSCSI utilizando el adaptador de iSCSI de software, el adaptador queda habilitado y la configuración de red se crea en el primer arranque. Si se deshabilita el adaptador, se volverá a habilitar cada vez que se arranque el host.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y, a continuación, en el icono **Agregar (+)**.
- 4 Seleccione **Software iSCSI Adapter** (Adaptador de iSCSI de software) y confirme que desea agregar el adaptador.

Resultados

El adaptador de iSCSI de software (vmhba#) está habilitado y aparece en la lista de adaptadores de almacenamiento. Después de habilitar el adaptador, el host le asigna el nombre iSCSI predeterminado. Si debe cambiar el nombre predeterminado, siga las convenciones de nomenclatura de iSCSI.

Pasos siguientes

Seleccione el adaptador y utilice la sección Adapter Details (Detalles del adaptador) para completar la configuración.

Modificar propiedades generales de los adaptadores de iSCSI

Es posible modificar el alias y el nombre iSCSI predeterminados asignados a los adaptadores de iSCSI. En el caso de los adaptadores de iSCSI de hardware independientes, también se puede cambiar la configuración IP predeterminada.

Importante Cuando modifique cualquier propiedad predeterminada de los adaptadores de iSCSI, asegúrese de darle el formato correcto a los nombres y las direcciones IP.

Requisitos previos

Privilegios necesarios: **Host .Configuración.Configuración de la partición de almacenamiento**

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador (vmhba#) que desea configurar.
- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Properties** (Propiedades) y en **Edit** (Editar) en el panel General.
- 5 Para cambiar el nombre iSCSI predeterminado del adaptador, escriba el nuevo nombre.

Asegúrese de que el nombre que ingrese sea un nombre universal único y tenga el formato adecuado; de lo contrario, es posible que algunos dispositivos de almacenamiento no reconozcan el adaptador de iSCSI.

6 (opcional) Introduzca el alias iSCSI.

El alias es un nombre que se utiliza para identificar el adaptador de iSCSI.

Resultados

Si cambia el nombre iSCSI, este se utilizará en las nuevas sesiones de iSCSI. Para las sesiones existentes, no se utilizará la nueva configuración hasta que la sesión se cierre y se vuelva a iniciar.

Crear conexiones de red para iSCSI

Configure conexiones para el tráfico entre los adaptadores de iSCSI de hardware dependiente o de software y los adaptadores de red física.

En las siguientes tareas se analiza la configuración de la red iSCSI con un conmutador estándar de vSphere.

Si se utiliza un conmutador distribuido de vSphere con varios puertos de vínculo superior, para el enlace de puertos se debe crear un grupo de puertos distribuidos por separado por cada NIC física. A continuación, establezca la directiva de formación de equipos de forma tal que cada grupo de puertos distribuidos tenga un solo puerto de vínculo superior activo. Para obtener información detallada sobre los conmutadores distribuidos de vSphere, consulte la documentación de *Redes de vSphere*.

Procedimiento

1 Crear un adaptador VMkernel único para iSCSI

Conecte el VMkernel, que ejecuta servicios para almacenamiento iSCSI, a un adaptador de red física.

2 Crear adaptadores VMkernel adicionales para iSCSI

Utilice esta tarea si tiene dos o más adaptadores de red físicos para iSCSI y desea conectar todos los adaptadores físicos a un solo conmutador estándar de vSphere. En esta tarea, se agregan los adaptadores físicos y los adaptadores VMkernel a un conmutador estándar de vSphere.

3 Cambiar directiva de red para iSCSI

Si utiliza un solo conmutador estándar de vSphere para conectar varios adaptadores VMkernel a varios adaptadores de red, configure la directiva de red de forma que solo un adaptador de red físico esté activo para cada adaptador VMkernel.

4 Vincular adaptadores VMkernel e iSCSI

Vincule un adaptador de iSCSI con un adaptador VMkernel.

5 Revisar detalles de enlace de puertos

Revise los detalles de redes del adaptador VMkernel enlazado al adaptador de iSCSI.

Crear un adaptador VMkernel único para iSCSI

Conecte el VMkernel, que ejecuta servicios para almacenamiento iSCSI, a un adaptador de red física.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en **Acciones > Agregar redes**.
- 3 Seleccione **Adaptador de red de VMkernel** y haga clic en **Siguiente**.
- 4 Seleccione **Nuevo conmutador estándar** para crear un conmutador estándar de vSphere.
- 5 Haga clic en el icono **Add adapters** (Agregar adaptadores) y seleccione el adaptador de red (vmnic#) para utilizarlo en iSCSI.

Asegúrese de asignar el adaptador a Active Adapters (Adaptadores activos).

Importante Si crea un adaptador VMkernel para de iSCSI hardware dependiente, seleccione el adaptador de red que corresponda al componente iSCSI. Consulte [Determinar la asociación entre iSCSI y los adaptadores de red](#).

- 6 Introduzca una etiqueta de red.

Una etiqueta de red es un nombre descriptivo que identifica al adaptador VMkernel que se está creando, por ejemplo, iSCSI.

- 7 Especifique la configuración IP.
- 8 Revise la información y haga clic en **Finish** (Finalizar).

Resultados

Creó el adaptador VMkernel virtual (vmk#) para un adaptador de red física (vmnic#) en el host.

Pasos siguientes

Si el host tiene un adaptador de red físico para tráfico iSCSI, debe enlazar el adaptador virtual que creó con el adaptador de iSCSI.

Si tiene varios adaptadores de red, cree adaptadores VMkernel adicionales y, a continuación, realice el enlace de iSCSI. La cantidad de adaptadores virtuales debe ser igual a la cantidad de adaptadores físicos del host.

Crear adaptadores VMkernel adicionales para iSCSI

Utilice esta tarea si tiene dos o más adaptadores de red físicos para iSCSI y desea conectar todos los adaptadores físicos a un solo conmutador estándar de vSphere. En esta tarea, se agregan los adaptadores físicos y los adaptadores VMkernel a un conmutador estándar de vSphere.

Requisitos previos

Cree un conmutador estándar de vSphere que asigne un adaptador VMkernel de iSCSI a un solo adaptador de red físico designado para el tráfico iSCSI.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.

- 2 Haga clic en la pestaña **Configurar** y en **Redes**.
- 3 Haga clic en **Conmutadores virtuales** y, desde la lista, seleccione el conmutador de vSphere que desea modificar.
- 4 Conecte los adaptadores de red adicionales al conmutador.
 - a Haga clic en el icono **Add host networking** (Agregar redes de host).
 - b Seleccione **Physical Network Adapters** (Adaptadores de red físicos) y haga clic en **Next** (Siguiendo).
 - c Asegúrese de estar utilizando el conmutador existente y haga clic en **Next** (Siguiendo).
 - d Haga clic en el icono **Add adapters** (Agregar adaptadores) y seleccione uno o más adaptadores (vmnic#) para utilizar con iSCSI.

Con adaptadores de iSCSI por hardware dependiente, seleccione solo las NIC que tienen un componente iSCSI correspondiente.
 - e Complete la configuración y haga clic en **Finish** (Finalizar).
- 5 Cree los adaptadores VMkernel de iSCSI para todos los adaptadores de red físicos que agregó.

La cantidad de interfaces VMkernel debe corresponderse con la cantidad de adaptadores de red físicos en el conmutador estándar de vSphere.
 - a Haga clic en el icono **Add host networking** (Agregar redes de host).
 - b Seleccione **Adaptador de red de VMkernel** y haga clic en **Siguiente**.
 - c Asegúrese de estar utilizando el conmutador existente y haga clic en **Next** (Siguiendo).
 - d Complete la configuración y haga clic en **Finish** (Finalizar).

Pasos siguientes

Cambie la directiva de red de todos los adaptadores VMkernel para que solo un adaptador de red físico esté activo para cada adaptador VMkernel. A continuación, puede enlazar los adaptadores VMkernel iSCSI con el software iSCSI o los adaptadores de iSCSI de hardware dependiente.

Cambiar directiva de red para iSCSI

Si utiliza un solo conmutador estándar de vSphere para conectar varios adaptadores VMkernel a varios adaptadores de red, configure la directiva de red de forma que solo un adaptador de red físico esté activo para cada adaptador VMkernel.

De forma predeterminada, para cada adaptador VMkernel del conmutador estándar de vSphere, todos los adaptadores de red aparecen como activos. Debe anular esta configuración para que cada adaptador VMkernel se asigne a un solo físico activo correspondiente. Por ejemplo, vmk1 se asigna a vmnic1, vmk2 se asigna a vmnic2 y así sucesivamente.

Requisitos previos

Cree un conmutador estándar de vSphere que conecte el VMkernel con adaptadores de red físicos diseñados para el tráfico iSCSI. La cantidad de adaptadores VMkernel debe ser igual a la cantidad de adaptadores físicos en el conmutador estándar de vSphere.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar** y en **Redes**.
- 3 Haga clic en **Conmutadores virtuales** y, desde la lista, seleccione el conmutador de vSphere que desea modificar.
- 4 En el diagrama de vSwitch, seleccione el adaptador VMkernel y haga clic en el icono **Edit Settings** (Editar configuración).
- 5 En el asistente **Edit Settings** (Editar configuración), haga clic en **Teaming and Failover** (Formación de equipos y conmutación por error) y haga clic en **Override** (Anular) en Failover Order (Orden de conmutación por error).
- 6 Designe como activo solo un adaptador físico y mueva los demás adaptadores a la categoría **Unused Adapters** (Adaptadores sin utilizar).
- 7 Repita del [Paso 4](#) al [Paso 6](#) para cada interfaz VMkernel iSCSI en el conmutador estándar de vSphere.

Ejemplo: Directiva de red de iSCSI

La tabla siguiente muestra la asignación de iSCSI adecuada en la que solo un adaptador de red físico está activo para cada adaptador VMkernel.

Adaptador VMkernel (vmk#)	Adaptador de red físico (vmnic#)
vmk1	Active Adapters (Adaptadores activos) vmnic1
	Unused Adapters (Adaptadores sin utilizar) vmnic2
vmk2	Active Adapters (Adaptadores activos) vmnic2
	Unused Adapters (Adaptadores sin utilizar) vmnic1

Pasos siguientes

Después de realizar esta tarea, enlace los adaptadores virtuales VMkernel al software iSCSI o a los adaptadores de iSCSI de hardware dependiente.

Vincular adaptadores VMkernel e iSCSI

Vincule un adaptador de iSCSI con un adaptador VMkernel.

Requisitos previos

Cree un adaptador VMkernel virtual para cada adaptador de red físico del host. Si utiliza varios adaptadores VMkernel, configure la directiva de red correcta.

Privilegios necesarios: **Host.Configuración.Configuración de la partición de almacenamiento**

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Storage Adapters** (Adaptadores de almacenamiento) y seleccione en la lista el adaptador de iSCSI dependiente o de software para configurar.
- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Network Port Binding** (Enlace de puertos de red) y en **Add** (Agregar).
- 5 Seleccione un adaptador VMkernel para unir al adaptador de iSCSI.

Nota Asegúrese de que la directiva de red del adaptador VMkernel cumpla con los requisitos de unión.

Se puede vincular el adaptador de iSCSI de software con uno o más adaptadores VMkernel. En el caso de un adaptador de iSCSI de hardware dependiente, solo hay disponible un adaptador VMkernel asociado con la NIC física correcta.

- 6 Haga clic en **OK** (Aceptar).

Resultados

La conexión de red aparece en la lista de enlaces de puertos VMkernel para el adaptador de iSCSI.

Revisar detalles de enlace de puertos

Revise los detalles de redes del adaptador VMkernel enlazado al adaptador de iSCSI.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Storage Adapters** (Adaptadores de almacenamiento) y seleccione el adaptador de iSCSI de software o dependiente en la lista.
- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Network Port Binding** (Enlace de puertos de red) y en **View Details** (Ver detalles).
- 5 Revise la información sobre el adaptador VMkernel alternando entre las pestañas disponibles.

Configurar la detección dinámica o estática de iSCSI

Con la detección dinámica, cada vez que el iniciador se contacte con el sistema de almacenamiento iSCSI especificado, le enviará una solicitud de SendTargets. El sistema iSCSI le responde al iniciador y le suministra una lista de destinos disponibles. Además del método de detección dinámica, se puede utilizar una detección estática e introducir manualmente la información de los destinos.

Al configurar la detección estática o dinámica, solo se pueden agregar destinos iSCSI nuevos. No se puede cambiar ningún parámetro de un destino existente. Para hacer cambios, quite el destino existente y agregue uno nuevo.

Requisitos previos

Privilegios necesarios: **Host.Configuración.Configuración de la partición de almacenamiento**

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Storage Adapters** (Adaptadores de almacenamiento) y seleccione el adaptador de iSCSI que desea configurar en la lista.
- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Targets** (Destinos).
- 5 Configure el método de detección.

Opción	Descripción
Detección dinámica	<ol style="list-style-type: none"> a Haga clic en Dynamic Discovery (Detección dinámica) y, a continuación, en Add (Agregar). b Escriba la dirección IP o el nombre DNS del sistema de almacenamiento y haga clic en OK (Aceptar). c Vuelva a examinar el adaptador de iSCSI. <p>Después de establecer la sesión de SendTargets con el sistema iSCSI, el host completa la lista de detección estática con todos los destinos recién detectados.</p>
Detección estática	<ol style="list-style-type: none"> a Haga clic en Static Discovery (Detección estática) y, a continuación, en Add (Agregar). b Introduzca la información del destino y haga clic en OK (Aceptar). c Vuelva a examinar el adaptador de iSCSI.

Deshabilitar el adaptador de iSCSI de software

Si no necesita el adaptador de iSCSI de software, puede deshabilitarlo.

Al deshabilitar el adaptador de iSCSI de software, se lo marca para su eliminación. El adaptador se quitará del host durante el próximo reinicio del host. Después de su eliminación, todas las máquinas virtuales y otros datos en los dispositivos de almacenamiento relacionados con este adaptador quedan inaccesibles para el host.

Requisitos previos

Privilegios necesarios: **Host.Configuración.Configuración de la partición de almacenamiento**

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Storage Adapters** (Adaptadores de almacenamiento) y seleccione el adaptador de iSCSI de software en la lista.
- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Properties** (Propiedades).
- 5 Haga clic en **Disable** (Deshabilitar) y confirme que desea deshabilitar el adaptador.
El estado indica que el adaptador está deshabilitado.
- 6 Reinicie el host.
Después del reinicio, el adaptador ya no aparece en la lista de adaptadores de almacenamiento.

Resultados

El adaptador de iSCSI de software ya no está disponible, y no se puede acceder a los dispositivos de almacenamiento asociados con él. Puede activar el adaptador más adelante.

Modificar propiedades generales de los adaptadores de iSCSI

Es posible modificar el alias y el nombre iSCSI predeterminados asignados a los adaptadores de iSCSI. En el caso de los adaptadores de iSCSI de hardware independientes, también se puede cambiar la configuración IP predeterminada.

Importante Cuando modifique cualquier propiedad predeterminada de los adaptadores de iSCSI, asegúrese de darle el formato correcto a los nombres y las direcciones IP.

Requisitos previos

Privilegios necesarios: **Host .Configuración.Configuración de la partición de almacenamiento**

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador (vmhba#) que desea configurar.
- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Properties** (Propiedades) y en **Edit** (Editar) en el panel General.

- 5 Para cambiar el nombre iSCSI predeterminado del adaptador, escriba el nuevo nombre.

Asegúrese de que el nombre que ingrese sea un nombre universal único y tenga el formato adecuado; de lo contrario, es posible que algunos dispositivos de almacenamiento no reconozcan el adaptador de iSCSI.

- 6 (opcional) Introduzca el alias iSCSI.

El alias es un nombre que se utiliza para identificar el adaptador de iSCSI.

Resultados

Si cambia el nombre iSCSI, este se utilizará en las nuevas sesiones de iSCSI. Para las sesiones existentes, no se utilizará la nueva configuración hasta que la sesión se cierre y se vuelva a iniciar.

Configurar la red de iSCSI

Los adaptadores de iSCSI de hardware dependiente y software dependen de las redes VMkernel. Si utiliza los adaptadores de iSCSI de hardware dependiente o software, debe configurar conexiones para el tráfico entre el componente iSCSI y los adaptadores de red físicos.

La configuración de la conexión de red implica la creación de un adaptador VMkernel virtual para cada adaptador de red físico. A continuación, asocia el adaptador VMkernel con un adaptador de iSCSI adecuado. Este proceso se conoce como enlace de puertos.

Para observar las consideraciones específicas sobre cuándo y cómo utilizar las conexiones de red con iSCSI de software, consulte el artículo de la base de conocimientos de VMware en <http://kb.vmware.com/kb/2038869>.

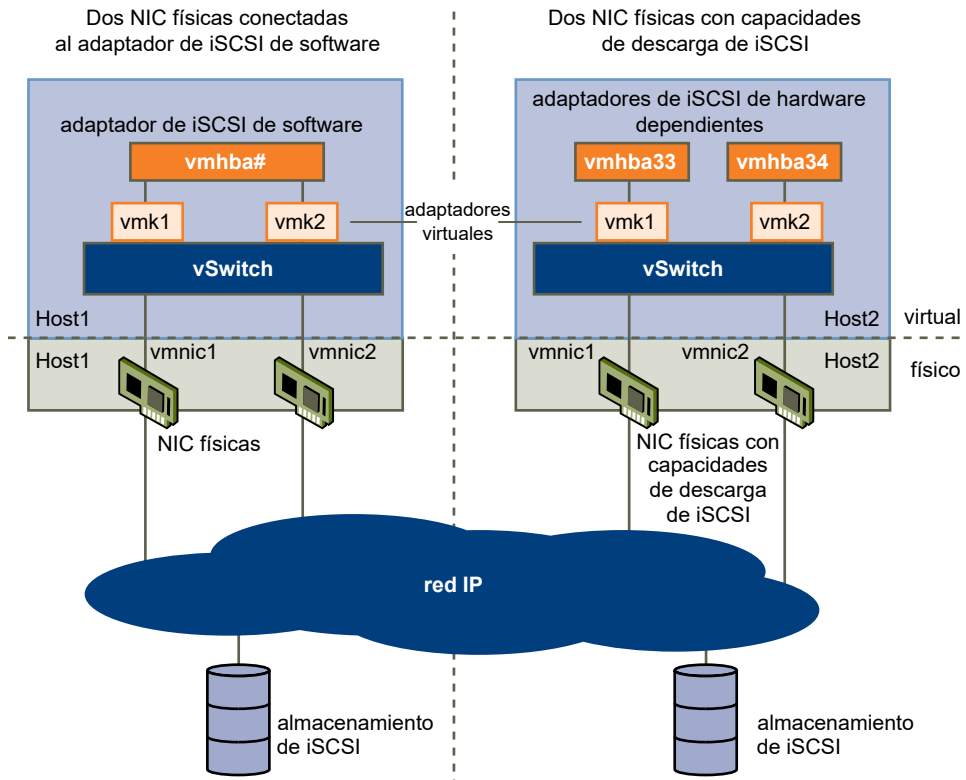
Varios adaptadores de red en la configuración de iSCSI

Si el host tiene más de un adaptador de red físico para iSCSI de hardware dependiente y software, utilice los adaptadores para múltiples rutas.

Puede conectar el adaptador de iSCSI de software con cualquier NIC física disponible en el host. Los adaptadores de iSCSI dependientes deben estar conectados solo a sus propias NIC físicas.

Nota Las NIC físicas deben estar en la misma subred que el sistema de almacenamiento iSCSI al que se conectan.

Figura 10-1. Redes con iSCSI



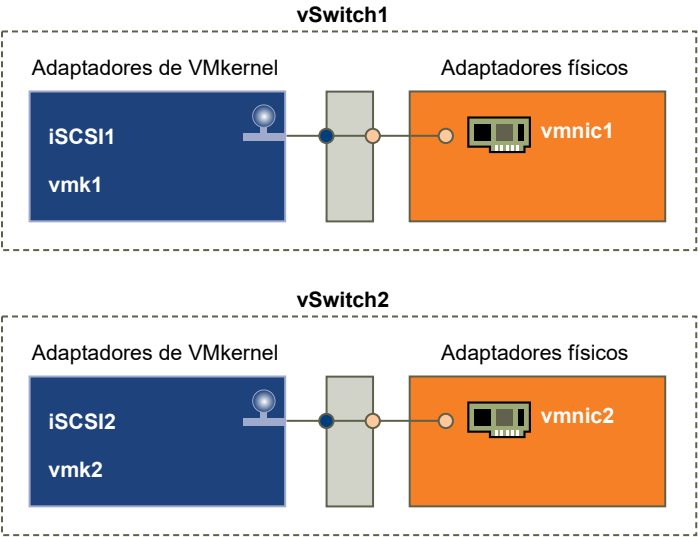
El adaptador de iSCSI y la NIC física se conectan a través de un adaptador VMkernel virtual, también llamado adaptador de red virtual o puerto VMkernel. Se crea un adaptador VMkernel (vmk) en un conmutador de vSphere (vSwitch) con una asignación 1:1 entre cada adaptador de red físico y virtual.

Una forma de lograr la asignación 1:1 cuando se dispone de varias NIC es designar un conmutador de vSphere distinto para cada par de adaptadores virtual a físico.

Nota Si se utilizan conmutadores de vSphere distintos, estos se deben conectar a distintas subredes IP. De lo contrario, los adaptadores VMkernel pueden experimentar problemas de conectividad y el host no podrá detectar los LUN de iSCSI.

Los ejemplos siguientes muestran configuraciones que utilizan conmutadores estándar de vSphere, pero también se pueden utilizar conmutadores distribuidos. Para obtener más información acerca de los conmutadores distribuidos de vSphere, consulte la documentación de *Redes de vSphere*.

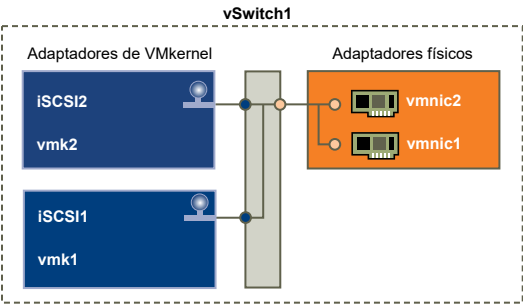
Figura 10-2. Asignar adaptadores 1:1 en conmutadores estándar de vSphere distintos



Una alternativa es agregar todas las NIC y los adaptadores VMkernel a un solo conmutador estándar de vSphere. En este caso, se debe anular la configuración de red predeterminada y comprobar que cada adaptador VMkernel se asigne a solo un adaptador físico activo correspondiente.

Nota Se debe utilizar la configuración de un solo vSwitch si los adaptadores VMkernel están en la misma subred.

Figura 10-3. Asignar adaptadores 1:1 en un conmutador estándar de vSphere



La tabla siguiente resume la configuración de redes iSCSI que se trata en este tema.

Tabla 10-2. Configuración de redes para iSCSI

Adaptadores de iSCSI	Adaptadores VMkernel (Puertos)	Adaptadores físicos (NIC)
iSCSI de software		
vmhba32	vmk1	vmnic1
	vmk2	vmnic2
iSCSI de hardware dependiente		

Tabla 10-2. Configuración de redes para iSCSI (continuación)

Adaptadores de iSCSI	Adaptadores VMkernel (Puertos)	Adaptadores físicos (NIC)
vmhba33	vmk1	vmnic1
vmhba34	vmk2	vmnic2

Instrucciones de utilización de enlace de puertos iSCSI en ESXi

Puede utilizar varios adaptadores VMkernel enlazados a iSCSI para tener varias rutas de acceso a una matriz iSCSI que transmita una sola dirección IP.

Cuando utilice enlace de puertos para múltiples rutas, siga estas instrucciones:

- Los puertos iSCSI del destino de matriz deben residir en el mismo dominio de difusión y la misma subred IP que los adaptadores VMkernel.
- Todos los adaptadores VMkernel utilizados para el enlace de puertos iSCSI deben residir en el mismo dominio de difusión y la misma subred IP.
- Todos los adaptadores VMkernel utilizados para la conectividad iSCSI deben residir en el mismo conmutador virtual.
- El enlace de puertos no admite el enrutamiento de red.

No utilice enlace de puertos ante cualquiera de las siguientes condiciones:

- Los puertos iSCSI del destino de matriz están en un dominio de difusión y subred IP diferente.
- Los adaptadores VMkernel utilizados para la conectividad iSCSI existen en diferentes dominios de difusión, subredes IP o utilizan conmutadores virtuales distintos.
- Se requiere enrutamiento para comunicarse con la matriz iSCSI.

Crear conexiones de red para iSCSI

Configure conexiones para el tráfico entre los adaptadores de iSCSI de hardware dependiente o de software y los adaptadores de red física.

En las siguientes tareas se analiza la configuración de la red iSCSI con un conmutador estándar de vSphere.

Si se utiliza un conmutador distribuido de vSphere con varios puertos de vínculo superior, para el enlace de puertos se debe crear un grupo de puertos distribuidos por separado por cada NIC física. A continuación, establezca la directiva de formación de equipos de forma tal que cada grupo de puertos distribuidos tenga un solo puerto de vínculo superior activo. Para obtener información detallada sobre los conmutadores distribuidos de vSphere, consulte la documentación de *Redes de vSphere*.

Procedimiento

1 Crear un adaptador VMkernel único para iSCSI

Conecte el VMkernel, que ejecuta servicios para almacenamiento iSCSI, a un adaptador de red física.

2 Crear adaptadores VMkernel adicionales para iSCSI

Utilice esta tarea si tiene dos o más adaptadores de red físicos para iSCSI y desea conectar todos los adaptadores físicos a un solo conmutador estándar de vSphere. En esta tarea, se agregan los adaptadores físicos y los adaptadores VMkernel a un conmutador estándar de vSphere.

3 Cambiar directiva de red para iSCSI

Si utiliza un solo conmutador estándar de vSphere para conectar varios adaptadores VMkernel a varios adaptadores de red, configure la directiva de red de forma que solo un adaptador de red físico esté activo para cada adaptador VMkernel.

4 Vincular adaptadores VMkernel e iSCSI

Vincule un adaptador de iSCSI con un adaptador VMkernel.

5 Revisar detalles de enlace de puertos

Revise los detalles de redes del adaptador VMkernel enlazado al adaptador de iSCSI.

Crear un adaptador VMkernel único para iSCSI

Conecte el VMkernel, que ejecuta servicios para almacenamiento iSCSI, a un adaptador de red física.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en **Acciones > Agregar redes**.
- 3 Seleccione **Adaptador de red de VMkernel** y haga clic en **Siguiente**.
- 4 Seleccione **Nuevo conmutador estándar** para crear un conmutador estándar de vSphere.

- 5 Haga clic en el icono **Add adapters** (Agregar adaptadores) y seleccione el adaptador de red (vmnic#) para utilizarlo en iSCSI.

Asegúrese de asignar el adaptador a Active Adapters (Adaptadores activos).

Importante Si crea un adaptador VMkernel para de iSCSI hardware dependiente, seleccione el adaptador de red que corresponda al componente iSCSI. Consulte [Determinar la asociación entre iSCSI y los adaptadores de red](#).

- 6 Introduzca una etiqueta de red.

Una etiqueta de red es un nombre descriptivo que identifica al adaptador VMkernel que se está creando, por ejemplo, iSCSI.

- 7 Especifique la configuración IP.
- 8 Revise la información y haga clic en **Finish** (Finalizar).

Resultados

Creó el adaptador VMkernel virtual (vmk#) para un adaptador de red física (vmnic#) en el host.

Pasos siguientes

Si el host tiene un adaptador de red físico para tráfico iSCSI, debe enlazar el adaptador virtual que creó con el adaptador de iSCSI.

Si tiene varios adaptadores de red, cree adaptadores VMkernel adicionales y, a continuación, realice el enlace de iSCSI. La cantidad de adaptadores virtuales debe ser igual a la cantidad de adaptadores físicos del host.

Crear adaptadores VMkernel adicionales para iSCSI

Utilice esta tarea si tiene dos o más adaptadores de red físicos para iSCSI y desea conectar todos los adaptadores físicos a un solo conmutador estándar de vSphere. En esta tarea, se agregan los adaptadores físicos y los adaptadores VMkernel a un conmutador estándar de vSphere.

Requisitos previos

Cree un conmutador estándar de vSphere que asigne un adaptador VMkernel de iSCSI a un solo adaptador de red físico designado para el tráfico iSCSI.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar** y en **Redes**.
- 3 Haga clic en **Conmutadores virtuales** y, desde la lista, seleccione el conmutador de vSphere que desea modificar.

- 4 Conecte los adaptadores de red adicionales al conmutador.
 - a Haga clic en el icono **Add host networking** (Agregar redes de host).
 - b Seleccione **Physical Network Adapters** (Adaptadores de red físicos) y haga clic en **Next** (Siguiente).
 - c Asegúrese de estar utilizando el conmutador existente y haga clic en **Next** (Siguiente).
 - d Haga clic en el icono **Add adapters** (Agregar adaptadores) y seleccione uno o más adaptadores (vmnic#) para utilizar con iSCSI.

Con adaptadores de iSCSI por hardware dependiente, seleccione solo las NIC que tienen un componente iSCSI correspondiente.

- e Complete la configuración y haga clic en **Finish** (Finalizar).
- 5 Cree los adaptadores VMkernel de iSCSI para todos los adaptadores de red físicos que agregó.

La cantidad de interfaces VMkernel debe corresponderse con la cantidad de adaptadores de red físicos en el conmutador estándar de vSphere.

- a Haga clic en el icono **Add host networking** (Agregar redes de host).
 - b Seleccione **Adaptador de red de VMkernel** y haga clic en **Siguiente**.
 - c Asegúrese de estar utilizando el conmutador existente y haga clic en **Next** (Siguiente).
 - d Complete la configuración y haga clic en **Finish** (Finalizar).

Pasos siguientes

Cambie la directiva de red de todos los adaptadores VMkernel para que solo un adaptador de red físico esté activo para cada adaptador VMkernel. A continuación, puede enlazar los adaptadores VMkernel iSCSI con el software iSCSI o los adaptadores de iSCSI de hardware dependiente.

Cambiar directiva de red para iSCSI

Si utiliza un solo conmutador estándar de vSphere para conectar varios adaptadores VMkernel a varios adaptadores de red, configure la directiva de red de forma que solo un adaptador de red físico esté activo para cada adaptador VMkernel.

De forma predeterminada, para cada adaptador VMkernel del conmutador estándar de vSphere, todos los adaptadores de red aparecen como activos. Debe anular esta configuración para que cada adaptador VMkernel se asigne a un solo físico activo correspondiente. Por ejemplo, vmk1 se asigna a vmnic1, vmk2 se asigna a vmnic2 y así sucesivamente.

Requisitos previos

Cree un conmutador estándar de vSphere que conecte el VMkernel con adaptadores de red físicos diseñados para el tráfico iSCSI. La cantidad de adaptadores VMkernel debe ser igual a la cantidad de adaptadores físicos en el conmutador estándar de vSphere.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar** y en **Redes**.
- 3 Haga clic en **Conmutadores virtuales** y, desde la lista, seleccione el conmutador de vSphere que desea modificar.
- 4 En el diagrama de vSwitch, seleccione el adaptador VMkernel y haga clic en el icono **Edit Settings** (Editar configuración).
- 5 En el asistente **Edit Settings** (Editar configuración), haga clic en **Teaming and Failover** (Formación de equipos y conmutación por error) y haga clic en **Override** (Anular) en Failover Order (Orden de conmutación por error).
- 6 Designe como activo solo un adaptador físico y mueva los demás adaptadores a la categoría **Unused Adapters** (Adaptadores sin utilizar).
- 7 Repita del [Paso 4](#) al [Paso 6](#) para cada interfaz VMkernel iSCSI en el conmutador estándar de vSphere.

Ejemplo: Directiva de red de iSCSI

La tabla siguiente muestra la asignación de iSCSI adecuada en la que solo un adaptador de red físico está activo para cada adaptador VMkernel.

Adaptador VMkernel (vmk#)	Adaptador de red físico (vmnic#)
vmk1	Active Adapters (Adaptadores activos) vmnic1
	Unused Adapters (Adaptadores sin utilizar) vmnic2
vmk2	Active Adapters (Adaptadores activos) vmnic2
	Unused Adapters (Adaptadores sin utilizar) vmnic1

Pasos siguientes

Después de realizar esta tarea, enlace los adaptadores virtuales VMkernel al software iSCSI o a los adaptadores de iSCSI de hardware dependiente.

Vincular adaptadores VMkernel e iSCSI

Vincule un adaptador de iSCSI con un adaptador VMkernel.

Requisitos previos

Cree un adaptador VMkernel virtual para cada adaptador de red físico del host. Si utiliza varios adaptadores VMkernel, configure la directiva de red correcta.

Privilegios necesarios: **Host.Configuración.Configuración de la partición de almacenamiento**

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Storage Adapters** (Adaptadores de almacenamiento) y seleccione en la lista el adaptador de iSCSI dependiente o de software para configurar.
- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Network Port Binding** (Enlace de puertos de red) y en **Add** (Agregar).
- 5 Seleccione un adaptador VMkernel para unir al adaptador de iSCSI.

Nota Asegúrese de que la directiva de red del adaptador VMkernel cumpla con los requisitos de unión.

Se puede vincular el adaptador de iSCSI de software con uno o más adaptadores VMkernel. En el caso de un adaptador de iSCSI de hardware dependiente, solo hay disponible un adaptador VMkernel asociado con la NIC física correcta.

- 6 Haga clic en **OK** (Aceptar).

Resultados

La conexión de red aparece en la lista de enlaces de puertos VMkernel para el adaptador de iSCSI.

Revisar detalles de enlace de puertos

Revise los detalles de redes del adaptador VMkernel enlazado al adaptador de iSCSI.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Storage Adapters** (Adaptadores de almacenamiento) y seleccione el adaptador de iSCSI de software o dependiente en la lista.
- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Network Port Binding** (Enlace de puertos de red) y en **View Details** (Ver detalles).
- 5 Revise la información sobre el adaptador VMkernel alternando entre las pestañas disponibles.

Administrar una red iSCSI

Se aplican consideraciones especiales a adaptadores de red, tanto físicos como VMkernel, que están asociados con un adaptador de iSCSI.

Después de crear conexiones de red para iSCSI, se habilita un indicador de iSCSI en distintos cuadros de diálogo de redes. Este indicador muestra que un adaptador de red virtual o físico está enlazado con iSCSI. Para evitar interrupciones en el tráfico iSCSI, siga estas instrucciones y consideraciones al administrar adaptadores de red virtuales y físicos enlazados con iSCSI:

- Asegúrese de que los adaptadores de red del VMkernel tengan asignadas direcciones en la misma subred que el portal de almacenamiento iSCSI al que se conectan.
- Los adaptadores de iSCSI que usan adaptadores VMkernel no pueden conectarse a puertos de iSCSI en diferentes subredes, incluso si los adaptadores de iSCSI detectan esos puertos.
- Al usar conmutadores vSphere individuales para conectar adaptadores de red físicos y adaptadores VMkernel, asegúrese de que los conmutadores vSphere se conecten con subredes de diferente IP.
- Si los adaptadores VMkernel están en la misma subred, deben conectarse a un solo vSwitch.
- Si migra adaptadores VMkernel a un conmutador de vSphere diferente, mueva los adaptadores físicos asociados.
- No cambie la configuración de los adaptadores VMkernel o los adaptadores de red físicos enlazados con iSCSI.
- No realice cambios que puedan romper la asociación de adaptadores VMkernel y adaptadores de red físicos. Puede romper la asociación si elimina uno de los adaptadores o el conmutador de vSphere que los conecta, o si cambia la directiva de red 1:1 para su conexión.

Solucionar problemas de red de iSCSI

Un cartel de advertencia indica que una directiva de grupo de puertos no cumple con los requisitos de un adaptador VMkernel enlazado con iSCSI.

Problema

Se considera que la directiva de grupo de puertos del adaptador VMkernel no cumple con los requisitos en los casos siguientes:

- El adaptador VMkernel no está conectado a un adaptador de red físico activo.
- El adaptador VMkernel está conectado a más de un adaptador de red físico.
- El adaptador VMkernel está conectado a uno o más adaptadores físicos en espera.
- Se cambia el adaptador físico activo.

Solución

Siga los pasos en [Cambiar directiva de red para iSCSI](#) para configurar la directiva de red correcta para el adaptador VMkernel enlazado con iSCSI.

Usar tramas gigantes con iSCSI

ESXi admite la utilización de tramas gigantes con iSCSI.

Las tramas gigantes son tramas Ethernet con un tamaño superior a 1.500 bytes. El parámetro de unidad de transmisión máxima (MTU) generalmente se utiliza para medir el tamaño de las tramas gigantes. ESXi permite tramas gigantes con una MTU de hasta 9.000 bytes.

Cuando se utilizan tramas gigantes para el tráfico iSCSI, aplican las consideraciones siguientes:

- La red debe ser compatible con tramas gigantes de extremo a extremo para que las tramas gigantes sean eficaces.
- Consulte con los proveedores para asegurarse de que las NIC físicas y los HBA de iSCSI sean compatibles con tramas gigantes.
- Para configurar y comprobar conmutadores de red físicos para tramas gigantes, consulte la documentación del proveedor.

La tabla siguiente explica el nivel de compatibilidad que proporciona ESXi para las tramas gigantes.

Tabla 10-3. Compatibilidad con tramas gigantes

Tipo de adaptadores de iSCSI	Compatibilidad con tramas gigantes
iSCSI de software	Compatible
iSCSI de hardware dependiente	Compatible. Compruebe con el proveedor.
iSCSI de hardware independiente	Compatible. Compruebe con el proveedor.

Habilitar tramas gigantes para iSCSI de hardware dependiente y de software

Para habilitar tramas gigantes para adaptadores de iSCSI de software y de hardware dependiente en vSphere Web Client, cambie el valor predeterminado del parámetro de unidades de transmisión máximas (MTU).

Puede cambiar el parámetro MTU en el conmutador de vSphere que usa para el tráfico iSCSI. Para obtener más información, consulte la documentación de *Redes de vSphere*.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar** y en **Redes**.
- 3 Haga clic en **Conmutadores virtuales** y, desde la lista, seleccione el conmutador de vSphere que desea modificar.
- 4 Haga clic en el icono **Edit Settings** (Editar configuración).
- 5 En la página Properties (Propiedades), cambie el parámetro MTU.

Este paso establece la MTU para todas las NIC físicas en ese conmutador estándar. El valor de MTU debe configurarse con el tamaño de MTU máximo en todas las NIC conectadas al conmutador estándar. ESXi admite un tamaño de MTU de hasta 9.000 Bytes.

Habilitar tramas gigantes para iSCSI de hardware independiente

Para habilitar tramas gigantes para adaptadores de iSCSI de hardware independiente en vSphere Web Client, cambie el valor predeterminado del parámetro de unidades de transmisión máximas (MTU).

Utilice la configuración de Advanced Options (Opciones avanzadas) para cambiar el parámetro MTU en el HBA iSCSI.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Storage Adapters** (Adaptadores de almacenamiento) y seleccione el adaptador de iSCSI de hardware independiente de la lista de adaptadores.
- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Advanced Options** (Opciones avanzadas) y, a continuación, en **Edit** (Editar).
- 5 Cambie el valor del parámetro MTU.

ESXi admite un tamaño máximo de 9.000 bytes para MTU.

Configurar direcciones de detección para adaptadores de iSCSI

Se deben configurar direcciones de detección de destino, para que el adaptador de iSCSI pueda determinar qué recurso de almacenamiento de la red está disponible para el acceso.

El sistema ESXi es compatible con estos métodos de detección:

Detección dinámica

También conocida como detección SendTargets. Cada vez que el iniciador contacta con un servidor iSCSI especificado, el iniciador envía la solicitud de SendTargets al servidor. El servidor responde proporcionando una lista de destinos disponibles al iniciador. Los nombres y las direcciones IP de estos destinos aparecen en la pestaña **Static Discovery** (Detección estática). Si se quita un destino estático agregado con la detección dinámica, el destino puede ser devuelto a la lista la próxima vez que se vuelva a examinar, que se restablezca el adaptador de iSCSI o que se reinicie el host.

Nota Con iSCSI de hardware dependiente y software, ESXi filtra las direcciones de destino según la familia de IP de la dirección del servidor iSCSI especificado. Si la dirección es IPv4, se filtran las direcciones IPv6 que pueden aparecer en la respuesta SendTargets desde el servidor iSCSI y se las excluye. Cuando se utilizan nombres DNS para especificar un servidor iSCSI o cuando la respuesta SendTargets desde el servidor iSCSI tiene nombres DNS, ESXi depende de la familia de IP de la primera entrada resuelta de la búsqueda de DNS.

Detección estática

Además del método de detección dinámica, se puede utilizar una detección estática e introducir manualmente la información de los destinos. El adaptador de iSCSI utiliza una lista de destinos que se proporcionan para ponerse en contacto y comunicarse con los servidores iSCSI.

Configurar la detección dinámica o estática de iSCSI

Con la detección dinámica, cada vez que el iniciador se contacte con el sistema de almacenamiento iSCSI especificado, le enviará una solicitud de SendTargets. El sistema iSCSI le responde al iniciador y le suministra una lista de destinos disponibles. Además del método de detección dinámica, se puede utilizar una detección estática e introducir manualmente la información de los destinos.

Al configurar la detección estática o dinámica, solo se pueden agregar destinos iSCSI nuevos. No se puede cambiar ningún parámetro de un destino existente. Para hacer cambios, quite el destino existente y agregue uno nuevo.

Requisitos previos

Privilegios necesarios: **Host.Configuración.Configuración de la partición de almacenamiento**

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Storage Adapters** (Adaptadores de almacenamiento) y seleccione el adaptador de iSCSI que desea configurar en la lista.
- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Targets** (Destinos).
- 5 Configure el método de detección.

Opción	Descripción
Detección dinámica	<ol style="list-style-type: none"> a Haga clic en Dynamic Discovery (Detección dinámica) y, a continuación, en Add (Agregar). b Escriba la dirección IP o el nombre DNS del sistema de almacenamiento y haga clic en OK (Aceptar). c Vuelva a examinar el adaptador de iSCSI. <p>Después de establecer la sesión de SendTargets con el sistema iSCSI, el host completa la lista de detección estática con todos los destinos recién detectados.</p>
Detección estática	<ol style="list-style-type: none"> a Haga clic en Static Discovery (Detección estática) y, a continuación, en Add (Agregar). b Introduzca la información del destino y haga clic en OK (Aceptar). c Vuelva a examinar el adaptador de iSCSI.

Quitar destinos iSCSI dinámicos o estáticos

Quite los servidores iSCSI que aparecen en la lista de destinos.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Storage Adapters** (Adaptadores de almacenamiento) y seleccione en la lista el adaptador de iSCSI que desea modificar.
- 4 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Targets** (Destinos).
- 5 Cambie entre **Dynamic Discovery** (Detección dinámica) y **Static Discovery** (Detección estática).
- 6 Seleccione el servidor iSCSI que desea quitar y haga clic en **Remove** (Quitar).
- 7 Vuelva a examinar el adaptador de iSCSI.

Si va a quitar el destino estático que se detectó de forma dinámica, debe quitarlo del sistema de almacenamiento antes de volver a examinar. De lo contrario, el host detecta y agrega automáticamente el destino a la lista de destinos estáticos cuando se vuelva a examinar el adaptador.

Configurar parámetros CHAP para adaptadores de iSCSI

Dado que las redes IP que utiliza la tecnología iSCSI para conectarse a destinos remotos no protege los datos que transporta, se debe garantizar la seguridad de la conexión. Uno de los protocolos que iSCSI implementa es el protocolo Challenge Handshake Authentication Protocol (CHAP), que comprueba la legitimidad de los iniciadores que acceden a los destinos en la red.

CHAP utiliza un algoritmo de enlace triple para comprobar la identidad del host y, si corresponde, del destino iSCSI cuando el host y el destino establecen una conexión. La comprobación se basa en un valor privado predefinido, o un secreto CHAP, que comparten el iniciador y el destino.

ESXi admite la autenticación de CHAP en el nivel del adaptador. En este caso, todos los destinos reciben el mismo nombre y el mismo secreto CHAP por parte del iniciador iSCSI. En el caso de los adaptadores de iSCSI de hardware dependiente y de software, ESXi también admite la autenticación CHAP por destino, que permite configurar distintas credenciales para cada destino para lograr un nivel de mayor de seguridad.

Seleccionar el método de autenticación de CHAP

ESXi admite CHAP unidireccional para todos los tipos de iniciadores iSCSI, y CHAP bidireccional para iSCSI de software y hardware dependiente.

Antes de configurar CHAP, compruebe si CHAP está habilitado en el sistema de almacenamiento iSCSI y compruebe el método de autenticación de CHAP que admite el sistema. Si CHAP está habilitado, habilítelo para los iniciadores y asegúrese de que las credenciales de autenticación de CHAP coincidan con las credenciales en el almacenamiento iSCSI.

ESXi admite los siguientes métodos de autenticación de CHAP:

CHAP unidireccional

En la autenticación de CHAP unidireccional, el destino autentica el iniciador, pero el iniciador no autentica el destino.

CHAP bidireccional

En la autenticación de CHAP bidireccional, un nivel adicional de seguridad permite que el iniciador autentique el destino. VMware admite este método solo para adaptadores de iSCSI de software y de hardware dependiente.

Para adaptadores de iSCSI de software y hardware dependiente, se puede establecer CHAP unidireccional y CHAP bidireccional para cada adaptador en el nivel del destino. iSCSI de hardware independiente admite CHAP solo en el nivel del adaptador.

Cuando establezca los parámetros de CHAP, especifique un nivel de seguridad para CHAP.

Nota Cuando se especifica el nivel de seguridad de CHAP, la forma en que responde la matriz de almacenamiento depende de la implementación de CHAP de la matriz, y es específica del proveedor. Para obtener información sobre el comportamiento de la autenticación de CHAP en diferentes configuraciones de iniciador y destino, consulte la documentación de la matriz.

Tabla 10-4. Nivel de seguridad de CHAP

Nivel de seguridad de CHAP	Descripción	Compatible
None (Ninguno)	El host no utiliza autenticación de CHAP. Seleccione esta opción para deshabilitar la autenticación, en caso de que se encuentre habilitada.	iSCSI de software iSCSI de hardware dependiente iSCSI de hardware independiente
Use unidirectional CHAP if required by target (Usar CHAP unidireccional, si el destino lo requiere)	El host prefiere una conexión que no sea CHAP, pero se puede utilizar una conexión CHAP si el destino lo requiere.	iSCSI de software iSCSI de hardware dependiente
Use unidirectional CHAP unless prohibited by target (Usar CHAP unidireccional, a menos que el destino lo prohíba)	El host prefiere CHAP, pero se pueden utilizar conexiones que no sean CHAP si el destino no admite CHAP.	iSCSI de software iSCSI de hardware dependiente iSCSI de hardware independiente
Use unidirectional CHAP (Usar CHAP unidireccional)	El host requiere una autenticación de CHAP correcta. La conexión genera un error si falla la negociación de CHAP.	iSCSI de software iSCSI de hardware dependiente iSCSI de hardware independiente
Use bidirectional CHAP (Utilizar CHAP bidireccional)	Tanto el host como el destino admiten CHAP bidireccional.	iSCSI de software iSCSI de hardware dependiente

Configurar CHAP para un adaptador de iSCSI

Cuando se configura el nombre y el secreto del CHAP en el nivel del adaptador de iSCSI, todos los destinos reciben los mismos parámetros del adaptador. De forma predeterminada, todas las direcciones de detección o destinos estáticos heredan los parámetros del CHAP configurados en el nivel del adaptador.

El nombre de CHAP no debe superar los 511 caracteres alfanuméricos, mientras que el secreto CHAP no debe superar los 255 caracteres alfanuméricos. Algunos adaptadores, por ejemplo, el adaptador QLogic, pueden tener límites más bajos: 255 caracteres para el nombre de CHAP y 100 para el secreto CHAP.

Requisitos previos

- Antes de configurar los parámetros de CHAP para iSCSI de hardware dependiente o de software, determine si desea configurar CHAP unidireccional o bidireccional. Los adaptadores iSCSI de hardware independiente no admiten CHAP bidireccional.
- Compruebe los parámetros de CHAP configurados en el almacenamiento. Los parámetros configurados deben coincidir con los del almacenamiento.
- Privilegios necesarios: **Host.Configuración.Configuración de la partición de almacenamiento**

Procedimiento

- 1 Muestre los adaptadores de almacenamiento y seleccione el adaptador de iSCSI que desea configurar.
- 2 En Adapter Details (Detalles del adaptador), haga clic en la pestaña **Properties** (Propiedades) y, a continuación, haga clic en **Edit** (Editar) en el panel Authentication (Autenticación).
- 3 Especifique el método de autenticación.
 - **None (Ninguno)**
 - **Use unidirectional CHAP if required by target (Usar CHAP unidireccional, si el destino lo requiere)**
 - **Use unidirectional CHAP unless prohibited by target (Usar CHAP unidireccional, a menos que el destino lo prohíba)**
 - **Use unidirectional CHAP (Usar CHAP unidireccional)**
 - **Use bidirectional CHAP (Usar CHAP bidireccional).** Para configurar el CHAP bidireccional, debe seleccionar esta opción.
- 4 Especifique el nombre de CHAP saliente.

Asegúrese de que el nombre que especifique coincida con el nombre configurado en el lado del almacenamiento.

- Para establecer el nombre de CHAP con el nombre del adaptador de iSCSI, seleccione **Use initiator name** (Usar nombre del iniciador).

- Para establecer el nombre de CHAP con cualquier otro nombre distinto del nombre del iniciador iSCSI, desactive la casilla **Use initiator name** (Usar nombre del iniciador) y escriba un nombre en el cuadro de texto **Name** (Nombre).
- 5 Introduzca el secreto de CHAP saliente que desea utilizar como parte de la autenticación. Utilice la misma contraseña que escribió en el lado del almacenamiento.
 - 6 Si configura CHAP bidireccional, especifique credenciales de CHAP entrantes.
Asegúrese de utilizar diferentes secretos para el CHAP saliente y entrante.
 - 7 Haga clic en **OK** (Aceptar).
 - 8 Vuelva a examinar el adaptador de iSCSI.

Resultados

Si cambia los parámetros de CHAP, se utilizarán para nuevas sesiones de iSCSI. En las sesiones existentes, la nueva configuración no se utiliza a menos que cierre la sesión y vuelva a iniciarla.

Configurar CHAP para un destino

Si utiliza adaptadores de iSCSI de hardware dependiente e independiente, puede configurar diferentes credenciales CHAP para cada dirección de detección o destino estático.

El nombre de CHAP no debe superar los 511 caracteres alfanuméricos, en tanto que el secreto CHAP no debe superar los 255 caracteres alfanuméricos.

Requisitos previos

- Antes de configurar los parámetros de CHAP para iSCSI de hardware dependiente o de software, determine si desea configurar CHAP unidireccional o bidireccional.
- Compruebe los parámetros de CHAP configurados en el almacenamiento. Los parámetros configurados deben coincidir con los del almacenamiento.
- Acceda a los adaptadores de almacenamiento.
- Privilegios necesarios: **Host.Configuración.Configuración de la partición de almacenamiento**

Procedimiento

- 1 Seleccione el adaptador de iSCSI que desea configurar y haga clic en la pestaña **Targets** (Destinos), en Adapter Details (Detalles del adaptador).
- 2 Haga clic en **Dynamic Discovery** (Detección dinámica) o **Static Discovery** (Detección estática).
- 3 En la lista de destinos disponibles, seleccione el destino que desea configurar y haga clic en **Authentication** (Autenticación).
- 4 Anule la selección de **Inherit settings from parent** (Heredar configuración del primario) y especifique el método de autenticación.
 - **None (Ninguno)**

- **Use unidirectional CHAP if required by target (Usar CHAP unidireccional, si el destino lo requiere)**
 - **Use unidirectional CHAP unless prohibited by target (Usar CHAP unidireccional, a menos que el destino lo prohíba)**
 - **Use unidirectional CHAP (Usar CHAP unidireccional)**
 - **Use bidirectional CHAP (Usar CHAP bidireccional).** Para configurar el CHAP bidireccional, debe seleccionar esta opción.
- 5 Especifique el nombre de CHAP saliente.
- Asegúrese de que el nombre que especifique coincida con el nombre configurado en el lado del almacenamiento.
- Para establecer el nombre de CHAP con el nombre del adaptador de iSCSI, seleccione **Use initiator name** (Usar nombre del iniciador).
 - Para establecer el nombre de CHAP con cualquier otro nombre distinto del nombre del iniciador iSCSI, desactive la casilla **Use initiator name** (Usar nombre del iniciador) y escriba un nombre en el cuadro de texto **Name** (Nombre).
- 6 Introduzca el secreto de CHAP saliente que desea utilizar como parte de la autenticación. Utilice la misma contraseña que escribió en el lado del almacenamiento.
- 7 Si configura un CHAP bidireccional, especifique las credenciales CHAP entrantes.
- Asegúrese de utilizar diferentes secretos para el CHAP saliente y entrante.
- 8 Haga clic en **OK** (Aceptar).
- 9 Vuelva a examinar el adaptador de iSCSI.

Resultados

Si cambia los parámetros de CHAP, se utilizarán para nuevas sesiones de iSCSI. Para las sesiones actuales, no se utilizará la configuración nueva hasta que cierre la sesión y vuelva a iniciarla.

Deshabilitar CHAP

Se puede deshabilitar CHAP si el sistema de almacenamiento no lo requiere.

Si se deshabilita CHAP en un sistema que requiere la autenticación de CHAP, las sesiones de iSCSI existentes permanecen activas hasta que se reinicia el host, finaliza la sesión mediante la línea de comandos o el sistema de almacenamiento fuerza un cierre de sesión. Una vez finalizada la sesión, ya no se puede conectar a los destinos que requieren CHAP.

Privilegios necesarios: **Host.Configuración.Configuración de la partición de almacenamiento**

Procedimiento

- 1 Abra el cuadro de diálogo CHAP Credentials (Credenciales de CHAP).

- En el caso de adaptadores de iSCSI de hardware dependiente y de software, para deshabilitar solo CHAP mutuo y dejar CHAP unidireccional, seleccione **Do not use CHAP** (No utilizar CHAP) en el área de CHAP mutuo.

- Para deshabilitar CHAP unidireccional, seleccione **Do not use CHAP** (No utilizar CHAP) en el área de CHAP.

El CHAP mutuo, si está configurado, pasa automáticamente a la opción **Do not use CHAP** (No utilizar CHAP) al deshabilitar CHAP unidireccional.

- Haga clic en **OK** (Aceptar).

Configurar los parámetros avanzados de iSCSI

Es posible que deba configurar parámetros adicionales de los iniciadores iSCSI. Por ejemplo, algunos sistemas de almacenamiento iSCSI requieren una redirección a través del protocolo Address Resolution Protocol (ARP) para mover de manera dinámica el tráfico iSCSI de un puerto a otro. En este caso, debe activar la redirección de ARP en el host.

En la siguiente tabla, se enumeran los parámetros avanzados de iSCSI que se pueden configurar con vSphere Web Client. Además, se pueden utilizar los comandos de la CLI de vSphere para configurar algunos de los parámetros avanzados. Para obtener más información, consulte la documentación de *Introducción a vSphere Command-Line Interface*.

Importante No realice ningún cambio en la configuración avanzada de iSCSI, a menos que el soporte de VMware o los proveedores de almacenamiento se lo indiquen.

Tabla 10-5. Parámetros adicionales de los iniciadores iSCSI

Parámetro avanzado	Descripción	Configurable en
Header Digest (Resumen de encabezados)	Aumenta la integridad de los datos. Cuando el resumen de encabezados está habilitado, el sistema realiza una suma de comprobación en la parte del encabezado de cada unidad de datos de protocolo (PDU) de iSCSI y la comprueba con el algoritmo CRC32C.	iSCSI de software iSCSI de hardware dependiente
Data Digest (Resumen de datos)	Aumenta la integridad de los datos. Cuando el resumen de datos está habilitado, el sistema realiza una suma de comprobación en la parte de datos de cada PDU y la comprueba con el algoritmo CRC32C.	iSCSI de software iSCSI de hardware dependiente
Nota Los sistemas que utilizan procesadores Intel Nehalem descargan los cálculos del resumen de iSCSI para el software iSCSI, lo que reduce el impacto sobre el rendimiento.		
Maximum Outstanding R2T (R2T máximas pendientes)	Define las PDU listas para la transferencia (R2T) que pueden estar en transición antes de recibir una PDU de reconocimiento.	iSCSI de software iSCSI de hardware dependiente
First Burst Length (Primera duración de ráfaga)	Especifica la cantidad máxima de datos no solicitados que un iniciador iSCSI puede enviar al destino durante la ejecución de un solo comando SCSI, en bytes.	iSCSI de software iSCSI de hardware dependiente

Tabla 10-5. Parámetros adicionales de los iniciadores iSCSI (continuación)

Parámetro avanzado	Descripción	Configurable en
Maximum Burst Length (Máxima duración de ráfaga)	Carga útil de datos de SCSI máxima en una secuencia de iSCSI de entrada de datos o de salida de datos solicitada, en bytes.	iSCSI de software iSCSI de hardware dependiente
Maximum Receive Data Segment Length (Longitud máxima del segmento de datos recibida)	Longitud máxima del segmento de datos, en bytes, que puede recibirse en una PDU de iSCSI.	iSCSI de software iSCSI de hardware dependiente
Session Recovery Timeout (Tiempo de espera de recuperación de la sesión)	Especifica la cantidad de tiempo, en segundos, que puede transcurrir mientras se recupera una sesión. Si el tiempo de espera supera el límite, el iniciador iSCSI finaliza la sesión.	iSCSI de software iSCSI de hardware dependiente
No-Op Interval (Intervalo de No-Op)	Especifica el intervalo, en segundos, entre las solicitudes de NOP-Out enviadas del iniciador iSCSI a un destino iSCSI. Las solicitudes NOP-Out actúan como el mecanismo de ping para comprobar que existe una conexión activa entre el iniciador iSCSI y el destino iSCSI.	iSCSI de software iSCSI de hardware dependiente
No-Op Timeout (Tiempo de espera de No-Op)	Especifica la cantidad de tiempo, en segundos, que puede transcurrir antes de que el host reciba un mensaje de NOP-In. El destino iSCSI envía el mensaje en respuesta a la solicitud de NOP-Out. Cuando se supera el límite del tiempo de espera de no-op, el iniciador finaliza la sesión actual y comienza una nueva.	iSCSI de software iSCSI de hardware dependiente
ARP Redirect (Redirección de ARP)	Permite que los sistemas de almacenamiento muevan de manera dinámica el tráfico iSCSI de un puerto a otro. Los sistemas de almacenamiento requieren que ARP lleve a cabo una conmutación por error basada en matrices.	iSCSI de software iSCSI de hardware dependiente iSCSI de hardware independiente
Delayed ACK (ACK demorado)	Permite que los sistemas demoren el reconocimiento de los paquetes de datos recibidos.	iSCSI de software iSCSI de hardware dependiente

Configurar los parámetros avanzados de iSCSI

La configuración avanzada de iSCSI controla los parámetros, como el encabezado y el resumen de datos, la redirección de ARP, ACK demorado, etc.

Precaución No haga cambios en la configuración de iSCSI avanzada a menos que esté trabajando con el equipo de soporte de VMware o que tenga información detallada sobre los valores que debe asignar a la configuración.

Requisitos previos

Privilegios necesarios: **Host.Configuración.Configuración de la partición de almacenamiento**

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Almacenamiento**, haga clic en **Adaptadores de almacenamiento** y seleccione el adaptador (vmhba#) que desea configurar.
- 4 Configure los parámetros avanzados.
 - Para configurar los parámetros avanzados en el nivel del adaptador, en Adapter Details (Detalles del adaptador), haga clic en la pestaña **Advanced Options** (Opciones avanzadas) y, a continuación, haga clic en **Edit** (Editar).
 - Configure los parámetros avanzados en el nivel del destino.
 - a Haga clic en la pestaña **Targets** (Destinos) y, a continuación, haga clic en **Dynamic Discovery** (Detección dinámica) o en **Static Discovery** (Detección estática).
 - b En la lista de destinos disponibles, seleccione el destino que desea configurar y haga clic en **Advanced Options** (Opciones avanzadas).
- 5 Introduzca todos los valores requeridos de los parámetros avanzados que desea modificar.

Administrar sesiones de iSCSI

Para comunicarse entre sí, los iniciadores iSCSI y los destinos establecen sesiones iSCSI. Puede revisar y administrar las sesiones iSCSI con vSphere CLI.

De forma predeterminada, los iniciadores iSCSI de hardware dependiente e iSCSI de software inician una sesión iSCSI entre cada puerto del iniciador y cada puerto de destino. Si el iniciador iSCSI o el destino tienen más de un puerto, se pueden establecer varias sesiones en el host. La cantidad predeterminada de sesiones para cada destino equivale a la cantidad de puertos en el adaptador de iSCSI multiplicada por la cantidad de puertos de destino.

Con vSphere CLI, puede mostrar todas las sesiones actuales para analizarlas y depurarlas. Para crear más rutas de acceso a los sistemas de almacenamiento, puede aumentar la cantidad predeterminada de sesiones duplicando las sesiones existentes entre el adaptador de iSCSI y los puertos de destino.

También puede establecer una sesión con un puerto de destino específico. Esto puede resultar útil si el host se conecta a un sistema de almacenamiento de un puerto que, de manera predeterminada, presenta solo un puerto de destino al iniciador, pero puede redireccionar sesiones adicionales a distintos puertos de destino. Establecer una sesión nueva entre el iniciador iSCSI y otro puerto de destino crea una ruta de acceso adicional al sistema de almacenamiento.

Las consideraciones siguientes aplican a la administración de sesión de iSCSI:

- Algunos sistemas de almacenamiento no admiten varias sesiones del mismo extremo o nombre de iniciador. Los intentos de crear varias sesiones en tales destinos puede resultar en un comportamiento impredecible de su entorno iSCSI.

- Los proveedores de almacenamiento pueden proporcionar administradores de sesión automáticos. Utilizar los administradores de sesión automáticos para agregar o eliminar sesiones no garantiza resultados duraderos y puede interferir con el rendimiento del almacenamiento.

Revisar las sesiones iSCSI

Utilice el comando vCLI para mostrar sesiones iSCSI entre un adaptador de iSCSI y un sistema de almacenamiento.

En el procedimiento, **--server=server_name** especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Para enumerar las sesiones iSCSI, ejecute el siguiente comando:

```
esxcli --server=server_name iscsi session list
```

Este comando toma estas opciones:

Opción	Descripción
-A --adapter= <i>str</i>	El nombre del adaptador de iSCSI, por ejemplo, vmhba34.
-s --isid= <i>str</i>	El identificador de la sesión iSCSI.
-n --name= <i>str</i>	El nombre del destino iSCSI, por ejemplo, iqn.X.

Agregar sesiones iSCSI

Utilice vCLI para agregar una sesión iSCSI a un destino que especifique o para duplicar una sesión existente. Al duplicar las sesiones, aumenta la cantidad de sesiones predeterminada y se crean rutas de acceso adicionales a los sistemas de almacenamiento.

En el procedimiento, **--server=server_name** especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Para agregar o duplicar una sesión iSCSI, ejecute el comando siguiente:

```
esxcli --server=nombre_del_servidor iscsi session add
```

Este comando toma estas opciones:

Opción	Descripción
-A --adapter= <i>str</i>	El nombre del adaptador de iSCSI, por ejemplo, vmhba34. Esta opción es obligatoria.
-s --isid= <i>str</i>	El ISID de la sesión que se desea duplicar. Para encontrarlo, enumere todas las sesiones.
-n --name= <i>str</i>	El nombre del destino iSCSI, por ejemplo, iqn.X.

Pasos siguientes

Vuelva a examinar el adaptador de iSCSI.

Quitar sesiones iSCSI

Utilice el comando vCLI para quitar una sesión iSCSI entre un adaptador de iSCSI y un destino.

En el procedimiento, **--server=server_name** especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Para quitar una sesión, ejecute el siguiente comando:

```
esxcli --server=server_name iscsi session remove
```

Este comando toma estas opciones:

Opción	Descripción
-A --adapter= <i>str</i>	El nombre del adaptador de iSCSI, por ejemplo, vmhba34. Esta opción es obligatoria.
-s --isid= <i>str</i>	El ISID de la sesión que se desea quitar. Para encontrarlo, enumere todas las sesiones.
-n --name= <i>str</i>	El nombre del destino iSCSI, por ejemplo, iqn.X.

Pasos siguientes

Vuelva a examinar el adaptador de iSCSI.

Arrancar desde SAN iSCSI

11

Cuando se configura el host para arrancar desde una SAN, la imagen de arranque del host se almacena en uno o más LUN en el sistema de almacenamiento SAN. Cuando el host arranca, lo hace desde el LUN en la SAN, no desde su disco local.

Puede utilizar el arranque desde SAN si no desea ocuparse del mantenimiento del almacenamiento local o si tiene configuraciones de hardware sin discos, por ejemplo, sistemas blade.

ESXi admite distintos métodos de arranque desde la SAN iSCSI.

Tabla 11-1. Compatibilidad con arranque desde SAN iSCSI

iSCSI de hardware independiente	iSCSI de software e iSCSI de hardware dependiente
Configure el HBA de iSCSI para que arranque desde la SAN. Para obtener información sobre la configuración del HBA, consulte Configurar adaptador de iSCSI de hardware independiente para el arranque de SAN	Utilice el adaptador de red compatible con iBFT. Para obtener información, consulte Descripción general del arranque de iBFT de iSCSI .

Este capítulo incluye los siguientes temas:

- [Recomendaciones generales de arranque desde SAN iSCSI](#)
- [Preparar SAN iSCSI](#)
- [Configurar adaptador de iSCSI de hardware independiente para el arranque de SAN](#)
- [Descripción general del arranque de iBFT de iSCSI](#)

Recomendaciones generales de arranque desde SAN iSCSI

Si planea configurar y utilizar un LUN iSCSI como dispositivo de arranque del host, debe seguir ciertas instrucciones generales.

Las siguientes instrucciones se aplican al arranque desde iSCSI e iBFT de hardware independiente.

- Repase todas las recomendaciones del distribuidor de hardware que se utiliza en la configuración de arranque.

- Para conocer los requisitos previos y los requisitos de instalación, consulte *Instalación y configuración de vSphere*.
- Utilice direcciones IP estáticas para reducir las posibilidades de conflictos con DHCP.
- Utilice LUN diferentes para particiones de arranque y almacenes de datos de VMFS.
- Configure ACL adecuadas en el sistema de almacenamiento.
 - El LUN de arranque debe ser visible solo para el host que usa el LUN. No debe permitirse que ningún otro host de la SAN vea ese LUN de arranque.
 - Si se usa un LUN para un almacén de datos de VMFS, varios hosts pueden compartirlo. Es posible hacer esto mediante las ACL de los sistemas de almacenamiento.
- Configure una partición de diagnóstico.
 - Solo con iSCSI de hardware independiente es posible colocar la partición de diagnóstico en el LUN de arranque. Si configura la partición de diagnóstico en el LUN de arranque, este LUN no podrá compartirse entre varios hosts. Si se utiliza un LUN distinto para la partición de diagnóstico, varios hosts pueden compartirlo.
 - Si el arranque se realiza desde una SAN con iBFT, no se puede configurar una partición de diagnóstico en un LUN de SAN. Para recopilar la información de diagnóstico del host, utilice vSphere ESXi Dump Collector en un servidor remoto. Para obtener información sobre ESXi Dump Collector, consulte *Instalación y configuración de vSphere y Redes de vSphere*.

Preparar SAN iSCSI

Antes de configurar el host para arrancar desde un LUN iSCSI, prepare y configure la red de área de almacenamiento.

Precaución Si utiliza una instalación generada por script para instalar ESXi cuando arranca desde una SAN, debe realizar pasos especiales para evitar la pérdida de datos no intencionada.

Procedimiento

- 1 Conecte los cables de red, consulte cualquier guía de cableado que se aplique a la instalación.
- 2 Compruebe que haya conectividad IP entre el sistema de almacenamiento y el servidor.

Esto incluye una configuración adecuada de cualquier enrutador o conmutador en la red de almacenamiento. Los sistemas de almacenamiento deben poder hacer ping a los adaptadores de iSCSI en los hosts.

3 Configure el sistema de almacenamiento.

- a Cree un volumen (o LUN) en el sistema de almacenamiento desde el cual pueda arrancar el host.
- b Configure el sistema de almacenamiento para que el host tenga acceso al LUN asignado.
Esto podría involucrar la actualización de ACL con las direcciones IP, los nombres iSCSI y el parámetro de autenticación de CHAP que se utiliza en el host. En algunos sistemas de almacenamiento, además de proporcionar información de acceso para el host ESXi, también se debe asociar de manera explícita el LUN asignado con el host.
- c Asegúrese de que el LUN se presente correctamente al host.
- d Compruebe que ningún otro sistema tenga acceso al LUN configurado.
- e Registre el nombre iSCSI y las direcciones IP de los destinos asignados al host.
Debe tener esta información para configurar los adaptadores de iSCSI.

Configurar adaptador de iSCSI de hardware independiente para el arranque de SAN

Si el host ESXi utiliza un adaptador de iSCSI de hardware independiente, como un HBA de QLogic, debe configurar el adaptador para que arranque desde SAN.

Este procedimiento analiza cómo habilitar el HBA de iSCSI de QLogic para arrancar desde SAN. Para obtener más información y detalles más actualizados sobre las opciones de configuración del adaptador QLogic, consulte el sitio web de QLogic.

Requisitos previos

Debido a que primero debe arrancar desde los medios de instalación de VMware, configure el host para que arranque desde el CD/DVD-ROM. Para lograrlo, cambie la secuencia de arranque del sistema en la configuración del BIOS del sistema.

Procedimiento

- 1 Inserte el CD/DVD de instalación en la unidad de CD/DVD-ROM y reinicie el host.
- 2 Utilice el BIOS para establecer el host para que arranque primero desde la unidad de CD/DVD-ROM.
- 3 Durante el POST del servidor, presione Ctrl+q para acceder al menú de configuración del HBA de iSCSI de QLogic.
- 4 Seleccione el puerto de E/S que desea configurar.

De forma predeterminada, el modo de arranque del adaptador está deshabilitado.

- 5 Configure el HBA.
 - a En el menú **Fast!UTIL Options (Opciones de Fast!UTIL)**, seleccione **Configuration Settings (Opciones de configuración) > Host Adapter Settings (Configuración del adaptador de host)**.
 - b Configure las opciones siguientes del adaptador del host: dirección IP del iniciador, máscara de subred, puerta de enlace, nombre iSCSI del iniciador y CHAP (si se requiere).
- 6 Configure las opciones de iSCSI.
Consulte [Configurar las opciones de arranque de iSCSI](#).
- 7 Guarde los cambios y reinicie el sistema.

Configurar las opciones de arranque de iSCSI

Cuando se configura el host ESXi para arrancar desde iSCSI, se deben configurar las opciones de arranque de iSCSI.

Procedimiento

- 1 En el menú **Fast!UTIL Options** (Opciones de Fast!UTIL), seleccione **Configuration Settings (Opciones de configuración) > iSCSI Boot Settings (Opciones de arranque de iSCSI)**.
- 2 Para poder establecer SendTargets, configure el modo Adapter Boot (Arranque del adaptador) en **Manual**.
- 3 Seleccione **Primary Boot Device Settings** (Configuración del dispositivo de arranque principal).
 - a Escriba los valores de **Target IP** (IP de destino) y **Target Port** (Puerto de destino) de detección.
 - b Puede dejar en blanco los campos **Boot LUN** (LUN de arranque) y **iSCSI Name** (Nombre iSCSI) si solo un destino iSCSI y un LUN se encuentran en la dirección especificada desde la que se realizará el arranque. De lo contrario, debe especificar estos campos para asegurarse de no arrancar desde un volumen de algún otro sistema. Una vez alcanzado el sistema de almacenamiento de destino, estos campos se completan después de volver a examinar.
 - c Guarde los cambios.
- 4 En el menú **iSCSI Boot Settings** (Opciones de arranque de iSCSI), seleccione el dispositivo de arranque principal. Se vuelve a examinar automáticamente el HBA para encontrar LUN de destino nuevos.
- 5 Seleccione el destino iSCSI.

Nota Si hay más de un LUN en el destino, puede elegir un identificador de LUN específico. Para ello, presione **Entrar** después de ubicar el dispositivo iSCSI.

- 6 Regrese al menú **Primary Boot Device Setting** (Configuración del dispositivo de arranque principal). Después de volver a examinar, los campos **Boot LUN** (LUN de arranque) y **iSCSI Name** (Nombre iSCSI) se completan. Cambie el valor de **Boot LUN** (LUN de arranque) al identificador del LUN deseado.

Descripción general del arranque de iBFT de iSCSI

Los hosts ESXi pueden arrancar desde una SAN iSCSI mediante los adaptadores de iSCSI de hardware dependiente o de software y los adaptadores de red.

Para implementar ESXi y hacer un arranque desde la SAN iSCSI, el host debe tener un adaptador de red para arranque de iSCSI que admita el formato de tabla de firmware de arranque de iSCSI (iBFT). La iBFT es un método de comunicación de parámetros del dispositivo de arranque de iSCSI con un sistema operativo.

Antes de instalar ESXi y hacer un arranque desde SAN iSCSI, configure los parámetros de redes y arranque de iSCSI en el adaptador de red, y habilite el adaptador para el arranque de iSCSI. Debido a que la configuración del adaptador de red depende del proveedor, es necesario consultar la documentación del proveedor para obtener instrucciones.

La primera vez que se ejecuta un arranque desde iSCSI, el firmware de arranque de iSCSI del sistema se conecta a un destino iSCSI. Si el inicio de sesión se realiza correctamente, el firmware guarda los parámetros de redes y de arranque de iSCSI en la iBFT, y almacena la tabla en la memoria del sistema. El sistema usa esta tabla para configurar las redes y su propia conexión de iSCSI, y para ejecutar el arranque.

En la siguiente lista se describe la secuencia de arranque de iBFT de iSCSI.

- 1 Al reiniciarse, el BIOS del sistema detecta el firmware de arranque de iSCSI en el adaptador de red.
- 2 El firmware de arranque de iSCSI usa los parámetros de arranque preconfigurados para conectarse con el destino iSCSI especificado.
- 3 Si la conexión con el destino iSCSI se realiza correctamente, el firmware de arranque de iSCSI escribe los parámetros de redes y de arranque de iSCSI en la iBFT, y almacena la tabla en la memoria del sistema.

Nota El sistema usa esta tabla para configurar las redes y su propia conexión de iSCSI, y para ejecutar el arranque.

- 4 El BIOS arranca el dispositivo de arranque.
- 5 El VMkernel se empieza a cargar y controla la operación de arranque.
- 6 A continuación, el VMkernel usa los parámetros de arranque de la iBFT para conectarse al destino iSCSI.
- 7 Una vez establecida la conexión de iSCSI, el sistema arranca.

Consideraciones sobre el arranque de iBFT de iSCSI

Cuando se arranca el host ESXi desde iSCSI mediante adaptadores de red habilitados para iBFT, se deben tener en cuenta ciertas consideraciones.

- Actualice el código de arranque de NIC y el firmware de iBFT mediante las herramientas suministradas por el proveedor antes de intentar instalar y arrancar VMware ESXi. Consulte la documentación del proveedor y el HCL de VMware para conocer el código de arranque y las versiones del firmware de iBFT compatibles para el arranque de iBFT de VMware ESXi.
- El arranque de iBFT de iSCSI no admite la conmutación por error para adaptadores de red habilitados para iBFT.
- Después de configurar el host para que arranque desde la iBFT de iSCSI, se aplican las siguientes restricciones:
 - No puede deshabilitar el adaptador de iSCSI del software. Si la configuración de iBFT está presente en el BIOS, el host vuelve a habilitar el adaptador de iSCSI del software durante cada reinicio.

Nota Si no usa el adaptador de red habilitado para iBFT para el arranque de iSCSI y no desea que el adaptador de iSCSI del software esté siempre habilitado, elimine la configuración de iBFT del adaptador de red.

- No puede eliminar el destino de arranque de iBFT de iSCSI mediante vSphere Web Client. El destino aparece en la lista de destinos estáticos de adaptadores.

Configurar arranque de iBFT desde SAN

Puede arrancar desde la SAN iSCSI con el adaptador de iSCSI de software, o bien con un adaptador de iSCSI de hardware dependiente y un adaptador de red. El adaptador de red debe ser compatible con iBFT.

Cuando se configura el host para arrancar con iBFT, se deben realizar varias tareas.

Procedimiento

1 Configurar los parámetros de arranque de iSCSI

Para comenzar un proceso de arranque de iSCSI, un adaptador de red en el host debe tener un firmware de arranque de iSCSI especialmente configurado. Al configurar el firmware, debe especificar los parámetros de iSCSI y de redes, además de habilitar el adaptador para el arranque de iSCSI.

2 Cambiar secuencia de arranque en el BIOS

Cuando configure el host para arrancar desde iBFT iSCSI, cambie la secuencia de arranque para forzar al host a arrancar en el orden adecuado.

3 Instalación de ESXi en un destino iSCSI

Cuando configure el host para que arranque desde la iBFT de iSCSI, instale la imagen de ESXi en el LUN de destino.

4 Arrancar ESXi desde un destino iSCSI

Después de preparar el host para un arranque de iSCSI de iBFT y copiar la imagen de ESXi al destino iSCSI, se debe efectuar el arranque propiamente dicho.

Configurar los parámetros de arranque de iSCSI

Para comenzar un proceso de arranque de iSCSI, un adaptador de red en el host debe tener un firmware de arranque de iSCSI especialmente configurado. Al configurar el firmware, debe especificar los parámetros de iSCSI y de redes, además de habilitar el adaptador para el arranque de iSCSI.

La configuración en el adaptador de red puede ser dinámica o estática. Si utiliza la configuración dinámica, indica que todos los parámetros de arranque del destino y del iniciador se adquirieron mediante DHCP. Para la configuración estática, debe escribir manualmente datos, entre ellos la dirección IP del host y el IQN del iniciador, además de los parámetros de destino.

Procedimiento

- ◆ En el adaptador de red que utiliza para el arranque desde iSCSI, especifique los parámetros de iSCSI y de redes.

Debido a que la configuración del adaptador de red depende del proveedor, es necesario consultar la documentación del proveedor para obtener instrucciones.

Cambiar secuencia de arranque en el BIOS

Cuando configure el host para arrancar desde iBFT iSCSI, cambie la secuencia de arranque para forzar al host a arrancar en el orden adecuado.

Cambie la secuencia de arranque del BIOS a la siguiente:

- iSCSI
- DVD-ROM

Debido a que el procedimiento de cambio de la secuencia de arranque en el BIOS es específico de cada proveedor, consulte la documentación del proveedor para obtener instrucciones. El procedimiento de muestra siguiente explica cómo cambiar la secuencia de arranque en un host Dell con un adaptador de red Broadcom.

Procedimiento

- 1 Encienda el host.
- 2 Durante la prueba automática de encendido (POST), presione F2 para entrar a la configuración del BIOS.
- 3 En Configuración del BIOS, seleccione **Boot Sequence** (Secuencia de arranque) y presione Entrar.
- 4 En el menú Boot Sequence (Secuencia de arranque) acomode los elementos de arranque de forma que iSCSI preceda al DVD-ROM.

- 5 Presione Esc para salir del menú Boot Sequence (Secuencia de arranque).
- 6 Presione Esc para salir de la configuración del BIOS.
- 7 Seleccione **Save Changes** (Guardar cambios) y haga clic en **Exit** (Salir) para salir del menú de configuración del BIOS.

Instalación de ESXi en un destino iSCSI

Cuando configure el host para que arranque desde la iBFT de iSCSI, instale la imagen de ESXi en el LUN de destino.

Requisitos previos

- Configure el firmware de arranque de iSCSI en la NIC de arranque para que apunte al LUN de destino que desea usar como LUN de arranque.
- Cambie la secuencia de arranque en el BIOS de modo que iSCSI preceda al DVD-ROM.
- Si usa adaptadores Broadcom, establezca **Boot to iSCSI target** (Arrancar en destino iSCSI) en **Disabled** (Deshabilitado).

Procedimiento

- 1 Inserte los medios de instalación en la unidad de CD/DVD-ROM y reinicie el host.
- 2 Cuando se inicie el instalador, siga el procedimiento típico de instalación.
- 3 Cuando el sistema se lo indique, seleccione el LUN iSCSI como el destino de instalación.
El instalador copia la imagen de arranque de ESXi en el LUN iSCSI.
- 4 Una vez que se reinicia el sistema, extraiga el DVD de instalación.

Arrancar ESXi desde un destino iSCSI

Después de preparar el host para un arranque de iSCSI de iBFT y copiar la imagen de ESXi al destino iSCSI, se debe efectuar el arranque propiamente dicho.

Requisitos previos

- Configure el firmware de arranque de iSCSI en la NIC de arranque para que apunte al LUN de arranque.
- Cambie la secuencia de arranque en el BIOS de modo que iSCSI preceda al dispositivo de arranque.
- Si utiliza adaptadores Broadcom, establezca **Boot to iSCSI target** (Arrancar en destino iSCSI) como **Enabled** (Habilitado).

Procedimiento

1 Reinicie el host.

El host arranca desde el LUN iSCSI con los datos de iBFT. Durante el primer arranque, el script de inicialización iSCSI configura las redes predeterminadas. La configuración de red es persistente durante los reinicios siguientes.

2 (opcional) Para ajustar la configuración de redes, utilice vSphere Web Client.

Prácticas recomendadas para redes

Para arrancar el host ESXi desde iSCSI con iBFT, debe configurar adecuadamente las redes.

Para una mayor seguridad y un mejor rendimiento, es conveniente contar con adaptadores de red redundantes en el host.

Para saber de qué forma se deben configurar los adaptadores de red, determine si el entorno utiliza redes compartidas o aisladas para el tráfico iSCSI y el tráfico de administración de hosts.

Redes de administración y de iSCSI compartidas

Configure los parámetros de iSCSI y de redes en el primer adaptador de red en el host. Después de que arranque el host, puede agregar adaptadores de red secundarios al grupo de puertos predeterminado.

Redes de administración y de iSCSI aisladas

Al configurar redes de administración y de iSCSI aisladas, siga estas instrucciones para evitar problemas con el ancho de banda.

- Las redes aisladas deben estar en subredes diferentes.
- Si utiliza VLAN para aislar las redes, deben tener subredes diferentes para garantizar que las tablas de enrutamiento estén configuradas adecuadamente.
- VMware recomienda configurar el adaptador y el destino iSCSI para que estén en la misma subred. Si configura el adaptador y el destino iSCSI en subredes diferentes, se aplican las siguientes restricciones:
 - La puerta de enlace VMkernel predeterminada debe tener la capacidad de enrutar el tráfico de administración y el tráfico iSCSI.
 - Después de arrancar el host, podrá utilizar el adaptador de red compatible con iBFT solo para iBFT. No podrá utilizar el adaptador para otro tipo de tráfico iSCSI.
- Utilice el primer adaptador de red física para la red de administración.
- Utilice el segundo adaptador de red física para la red iSCSI. Asegúrese de configurar iBFT.
- Después de que arranque el host, puede agregar adaptadores de red secundarios a las redes de iSCSI y de administración.

Cambiar la configuración de arranque de iSCSI iBFT

Actualice iBFT en caso de que cambie la configuración de opciones como el nombre de IQN, la dirección IP, etc., en el almacenamiento iSCSI o en el host. Esta tarea asume que el LUN de arranque y los datos almacenados en el LUN permanecen intactos.

Procedimiento

- 1 Apague el host ESXi.
- 2 Cambie la configuración de almacenamiento iSCSI.
- 3 Actualice iBFT en el host con la nueva configuración.
- 4 Reinicie el host.

El host arrancará con la nueva información almacenada en iBFT.

Solucionar problemas de arranque de iSCSI de iBFT

Los temas en esta sección ayudan a identificar y a solucionar problemas que pueden surgir al utilizar el arranque de iSCSI de iBFT.

La pérdida de la puerta de enlace del sistema provoca la pérdida de la conectividad de red

La conectividad de red se pierde cuando se elimina un grupo de puertos asociado con el adaptador de red de iBFT.

Problema

La pérdida de la conectividad de red ocurre una vez que se elimina un grupo de puertos.

Causa

Cuando se especifica una puerta de enlace en el adaptador de red habilitado para iBFT durante la instalación de ESXi, esta puerta de enlace se convierte en la puerta de enlace predeterminada del sistema. Si se elimina el grupo de puertos asociado con el adaptador de red, se pierde la puerta de enlace predeterminada del sistema. Esta acción provoca la pérdida de la conectividad de red.

Solución

No establezca una puerta de enlace de iBFT a menos que sea necesario. Si se requiere una puerta de enlace, después de la instalación, establezca manualmente la puerta de enlace que utiliza la red de administración como la predeterminada del sistema.

El cambio de los parámetros de arranque de iSCSI provoca que ESXi arranque en modo sin estado

El cambio de los parámetros de arranque de iSCSI en el adaptador de red después del arranque inicial no actualiza la configuración de redes ni iSCSI en el host ESXi.

Problema

Si cambia los parámetros de arranque de iSCSI en el adaptador de red después del arranque inicial de ESXi desde iSCSI, el host arrancará en modo sin estado.

Causa

El firmware utiliza la configuración de arranque actualizada y puede conectarse con el destino iSCSI para cargar la imagen de ESXi. Sin embargo, cuando está cargado, el sistema no incorpora los nuevos parámetros, sino que continúa utilizando los parámetros persistentes de redes y de iSCSI del arranque anterior. En consecuencia, el host no puede conectarse con el destino y arranca en modo sin estado.

Solución

- 1 Utilice vSphere Web Client para conectarse con el host ESXi.
- 2 Vuelva a configurar el iSCSI y las redes en el host para que coincidan con los parámetros de iBFT.
- 3 Vuelva a examinar.

Prácticas recomendadas de almacenamiento iSCSI

12

Al utilizar ESXi con SAN iSCSI, siga las prácticas recomendadas que ofrece VMware para evitar problemas.

Consulte a su representante de almacenamiento si su sistema de almacenamiento admite las características de aceleración de hardware de Storage API - Array Integration. Si las admite, consulte la documentación del proveedor para obtener información sobre cómo habilitar la compatibilidad con la aceleración de hardware en el sistema de almacenamiento. Para obtener más información, consulte [Capítulo 23 Aceleración de hardware de almacenamiento](#).

Este capítulo incluye los siguientes temas:

- [Evitar problemas en una SAN iSCSI](#)
- [Optimización del rendimiento del almacenamiento SAN iSCSI](#)
- [Comprobar estadísticas del conmutador Ethernet](#)

Evitar problemas en una SAN iSCSI

Al utilizar ESXi en conjunto con una SAN, se deben seguir instrucciones específicas para evitar problemas en la SAN.

Es necesario seguir estas recomendaciones para evitar problemas con la configuración de SAN:

- Coloque un solo almacén de datos de VMFS en cada LUN. No se recomiendan múltiples almacenes de datos de VMFS en un LUN.
- No cambie la directiva de rutas de acceso que el sistema establece a menos que comprenda las consecuencias de realizar esa modificación.
- Documente todo. Incluya información sobre configuración, control de acceso, almacenamiento, conmutador, configuración de servidor y HBA iSCSI, versiones de software y firmware, y planificación del cableado de almacenamiento.
- Planificación en caso de errores:
 - Haga varias copias de los mapas de topología. Para cada elemento, tenga en cuenta lo que sucede con la SAN si el elemento presenta errores.
 - Verifique diferentes vínculos, conmutadores, HBA y otros elementos para asegurarse de no haber omitido ningún punto de error crítico en el diseño.

- Compruebe que los HBA iSCSI estén instalados en las ranuras correctas en el host ESXi, según la velocidad de bus y ranura. Equilibre la carga del bus PCI entre los buses disponibles del servidor.
- Familiarícese con los distintos puntos de supervisión en la red de almacenamiento, en todos los puntos de visibilidad, incluidos los gráficos de rendimiento de ESXi, las estadísticas del conmutador Ethernet y las estadísticas de rendimiento del almacenamiento.
- Tenga cuidado cuando cambie los identificadores de los LUN que tienen almacenes de datos de VMFS utilizados por el host. Si cambia el identificador, las máquinas virtuales que se ejecutan en el almacén de datos de VMFS fallan.

Si no hay máquinas virtuales en ejecución en el almacén de datos de VMFS, después de cambiar el identificador del LUN, debe volver a examinar para restablecer el identificador en el host. Para obtener información sobre cómo volver a examinar, consulte [Operaciones para actualizar y volver a examinar el almacenamiento](#).

- Si necesita cambiar el nombre iSCSI predeterminado del adaptador de iSCSI, asegúrese de que el nombre que introduce sea universalmente único y tenga el formato correcto. Para evitar problemas de acceso al almacenamiento, jamás asigne el mismo nombre iSCSI a los diferentes adaptadores, ni siquiera en hosts diferentes.

Optimización del rendimiento del almacenamiento SAN iSCSI

Hay varios factores que contribuyen a la optimización del entorno típico de SAN.

Si el entorno de red está bien configurado, los componentes de iSCSI proporcionan una capacidad de proceso adecuada y una latencia suficientemente baja para iniciadores y destinos iSCSI.

Si la red está congestionada y los vínculos, conmutadores y enrutadores están saturados, el rendimiento de iSCSI se verá afectado y es posible que no sea el adecuado para los entornos de ESXi.

Rendimiento del sistema de almacenamiento

El rendimiento del sistema de almacenamiento es uno de los principales factores que contribuye al rendimiento de todo el entorno de iSCSI.

Si se producen problemas con el rendimiento del sistema de almacenamiento, consulte la documentación del proveedor del sistema de almacenamiento para acceder a toda la información relevante.

Al asignar LUN, recuerde que puede acceder a todos los LUN compartidos a través de una serie de hosts, y que pueden ejecutarse varias máquinas virtuales en cada host. Un LUN utilizado por el host ESXi puede atender operaciones de E/S desde varias aplicaciones diferentes que se ejecuten en distintos sistemas operativos. Debido a esta carga de trabajo diversa, el grupo RAID que contiene los LUN de ESXi no debe incluir LUN que utilicen otros hosts y que no ejecuten ESXi para aplicaciones de uso intensivo de E/S.

Habilite el almacenamiento en caché de lectura y de escritura.

El equilibrio de carga es el proceso de distribuir solicitudes de E/S de servidores en todos los SP disponibles y las rutas de acceso a servidores de hosts asociadas. El objetivo es optimizar el rendimiento en términos de capacidad de proceso (E/S por segundo, megabytes por segundo o tiempos de respuesta).

Los sistemas de almacenamiento SAN requieren un rediseño y ajuste continuos para garantizar que las operaciones de E/S sean equilibradas en todas las rutas de acceso del sistema de almacenamiento. Para cumplir con este requisito, distribuya las rutas de acceso a los LUN entre todos los SP. De esa manera, se podrá proporcionar un equilibrio de carga óptimo. Una supervisión exhaustiva indica en qué momento es necesario volver a equilibrar manualmente la distribución de LUN.

Para ajustar sistemas de almacenamiento equilibrados estadísticamente se deben supervisar estadísticas de rendimiento específicas (como operaciones de E/S por segundo, bloques por segundo y tiempos de respuesta), y es necesario distribuir la carga de trabajo de LUN para propagar la carga de trabajo en todos los SP.

Rendimiento del servidor con iSCSI

Se deben tener en cuenta varios factores para garantizar un rendimiento óptimo del servidor.

Cada aplicación del servidor debe tener acceso a su almacenamiento designado con las condiciones siguientes:

- Velocidad de E/S alta (cantidad de operaciones de E/S por segundo)
- Alta capacidad de proceso (megabytes por segundo)
- Latencia mínima (tiempos de respuesta)

Dado que cada aplicación tiene distintos requisitos, puede cumplir estos objetivos eligiendo un grupo RAID adecuado en el sistema de almacenamiento. Para alcanzar los objetivos de rendimiento, realice las tareas siguientes:

- Coloque cada LUN en un grupo RAID que proporcione los niveles de rendimiento necesarios. Preste atención a las actividades y la utilización de recursos de otros LUN en el grupo RAID asignado. Es posible que un grupo RAID de alto rendimiento que tiene demasiadas aplicaciones que realizan operaciones de E/S en él no cumpla con los objetivos de rendimiento requeridos por una aplicación que se ejecuta en el host ESXi.
- Proporcione a cada servidor un número suficiente de adaptadores de red o adaptadores de hardware de iSCSI para permitir la máxima capacidad de proceso de todas las aplicaciones alojadas en el servidor durante el período pico. La propagación de E/S en varios puertos proporciona una mayor capacidad de proceso y una menor latencia para cada aplicación.
- Para proporcionar redundancia para iSCSI de software, asegúrese de que el iniciador esté conectado a todos los adaptadores de red usados para la conectividad de iSCSI.

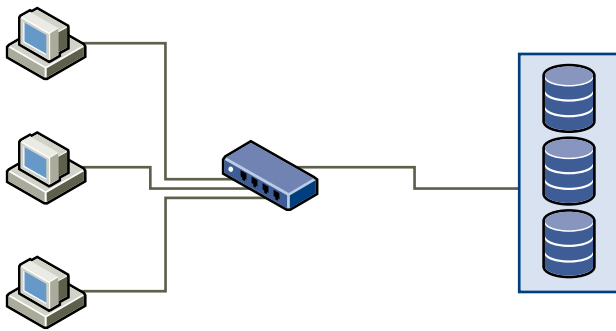
- Cuando se asignan LUN o grupos RAID a sistemas ESXi, varios sistemas operativos utilizan y comparten ese recurso. Como resultado, el rendimiento requerido de cada LUN en el subsistema de almacenamiento puede ser mucho mayor si se trabaja con sistemas ESXi que si se utilizan máquinas físicas. Por ejemplo, si espera ejecutar cuatro aplicaciones de uso intensivo de E/S, asigne el cuádruple de capacidad de rendimiento al LUN de ESXi.
- Cuando se utilizan varios sistemas ESXi junto con vCenter Server, el rendimiento que se necesita del subsistema de almacenamiento aumenta en consecuencia.
- La cantidad de E/S pendientes necesaria por las aplicaciones que se ejecutan en un sistema ESXi deben coincidir con la cantidad de E/S que puede manejar la SAN.

Rendimiento de la red

Una SAN típica consiste en una recopilación de equipos conectados a una recopilación de sistemas de almacenamiento a través de una red de conmutadores. Varios equipos acceden generalmente al mismo almacenamiento.

En la imagen Conectar un solo vínculo Ethernet con el almacenamiento se muestran varios equipos conectados con un sistema de almacenamiento a través de un conmutador Ethernet. En esta configuración, cada equipo se conecta a través de un solo vínculo Ethernet al conmutador, que también se conecta al sistema de almacenamiento a través de un solo vínculo Ethernet. En la mayoría de las configuraciones con conmutadores modernos y tráfico típico, esto no es un problema.

Figura 12-1. Conectar un solo vínculo Ethernet con el almacenamiento

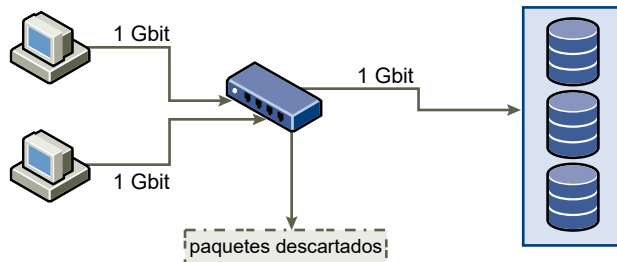


Cuando los sistemas leen datos del almacenamiento, la respuesta máxima del almacenamiento es enviar datos suficientes para completar el vínculo entre los sistemas de almacenamiento y el conmutador Ethernet. Es poco probable que cada sistema o máquina virtual solos haga uso total de la velocidad de red de manera individual, pero esta situación puede esperarse cuando muchos sistemas comparten un dispositivo de almacenamiento.

Cuando se escriben datos en el almacenamiento, varios sistemas o máquinas virtuales pueden intentar completar los vínculos. Como se muestra en la figura Paquetes descartados, cuando sucede esto, el conmutador entre los sistemas y el sistema de almacenamiento debe descartar datos. Esto sucede porque, si bien tiene una conexión única con el dispositivo de

almacenamiento, tiene más tráfico para enviar al sistema de almacenamiento que el que puede transportar un solo vínculo. En este caso, el conmutador descarta paquetes de red porque la cantidad de datos que puede transmitir está limitada por la velocidad del vínculo entre este y el sistema de almacenamiento.

Figura 12-2. Paquetes descartados



La recuperación de datos de los paquetes de red descartados provoca una gran degradación del rendimiento. Además del tiempo dedicado a determinar que se descartaron datos, la retransmisión utiliza ancho de banda que, de lo contrario, podría usarse para transacciones actuales.

El protocolo Transmission Control Protocol (TCP) traslada el tráfico iSCSI en la red. TCP es un protocolo de transmisión confiable que garantiza que se vuelva a intentar la transmisión de los paquetes descartados para que estos alcancen, eventualmente, su destino. TCP está diseñado para recuperar datos a partir de paquetes descartados y volver a transmitirlos de forma rápida y sencilla. Sin embargo, cuando el conmutador descarta paquetes con cualquier regularidad, la capacidad de proceso de la red se ve afectada de forma significativa. La red se congestiona con solicitudes de reenvío de datos y con los paquetes reenviados, y se transfieren en realidad menos datos que en una red sin congestionamiento.

La mayoría de los conmutadores Ethernet pueden almacenar datos en búfer y darle a todos los dispositivos que intentan enviar datos la misma oportunidad de llegar a destino. Esta capacidad de almacenar en búfer algunas transmisiones, junto con muchos sistemas que limitan la cantidad de comandos pendientes, permite que, a su vez, se envíen pequeñas ráfagas desde varios sistemas a un sistema de almacenamiento.

Si las transacciones son grandes y varios servidores intentan enviar datos a través de un solo puerto de conmutador, puede excederse la capacidad de un conmutador de almacenar en búfer una solicitud mientras se transmite otra. En este caso, el conmutador descarta los datos que no puede enviar y el sistema de almacenamiento debe solicitar la retransmisión del paquete descartado. Por ejemplo, si un conmutador Ethernet puede almacenar en búfer 32 KB en un puerto de entrada, pero el servidor conectado piensa que puede enviar 256 KB al dispositivo de almacenamiento, se descartan algunos de los datos.

La mayoría de los conmutadores administrados proporcionan información sobre paquetes descartados, algo similar a lo siguiente:

```
*: interface is up
IHQ: pkts in input hold queue      IQD: pkts dropped from input queue
```

```

OHQ: pkts in output hold queue      OQD: pkts dropped from output queue
RXBS: rx rate (bits/sec)            RXPS: rx rate (pkts/sec)
TXBS: tx rate (bits/sec)            TXPS: tx rate (pkts/sec)
TRTL: throttle count

```

Tabla 12-1. Información de conmutador de muestra

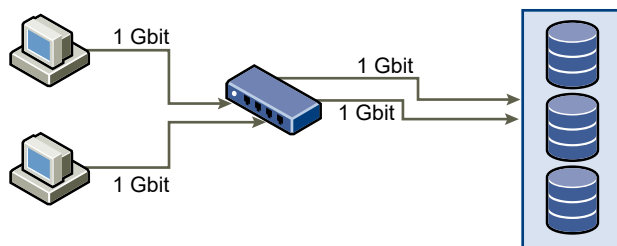
Interfaz	IHQ	IQD	OHQ	OQD	RXBS	RXPS	TXBS	TXPS	TRTL
* GigabitEthernet0/1	3	9922	0	0	476303000	62273	477840000	63677	0

En este ejemplo de un conmutador Cisco, el ancho de banda usado es de 476.303.000 bits/segundo, que es menos de la mitad de la velocidad de cable. A pesar de esto, el puerto almacena en búfer los paquetes entrantes y descarta otros. La línea final de este resumen de interfaz indica que este puerto ya descartó casi 10.000 paquetes entrantes en la columna IQD.

Los cambios de configuración para evitar este problema incluyen comprobar que los diversos vínculos Ethernet de entrada no estén canalizados a un vínculo de salida, ya que provocaría un vínculo con exceso de suscripciones. Cuando se conmuta una cantidad de vínculos que transmiten casi al límite de su capacidad a una cantidad de vínculos menor, es posible que se produzca un exceso de suscripciones.

En general, las aplicaciones o los sistemas que escriben muchos datos en el almacenamiento, como sistemas de adquisición de datos o de registro de transacciones, no deben compartir vínculos Ethernet en un dispositivo de almacenamiento. Estos tipos de aplicaciones tienen mejor rendimiento con varias conexiones a los dispositivos de almacenamiento.

La imagen Varias conexiones del conmutador al almacenamiento muestra varias conexiones del conmutador al almacenamiento.

Figura 12-3. Varias conexiones del conmutador al almacenamiento

La utilización de VLAN o VPN no proporciona una solución adecuada al problema de exceso de suscripciones de vínculos en configuraciones compartidas. Las VLAN y otras particiones virtuales de una red proporcionan una forma de designar una red lógicamente, pero no cambian las capacidades físicas de los vínculos y los troncos entre los conmutadores. Cuando el tráfico de almacenamiento y otro tráfico de red terminan compartiendo conexiones físicas, como harían con

una VPN, existe la posibilidad de que se produzcan un exceso de suscripciones y la pérdida de paquetes. Lo mismo ocurre con las VLAN que comparten troncos entre conmutadores. El diseño de rendimiento de una SAN debe tener en cuenta las limitaciones físicas de la red, no las asignaciones lógicas.

Comprobar estadísticas del conmutador Ethernet

Muchos conmutadores Ethernet ofrecen diferentes métodos para supervisar el estado del conmutador.

Los conmutadores que tienen puertos funcionando cerca de su capacidad de proceso máxima la mayor parte del tiempo no brindan un rendimiento óptimo. Si tiene puertos en una SAN iSCSI funcionando cerca del máximo, reduzca la carga. Si el puerto está conectado con un sistema ESXi o almacenamiento iSCSI, puede reducir la carga a través del equilibrio de carga manual.

Si el puerto está conectado entre varios conmutadores o enrutadores, considere instalar vínculos adicionales entre estos componentes para soportar mayor carga. Generalmente, los conmutadores Ethernet también ofrecen información sobre errores de transmisión, paquetes en cola y paquetes Ethernet descartados. Si el conmutador informa regularmente cualquiera de estas condiciones en puertos que se usen para el tráfico iSCSI, el rendimiento de la SAN iSCSI no será bueno.

Administrar dispositivos de almacenamiento

13

Administre los dispositivos de almacenamiento locales y en red a los que tiene acceso el host ESXi.

Este capítulo incluye los siguientes temas:

- Características de los dispositivos de almacenamiento
- Descripción de la nomenclatura de dispositivos de almacenamiento
- Operaciones para actualizar y volver a examinar el almacenamiento
- Identificar problemas de conectividad del dispositivo
- Habilitar o deshabilitar el LED localizador en dispositivos de almacenamiento

Características de los dispositivos de almacenamiento

Se pueden ver todos los dispositivos de almacenamiento o los LUN disponibles para el host, incluidos todos los dispositivos en red y locales. Si se usan complementos de múltiples rutas de terceros, los dispositivos de almacenamiento disponibles por medio de los complementos también aparecen en la lista.

Se puede ver una lista independiente de los dispositivos de almacenamiento disponibles para un adaptador en particular.

Generalmente, al consultar los dispositivos de almacenamiento, se ve la siguiente información.

Tabla 13-1. Información de dispositivos de almacenamiento

Información de dispositivos de almacenamiento	Descripción
Name (Nombre)	También llamado Nombre para mostrar. Es un nombre que el host ESXi asigna al dispositivo según el tipo de almacenamiento y el fabricante. Puede cambiar este nombre por el nombre que desee.
Identificador	Un identificador universalmente único que es intrínseco al dispositivo.
Estado operativo	Indica si el dispositivo está montado o desmontado. Para obtener información detallada, consulte Separar dispositivos de almacenamiento .
LUN	Número de unidad lógica (LUN) en el destino SCSI. El número LUN se obtiene del sistema de almacenamiento. Si un destino tiene un solo LUN, el número LUN siempre es cero (0).

Tabla 13-1. Información de dispositivos de almacenamiento (continuación)

Información de dispositivos de almacenamiento	Descripción
Tipo	Tipo de dispositivo, por ejemplo, disco o CD-ROM.
Tipo de unidad	Información que especifica si el dispositivo es una unidad flash o una unidad HDD regular. Para obtener información sobre las unidades flash, consulte Capítulo 14 Trabajar con dispositivos flash .
Transporte	Protocolo de transporte que usa el host para acceder al dispositivo. El protocolo depende del tipo de almacenamiento que se usa. Consulte Tipos de almacenamiento físico .
Capacity (Capacidad)	Capacidad total del dispositivo de almacenamiento.
Propietario	El complemento, como NMP o el complemento de un tercero, que el host usa para administrar las rutas de acceso al dispositivo de almacenamiento. Para obtener información detallada, consulte Administrar varias rutas de acceso .
Aceleración de hardware	Información sobre si el dispositivo de almacenamiento asiste al host en las operaciones de administración de máquinas virtuales. El estado puede ser Supported (Compatible), Not Supported (No compatible) o Unknown (Desconocido). Para obtener información detallada, consulte Capítulo 23 Aceleración de hardware de almacenamiento .
Ubicación	Una ruta de acceso al dispositivo de almacenamiento en el directorio <code>/vmfs/devices/</code> .
Formato de partición	Un esquema de particiones que usa el dispositivo de almacenamiento. Puede ser un formato de registro de arranque maestro (MBR) o de tabla de particiones GUID (GPT). Los dispositivos GPT pueden admitir almacenes de datos mayores a 2 TB. Para obtener más información, consulte Almacenes de datos de VMFS y formatos de disco de almacenamiento .
Particiones	Particiones principales y lógicas, incluido un almacén de datos de VMFS, si está configurado.
Directivas de múltiples rutas (almacenes de datos de VMFS)	Directiva de selección de rutas de acceso y directiva de tipo de matriz de almacenamiento que usa el host para administrar las rutas de acceso al almacenamiento. Para obtener más información, consulte Capítulo 17 Descripción de múltiples rutas y conmutación por error .
Rutas de acceso (almacenes de datos de VMFS)	Rutas de acceso que se utilizan para acceder al almacenamiento y a su estado.

Mostrar dispositivos de almacenamiento de un host

Muestre todos los dispositivos de almacenamiento disponibles para un host. Si se utiliza algún complemento de múltiples rutas de terceros, los dispositivos de almacenamiento disponibles por medio de los complementos también aparecen en la lista.

La vista Storage Devices (Dispositivos de almacenamiento) permite enumerar los dispositivos de almacenamiento de los hosts, analizar la información y modificar las propiedades.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.

- 3 En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento**.

Todos los dispositivos de almacenamiento disponibles para el host aparecen enumerados en Storage Devices (Dispositivos de almacenamiento).

- 4 Para ver los detalles de un dispositivo específico, seleccione el dispositivo en la lista.
- 5 Utilice las pestañas en Device Details (Detalles del dispositivo) para acceder a la información adicional y modificar las propiedades del dispositivo seleccionado.

Pestaña	Descripción
Properties (Propiedades)	Vea las propiedades y características del dispositivo. Vea y modifique las directivas de múltiples rutas para el dispositivo.
Rutas de acceso	Muestre las rutas de acceso disponibles para el dispositivo. Permite deshabilitar o habilitar una ruta de acceso seleccionada.

Mostrar dispositivos de almacenamiento para un adaptador

Muestre una lista de dispositivos de almacenamiento a los que se pueda acceder a través de un adaptador de almacenamiento específico en el host.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en Storage Adapters (Adaptadores de almacenamiento).
Todos los adaptadores de almacenamiento instalados en el host aparecen en el listado de Storage Adapters (Adaptadores de almacenamiento).
- 4 Seleccione el adaptador en la lista y haga clic en la pestaña **Devices** (Dispositivos).
Aparecen los dispositivos de almacenamiento a los que puede acceder el host a través del adaptador.

Descripción de la nomenclatura de dispositivos de almacenamiento

Cada dispositivo de almacenamiento, o LUN, se identifica con varios nombres.

Identificadores de dispositivo

Según el tipo de almacenamiento, el host ESXi utiliza distintos algoritmos y convenciones para generar un identificador para cada dispositivo de almacenamiento.

Identificadores SCSI INQUIRY.

El host utiliza el comando SCSI INQUIRY para consultar un dispositivo de almacenamiento y utiliza los datos resultantes, en especial la información de la página 83, para generar un

identificador único. Los identificadores de dispositivos basados en la página 83 son únicos en todos los hosts, persistentes y tienen uno de los formatos siguientes:

- *naa.number*
- *t10.number*
- *eui.number*

Estos formatos se adhieren a los estándares del comité T10. Consulte la documentación de SCSI-3 en el sitio web del comité T10.

Identificador basado en rutas de acceso.

Cuando el dispositivo no proporciona la información de la página 83, el host genera un nombre *mpx.path*, en el que *path* representa la primera ruta de acceso al dispositivo, por ejemplo, *mpx.vmhba1:C0:T1:L3*. Este identificador puede utilizarse del mismo modo que el identificador SCSI INQUIRY.

El identificador *mpx.* se crea para dispositivos locales sobre la suposición de que los nombres de ruta de acceso son únicos. Sin embargo, este identificador no es ni único ni persistente, y puede cambiar después de cada arranque.

Generalmente, la ruta de acceso al dispositivo tiene el formato siguiente:

vmhbaAdapter:CChannel:TTarget:LLUN

- *vmhbaAdapter* es el nombre del adaptador de almacenamiento. El nombre se refiere al adaptador físico en el host, no a la controladora SCSI que usan las máquinas virtuales.
- *CChannel* es el número de canal de almacenamiento.

Los adaptadores de iSCSI de software y los adaptadores de hardware dependiente utilizan el número de canal para mostrar varias rutas de acceso al mismo destino.

- *TTarget* es el número de destino. El host determina la numeración de destinos y esta puede cambiar si las asignaciones de destinos visibles para el host cambian. Los destinos compartidos entre distintos hosts no pueden tener el mismo número de destino.
- *LLUN* es el número LUN que muestra la posición del LUN en el destino. El número LUN se obtiene del sistema de almacenamiento. Si un destino tiene un solo LUN, el número LUN siempre es cero (0).

Por ejemplo, *vmhba1:C0:T3:L1* representa al LUN1 en el destino 3 al que se accede a través del adaptador de almacenamiento *vmhba1* y del canal 0.

Identificador heredado

Además de los identificadores SCSI INQUIRY o *mpx.*, para cada dispositivo, ESXi genera un nombre heredado alternativo. El identificador tiene el formato siguiente:

vml.number

El identificador heredado incluye una serie de dígitos que son únicos del dispositivo y pueden derivar, en parte, de la información de la página 83, si está disponible. En los dispositivos no locales que no admiten la información de la página 83, se usa el nombre vml. como el único identificador exclusivo disponible.

Ejemplo: Mostrar nombres de dispositivo en vSphere CLI

Puede utilizar el comando `esxcli --server=server_name storage core device list` para mostrar todos los nombres de dispositivo en vSphere CLI. El resultado es similar al ejemplo siguiente:

```
# esxcli --server=server_name storage core device list
naa.number
    Display Name: DGC Fibre Channel Disk(naa.number)
    ...
    Other UIDs:vml.number
```

Cambiar nombre de los dispositivos de almacenamiento

Se puede cambiar el nombre para mostrar de un dispositivo de almacenamiento. El host ESXi asigna el nombre para mostrar según el tipo de almacenamiento y el fabricante.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento**.
- 4 Seleccione el dispositivo al que desea cambiar el nombre y haga clic en **Rename** (Cambiar nombre).
- 5 Cambie el nombre del dispositivo a un nombre descriptivo.

Operaciones para actualizar y volver a examinar el almacenamiento

La operación de actualización de almacenes de datos, dispositivos de almacenamiento y adaptadores de almacenamiento actualiza la información de almacenamiento y las listas que se muestran en vSphere Web Client. Por ejemplo, actualiza información como la capacidad del almacén de datos. Cuando realiza tareas de administración de almacenamiento o hace cambios en la configuración de SAN, es posible que necesite volver a examinar el almacenamiento.

Cuando realiza operaciones de administración del almacén de datos de VMFS, como crear un almacén de datos de VMFS o RDM, agregar una extensión y aumentar o eliminar un almacén de datos de VMFS, el host o vCenter Server vuelven a examinar el almacenamiento y lo actualizan automáticamente. Puede deshabilitar la característica automática para volver a examinar si desactiva la opción Host Rescan Filter (Filtro para volver a examinar el host). Consulte [Desactivar los filtros de almacenamiento](#).

En ciertos casos, debe volver a examinar de forma manual. Puede volver a examinar todo el almacenamiento disponible para el host, o bien si utiliza vCenter Server, para todos los hosts en una carpeta, un clúster y un centro de datos.

Si los cambios que realiza son exclusivos para el almacenamiento conectado a través de un adaptador específico, vuelva a examinar ese adaptador.

Vuelva a examinar de forma manual cada vez que haga uno de los cambios siguientes:

- Al dividir en zonas una matriz de discos nueva en una SAN.
- Al crear LUN nuevos en una SAN.
- Al cambiar el enmascaramiento de las rutas de acceso en un host.
- Reconectar un cable.
- Al cambiar la configuración de CHAP (solo iSCSI).
- Al agregar o quitar direcciones estáticas o de detección (solo iSCSI).
- Al agregar un solo host a vCenter Server después de editar o quitar de vCenter Server un almacén de datos compartido por los hosts de vCenter Server y el mismo host.

Importante Si vuelve a examinar cuando una ruta de acceso no está disponible, el host quita la ruta de acceso de la lista de rutas de acceso al dispositivo. La ruta de acceso vuelve a aparecer en la lista cuando vuelve a estar disponible y vuelve a funcionar.

Realizar la operación para volver a examinar el almacenamiento

Cuando se realizan cambios en la configuración de SAN, es posible que haya que volver a examinar el almacenamiento. Puede volver a examinar todo el almacenamiento disponible para el host, el clúster o el centro de datos. Si los cambios que realiza son aislados para un almacenamiento al que se accede a través de un host específico, vuelva a examinar solo este host.

Procedimiento

- 1 En el navegador de objetos de vSphere Web Client, desplácese hasta un host, un clúster, un centro de datos o una carpeta que contenga hosts.
- 2 Seleccione **Storage (Almacenamiento) > Rescan Storage (Volver a examinar almacenamiento)** en el menú contextual.

3 Especifique la extensión del nuevo análisis.

Opción	Descripción
Scan for New Storage Devices (Buscar nuevos dispositivos de almacenamiento)	Vuelva a examinar todos los adaptadores para detectar nuevos dispositivos de almacenamiento. Si se detectan nuevos dispositivos, estos aparecen en la lista de dispositivos.
Scan for New VMFS Volumes (Buscar nuevos volúmenes VMFS)	Vuelva a examinar todos los dispositivos de almacenamiento para detectar almacenes de datos nuevos que se hayan agregado desde la última exploración. Todos los almacenes de datos nuevos aparecen en la lista de almacenes de datos.

Realizar la operación para volver a examinar el adaptador

Cuando se hacen cambios en la configuración de SAN y los cambios son exclusivos para el almacenamiento al que se accede a través de un adaptador específico, vuelva a examinar solo ese adaptador.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Storage Adapters** (Adaptadores de almacenamiento) y seleccione en la lista el adaptador que desea volver a examinar.
- 4 Haga clic en el icono **Rescan Adapter** (Volver a examinar adaptador).

Cambiar la cantidad de dispositivos de almacenamiento examinados

Mientras que un host ESXi se limita a acceder a 256 dispositivos de almacenamiento SCSI, el rango de identificadores de LUN puede ir del 0 al 1023. ESXi omite los identificadores de LUN 1024 o mayores. `Disk.MaxLUN` controla este límite; su valor predeterminado de 1.024.

El valor de `Disk.MaxLUN` también determina cuántos LUN intentará detectar el código de tecla SCSI mediante los comandos individuales de consulta INQUIRY si el destino SCSI no admite la detección directa mediante REPORT_LUNS.

Se puede modificar el parámetro `Disk.MaxLUN` según las necesidades. Por ejemplo, si el entorno tiene una cantidad menor de dispositivos de almacenamiento con identificador de LUN del 0 al 100, se puede establecer el valor a 101 para mejorar la velocidad de detección del dispositivo en destinos que no admiten REPORT_LUNS. Si se reduce el valor, se puede acortar el tiempo para volver a examinar y el tiempo de arranque. Sin embargo, el tiempo necesario para volver a examinar los dispositivos de almacenamiento puede depender de otros factores, como el tipo de sistema de almacenamiento y la carga presente en el sistema de almacenamiento.

En otros casos, es posible que haya que aumentar el valor si el entorno utiliza identificadores de LUN mayores que 1.023.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Sistema**, haga clic en **Configuración avanzada del sistema**.
- 4 En Advanced System Settings (Configuración avanzada del sistema), seleccione **Disk.MaxLUN** y haga clic en el icono **Edit** (Editar).
- 5 Cambie el valor actual por el valor de su elección y haga clic en **OK** (Aceptar).

El valor que introduzca especifica el identificador de LUN que viene después del último que desea detectar.

Por ejemplo, para detectar identificadores de LUN del 0 al 100, establezca **Disk.MaxLUN** en 101.

Identificar problemas de conectividad del dispositivo

Cuando el host ESXi tiene un problema durante la conexión con un dispositivo de almacenamiento, el host trata el problema como permanente o temporal según ciertos factores.

Los problemas de conectividad de almacenamiento se producen por distintos motivos. Aunque ESXi no siempre puede determinar el motivo de la falta de disponibilidad de un dispositivo de almacenamiento o sus rutas de acceso, el host diferencia entre un estado de pérdida permanente de dispositivo (Permanent Device Loss, PDL) y un estado transitorio de todas las rutas de acceso inactivas (All Paths Down, APD) de almacenamiento.

Pérdida permanente del dispositivo (Permanent Device Loss, PDL)

Una condición que se produce cuando un dispositivo de almacenamiento tiene errores permanentes o se elimina o excluye administrativamente. No se espera que vuelva a estar disponible. Cuando el dispositivo está permanentemente no disponible, ESXi recibe los códigos de detección apropiados o un rechazo de inicio de sesión por parte de las matrices de almacenamiento, y puede reconocer que el dispositivo se perdió de manera permanente.

Todas las rutas de acceso inactivas (All Paths Down, APD)

Una condición que se produce cuando un dispositivo de almacenamiento es inaccesible para el host y ninguna de las rutas de acceso al dispositivo está disponible. ESXi trata esto como una condición transitoria, ya que generalmente los problemas del dispositivo son temporales, y se espera que vuelva a estar disponible.

Detectar condiciones de PDL

Se considera que un dispositivo de almacenamiento está en estado de pérdida permanente de dispositivo (Permanent Device Loss, PDL) cuando se vuelve no disponible de manera permanente para el host ESXi.

Por lo general, la condición de PDL se produce cuando un dispositivo se elimina sin intención o su identificador único cambia, o cuando el dispositivo tiene un error de hardware irreparable.

Cuando la matriz de almacenamiento determina que un dispositivo no está disponible de manera permanente, envía códigos de detección SCSI al host ESXi. Los códigos de detección permiten que el host reconozca que el dispositivo falló y registra su estado como PDL. Los códigos de detección deben recibirse en todas las rutas de acceso del dispositivo para que se lo considere perdido de manera permanente.

Después de registrar el estado PDL del dispositivo, el host interrumpe los intentos de volver a establecer la conectividad o emitir comandos al dispositivo para evitar bloquearse o quedarse sin capacidad de respuesta.

vSphere Web Client muestra la siguiente información acerca del dispositivo:

- El estado operativo del dispositivo cambia a `Lost Communication`.
- Todas las rutas de acceso se muestran como `Dead`.
- Los almacenes de datos del dispositivo aparecen atenuados.

El host quita automáticamente el dispositivo en estado PDL y todas las rutas de acceso hacia el dispositivo si no existen conexiones abiertas a este, o después de que se cierra la última conexión. Para deshabilitar la eliminación automática de rutas de acceso, establezca el parámetro avanzado `Disk.AutoremoveOnPDL` del host en 0. Consulte [Establecer atributos de host avanzados](#).

Si el dispositivo regresa de la condición de PDL, el host puede detectarlo, pero lo trata como un dispositivo nuevo. No se garantiza la consistencia de los datos para las máquinas virtuales en el dispositivo recuperado.

Nota El host no puede detectar condiciones de PDL y sigue tratando los problemas de conectividad del dispositivo como APD cuando un dispositivo de almacenamiento genera errores permanentemente en una forma que no devuelve códigos de detección SCSI adecuados o rechaza el inicio de sesión iSCSI.

Pérdida permanente de dispositivo y códigos de detección SCSI

El siguiente ejemplo de código de detección SCSI de un registro del VMkernel indica que el dispositivo está en estado PDL.

```
H:0x0 D:0x2 P:0x0 Valid sense data: 0x5 0x25 0x0 or Logical Unit Not Supported
```

Para obtener información sobre los códigos de detección SCSI, consulte *Solución de problemas de almacenamiento* en *Solución de problemas de vSphere*.

Pérdida permanente de dispositivo e iSCSI

En el caso de las matrices iSCSI con un solo LUN por destino, PDL se detecta a través de un error en el inicio de sesión iSCSI. Una matriz de almacenamiento iSCSI rechaza el intento del host de iniciar una sesión iSCSI con el motivo `Target Unavailable` (Destino no disponible). Como sucede con los códigos de detección, esta respuesta debe recibirse en todas las rutas de acceso para que el dispositivo se considere perdido de manera permanente.

Pérdida permanente de dispositivo y máquinas virtuales

Después de registrar el estado PDL del dispositivo, el host finaliza todas las operaciones de E/S de las máquinas virtuales. vSphere HA puede detectar PDL y reiniciar las máquinas virtuales con errores. Para obtener más información, consulte [Alta disponibilidad y problemas de conectividad del dispositivo](#).

Eliminar dispositivo de almacenamiento planificada

Cuando un dispositivo de almacenamiento funciona mal, puede evitar la condición de pérdida de dispositivo permanente (Permanent Device Loss, PDL) o todas las rutas de acceso inactivas (All Paths Down, APD), y quitar y volver a conectar de forma planificada el dispositivo de almacenamiento.

La eliminación del dispositivo planificada es una desconexión intencional de un dispositivo de almacenamiento. También es posible que planifique quitar un dispositivo por motivos como la actualización de hardware o la reconfiguración de los dispositivos de almacenamiento. Cuando se realiza una eliminación y reconexión ordenada de un dispositivo de almacenamiento, se completan varias tareas.

- 1 Migre las máquinas virtuales del dispositivo que planifica separar.
Consulte la documentación de *Administración de vCenter Server y hosts*.
- 2 Desmonte el almacén de datos implementado en el dispositivo.
Consulte [Desmontar almacenes de datos](#).
- 3 Separe el dispositivo de almacenamiento.
Consulte [Separar dispositivos de almacenamiento](#).
- 4 En el caso de un dispositivo iSCSI con un solo LUN por destino, elimine la entrada de destino estático de cada HBA de iSCSI que tenga una ruta de acceso al dispositivo de almacenamiento.
Consulte [Quitar destinos iSCSI dinámicos o estáticos](#).
- 5 Realice cualquier reconfiguración necesaria del dispositivo de almacenamiento con la consola matriz.
- 6 Vuelva a conectar el dispositivo de almacenamiento.
Consulte [Asociar dispositivos de almacenamiento](#).

- 7 Monte el almacén de datos y reinicie las máquinas virtuales. Consulte [Montar almacenes de datos](#).

Separar dispositivos de almacenamiento

Desconecte de forma segura un dispositivo de almacenamiento del host.

Es posible que se deba desconectar el dispositivo para que el host no pueda acceder cuando, por ejemplo, se realice una actualización de hardware del lado del almacenamiento.

Requisitos previos

- El dispositivo no contiene ningún almacén de datos.
- Ninguna máquina virtual usa el dispositivo como disco RDM.
- El dispositivo no contiene una partición de diagnóstico o una partición desde cero.

Procedimiento

- 1 En vSphere Web Client, muestre los dispositivos de almacenamiento.
- 2 Seleccione el dispositivo que desea desconectar y haga clic en el icono **Detach** (Desconectar).

Resultados

El dispositivo deja de ser accesible. El estado operativo del dispositivo cambia a Unmounted (Desmontado).

Pasos siguientes

Si varios hosts comparten el dispositivo, desconecte el dispositivo de cada host.

Asociar dispositivos de almacenamiento

Vuelva a conectar un dispositivo de almacenamiento que desconectó anteriormente.

Procedimiento

- 1 En vSphere Web Client, muestre los dispositivos de almacenamiento.
- 2 Seleccione el dispositivo de almacenamiento desconectado y haga clic en el icono **Attach** (Conectar).

Resultados

El dispositivo vuelve a ser accesible.

Recuperar condiciones de PDL

Una condición de pérdida permanente de dispositivo (Permanent Device Loss, PDL) no planificada ocurre cuando un dispositivo de almacenamiento deja de estar disponible permanentemente sin desconectarlo adecuadamente del host ESXi.

Los elementos siguientes en vSphere Web Client indican que el dispositivo está en estado de PDL:

- El almacén de datos implementado en el dispositivo no está disponible.
- El estado operativo del dispositivo cambia a Lost Communication (Comunicación perdida).
- Todas las rutas de acceso aparecen como Dead (Inactivas).
- En el archivo de registro VMkernel aparece una advertencia acerca de que el dispositivo se encuentra inaccesible permanentemente.

Para recuperarse de una condición de PDL no planificada y quitar el dispositivo no disponible del host, se deben realizar algunas tareas.

- 1 Apague y cancele el registro de todas las máquinas virtuales que están en ejecución en los almacenes de datos afectados por la condición de PDL.

- 2 Desmonte el almacén de datos.

Consulte [Desmontar almacenes de datos](#).

- 3 Vuelva a examinar todos los hosts ESXi que tenían acceso al dispositivo.

Consulte [Realizar la operación para volver a examinar el almacenamiento](#).

Nota Si el proceso de volver a examinar no se completa correctamente y el host sigue mostrando el dispositivo, es posible que aún existan algunas operaciones de E/S pendientes o referencias activas al dispositivo. Busque las máquinas virtuales, las plantillas, las imágenes ISO, las asignaciones de dispositivos sin formato y demás que todavía puedan tener una referencia activa al dispositivo o al almacén de datos.

Manejar condiciones de APD transitorias

Se considera que un dispositivo de almacenamiento se encuentra en el estado con todas las rutas de acceso inactivas (All Paths Down, APD) cuando no está disponible para el host ESXi durante un período indeterminado.

Los motivos de un estado APD pueden ser, por ejemplo, un conmutador con errores o un cable de almacenamiento desconectado.

A diferencia del estado de pérdida de dispositivo permanente (Permanent Device Loss, PDL), el host considera que el estado APD es transitorio y espera que el dispositivo esté nuevamente disponible.

El host vuelve a intentar de manera indefinida los comandos emitidos con el fin de restablecer la conectividad con el dispositivo. Si los reintentos de los comandos del host no se ejecutan durante un período prolongado, el host y sus máquinas virtuales pueden correr el riesgo de tener problemas de rendimiento y de una potencial falta de respuesta.

Para evitar estos problemas, el host utiliza la característica de manejo de APD predeterminada. Cuando un dispositivo entra en el estado APD, el sistema activa de inmediato un temporizador para permitir que el host siga reintentando comandos de máquinas no virtuales durante un período limitado.

De manera predeterminada, el tiempo de espera de APD es de 140 segundos, un lapso por lo general más largo que el requerido por la mayoría de los dispositivos para recuperarse de una pérdida de conexión. Si el dispositivo vuelve a estar disponible en este lapso, el host y su máquina virtual seguirán ejecutándose sin experimentar ningún problema.

Si el dispositivo no se recupera y se cumple el tiempo de espera, el host detiene sus intentos y finaliza todas las E/S de máquinas no virtuales. Las E/S de máquinas virtuales seguirán reintentándose. vSphere Web Client muestra la siguiente información del dispositivo con el tiempo de espera de APD cumplido:

- El estado operativo del dispositivo cambia a `Dead or Error`.
- Todas las rutas de acceso se muestran como `Dead`.
- Los almacenes de datos en el dispositivo se atenúan.

Aunque el dispositivo y los almacenes de datos no están disponibles, las máquinas virtuales siguen respondiendo. Puede apagar las máquinas virtuales o migrarlas a otro almacén de datos o host.

Si más tarde las rutas de acceso del dispositivo se vuelven operativas, las E/S posteriores al dispositivo se emitirán normalmente y finalizará todo el tratamiento especial de APD.

Deshabilitar el manejo de APD de almacenamiento

El manejo de todas las rutas de acceso inactivas (All Paths Down, APD) de almacenamiento en el host ESXi está habilitado de manera predeterminada. Cuando está habilitado, el host continúa reintentando la ejecución de comandos de E/S de máquinas no virtuales en un dispositivo de almacenamiento en estado APD durante un período limitado. Cuando caduca este período, el host interrumpe los reintentos y finaliza todas las operaciones de E/S de las máquinas no virtuales. Es posible deshabilitar la característica de manejo de APD en el host.

Si se deshabilita el manejo de APD, el host continúa reintentando la ejecución de los comandos emitidos indefinidamente, con la intención de volver a conectarse con el dispositivo APD. Este comportamiento es similar al que se produce en ESXi versión 5.0. Esto puede causar que las máquinas virtuales en el host superen su tiempo de espera de E/S interno y dejen de responder o generen errores. El host podría desconectarse de vCenter Server.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Sistema**, haga clic en **Configuración avanzada del sistema**.
- 4 En Advanced System Settings (Configuración avanzada del sistema), seleccione el parámetro **Misc.APDHandlingEnable** y haga clic en el icono `Edit`.
- 5 Cambie el valor a `0`.

Resultados

Si deshabilitó el manejo de APD, puede volver a habilitarlo cuando un dispositivo entre al estado APD. La característica de manejo de APD interna se activa inmediatamente, y el temporizador se inicia con el valor de tiempo de espera actual para cada dispositivo en APD.

Cambiar los límites de tiempo de espera para APD de almacenamiento

El parámetro de tiempo de espera controla cuántos segundos el host ESXi reintentará comandos de E/S de máquina no virtual hacia un dispositivo de almacenamiento en un estado de todas las rutas de acceso inactivas (All Paths Down, APD). Si es necesario, puede cambiar el valor de tiempo de espera predeterminado.

El temporizador se inicia inmediatamente después de que el dispositivo entra en estado APD. Cuando caduca el tiempo de espera, el host marca el dispositivo APD como inaccesible y genera un error en todas las E/S de máquina no virtual pendientes o nuevas. Seguirán reintentándose las E/S de máquina virtual.

El parámetro de tiempo de espera predeterminado en el host es de 140 segundos. Puede aumentar el valor del tiempo de espera si, por ejemplo, los dispositivos de almacenamiento conectados al host ESXi tardan más de 140 segundos en recuperarse de una pérdida de conexión.

Nota Si cambia el valor de tiempo de espera con un APD en curso, no afectará el tiempo de espera de ese APD.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Sistema**, haga clic en **Configuración avanzada del sistema**.
- 4 En Advanced System Settings (Configuración avanzada del sistema), seleccione el parámetro **Misc.APDTimeout** y haga clic en el icono **Edit**.
- 5 Cambie el valor predeterminado.

Puede introducir un valor entre 20 y 99999 segundos.

Comprobar el estado de conexión de un dispositivo de almacenamiento

Use el comando `esxccli` para comprobar el estado de conexión de un dispositivo de almacenamiento en particular.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- 1 Ejecute el comando `esxcli --server=server_name storage core device list -d=device_ID`.
- 2 Compruebe el estado de conexión en el campo `Status:` (Estado:).
 - `on`: el dispositivo está conectado.
 - `dead`: el dispositivo entró al estado APD. Se inicia el temporizador de APD.
 - `dead timeout`: caducó el tiempo de espera de APD.
 - `not connected`: el dispositivo está en estado PDL.

Alta disponibilidad y problemas de conectividad del dispositivo

Cuando un dispositivo entra en estado de pérdida permanente de dispositivo (Permanent Device Loss, PDL) o de todas las rutas de acceso inactivas (All Paths Down, APD), vSphere High Availability (HA) puede detectar problemas de conectividad y proporcionar una recuperación automática de todas las máquinas virtuales afectadas.

vSphere HA utiliza VM Component Protection (VMCP) (Protección de componentes de la máquina virtual [VMCP]) para proteger las máquinas virtuales que se ejecutan en un host en un clúster de vSphere HA de errores de accesibilidad. Para obtener más información sobre VMCP y cómo configurar respuestas para los almacenes de datos y las máquinas virtuales cuando ocurre una condición de APD o PDL, consulte la documentación de *Disponibilidad de vSphere*.

Habilitar o deshabilitar el LED localizador en dispositivos de almacenamiento

Utilice el LED localizador para identificar dispositivos de almacenamiento específicos y poder reconocerlos entre otros dispositivos. Es posible encender o apagar el LED localizador.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Almacenamiento**, haga clic en **Dispositivos de almacenamiento**.

- 4 En la lista de dispositivos de almacenamiento, seleccione uno o varios discos y habilite o deshabilite el indicador del LED localizador.

Opción	Descripción
Enable (Habilitar)	Haga clic en el icono Turns on the locator LED (Enciende el LED localizador).
Disable (Deshabilitar)	Haga clic en el icono Turns off the locator LED (Apaga el LED localizador).

Trabajar con dispositivos flash

14

Además de las unidades de disco duro (HDD) de almacenamiento normales, vSphere es compatible con dispositivos de almacenamiento flash.

A diferencia de los HDD normales que son dispositivos electromecánicos que contienen partes móviles, los dispositivos flash utilizan semiconductores como medio de almacenamiento y no tienen partes móviles. Por lo general, los dispositivos flash son muy resistentes y proporcionan un acceso más rápido a los datos.

Para detectar dispositivos flash, ESXi utiliza un mecanismo de consulta basado en estándares T10. El host ESXi puede detectar dispositivos flash en varias matrices de almacenamiento. Compruebe con el proveedor si la matriz de almacenamiento es compatible con el mecanismo de ESXi de detección de dispositivos flash.

Una vez que el host detecta los dispositivos flash, es posible utilizarlos para diversas tareas y funcionalidades.

Este capítulo incluye los siguientes temas:

- Usar dispositivos flash con vSphere
- Marcado de dispositivos de almacenamiento
- Supervisar dispositivos flash
- Prácticas recomendadas para dispositivos flash
- Acerca del recurso flash virtual
- Configurar la memoria caché de intercambio del host

Usar dispositivos flash con vSphere

En el entorno de vSphere, los dispositivos flash se pueden utilizar para diversas funcionalidades.

Tabla 14-1. Usar dispositivos flash con vSphere

Funcionalidad	Descripción
Virtual SAN	Virtual SAN requiere dispositivos flash. Para obtener más información, consulte la documentación sobre <i>Administración de VMware Virtual SAN</i> .
VMFS Datastores (Almacenes de datos de VMFS)	<p>Puede crear almacenes de datos de VMFS en dispositivos flash. Use los almacenes de datos con los siguientes propósitos:</p> <ul style="list-style-type: none"> ■ Almacenar máquinas virtuales. Algunos sistemas operativos invitados pueden identificar discos virtuales almacenados en estos almacenes de datos como discos virtuales flash. Consulte Identificar discos virtuales flash. ■ Asigne espacio del almacén de datos para la memoria caché de intercambio del host ESXi. Consulte Configurar la memoria caché de intercambio del host
Virtual Flash Resource (VFFS) (Recurso flash virtual)	<p>Configure un recurso flash virtual y úselo para las siguientes funcionalidades:</p> <ul style="list-style-type: none"> ■ Úselo como Flash Read Cache virtual para las máquinas virtuales. Consulte Capítulo 15 Acerca de VMware vSphere Flash Read Cache. ■ Asigne el recurso flash virtual para la memoria caché de intercambio del host ESXi. Este es un método alternativo para la configuración de la memoria caché del host que usa volúmenes VFFS en lugar de almacenes de datos de VMFS. Consulte Configurar la memoria caché de intercambio del host con un recurso flash virtual. ■ Si el proveedor lo solicita, utilice el recurso flash virtual para los filtros de E/S de almacenamiento en caché. Consulte Capítulo 21 Filtrar E/S de máquinas virtuales.

Identificar discos virtuales flash

Los sistemas operativos invitados pueden identificar discos virtuales que residen en almacenes de datos basados en flash como discos virtuales flash.

Para comprobar si esta característica está habilitada, los sistemas operativos invitados pueden usar comandos de consulta estándares como SCSI VPD Page (B1h) para dispositivos SCSI y ATA IDENTIFY DEVICE (Word 217) para dispositivos IDE.

Para los clones asociados, las instantáneas nativas y los discos delta, los comandos de consulta informan del estado de flash virtual del disco base.

Los sistemas operativos pueden detectar que un disco virtual es un disco flash en las siguientes condiciones:

- La detección de discos virtuales flash se admite en hosts ESXi 5.x y posteriores, y en la versión de hardware virtual 8 o posterior.
- La detección de discos virtuales flash se admite solo en VMFS5 o versiones posteriores.
- Si los discos virtuales se encuentran en almacenes de datos de VMFS compartidos con extensiones de dispositivos flash, el dispositivo debe estar marcado como flash en todos los hosts.
- Para que un disco virtual se identifique como flash virtual, todas las extensiones físicas subyacentes deben tener una copia de seguridad flash.

Marcado de dispositivos de almacenamiento

Es posible utilizar vSphere Web Client para marcar dispositivos de almacenamiento que no son reconocidos automáticamente como dispositivos flash locales.

Cuando se configura Virtual SAN o un recurso de flash virtual, el entorno de almacenamiento debe incluir dispositivos flash locales.

Sin embargo, ESXi no puede reconocer ciertos dispositivos de almacenamiento como dispositivos flash si los proveedores no incluyen compatibilidad con la detección automática de dispositivos flash. En otros casos, ciertos dispositivos flash SAS no SATA podrían no detectarse como locales. Cuando los dispositivos no se reconocen como flash locales, se excluyen de la lista de dispositivos ofrecidos para Virtual SAN o recurso flash virtual. El marcado de estos dispositivos como flash locales permite que estén disponibles para una SAN virtual y un recurso flash virtual.

Marcar dispositivos de almacenamiento como flash

Si ESXi no reconoce automáticamente los dispositivos como flash, márkelos como dispositivos flash.


ESXi no reconoce ciertos dispositivos como flash cuando los proveedores no admiten la detección automática de discos flash. La columna Tipo de unidad de los dispositivos muestra HDD como el tipo.

Precaución El marcado de los discos HDD como discos flash puede deteriorar el rendimiento de los almacenes de datos y los servicios que los utilizan. Marque los discos como flash solo si está seguro de que son discos flash.

Requisitos previos

Compruebe que el dispositivo no esté en uso.

Procedimiento

- 1 Desplácese hasta el host en el navegador de objetos de vSphere Web Client.
- 2 Haga clic en la pestaña **Administrar** y en **Almacenamiento**.
- 3 Haga clic en **Dispositivos de almacenamiento**.
- 4 En la lista de dispositivos de almacenamiento, seleccione uno o varios dispositivos HDD que deben reconocerse como dispositivos flash y haga clic en el icono **Marcar como discos flash** .
- 5 Haga clic en **Sí** para guardar los cambios.

Resultados

El tipo de dispositivo cambia a flash.

Pasos siguientes

Si el dispositivo flash que marca se comparte entre varios hosts, asegúrese de marcar el dispositivo en todos los hosts que comparten el dispositivo.

Marcar dispositivos de almacenamiento como locales

ESXi permite marcar dispositivos como locales. Esto es útil en los casos en que ESXi no puede determinar si ciertos dispositivos son locales.

Requisitos previos

- Asegúrese de que el dispositivo no esté compartido.
- Apague las máquinas virtuales que residen en ese dispositivo y desmonte los almacenes de datos asociados.

Procedimiento

- 1 Desplácese hasta el host en el navegador de objetos de vSphere Web Client.
- 2 Haga clic en la pestaña **Manage** (Administrar) y en **Storage** (Almacenamiento).
- 3 Haga clic en **Storage Devices** (Dispositivos de almacenamiento).
- 4 En la lista de dispositivos de almacenamiento, seleccione uno o varios dispositivos remotos que deben marcarse como locales y haga clic en el icono **Mark as Local for the Host** (Marcar como local para el host).
- 5 Haga clic en **Yes** (Sí) para guardar los cambios.

Supervisar dispositivos flash

Puede supervisar ciertos parámetros de dispositivos flash críticos, entre ellos, el indicador de desgaste de soporte físico, la temperatura y el conteo de sector reasignado, desde un host ESXi.

Use el comando `esxcli` para supervisar dispositivos flash.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Ejecute el siguiente comando para mostrar las estadísticas del dispositivo flash:

```
esxcli server=server_name storage core device smart get -d=flash device_ID
```

Prácticas recomendadas para dispositivos flash

Siga estas prácticas recomendadas al utilizar dispositivos flash en el entorno de vSphere.

- Asegúrese de utilizar el firmware más reciente con dispositivos flash. Consulte con frecuencia a los proveedores de almacenamiento para saber si existen actualizaciones.
- Supervise con atención la intensidad con que utiliza el dispositivo flash y calcule su vida útil estimada. La expectativa de vida útil depende de qué tan activamente siga utilizando el dispositivo flash.

Vida útil estimada para dispositivos flash

Al trabajar con dispositivos flash, supervise qué tan activamente los utiliza y calcule su duración estimada.

Por lo general, los proveedores de almacenamiento proporcionan estimaciones de duración confiables para un dispositivo flash en condiciones ideales. Por ejemplo, un proveedor puede garantizar una duración de 5 años en condiciones de 20 GB de escritura por día. Sin embargo, la expectativa de vida útil más realista del dispositivo depende de cuántas escrituras genera realmente el host ESXi por día. Siga estos pasos para calcular la duración del dispositivo flash.

Requisitos previos

Tenga en cuenta la cantidad de días que transcurrieron desde el último reinicio del host ESXi. Por ejemplo, diez días.

Procedimiento

- 1 Obtenga el número total de bloques escritos en el dispositivo flash desde el último reinicio.

Ejecute el comando **esxcli storage core device stats get -d=device_ID**. Por ejemplo:

```
~ # esxcli storage core device stats get -d t10.aaaaaaaaaaaaaaaa
Device: t10.aaaaaaaaaaaaaaaa
Successful Commands: xxxxxxxx
Blocks Read: xxxxxxxx
Blocks Written: 629145600
Read Operations: xxxxxxxx
```

El elemento "Blocks Written" muestra el número de bloques escritos en el dispositivo desde el último reinicio. En este ejemplo, el valor es 629.145.600. Después de cada reinicio, se restablece en 0.

- 2 Calcule el número total de escrituras y conviértalo a GB.

Un bloque tiene 512 bytes. Para calcular el número total de escrituras, multiplique el valor de "Blocks Written" por 512 y convierta el valor resultante a GB.

En este ejemplo, el número total de escrituras desde el último reinicio es de aproximadamente 322 GB.

- 3 Calcule el número promedio de escrituras por día en GB.

Divida el número total de escrituras por el número de días transcurridos desde el último reinicio.

Si el último reinicio fue hace diez días, el resultado es 32 GB de escrituras por día. Puede promediar este número para un período determinado..

- 4 Haga una estimación de la duración del dispositivo con la fórmula siguiente:

vendor provided number of writes per day multiplicado por *vendor provided life span* dividido por *actual average number of writes per day*

Por ejemplo, si el proveedor garantiza una duración de 5 años con 20 GB de escritura diarios y la cantidad de escrituras diarias real es de 30 GB, la duración del dispositivo flash será de aproximadamente 3,3 años.

Acerca del recurso flash virtual

Puede combinar dispositivos flash locales en un host ESXi en una única capa de almacenamiento en caché virtualizada denominada recurso flash virtual.

Cuando se configura el recurso flash virtual, se crea un sistema de archivos nuevo: el sistema de archivos flash virtual (VFFS). VFFS deriva de VMFS, que está optimizado para dispositivos flash y se usa para agrupar los dispositivos flash físicos en un grupo único de recursos de almacenamiento en caché. Como recurso no persistente, no puede usarse para almacenar máquinas virtuales.

Las funcionalidades de vSphere siguientes requieren el recurso flash virtual:

- Memoria caché de lectura de máquina virtual. Consulte [Capítulo 15 Acerca de VMware vSphere Flash Read Cache](#).
- Memoria caché de intercambio de host. Consulte [Configurar la memoria caché de intercambio del host con un recurso flash virtual](#).
- Filtros de E/S de almacenamiento en caché, si los proveedores lo solicitan. Consulte [Capítulo 21 Filtrar E/S de máquinas virtuales](#).

Antes de configurar el recurso flash virtual, asegúrese de estar utilizando dispositivos aprobados según la *Guía de compatibilidad de VMware*.

Consideraciones sobre el recurso flash virtual

Al configurar un recurso flash virtual que consumen los hosts y las máquinas virtuales de ESXi, se deben tener en cuenta diversas consideraciones.

- Se puede tener un solo recurso flash virtual, también llamado volumen VFFS, en un solo host ESXi. El recurso flash virtual se administra solo en el nivel del host.
- El recurso flash virtual no se puede utilizar para almacenar máquinas virtuales. El recurso flash virtual es solo una capa de almacenamiento en caché.
- Solo es posible utilizar dispositivos flash locales para el recurso flash virtual.
- Puede crear el recurso flash virtual desde dispositivos flash combinados. Todos los tipos de dispositivos se tratan del mismo modo, y no se realiza distinción entre la conectividad SAS, SATA o PCI Express. Al crear el recurso desde dispositivos flash combinados, asegúrese de agrupar los dispositivos de rendimiento similar para maximizar el rendimiento.
- No se pueden utilizar los mismos dispositivos flash locales para el recurso flash virtual y Virtual SAN. Cada uno requiere su propio dispositivo flash dedicado y exclusivo.
- Después de configurar un recurso flash virtual, los hosts ESXi pueden utilizar y consumir la capacidad disponible total como memoria caché de intercambio del host y máquinas virtuales como memoria caché de lectura.
- No se pueden seleccionar dispositivos flash individuales para utilizar como memoria caché de intercambio o memoria caché de lectura. Todos los dispositivos flash se combinan en una sola entidad de recursos flash.

Configurar un recurso flash virtual

Puede configurar un recurso flash virtual o agregar capacidad a un recurso flash virtual existente.

Para configurar un recurso flash virtual, se deben utilizar dispositivos flash locales conectados al host. Para aumentar la capacidad del recurso flash virtual, es posible agregar más dispositivos, hasta la cantidad máxima indicada en la documentación de *Máximos de configuración*. Un dispositivo flash individual debe estar asignado exclusivamente al recurso flash virtual, y no puede compartirse con ningún otro servicio de vSphere, como Virtual SAN o VMFS.

Procedimiento

- 1 En vSphere Web Client, desplácese hasta el host.
- 2 Haga clic en la pestaña **Manage** (Administrar) y en **Settings** (Configuración).
- 3 En Virtual Flash (Flash virtual), seleccione **Virtual Flash Resource Management** (Administración de recursos flash virtuales) y haga clic en **Add Capacity** (Agregar capacidad).

- 4 En la lista de dispositivos flash disponibles, seleccione uno o varios dispositivos que desea utilizar con el recurso flash virtual y haga clic en **OK** (Aceptar).

En ciertas circunstancias, es posible que no se muestren dispositivos flash en la lista. Para obtener más información, consulte la sección Solución de problemas de dispositivos flash en la documentación de *Solución de problemas de vSphere*.

Resultados

Se crea el recurso flash virtual. El área Device Backing (Copia de seguridad de los dispositivos) enumera todos los dispositivos que se utilizan para el recurso flash virtual.

Pasos siguientes

El recurso flash virtual se puede utilizar para la configuración de la memoria caché en el host y de Flash Read Cache en los discos virtuales. Además, es posible que los filtros de E/S de memoria caché desarrollados mediante vSphere API para los filtros de E/S requieran el recurso flash virtual.

Para aumentar la capacidad, agregue más dispositivos flash al recurso flash virtual.

Quitar el recurso flash virtual

Es posible que deba quitar un recurso flash virtual implementado en dispositivos flash locales para liberar los dispositivos para otros servicios.

No puede quitar un recurso flash virtual si está configurado con memoria caché de intercambio del host o si el host tiene máquinas virtuales encendidas y configuradas con Flash Read Cache.

Procedimiento

- 1 En vSphere Web Client, desplácese hasta el host con flash virtual configurado.
- 2 Haga clic en la pestaña **Manage** (Administrar) y en **Settings** (Configuración).
- 3 En Virtual Flash (Flash virtual), seleccione **Virtual Flash Resource Management** (Administración de recursos flash virtuales) y haga clic en **Remove All** (Quitar todo).

Resultados

Después de quitar el recurso flash virtual y borrar el dispositivo flash, el dispositivo estará disponible para otras operaciones.

Configuración avanzada de flash virtual

Se pueden cambiar las opciones avanzadas de flash virtual.

Procedimiento

- 1 En vSphere Web Client, desplácese hasta el host.
- 2 Haga clic en la pestaña **Manage** (Administrar) y en **Settings** (Configuración).
- 3 En **System** (Sistema), haga clic en **Advanced System Settings** (Configuración avanzada del sistema).

- 4 Seleccione la configuración que desea cambiar y haga clic en el botón **Edit** (Editar).

Opción	Descripción
VFLASH.VFlashResourceUsageThreshold	El sistema activa la alarma <code>Host vFlash resource usage</code> cuando la utilización de un recurso de flash virtual supera el umbral. El umbral predeterminado es del 80 %. Puede cambiar este umbral a un valor apropiado. La alarma se borra automáticamente cuando la utilización del recurso flash virtual cae por debajo del umbral.
VFLASH.MaxResourceGBForVmCache	Un host ESXi almacena metadatos de Flash Read Cache en la memoria RAM. El límite predeterminado del tamaño total de la memoria caché de la máquina virtual en el host es de 2 TB. Esta opción se puede volver a configurar. Es necesario reiniciar el host para que la nueva configuración se aplique.

- 5 Haga clic en **OK** (Aceptar).

Configurar la memoria caché de intercambio del host

Los hosts ESXi pueden utilizar una parte de una entidad de almacenamiento respaldada por flash como memoria caché de intercambio compartida por todas las máquinas virtuales.

La memoria caché en el nivel del host está compuesta por archivos en un disco de latencia baja que ESXi utiliza como memoria caché con reescritura para archivos de intercambio de máquinas virtuales. Todas las máquinas virtuales que se ejecutan en el host comparten la memoria caché. El intercambio en el nivel del host de páginas de máquinas virtuales aprovecha al máximo el espacio de dispositivos flash potencialmente limitado.

Según el entorno y el paquete de licencias, están disponibles los siguientes métodos de configuración de la memoria caché de intercambio de nivel en el nivel del host. Los dos métodos ofrecen resultados similares.

- Es posible crear un almacén de datos de VMFS en un dispositivo flash y, posteriormente, utilizar el almacén de datos con el fin de asignar espacio para la memoria caché del host. El host reserva una cierta cantidad de espacio para intercambiar con la memoria caché del host.
- Si se dispone de una licencia de vSphere adecuada que permite configurar y administrar un recurso flash virtual, se puede utilizar el recurso para configurar la memoria caché de intercambio en el host. La memoria caché de intercambio del host se asigna desde una porción del recurso flash virtual.

Configurar la memoria caché del host con un almacén de datos de VMFS

Active la capacidad del host para cambiar a la memoria caché del host. También puede cambiar el porcentaje de espacio asignado para la memoria caché del host.

Utilice esta tarea si no tiene una licencia adecuada que permita configurar y administrar un recurso flash virtual. Si tiene una licencia, utilice el recurso flash virtual para la configuración de la memoria caché del host.

Requisitos previos

Cree un almacén de datos de VMFS respaldado por flash. Consulte [Crear un almacén de datos de VMFS](#).

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Host Cache Configuration** (Configuración de la memoria caché del host).
- 4 Seleccione el almacén de datos en la lista y haga clic en el icono **Allocate space for host cache** (Asignar espacio para la memoria caché del host).
- 5 Para habilitar la memoria caché de intercambio del host en cada almacén de datos, active casilla **Allocate space for host cache** (Asignar espacio para la memoria caché del host).

De manera predeterminada, se asigna el espacio máximo disponible para la memoria caché del host.
- 6 (opcional) Para cambiar el tamaño de la memoria caché del host, seleccione **Custom size** (Personalizar tamaño) y realice los ajustes correspondientes.
- 7 Haga clic en **OK** (Aceptar).

Configurar la memoria caché de intercambio del host con un recurso flash virtual

Puede reservar una cierta cantidad de recursos flash virtuales para la memoria caché de intercambio del host.

Requisitos previos

Configure un recurso flash virtual. [Configurar un recurso flash virtual](#).

Nota Si el host ESXi configurado con flash virtual está en modo de mantenimiento, no puede agregar o modificar la memoria caché de intercambio del host. Primero debe salir del modo de mantenimiento en el host para configurar la memoria caché de intercambio del host.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En Virtual Flash (Flash virtual), seleccione **Virtual Flash Host Swap Cache Configuration** (Configuración de la memoria caché de intercambio del host con flash virtual) y haga clic en **Edit** (Editar).
- 4 Active la casilla **Enable virtual flash host swap cache** (Habilitar memoria caché de intercambio del host con flash virtual).

- 5 Especifique la cantidad de recurso flash virtual que desea reservar para la memoria caché de intercambio del host.
- 6 Haga clic en **OK** (Aceptar).

Acerca de VMware vSphere Flash Read Cache

15

Flash Read Cache™ permite acelerar el rendimiento de las máquinas virtuales a través de la utilización de dispositivos flash residentes como memoria caché.

Flash Read Cache se puede reservar para cualquier disco virtual individual. Flash Read Cache se crea solo cuando se enciende una máquina virtual, y se descarta cuando esa máquina se suspende o se apaga. Al migrar una máquina virtual, es posible migrar la memoria caché. De forma predeterminada, la memoria caché se migra si el módulo flash virtual en los hosts de origen y de destino son compatibles. Si no se migra la memoria caché, esta se recrea en el host de destino. Es posible cambiar el tamaño de la memoria caché mientras la máquina virtual está encendida. En esta instancia, se descarta la memoria caché existente y se crea una nueva memoria caché de escritura intermedia, lo que produce un período de transición de la memoria caché. La ventaja de crear una memoria caché nueva es que su tamaño puede coincidir mejor con los datos activos de la aplicación.

Flash Read Cache admite memoria de almacenamiento en caché de escritura intermedia o de lectura. No se admite memoria caché con reescritura ni almacenamiento en caché de escritura. Las lecturas de datos se realizan desde la memoria caché, si están presentes. Las escrituras de datos se envían al almacenamiento de respaldo, como una SAN o una NAS. Todos los datos que se leen desde o se escriben en el almacenamiento de respaldo se almacenan incondicionalmente en la memoria caché.

Flash Read Cache no admite RDM en términos de compatibilidad física. Los RDM de compatibilidad virtual son compatibles con Flash Read Cache.

Para obtener más información sobre Flash Read Cache, mire el vídeo.



Configuración de vSphere Flash Read Cache

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_pbinee4w/uiConfId/49694343/)

Nota No todas las cargas de trabajo se benefician con Flash Read Cache. El aumento del rendimiento depende del patrón de carga de trabajo y del tamaño del conjunto de trabajo. Las cargas de trabajo de lectura intensiva con conjuntos de trabajo que caben en la memoria caché pueden aprovechar la configuración de Flash Read Cache como un beneficio. Al configurar Flash Read Cache para las cargas de trabajo de lectura intensiva, hay recursos adicionales de E/S disponibles en el almacenamiento compartido, lo que puede provocar un aumento del rendimiento de otras cargas de trabajo aunque no estén configuradas para utilizar Flash Read Cache.

Este capítulo incluye los siguientes temas:

- [Compatibilidad con DRS para Flash Read Cache](#)
- [Compatibilidad de vSphere High Availability con Flash Read Cache](#)
- [Configurar Flash Read Cache para una máquina virtual](#)
- [Migrar máquinas virtuales con Flash Read Cache](#)

Compatibilidad con DRS para Flash Read Cache

DRS es compatible con flash virtual como recurso.

DRS administra máquinas virtuales con reservas de Flash Read Cache. Cada vez que se ejecuta DRS, muestra la capacidad de flash virtual disponible informada por el host ESXi. Cada host admite un recurso de flash virtual. DRS selecciona un host que tenga la capacidad de flash virtual suficiente para iniciar una máquina virtual. DRS trata las máquinas virtuales activas con Flash Read Cache como software afín a su host actual, y las mueve solo por motivos obligatorios o necesarios para corregir la sobreutilización del host.

Compatibilidad de vSphere High Availability con Flash Read Cache

Flash Read Cache es compatible con High Availability (HA).

Cuando vSphere HA reinicia una máquina virtual configurada con Flash Read Cache, la máquina virtual se reinicia en un host del clúster donde se cumplen las reservas de Flash Read Cache, CPU, memoria y sobrecarga. vSphere HA no reiniciará una máquina virtual si la memoria flash no reservada es insuficiente para cumplir la reserva de flash virtual. Si el host de destino no tiene suficientes recursos de flash virtual disponibles, debe volver a configurar manualmente una máquina virtual para reducir o descartar Flash Read Cache.

Configurar Flash Read Cache para una máquina virtual

Puede configurar Flash Read Cache para una máquina virtual compatible con ESXi 5.5 o posterior.

La activación de Flash Read Cache permite especificar una reserva de tamaño de memoria caché y de tamaño de bloque.

El tamaño de bloque es la cantidad mínima de bytes contiguos que pueden almacenarse en la memoria caché. Este tamaño de bloque puede ser mayor que el tamaño de bloque de disco nominal de 512 bytes, entre 4 KB y 1024 KB. Si un sistema operativo invitado escribe un solo bloque de disco de 512 bytes, se almacenarán en caché los bytes de tamaño de bloque de memoria caché adyacentes. No se debe confundir el tamaño de bloque de memoria caché con el tamaño de bloque de disco.

La reserva es un tamaño de reserva de los bloques de memoria caché. Hay una cantidad mínima de 256 bloques de memoria caché. Si el tamaño de bloque de memoria caché es de 1 MB, el tamaño de memoria caché mínimo es de 256 MB. Si el tamaño de bloque de memoria caché es de 4 KB, el tamaño de memoria caché mínimo es de 1 MB.

Para obtener más información sobre las directrices de tamaño, busque el informe técnico *Performance of vSphere Flash Read Cache in VMware vSphere* (Rendimiento de vSphere Flash Read Cache en VMware vSphere) en el sitio web de VMware.

Requisitos previos

- Configure un recurso flash virtual.
- Compruebe que la máquina virtual sea compatible con ESXi 5.5 o posterior.

Procedimiento

- 1 Para buscar una máquina virtual, seleccione un centro de datos, una carpeta, un clúster, un grupo de recursos, un host o una vApp.
- 2 Haga clic en la pestaña **Related Objects** (Objetos relacionados) y en **Virtual Machines** (Máquinas virtuales).
- 3 Haga clic con el botón derecho en la máquina virtual y seleccione **Edit Settings** (Editar configuración).
- 4 En la pestaña **Virtual Hardware** (Hardware virtual), expanda la opción **Hard disk** (Disco duro) para ver las opciones del disco.
- 5 Para habilitar Flash Read Cache en la máquina virtual, introduzca un valor en el cuadro de texto **Virtual Flash Read Cache** (Flash Read Cache virtual).
- 6 Haga clic en **Advanced** (Opciones avanzadas) para especificar los siguientes parámetros.

Opción	Descripción
Reservation (Reserva)	Seleccione una reserva de tamaño de memoria caché.
Block Size (Tamaño de bloque)	Seleccione un tamaño de bloque.

- 7 Haga clic en **OK** (Aceptar).

Migrar máquinas virtuales con Flash Read Cache

Cuando se migra una máquina virtual encendida de un host a otro, es posible especificar si se migrará el contenido de Flash Read Cache junto con los discos virtuales.

Requisitos previos

Si planea migrar el contenido de Flash Read Cache, configure un recurso de flash virtual suficiente en el host de destino.

Procedimiento

- 1 Haga clic con el botón derecho en la máquina virtual en ejecución y seleccione **Migrar**.
- 2 Especifique el tipo de migración.

Opción	Descripción
Cambiar solo recurso informático	Migra las máquinas virtuales a otro host o clúster.
Cambiar recurso informático y almacenamiento	Migra las máquinas virtuales a un clúster o un host específico y su almacenamiento a un clúster de almacenes de datos o un almacén de datos específico.

- 3 Seleccione el host de destino y haga clic en **Siguiente**.
- 4 Especifique una configuración de migración para todos los discos virtuales configurados con Flash Read Cache virtual. Este parámetro de migración no se muestra si no se cambia el host y solo se cambia el almacén de datos.

Configuración de migración de Flash Read Cache	Descripción
Migrar siempre el contenido de la memoria caché	La migración de máquina virtual continúa solo si se puede migrar todo el contenido de la memoria caché al host de destino. Esta opción es útil cuando la memoria caché es pequeña o el tamaño de la memoria caché es similar a los datos activos de la aplicación.
No migrar el contenido de la memoria caché	Elimina la memoria caché de escritura inmediata. La memoria caché se vuelve a crear en el host de destino. Esta opción es útil cuando el tamaño de la memoria caché es grande o mayor que los datos activos de la aplicación.

- 5 Si hay varios discos virtuales con Flash Read Cache, se puede ajustar la configuración de migración de cada disco individual.
 - a Haga clic en **Opciones avanzadas**.
 - b Seleccione un disco virtual cuya configuración de migración desee modificar.
 - c En el menú desplegable de la columna **Configuración de migración de Flash Read Cache virtual**, seleccione la opción que corresponda.
- 6 Complete la configuración de migración y haga clic en **Finalizar**.

Pasos siguientes

Para comprobar que la migración haya finalizado correctamente, consulte la pestaña **Resumen** de la máquina virtual:

- Compruebe que en la pestaña se muestre la dirección IP correcta del host de destino.
- Compruebe que en el panel Hardware de máquina virtual se muestre la información correcta de Flash Read Cache virtual para cada disco virtual.

Trabajar con almacenes de datos

16

Los almacenes de datos son contenedores lógicos, de manera análoga a los sistemas de archivos, que ocultan aspectos específicos de almacenamiento físico y ofrecen un modelo uniforme para almacenar archivos de máquinas virtuales. Los almacenes de datos también pueden utilizarse para almacenar imágenes ISO, plantillas de máquinas virtuales e imágenes de disquete.

Según el almacenamiento que se utilice, los almacenes de datos pueden ser de los siguientes tipos:

- Almacenes de datos de VMFS que están respaldados por el formato Virtual Machine File System. Consulte [Descripción de los almacenes de datos de VMFS](#).
- Almacenes de datos de NFS que están respaldados por el formato Network File System (NFS). Consulte [Descripción de los almacenes de datos de Network File System](#).
- Almacenes de datos de Virtual SAN. Consulte la documentación de *Administración de VMware Virtual SAN*.
- Almacenes de datos de Virtual Volumes. Consulte [Capítulo 19 Trabajar con Virtual Volumes](#).

Una vez creados los almacenes de datos, se pueden realizar varias operaciones administrativas en ellos. Ciertas operaciones, como el cambio de nombre de los almacenes de datos, están disponibles para todos los tipos de almacenes de datos. Por otro lado, hay otras que se aplican a tipos específicos de almacenes de datos.

También se pueden organizar almacenes de datos de diferentes formas. Por ejemplo, agrupándolos en carpetas de acuerdo con las prácticas de negocios. Así es posible asignar en el mismo momento los mismos permisos y las mismas alarmas en los almacenes de datos del grupo.

También se pueden agregar almacenes de datos a los clústeres de almacenes de datos. Un clúster de almacenes de datos es una colección de almacenes de datos con recursos compartidos y una interfaz de administración compartida. Cuando crea un clúster de almacenes de datos, puede usar Storage DRS para administrar recursos de almacenamiento. Para obtener información sobre los clústeres de almacenes de datos, consulte la documentación de *Administración de recursos de vSphere*.

Este capítulo incluye los siguientes temas:

- [Descripción de los almacenes de datos de VMFS](#)
- [Descripción de los almacenes de datos de Network File System](#)

- Crear almacenes de datos
- Administrar almacenes de datos de VMFS duplicados
- Actualizar los almacenes de datos de VMFS
- Aumentar la capacidad de un almacén de datos de VMFS
- Operaciones administrativas para almacenes de datos
- Configurar reflejo de discos dinámico
- Recopilar información de diagnóstico para hosts ESXi en un dispositivo de almacenamiento
- Comprobar la coherencia de los metadatos con VOMA
- Configurar la memoria caché de bloque de puntero de VMFS

Descripción de los almacenes de datos de VMFS

Para almacenar discos virtuales, ESXi utiliza almacenes de datos, que son contenedores lógicos que ocultan los aspectos específicos del almacenamiento físico de las máquinas virtuales y ofrecen un modelo uniforme para almacenar archivos de máquinas virtuales. Los almacenes de datos que implementa en dispositivos de almacenamiento en bloque utilizan el formato de vSphere VMFS, un formato de sistema de archivos de alto rendimiento especial que está optimizado para almacenar máquinas virtuales.

Se han publicado varias versiones del sistema de archivos VMFS desde su creación. En la siguiente tabla se muestran las relaciones entre los hosts y las versiones de VMFS.

Tabla 16-1. Acceso del host a la versión de VMFS

VMFS	Host ESX/ESXi 3.x	Host ESX/ESXi 4.x	Host ESXi 5.x	Host ESXi 6.x
VMFS2	RO	RO	N	N
VMFS3	RW	RW	RW	RW
				Nota Puede seguir usando almacenes de datos VMFS3 existentes, pero no puede crear nuevos. Si tiene almacenes de datos VMFS3 existentes, actualícelos a VMFS5.
VMFS5	N	N	RW	RW

- RW: compatibilidad total con lectura y escritura. Puede crear y encender máquinas virtuales.
- RO: compatibilidad solo de lectura. No puede crear ni encender máquinas virtuales.

- N: Sin acceso. Los hosts ESXi 5.x y posteriores no son compatibles con VMFS2. Si el almacén de datos se formateó con VMFS2, en primer lugar debe actualizar el almacén de datos a VMFS3 con hosts heredados.

Use vSphere Web Client para configurar un almacén de datos de VMFS por adelantado en un dispositivo de almacenamiento en bloque que el host ESXi detecte. Un almacén de datos de VMFS puede extenderse para abarcar varias extensiones de almacenamiento físico, incluidas LUN de SAN y almacenamiento local. Esta característica permite agrupar almacenamiento y brinda flexibilidad para crear el almacén de datos necesario para las máquinas virtuales.

Nota El agrupamiento de hardware compatible con ATS crea un almacén de datos de VMFS extendido que puede usar el mecanismo de bloqueo solo con ATS. Si alguno de los dispositivos no es compatible con ATS, el almacén de datos no podrá ser solo de ATS, sino que utilizará el bloqueo ATS+SCSI.

Puede aumentar la capacidad de un almacén de datos mientras las máquinas virtuales se están ejecutando en el almacén de datos. Esta capacidad permite agregar espacio nuevo a los almacenes de datos de VMFS a medida que la máquina virtual lo requiera. VMFS está diseñado para acceso simultáneo desde varias máquinas físicas, y aplica los controles de acceso adecuados en archivos de máquinas virtuales.

Características de los almacenes de datos VMFS5

VMFS5 ofrece muchas mejoras de escalabilidad y rendimiento.

VMFS5 tiene las siguientes características:

- Dispositivos de almacenamiento superiores a 2 TB para cada extensión de VMFS5.
- Admite máquinas virtuales con discos virtuales de gran capacidad o discos superiores a 2 TB.
- Mayores límites de recursos como descriptores de archivos.
- Tamaño estándar de bloque del sistema de archivos de 1 MB y compatibilidad con discos virtuales de 2 TB.
- Tamaño de disco superior a 2 TB para RDM.
- Compatibilidad con archivos pequeños de 1 KB.
- Capacidad de abrir cualquier archivo ubicado en un almacén de datos VMFS5 en modo compartido por un máximo de 32 hosts.
- Mejoras de escalabilidad en dispositivos de almacenamiento compatibles con la aceleración de hardware. Para obtener información, consulte [Capítulo 23 Aceleración de hardware de almacenamiento](#).
- Uso predeterminado de mecanismos de bloqueo solo con ATS en dispositivos de almacenamiento compatibles con ATS. Para obtener información sobre el bloqueo solo con ATS y cómo actualizar a ese tipo de bloqueo, consulte [Mecanismos de bloqueo de VMFS](#).

- Capacidad de recuperar espacio de almacenamiento físico en dispositivos de almacenamiento de aprovisionamiento fino. Para obtener información, consulte [Aprovisionamiento fino de matrices y almacenes de datos de VMFS](#).
- Proceso de actualización en línea que actualiza los almacenes de datos existentes sin interrumpir los hosts o las máquinas virtuales actualmente en ejecución. Para obtener información, consulte [Actualizar los almacenes de datos de VMFS](#).

Para obtener información sobre las limitaciones de tamaño de bloques de un almacén de datos de VMFS, consulte el artículo de la base de conocimientos de VMware en <http://kb.vmware.com/kb/1003565>.

Almacenes de datos de VMFS y formatos de disco de almacenamiento

Los dispositivos de almacenamiento compatibles con el host pueden usar el formato de registro maestro de arranque (MBR) o el formato de tabla de particiones GUID (GPT).

Si crea un almacén de datos VMFS5 nuevo, el dispositivo adoptará el formato GPT. El formato GPT permite crear almacenes de datos superiores a 2 TB y de 64 TB como máximo para una sola extensión.

Los almacenes de datos VMFS3 siguen utilizando el formato MBR para sus dispositivos de almacenamiento. Tenga en cuenta los siguientes aspectos al trabajar con almacenes de datos VMFS3:

- Para almacenes de datos VMFS3, el límite de 2 TB se sigue aplicando incluso si el dispositivo de almacenamiento tiene una capacidad superior. Para poder usar todo el espacio de almacenamiento, actualice el almacén de datos VMFS3 a VMFS5. La conversión del formato MBR a GPT sucederá solo después de expandir el almacén de datos a un tamaño superior a 2 TB.
- Cuando actualiza un almacén de datos VMFS3 a VMFS5, el almacén de datos utilizará el formato MBR. La conversión a GPT se produce solo después de expandir el almacén de datos a un tamaño mayor que 2 TB.
- Al actualizar un almacén de datos VMFS3, elimine del dispositivo de almacenamiento todas las particiones que ESXi no reconozca, por ejemplo, particiones que utilicen los formatos EXT2 o EXT3. En caso contrario, el host no podrá formatear el dispositivo con GPT y la actualización generará un error.
- No puede expandir un almacén de datos VMFS3 en dispositivos que cuenten con el formato de partición GPT.

Almacenes de datos de VMFS como repositorios

ESXi puede dar formato a los dispositivos de almacenamiento basados en SCSI como almacenes de datos de VMFS. Los almacenes de datos de VMFS actúan principalmente como repositorios de máquinas virtuales.

Con VMFS5, se pueden tener hasta 256 almacenes de datos de VMFS por host, con un tamaño máximo de 64 TB. El tamaño mínimo requerido para un almacén de datos de VMFS es 1,3 GB; sin embargo, el tamaño mínimo recomendado es de 2 GB.

Nota Asimismo, siempre se debe tener un solo almacén de datos de VMFS para cada LUN.

Es posible almacenar varias máquinas virtuales en el mismo almacén de datos de VMFS. Cada máquina virtual, encapsulada en un conjunto de archivos, ocupa un único directorio separado. En el sistema operativo dentro de la máquina virtual, VMFS preserva la semántica del sistema de archivos interno, que garantiza el comportamiento correcto de la aplicación y la integridad de los datos de las aplicaciones que se ejecutan en las máquinas virtuales.

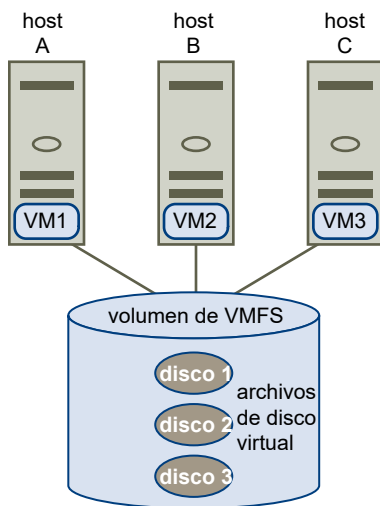
Cuando se ejecutan varias máquinas virtuales, VMFS proporciona mecanismos de bloqueo específicos para los archivos de máquina virtual, a fin de que las máquinas puedan operar de forma segura en un entorno de SAN en el que varios hosts ESXi comparten el mismo almacén de datos de VMFS.

Además de las máquinas virtuales, el almacén de datos de VMFS puede almacenar otros archivos, como plantillas de máquina virtual e imágenes ISO.

Compartir un almacén de datos de VMFS entre hosts

Como sistema de archivos de clúster, VMFS permite que varios hosts ESXi accedan a los mismos almacenes de datos de VMFS de manera simultánea.

Figura 16-1. Compartir un almacén de datos de VMFS entre hosts



Para obtener información sobre la cantidad máxima de hosts que pueden conectarse a un solo almacén de datos de VMFS, consulte el documento de *Valores máximos de configuración*.

Para impedir que varios hosts accedan a la misma máquina virtual a la vez, VMFS ofrece bloqueo en disco.

Compartir el volumen VMFS entre varios hosts ofrece varias ventajas, por ejemplo:

- Se pueden utilizar VMware Distributed Resource Scheduling (DRS) y VMware High Availability (HA).

Se pueden distribuir máquinas virtuales en diferentes servidores físicos. Esto significa que se ejecuta una combinación de máquinas virtuales en cada servidor para que no todos experimenten una demanda alta en la misma área al mismo tiempo. Si un servidor genera un error, es posible reiniciar las máquinas virtuales en otro servidor físico. Si hay un error, se activa el bloqueo en disco de cada máquina virtual. Para obtener más información sobre VMware DRS, consulte la documentación de *Administración de recursos de vSphere*. Para obtener información sobre VMware HA, consulte la documentación de *Disponibilidad de vSphere*.

- vMotion se puede utilizar para migrar máquinas virtuales en ejecución de un servidor físico al otro. Para obtener información sobre la migración de máquinas virtuales, consulte la documentación de *Administración de vCenter Server y hosts*.

Para crear un almacén de datos compartido, móntelo en los hosts ESXi que requieran acceso al almacén de datos. Consulte [Montar almacenes de datos](#).

Actualizaciones de metadatos de VMFS

Un almacén de datos de VMFS incluye archivos, directorios, enlaces simbólicos, archivos de descriptores RDM, etc. de máquinas virtuales. El almacén de datos también mantiene una vista coherente de toda la información de asignación de estos objetos. Esta información de asignación se denomina metadatos.

Los metadatos se actualizan cada vez que se realizan operaciones de administración de almacenes de datos o máquinas virtuales. Algunos ejemplos de operaciones que requieren actualizaciones de metadatos son los siguientes:

- Creación, ampliación o bloqueo de un archivo de máquina virtual
- Cambio de los atributos de un archivo
- Encendido o apagado de una máquina virtual
- Creación o eliminación de un almacén de datos de VMFS
- Expansión de un almacén de datos de VMFS
- Creación de una plantilla
- Implementación de una máquina virtual desde una plantilla
- Migración de una máquina virtual con vMotion

Cuando los cambios en los metadatos se realizan en un entorno de almacenamiento compartido, VMFS utiliza mecanismos de bloqueo especiales para proteger sus datos y evitar que varios hosts escriban en los metadatos de manera simultánea.

Mecanismos de bloqueo de VMFS

En un entorno de almacenamiento compartido, cuando varios hosts acceden al mismo almacén de datos de VMFS, se utilizan mecanismos de bloqueo específicos. Estos mecanismos de bloqueo evitan que varios hosts escriban simultáneamente en los metadatos y garantiza que no se dañen los datos.

Según la configuración y el tipo de almacenamiento subyacente, un almacén de datos de VMFS puede usar exclusivamente la prueba atómica y configurar un mecanismo de bloqueo (solo ATS), o usar una combinación de reservas ATS y SCSI (ATS+SCSI).

Mecanismo de solo ATS

En el caso de los dispositivos de almacenamiento que admiten especificaciones de VAAI basadas en estándares T10, VMFS proporciona bloqueo de ATS, también denominado bloqueo asistido por hardware. El algoritmo de ATS admite el bloqueo discreto por sector de disco. Todos los almacenes de datos VMFS5 con formato nuevo usan el mecanismo de solo ATS si el almacenamiento subyacente lo admite, y nunca usan reservas SCSI.

Cuando crea un almacén de datos multiextensión que usa ATS, vCenter Server filtra los dispositivos que no son ATS. Este filtrado permite usar solo aquellos dispositivos que admiten ATS primitiva.

En ciertos casos, es posible que deba apagar la configuración solo ATS para un almacén de datos VMFS5. Para obtener información, consulte [Cambiar el mecanismo de bloqueo a ATS+SCSI](#).

Mecanismo ATS+SCSI

Un almacén de datos de VMFS que admite el mecanismo ATS+SCSI está configurado para usar ATS e intenta usarlo cuando es posible. Si ATS presenta errores, el almacén de datos de VMFS se revierte a las reservas SCSI. A diferencia del bloqueo de ATS, las reservas SCSI bloquean un dispositivo de almacenamiento completo mientras se realiza una operación que requiere protección de metadatos. Una vez completada la operación, VMFS libera la reserva y las otras operaciones pueden continuar.

Los almacenes de datos que usan el mecanismo ATS+SCSI incluyen almacenes de datos VMFS5 que se actualizaron desde VMFS3. Además, los almacenes de datos VMFS5 nuevos en dispositivos de almacenamiento que no admiten ATS usan el mecanismo ATS+SCSI.

Si el almacén de datos de VMFS se revierte a las reservas de SCSI, es posible que note una degradación en el rendimiento provocada por reservas SCSI excesivas. Para obtener información sobre cómo reducir las reservas SCSI, consulte la documentación *Solución de problemas de vSphere*.

Mostrar información de bloqueo de VMFS

Utilice el comando `esxcli` para obtener información sobre el mecanismo de bloqueo que utiliza un almacén de datos de VMFS.

En el procedimiento, **--server=server_name** especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Para mostrar información relacionada con mecanismos de bloqueo de VMFS, ejecute el siguiente comando:

```
esxcli --server=server_name storage vmfs lockmode list.
```

Resultados

La tabla enumera elementos que podría incluir la salida del comando.

Tabla 16-2. Información de bloqueo de VMFS

Campos	Valores	Descripciones
Locking Mode (Modo de bloqueo)		Indica la configuración de bloqueo del almacén de datos.
	ATS-only (Solo con ATS)	El almacén de datos está configurado para utilizar el mecanismo de bloqueo solo con ATS.
	ATS+SCSI	El almacén de datos está configurado para utilizar ATS, pero puede revertir a SCSI si ATS genera errores o no es compatible.
	ATS upgrade pending (Actualización de ATS pendiente)	El almacén de datos está en el proceso de una actualización en línea al mecanismo de bloqueo solo con ATS.
	ATS downgrade pending (Degradación de ATS pendiente)	El almacén de datos está en el proceso de una degradación en línea al mecanismo de bloqueo de ATS+SCSI.
ATS Compatible (Compatible con ATS)		Indica si el almacén de datos puede configurarse para el mecanismo de bloqueo solo con ATS.
ATS Upgrade Modes (Modos de actualización de ATS)		Indica el tipo de actualización compatible con el almacén de datos.
	None (Ninguno)	El almacén de datos no es compatible con el mecanismo de bloqueo solo con ATS.

Tabla 16-2. Información de bloqueo de VMFS (continuación)

Campos	Valores	Descripciones
	Online (En línea)	El almacén de datos puede utilizarse durante su actualización al mecanismo de bloqueo solo con ATS.
	Offline (Sin conexión)	El almacén de datos no puede utilizarse durante su actualización al mecanismo de bloqueo solo con ATS.
ATS Incompatibility Reason (Motivo de incompatibilidad con ATS)		Si el almacén de datos no es compatible con el mecanismo de bloqueo de solo ATS, indica el motivo de la incompatibilidad.

Cambiar bloqueo de VMFS al modo de solo con ATS

Si los almacenes de datos VMFS5 utilizan el mecanismo de bloqueo ATS+SCSI, puede cambiarlo al modo de bloqueo solo con ATS.

Por lo general, los almacenes de datos VMFS5 que se actualizaron de VMFS3 utilizan el mecanismo de bloqueo ATS+SCSI. Si los almacenes de datos se implementan en hardware compatible con ATS, por lo general, cumplen los requisitos para actualizarse al modo de bloqueo solo con ATS. Según el entorno de vSphere, se puede utilizar uno de los siguientes modos de actualización:

- La actualización en línea a bloqueo solo con ATS está disponible para la mayoría de los almacenes de datos VMFS5 de una sola extensión. Mientras se realiza la actualización en línea en uno de los hosts, otros hosts pueden seguir utilizando el almacén de datos.
- La actualización sin conexión a bloqueo solo con ATS debe utilizarse en almacenes de datos VMFS5 que abarcan varias extensiones físicas. Los almacenes de datos compuestos por varias extensiones no cumplen los requisitos para la actualización en línea. Estos almacenes de datos requieren que ningún host utilice activamente los almacenes de datos en el momento de la solicitud de actualización.

Procedimiento

1 Preparar una actualización a bloqueo solo con ATS

Debe seguir varios pasos para preparar el entorno para una actualización en línea o sin conexión al bloqueo solo con ATS.

2 Actualizar mecanismo de bloqueo a solo con ATS

Si un almacén de datos de VMFS es compatible solo con ATS, es posible actualizar su mecanismo de bloqueo de ATS+SCSI a solo con ATS.

Preparar una actualización a bloqueo solo con ATS

Debe seguir varios pasos para preparar el entorno para una actualización en línea o sin conexión al bloqueo solo con ATS.

Procedimiento

- 1 Actualice todos los hosts que acceden al almacén de datos VMFS5 a la versión más nueva de vSphere.
- 2 Para determinar si el almacén de datos cumple con los requisitos para una actualización de su mecanismo de bloqueo actual, ejecute el comando `esxcli storage vmfs lockmode list`.

Los siguientes campos de salida a modo de ejemplo indican que el almacén de datos cumple con los requisitos para la actualización. Además, muestran el mecanismo de bloqueo actual y un modo de actualización disponible para el almacén de datos.

```
Locking Mode   ATS Compatible   ATS Upgrade Modes
-----
ATS+SCSI      true             Online or Offline
```

- 3 Según el modo de actualización disponible para el almacén de datos, realice una de las siguientes acciones:

Modo de actualización	Acción
Online (En línea)	Compruebe que todos los hosts tengan una conectividad de almacenamiento coherente con el almacén de datos de VMFS.
Offline (Sin conexión)	Compruebe que ningún host esté utilizando activamente el almacén de datos.

Actualizar mecanismo de bloqueo a solo con ATS

Si un almacén de datos de VMFS es compatible solo con ATS, es posible actualizar su mecanismo de bloqueo de ATS+SCSI a solo con ATS.

La mayoría de los almacenes de datos que no expanden varias extensiones cumplen con los requisitos de una actualización en línea. Mientras se realiza la actualización en línea en uno de los hosts ESXi, otros hosts pueden seguir utilizando el almacén de datos. La actualización en línea se completa solo después de que todos los hosts hayan cerrado el almacén de datos.

Requisitos previos

Si planea completar la actualización del mecanismo de bloqueo colocando el almacén de datos en modo de mantenimiento, deshabilite Storage DRS. Este requisito previo se aplica solo a una actualización en línea.

Procedimiento

- 1 Para realizar una actualización del mecanismo de bloqueo, ejecute el siguiente comando:

```
esxcli storage vmfs lockmode set -a|--ats -l|--volume-label= VMFS label -u|--volume-uuid= VMFS UUID.
```

2 Para una actualización en línea, se requieren pasos adicionales.

- a Cierre el almacén de datos en todos los hosts que tengan acceso al almacén de datos, de modo tal que los hosts puedan reconocer el cambio.

Puede utilizar uno de los siguientes métodos:

- Desmontar y montar el almacén de datos.
- Colocar el almacén de datos en modo de mantenimiento y salir del modo de mantenimiento.

- b Compruebe que el estado de Locking Mode (Modo de bloqueo) del almacén de datos haya cambiado a ATS-only (Solo con ATS). Para hacerlo, ejecute el comando siguiente:

```
esxcli storage vmfs lockmode list
```

- c Si el modo de bloqueo muestra cualquier otro estado (por ejemplo, ATS UPGRADE PENDING [Actualización de ATS pendiente]), compruebe qué host aún no procesó la actualización. Para ello, ejecute el comando siguiente:

```
esxcli storage vmfs host list
```

Cambiar el mecanismo de bloqueo a ATS+SCSI

Al crear un almacén de datos VMFS5 en un dispositivo que admite el bloqueo de prueba y configuración atómica (ATS), se configura el almacén de datos para que utilice el mecanismo de bloqueo solo con ATS. En ciertas circunstancias, es posible que deba degradar el bloqueo solo con ATS a ATS+SCSI.

Es posible que deba pasar al mecanismo de bloqueo ATS+SCSI cuando, por ejemplo, el dispositivo de almacenamiento se degrade o las actualizaciones de firmware generen errores y el dispositivo ya no admita ATS.

El proceso de degradación es similar a la actualización solo a ATS. Al igual que con la actualización, según la configuración de almacenamiento, podrá realizar la degradación en modo en línea o sin conexión.

Procedimiento

- 1 Para cambiar el mecanismo de bloqueo a ATS+SCSI, ejecute el siguiente comando:

```
esxcli storage vmfs lockmode set -s|--scsi -l|--volume-label= VMFS label
-u|--volume-uuid= VMFS UUID.
```

- 2 Para el modo en línea, cierre el almacén de datos en todos los hosts que tengan acceso al almacén de datos para que los hosts puedan reconocer el cambio.

Descripción de los almacenes de datos de Network File System

Un cliente NFS integrado en ESXi utiliza el protocolo Network File System (NFS) mediante TCP/IP para acceder a un volumen NFS designado ubicado en un servidor NAS. El host ESXi puede

montar el volumen y utilizarlo para sus necesidades de almacenamiento. vSphere es compatible con las versiones 3 y 4.1 del protocolo NFS.

En general, un administrador de almacenamiento crea el directorio o el volumen NFS, y este se exporta del servidor NFS. No es necesario que al volumen NFS se le dé formato con un sistema de archivos local, como VMFS. Es posible montar el volumen directamente en los hosts ESXi y usarlo para almacenar y arrancar máquinas virtuales del mismo modo en que se utilizan los almacenes de datos de VMFS.

Además de almacenar discos virtuales en almacenes de datos de NFS, se puede utilizar NFS como un repositorio central de imágenes ISO, plantillas de máquina virtual, etc. Si utiliza el almacén de datos para imágenes ISO, puede conectar el dispositivo de CD-ROM de la máquina virtual a un archivo ISO en el almacén de datos e instalar un sistema operativo invitado desde el archivo ISO.

ESXi es compatible con las siguientes capacidades de almacenamiento en la mayoría de los volúmenes NFS:

- vMotion y Storage vMotion
- High Availability (HA) y Distributed Resource Scheduler (DRS)
- Fault Tolerance (FT) y Host Profiles

Nota NFS 4.1 no es compatible con Fault Tolerance heredada.

- Imágenes ISO, que se presentan como CD-ROM a las máquinas virtuales
- Instantáneas de la máquina virtual
- Máquinas virtuales con discos virtuales de gran capacidad, o discos de más de 2 TB. Los discos virtuales creados en almacenes de datos de NFS son de aprovisionamiento fino de forma predeterminada, a menos que se utilice la aceleración de hardware que admite la operación Reserve Space (Reserva de espacio). NFS 4.1 no admite la aceleración de hardware. Para obtener información, consulte [Aceleración de hardware en dispositivos NAS](#).

Instrucciones y requisitos de almacenamiento NFS

Al utilizar el almacenamiento NFS, se deben seguir ciertas instrucciones de configuración, redes y almacenes de datos de NFS.

Instrucciones de configuración de servidores NFS

- Asegúrese de que los servidores NFS que use estén enumerados en *VMware HCL*. Utilice la versión correcta de firmware del servidor.
- Cuando configure el almacenamiento NFS, siga la recomendación del proveedor de almacenamiento.
- Asegúrese de que el volumen NFS se exporte mediante NFS por medio de TCP.

- Asegúrese de que el servidor NFS exporte un uso compartido determinado, como NFS 3 o NFS 4.1, pero que no proporcione ambas versiones del protocolo para el mismo uso compartido. El servidor debe implementar esta directiva porque ESXi no evita el montaje del mismo uso compartido a través de diferentes versiones de NFS.
- NFS 3 y la versión NFS 4.1 que no pertenece a Kerberos no admiten la funcionalidad de usuarios delegados que permite el acceso a volúmenes NFS mediante credenciales no raíz. Si usa NFS 3 o la versión NFS 4.1 que no pertenece a Kerberos, asegúrese de que todos los hosts tengan acceso de raíz al volumen. Los distintos proveedores de almacenamiento tienen diferentes métodos para habilitar esta funcionalidad, pero esto generalmente se hace en los servidores NAS mediante la opción `no_root_squash`. Si el servidor NAS no otorga acceso de raíz, es posible que aún se pueda montar el almacén de datos de NFS en el host. Sin embargo, no se podrán crear máquinas virtuales en el almacén de datos.
- Si el volumen NFS subyacente (en el que se almacenan los archivos) es de solo lectura, asegúrese de que el servidor NFS exporte el volumen como uso compartido de solo lectura o configure el volumen como un almacén de datos de solo lectura en el host ESXi. De lo contrario, el host considerará que el almacén de datos es de lectura y escritura, y posiblemente no podrá abrir los archivos.

Instrucciones para redes NFS

- Para la conectividad de red, el host requiere un adaptador de red estándar.
- ESXi admite conmutadores de red de Capa 2 y Capa 3. Si usa conmutadores de Capa 3, los hosts ESXi y las matrices de almacenamiento NFS deben estar en diferentes subredes y el conmutador de red debe controlar la información de enrutamiento.
- Se requiere un grupo de puertos VMkernel para el almacenamiento NFS. Puede crear un nuevo grupo de puertos VMkernel para almacenamiento IP en un conmutador virtual existente (vSwitch) o en un nuevo vSwitch una vez que esté configurado. El vSwitch puede ser un conmutador estándar de vSphere (VSS) o un conmutador distribuido de vSphere (VDS).
- Si usa varios puertos para el tráfico NFS, asegúrese de configurar correctamente los conmutadores virtuales y los conmutadores físicos. Para obtener información, consulte el documento *Redes de vSphere*.
- NFS 3 y NFS 4.1 que no pertenece a Kerberos admiten IPv4 e IPv6.

Instrucciones para almacenes de datos de NFS

- Para utilizar NFS 4.1, actualice el entorno de vSphere a la versión 6.x. No puede montar un almacén de datos NFS 4.1 en hosts que no admiten la versión 4.1.
- No se pueden utilizar diferentes versiones de NFS para montar el mismo almacén de datos. Los clientes de NFS 3 y NFS 4.1 no utilizan el mismo protocolo de bloqueo. Como resultado, si se accede a los mismos discos virtuales desde dos clientes no compatibles, se puede producir un comportamiento incorrecto y los datos pueden dañarse.
- Los almacenes de datos NFS 3 y NFS 4.1 pueden coexistir en el mismo host.

- vSphere no admite actualizaciones de almacenes de datos de la versión 3 a 4.1 de NFS.
- Al montar el mismo volumen NFS 3 en diferentes hosts, compruebe que los nombres de servidor y carpeta sean idénticos en todos los hosts. Si los nombres no coinciden, los hosts verán el mismo volumen NFS versión 3 como dos almacenes de datos diferentes. Este error puede provocar que características como vMotion no funcionen correctamente. Un ejemplo de esta discrepancia consiste en la introducción de `filer` como el nombre del servidor en un host y `filer.domain.com` en el otro. Esta instrucción no se aplica a la versión 4.1 de NFS.
- Si utiliza caracteres no ASCII para nombrar almacenes de datos y máquinas virtuales, asegúrese de que el servidor NFS subyacente ofrezca compatibilidad de internacionalización. Si el servidor no admite caracteres internacionales, use solo caracteres ASCII. De lo contrario, se producirán errores inesperados.

Protocolos NFS y ESXi

ESXi es compatible con las versiones 3 y 4.1 de los protocolos NFS. Para ser compatible con ambas versiones, ESXi utiliza dos clientes NFS diferentes.

Protocolo NFS versión 3

vSphere es compatible con la versión 3 de NFS en TCP. Al utilizar esta versión, se deben tener en cuenta las siguientes consideraciones:

- Con la versión 3 de NFS, el tráfico de almacenamiento se transmite por la LAN en un formato sin cifrar. Debido a esta seguridad limitada, utilice el almacenamiento NFS solo en redes de confianza y aísle el tráfico en conmutadores físicos individuales. También puede utilizar una VLAN privada.
- NFS 3 utiliza solo una conexión TCP de E/S. En consecuencia, ESXi admite la E/S en solo una dirección IP o un nombre de host del servidor NFS, y no admite varias rutas de acceso. Según la infraestructura y la configuración de la red, puede utilizar la pila de red para configurar varias conexiones a los destinos de almacenamiento. En este caso, debe tener varios almacenes de datos y cada uno de ellos debe utilizar conexiones de red individuales entre el host y el almacenamiento.
- Con NFS 3, ESXi no admite la funcionalidad de usuarios delegados, que permite acceder a los volúmenes NFS con credenciales que no son raíz. Debe asegurarse de que cada host tenga acceso de raíz al volumen.
- NFS 3 admite la aceleración de hardware para permitir que el host se integre con los dispositivos NAS y utiliza varias operaciones de hardware que ofrece el almacenamiento NAS. Para obtener más información, consulte [Aceleración de hardware en dispositivos NAS](#).
- Con la aceleración de hardware, es posible crear un disco virtual de aprovisionamiento grueso en almacenes de datos NFS 3.

- El bloqueo de NFS 3 en ESXi no utiliza el protocolo Network Lock Manager (NLM). En cambio, VMware ofrece su propio protocolo de bloqueo. Para implementar los bloqueos de NFS 3, se crean archivos de bloqueo en el servidor NFS. Los archivos de bloqueo se llaman `.lock-file_id`.

Protocolo NFS versión 4.1

Al utilizar NFS 4.1, se deben tener en cuenta las siguientes consideraciones:

- NFS 4.1 ofrece múltiples rutas para los servidores que admiten el enlace troncal de sesiones. Cuando el enlace troncal está disponible, se pueden utilizar varias direcciones IP para acceder a un solo volumen NFS. No se admite el enlace troncal del identificador de cliente.
- NFS 4.1 no admite la aceleración de hardware. Esta limitación no permite crear discos virtuales gruesos en los almacenes de datos NFS 4.1.
- NFS 4.1 admite el protocolo de autenticación Kerberos para proteger la comunicación con el servidor NFS. Para obtener más información, consulte [Usar credenciales Kerberos para NFS 4.1](#).
- NFS 4.1 utiliza reservas de recursos compartidos como mecanismo de bloqueo.
- NFS 4.1 admite el bloqueo de archivos incorporados.
- NFS 4.1 admite el acceso a archivos por parte de usuarios no raíz cuando se utiliza con Kerberos.
- NFS 4.1 admite montajes tradicionales sin Kerberos. En este caso, siga las instrucciones de seguridad y acceso de raíz recomendadas para la versión 3 de NFS.
- No admite montajes de AUTH_SYS y Kerberos simultáneos.
- NFS 4.1 con Kerberos no admite IPv6. NFS 4.1 con AUTH_SYS es compatible con IPv4 e IPv6.

Protocolos NFS y soluciones de vSphere

Características de vSphere	NFS versión 3	NFS versión 4.1
vMotion y Storage vMotion	Sí	Sí
High Availability (HA)	Sí	Sí
Fault Tolerance (FT)	Sí	Sí
Distributed Resource Scheduler (DRS)	Sí	Sí
Host Profiles	Sí	Sí
Storage DRS	Sí	No
Storage I/O Control	Sí	No
Site Recovery Manager	Sí	No
Virtual Volumes	Sí	No

Actualizaciones de la versión de NFS

vSphere no admite conversiones automáticas del almacén de datos de la versión 3 a la versión 4.1 de NFS. Si desea actualizar un almacén de datos NFS 3, las siguientes opciones están disponibles:

- Puede crear un nuevo almacén de datos NFS 4.1 y después utilizar Storage vMotion para migrar máquinas virtuales del almacén de datos anterior al nuevo.
- Utilizar los métodos de conversión que proporciona el servidor de almacenamiento NFS. Para obtener más información, póngase en contacto con su proveedor de almacenamiento.
- Desmontar desde una versión y después montar en la otra.

Precaución Si utiliza esta opción, asegúrese de desmontar el almacén de datos de todos los hosts que tengan acceso al almacén de datos. El almacén de datos jamás podrá montarse al utilizar ambos protocolos al mismo tiempo.

Configuraciones de firewall para almacenamiento NFS

ESXi incluye un firewall entre la interfaz de administración y la red. El firewall está habilitado de manera predeterminada. En el momento de la instalación, el firewall de ESXi está configurado para bloquear el tráfico entrante y saliente, a excepción del tráfico de los servicios predeterminados, como NFS.

Los servicios compatibles, incluido NFS, se describen en un archivo de configuración de un conjunto de reglas en el directorio `/etc/vmware/firewall/` del firewall de ESXi. El archivo contiene reglas de firewall y enumera la relación de cada regla con puertos y protocolos.

El comportamiento del conjunto de reglas del cliente NFS (`nfsClient`) es diferente a otros conjuntos de reglas. Cuando el conjunto de reglas del cliente NFS está habilitado, todos los puertos TCP salientes están abiertos para los hosts de destino que se incluyen en la lista de direcciones IP permitidas.

El conjunto de reglas de NFS 4.1 abre conexiones salientes al puerto de destino 2049, que es el puerto nombrado en la especificación para el protocolo versión 4.1. Las conexiones salientes se abren para todas las direcciones IP al montar por primera vez la unidad. Este puerto permanece abierto hasta que se reinicia el host ESXi.

Para obtener más información sobre las configuraciones del firewall, consulte la documentación de *Seguridad de vSphere*.

Comportamiento de firewall del cliente NFS

El conjunto de reglas de firewall del cliente NFS se comporta de forma diferente a otros conjuntos de reglas de firewall de ESXi. ESXi configura los parámetros del cliente NFS cuando se monta o desmonta un almacén de datos de NFS. El comportamiento varía según la versión de NFS.

Cuando se agrega, monta o desmonta un almacén de datos de NFS, el comportamiento que se obtiene varía según la versión de NFS.

Comportamiento de firewall de NFS v3

Cuando se agrega o monta un almacén de datos de NFS v3, ESXi comprueba el estado del conjunto de reglas de firewall del cliente NFS (`nfsClient`).

- Si el conjunto de reglas `nfsClient` está deshabilitado, ESXi habilita el conjunto de reglas y deshabilita la directiva Permitir todas las direcciones IP estableciendo la marca `allowedAll` en `FALSE`. La dirección IP del servidor NFS se agrega a la lista de direcciones IP salientes permitidas.
- Si el conjunto de reglas `nfsClient` está habilitado, el estado del conjunto de reglas y la directiva de direcciones IP permitidas no se cambian. La dirección IP del servidor NFS se agrega a la lista de direcciones IP salientes permitidas.

Nota Si habilita manualmente el conjunto de reglas `nfsClient` o configura manualmente la directiva Permitir todas las direcciones IP, ya sea antes o después de agregar un almacén de datos de NFS v3 al sistema, la configuración se anula cuando se desmonta el último almacén de datos de NFS v3. El conjunto de reglas `nfsClient` se deshabilita cuando se desmontan todos los almacenes de datos de NFS v3.

Cuando se quita o se desmonta un almacén de datos de NFS v3, ESXi realiza una de las siguientes acciones.

- Si ninguno de los almacenes de datos de NFS v3 restantes se monta desde el servidor del almacén de datos que se desmonta, ESXi quita la dirección IP del servidor de la lista de direcciones IP salientes.
- Si ninguno de los almacenes de datos de NFS v3 permanece después de la operación de desmontaje, ESXi deshabilita el conjunto de reglas de firewall de `nfsClient`.

Comportamiento de firewall de NFS v4.1

Cuando se monta el primer almacén de datos NFS v4.1, ESXi habilita el conjunto de reglas `nfs41client` y establece su marca `allowedAll` en `TRUE`. Esta acción abre el puerto 2049 para todas las direcciones IP. Cuando se desmonta el almacén de datos NFS v4.1, el estado del firewall no se ve afectado. De esta forma, el primer montaje de NFS v4.1 abre el puerto 2049, y ese puerto permanece habilitado a menos que se cierre explícitamente.

Comprobar los puertos de firewall para clientes NFS

Para habilitar el acceso al almacenamiento NFS, ESXi abre automáticamente puertos de firewall para los clientes NFS cuando se monta un almacén de datos de NFS. Por motivos de solución de problemas, es posible que deba comprobar que los puertos estén abiertos.

Procedimiento

- 1 En vSphere Web Client, seleccione el host ESXi.
- 2 Haga clic en la pestaña **Manage** (Administrar) y, a continuación, en **Settings** (Configuración).

- 3 Seleccione **Security Profile** (Perfil de seguridad) en el área **System** (Sistema) y haga clic en **Edit** (Editar).
- 4 Desplácese hacia abajo hasta encontrar la versión correspondiente de NFS para asegurarse de que el puerto esté abierto.

Usar las conexiones enrutadas de Capa 3 para acceder al almacenamiento NFS

Cuando utilice conexiones enrutadas de Capa 3 (L3) para acceder a almacenamiento NFS, debe tener en cuenta ciertos requisitos y restricciones.

Asegúrese de que el entorno cumpla los siguientes requisitos:

- Utilice el protocolo Hot Standby Router (HSRP) de Cisco en un enrutador IP. Si utiliza un enrutador de otra marca, asegúrese de usar el protocolo Virtual Router Redundancy Protocol (VRRP).
- Utilice calidad de servicio (QoS) para priorizar el tráfico L3 de NFS en redes con ancho de banda limitado, o en redes que experimentan congestiones. Para obtener detalles, consulte la documentación del enrutador.
- Siga las prácticas recomendadas por el proveedor de almacenamiento referidas a L3 de NFS enrutado. Para obtener detalles, póngase en contacto con el proveedor de almacenamiento.
- Deshabilite la administración de recursos de E/S de la red (NetIORM).
- Si piensa usar sistemas con conmutadores ubicados en la parte superior del bastidor o de la partición de dispositivos de E/S que dependen del conmutador, póngase en contacto con el proveedor del sistema para obtener información sobre compatibilidad y soporte.

En un entorno L3, se aplican las siguientes restricciones:

- El entorno no admite VMware Site Recovery Manager.
- El entorno admite únicamente el protocolo NFS. No use otros protocolos de almacenamiento, como FCoE, en la misma red física.
- El tráfico NFS en este entorno no es compatible con IPv6.
- El tráfico NFS en este entorno puede enrutarse solo a través de una LAN. No existe compatibilidad con otros entornos como WAN.

Configurar entorno de almacenamiento NFS

Se deben realizar varios pasos de configuración antes de montar un almacén de datos de NFS en vSphere.

Requisitos previos

- Familiarícese con las instrucciones en [Instrucciones y requisitos de almacenamiento NFS](#).
- Para obtener detalles sobre la configuración del almacenamiento NFS, consulte la documentación del proveedor de almacenamiento.

Procedimiento

- 1 En el servidor NFS, configure un volumen NFS y expórtelo para montarlo en los hosts ESXi.
 - a Tome nota de la dirección IP o del nombre DNS del servidor NFS y de la ruta de acceso completa, o del nombre de carpeta, del recurso compartido de NFS.

En NFS 4.1 se pueden recopilar varias direcciones IP o nombres de DNS para aprovechar la compatibilidad con múltiples rutas que proporciona un almacén de datos NFS 4.1. NFS 3 y NFS 4.1 sin Kerberos admiten direcciones IPv4 e IPv6.
 - b Si planifica utilizar la autenticación Kerberos con NFS 4.1, especifique las credenciales Kerberos que utilizará ESXi para la autenticación.
- 2 En cada host ESXi, configure un puerto de red del VMkernel para el tráfico NFS.

Para obtener más información, consulte la documentación sobre *Redes de vSphere*.
- 3 Si planifica utilizar la autenticación Kerberos con el almacén de datos NFS 4.1, configure los hosts ESXi para la autenticación Kerberos.

Asegúrese de cada host que monta este almacén de datos sea parte de un dominio de Active Directory y de que estén establecidas sus credenciales de autenticación de NFS.

Pasos siguientes

Ahora puede crear un almacén de datos de NFS en los hosts ESXi.

Usar credenciales Kerberos para NFS 4.1

Con la versión 4.1 de NFS, ESXi admite el mecanismo de autenticación Kerberos.

Kerberos es un servicio de autenticación que permite instalar un cliente de NFS 4.1 en ESXi para probar su identidad en un servidor NFS antes de montar un recurso compartido de NFS. Kerberos utiliza criptografía para funcionar en una conexión de red no segura. La implementación de Kerberos de vSphere para NFS 4.1 solo permite la comprobación de identidad del cliente y servidor, y no proporciona servicios de integridad o confidencialidad de datos.

Al utilizar la autenticación Kerberos, se deben tener en cuenta las siguientes consideraciones:

- ESXi utiliza la versión 5 de Kerberos con un dominio de Active Directory y el centro de distribución de claves (KDC).
- Como administrador de vSphere, debe especificar credenciales de Active Directory para proporcionar acceso a un usuario de NFS a los almacenes de datos Kerberos de NFS 4.1. Se utiliza un único conjunto de credenciales para acceder a todos los almacenes de datos Kerberos montados en ese host.
- Cuando varios hosts ESXi comparten el mismo almacén de datos de NFS 4.1, se deben utilizar las mismas credenciales de Active Directory para todos los hosts que tienen acceso al almacén de datos compartido. Para automatizar esta tarea, configure el usuario en los perfiles de host y aplique el perfil a todos los hosts ESXi.
- NFS 4.1 no admite montajes de AUTH_SYS y Kerberos simultáneos.

- NFS 4.1 con Kerberos no admite IPv6. Solo se admite IPv4.

Configurar hosts ESXi para la autenticación Kerberos

Si utiliza NFS 4.1 con Kerberos, debe realizar varias tareas para configurar los hosts para la autenticación Kerberos.

Cuando varios hosts ESXi comparten el mismo almacén de datos de NFS 4.1, se deben utilizar las mismas credenciales de Active Directory para todos los hosts que tienen acceso al almacén de datos compartido. Para automatizar esta tarea, configure el usuario en los perfiles de host y aplique el perfil a todos los hosts ESXi.

Requisitos previos

- Asegúrese de que los servidores de Microsoft Active Directory (AD) y NFS estén configurados para utilizar Kerberos.
- Habilite el modo de cifrado DES-CBC-MD5 en AD. El cliente NFS 4.1 admite solo este modo de cifrado.
- Asegúrese de que las exportaciones del servidor NFS estén configuradas para otorgar acceso completo al usuario de Kerberos.

Procedimiento

1 [Configurar DNS para NFS 4.1 con Kerberos](#)

Cuando utiliza NFS 4.1 con Kerberos, debe cambiar la configuración de DNS en los hosts ESXi para indicarle al servidor DNS que está configurado para enviar registros DNS al centro de distribución de claves (KDC) de Kerberos. Por ejemplo, utilice la dirección del servidor de Active Directory, si AD se utiliza como servidor DNS.

2 [Configurar protocolo Network Time Protocol para NFS 4.1 con Kerberos](#)

Si usa NFS 4.1 con Kerberos, configure el protocolo de tiempo de red (NTP) para asegurarse de que todos los hosts ESXi en la red de vSphere estén sincronizados.

3 [Habilitar la autenticación Kerberos en Active Directory](#)

Si se utiliza almacenamiento NFS 4.1 con Kerberos, se debe agregar cada host ESXi a un dominio de Active Directory y habilitar la autenticación Kerberos. Kerberos se integra con Active Directory para habilitar el inicio de sesión único y proporciona una capa adicional de seguridad cuando se utiliza en una conexión de red que no es segura.

Pasos siguientes

Después de configurar el host para Kerberos, puede crear un almacén de datos NFS 4.1 con Kerberos habilitado.

Configurar DNS para NFS 4.1 con Kerberos

Cuando utiliza NFS 4.1 con Kerberos, debe cambiar la configuración de DNS en los hosts ESXi para indicarle al servidor DNS que está configurado para enviar registros DNS al centro de

distribución de claves (KDC) de Kerberos. Por ejemplo, utilice la dirección del servidor de Active Directory, si AD se utiliza como servidor DNS.

Procedimiento

- 1 En vSphere Web Client, desplácese hasta el host.
- 2 Haga clic en la pestaña **Manage** (Administrar) y en **Networking** (Redes) y seleccione **TCP/IP configuration** (Configuración de TCP/IP).
- 3 Seleccione **TCP/IP configuration** (Configuración de TCP/IP) y haga clic en el icono **Edit** (Editar).
- 4 Introduzca la información de la configuración de DNS.

Opción	Descripción
Domain (Dominio)	Nombre del dominio de AD
Preferred DNS server (Servidor DNS preferido)	IP del servidor de AD
Search domains (Buscar dominios)	Nombre del dominio de AD

Configurar protocolo Network Time Protocol para NFS 4.1 con Kerberos

Si usa NFS 4.1 con Kerberos, configure el protocolo de tiempo de red (NTP) para asegurarse de que todos los hosts ESXi en la red de vSphere estén sincronizados.

Procedimiento

- 1 Seleccione el host en el inventario de vSphere.
 - 2 Haga clic en la pestaña **Manage** (Administrar) y en **Settings** (Configuración).
 - 3 En la sección System (Sistema), seleccione **Time Configuration** (Configuración de hora).
 - 4 Haga clic en **Edit** (Editar) y configure el servidor NTP.
 - a Seleccione **Use Network Time Protocol (Enable NTP client)** (Usar protocolo de hora de red [Habilitar el cliente NTP]).
 - b Establezca la directiva de inicio del servicio NTP.
 - c Introduzca la dirección IP de los servidores NTP con los que desea realizar la sincronización.
 - d En la sección NTP Service Status (Estado del servicio NTP), haga clic en **Start** (Iniciar) o **Restart** (Reiniciar).
 - 5 Haga clic en **OK** (Aceptar).
- El host se sincroniza con el servidor NTP.

Habilitar la autenticación Kerberos en Active Directory

Si se utiliza almacenamiento NFS 4.1 con Kerberos, se debe agregar cada host ESXi a un dominio de Active Directory y habilitar la autenticación Kerberos. Kerberos se integra con Active Directory para habilitar el inicio de sesión único y proporciona una capa adicional de seguridad cuando se utiliza en una conexión de red que no es segura.

Requisitos previos

Configure un dominio de AD y una cuenta de administrador de dominio con los derechos para agregar hosts al dominio.

Procedimiento

- 1 Agregue un host ESXi a un dominio de Active Directory.
 - a En vSphere Web Client, seleccione el host ESXi.
 - b Haga clic en la pestaña **Manage** (Administrar) y en **Settings** (Configuración).
 - c En System (Sistema), seleccione **Authentication Services** (Servicios de autenticación).
 - d Haga clic en **Join Domain** (Unirse al dominio), proporcione la configuración del dominio y haga clic en **OK** (Aceptar).

El tipo de servicios de directorio cambia a Active Directory.

- 2 Configure o edite las credenciales de un usuario Kerberos de NFS.
 - a En NFS Kerberos Credentials (Credenciales Kerberos de NFS), haga clic en **Edit** (Editar).
 - b Escriba un nombre de usuario y contraseña.

Se accederá a los archivos almacenados en todos los almacenes de datos Kerberos con estas credenciales.

El estado de las credenciales Kerberos de NFS cambia a Enabled (Habilitado).

Crear almacenes de datos

Puede utilizar el asistente New Datastore (Nuevo almacén de datos) para crear almacenes de datos. Según el tipo de almacenamiento que tenga en el entorno y de las necesidades de almacenamiento, puede crear un almacén de datos de VMFS, NFS o virtual.

Al habilitar Virtual SAN, se crea un almacén de datos de Virtual SAN de forma automática. Para obtener información, consulte el documento *Administración de VMware Virtual SAN*.

También puede utilizar el asistente New Datastore (Nuevo almacén de datos) para administrar copias del almacén de datos de VMFS.

- **Crear un almacén de datos de VMFS**

Los almacenes de datos de VMFS sirven como repositorios para las máquinas virtuales. Los almacenes de datos de VMFS se pueden configurar en cualquier dispositivo de almacenamiento basado en SCSI que el host detecte, incluidos el canal de fibra, iSCSI y los dispositivos de almacenamiento local.

- **Crear un almacén de datos de NFS**

Puede utilizar el asistente **New Datastore** (Nuevo almacén de datos) para montar un volumen NFS.

- **Crear un almacén de datos virtual**

Puede utilizar el asistente **New Datastore** (Nuevo almacén de datos) para crear un almacén de datos virtual.

Crear un almacén de datos de VMFS

Los almacenes de datos de VMFS sirven como repositorios para las máquinas virtuales. Los almacenes de datos de VMFS se pueden configurar en cualquier dispositivo de almacenamiento basado en SCSI que el host detecte, incluidos el canal de fibra, iSCSI y los dispositivos de almacenamiento local.

Nota No puede crear almacenes de datos de VMFS3 en vSphere 6.x. Aunque los almacenes de datos de VMFS3 existentes sigan estando disponibles y se puedan utilizar, debe actualizarlos a VMFS5.

Requisitos previos

Instale y configure todos los adaptadores que requiere el almacenamiento. Vuelva a examinar los adaptadores para detectar los dispositivos de almacenamiento recientemente agregados.

Procedimiento

- 1 En el navegador de vSphere Web Client, seleccione **Listas de inventario global > Almacenes de datos**.
- 2 Haga clic en el icono **Nuevo almacén de datos**.
- 3 Escriba el nombre del almacén de datos y, si es necesario, seleccione la ubicación en la que colocará el almacén de datos.

vSphere Web Client aplica un límite de 42 caracteres para el nombre del almacén de datos.
- 4 Seleccione VMFS como el tipo de almacén de datos.

- 5 Seleccione el dispositivo que desea usar para el almacén de datos.

Importante El dispositivo que seleccione no debe mostrar ningún valor en la columna Volumen de instantánea. Si aparece un valor, el dispositivo contiene una copia de un almacén de datos de VMFS existente. Para obtener información sobre cómo administrar copias de almacenes de datos, consulte [Administrar almacenes de datos de VMFS duplicados](#).

- 6 Especifique la configuración de la partición.

Opción	Descripción
Utilizar todas las particiones disponibles	Dedica el disco completo a un solo almacén de datos de VMFS. Si se selecciona esta opción, se eliminan todos los sistemas de archivos y los datos almacenados en este dispositivo.
Utilizar espacio libre	Implementa un almacén de datos de VMFS en el espacio libre del disco.

- 7 (opcional) Si el espacio asignado para el almacén de datos es excesivo para el objetivo buscado, ajuste los valores de capacidad en el campo Tamaño del almacén de datos.
De manera predeterminada, se asigna todo el espacio libre en el dispositivo de almacenamiento.
- 8 En la página Listo para finalizar, revise la información de configuración del almacén de datos y haga clic en **Finalizar**.

Resultados

Se crea el almacén de datos en el dispositivo de almacenamiento basado en SCSI. Está disponible para todos los hosts que tienen acceso al dispositivo.

Crear un almacén de datos de NFS

Puede utilizar el asistente **New Datastore** (Nuevo almacén de datos) para montar un volumen NFS.

Requisitos previos

- Configure el entorno de almacenamiento NFS.
- Si desea utilizar la autenticación Kerberos con el almacén de datos NFS 4.1, asegúrese de configurar los hosts ESXi para la autenticación Kerberos.

Procedimiento

- 1 En el navegador de vSphere Web Client, seleccione **Listas de inventario global > Almacenes de datos**.
- 2 Haga clic en el icono **Nuevo almacén de datos**.
- 3 Escriba el nombre del almacén de datos y, si es necesario, seleccione la ubicación en la que colocará el almacén de datos.

vSphere Web Client aplica un límite de 42 caracteres para el nombre del almacén de datos.

- 4 Seleccione NFS como el tipo de almacén de datos.
- 5 Especifique la versión de NFS.
 - NFS 3
 - NFS 4.1

Importante Si varios hosts acceden al mismo almacén de datos, debe utilizar el mismo protocolo en todos los hosts.

- 6 Escriba el nombre del servidor o la dirección IP y el nombre de la carpeta de punto de montaje.

Con NFS 4.1, puede agregar varias direcciones IP o nombres de servidores si el servidor admite el enlace troncal. El host utiliza estos valores para lograr la habilitación de múltiples rutas al punto de montaje del servidor NFS.

Puede utilizar las direcciones IPv4 o IPv6 para NFS 3 y para NFS 4.1 sin Kerberos.
- 7 Seleccione **Mount NFS read only** (Montar NFS de solo lectura) si el servidor NFS exporta el volumen como de solo lectura.
- 8 Si utiliza la autenticación Kerberos con NFS 4.1, habilite Kerberos en el almacén de datos.
- 9 Si está creando un almacén de datos en el nivel del clúster o del centro de datos, seleccione los hosts que montan el almacén de datos.
- 10 Revise las opciones de configuración y haga clic en **Finish** (Finalizar).

Crear un almacén de datos virtual

Puede utilizar el asistente **New Datastore** (Nuevo almacén de datos) para crear un almacén de datos virtual.

Procedimiento

- 1 En el navegador de vSphere Web Client, seleccione **Listas de inventario global > Almacenes de datos**.
- 2 Haga clic en el icono **Nuevo almacén de datos**.
- 3 Escriba el nombre del almacén de datos y, si es necesario, seleccione la ubicación en la que colocará el almacén de datos.

Asegúrese de utilizar un nombre que no duplique el de otro almacén de datos en el entorno del centro de datos.

Si monta el mismo almacén de datos virtual en varios hosts, el nombre del almacén de datos debe ser uniforme entre todos los hosts.
- 4 Seleccione **VVOL** como tipo de almacén de datos.
- 5 En la lista de contenedores de almacenamiento, seleccione un contenedor de almacenamiento de respaldo.

- 6 Seleccione los hosts que requieren acceso al almacén de datos.
- 7 Revise las opciones de configuración y haga clic en **Finish** (Finalizar).

Pasos siguientes

Después de crear el almacén de datos virtual, puede realizar operaciones de almacenes de datos como cambiar el nombre del almacén de datos, explorar los archivos del almacén de datos, desmontar el almacén de datos, etc.

No puede agregar el almacén de datos virtual a un clúster de almacenes de datos.

Administrar almacenes de datos de VMFS duplicados

Cuando un dispositivo de almacenamiento contiene una copia del almacén de datos de VMFS, se puede montar el almacén de datos con la firma existente o asignar una firma nueva.

Cada almacén de datos de VMFS creado en un disco de almacenamiento tiene una firma única, también llamado UUID, que se almacena en el superbloque del sistema de archivos. Cuando el disco de almacenamiento se replica o su instantánea se crea en el almacenamiento, la copia de disco resultante es idéntica, byte por byte, al disco original. Como resultado, si el disco de almacenamiento original contiene un almacén de datos de VMFS con UUID X, la copia del disco contendrá un almacén de datos de VMFS idéntico, o bien una copia del almacén de datos de VMFS, con el mismo UUID X.

Además de la creación de instantáneas y la replicación del LUN, las siguientes operaciones del dispositivo de almacenamiento pueden hacer que ESXi marque el almacén de datos existente en el dispositivo como una copia del almacén de datos original:

- Cambios en el identificador del LUN
- Cambios en el tipo de dispositivo SCSI (por ejemplo, de SCSI-2 a SCSI-3)
- Habilitación del cumplimiento de SPC-2

ESXi puede detectar la copia del almacén de datos de VMFS y mostrarla en vSphere Web Client. Existe la opción de montar la copia del almacén de datos con su UUID original, o bien cambiar el UUID para volver a firmar el almacén de datos.

La elección entre volver a firmar o montar sin volver a firmar depende de cómo se enmascaran los LUN en el entorno de almacenamiento. Si los hosts pueden ver las dos copias del LUN, entonces se recomienda volver a firmar. De lo contrario, se recomienda el montaje.

Conservar la firma de almacén de datos existente

Si no se necesita volver a firmar una copia del almacén de datos de VMFS, se la puede montar sin cambiar la firma.

Se puede mantener la firma, por ejemplo, si se conservan copias sincronizadas de las máquinas virtuales en un sitio secundario como parte de un plan de recuperación ante desastres. En el caso de que ocurra un desastre en el sitio principal, se monta la copia del almacén de datos y se encienden las máquinas virtuales en el sitio secundario.

Requisitos previos

- Vuelva a examinar el almacenamiento en el host para actualizar la vista de los dispositivos de almacenamiento presentados al host.
- Desmunte el almacén de datos de VMFS original que tiene el mismo UUID que la copia que planifica montar. Puede montar la copia del almacén de datos de VMFS solo si no entra en conflicto con el almacén de datos de VMFS original.

Procedimiento

- 1 En el navegador de vSphere Web Client, seleccione **Listas de inventario global > Almacenes de datos**.
- 2 Haga clic en el icono **Nuevo almacén de datos**.
- 3 Escriba el nombre del almacén de datos y, si es necesario, seleccione la ubicación en la que colocará el almacén de datos.
- 4 Seleccione VMFS como el tipo de almacén de datos.
- 5 En la lista de dispositivos de almacenamiento, seleccione el dispositivo que tiene un valor específico en la columna Snapshot Volume (Volumen de instantánea).

El valor presente en la columna Snapshot Volume (Volumen de instantánea) indica que el dispositivo es una copia que contiene una copia de un almacén de datos de VMFS existente.
- 6 En Mount Options (Opciones de montaje), seleccione **Keep Existing Signature** (Mantener firma existente).
- 7 Revise la información de configuración del almacén de datos y haga clic en **Finish** (Finalizar).

Pasos siguientes

Si más adelante se desea volver a firmar el almacén de datos montado, primero es necesario desmontarlo.

Volver a firmar una copia de un almacén de datos de VMFS

Utilice la opción para volver a firmar el almacén de datos si desea retener los datos almacenados en la copia del almacén de datos de VMFS.

Cuando vuelve a firmar una copia de VMFS, ESXi asigna una firma nueva (UUID) a la copia y monta la copia como un almacén de datos distinto del original. Se actualizan todas las referencias a la firma original en todos los archivos de configuración de la máquina virtual.

Al volver a firmar un almacén de datos, tenga en cuenta los siguientes puntos:

- Volver a firmar un almacén de datos es una acción irreversible.

- Luego de volver a firmar, la réplica del dispositivo de almacenamiento que contenía la copia de VMFS ya no se trata como una réplica.
- Un almacén de datos extendido puede volver a firmarse solamente si todas sus extensiones están en línea.
- El proceso de volver a firmar tolera errores y bloqueos. Si el proceso se interrumpe, es posible reanudarlo más adelante.
- Es posible montar el almacén de datos de VMFS nuevo sin riesgos de que el UUID entre en conflicto con las UUID de cualquier otro almacén de datos, como un antecesor o un secundario en una jerarquía de instantáneas de dispositivos de almacenamiento.

Requisitos previos

- Desmunte la copia del almacén de datos.
- Vuelva a examinar el almacenamiento en el host para actualizar la vista de los dispositivos de almacenamiento presentados al host.

Procedimiento

- 1 En el navegador de vSphere Web Client, seleccione **Listas de inventario global > Almacenes de datos**.
- 2 Haga clic en el icono **Nuevo almacén de datos**.
- 3 Escriba el nombre del almacén de datos y, si es necesario, seleccione la ubicación en la que colocará el almacén de datos.
- 4 Seleccione VMFS como el tipo de almacén de datos.
- 5 En la lista de dispositivos de almacenamiento, seleccione el dispositivo que tiene un valor específico en la columna Snapshot Volume (Volumen de instantánea).

El valor presente en la columna Snapshot Volume (Volumen de instantánea) indica que el dispositivo es una copia que contiene una copia de un almacén de datos de VMFS existente.
- 6 En Mount Options (Opciones de montaje), seleccione **Assign a New Signature** (Asignar una nueva firma) y haga clic en **Next** (Siguiente).
- 7 Revise la información de configuración del almacén de datos y haga clic en **Finish** (Finalizar).

Actualizar los almacenes de datos de VMFS

Si los almacenes de datos se formatearon con VMFS2 O VMFS3, debe actualizarlos a VMFS5.

Al realizar actualizaciones de almacenes de datos, tenga en cuenta los siguientes puntos:

- Para actualizar un almacén de datos de VMFS2, utilice un proceso de dos pasos que implica primero actualizar VMFS2 a VMFS3. Para acceder al almacén de datos de VMFS2 y realizar la conversión de VMFS2 a VMFS3, utilice un host ESX/ESXi 4.x o anterior.

Una vez que actualiza el almacén de datos de VMFS2 a VMFS3, este aparece disponible en el host ESXi 6.x, donde se completa el proceso de actualización a VMFS5.

- Es posible realizar la actualización de VMFS3 a VMFS5 mientras el almacén de datos se está utilizando con máquinas virtuales encendidas.
- Al realizar una actualización, el host conserva todos los archivos en el almacén de datos.
- La actualización del almacén de datos es un proceso unidireccional. Una vez que se actualizó el almacén de datos, no se lo puede revertir a su formato de VMFS anterior.

Un almacén de datos de VMFS5 actualizado es diferente a uno de VMFS5 recientemente formateado.

Tabla 16-3. Comparar almacenes de datos de VMFS5 actualizados y recientemente formateados

Características	VMFS5 actualizado	VMFS5 formateado
Tamaño de bloque de archivo	1, 2, 4 y 8 MB	1 MB
Tamaño de sub-bloque	64 KB	8 KB
Formato de partición	MBR. La conversión a GPT se produce solo después de expandir el almacén de datos a un tamaño mayor que 2 TB.	GPT
Límites del almacén de datos	Conserva los límites del almacén de datos de VMFS3.	
Mecanismo de bloqueo de VMFS	ATS+SCSI	Solo con ATS (en hardware compatible con ATS) ATS+SCSI (en hardware no compatible con ATS)

Para obtener más información sobre los mecanismos de bloqueo de VMFS y cómo actualizar solo a ATS, consulte [Mecanismos de bloqueo de VMFS](#).

Actualizar un almacén de datos a VMFS5

Si utiliza almacenes de datos VMFS3, debe actualizarlos a VMFS5.

Puede realizar una actualización mientras el almacén de datos está en uso con las máquinas virtuales encendidas.

Requisitos previos

- Si tiene un almacén de datos VMFS2, primero debe actualizarlo a VMFS3 con un host ESX/ESXi 3.x o ESX/ESXi 4.x. Utilice vSphere Host Client para acceder al host.
- Todos los hosts que acceden al almacén de datos deben admitir VMFS5.
- Compruebe que el volumen que se actualizará tenga al menos 2 MB de espacio libre. Revise la pestaña Resumen del almacén de datos para obtener esta información.

Procedimiento

- 1 En el navegador de vSphere Web Client, seleccione **Listas de inventario global > Almacenes de datos**.
- 2 Haga clic en el almacén de datos que desea actualizar.
- 3 Haga clic en la pestaña **Configurar**.
- 4 Haga clic en **Actualizar a VMFS5**.
- 5 Compruebe que los hosts que acceden al almacén de datos sean compatibles con VMFS5.
- 6 Haga clic en **Aceptar** para iniciar la actualización.
- 7 Vuelva a examinar todos los hosts asociados con el almacén de datos.

Resultados

El almacén de datos se actualiza a VMFS5 y está disponible para todos los hosts que estén asociados con el almacén de datos.

Aumentar la capacidad de un almacén de datos de VMFS

Si el almacén de datos de VMFS requiere más espacio, aumente la capacidad del almacén de datos. Puede aumentar dinámicamente la capacidad si amplía una extensión del almacén de datos o agrega una extensión nueva.

Utilice uno de los siguientes métodos para aumentar la capacidad de un almacén de datos:

- Amplíe dinámicamente cualquier extensión de almacén de datos expandible para llenar la capacidad adyacente disponible. La extensión se considera expandible cuando el dispositivo de almacenamiento subyacente tiene espacio libre inmediatamente después de la extensión.
- Agregue dinámicamente una extensión nueva. El almacén de datos puede expandir un máximo de 32 extensiones, con un tamaño superior a 2 TB cada una, y seguir apareciendo como un solo volumen. El almacén de datos de VMFS extendido puede utilizar cualquiera de las extensiones o todas ellas en cualquier momento. No es necesario que complete una extensión en especial para poder utilizar la siguiente.

Nota Los almacenes de datos que admiten solo bloqueo asistido por hardware, también denominado mecanismo de prueba y configuración atómica (ATS), no pueden expandirse a dispositivos sin bloqueo con ATS. Para obtener más información, consulte [Mecanismos de bloqueo de VMFS](#).

Aumentar la capacidad de un almacén de datos de VMFS

Cuando necesita agregar máquinas virtuales a un almacén de datos o cuando las máquinas virtuales que se ejecutan en un almacén de datos requieren más espacio, puede aumentar dinámicamente la capacidad de un almacén de datos de VMFS.

Si un almacén de datos encendió máquinas virtuales y se completa al 100 %, puede aumentar la capacidad del almacén de datos solo desde el host con el que están registradas las máquinas virtuales encendidas.

Procedimiento

- 1 En el navegador de vSphere Web Client, seleccione **Listas de inventario global > Almacenes de datos**.
- 2 Seleccione el almacén de datos al que desea agregar capacidad y haga clic en el icono Increase Datastore Capacity (Aumentar capacidad del almacén de datos).
- 3 Seleccione un dispositivo de la lista de dispositivos de almacenamiento.

La selección depende de si hay disponible un dispositivo de almacenamiento ampliable.

Opción	Descripción
Para expandir una extensión existente	Seleccione el dispositivo para el cual la columna Expandable (Ampliable) diga YES (Sí). Un dispositivo de almacenamiento se informa como ampliable cuando tiene espacio libre inmediatamente después de la extensión.
Para agregar una extensión nueva	Seleccione el dispositivo para el cual la columna Expandable (Ampliable) diga NO.

- 4 Revise **Current Disk Layout** (Diseño del disco actual) para ver las configuraciones disponibles y haga clic en **Next** (Siguiente).
- 5 Seleccione una opción de configuración del panel inferior.

Según el diseño actual del disco y las opciones que seleccionó anteriormente, pueden variar las opciones que verá.

Opción	Descripción
Use free space to add new extent (Utilizar espacio libre para agregar una extensión nueva)	Agrega el espacio libre de este disco como una extensión nueva.
Use free space to expand existing extent (Utilizar el espacio libre para expandir la extensión existente)	Expande una extensión existente a la capacidad necesaria.
Use free space (Utilizar espacio libre)	Implementa una extensión en el espacio libre restante del disco. Esta opción está disponible solo cuando agrega una extensión.
Use all available partitions (Utilizar todas las particiones disponibles)	Dedica el disco completo a una sola extensión. Esta opción está disponible solo cuando agrega una extensión y cuando el disco al que está dando formato no está en blanco. Se reformatea el disco y se eliminan los almacenes de datos junto con los datos que contengan.

- 6 Establezca la capacidad de la extensión.

El tamaño mínimo de la extensión es de 1,3 GB. De forma predeterminada, todo el espacio libre en el dispositivo de almacenamiento está disponible.

- 7 Haga clic en **Next** (Siguiente).

- 8 Revise el diseño propuesto y la configuración nueva del almacén de datos y haga clic en **Finish** (Finalizar).

Operaciones administrativas para almacenes de datos

Una vez creados los almacenes de datos, se pueden realizar varias operaciones administrativas en ellos. Ciertas operaciones, como el cambio de nombre de los almacenes de datos, están disponibles para todos los tipos de almacenes de datos. Otras aplican a tipos de almacenes de datos específicos.

- **Cambiar nombre del almacén de datos**

Puede cambiar el nombre de un almacén de datos existente. Puede cambiar el nombre de un almacén de datos en el que se están ejecutando máquinas virtuales sin consecuencias negativas.

- **Desmontar almacenes de datos**

Al desmontar un almacén de datos, este permanece intacto aunque ya no es visible desde los hosts especificados. El almacén de datos sigue apareciendo en otros hosts, donde permanece montado.

- **Montar almacenes de datos**

Es posible montar un almacén de datos que se desmontó previamente. También puede montar un almacén de datos en hosts adicionales para transformarlo en un almacén de datos compartido.

- **Quitar almacenes de datos de VMFS**

Se puede eliminar cualquier tipo de almacén de datos de VMFS, incluidas las copias que se hayan montado sin volver a firmar. Cuando se elimina un almacén de datos, este se destruye y desaparece de todos los hosts que tienen acceso al almacén de datos.

- **Usar el explorador del almacén de datos**

Utilice el explorador de archivos del almacén de datos para administrar el contenido de los almacenes de datos. Puede examinar las carpetas y los archivos que se encuentran en el almacén de datos. También puede usar el explorador para cargar archivos y ejecutar tareas administrativas en las carpetas y los archivos.

- **Desactivar los filtros de almacenamiento**

Cuando se realizan operaciones de administración de almacenes de datos de VMFS, vCenter Server utiliza los filtros predeterminados de protección de almacenamiento. Los filtros ayudan a evitar daños en el almacenamiento al recuperar solo los dispositivos de almacenamiento que se pueden utilizar para una operación determinada. Los dispositivos que no son adecuados no se pueden seleccionar porque no se muestran. Para ver todos los dispositivos, puede desactivar los filtros.

Cambiar nombre del almacén de datos

Puede cambiar el nombre de un almacén de datos existente. Puede cambiar el nombre de un almacén de datos en el que se están ejecutando máquinas virtuales sin consecuencias negativas.

Procedimiento

- 1 En el navegador de vSphere Web Client, seleccione **Listas de inventario global > Almacenes de datos**.
- 2 Seleccione el almacén de datos cuyo nombre desea cambiar.
- 3 Seleccione **Cambiar nombre** en el menú contextual.
- 4 Escriba un nombre de almacén de datos nuevo.

vSphere Web Client aplica un límite de 42 caracteres para el nombre del almacén de datos.

Resultados

El nombre nuevo aparecerá en todos los hosts que tienen acceso al almacén de datos.

Desmontar almacenes de datos

Al desmontar un almacén de datos, este permanece intacto aunque ya no es visible desde los hosts especificados. El almacén de datos sigue apareciendo en otros hosts, donde permanece montado.

No realice ninguna operación de configuración que pueda provocar operaciones de E/S en el almacén de datos mientras el desmontaje está en curso.

Nota Asegúrese de que el almacén de datos no se use para los latidos de vSphere HA. Los latidos de vSphere HA no evitan el desmontaje del almacén de datos. Sin embargo, si el almacén de datos se utiliza para los latidos, desmontarlo podría provocar que el host genere errores y reinicie todas las máquinas virtuales activas.

Requisitos previos

Cuando sea apropiado, antes de desmontar almacenes de datos, asegúrese de que se cumplan los siguientes requisitos previos:

- Ninguna máquina virtual debe residir en el almacén de datos.
- El almacén de datos no debe estar administrado por Storage DRS.
- Storage I/O Control debe estar deshabilitado para este almacén de datos.

Procedimiento

- 1 En el navegador de vSphere Web Client, seleccione **Listas de inventario global > Almacenes de datos**.
- 2 Haga clic con el botón derecho en el almacén de datos que desea desmontar y seleccione **Unmount Datastore** (Desmontar almacén de datos).

- 3 Si el almacén de datos es un recurso compartido, especifique los hosts que no deben acceder a él.
- 4 Confirme que desea desmontar el almacén de datos.

Resultados

Después de desmontar un almacén de datos de VMFS de todos los hosts, el almacén de datos se marca como inactivo. Si desmonta un NFS o un almacén de datos virtual de todos los hosts, el almacén de datos desaparece del inventario.

Pasos siguientes

Si desmontó el almacén de datos de VMFS como parte de un procedimiento de eliminación de almacenamiento ordenado, ahora puede desconectar el dispositivo de almacenamiento que respalda el almacén de datos. Consulte [Separar dispositivos de almacenamiento](#).

Montar almacenes de datos

Es posible montar un almacén de datos que se desmontó previamente. También puede montar un almacén de datos en hosts adicionales para transformarlo en un almacén de datos compartido.

Un almacén de datos de VMFS que se desmontó de todos los hosts permanece en el inventario, pero se marca como inaccesible. Puede usar esta tarea para montar el almacén de datos de VMFS en un host específico o en varios hosts.

Si desmontó un NFS o un almacén de datos virtual de todos los hosts, el almacén de datos desaparece del inventario. Para montar el NFS o el almacén de datos virtual que se quitó del inventario, use el asistente Nuevo almacén de datos.

Un almacén de datos de cualquier tipo que se desmonta de algunos hosts mientras está montado en otros, se muestra como activo en el inventario.

Procedimiento

- 1 En el navegador de vSphere Web Client, seleccione **Listas de inventario global > Almacenes de datos**.
- 2 Haga clic con el botón derecho en el almacén de datos que desea montar y seleccione una de las opciones siguientes:
 - **Montar almacén de datos**
 - **Montar almacén de datos en hosts adicionales**Según el tipo de almacén de datos que use, verá una opción o la otra.
- 3 Seleccione los hosts que deberían acceder al almacén de datos.

Quitar almacenes de datos de VMFS

Se puede eliminar cualquier tipo de almacén de datos de VMFS, incluidas las copias que se hayan montado sin volver a firmar. Cuando se elimina un almacén de datos, este se destruye y desaparece de todos los hosts que tienen acceso al almacén de datos.

Nota La operación de eliminación del almacén de datos elimina de manera permanente todos los archivos asociados a las máquinas virtuales en el almacén de datos. Aunque es posible eliminar el almacén de datos sin necesidad de desmontar, es preferible que primero se desmonte el almacén de datos.

Requisitos previos

- Quite o migre todas las máquinas virtuales del almacén de datos.
- Asegúrese de que ningún otro host acceda al almacén de datos.
- Deshabilite Storage DRS para el almacén de datos.
- Deshabilite Storage I/O Control para el almacén de datos.
- Asegúrese de que el almacén de datos no se use para los latidos de vSphere HA.

Procedimiento

- 1 En el navegador de vSphere Web Client, seleccione **Listas de inventario global > Almacenes de datos**.
- 2 Haga clic con el botón derecho en el almacén de datos para quitarlo.
- 3 Seleccione **Delete Datastore** (Eliminar almacén de datos).
- 4 Confirme que desea quitar el almacén de datos.

Usar el explorador del almacén de datos

Utilice el explorador de archivos del almacén de datos para administrar el contenido de los almacenes de datos. Puede examinar las carpetas y los archivos que se encuentran en el almacén de datos. También puede usar el explorador para cargar archivos y ejecutar tareas administrativas en las carpetas y los archivos.

- [Cargar archivos en almacenes de datos](#)
Use el explorador de archivos del almacén de datos para cargar archivos a almacenes de datos a los que pueda accederse desde hosts ESXi.
- [Copiar archivos o carpetas de almacenes de datos](#)
Utilice el explorador del almacén de datos para copiar archivos o carpetas a una nueva ubicación en el mismo almacén de datos o en otro.
- [Mover archivos o carpetas de almacenes de datos](#)
Utilice el explorador del almacén de datos para mover las carpetas o los archivos a una ubicación nueva, ya sea en el mismo almacén de datos o en uno diferente.


- [Cambiar nombre de archivos o carpetas de almacenes de datos](#)







Utilice el explorador de almacenes de datos para cambiar el nombre de archivos o carpetas.

- [Expandir discos virtuales finos](#)

Si creó un disco virtual en formato fino, puede convertir el disco fino a un disco virtual con formato de aprovisionamiento grueso.

Procedimiento

- 1 Abra el navegador del almacén de datos.
 - a Muestre el almacén de datos en el inventario.
 - b Haga clic con el botón derecho en el almacén de datos y seleccione **Examinar archivos** ().
- 2 Para explorar el contenido del almacén de datos, desplácese hasta las carpetas y los archivos existentes.
- 3 Para ejecutar las tareas administrativas, puede usar diversos iconos y opciones.

Iconos y opciones	Descripciones
	Instalar el complemento de integración de clientes o Cargar un archivo en el almacén de datos. Consulte Cargar archivos en almacenes de datos .
	Crear una carpeta en el almacén de datos.
	Copiar las carpetas o los archivos seleccionados en una ubicación nueva, ya sea en el mismo almacén de datos o en uno diferente. Consulte Copiar archivos o carpetas de almacenes de datos .
	Mover las carpetas o los archivos seleccionados a una ubicación nueva, ya sea en el mismo almacén de datos o en uno diferente. Consulte Mover archivos o carpetas de almacenes de datos .
	Cambiar el nombre de las carpetas o de los archivos seleccionados. Consulte Cambiar nombre de archivos o carpetas de almacenes de datos .
	Eliminar las carpetas o los archivos seleccionados.
Expandir	Convertir un disco virtual fino seleccionado en disco grueso. Esta opción solo se aplica a discos con aprovisionamiento fino. Consulte Expandir discos virtuales finos .

Pasos siguientes

Mire el vídeo siguiente para obtener más información.



Uso del explorador de almacenes de datos en vSphere Web Client
[\(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_huoxtz17/uiConfId/49694343/\)](https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_huoxtz17/uiConfId/49694343/)


Cargar archivos en almacenes de datos

Use el explorador de archivos del almacén de datos para cargar archivos a almacenes de datos a los que pueda accederse desde hosts ESXi.



Además de su uso tradicional como almacenamiento para archivos de máquinas virtuales, los almacenes de datos pueden servir para almacenar datos o archivos relacionados con máquinas virtuales. Por ejemplo, puede cargar imágenes ISO de sistemas operativos desde un equipo local a un almacén de datos en el host. A continuación, puede usar esas imágenes para instalar sistemas operativos invitados en las máquinas virtuales nuevas.

Nota No se pueden cargar archivos directamente a almacenes de datos de Virtual Volumes. Primero se debe crear una carpeta en el almacén de datos de Virtual Volumes para después poder cargar los archivos en la carpeta. Las carpetas creadas en los almacenes de datos de volumen virtual para almacenamiento en bloque, tienen una capacidad de almacenamiento limitada de 4 GB. El almacén de datos de vVols es compatible con cargas directas de carpetas.

Requisitos previos

- Privilegio necesario: **Almacén de datos.Examinar almacén de datos**
- Seleccione el icono  y compruebe la etiqueta. Si la etiqueta dice Instalar el complemento de integración de clientes, debe instalar el complemento para poder cargar archivos. Haga clic en el icono y siga las indicaciones. Tras la instalación, la etiqueta cambia a Cargar un archivo en el almacén de datos.

Procedimiento

- 1 Abra el navegador del almacén de datos.
 - a Muestre el almacén de datos en el inventario.
 - b Haga clic con el botón derecho en el almacén de datos y seleccione **Examinar archivos** .
- 2 (opcional) Cree una carpeta para almacenar el archivo.
- 3 Seleccione la carpeta de destino y haga clic en el icono **Cargar un archivo en el almacén de datos** .
- 4 Localice el elemento que desea cargar en el equipo local y haga clic en **Abrir**.
- 5 Actualice el explorador de archivos del almacén de datos para ver el archivo cargado en la lista.

Pasos siguientes

Es posible que tenga problemas si implementa una plantilla de OVF que anteriormente se exportó y que después se cargó en el almacén de datos. Para obtener información detallada y una solución alternativa, consulte el artículo [2117310](#) de la base de conocimientos de VMware.

Copiar archivos o carpetas de almacenes de datos

Utilice el explorador del almacén de datos para copiar archivos o carpetas a una nueva ubicación en el mismo almacén de datos o en otro.


Los archivos de discos virtuales se mueven o copian sin conversión de formato. Si transfiere un disco virtual a un almacén de datos que pertenece a un host diferente del host de origen, es posible que necesite convertir el disco virtual. De lo contrario, quizás no pueda usar el disco.

No se pueden copiar archivos de máquina virtual de un vCenter Server a otro.

Requisitos previos

Privilegio necesario: **Almacén de datos.Examinar almacén de datos**

Procedimiento

- 1 Abra el navegador del almacén de datos.
 - a Muestre el almacén de datos en el inventario.
 - b Haga clic con el botón derecho en el almacén de datos y seleccione **Examinar archivos** .
- 2 Desplácese hasta el objeto que desea copiar, se trate de un archivo o de una carpeta.
- 3 Seleccione el objeto y haga clic en el icono **Copiar selección a una nueva ubicación**.
- 4 Especifique la ubicación de destino.
- 5 (opcional) Seleccione **Sobrescribir archivos y carpetas con nombres coincidentes en el destino**.
- 6 Haga clic en **Aceptar**.

Mover archivos o carpetas de almacenes de datos


Utilice el explorador del almacén de datos para mover las carpetas o los archivos a una ubicación nueva, ya sea en el mismo almacén de datos o en uno diferente.

Nota Los archivos de discos virtuales se mueven o copian sin conversión de formato. Si mueve un disco virtual a un almacén de datos en un tipo diferente de host desde el host de origen, posiblemente deba convertir los discos virtuales antes de utilizarlos.

Requisitos previos

Privilegios necesarios: **Almacén de datos.Examinar almacén de datos**

Procedimiento

- 1 Abra el navegador del almacén de datos.
 - a Muestre el almacén de datos en el inventario.
 - b Haga clic con el botón derecho en el almacén de datos y seleccione **Examinar archivos** .

- 2 Desplácese hasta el objeto que desea mover, ya sea un archivo o una carpeta.
- 3 Seleccione el objeto y haga clic en el icono **Move selection to a new location** (Mover selección a una nueva ubicación).
- 4 Especifique la ubicación de destino.
- 5 (opcional) Seleccione **Overwrite files and folders with matching names at the destination** (Sobrescribir archivos y carpetas con nombres coincidentes en el destino).
- 6 Haga clic en **OK** (Aceptar).


Cambiar nombre de archivos o carpetas de almacenes de datos

Utilice el explorador de almacenes de datos para cambiar el nombre de archivos o carpetas.

Requisitos previos

Privilegios necesarios: **Almacén de datos.Examinar almacén de datos**

Procedimiento

- 1 Abra el navegador del almacén de datos.
 - a Muestre el almacén de datos en el inventario.
 - b Haga clic con el botón derecho en el almacén de datos y seleccione **Examinar archivos** .
- 2 Desplácese hasta el objeto cuyo nombre desea cambiar, ya sea un archivo o una carpeta.
- 3 Seleccione el objeto y haga clic en el icono **Rename selection** (Cambiar el nombre de la selección).
- 4 Especifique el nombre nuevo y haga clic en **OK** (Aceptar).

Expandir discos virtuales finos

Si creó un disco virtual en formato fino, puede convertir el disco fino a un disco virtual con formato de aprovisionamiento grueso.

Puede utilizar el explorador del almacén de datos para expandir el disco virtual.

Requisitos previos


- Asegúrese de que el almacén de datos donde se encuentra la máquina virtual tenga espacio suficiente.
- Asegúrese de que el disco virtual sea fino.
- Quite las instantáneas.
- Apague la máquina virtual.

Procedimiento

- 1 Desplácese hasta la carpeta del disco virtual que desea expandir.
 - a En vSphere Web Client, desplácese hasta la máquina virtual.
 - b Haga doble clic en la máquina virtual para mostrar la información.
 - c Haga clic en la pestaña **Objetos relacionados** y haga clic en **Almacenes de datos**.
Se enumera el almacén de datos que almacena los archivos de la máquina virtual.
 - d Seleccione el almacén de datos y haga clic en el icono **Desplazarse hasta el explorador de archivos en el almacén de datos**.

El explorador del almacén de datos muestra el contenido del almacén de datos.

- 2 Abra la carpeta de la máquina virtual y desplácese hasta el archivo del disco virtual que desea convertir.

El archivo tiene la extensión `.vmdk` y está marcado con el icono de disco virtual (.

- 3 Haga clic con el botón derecho en el archivo de disco virtual y seleccione **Inflar**.

Nota Es posible que la opción no esté disponible si el disco virtual es grueso o si la máquina virtual está en ejecución.

Resultados

El disco virtual inflado ocupa el espacio del almacén de datos completo que se le aprovisionó originalmente.

Desactivar los filtros de almacenamiento

Cuando se realizan operaciones de administración de almacenes de datos de VMFS, vCenter Server utiliza los filtros predeterminados de protección de almacenamiento. Los filtros ayudan a evitar daños en el almacenamiento al recuperar solo los dispositivos de almacenamiento que se pueden utilizar para una operación determinada. Los dispositivos que no son adecuados no se pueden seleccionar porque no se muestran. Para ver todos los dispositivos, puede desactivar los filtros.

Requisitos previos

Antes de cambiar los filtros de los dispositivos, consulte con el equipo de soporte de VMware. Puede desactivar los filtros solo si tiene otros métodos para evitar daños en los dispositivos.

Procedimiento

- 1 Desplácese hasta vCenter Server en el navegador de objetos de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Configuración**, haga clic en **Configuración avanzada** y, a continuación, en **Editar**.

4 Especifique el filtro que desea desactivar.

- a En el cuadro de texto **Nombre** en la parte inferior de la página, introduzca un nombre adecuado para el filtro.

Nombre	Descripción
config.vpxd.filter.vmfsFilter	Filtro de VMFS
config.vpxd.filter.rdmFilter	Filtro de RDM
config.vpxd.filter.sameHostsAndTranportsFilter	Filtro de mismo host y transportes
config.vpxd.filter.hostRescanFilter	Filtro de nueva exploración de host
Nota Si se desactiva este filtro, los hosts continúan realizando nuevas exploraciones cada vez que se presenta un nuevo LUN ante un host o un clúster.	

- b En el cuadro de texto **Valor**, escriba **False** para la clave especificada.

5 Haga clic en **Agregar** y, a continuación, en **Aceptar** para guardar los cambios.

No es necesario reiniciar el sistema vCenter Server.

Filtrado de almacenamiento

vCenter Server ofrece filtros de almacenamiento como ayuda para evitar daños o degradación del rendimiento en dispositivos de almacenamiento que pueden deberse a una utilización no admitida de esos dispositivos. Estos filtros están disponibles de forma predeterminada.

Tabla 16-4. Filtros de almacenamiento

Nombre del filtro	Descripción
config.vpxd.filter.vmfsFilter (Filtro de VMFS)	Filtra dispositivos de almacenamiento o LUN que un almacén de datos de VFMS ya utiliza en cualquier host administrado por vCenter Server. Los LUN no aparecen como candidatos para formatear con otro almacén de datos de VMFS o disponible para utilizarse como un RDM.
config.vpxd.filter.rdmFilter (Filtro de RDM)	Filtra los LUN que ya son utilizados como referencia por un RDM en cualquier host administrado por vCenter Server. Los LUN no aparecen como candidatos para formatearse con VMFS o para que un RDM diferente los utilice. Para que las máquinas virtuales accedan al mismo LUN, deben compartir el mismo archivo de asignación de RDM. Para obtener información sobre este tipo de configuración, consulte la documentación de <i>Administración de recursos de vSphere</i> .

Tabla 16-4. Filtros de almacenamiento (continuación)

Nombre del filtro	Descripción
config.vpxd.filter.sameHostsAndTransportFilter (Filtro de mismo host y transportes)	<p>Filtra los LUN que no cumplen los requisitos para ser utilizados como extensiones de almacenes de datos de VMFS debido a la incompatibilidad del host o del tipo de almacenamiento. Evita que agregue los siguientes LUN como extensiones:</p> <ul style="list-style-type: none"> ■ LUN no expuesto a todos los hosts que comparten el almacén de datos de VMFS original. ■ LUN que utilizan un tipo de almacenamiento diferente del que utiliza el almacén de datos de VMFS original. Por ejemplo, no puede agregar una extensión de canal de fibra a un almacén de datos de VMFS en un dispositivo de almacenamiento local.
config.vpxd.filter.hostRescanFilter (Filtro para volver a examinar el host)	<p>Vuelve a examinar y actualiza automáticamente almacenes de datos de VMFS después de realizar operaciones de administración de almacenes de datos. El filtro ayuda a contar con un panorama coherente de todos los almacenes de datos de VMFS en todos los hosts administrados por vCenter Server.</p> <p>Nota Si presenta un nuevo LUN a un host o un clúster, el host vuelve a examinarlo automáticamente, sin importar si el filtro para volver a examinar el host está activado o desactivado.</p>

Configurar reflejo de discos dinámico

Generalmente, no se puede usar un software de administración de volúmenes lógicos en máquinas virtuales para reflejar discos virtuales. Sin embargo, si las máquinas virtuales de Microsoft Windows admiten discos dinámicos, se pueden proteger las máquinas virtuales de una pérdida del dispositivo de almacenamiento no planificada reflejando los discos virtuales en dos LUN de SAN.

Requisitos previos

- Use una máquina virtual de Windows que admita discos dinámicos.
- Privilegios necesarios: **Avanzado**

Procedimiento

- 1 Cree una máquina virtual con dos discos virtuales.
Asegúrese de colocar los discos en distintos almacenes de datos.
- 2 Inicie sesión en la máquina virtual y configure los discos como discos reflejados dinámicos.
Consulte la documentación de Microsoft.
- 3 Una vez sincronizados los discos, apague la máquina virtual.

- 4 Cambie la configuración de la máquina virtual para permitir el uso de la creación de reflejo del disco dinámico.
 - a Haga clic con el botón derecho en la máquina virtual y seleccione **Edit Settings** (Editar configuración).
 - b Haga clic en la pestaña **VM Options** (Opciones de máquina virtual) y expanda el menú **Advanced** (Opciones avanzadas).
 - c Haga clic en **Edit Configuration** (Editar configuración) junto a Configuration Parameters (Parámetros de configuración).
 - d Haga clic en **Add Row** (Agregar fila) y agregue los parámetros siguientes:

Name (Nombre)	Valor
scsi#.returnNoConnectDuringAPD	True
scsi#.returnBusyOnNoConnectStatus	False

- e Haga clic en **OK** (Aceptar).

Recopilar información de diagnóstico para hosts ESXi en un dispositivo de almacenamiento

Durante un error del host, ESXi debe poder guardar la información de diagnóstico en una ubicación preconfigurada para fines de diagnóstico y soporte técnico.

Generalmente, durante la instalación de ESXi, se crea una partición en un dispositivo de almacenamiento local para recopilar información de diagnóstico, también conocida como volcado de núcleo de VMkernel. Este comportamiento predeterminado se puede anular si, por ejemplo, se utilizan dispositivos de almacenamiento compartido en lugar de almacenamiento local. A fin de evitar un formateo automático de los dispositivos locales, desconecte los dispositivos del host antes de instalar ESXi y encender el host por primera vez. Posteriormente, puede configurar una ubicación para recopilar información de diagnóstico en un dispositivo de almacenamiento local o remoto.

Al usar dispositivos de almacenamiento, se puede seleccionar una de dos opciones para configurar la recopilación en volcado de núcleo. Es posible usar una partición de diagnóstico preconfigurada de un dispositivo de almacenamiento o utilizar un archivo de un almacén de datos de VMFS.

■ [Configurar una partición de dispositivo como ubicación de volcado de núcleo](#)

Cree una partición de diagnóstico para el host ESXi.

■ [Configurar un archivo como ubicación de volcado de núcleo](#)

Si el tamaño de la partición para los volcados de memoria disponible no es suficiente, puede configurar ESXi para que genere el volcado de núcleo como un archivo.

Configurar una partición de dispositivo como ubicación de volcado de núcleo

Cree una partición de diagnóstico para el host ESXi.

Al crear una partición de diagnóstico, se aplican las consideraciones siguientes:

- No se puede crear una partición de diagnóstico en un LUN iSCSI al que se accede a través de un adaptador de iSCSI de hardware dependiente o de software. Para obtener más información sobre las particiones de diagnóstico con iSCSI, consulte [Recomendaciones generales de arranque desde SAN iSCSI](#).
- No se puede crear una partición de diagnóstico en un LUN de FCoE de software.
- A menos que utilice servidores sin discos, configure la partición de diagnóstico en el almacenamiento local.
- Cada host debe tener una partición de diagnóstico de 2,5 GB. Si varios hosts comparten una partición de diagnóstico en un LUN de SAN, la partición debe tener el tamaño suficiente para alojar los volcados de núcleo de todos los hosts.
- Si un host que utiliza una partición de diagnóstico compartida tiene errores, reinicie el host y extraiga los archivos de registro inmediatamente a continuación. De lo contrario, es posible que el segundo host que genere errores antes de recopilar los datos de diagnóstico del primer host no pueda guardar el volcado de núcleo.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic con el botón derecho en el host y seleccione **Add Diagnostic Partition** (Agregar partición de diagnóstico).

Si no ve esta opción, el host ya tiene una partición de diagnóstico.

- 3 Especifique el tipo de partición de diagnóstico.

Opción	Descripción
Private local (Local privado)	Crea la partición de diagnóstico en un disco local. Esta partición almacena información de errores solo para su host.
Private SAN storage (Almacenamiento de SAN privado)	Crea la partición de diagnóstico en un LUN de SAN no compartido. Esta partición almacena información de errores solo para su host.
Shared SAN storage (Almacenamiento de SAN compartido)	Crea la partición de diagnóstico en un LUN de SAN compartido. A esta partición se accede por varios hosts y puede almacenar información de errores para más de un host.

- 4 Haga clic en **Next** (Siguiente).
- 5 Seleccione el dispositivo que se utilizará para la partición de diagnóstico y haga clic en **Next** (Siguiente).
- 6 Revise la información de configuración de la partición y haga clic en **Finish** (Finalizar).

Comprobar una partición de diagnóstico

Use el comando `esxcli` para comprobar si hay una partición de diagnóstico establecida.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Enumere las particiones para comprobar que haya una partición de diagnóstico establecida.

```
esxcli --server=server_name system coredump partition list
```

Resultados

Si hay una partición de diagnóstico establecida, el comando muestra información sobre ella. De lo contrario, el comando muestra que no hay una partición activa y configurada.

Pasos siguientes

Para administrar la partición de diagnóstico del host, use los comandos de vCLI. Consulte *Ejemplos y conceptos de vSphere Command-Line Interface*.

Configurar un archivo como ubicación de volcado de núcleo

Si el tamaño de la partición para los volcados de memoria disponible no es suficiente, puede configurar ESXi para que genere el volcado de núcleo como un archivo.

Generalmente, durante la instalación de ESXi se crea una partición para los volcados de núcleo de 2,5 GB. En las actualizaciones de ESXi 5.0 y anteriores, la partición para los volcados de núcleo está limitada a 100 MB. En este tipo de actualización, el sistema puede crear un archivo para el volcado de núcleo en un almacén de datos de VMFS durante el proceso de arranque. Si no crea un archivo para el volcado de núcleo, es posible crear el archivo manualmente.

Nota iSCSI de software y FCoE de software no se admiten en las ubicaciones de los archivos para el volcado de núcleo.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- 1 Cree un archivo para el volcado de núcleo del almacén de datos de VMFS con el comando siguiente:

```
esxcli system coredump file add
```

El comando toma las opciones siguientes, pero no son obligatorias y pueden omitirse:

Opción	Descripción
--datastore -d <i>datastore_UUID or datastore_name</i>	Si no se proporciona, el sistema selecciona un almacén de datos de tamaño suficiente.
--file -f <i>file_name</i>	Si no se proporciona, el sistema especifica un nombre único para el archivo para el volcado de núcleo.
--size -s <i>file_size_MB</i>	Si no se proporciona, el sistema crea un archivo del tamaño adecuado para la memoria instalada en el host.

- 2 Compruebe que se haya creado el archivo:

```
esxcli system coredump file list
```

Puede ver un resultado similar al siguiente:

Path	Active	Configured	Size
-----	-----	-----	-----
/vmfs/volumes/52b021c3-.../vmkdump/test.dumpfile	false	false	104857600

- 3 Active el archivo para el volcado de núcleo para el host:

```
esxcli system coredump file set
```

El comando admite las siguientes opciones:

Opción	Descripción
--path -p	La ruta de acceso del archivo para el volcado de núcleo que se usará. Debe ser un archivo preasignado.
--smart -s	Esta marca se puede usar solo con --enable -e=true . Hará que el archivo se seleccione con el algoritmo de selección inteligente. Por ejemplo, esxcli system coredump file set --smart --enable true

- 4 Compruebe que el archivo para el volcado de núcleo esté activo y configurado:

```
esxcli system coredump file list
```

Un resultado similar al siguiente indica que el archivo para el volcado de núcleo está activo y configurado:

Path	Active	Configured	Size
-----	-----	-----	-----
/vmfs/volumes/52b021c3-.../vmkdump/test.dumpfile	True	True	104857600

Pasos siguientes

Para obtener información sobre otros comandos que puede usar para administrar los archivos para el volcado de núcleo, consulte la documentación de *Referencia de vSphere Command-Line Interface*.

Desactivar y eliminar un archivo de volcado de núcleo

Desactive un archivo de volcado de núcleo configurado y, si es necesario, quítelo del almacén de datos de VMFS.

Puede desactivar temporalmente el archivo de volcado de núcleo. Si no desea utilizar el archivo desactivado, puede quitarlo del almacén de datos de VMFS. Para quitar el archivo que no se ha desactivado, puede utilizar el comando `esxcli system coredump file remove` con la opción `--force | -F`.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- 1 Desactive el archivo de volcado de núcleo con el siguiente comando:

```
esxcli system coredump file set --unconfigure | -u
```

- 2 Quite el archivo del almacén de datos de VMFS:

```
esxcli system coredump file remove --file | -f file_name
```

El comando admite las siguientes opciones:

Opción	Descripción
<code>--file -f</code>	Especifique el nombre del archivo de volcado que desea quitar. Si no se especifica un nombre de archivo, se eliminará el archivo de volcado de núcleo configurado.
<code>--force -F</code>	Desactive y elimine la configuración del archivo de volcado que se desea quitar. Esta opción se requiere si el archivo aún no se desactivó y sigue activo.

Resultados

El archivo de volcado de núcleo se desactiva y se quita del almacén de datos de VMFS.

Comprobar la coherencia de los metadatos con VOMA

Use vSphere On-disk Metadata Analyser (VOMA) para identificar y solucionar incidentes de daños de metadatos que afectan los sistemas de archivos o volúmenes lógicos subyacentes.

Problema

Puede que necesite comprobar la consistencia de los metadatos de un sistema de archivos o un volumen lógico que hace copia de seguridad del sistema de archivos cuando experimenta problemas con diversas funcionalidades en un almacén de datos de VMFS o un recurso flash virtual. Por ejemplo, es posible que desee realizar una comprobación de metadatos si se produce uno de los siguientes casos:

- Experimenta interrupciones en el almacenamiento.
- Después de volver a construir RAID o realizar un reemplazo de disco.
- Ve errores de metadatos en el archivo `vmkernel.log`.
- No puede tener acceso a archivos en un VMFS.
- Ve que se informa sobre daños para un almacén de datos en las pestañas de eventos de vCenter Server.

Solución

Para comprobar la consistencia de datos, ejecute VOMA en la CLI de un host ESXi. Se puede usar VOMA para comprobar y solucionar problemas de inconsistencia de metadatos para un almacén de datos de VMFS o un recurso flash virtual. Para resolver errores que informe VOMA, consulte Soporte de VMware.

Siga estas directrices cuando use la herramienta VOMA:

- Asegúrese de que el almacén de datos de VMFS que analiza no se extienda en múltiples extensiones. Puede ejecutar VOMA solo para un almacén de datos de una sola extensión.
- Apague las máquinas virtuales que estén en ejecución o mígrelas a un almacén de datos diferente.

En el siguiente ejemplo se demuestra cómo usar VOMA para comprobar la consistencia de los metadatos de VMFS.

- 1 Obtenga el nombre y número de partición del dispositivo que hace la copia de seguridad del almacén de datos de VMFS que necesita comprobar.

```
#esxcli storage vmfs extent list
```

Las columnas Device Name (Nombre del dispositivo) y Partition (Partición) en el resultado identifican el dispositivo. Por ejemplo:

Volume Name	XXXXXXXXX	Device Name	Partition
1TB_VMFS5	XXXXXXXXX	naa.600508e000000000b367477b3be3d703	3

- 2 Ejecute VOMA para comprobar errores de VMFS.

Proporciona una ruta de acceso absoluta a la partición del dispositivo que realiza la copia de seguridad del almacén de datos de VMFS, y entregue un número de partición con el nombre del dispositivo. Por ejemplo:

```
# voma -m vmfs -f check -d /vmfs/devices/disks/
naa.600508e000000000b367477b3be3d703:3
```

El resultado enumera posibles errores. Por ejemplo, el siguiente resultado indica que la dirección de latido no es válida.

```
XXXXXXXXXXXXXXXXXXXXXXXXX
Phase 2: Checking VMFS heartbeat region
  ON-DISK ERROR: Invalid HB address
Phase 3: Checking all file descriptors.
Phase 4: Checking pathname and connectivity.
Phase 5: Checking resource reference counts.

Total Errors Found:          1
```

Entre las opciones de comandos que toma la herramienta VOMA se incluyen las siguientes.

Tabla 16-5. Opciones de comandos de VOMA

Opción de comando	Descripción
-m --module	<p>El módulo que se debe ejecutar:</p> <ul style="list-style-type: none"> ■ vmfs. Esta es una opción predeterminada. Puede comprobar almacenes de datos de VMFS3 y VMFS 5. Si especifica este módulo, también se realizan comprobaciones mínimas para LVM. ■ vmfsl. Comprueba los sistemas de archivos que realizan copias de seguridad de sistemas flash virtuales. ■ lvm. Comprueba volúmenes lógicos que realizan copias de seguridad de almacenes de datos de VMFS.
-f --func	<p>Funciones que se realizarán:</p> <ul style="list-style-type: none"> ■ query. Enumera funciones compatibles con el módulo. ■ check. Comprueba errores. ■ fix. Comprueba y soluciona errores.
-d --device	<p>Dispositivo o disco que se va a inspeccionar. Asegúrese de proporcionar la ruta de acceso absoluta hacia la partición del dispositivo que realiza la copia de seguridad del almacén de datos de VMFS. Por ejemplo, /vmfs/devices/disks/naa.00000000000000000000000000000000:1.</p>
-s --logfile	<p>Especifica el archivo de registro para mostrar los resultados.</p>
-v --version	<p>Muestra la versión de VOMA.</p>
-h --help	<p>Muestra el mensaje de ayuda para el comando VOMA.</p>

Configurar la memoria caché de bloque de puntero de VMFS

Se pueden usar parámetros de VMFS avanzados para configurar la memoria caché del bloque del puntero.

Conforme aumenta el tamaño de los archivos de la máquina virtual en los almacenes de datos de VMFS, la cantidad de bloques del puntero que usan estos archivos también aumenta. Los bloques del puntero se usan para dirigirse a bloques de archivo en archivos grandes de máquina virtual y discos virtuales en el almacén de datos de VMFS.

Es posible configurar los tamaños mínimo y máximo de la memoria caché de bloque del puntero en cada host ESXi. Cuando el tamaño de la memoria caché asignada al bloque del puntero se acerca al tamaño máximo configurado, un mecanismo de expulsión elimina algunas entradas del bloque del puntero de la memoria caché.

El tamaño máximo de la memoria caché de bloque del puntero debe estar basado en el tamaño de trabajo de todos los archivos de disco virtual abiertos que residen en los almacenes de datos de VMFS. Todos los almacenes de datos de VMFS en el host usan una sola memoria caché de bloque del puntero.

El valor mínimo se basa en la memoria mínima garantizada que el sistema puede asignar a la memoria caché. 1 TB de espacio de archivo abierto requiere aproximadamente 4 MB de memoria.

Para configurar los valores mínimo y máximo de la memoria caché del bloque del puntero, use el cuadro de diálogo **Configuración avanzada del sistema** de vSphere Web Client.

Tabla 16-6. Parámetros avanzados para regular la memoria caché de bloque del puntero

Parámetro	Valores	Descripción
VMFS3.MaxAddressableSpaceTB	El valor predeterminado es 32 (en TB).	Tamaño máximo de todos los archivos abiertos que la memoria caché de VMFS admite antes de comenzar la expulsión.
VMFS3.MinAddressableSpaceTB	El valor predeterminado es 10 (en TB).	Tamaño mínimo de todos los archivos abiertos que la memoria caché de VMFS garantiza admitir.

Puede usar el comando `esxcli storage vmfs pbcache` para obtener información acerca del tamaño de la memoria caché del bloque del puntero y otras estadísticas. Esta información lo ayuda a ajustar los tamaños mínimo y máximo de la memoria caché del bloque del puntero, para que pueda obtener el máximo rendimiento.

Establecer atributos de host avanzados

Puede establecer atributos avanzados para un host.

Precaución No se admite la modificación de opciones avanzadas a menos que el soporte técnico de VMware o un artículo de la base de conocimientos le otorgue instrucciones para hacerlo. En todos los otros casos, no se admite el cambio de estas opciones. En la mayoría de los casos, la configuración predeterminada proporciona resultados óptimos.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Administrar** y en **Configuración**.
- 3 En **Sistema**, haga clic en **Configuración avanzada del sistema**.
- 4 En Configuración avanzada, seleccione el elemento apropiado.
- 5 Haga clic en el botón **Editar** para editar el valor.
- 6 Haga clic en **Aceptar**.

Obtener información para la memoria caché de bloque del puntero de VMFS

Puede obtener información sobre el uso de la memoria caché de bloque del puntero de VMFS. Esta información ayuda a comprender cuánto espacio consume la memoria caché de bloque del puntero. También puede identificar si es necesario ajustar los tamaños mínimos y máximos de la memoria caché de bloque del puntero.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Para obtener o restablecer las estadísticas de la memoria caché de bloque del puntero, use el siguiente comando:

```
esxcli storage vmfs pbcache
```

Opción	Descripción
get	Obtener estadísticas de la memoria caché de bloque del puntero de VMFS.
reset	Restablecer las estadísticas de la memoria caché de bloque del puntero de VMFS.

Ejemplo: Obtención de estadísticas de la memoria caché de bloque del puntero

```
#esxcli storage vmfs pbcache get
Cache Capacity Miss Ratio: 0 %
Cache Size: 0 MiB
Cache Size Max: 132 MiB
Cache Usage: 0 %
Cache Working Set: 0 TiB
Cache Working Set Max: 32 TiB
Vmfs Heap Overhead: 0 KiB
Vmfs Heap Size: 23 MiB
Vmfs Heap Size Max: 256 MiB
```


Descripción de múltiples rutas y conmutación por error

17

Para mantener una conexión constante entre un host y su almacenamiento, ESXi admite múltiples rutas. La habilitación de múltiples rutas es una técnica que permite utilizar más de una ruta de acceso física que transfiere datos entre el host y un dispositivo de almacenamiento externo.

En caso de error en cualquier elemento de la red SAN, como un adaptador, conmutador o cable, ESXi puede cambiar a otra ruta de acceso física, que no utiliza el componente con errores. Este proceso de conmutación de ruta de acceso para evitar componentes con errores se conoce como conmutación por error de ruta de acceso.

Además de la conmutación por error de ruta de acceso, las múltiples rutas proporcionan equilibrio de carga. El equilibrio de carga es el proceso de distribuir las cargas de E/S a través de varias rutas de acceso físicas. El equilibrio de carga reduce o elimina los cuellos de botella potenciales.

Nota La E/S de la máquina virtual podría retrasarse hasta sesenta segundos mientras tiene lugar la conmutación por error de ruta de acceso. Estos retrasos permiten que la SAN establezca su configuración después de los cambios de topología. En general, los retrasos de E/S pueden ser más largos en matrices activas-pasivas y más cortos en matrices activas-activas.

Este capítulo incluye los siguientes temas:

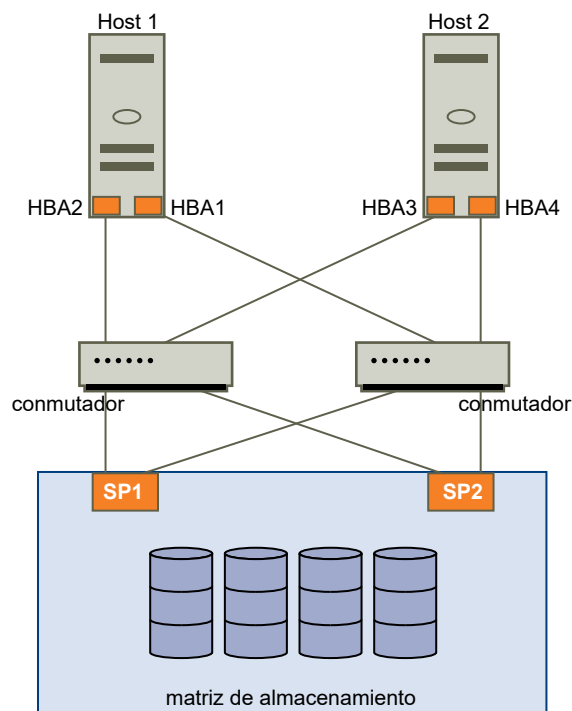
- [Conmutación por error con canal de fibra](#)
- [Conmutación por error basada en host con iSCSI](#)
- [Conmutación por error basada en matrices con iSCSI](#)
- [Conmutación por error de rutas de acceso y máquinas virtuales](#)
- [Administrar varias rutas de acceso](#)
- [Módulo de múltiples rutas de VMware](#)
- [Explorar y notificar rutas de acceso](#)
- [Administrar rutas de acceso de almacenamiento y complementos de múltiples rutas](#)
- [Colas de programación de E/S de máquinas virtuales](#)

Conmutación por error con canal de fibra

Para admitir múltiples rutas, por lo general el host tiene dos o más HBA disponibles. Esta configuración complementa la configuración de múltiples rutas SAN que generalmente ofrece uno o dos conmutadores en el tejido SAN y uno o dos procesadores de almacenamiento en el propio dispositivo de la matriz de almacenamiento.

En la siguiente ilustración, se conectan varias rutas físicas a cada servidor con el dispositivo de almacenamiento. Por ejemplo, si HBA1 o el enlace entre HBA1 y el conmutador de FC genera errores, HBA2 asume el control y permite la conexión entre el servidor y el conmutador. El proceso mediante el cual un HBA asume el control en lugar de otro se denomina conmutación por error HBA.

Figura 17-1. Múltiples rutas y conmutación por error con el canal de fibra



De manera similar, si SP1 genera errores o los enlaces entre SP1 y los conmutadores se interrumpen, SP2 asume el control y permite la conexión entre el conmutador y el dispositivo de almacenamiento. Este proceso se denomina conmutación por error SP. VMware ESXi admite ambas conmutaciones por error HBA y SP con su capacidad de múltiples rutas.

Conmutación por error basada en host con iSCSI

Al configurar el host ESXi para múltiples rutas y conmutación por error, puede utilizar varios HBA iSCSI o varias NIC, según el tipo de adaptadores de iSCSI en el host.

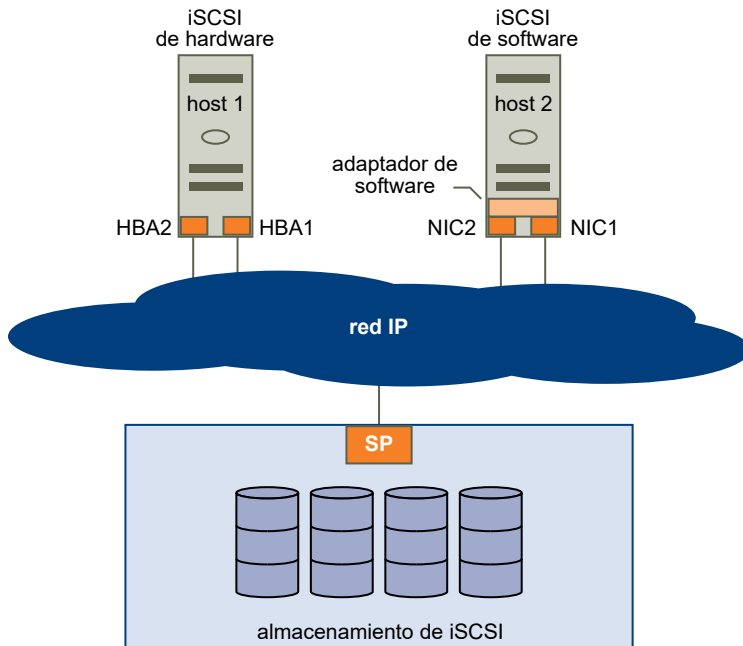
Para obtener información sobre los diferentes tipos de adaptadores de iSCSI, consulte [Iniciadores iSCSI](#).

Cuando se utiliza la funcionalidad de múltiples rutas, se aplican consideraciones específicas.

- ESXi no admite múltiples rutas cuando combina un adaptador de hardware independiente con adaptadores de iSCSI de software o de iSCSI dependientes en el mismo host.
- Se admite habilitar múltiples rutas entre adaptadores de software y dependientes en el mismo host.
- En hosts diferentes, se pueden combinar adaptadores dependientes e independientes.

En la siguiente ilustración se muestran opciones de configuración de múltiples rutas posibles con diferentes tipos de iniciadores iSCSI.

Figura 17-2. Conmutar por error de rutas de acceso con base en host



Conmutación por error con iSCSI de hardware

Con iSCSI de hardware, el host generalmente tiene dos o más adaptadores de iSCSI de hardware disponibles desde los cuales puede establecerse comunicación con el sistema de almacenamiento a través de uno o varios conmutadores. De manera alternativa, la configuración puede incluir un adaptador y dos procesadores de almacenamiento, para que el adaptador pueda utilizar una ruta de acceso diferente para comunicarse con el sistema de almacenamiento.

En la ilustración de la conmutación por error de rutas de acceso basada en host, Host1 tiene dos adaptadores de iSCSI de hardware, HBA1 y HBA2, que ofrecen dos rutas de acceso físicas al sistema de almacenamiento. Los complementos de múltiples rutas en el host, ya se trate de NMP del VMkernel o de MPP de terceros, pueden acceder a las rutas de acceso de forma predeterminada y supervisar el estado de cada ruta de acceso física. Si, por ejemplo, HBA1 o el vínculo entre HBA1 y la red generan errores, los complementos de múltiples rutas pueden conmutar la ruta de acceso por HBA2.

Conmutación por error con iSCSI de software

Con iSCSI de software, como se muestra en Host2 de la ilustración de la conmutación por error de rutas de acceso basada en host, se pueden utilizar varias NIC que ofrecen funcionalidades de conmutación por error y equilibrio de carga para conexiones iSCSI entre el host y los sistemas de almacenamiento.

Para esta configuración, debido a que los complementos de múltiples rutas no tienen acceso directo a las NIC físicas en el host, en primer lugar se debe conectar cada NIC física a un puerto VMkernel distinto. A continuación, asocie todos los puertos VMkernel con el iniciador iSCSI de software mediante una técnica de enlace de puertos. En consecuencia, cada puerto VMkernel conectado a una NIC distinta se convierte en una ruta de acceso diferente que pueden utilizar la pila de almacenamiento iSCSI y sus complementos de múltiples rutas con reconocimiento de almacenamiento.

Para obtener información sobre cómo configurar múltiples rutas para iSCSI de software, consulte [Configurar la red de iSCSI](#).

Conmutación por error basada en matrices con iSCSI

Algunos sistemas de almacenamiento iSCSI administran el uso de rutas de acceso de sus puertos de forma automática y transparente para ESXi.

Cuando se utiliza uno de estos sistemas de almacenamiento, el host no ve varios puertos en el almacenamiento y no puede elegir el puerto de almacenamiento al que se conecta. Estos sistemas tienen una sola dirección de puerto virtual que el host utiliza para comunicarse inicialmente.

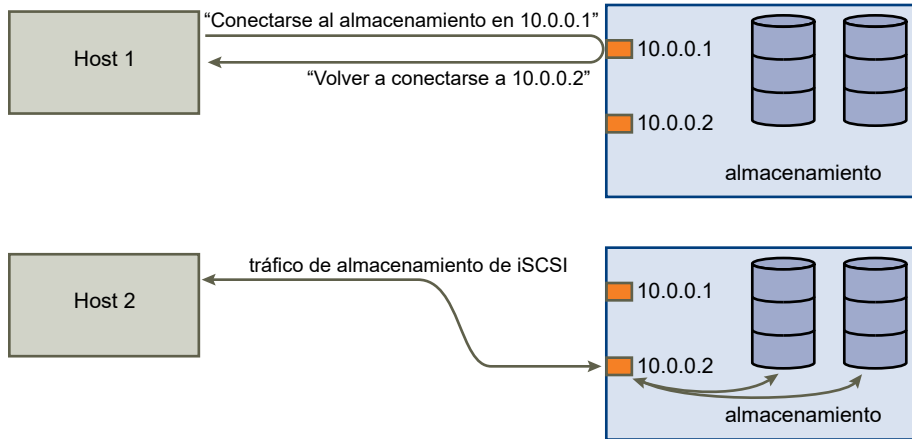
Durante esta comunicación inicial, el sistema de almacenamiento puede redirigir el host para comunicarse con otro puerto en el sistema de almacenamiento. Los iniciadores iSCSI en el host obedecen a esta solicitud de reconexión y se conectan con un puerto distinto en el sistema. El sistema de almacenamiento utiliza esta técnica para propagar la carga en los puertos disponibles.

Si el host ESXi pierde la conexión con uno de estos puertos, intenta automáticamente reconectarse con el puerto virtual del sistema de almacenamiento, y debería redirigirse a un puerto activo y utilizable. Esta reconexión y redirección sucede rápidamente, y por lo general no interrumpe las máquinas virtuales en ejecución. Estos sistemas de almacenamiento también pueden solicitar que los iniciadores iSCSI se reconecten al sistema para cambiar el puerto de almacenamiento al que están conectados. Esto permite un uso más eficaz de los diversos puertos.

La ilustración de la redirección de puertos muestra un ejemplo de la redirección de puertos. El host intenta conectarse al puerto virtual 10.0.0.1. El sistema de almacenamiento redirige esta solicitud a 10.0.0.2. El host se conecta con 10.0.0.2 y utiliza ese puerto para la comunicación de E/S.

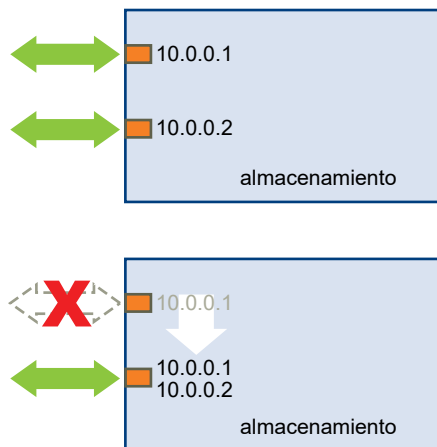
Nota El sistema de almacenamiento no siempre redirige las conexiones. El puerto en 10.0.0.1 también podría utilizarse para tráfico.

Figura 17-3. Redirigir puertos



Si el puerto en el sistema de almacenamiento que actúa como puerto virtual deja de estar disponible, el sistema de almacenamiento reasigna la dirección del puerto virtual a otro puerto en el sistema. La reasignación de puertos muestra un ejemplo de este tipo de reasignación. En este caso, el puerto virtual 10.0.0.1 deja de estar disponible y el sistema de almacenamiento reasigna la dirección IP del puerto virtual a un puerto diferente. El segundo puerto responde a ambas direcciones.

Figura 17-4. Reasignar puertos



Con este tipo de conmutación por error basada en matrices, puede tener varias rutas de acceso al almacenamiento solo si utiliza varios puertos en el host ESXi. Estas rutas de acceso son activas-activas. Para obtener información adicional, consulte [Administrar sesiones de iSCSI](#).

Conmutación por error de rutas de acceso y máquinas virtuales

La conmutación por error de la ruta de acceso ocurre cuando la ruta de acceso activa a un LUN se cambia de una ruta de acceso a otra, generalmente debido al error de un componente de la SAN en la ruta de acceso actual.

Cuando una ruta de acceso genera errores, la E/S de almacenamiento puede pausarse durante 30 a 60 segundos hasta que el host determine que el vínculo no está disponible y complete la conmutación por error. Si intenta mostrar el host, sus dispositivos de almacenamiento o sus adaptadores, es posible que la operación parezca atascarse. Es posible que parezca que las máquinas virtuales con los discos instalados en la SAN no responden. Una vez completada la conmutación por error, E/S reanuda sus actividades normalmente y las máquinas virtuales siguen ejecutándose.

Sin embargo, cuando una conmutación por error toma mucho tiempo para completarse, es posible que una máquina virtual de Windows interrumpa la E/S y eventualmente ocurra un error. Para evitar un error, configure el valor de tiempo de espera de disco para la máquina virtual de Windows en 60 segundos, como mínimo.

Establecer el tiempo de espera en un sistema operativo invitado Windows

Aumente el valor de tiempo de espera de disco estándar en un sistema operativo invitado de Windows para evitar interrupciones durante una conmutación por error de la ruta de acceso.

Este procedimiento explica cómo cambiar el valor de tiempo de espera con el registro de Windows.

Requisitos previos

Realice una copia de seguridad del registro de Windows.

Procedimiento

- 1 Seleccione **Start (Inicio) > Run (Ejecutar)**.
- 2 Escriba **regedit.exe** y haga clic en **OK (Aceptar)**.
- 3 En la vista de jerarquía del panel izquierdo, haga doble clic en **HKEY_LOCAL_MACHINE > System (Sistema) > CurrentControlSet (Conjunto de controles actual) > Services (Servicios) > Disk (Disco)**.
- 4 Haga doble clic en **TimeOutValue** (Valor de tiempo de espera).
- 5 Configure los datos de valor a 0x3c (hexadecimal) o 60 (decimal) y haga clic en **OK (Aceptar)**.
Luego de hacer este cambio, Windows espera 60 segundos como mínimo para que se completen las operaciones de disco demoradas antes de generar errores.
- 6 Reinicie el sistema operativo invitado para que se aplique el cambio.

Administrar varias rutas de acceso

Para administrar múltiples rutas de almacenamiento, ESXi utiliza la recopilación de Storage APIs, también denominada Pluggable Storage Architecture (PSA). PSA es un marco modular abierto que coordina la operación simultánea de varios complementos de múltiples rutas (MPP). PSA permite que los desarrolladores de software de terceros diseñen sus propias técnicas de equilibrio

de la carga y mecanismos de conmutación por error para una matriz de almacenamiento en particular, e insertar el código directamente en la ruta de acceso de E/S de almacenamiento de ESXi.

Los temas que tratan la administración de rutas de acceso utilizan los acrónimos siguientes:

Tabla 17-1. Acrónimos de múltiples rutas

Acrónimo	Definición
PSA	Pluggable Storage Architecture
NMP	Native Multipathing Plug-In (Complemento de múltiples rutas nativo). Módulo de múltiples rutas de VMware genérico.
PSP	Path Selection Plug-In (Complemento de selección de rutas de acceso), también denominado directiva de selección de rutas de acceso. Controla la selección de rutas de acceso de un dispositivo determinado.
SATP	Storage Array Type Plug-In (Complemento de tipo de matriz de almacenamiento), también denominado directiva de tipo de matriz de almacenamiento. Controla la conmutación por error de rutas de acceso de una matriz de almacenamiento determinada.

El complemento de múltiples rutas VMkernel que ESXi proporciona de forma predeterminada es el complemento de múltiples rutas nativo (NMP) de VMware. El NMP es un módulo extensible que administra subcomplementos. Existen dos tipos de subcomplementos de NMP, complementos de tipo de matriz de almacenamiento (SATP) y complementos de selección de ruta de acceso (PSP). Los SATP y PSP pueden ser incorporados y proporcionados por VMware, o bien pueden ser proporcionados por un tercero.

Si se necesita una funcionalidad de múltiples rutas, un tercero también puede proporcionar un MPP para ejecutarlo además del NMP predeterminado, o bien para reemplazarlo.

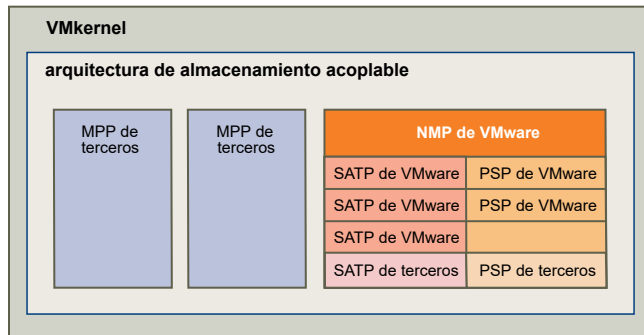
Cuando coordina el NMP de VMware y cualquier MPP de terceros instalado, PSA realiza las tareas siguientes:

- Carga y descarga complementos de múltiples rutas.
- Oculta las especificaciones de máquinas virtuales de un complemento en particular.
- Enruta las solicitudes de E/S de un dispositivo lógico específico al MPP que administra ese dispositivo.
- Controla la cola de E/S a los dispositivos lógicos.
- Implementa el uso compartido del ancho de banda de dispositivos lógicos entre máquinas virtuales.
- Controla la cola de E/S a los HBA de almacenamiento físico.
- Controla la detección y eliminación de rutas de acceso físicas.

- Proporciona estadísticas de E/S de rutas de acceso físicas y dispositivos lógicos.

Como muestra la ilustración de Pluggable Storage Architecture, varios MPP de terceros pueden ejecutarse en paralelo con el NMP de VMware. Una vez instalados, los MPP de terceros reemplazan el comportamiento del NMP y toman el control total de las operaciones de conmutación por error y equilibrio de la carga de la ruta de acceso de los dispositivos de almacenamiento especificados.

Figura 17-5. Pluggable Storage Architecture



Los módulos de múltiples rutas realizan las operaciones siguientes:

- Administran la notificación y la anulación de notificación de una ruta de acceso física.
- Administran la creación, el registro y la anulación de registro de los dispositivos lógicos.
- Asocian rutas de acceso físicas con dispositivos lógicos.
- Admiten la detección y corrección de errores de rutas de acceso.
- Procesan solicitudes de E/S para dispositivos lógicos:
 - Seleccionan la ruta de acceso física óptima para la solicitud.
 - Según el dispositivo de almacenamiento, realizan acciones específicas necesarias para controlar los errores de rutas de acceso y los reintentos de comandos de E/S.
- Admiten tareas de administración, como el restablecimiento de dispositivos lógicos.

Módulo de múltiples rutas de VMware

De forma predeterminada, ESXi proporciona un módulo de múltiples rutas extensible denominado complemento de múltiples rutas nativo (NMP).

Por lo general, el NMP de VMware admite todas las matrices de almacenamiento enumeradas en el HCL de almacenamiento de VMware y proporciona un algoritmo de selección de rutas de acceso predeterminado en función del tipo de matriz. El NMP asocia un conjunto de rutas de acceso físicas con un dispositivo de almacenamiento específico, o LUN. Los detalles específicos de manejar la conmutación por error de la ruta de acceso para una matriz de almacenamiento

determinada se delegan a un complemento de tipo de matriz de almacenamiento (SATP). A los detalles específicos para determinar qué ruta de acceso física se utiliza para emitir una solicitud de E/S a un dispositivo de almacenamiento los maneja un complemento de selección de rutas de acceso (PSP). Los SATP y PSP son subcomplementos dentro del módulo de NMP.

Con ESXi, el SATP adecuado para la matriz utilizada se instala automáticamente. No es necesario que obtenga o descargue ningún SATP.

SATP de VMware

Los complementos de tipo de matriz de almacenamiento (SATP) se ejecutan junto con NMP de VMware y son responsables de operaciones específicas de matriz.

ESXi ofrece un SATP para cada tipo de matriz que VMware admite. También proporciona SATP predeterminados que admiten matrices de almacenamiento ALUA y activo-activo no específico, y el SATP local para dispositivos conectados directamente. Cada SATP incluye características especiales de un cierto tipo de matriz de almacenamiento y puede realizar las operaciones específicas de matriz necesarias para detectar el estado de la ruta de acceso y activar una ruta de acceso inactiva. Como resultado, el módulo NMP mismo puede funcionar con varias matrices de almacenamiento sin tener que estar pendiente de las especificaciones del dispositivo de almacenamiento.

Una vez que el NMP determina qué SATP usar para un dispositivo de almacenamiento específico y asocia el SATP con las rutas de acceso físicas para ese dispositivo de almacenamiento, el SATP implementa las tareas que incluyen las siguientes:

- Supervisa el estado de cada ruta de acceso física.
- Informa los cambios de estado de cada ruta de acceso física.
- Realiza acciones específicas de matriz necesarias para la conmutación por error del almacenamiento. Por ejemplo, en el caso de dispositivos activo-pasivos, puede activar las rutas de acceso pasivas.

PSP de VMware

Los complementos de selección de ruta de acceso (PSP) son subcomplementos del NMP de VMware y son los responsables de elegir una ruta de acceso física para las solicitudes de E/S.

El NMP de VMware asigna una PSP predeterminado para cada dispositivo lógico basado en el SATP asociado con las rutas de acceso físicas a ese dispositivo. Es posible anular la PSP predeterminada. Para obtener información, consulte [Explorar y notificar rutas de acceso](#).

De forma predeterminada, el NMP de VMware es compatible con las PSP siguientes:

VMW_PSP_MRU

El host selecciona la ruta de acceso que utilizó más recientemente. Cuando la ruta de acceso deja de estar disponible, el host selecciona una ruta de acceso alternativa. El host no revierte a la ruta de acceso original cuando esa ruta vuelve a estar disponible. No hay configuración

de ruta de acceso preferida con la directiva MRU. MRU es la directiva predeterminada en la mayoría de los dispositivos de almacenamiento activos-pasivos.

La capacidad de clasificación de VMW_PSP_MRU permite asignar una clasificación a rutas de acceso individuales. Para establecer clasificaciones a rutas de acceso individuales, utilice el comando `esxcli storage nmp psp generic pathconfig set`. Para obtener información detallada, consulte el artículo de la base de conocimientos de VMware en <http://kb.vmware.com/kb/2003468>.

La directiva se muestra en el cliente como la directiva de selección de ruta de acceso Most Recently Used (Utilizada recientemente) (VMware).

VMW_PSP_FIXED

El host utiliza la ruta de acceso preferida designada, si se ha configurado. En caso contrario, selecciona la primera ruta de acceso de trabajo detectada en la hora de arranque del sistema. Si desea que el host utilice una ruta de acceso preferida en particular, especifíquela manualmente. La directiva fija es la predeterminada para la mayoría de los dispositivos de almacenamiento activos-activos.

Nota Si el host utiliza una ruta de acceso preferida predeterminada y el estado de la ruta de acceso pasa a ser Dead (Inactiva), se selecciona una ruta de acceso nueva como preferida. Sin embargo, si designa explícitamente la ruta de acceso preferida, seguirá siendo preferida incluso si no puede accederse a ella.

Se muestra en el cliente como la directiva de selección de ruta de acceso Fixed (Fija) (VMware).

VMW_PSP_RR

El host utiliza un algoritmo de selección automática de rutas de acceso que rota por todas las rutas de acceso activas al conectarse a matrices activas-pasivas, o por todas las rutas de acceso disponibles al conectarse a matrices activas-activas. RR es la opción predeterminada para una serie de matrices, y puede utilizarse con matrices activas-activas y activas-pasivas para implementar el equilibrio de carga entre rutas de acceso para diferentes LUN.

Se muestra en el cliente como la directiva de selección de ruta de acceso round robin (VMware).

Flujo NMP de E/S de VMware

Cuando una máquina virtual emite una solicitud de E/S a un dispositivo de almacenamiento administrado por el NMP, se lleva a cabo el proceso siguiente.

- 1 El NMP llama al PSP asignado a este dispositivo de almacenamiento.
- 2 El PSP selecciona una ruta de acceso física adecuada en la cual se pueda emitir la E/S.
- 3 El NMP emite la solicitud de E/S en la ruta de acceso seleccionada por el PSP.
- 4 Si la operación de E/S se realiza correctamente, el NMP informa la finalización.

- 5 De lo contrario, el NMP llama al SATP adecuado.
- 6 El SATP interpreta los errores de comando de E/S y, cuando corresponde, activa las rutas de acceso inactivas.
- 7 Se le pide al PSP que seleccione la nueva ruta de acceso en la cual se pueda emitir la E/S.

Explorar y notificar rutas de acceso

Cuando inicia el host ESXi o vuelve a examinar el adaptador de almacenamiento, el host detecta todas las rutas de acceso físicas hacia los dispositivos de almacenamiento disponibles para el host. En función de un conjunto de reglas de notificación, el host determina qué complemento de múltiples rutas (MPP) debe notificar las rutas de acceso hacia un dispositivo en particular y asumir la responsabilidad de administrar la compatibilidad con múltiples rutas para el dispositivo.

De forma predeterminada, el host realiza una evaluación periódica de las rutas de acceso cada 5 minutos, lo que ocasiona que el MPP notifique las rutas de acceso no notificadas.

Las reglas de notificación son numeradas. Para cada ruta de acceso física, el host ejecuta todas las reglas de notificación comenzando por el número más bajo. Los atributos de la ruta de acceso física se comparan con la especificación de la ruta de acceso en una regla de notificación. Si se produce una coincidencia, el host asigna el MPP especificado en la regla de notificación para que administre la ruta de acceso física. Esto continúa hasta que los MPP correspondientes notifiquen todas las rutas de acceso físicas, sea con complementos de múltiples rutas de terceros o con el complemento de múltiples rutas nativo (NMP).

Para las rutas de acceso administradas por el módulo de NMP, se aplica un segundo conjunto de reglas de notificación. Estas reglas determinan qué complemento de tipo de matriz de almacenamiento (SATP) debe utilizarse para administrar las rutas de acceso para un tipo específico de matriz de almacenamiento, y qué complemento de selección de rutas de acceso (PSP) debe utilizarse para cada dispositivo de almacenamiento.

Utilice vSphere Web Client para ver qué SATP y qué PSP está utilizando el host para un dispositivo de almacenamiento específico y el estado de todas las rutas de acceso disponibles de este dispositivo de almacenamiento. Si es necesario, puede cambiar el PSP predeterminado de VMware a través del cliente. Para cambiar el SATP predeterminado, debe modificar las reglas de notificación con la CLI de vSphere.

Puede encontrar información sobre la modificación de las reglas de notificación en [Administrar rutas de acceso de almacenamiento y complementos de múltiples rutas](#).

Para obtener más información sobre los comandos disponibles para administrar PSA, consulte *Introducción a vSphere Command-Line Interface*.

Para acceder a una lista completa de matrices de almacenamiento y sus correspondientes SATP y PSP, consulte la sección de referencia de modelos de matrices SAN de *Guía de compatibilidad de vSphere*.

Ver información de rutas de acceso

Puede revisar la directiva de tipo de matriz de almacenamiento (SATP) y la directiva de selección de rutas de acceso (PSP) que el host ESXi utiliza para un determinado dispositivo de almacenamiento, además del estado de todas las rutas de acceso disponibles para este dispositivo de almacenamiento. Puede acceder a la información de la ruta de acceso desde las vistas Datastores (Almacenes de datos) y Devices (Dispositivos). En los almacenes de datos, debe revisar las rutas de acceso que conectan al dispositivo donde está implementado el almacén de datos.

La información de la ruta de acceso incluye la SATP asignada para administrar el dispositivo, la PSP, una lista de rutas de acceso y el estado de cada ruta de acceso. Puede aparecer la siguiente información sobre el estado de la ruta de acceso:

Active

Rutas de acceso disponibles para emitir E/S a un LUN. Las rutas de trabajo que actualmente se utilizan para transferir datos se marcan como activas (E/S).

En espera

Si se produce un error en las rutas de acceso activas, la ruta de acceso puede entrar en funcionamiento rápidamente y utilizarse para E/S.

Deshabilitada

La ruta de acceso está deshabilitada y no pueden transferirse datos.

Inactiva

El software no pudo conectarse al disco a través de esta ruta de acceso.

Si utiliza la directiva de rutas de acceso **Fixed** (Fija), podrá ver cuál es la ruta de acceso preferida. La ruta de acceso preferida se marca con un asterisco (*) en la columna Preferred (Preferida).

También aparece el nombre de cada ruta de acceso. El nombre incluye parámetros que describen la ruta de acceso: identificador del adaptador, identificador de destino e identificador del dispositivo. Por lo general, el nombre de una ruta de acceso tiene un formato similar al siguiente:

```
fc.adapterID-fc.targetID-naa.deviceID
```

Nota Cuando se utiliza el editor de perfiles de host para editar las rutas de acceso, se debe especificar los tres parámetros que describen la ruta: identificador del adaptador, identificador de destino e identificador del dispositivo.

Ver las rutas de acceso de los almacenes de datos

Revise las rutas de acceso que se conectan a los dispositivos de almacenamiento que respaldan a los almacenes de datos.

Procedimiento

- 1 En el navegador de vSphere Web Client, seleccione **Listas de inventario global > Almacenes de datos**.
- 2 Haga clic en el almacén de datos para mostrar la información.
- 3 Haga clic en la pestaña **Configurar**.
- 4 Haga clic en **Connectivity and Multipathing** (Conectividad y habilitación de múltiples rutas).
- 5 Si el almacén de datos es compartido, seleccione un host para ver los detalles de múltiples rutas para los dispositivos.
- 6 En Multipathing Details (Detalles de múltiples rutas), revise las directivas de múltiples rutas y las rutas de acceso del dispositivo de almacenamiento que respalda al almacén de datos.

Ver rutas de acceso de dispositivos de almacenamiento

Visualice las directivas de múltiples rutas que utiliza el host para un dispositivo de almacenamiento específico y el estado de todas las rutas de acceso disponibles para este dispositivo de almacenamiento.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Storage Devices** (Dispositivos de almacenamiento).
- 4 Seleccione el dispositivo de almacenamiento cuyas rutas de acceso desea ver.
- 5 Haga clic en la pestaña **Properties** (Propiedades) y revise los detalles en Multipathing Policies (Directivas de múltiples rutas).
- 6 Haga clic en la pestaña **Paths** (Rutas de acceso) para revisar todas las rutas de acceso disponibles para el dispositivo de almacenamiento.

Establecer una directiva de selección de rutas de acceso

Para cada dispositivo de almacenamiento, el host ESXi establece la directiva de selección de rutas de acceso según las reglas de notificación.

De forma predeterminada, VMware admite las siguientes directivas de selección de rutas de acceso. Si tiene una PSP de terceros instalada en el host, su directiva también aparecerá en la lista.

Fixed (Fija) (VMware)

El host utiliza la ruta de acceso preferida designada, si se ha configurado. En caso contrario, selecciona la primera ruta de acceso de trabajo detectada en la hora de arranque del sistema. Si desea que el host utilice una ruta de acceso preferida en particular, especifíquela

manualmente. La directiva fija es la predeterminada para la mayoría de los dispositivos de almacenamiento activos-activos.

Nota Si el host utiliza una ruta de acceso preferida predeterminada y el estado de la ruta de acceso pasa a ser Dead (Inactiva), se selecciona una ruta de acceso nueva como preferida. Sin embargo, si designa explícitamente la ruta de acceso preferida, seguirá siendo preferida incluso si no puede accederse a ella.

Most Recently Used (Utilizados más recientemente) (VMware)

El host selecciona la ruta de acceso que utilizó más recientemente. Cuando la ruta de acceso deja de estar disponible, el host selecciona una ruta de acceso alternativa. El host no revierte a la ruta de acceso original cuando esa ruta vuelve a estar disponible. No hay configuración de ruta de acceso preferida con la directiva MRU. MRU es la directiva predeterminada en la mayoría de los dispositivos de almacenamiento activos-pasivos.

Round robin (VMware)

El host utiliza un algoritmo de selección automática de rutas de acceso que rota por todas las rutas de acceso activas al conectarse a matrices activas-pasivas, o por todas las rutas de acceso disponibles al conectarse a matrices activas-activas. RR es la opción predeterminada para una serie de matrices, y puede utilizarse con matrices activas-activas y activas-pasivas para implementar el equilibrio de carga entre rutas de acceso para diferentes LUN.

Cambiar la directiva de selección de rutas de acceso

Generalmente, no es necesario cambiar la configuración de múltiples rutas predeterminada que usa el host para un dispositivo de almacenamiento específico. Sin embargo, si se desean hacer cambios, se puede utilizar el cuadro de diálogo **Edit Multipathing Policies** (Editar directivas de múltiples rutas) para modificar una directiva de selección de ruta de acceso y especificar la ruta de acceso preferida de la directiva Fixed (Fija). También se puede utilizar este cuadro de diálogo para cambiar las múltiples rutas de los extremos de protocolo basado en SCSI.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Storage Devices** (Dispositivos de almacenamiento) o **Protocol Endpoints** (Extremos de protocolo).
- 4 Seleccione el elemento cuyas rutas de acceso desea cambiar y haga clic en la pestaña **Properties** (Propiedades).
- 5 En Multipathing Policies (Directivas de múltiples rutas), haga clic en **Edit Multipathing** (Editar múltiples rutas).

6 Seleccione una directiva de ruta de acceso.

De forma predeterminada, VMware admite las siguientes directivas de selección de rutas de acceso. Si tiene una PSP de terceros instalada en el host, su directiva también aparecerá en la lista.

- Fixed (Fija) (VMware)
- Most Recently Used (Utilizados más recientemente) (VMware)
- Round robin (VMware)

7 Para la directiva fija, especifique la ruta de acceso preferida.

8 Haga clic en **OK** (Aceptar) para guardar la configuración y salir del cuadro de diálogo.

Deshabilitar rutas de acceso de almacenamiento

Las rutas de acceso se pueden deshabilitar temporalmente para realizar mantenimiento o por otras razones.

Puede deshabilitar una ruta de acceso desde el panel Paths (Rutas de acceso). Existen varias formas de acceder al panel Paths (Rutas de acceso), desde una vista de almacén de datos, dispositivo de almacenamiento o adaptador. Esta tarea explica cómo deshabilitar una ruta de acceso con una vista de dispositivo de almacenamiento.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Storage Devices** (Dispositivos de almacenamiento).
- 4 Seleccione los dispositivos de almacenamiento cuyas rutas de acceso desee deshabilitar y haga clic en la pestaña **Paths** (Rutas de acceso).
- 5 Seleccione la ruta de acceso que desea deshabilitar y haga clic en **Disable** (Deshabilitar).

Administrar rutas de acceso de almacenamiento y complementos de múltiples rutas

Utilice los comandos `esxcli` para administrar los complementos de múltiples rutas y las rutas de acceso de almacenamiento asignadas a ellos.

Puede mostrar todos los complementos de múltiples rutas disponibles en el host. Puede enumerar cualquier MPP de terceros, al igual que NMP y SATP del host, y revisar las rutas de acceso que reclaman. También puede definir nuevas rutas de acceso y especificar qué complemento de múltiples rutas debe reclamar las rutas de acceso.

Para obtener más información sobre los comandos disponibles para administrar la PSA, consulte *Introducción a vSphere Command-Line Interface*.

Consideraciones sobre múltiples rutas

Se aplican consideraciones específicas cuando se administran reglas de notificación y complementos de múltiples rutas de almacenamiento.

Las siguientes consideraciones serán útiles para la habilitación de múltiples rutas:

- Si no hay una SATP asignada al dispositivo por las reglas de notificación, la SATP predeterminada para dispositivos iSCSI o de canal de fibra es VMW_SATP_DEFAULT_AA. La PSP predeterminada es VMW_PSP_FIXED.
- Cuando el sistema busca las reglas de SATP con el fin de localizar una SATP para un determinado dispositivo, en primer lugar busca las reglas del controlador. Si no hay coincidencias, se buscan las reglas del proveedor/modelo y, por último, las reglas de transporte. Si no hay coincidencias, NMP selecciona la SATP predeterminada para el dispositivo.
- Si se asigna VMW_SATP_ALUA a un dispositivo de almacenamiento específico, pero el dispositivo no se basa en ALUA, no se producirán coincidencias de reglas de notificación para ese dispositivo. La SATP predeterminada reclama el dispositivo en función de su tipo de transporte.
- La PSP predeterminada para todos los dispositivos reclamados por VMW_SATP_ALUA es VMW_PSP_MRU. VMW_PSP_MRU selecciona una ruta de acceso activa/optimizada, según lo informado por VMW_SATP_ALUA, o bien una ruta de acceso activa/no optimizada en caso de que no haya una ruta activa/optimizada. Esta ruta de acceso se utiliza hasta que haya una ruta de acceso mejor disponible (MRU). Por ejemplo, si VMW_PSP_MRU actualmente utiliza una ruta de acceso activa/no optimizada y en algún momento hay una ruta de acceso activa/optimizada disponible, VMW_PSP_MRU pasará a utilizar esta última.
- Aunque por lo general se selecciona VMW_PSP_MRU para matrices ALUA de forma predeterminada, ciertas matrices de almacenamiento ALUA deben utilizar VMW_PSP_FIXED. Para comprobar si la matriz de almacenamiento requiere VMW_PSP_FIXED, consulte la *Guía de compatibilidad de VMware* o póngase en contacto con el proveedor de almacenamiento. Al utilizar VMW_PSP_FIXED con matrices ALUA, a menos que se especifique explícitamente una ruta de acceso preferida, el host ESXi selecciona la ruta de trabajo más óptima y la designa como ruta de acceso preferida predeterminada. Si la ruta seleccionada por el host deja de estar disponible, se seleccionará una ruta de acceso alternativa disponible. Sin embargo, si designa explícitamente la ruta de acceso preferida, seguirá siéndolo más allá de cuál sea su estado.
- De forma predeterminada, la regla de notificación de PSA 101 enmascara pseudodispositivos de matrices Dell. No elimine esta regla, a menos que quiera desenmascarar estos dispositivos.

Lista de reglas de notificación de múltiples rutas para el host

Utilice el comando `esxcli` para ver la lista de las reglas de notificación de múltiples rutas disponibles.

Las reglas de notificación indican qué complemento de múltiples rutas (el NMP o cualquier MPP de terceros) administra una ruta de acceso física determinada. Cada regla de notificación identifica un conjunto de rutas de acceso según los siguientes parámetros:

- Cadenas de proveedor/modelo
- Transporte, como SATA, IDE, canal de fibra, entre otros
- Ubicación del adaptador, destino o LUN
- Controlador del dispositivo, por ejemplo, Mega-RAID

En el procedimiento, **--server=server_name** especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Ejecute el comando **esxcli --server=server_name storage core claimrule list --claimrule-class=MP** para ver una lista de las reglas de notificación de múltiples rutas.

Ejemplo: Resultados de muestra del comando `esxcli storage core claimrule list`

Rule	Class	Rule	Class	Type	Plugin	Matches
MP		0	runtime	transport	NMP	transport=usb
MP		1	runtime	transport	NMP	transport=sata
MP		2	runtime	transport	NMP	transport=ide
MP		3	runtime	transport	NMP	transport=block
MP		4	runtime	transport	NMP	transport=unknown
MP		101	runtime	vendor	MASK_PATH	vendor=DELL model=Universal Xport
MP		101	file	vendor	MASK_PATH	vendor=DELL model=Universal Xport
MP		200	runtime	vendor	MPP_1	vendor=NewVend model=*
MP		200	file	vendor	MPP_1	vendor=NewVend model=*
MP		201	runtime	location	MPP_2	adapter=vmhba41 channel=* target=* lun=*
MP		201	file	location	MPP_2	adapter=vmhba41 channel=* target=* lun=*
MP		202	runtime	driver	MPP_3	driver=megaraid
MP		202	file	driver	MPP_3	driver=megaraid
MP		65535	runtime	vendor	NMP	vendor=* model=*

Este ejemplo indica lo siguiente:

- El NMP reclama todas las rutas de acceso conectadas a dispositivos de almacenamiento que utilizan transporte USB, SATA, IDE y SCSI en bloque.
- Puede utilizar el módulo MASK_PATH para ocultar dispositivos no utilizados del host. De forma predeterminada, la regla de notificación de PSA 101 enmascara pseudodispositivos de matriz Dell con una cadena de proveedor DELL y una cadena de modelo Universal Xport.

- El módulo MPP_1 reclama todas las rutas de acceso conectadas con cualquier modelo de la matriz de almacenamiento NewVend.
- El módulo MPP_3 reclama las rutas de acceso a dispositivos de almacenamiento administrados por el controlador de dispositivo Mega-RAID.
- NMP reclama todas las rutas de acceso no descritas en las reglas anteriores.
- La columna Rule Class (Clase de regla) en los resultados describe la categoría de la regla de notificación. Puede ser complemento de múltiples rutas (MP), filtro o VAAI.
- La columna Class (Clase) muestra qué reglas se definen y cuáles se cargan. El parámetro `file` en la columna Class (Clase) indica que la regla está definida. El parámetro `runtime` indica que la regla se cargó en el sistema. Para que una regla de notificación definida por el usuario esté activa, deben existir dos líneas con el mismo número de regla: una para la regla con el parámetro `file` y otra con `runtime`. Varias reglas de numeración baja tienen una sola línea con la clase de `runtime`. Se trata de reglas de notificación definidas por el sistema que no pueden modificarse.

Mostrar módulos de múltiples rutas

Use el comando `esxcli` para enumerar todos los módulos de múltiples rutas cargados en el sistema. Los módulos de múltiples rutas administran las rutas de acceso físicas que conectan el host con el almacenamiento.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Para enumerar los módulos de múltiples rutas, ejecute el siguiente comando:

```
esxcli --server=server_name storage core plugin list --plugin-class=MP
```

Resultados

Este comando generalmente muestra el módulo NMP y, si está cargado, el módulo MASK_PATH. También se muestran los módulos MPP de terceros en el caso de que se hayan cargado.

Mostrar SATP para el host

Use el comando `esxcli` para enumerar los SATP de NMP de VMware cargados en el sistema. Muestre información sobre los SATP.

En el procedimiento, **--server=server_name** especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Para enumerar los SATP de VMware, ejecute el comando siguiente:

```
esxcli --server=server_name storage nmp satp list
```

Resultados

En cada SATP, el resultado muestra información sobre el tipo de matriz de almacenamiento o sistema que este SATP admite y el PSP predeterminado de cualquier LUN que use este SATP. Placeholder (plugin not loaded) (Marcador de posición [complemento no cargado]) en la columna Description (Descripción) indica que el SATP no se cargó.

Mostrar dispositivos de almacenamiento NMP

Use el comando `esxcli` para enumerar todos los dispositivos de almacenamiento que controla VMware NMP y mostrar información de SATP y PSP asociada con cada dispositivo.

En el procedimiento, **--server=server_name** especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Para enumerar todos los dispositivos de almacenamiento, ejecute el comando siguiente:

```
esxcli --server=server_name storage nmp device list
```

Use la opción **--device | -d=device_ID** para filtrar los resultados de este comando para que muestren un solo dispositivo.

Agregar reglas de notificación de múltiples rutas

Utilice los comandos `esxcli` para agregar una nueva regla de notificación de PSA de múltiples rutas al conjunto de reglas de notificación en el sistema. Para que la nueva regla de notificación sea activa, primero debe definir la regla y, a continuación, cargarla en el sistema.

Se agrega una nueva regla de notificación de PSA cuando, por ejemplo, se carga un nuevo complemento de múltiples rutas (MPP) y deben definirse qué rutas de acceso debe reclamar este módulo. Es posible que deba crearse una regla de notificación si se agregaron rutas de acceso nuevas a un MPP existente para poder reclamarlas.

Precaución Al crear nuevas reglas de notificación, realice los pasos necesarios para evitar una situación donde diferentes MPP reclaman diferentes rutas de acceso físicas al mismo LUN. A menos que uno de los MPP sea MASK_PATH MPP, esta configuración producirá problemas de rendimiento.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- 1 Para definir una nueva regla de notificación, ejecute el comando siguiente:

```
esxcli --server=server_name storage core claimrule add
```

El comando admite las siguientes opciones:

Opción	Descripción
<code>-A --adapter=<str></code>	Indique el adaptador de las rutas de acceso que se utilizará en esta operación.
<code>-u --autoassign</code>	El sistema asignará automáticamente un identificador de regla.
<code>-C --channel=<long></code>	Indique el canal de las rutas de acceso que se utilizará en esta operación.
<code>-c --claimrule-class=<str></code>	Indique la clase de regla de notificación que se utilizará en esta operación. Los valores válidos son los siguientes: MP, Filter, VAAI.
<code>-d --device=<str></code>	Indique el identificador de dispositivo que se utilizará para esta operación.
<code>-D --driver=<str></code>	Indique el controlador de las rutas de acceso que se utilizará en esta operación.
<code>-f --force</code>	Fuerce a las reglas de notificación a ignorar las comprobaciones de validez e instalar la regla de todas formas.

Opción	Descripción
<code>--if-unset=<str></code>	Ejecute este comando si esta variable de usuario avanzado no está establecida en 1.
<code>-i --iqn=<str></code>	Indique el nombre calificado de iSCSI para el destino que se utilizará en esta operación.
<code>-L --lun=<long></code>	Indique el LUN de las rutas de acceso que se utilizará en esta operación.
<code>-M --model=<str></code>	Indique el modelo de las rutas de acceso que se utilizará en esta operación.
<code>-P --plugin=<str></code>	Indique qué complemento de PSA se utilizará en esta operación. (obligatorio)
<code>-r --rule=<long></code>	Indique el identificador de regla que se utilizará para esta operación.
<code>-T --target=<long></code>	Indique el destino de las rutas de acceso que se utilizará en esta operación.
<code>-R --transport=<str></code>	Indique el transporte de las rutas de acceso que se utilizará en esta operación. Los valores válidos son los siguientes: block, fc, iscsi, iscsivendor, ide, sas, sata, usb, parallel, unknown.
<code>-t --type=<str></code>	Indique qué tipo de coincidencia se utilizará para reclamar o anular la reclamación, o bien para claimrule. Los valores válidos son los siguientes: proveedor, ubicación, controlador, transporte, dispositivo, destino. (obligatorio)
<code>-V --vendor=<str></code>	Indique el proveedor de las rutas de acceso al usuario que se utilizará en esta operación.
<code>--wwnn=<str></code>	Indique el número de nodo universal para el destino que se utilizará en esta operación.
<code>--wwpn=<str></code>	Indique el número de puerto World-Wide Port Number para el destino que se utilizará en esta operación.

- 2 Para cargar la nueva regla de notificación en el sistema, ejecute el siguiente comando:

```
esxcli --server=server_name storage core claimrule load
```

Este comando carga todas las reglas de notificación de múltiples rutas recientemente creadas desde el archivo de configuración del sistema.

Ejemplo: Definir reglas de notificación de múltiples rutas

En el siguiente ejemplo, se agrega y se carga la regla número 500 para reclamar todas las rutas de acceso con la cadena del modelo NewMod y la cadena del proveedor NewVend para el complemento NMP.

```
# esxcli --server=server_name storage core claimrule add -r 500 -t vendor -V  
NewVend -M NewMod -P NMP  
  
# esxcli --server=server_name storage core claimrule load
```

Después de ejecutar el comando **esxcli --server=server_name storage core claimrule list**, verá la nueva regla de notificación en la lista.

Nota Las dos líneas de la regla de notificación, una con la clase de `runtime` y otra con la clase de `file`, indican que la nueva regla de notificación se cargó en el sistema y está activa.

Rule	Class	Rule	Class	Type	Plugin	Matches
MP		0	runtime	transport	NMP	transport=usb
MP		1	runtime	transport	NMP	transport=sata
MP		2	runtime	transport	NMP	transport=ide
MP		3	runtime	transport	NMP	transport=block
MP		4	runtime	transport	NMP	transport=unknown
MP		101	runtime	vendor	MASK_PATH	vendor=DELL model=Universal Xport
MP		101	file	vendor	MASK_PATH	vendor=DELL model=Universal Xport
MP		500	runtime	vendor	NMP	vendor=NewVend model=NewMod
MP		500	file	vendor	NMP	vendor=NewVend model=NewMod

Eliminar reglas de notificación de múltiples rutas

Utilice los comandos **esxcli** para quitar una regla de notificación de PSA de múltiples rutas del conjunto de reglas de notificación en el sistema.

En el procedimiento, **--server=server_name** especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de **esxcli** en ESXi Shell.

Procedimiento

- 1 Elimine una regla de notificación del conjunto de reglas de notificación.

```
esxcli --server=server_name storage core claimrule remove
```

Nota De forma predeterminada, la regla de notificación de PSA 101 enmascara pseudodispositivos de matrices Dell. No elimine esta regla, a menos que quiera desenmascarar estos dispositivos.

El comando admite las siguientes opciones:

Opción	Descripción
<code>-c --claimrule-class=<str></code>	Indique la clase de regla de notificación para utilizar en esta operación (MP, Filter [Filtro], VAAI).
<code>-P --plugin=<str></code>	Indique el complemento para utilizar en esta operación.
<code>-r --rule=<long></code>	Indique el identificador de regla que se utilizará para esta operación.

Este paso quita la regla de notificación de la clase File (Archivo).

- Quite la regla de notificación del sistema.

```
esxcli --server=server_name storage core claimrule load
```

Este paso quita la regla de notificación de la clase Runtime (Tiempo de ejecución).

Enmascarar rutas de acceso

Se puede evitar que el host acceda a los dispositivos de almacenamiento o LUN, o que utilice rutas de acceso individuales a un LUN. Utilice los comandos `esxcli` para enmascarar las rutas de acceso. Cuando se enmascaran rutas de acceso, se crean reglas de notificación que asignan el complemento MASK_PATH a las rutas de acceso especificadas.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- Compruebe cuál es el próximo identificador de regla disponible.

```
esxcli --server=server_name storage core claimrule list
```

Las reglas de notificación utilizadas para enmascarar las rutas de acceso deben tener identificadores de regla en el rango de 101 a 200. Si este comando muestra que las reglas 101 y 102 ya existen, se puede especificar el valor 103 para la regla que se desea agregar.

- Asigne el complemento MASK_PATH a una ruta de acceso. Para ello, cree una regla de notificación nueva para el complemento.

```
esxcli --server=server_name storage core claimrule add -P MASK_PATH
```

- Cargue la regla de notificación MASK_PATH en el sistema.

```
esxcli --server=server_name storage core claimrule load
```

- 4 Compruebe que la regla de notificación MASK_PATH se haya agregado correctamente.

```
esxcli --server=server_name storage core claimrule list
```

- 5 Si hay una regla de notificación para la ruta de acceso enmascarada, quítela.

```
esxcli --server=server_name storage core claiming unclaim
```

- 6 Ejecute las reglas de notificación de ruta de acceso.

```
esxcli --server=server_name storage core claimrule run
```

Resultados

Una vez asignado el complemento MASK_PATH a una ruta de acceso, el estado de la ruta de acceso se vuelve irrelevante y el host deja de mantenerlo. Como resultado, los comandos que muestran la información de la ruta de acceso enmascarada pueden mostrar el estado de la ruta de acceso como inactivo.

Ejemplo: Enmascaramiento de un LUN

En este ejemplo, se enmascara el LUN 20 en los destinos T1 y T2, a los que se accede a través de los adaptadores de almacenamiento vmhba2 y vmhba3.

```
1 #esxcli --server=server_name storage core claimrule list

2 #esxcli --server=server_name storage core claimrule add -P MASK_PATH -r 109 -t location -A
  vmhba2 -C 0 -T 1 -L 20
  #esxcli --server=server_name storage core claimrule add -P MASK_PATH -r 110 -t location -A
  vmhba3 -C 0 -T 1 -L 20
  #esxcli --server=server_name storage core claimrule add -P MASK_PATH -r 111 -t location -A
  vmhba2 -C 0 -T 2 -L 20
  #esxcli --server=server_name storage core claimrule add -P MASK_PATH -r 112 -t location -A
  vmhba3 -C 0 -T 2 -L 20

3 #esxcli --server=server_name storage core claimrule load

4 #esxcli --server=server_name storage core claimrule list

5 #esxcli --server=server_name storage core claiming unclaim -t location -A vmhba2
  #esxcli --server=server_name storage core claiming unclaim -t location -A vmhba3

6 #esxcli --server=server_name storage core claimrule run
```

Desenmascarar rutas de acceso

Cuando necesite que el host tenga acceso al dispositivo de almacenamiento enmascarado, quite la máscara de las rutas al dispositivo.

En el procedimiento, **--server=server_name** especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Nota Cuando se ejecuta una operación de anulación de notificación con una propiedad del dispositivo, por ejemplo, el identificador de dispositivo, el proveedor o el modelo, no se anula la notificación de las rutas de acceso que reclama el complemento MASK_PATH. El complemento MASK_PATH no realiza un seguimiento de ninguna propiedad del dispositivo de las rutas de acceso que notifica.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- 1 Elimine la regla de notificación MASK_PATH.

```
esxcli --server=server_name storage core claimrule remove -r rule#
```

- 2 Compruebe que la regla de notificación se haya eliminado correctamente.

```
esxcli --server=server_name storage core claimrule list
```

- 3 Vuelva a cargar las reglas de notificación de ruta de acceso del archivo de configuración al VMkernel.

```
esxcli --server=server_name storage core claimrule load
```

- 4 Ejecute el comando `esxcli --server=server_name storage core claiming unclaim` para cada ruta de acceso al dispositivo de almacenamiento enmascarado.

Por ejemplo:

```
esxcli --server=server_name storage core claiming unclaim -t location -A
vmhba0 -C 0 -T 0 -L 149
```

- 5 Ejecute las reglas de notificación de ruta de acceso.

```
esxcli --server=server_name storage core claimrule run
```

Resultados

El host ahora puede acceder al dispositivo de almacenamiento que estaba enmascarado.

Definir reglas de SATP de NMP

Las reglas de notificación de SATP de NMP especifican cuál SATP debe administrar un dispositivo de almacenamiento en particular. Generalmente, no es necesario que modifique las reglas de

SATP de NMP. Si necesita hacerlo, use los comandos `esxcli` para agregar una regla a la lista de reglas de notificación del SATP especificado.

Es posible que necesite crear una regla de SATP cuando instala un SATP de terceros para una matriz de almacenamiento específica.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- 1 Para agregar una regla de notificación para un SATP específico, ejecute el comando `esxcli --server=server_name storage nmp satp rule add`. El comando acepta las opciones siguientes.

Opción	Descripción
<code>-b --boot</code>	Es una regla predeterminada del sistema que se agrega en el momento del arranque. No modifique <code>esx.conf</code> ni agregue nada al perfil de host.
<code>-c --claim-option=string</code>	Establezca la cadena de opción de notificación cuando agrega una regla de notificación de SATP.
<code>-e --description=string</code>	Establezca la descripción de la regla de notificación cuando agrega una regla de notificación de SATP.
<code>-d --device=string</code>	Establezca el dispositivo cuando agrega reglas de notificación de SATP. Las reglas del dispositivo son mutuamente exclusivas con las reglas del proveedor/modelo y del controlador.
<code>-D --driver=string</code>	Establezca la cadena del controlador cuando agrega una regla de notificación de SATP. Las reglas del controlador son mutuamente exclusivas con las reglas del proveedor/modelo.
<code>-f --force</code>	Fuerce a las reglas de notificación a ignorar las comprobaciones de validez e instalar la regla de todas formas.
<code>-h --help</code>	Muestre el mensaje de ayuda.
<code>-M --model=string</code>	Establezca la cadena del modelo cuando agrega una regla de notificación a SATP. Las reglas del proveedor/modelo son mutuamente exclusivas con las reglas del controlador.
<code>-o --option=string</code>	Establezca la cadena de opción cuando agrega una regla de notificación de SATP.
<code>-P --psp=string</code>	Establezca el PSP predeterminado para la regla de notificación de SATP.
<code>-O --psp-option=string</code>	Establezca las opciones del PSP para la regla de notificación de SATP.

Opción	Descripción
<code>-s --satp=string</code>	El SATP para el que se agregará una regla nueva.
<code>-R --transport=string</code>	Establezca la cadena de tipo de transporte de notificación cuando agrega una regla de notificación de SATP.
<code>-t --type=string</code>	Establezca el tipo de cadena cuando agrega una regla de notificación de SATP.
<code>-V --vendor=string</code>	Establezca la cadena del proveedor cuando agrega reglas de notificación de SATP. Las reglas del proveedor/modelo son mutuamente exclusivas con las reglas del controlador.

Nota Cuando busca las reglas de SATP para ubicar un SATP de un dispositivo dado, el NMP busca primero las reglas del controlador. Si no hay coincidencia, se buscan las reglas del proveedor/modelo y, por último, las reglas de transporte. Si aún no hay coincidencia, el NMP selecciona un SATP predeterminado para el dispositivo.

2 Reinicie el host.

Ejemplo: Definir una regla de SATP de NMP

El comando de muestra siguiente asigna el complemento `VMW_SATP_INV` para administrar las matrices de almacenamiento con la cadena del proveedor `NewVend` y la cadena del modelo `NewMod`.

```
# esxcli --server=server_name storage nmp satp rule add -V NewVend -M NewMod -s VMW_SATP_INV
```

Si ejecuta el comando `esxcli --server=server_name storage nmp satp list -s VMW_SATP_INV`, puede ver que la regla nueva se agregó a la lista de reglas `VMW_SATP_INV`.

Colas de programación de E/S de máquinas virtuales

De forma predeterminada, vSphere proporciona un mecanismo que crea colas de programación para cada archivo de máquina virtual. Cada archivo, por ejemplo, `.vmdk`, obtiene sus propios controles de ancho de banda.

Este mecanismo garantiza que las operaciones de E/S de un archivo de máquina virtual en particular, por ejemplo, `.vmdk`, se coloquen en su propia cola independiente y no interfieran con las operaciones de E/S de otros archivos.

Esta funcionalidad está habilitada de forma predeterminada. Si debe deshabilitarla, puede hacerlo con el parámetro `VMkernel.Boot.isPerFileSchedModelActive` en la configuración avanzada del sistema.

Editar programación de E/S por archivo

El parámetro avanzado `VMkernel.Boot.isPerFileSchedModelActive` controla el mecanismo de programación de E/S por archivo. El mecanismo está habilitado de forma predeterminada.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Sistema**, haga clic en **Configuración avanzada del sistema**.
- 4 En Advanced System Settings (Configuración avanzada del sistema), seleccione el parámetro **VMkernel.Boot.isPerFileSchedModelActive** y haga clic en el icono **Edit** (Editar).
- 5 Seleccione una de las siguientes opciones:
 - Para deshabilitar el mecanismo de programación por archivo, cambie el valor a **No**.

Nota Después de desactivar el modelo de programación de E/S por archivo, el host se revierte al mecanismo de programación heredado que usa una sola cola de E/S. El host mantiene la cola de E/S única para cada par de máquina virtual y dispositivo de almacenamiento. Todas las E/S entre la máquina virtual y sus discos virtuales almacenados en el dispositivo de almacenamiento se trasladan a esta cola. Como resultado, las E/S de distintos discos virtuales pueden interferir entre sí al compartir el ancho de banda y afectar el rendimiento de las otras.

- Para volver a habilitar el mecanismo de programación por archivo, cambie el valor a **Yes** (Sí).
- 6 Reinicie el host para que se apliquen los cambios.

Utilizar comandos `esxcli` para habilitar o deshabilitar la programación de E/S por archivo

Puede utilizar los comandos `esxcli` para cambiar la funcionalidad de programación de E/S. La funcionalidad está habilitada de forma predeterminada.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Para habilitar o deshabilitar la programación de E/S por archivo, ejecute los siguientes comandos:

Opción	Descripción
<code>esxcli system settings kernel set -s isPerFileSchedModelActive -v FALSE</code>	Deshabilita la programación de E/S por archivo.
<code>esxcli system settings kernel set -s isPerFileSchedModelActive -v TRUE</code>	Habilita la programación de E/S por archivo.

Asignación de dispositivos sin formato

18

La asignación de dispositivos sin formato (RDM) proporciona un mecanismo para que la máquina virtual tenga acceso directo al LUN en el subsistema de almacenamiento físico.

Los siguientes temas contienen información sobre RDM y ofrecen instrucciones sobre cómo crear y administrar RDM.

Este capítulo incluye los siguientes temas:

- [Acerca de la asignación de dispositivos sin formato](#)
- [Características de la asignación de dispositivos sin formato](#)
- [Crear máquinas virtuales con RDM](#)
- [Administrar rutas de acceso para un LUN asignado](#)

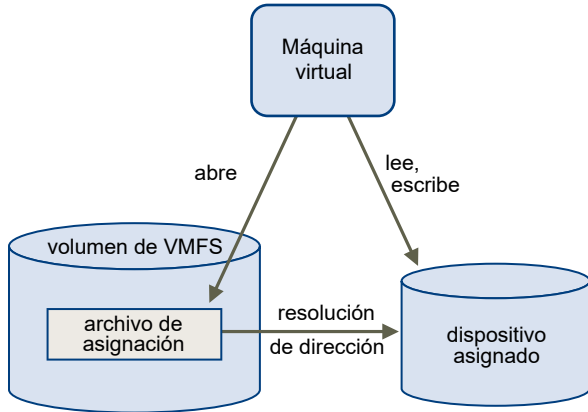
Acerca de la asignación de dispositivos sin formato

El RDM es un archivo de asignación en un volumen VMFS distinto que actúa como proxy de un dispositivo de almacenamiento físico sin formato. El RDM permite a una máquina virtual acceder directamente y utilizar el dispositivo de almacenamiento. El RDM contiene metadatos para administrar y redirigir el acceso del disco al dispositivo físico.

El archivo proporciona algunas de las ventajas del acceso directo a un dispositivo físico y mantiene algunas ventajas de un disco virtual en VMFS. Como resultado, combina la capacidad de administración de VMFS con el acceso de dispositivos sin formato.

Los RDM pueden describirse con términos como asignar un dispositivo sin formato a un almacén de datos, asignar un LUN del sistema o asignar un archivo de disco a un volumen de disco físico. Todos estos términos se refieren a los RDM.

Figura 18-1. Asignación de dispositivos sin formato



Si bien VMware recomienda utilizar almacenes de datos de VMFS para la mayoría de los almacenamientos de disco virtual, en ciertas ocasiones, es posible que se necesiten utilizar LUN sin formato o discos lógicos ubicados en una SAN.

Por ejemplo, se deben utilizar LUN sin formato con RDM en las situaciones siguientes:

- Cuando una instantánea de SAN u otras aplicaciones en capas se ejecutan en la máquina virtual. El RDM habilita mejor los sistemas de descarga de copia de seguridad escalables con la utilización de características inherentes a la SAN.
- En cualquier escenario de agrupación en clústeres de MSCS que expanda los hosts físicos: clústeres virtual a virtual y clústeres físico a virtual. En este caso, los datos de clúster y los discos de quórum deben configurarse como RDM en lugar de como discos virtuales en un VMFS compartido.

Piense en un RDM como un vínculo simbólico de un volumen VMFS a un LUN sin formato. La asignación hace que los LUN aparezcan como archivos en un volumen VMFS. Al RDM, no al LUN sin formato, se hace referencia en la configuración de la máquina virtual. El RDM contiene una referencia al LUN sin formato.

Con RDM, es posible:

- Utilizar vMotion para migrar las máquinas virtuales mediante LUN sin formato.
- Agregar LUN sin formato a las máquinas virtuales con vSphere Web Client.
- Utilizar funciones de los sistemas de archivo, como el bloqueo de archivos distribuido, permisos y nomenclaturas.

Hay dos modos de compatibilidad disponibles para los RDM:

- El modo de compatibilidad virtual permite a un RDM actuar exactamente como un archivo de disco virtual, incluida la utilización de instantáneas.
- El modo de compatibilidad física permite el acceso directo del dispositivo SCSI para aquellas aplicaciones que necesitan un control de nivel más bajo.

Beneficios de la asignación de dispositivos sin formato

Un RDM proporciona varios beneficios, pero no debe utilizarse en todas las situaciones. En general, los archivos de disco virtual son preferibles a los RDM gracias a su manejabilidad. Sin embargo, cuando se necesitan dispositivos sin procesar, debe usar el RDM.

El RDM ofrece varios beneficios.

Nombres persistentes descriptivos

Proporciona un nombre fácil para un dispositivo asignado. Cuando utiliza el RDM, no es necesario referirse al dispositivo por su nombre de dispositivo. Se puede referir a este por el nombre del archivo de asignación, por ejemplo:

```
/vmfs/volumes/myVolume/myVMDirectory/myRawDisk.vmdk
```

Resolución de nombres dinámica

Almacena información de identificación única de cada dispositivo asignado. VMFS asocia cada RDM con su dispositivo SCSI actual, independientemente de los cambios en la configuración física del servidor debido a cambios en el hardware del adaptador, cambios de rutas de acceso, reubicación del dispositivo, etc.

Bloqueo de archivos distribuido

Permite usar el bloqueo distribuido de VMFS para dispositivos SCSI sin procesar. El bloqueo distribuido en un RDM hace que sea seguro usar un LUN sin procesar compartido sin perder datos cuando dos máquinas virtuales en distintos servidores intentan acceder al mismo LUN.

Permisos de archivo

Posibilita los permisos de archivo. Los permisos del archivo de asignación se implementan en el momento de abrir el archivo para proteger el volumen asignado.

Operaciones del sistema de archivos

Permite usar las utilidades del sistema de archivos para trabajar con un volumen asignado, usando el archivo de asignación como proxy. La mayoría de las operaciones que son válidas para un archivo común pueden aplicarse al archivo de asignación y se redireccionan para funcionar en el dispositivo asignado.

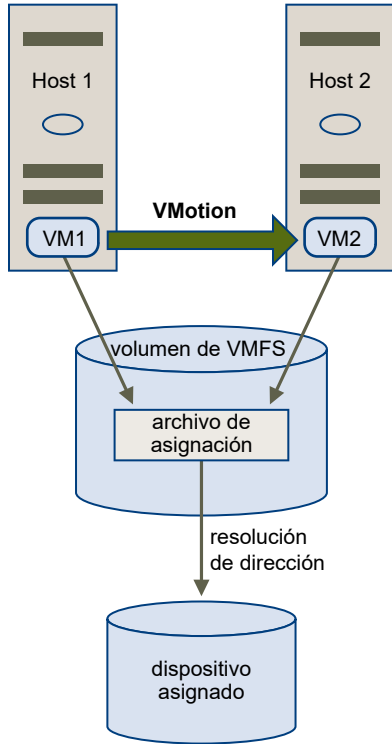
Instantáneas

Posibilita usar instantáneas de máquina virtual en un volumen asignado. Las instantáneas no están disponibles cuando el RDM se usa en modo de compatibilidad física.

vMotion

Permite migrar una máquina virtual con vMotion. El archivo de asignación actúa como proxy para permitir a vCenter Server migrar la máquina virtual con el mismo mecanismo que para migrar archivos de disco virtual.

Figura 18-2. vMotion de una máquina virtual con asignación de dispositivos sin formato



Agentes de administración de SAN

Posibilita ejecutar algunos agentes de administración de SAN dentro de una máquina virtual. De manera similar, cualquier software que necesita acceder a un dispositivo mediante comandos SCSI específicos de hardware puede ejecutarse en una máquina virtual. Este tipo de software se denomina software basado en destino de SCSI. Cuando usa agentes de administración de SAN, seleccione un modo de compatibilidad física para el RDM.

Virtualización de identificador de puerto N (NPIV)

Posibilita usar la tecnología NPIV que permite que un puerto HBA de canal de fibra único se registre en el tejido de canal de fibra con varios nombres de puertos universales (WWPN). Esta capacidad hace que el puerto HBA aparezca como varios puertos virtuales, cada uno con su propio identificador y nombre de puerto virtual. Las máquinas virtuales pueden, a continuación, reclamar cada uno de estos puertos y usarlos para todo el tráfico RDM.

Nota Puede usar NPIV solo para máquinas virtuales con discos RDM.

VMware funciona con proveedores de software de administración de almacenamiento para asegurar que su software funcione correctamente en entornos que incluyen ESXi. Algunas aplicaciones de este tipo son:

- software de administración de SAN
- Software de administración de recursos de almacenamiento (SRM)
- Software de instantáneas

■ Software de replicación

Este tipo de software usa un modo de compatibilidad física para los RDM de modo que el software pueda acceder a dispositivos SCSI directamente.

Varios productos de administración se ejecutan mejor de forma centralizada (no en la máquina de ESXi), mientras que otros se ejecutan bien en las máquinas virtuales. VMware no certifica estas aplicaciones ni proporciona una matriz de compatibilidad. Para saber si una aplicación de administración de SAN es compatible con un entorno de ESXi, póngase en contacto con el proveedor de software de administración de SAN.

Consideraciones y limitaciones de RDM

Al usar los RDM, hay que tener en cuenta ciertas consideraciones y limitaciones.

- El RDM no está disponible para los dispositivos de bloque de conexión directa ni para ciertos dispositivos RAID. El RDM usa un número de serie de SCSI para identificar el dispositivo asignado. Debido a que los dispositivos de bloque y algunos dispositivos RAID de conexión directa no exportan números de serie, no se pueden utilizar con los RDM.
- Si utiliza el RDM en el modo de compatibilidad física, no puede utilizar una instantánea con el disco. El modo de compatibilidad física permite a la máquina virtual administrar sus propias operaciones de creación de instantáneas o de reflejos basadas en almacenamiento.

Las instantáneas de máquina virtual están disponibles para RDM con modo de compatibilidad virtual.

- No se puede realizar una asignación a una partición de disco. Los RDM requieren que el dispositivo asignado sea un LUN completo.
- Si usa vMotion para migrar máquinas virtuales con RDM, asegúrese de que los identificadores de LUN sean coherentes para los RDM en todos los hosts ESXi implicados.
- Flash Read Cache no admite RDM en términos de compatibilidad física. Los RDM de compatibilidad virtual son compatibles con Flash Read Cache.

Características de la asignación de dispositivos sin formato

RDM es un archivo de asignación especial en un volumen VMFS que administra metadatos para su dispositivo asignado. El archivo de asignación se presenta ante el software de administración como un archivo común del disco, disponible para las operaciones normales del sistema de archivos. Para la máquina virtual, la capa de virtualización de almacenamiento presenta el dispositivo asignado como un dispositivo SCSI virtual.

Entre el contenido clave de los metadatos en el archivo de asignación se encuentran la ubicación del dispositivo asignado (resolución de nombres), el estado de bloqueo del dispositivo asignado, los permisos, etc.

Modos de compatibilidad virtual y física de RDM

Puede utilizar RDM en los modos de compatibilidad virtual o compatibilidad física. El modo virtual especifica la virtualización completa del dispositivo asignado. El modo físico especifica una virtualización SCSI mínima del dispositivo asignado y permite la mayor flexibilidad del software de administración de SAN.

En el modo virtual, el VMkernel envía solo READ y WRITE al dispositivo asignado. Para el sistema operativo invitado, el dispositivo asignado aparece exactamente igual que un archivo de disco virtual en un volumen VMFS. Las características reales de hardware están ocultas. Si utiliza un disco sin formato en modo virtual, puede aprovechar los beneficios de VMFS, como el bloqueo avanzado de archivos para protección de datos y las instantáneas para optimizar los procesos de desarrollo. El modo virtual también es más portátil en hardware de almacenamiento que en el modo físico, ya que presenta el mismo comportamiento que un archivo de disco virtual.

En el modo físico, el VMkernel pasa todos los comandos SCSI al dispositivo, con una sola excepción: el comando REPORT de los LUN se virtualiza para que el VMkernel pueda aislar el LUN con la máquina virtual al que pertenece. Caso contrario, se exponen todas las características físicas del hardware subyacente. El modo físico es útil para ejecutar agentes de administración de SAN u otro software basado en destinos SCSI en la máquina virtual. El modo físico también permite la agrupación en clústeres virtual a física para obtener una alta disponibilidad rentable.

VMFS5 es compatible con tamaños de disco superiores a 2 TB para RDM en los modos virtual y físico. No se pueden reubicar los RDM superiores a 2 TB en almacenes de datos que no sean VMFS5.

Resolución de nombres dinámica

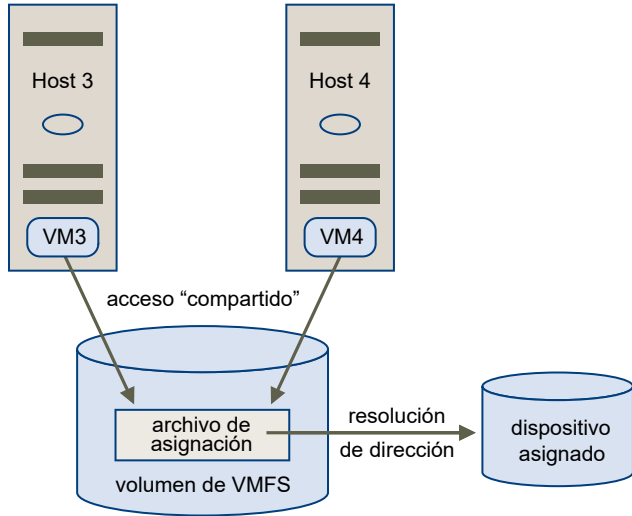
El archivo RDM admite la resolución de nombres dinámica cuando cambia la ruta de acceso a un dispositivo sin formato.

VMFS identifica de manera única todos los dispositivos de almacenamiento asignados y la identificación se almacena en sus estructuras de datos internas. Cualquier cambio en la ruta de acceso a un dispositivo sin formato, como un error en un conmutador de canal de fibra o el agregado de un HBA nuevo, puede cambiar el nombre del dispositivo. La resolución de nombres dinámica resuelve estos cambios y asocia automáticamente el dispositivo original con su nuevo nombre.

Asignación de dispositivos sin formato con clústeres de máquinas virtuales

Utilice el RDM con clústeres de máquinas virtuales que necesitan acceder al mismo LUN sin procesar en caso de ocurra conmutación por error. La configuración es similar a la de un clúster de máquina virtual que accede al mismo archivo de disco virtual, pero el RDM reemplaza el archivo del disco virtual.

Figura 18-3. Acceder desde máquinas virtuales con clúster



Comparar modos de acceso de dispositivos SCSI disponibles

Es posible acceder a un dispositivo de almacenamiento basado en SCSI mediante un archivo de disco virtual en un almacén de datos de VMFS, un RDM de modo virtual o un RDM de modo físico.

Si necesita ayuda en el momento de elegir entre los modos de acceso disponibles para dispositivos SCSI, consulte la siguiente tabla que ofrece una rápida comparación de las características disponibles en los diferentes modos.

Tabla 18-1. Características disponibles con asignaciones de discos virtuales y dispositivos sin formato

Características de ESXi	Archivo de disco virtual	RDM de modo virtual	RDM de modo físico
Comandos SCSI transmitidos	No	No	Sí Los REPORT LUN no se transmiten
Soporte de vCenter Server	Sí	Sí	Sí
Instantáneas	Sí	Sí	No
Bloqueo distribuido	Sí	Sí	Sí
Agrupar en clústeres	Solo sistemas Cluster-in-a-box	Sistema Cluster-in-a-box sistema Cluster-across-boxes	Agrupación en clústeres física a virtual sistema Cluster-across-boxes
Software basado en destinos de SCSI	No	No	Sí

VMware recomienda usar archivos de disco virtual para el tipo de agrupación en clústeres de sistemas Cluster-in-a-box. Si planea reconfigurar los clústeres de sistema Cluster-in-a-box, como clústeres de sistema Cluster-across-boxes, use el RDM de modo virtual para los clústeres de sistema Cluster-in-a-box.

Crear máquinas virtuales con RDM

Al otorgarle a la máquina virtual acceso directo a un LUN de SAN sin procesar, crea un disco RDM que reside en un almacén de datos de VMFS y que apunta al LUN. El RDM se crea como un disco inicial para una máquina virtual nueva o se agrega a una máquina virtual existente. Al crear el RDM, se especifica el LUN que se va a asignar y el almacén de datos en el que se debe colocar la RDM.

Aunque el archivo de disco RDM tiene la misma extensión `.vmdk` que un archivo de disco virtual normal, el RDM contiene solo información de asignación. Los datos del disco virtual actual se almacenan directamente en el LUN.

Este procedimiento da por sentado que se está creando una máquina virtual nueva. Para obtener más información, consulte la documentación de *Administración de máquinas virtuales de vSphere*.

Procedimiento

- 1 Haga clic con el botón derecho en cualquier objeto de inventario que sea un objeto primario válido de una máquina virtual, como un centro de datos, una carpeta, un clúster, un grupo de recursos o un host y seleccione **New Virtual Machine** (Nueva máquina virtual).
- 2 Seleccione **Create a new virtual machine** (Crear una nueva máquina virtual) y haga clic en **Next** (Siguiente).
- 3 Siga los pasos necesarios para crear una máquina virtual.
- 4 En la página Customize Hardware (Personalizar hardware), haga clic en la pestaña **Virtual Hardware** (Hardware virtual).
- 5 (opcional) Para eliminar el disco duro virtual predeterminado que creó el sistema para la máquina virtual, mueva el cursor sobre el disco y haga clic en el icono **Remove** (Quitar).
- 6 En el menú desplegable **New** (Nuevo) en la parte inferior de la página, seleccione **RDM Disk** (Disco RDM) y haga clic en **Add** (Agregar).
- 7 En la lista de dispositivos SAN o de LUN, seleccione un LUN sin procesar para que la máquina virtual acceda directamente y haga clic en **OK** (Aceptar).

El sistema crea un disco RDM que asigna la máquina virtual al LUN de destino. El disco RDM se muestra en la lista de dispositivos virtuales como un disco duro nuevo.

- 8 Haga clic en el triángulo **New Hard Disk** (Disco duro nuevo) para expandir las propiedades del disco RDM.
- 9 Seleccione una ubicación para el disco RDM.

Puede colocar el RDM en el mismo almacén de datos en el que residen los archivos de configuración de la máquina virtual o seleccionar un almacén de datos distinto.

Nota Para utilizar vMotion en máquinas virtuales con NPIV habilitada, asegúrese de que los archivos RDM y los archivos de máquina virtual se encuentren en el mismo almacén de datos. No es posible ejecutar Storage vMotion cuando la funcionalidad de NPIV está habilitada.

10 Seleccione un modo de compatibilidad.

Opción	Descripción
Physical (Físico)	Permite que el sistema operativo invitado acceda al hardware en forma directa. La compatibilidad física resulta útil cuando se usan aplicaciones basadas en SAN en la máquina virtual. No obstante, no es posible clonar una máquina virtual con RDM de compatibilidad física, crear una plantilla a partir de ella ni migrarla si la migración implica realizar una copia en el disco.
Virtual	Permite que el disco RDM se comporte como un disco virtual, para que se puedan utilizar características como creación de instantáneas, clonación, etc. Cuando se clona el disco para crear una plantilla a partir de él, el contenido del LUN se copia en un archivo de disco virtual .vmdk. Cuando se migra un disco RDM en modo de compatibilidad virtual, es posible migrar el archivo de asignación a un disco virtual o copiar el contenido del LUN en un disco virtual.

11 Si seleccionó el modo de compatibilidad virtual, seleccione un modo de disco.

Los modos de discos no están disponibles para los discos RDM que usan el modo de compatibilidad física.

Opción	Descripción
Dependent (Dependiente)	Se incluyen discos dependientes en las instantáneas.
Independent - Persistent (Independiente persistente)	Los discos en modo persistente se comportan como los discos convencionales en el equipo físico. Todos los datos que se escriben en un disco en modo persistente se escriben de forma permanente en el disco.
Independent - Nonpersistent (Independiente no persistente)	Los cambios en los discos en modo no persistente se descartan cuando se apaga o se reinicia la máquina virtual. Con el modo no persistente, puede reiniciar la máquina virtual con un disco virtual en el mismo estado cada vez. Los cambios en el disco se escriben y se leen desde un archivo de registro de rehacer que se elimina cuando se realiza un apagado o un reinicio.

12 Haga clic en **OK** (Aceptar).

Administrar rutas de acceso para un LUN asignado

Cuando utiliza máquinas virtuales con RDM, puede administrar rutas de acceso para los LUN sin formato asignados.

Procedimiento

- 1 En vSphere Web Client, desplácese hasta la máquina virtual.
- 2 Haga clic con el botón derecho en la máquina virtual y seleccione **Edit Settings** (Editar configuración).
- 3 Haga clic en la pestaña **Virtual Hardware** (Hardware virtual) y, a continuación, haga clic en **Hard Disk** (Disco duro) para expandir el menú de opciones del disco.
- 4 Haga clic en **Manage Paths** (Administrar rutas).

- 5 Utilice el cuadro de diálogo Edit Multipathing Policies (Editar directivas de múltiples rutas) para habilitar o deshabilitar rutas de acceso, establecer la directiva de múltiples rutas y especificar la ruta de acceso preferida.

Para obtener información sobre la administración de rutas de acceso, consulte [Capítulo 17 Descripción de múltiples rutas y conmutación por error](#).

La funcionalidad de Virtual Volumes cambia el paradigma de administración de almacenamiento de la administración del espacio interno de los almacenes de datos a la administración de objetos de almacenamiento abstractos controlados por matrices de almacenamiento. Con Virtual Volumes, una máquina virtual individual (no el almacén de datos) se convierte en una unidad de administración de almacenamiento, a la vez que el hardware de almacenamiento toma un control completo del contenido, del diseño y de la administración del disco virtual.

Históricamente, la administración de almacenamiento de vSphere se ha centrado en los almacenes de datos. Con este enfoque, los administradores de almacenamiento y los administradores de vSphere determinan de antemano los requisitos de almacenamiento de las máquinas virtuales. Posteriormente, el administrador de almacenamiento configura los recursos compartidos de LUN o NFS y los presenta a los hosts ESXi. El administrador de vSphere crea almacenes de datos basados en LUN o NFS, que luego usa como almacenamiento de máquinas virtuales. Generalmente, el almacén de datos es el nivel de granularidad más bajo en el que se produce la administración de datos desde el punto de vista del almacenamiento. Sin embargo, un solo almacén de datos contiene varias máquinas virtuales, que pueden tener diferentes requisitos. Con el enfoque tradicional, es difícil hacer una diferenciación teniendo en cuenta cada máquina virtual.

La funcionalidad de Virtual Volumes ayuda a mejorar la granularidad y permite diferenciar servicios de máquinas virtuales por aplicación mediante un nuevo enfoque de administración de almacenamiento. En lugar de determinar el almacenamiento de acuerdo con las características de un sistema de almacenamiento, Virtual Volumes lo hace en función de la necesidad de cada máquina virtual, lo que hace que el almacenamiento sea específico de cada máquina virtual.

Virtual Volumes asigna discos virtuales y sus derivados, clones, instantáneas y réplicas directamente a los objetos, llamados volúmenes virtuales, en un sistema de almacenamiento. Esta asignación permite que vSphere asigne operaciones de almacenamiento intensivas, como la creación de instantáneas, la clonación y la replicación, en el sistema de almacenamiento.

Al crear un volumen para cada disco virtual, es posible establecer directrices en un nivel óptimo. Se puede determinar de manera anticipada cuáles son los requisitos de almacenamiento de una aplicación y, posteriormente, comunicárselos al sistema de almacenamiento para que cree un disco virtual adecuado en función de esos requisitos. Por ejemplo, si la máquina virtual requiere una matriz de almacenamiento activa/activa, ya no será necesario seleccionar un almacén de datos que admita el modelo activo/activo, sino que se deberá crear un volumen virtual individual que se ubicará de forma automática en la matriz activa/activa.

Este capítulo incluye los siguientes temas:

- [Conceptos de Virtual Volumes](#)
- [Instrucciones sobre el uso de Virtual Volumes](#)
- [Virtual Volumes y protocolos de almacenamiento](#)
- [Arquitectura de Virtual Volumes](#)
- [Virtual Volumes y VMware Certificate Authority](#)
- [Antes de habilitar Virtual Volumes](#)
- [Configurar Virtual Volumes](#)
- [Aprovisionar máquinas virtuales en almacenes de datos virtuales](#)

Conceptos de Virtual Volumes

Con Virtual Volumes, los contenedores de almacenamiento abstracto reemplazan a los volúmenes de almacenamiento tradicionales basados en recursos compartidos de NFS o LUN. En vCenter Server, los almacenes de datos virtuales representan los contenedores de almacenamiento. Los almacenes de datos virtuales quitan los límites artificiales de los almacenes de datos tradicionales y se usan para almacenar volúmenes virtuales, objetos que encapsulan archivos de máquina virtual.

Mire el vídeo para conocer más sobre los diferentes componentes de la funcionalidad Virtual Volumes.



Virtual Volumes Parte 1: Conceptos

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_jvj5idt3/uiConfId/49694343/)

- [Virtual Volumes](#)

Los volúmenes virtuales son encapsulaciones de archivos de máquinas virtuales, discos virtuales y sus derivados.
- [Virtual Volumes y proveedores de almacenamiento](#)

Un proveedor de almacenamiento de Virtual Volumes, también denominado proveedor VASA, es un componente de software que actúa como servicio de reconocimiento del almacenamiento de vSphere. El proveedor media la comunicación fuera de banda entre vCenter Server y los hosts ESXi, por un lado, y un sistema de almacenamiento, por el otro.

■ Contenedores de almacenamiento

A diferencia del almacenamiento de vSphere basado en LUN y NFS tradicional, la funcionalidad Virtual Volumes no requiere volúmenes preconfigurados en el lado del almacenamiento. En cambio, Virtual Volumes usa un contenedor de almacenamiento, que es un grupo de capacidad de almacenamiento sin procesar o una adición de capacidades de almacenamiento que un sistema de almacenamiento puede proporcionar a los volúmenes virtuales.

■ Extremos de protocolo

A pesar de que los sistemas de almacenamiento administran todos los aspectos de los volúmenes virtuales, los hosts ESXi no tienen acceso directo a los volúmenes virtuales del lado del almacenamiento. En su lugar, los hosts ESXi usan un proxy de E/S lógico, denominado extremo de protocolo, para comunicarse con los volúmenes virtuales y los archivos de disco virtual que encapsulan los volúmenes virtuales. ESXi usa extremos de protocolo para establecer una ruta de acceso de datos a petición desde las máquinas virtuales a sus volúmenes virtuales respectivos.

■ Almacenes de datos virtuales

Un almacén de datos virtual representa un contenedor de almacenamiento en vCenter Server y vSphere Web Client.

■ Virtual Volumes y directivas de almacenamiento de máquina virtual

Una máquina virtual que se ejecuta en un almacén de datos virtual necesita una directiva de almacenamiento de máquina virtual.

Virtual Volumes

Los volúmenes virtuales son encapsulaciones de archivos de máquinas virtuales, discos virtuales y sus derivados.

Los volúmenes virtuales se almacenan de manera nativa en un sistema de almacenamiento que está conectado a través de Ethernet o SAN. Un sistema de almacenamiento compatible los exporta como objetos y el hardware los administra completamente en el lado del almacenamiento. Por lo general, un GUID único identifica un volumen virtual. Los volúmenes virtuales no se aprovisionan previamente, sino que se crean automáticamente al realizar operaciones de administración de máquinas virtuales. Entre estas operaciones se encuentran la creación y la clonación de máquinas virtuales, además de la creación de instantáneas. ESXi y vCenter Server asocian uno o varios volúmenes virtuales con una máquina virtual. El sistema crea los siguientes tipos de volúmenes virtuales para los elementos principales que componen la máquina virtual:

- Un volumen virtual de datos que se corresponde directamente con el archivo `.vmdk` de cada disco virtual. Al igual que los archivos de discos virtuales en almacenes de datos tradicionales, los volúmenes virtuales se presentan como discos SCSI ante las máquinas virtuales.
- Un volumen virtual de configuración, o un directorio de inicio, representa un pequeño directorio que contiene archivos de metadatos para una máquina virtual. Entre los archivos se encuentran un archivo `.vmx`, archivos de descriptores para discos virtuales, archivos de

registro, etc. El volumen virtual de configuración está formateado con un sistema de archivos. Cuando ESXi utiliza el protocolo SCSI para conectarse con el almacenamiento, los volúmenes virtuales de configuración se formatean con VMFS. Con el protocolo NFS, los volúmenes virtuales de configuración se presentan como un directorio NFS.

Pueden crearse volúmenes virtuales adicionales para otros componentes de máquina virtual y derivados de discos virtuales, como clones, instantáneas y réplicas. Estos volúmenes virtuales incluyen un volumen virtual de intercambio para alojar archivos de intercambio de máquinas virtuales y un volumen de memoria virtual para alojar el contenido de la memoria de la máquina virtual de una instantánea.

Al utilizar diferentes volúmenes virtuales para distintos componentes de la máquina virtual, es posible aplicar y manipular directivas de almacenamiento en el nivel de granularidad más fino. Por ejemplo, un volumen virtual que contenga un disco virtual puede tener un conjunto más completo de servicios de datos y niveles de rendimiento que el volumen virtual del disco de arranque de la máquina virtual. De manera similar, un volumen virtual de instantánea puede utilizar un nivel de almacenamiento diferente a comparación de un volumen virtual actual.

Virtual Volumes y proveedores de almacenamiento

Un proveedor de almacenamiento de Virtual Volumes, también denominado proveedor VASA, es un componente de software que actúa como servicio de reconocimiento del almacenamiento de vSphere. El proveedor media la comunicación fuera de banda entre vCenter Server y los hosts ESXi, por un lado, y un sistema de almacenamiento, por el otro.

El proveedor de almacenamiento se implementa a través de VMware API for Storage Awareness (VASA) y se utiliza para administrar todos los aspectos de almacenamiento de Virtual Volumes. El proveedor de almacenamiento se integra con el servicio de supervisión de almacenamiento (SMS), proporcionado con vSphere, para comunicarse con vCenter Server y los hosts ESXi.

El proveedor de almacenamiento proporciona información del almacenamiento subyacente, o el contenedor de almacenamiento en el caso de Virtual Volumes, para que las capacidades del contenedor de almacenamiento puedan aparecer en vCenter Server y vSphere Web Client. A continuación, a su vez, el proveedor de almacenamiento comunica los requisitos de almacenamiento de la máquina virtual, que se pueden definir en la forma de una directiva de almacenamiento, a la capa de almacenamiento. Este proceso de integración garantiza que un volumen virtual creado en la capa de almacenamiento cumpla con los requisitos detallados en la directiva.

Por lo general, los proveedores son los responsables de suministrar proveedores de almacenamiento que puedan integrarse con vSphere y admitir Virtual Volumes. Cada proveedor de almacenamiento debe tener certificación de VMware y estar correctamente implementado. Para obtener información sobre la implementación de un proveedor de almacenamiento de Virtual Volumes, póngase en contacto con el proveedor de almacenamiento.

Una vez implementado el proveedor de almacenamiento, este se debe registrar en vCenter Server, para que pueda comunicarse con vSphere a través de SMS.

Contenedores de almacenamiento

A diferencia del almacenamiento de vSphere basado en LUN y NFS tradicional, la funcionalidad Virtual Volumes no requiere volúmenes preconfigurados en el lado del almacenamiento. En cambio, Virtual Volumes usa un contenedor de almacenamiento, que es un grupo de capacidad de almacenamiento sin procesar o una adición de capacidades de almacenamiento que un sistema de almacenamiento puede proporcionar a los volúmenes virtuales.

Un contenedor de almacenamiento es parte del tejido de almacenamiento lógico y es una unidad lógica del hardware subyacente. El contenedor de almacenamiento agrupa de forma lógica los volúmenes virtuales según las necesidades de administración y gestión. Por ejemplo, el contenedor de almacenamiento puede contener todos los volúmenes virtuales creados para una empresa en una implementación multiempresa o un departamento en una implementación empresarial. Cada contenedor de almacenamiento funciona como un almacén de volúmenes virtuales, y los volúmenes virtuales se asignan de la capacidad del contenedor de almacenamiento.

Generalmente, un administrador de almacenamiento del lado del almacenamiento define los contenedores de almacenamiento. La cantidad de contenedores de almacenamiento, su capacidad y su tamaño dependen de la implementación específica del proveedor, pero se requiere al menos un contenedor para cada sistema de almacenamiento.

Nota Un único contenedor de almacenamiento no puede expandir distintas matrices físicas.

Luego de registrar un proveedor de almacenamiento asociado con el sistema de almacenamiento, vCenter Server detecta todos los contenedores de almacenamiento configurados junto con sus perfiles de funcionalidad de almacenamiento, extremos de protocolo y demás atributos. Un único contenedor de almacenamiento puede exportar varios perfiles de funcionalidad. Como resultado, las máquinas virtuales con distintas necesidades y diferente configuración de directivas de almacenamiento pueden ser parte del mismo contenedor de almacenamiento.

Inicialmente, todos los contenedores de almacenamiento detectados no están conectados a ningún host específico, y no se los puede ver en vSphere Web Client. Para montar un contenedor de almacenamiento, debe asignarlo a un almacén de datos virtual.

Extremos de protocolo

A pesar de que los sistemas de almacenamiento administran todos los aspectos de los volúmenes virtuales, los hosts ESXi no tienen acceso directo a los volúmenes virtuales del lado del almacenamiento. En su lugar, los hosts ESXi usan un proxy de E/S lógico, denominado extremo de protocolo, para comunicarse con los volúmenes virtuales y los archivos de disco virtual que encapsulan los volúmenes virtuales. ESXi usa extremos de protocolo para establecer una ruta de acceso de datos a petición desde las máquinas virtuales a sus volúmenes virtuales respectivos.

Cada volumen virtual está enlazado a un extremo de protocolo específico. Cuando una máquina virtual en el host realiza una operación de E/S, el extremo de protocolo direcciona la E/S al volumen virtual adecuado. Generalmente, un sistema de almacenamiento requiere una cantidad muy pequeña de extremos de protocolo. Un solo extremo de protocolo puede conectarse a cientos o miles de volúmenes virtuales.

Del lado del almacenamiento, el administrador de almacenamiento configura los extremos de protocolo, uno o varios por contenedor de almacenamiento. Los extremos de protocolo son una parte del tejido de almacenamiento físico y el sistema de almacenamiento los exporta, junto con los contenedores de almacenamiento asociados, a través de un proveedor de almacenamiento. Después de asignar un contenedor de almacenamiento a un almacén de datos virtual, ESXi descubre los extremos de protocolo, que se hacen visibles en vSphere Web Client. Los extremos de protocolo también pueden descubrirse cuando se vuelve a examinar el almacenamiento.

En vSphere Web Client, la lista de extremos de protocolo disponibles parece similar a la lista de dispositivos de almacenamiento del host. Pueden usarse distintos transportes de almacenamiento para exponer los extremos de protocolo a ESXi. Cuando se usa el transporte basado en SCSI, el extremo de protocolo representa un LUN de proxy definido por un WWN de LUN basado en T10. Para el protocolo NFS, el extremo de protocolo es un punto de montaje, como una dirección IP y un nombre del recurso compartido. Puede configurar la habilitación de múltiples rutas en un extremo de protocolo basado en SCSI, pero no en un extremo de protocolo basado en NFS. Sin embargo, sin importar el protocolo que use, una matriz de almacenamiento puede proporcionar varios extremos de protocolo para fines de disponibilidad.

Almacenes de datos virtuales

Un almacén de datos virtual representa un contenedor de almacenamiento en vCenter Server y vSphere Web Client.

Una vez que vCenter Server detecta los contenedores de almacenamiento exportados por los sistemas de almacenamiento, es necesario montarlos para poder utilizarlos. Puede utilizar el asistente de creación de almacén de datos en vSphere Web Client para asignar un contenedor de almacenamiento a un almacén de datos virtual. El almacén de datos virtual que crea corresponde directamente al contenedor de almacenamiento específico y se convierte en la representación del contenedor en vCenter Server y vSphere Web Client.

Desde una perspectiva de administrador de vSphere, el almacén de datos virtual es similar a cualquier otro almacén de datos y se usa para mantener máquinas virtuales. Como en los otros almacenes de datos, en el almacén de datos virtual se pueden buscar y enumerar los volúmenes virtuales por nombre de máquina virtual. Como en los almacenes de datos tradicionales, el almacén de datos virtual admite el montaje y el desmontaje. Sin embargo, las operaciones como la actualización y el cambio de tamaño no se aplican al almacén de datos virtual. El administrador de almacenamiento fuera de vSphere puede configurar la capacidad del almacén de datos virtual.

Los almacenes de datos virtuales se pueden usar con almacenes de datos de VMFS y NFS tradicionales, y con Virtual SAN.

Nota El tamaño de un volumen virtual debe ser un múltiplo de 1 MB y tener un tamaño mínimo de 1 MB. Como resultado, todos los discos virtuales que se aprovisionen en un almacén de datos virtual o se migren desde cualquier almacén de datos que no sea el virtual deben tener un tamaño que sea múltiplo par de 1 MB. Si el disco virtual que se migra al almacén de datos virtual no tiene un múltiplo par de 1 MB, extienda el disco manualmente al múltiplo par de 1 MB más próximo.

Virtual Volumes y directivas de almacenamiento de máquina virtual

Una máquina virtual que se ejecuta en un almacén de datos virtual necesita una directiva de almacenamiento de máquina virtual.

Una directiva de almacenamiento de máquina virtual es un conjunto de reglas que contienen requisitos de calidad de servicio y selección de una máquina virtual. Esta directiva aplica una selección adecuada de la máquina virtual dentro del almacenamiento de Virtual Volumes y garantiza que el almacenamiento cumpla los requisitos de la máquina virtual.

La interfaz de directivas de almacenamiento de máquina virtual se utiliza para crear una directiva de almacenamiento de Virtual Volumes. Cuando asigna la directiva nueva a la máquina virtual, la directiva se encarga de que el almacenamiento de Virtual Volumes cumpla los requisitos.

Si no crea una directiva de almacenamiento de máquina virtual compatible con el almacén de datos virtual, el sistema utilizará la directiva predeterminada sin requisitos. Esta es una directiva genérica para Virtual Volumes que no contiene reglas ni especificaciones de almacenamiento. La directiva permite que las matrices de almacenamiento de Virtual Volumes determinen la selección adecuada de los objetos de la máquina virtual.

Instrucciones sobre el uso de Virtual Volumes

La funcionalidad de Virtual Volumes ofrece varios beneficios y ventajas. Al trabajar con Virtual Volumes, debe seguir instrucciones específicas.

Virtual Volumes tiene las siguientes características:

- Virtual Volumes admite la descarga de una variedad de operaciones en el hardware de almacenamiento. Estas operaciones incluyen la creación de instantáneas, la clonación y Storage DRS.
- Con Virtual Volumes, puede usar servicios avanzados de almacenamiento que incluyen la replicación, el cifrado, la deduplicación y la compresión en discos virtuales individuales.
- Virtual Volumes admite características de vSphere como vMotion, Storage vMotion, instantáneas, clones vinculados, Flash Read Cache y DRS.
- Con Virtual Volumes, los proveedores de almacenamiento pueden usar servicios de instantáneas nativas para mejorar el rendimiento de las instantáneas de vSphere.

- Virtual Volumes se puede utilizar con matrices de almacenamiento que admitan vSphere APIs para la integración de matrices (VAAI).
- Virtual Volumes admite el software de creación de copias de seguridad que usa vSphere APIs for Data Protection (VADP).

Instrucciones y limitaciones de Virtual Volumes

Siga estas instrucciones al utilizar Virtual Volumes.

- Debido a que el entorno de Virtual Volumes requiere vCenter Server, Virtual Volumes no se puede utilizar con un host independiente.
- Virtual Volumes no admite RDM.
- Un contenedor de almacenamiento de Virtual Volumes no se puede expandir en matrices físicas diferentes.
- Los perfiles de host que contienen almacenes de datos virtuales son específicos de vCenter Server. Después de extraer este tipo de perfil de host, se lo podrá asociar solamente a los hosts y los clústeres administrados por el mismo vCenter Server que el host de referencia.

Virtual Volumes y protocolos de almacenamiento

La funcionalidad de Virtual Volumes admite canal de fibra, FCoE, iSCSI y NFS. Los transportes de almacenamiento exponen los extremos de protocolo a los hosts ESXi.

Cuando se utiliza el protocolo basado en SCSI, el extremo de protocolo representa un LUN definido por un WWN de LUN basado en T10. Para el protocolo NFS, el extremo de protocolo es un punto de montaje, como una dirección IP o nombre DNS y un nombre del recurso compartido.

Sin importar qué protocolo de almacenamiento se utilice, un volumen virtual, como archivos en otros almacenes de datos tradicionales, se presenta ante una máquina virtual como un disco SCSI. Virtual Volumes en matrices de discos admite el mismo conjunto de comandos SCSI que VMFS y utiliza ATS como mecanismo de bloqueo.

Virtual Volumes en dispositivos NAS admite las mismas llamadas a procedimiento remoto (RPC) de NFS que requieren los hosts ESXi para conectarse a los puntos de montaje de NFS.

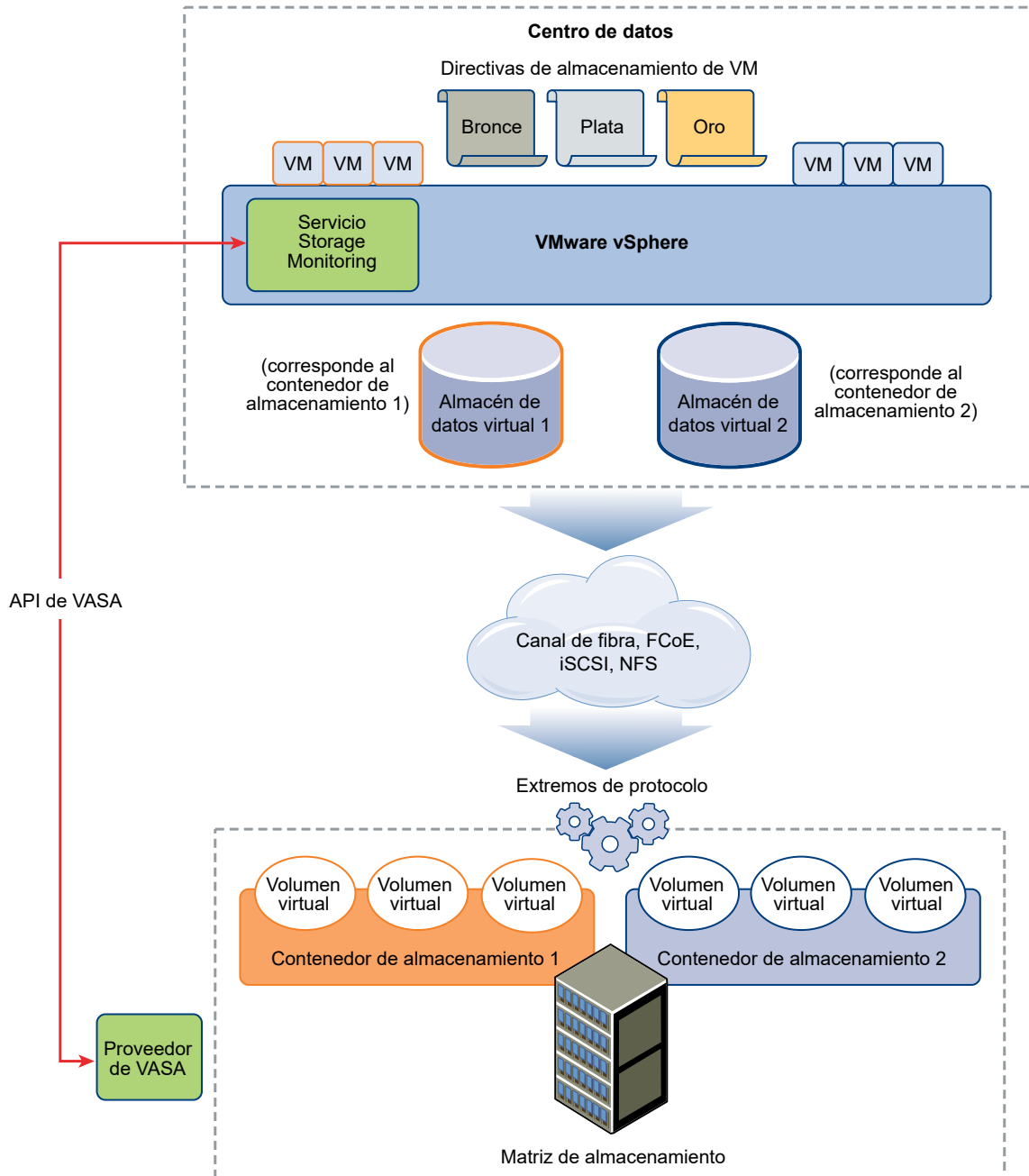
Estas consideraciones e instrucciones aplican cuando se utilizan distintos protocolos de almacenamiento:

- Con NFS, se puede utilizar la versión 3. Virtual Volumes no es compatible con NFS 4.1.
- No se admite el formato IPv6.
- Para iSCSI, debe activar el adaptador de iSCSI de software. Configure Dynamic Discovery (Detección dinámica) y escriba la dirección IP del proveedor de almacenamiento de Virtual Volumes. Consulte [Configurar adaptador de iSCSI de software](#).

- Se pueden configurar múltiples rutas en un extremo de protocolo basado en SCSI, pero no en un extremo de protocolo basado en NFS. Sin importar el protocolo que se utilice, una matriz de almacenamiento puede proporcionar varios extremos de protocolo para fines de disponibilidad.

Arquitectura de Virtual Volumes

Un diagrama arquitectónico proporciona una descripción general de cómo todos los componentes de la funcionalidad de Virtual Volumes interactúan entre sí.



Los volúmenes virtuales son objetos exportados por un sistema de almacenamiento compatible y generalmente se corresponden uno a uno con un disco de máquina virtual y otros archivos relacionados con máquina virtual. Un proveedor VASA crea y manipula fuera de banda, no en la ruta de acceso a los datos, un volumen virtual.

Un proveedor VASA, o un proveedor de almacenamiento, se desarrolla a través de vSphere API for Storage Awareness. El proveedor de almacenamiento habilita la comunicación entre la pila de vSphere (hosts ESXi, vCenter Server y vSphere Web Client), por una parte, y el sistema de almacenamiento, por otra. El proveedor VASA se ejecuta del lado del almacenamiento y se integra con el servicio de supervisión de almacenamiento (SMS) de vSphere para administrar todos los aspectos del almacenamiento de Virtual Volumes. El proveedor VASA asigna objetos de disco virtual y sus derivados, como clones, instantáneas y réplicas, directamente a los volúmenes virtuales del sistema de almacenamiento.

Los hosts ESXi no tienen acceso directo al almacenamiento de volúmenes virtuales. En su lugar, los hosts acceden a los volúmenes virtuales a través de un punto intermedio en la ruta de acceso de datos, denominado extremo de protocolo. Los extremos de protocolo establecen una ruta de acceso de datos a pedido desde las máquinas virtuales a sus volúmenes virtuales respectivos, y sirven de puerta de enlace para las operaciones de E/S dentro de banda entre los hosts ESXi y el sistema de almacenamiento. ESXi puede utilizar los protocolos de Fibre Channel, FCoE, iSCSI y NFS para la comunicación dentro de banda.

Los volúmenes virtuales residen dentro de los contenedores de almacenamiento que lógicamente representan un grupo de discos físicos en el sistema de almacenamiento. En la pila de vSphere, los contenedores de almacenamiento se presentan como almacenes de datos virtuales. Un solo contenedor de almacenamiento puede exportar varios conjuntos de capacidades de almacenamiento. Como resultado, cuando se crea una máquina virtual en el almacén de datos virtual, se pueden utilizar distintas directivas de almacenamiento para colocar los volúmenes virtuales dentro del mismo contenedor de almacenamiento, de forma tal que se cumpla con las distintas necesidades de almacenamiento de una máquina virtual.

Mire el vídeo para obtener información sobre la arquitectura de Virtual Volumes.



Virtual Volumes Parte 2: Arquitectura

(https://vmwaretv.vmware.com/embed/secure/iframe/entryId/1_9e6fnx3m/uiConfId/49694343/)

Virtual Volumes y VMware Certificate Authority

vSphere 6.0.x incluye VMware Certificate Authority (VMCA). De forma predeterminada, VMCA genera todos los certificados internos utilizados en el entorno de vSphere, incluidos los certificados para los hosts ESXi recién agregados y los proveedores VASA de almacenamiento que administran o representan sistemas de almacenamiento de Virtual Volumes.

Los certificados SSL protegen la comunicación con el proveedor VASA. Estos certificados provienen del proveedor VASA o VMCA.

- El proveedor VASA puede ofrecer directamente los certificados para que se utilicen a largo plazo. Pueden ser autogenerados y autofirmados, o bien derivar de una entidad de certificación externa.
- VMCA puede generar los certificados para que el proveedor VASA los utilice.

Cuando se registran un host o un proveedor VASA, VMCA sigue estos pasos automáticamente, sin avisarle al administrador de vSphere.

- 1 Cuando se agrega un proveedor VASA por primera vez al servicio de administración de almacenamiento (SMS) de vCenter Server, se genera un certificado autofirmado.
- 2 Después de comprobar el certificado, SMS pide una solicitud de firma de certificado (CSR) del proveedor VASA.
- 3 Después de recibir y validar la CSR, SMS la presenta a VMCA en nombre del proveedor VASA y solicita un certificado firmado por una entidad de certificación.

Es posible configurar VMCA para que funcione como entidad de certificación independiente o como subordinada a una entidad de certificación empresarial. Si se configura VMCA como una entidad de certificación subordinada, VMCA firma la CSR con la cadena completa.

- 4 Se transfieren el certificado firmado junto con el certificado raíz al proveedor VASA para que autentique todas las conexiones seguras futuras que provengan de SMS en vCenter Server y en los hosts ESXi.

Antes de habilitar Virtual Volumes

Para trabajar con Virtual Volumes, debe asegurarse de que el almacenamiento y el entorno de vSphere estén configurados correctamente.

Siga estas instrucciones para preparar el entorno del sistema de almacenamiento para Virtual Volumes. Para obtener información adicional, póngase en contacto con el proveedor de almacenamiento.

- El sistema de almacenamiento o la matriz de almacenamiento que utiliza debe poder admitir Virtual Volumes e integrarse con vSphere a través de vSphere API for Storage Awareness (VASA).
- Se debe implementar un proveedor de almacenamiento de Virtual Volumes.
- Se deben configurar los extremos de protocolo, los contenedores de almacenamiento y los perfiles de almacenamiento del lado del almacenamiento.

Prepare el entorno de vSphere.

- Asegúrese de seguir las instrucciones de instalación específicas del tipo de almacenamiento que utilice, canal de fibra, FCoE, iSCSI o NFS. Si es necesario, instale y configure los adaptadores de almacenamiento en los hosts ESXi.

Si utiliza iSCSI, active los adaptadores de iSCSI en los hosts ESXi. Configure Dynamic Discovery (Detección dinámica) y escriba la dirección IP del sistema de almacenamiento de Virtual Volumes.

- Sincronice todos los componentes en la matriz de almacenamiento con vCenter Server y todos los hosts ESXi. Utilice el protocolo Network Time Protocol (NTP) para realizar esta sincronización.

Sincronizar el entorno de almacenamiento de vSphere con un servidor horario de red

Antes de habilitar Virtual Volumes, compruebe que todas las máquinas de la red de vSphere tengan los relojes sincronizados.

Procedimiento

- 1 Seleccione el host en el inventario de vSphere.
- 2 Haga clic en la pestaña **Administrar** y en **Configuración**.
- 3 En la sección Sistema, seleccione **Configuración de hora**.
- 4 Haga clic en **Editar** y configure el servidor NTP.
 - a Seleccione **Usar protocolo de hora de red (Habilitar el cliente NTP)**.
 - b Establezca la directiva de inicio del servicio NTP.
 - c Introduzca la dirección IP de los servidores NTP con los que desea realizar la sincronización.
 - d En la sección Estado del servicio NTP, haga clic en **Iniciar** o **Reiniciar**.
- 5 Haga clic en **Aceptar**.
El host se sincroniza con el servidor NTP.

Configurar Virtual Volumes

Para configurar el entorno de Virtual Volumes, se deben completar una serie de pasos.

Requisitos previos

Siga las instrucciones que se incluyen en [Antes de habilitar Virtual Volumes](#).

Procedimiento

1 Registrar proveedores de almacenamiento de Virtual Volumes

El entorno de Virtual Volumes debe incluir proveedores de almacenamiento, también llamados proveedores VASA. Por lo general, los distribuidores independientes desarrollan proveedores de almacenamiento a través de VMware API for Storage Awareness (VASA). Los proveedores de almacenamiento facilitan la comunicación entre vSphere y el lado de almacenamiento. Debe registrar el proveedor de almacenamiento en vCenter Server para poder trabajar con Virtual Volumes.

2 Crear un almacén de datos virtual

Puede utilizar el asistente **New Datastore** (Nuevo almacén de datos) para crear un almacén de datos virtual.

3 Revisar y administrar extremos de protocolo

Los hosts ESXi utilizan un proxy de E/S lógico, denominado extremo de protocolo, para comunicarse con volúmenes virtuales y archivos de discos virtuales que los volúmenes virtuales encapsulan. A través de un proveedor de almacenamiento, el sistema de almacenamiento exporta los extremos de protocolo junto con los contenedores de almacenamiento asociados. Los extremos de protocolo se vuelven visibles en vSphere Web Client después de asignar un contenedor de almacenamiento a un almacén de datos virtual. Es posible revisar las propiedades de los extremos de protocolo y modificar opciones especiales.

4 (opcional) Cambiar la directiva de selección de rutas de acceso para un extremo de protocolo

Si el host ESXi utiliza transporte basado en SCSI para comunicarse con extremos de protocolo que representan a una matriz de almacenamiento, se pueden modificar las directivas de múltiples rutas asignadas a los extremos de protocolo. Utilice el cuadro de diálogo **Edit Multipathing Policies** (Editar directivas de múltiples rutas) para cambiar una directiva de selección de rutas de acceso.

Pasos siguientes

Ahora puede aprovisionar máquinas virtuales en el almacén de datos virtual. Para obtener más información sobre cómo crear máquinas virtuales, consulte la documentación de *Administración de máquinas virtuales de vSphere*.

Para obtener información sobre solución de problemas, consulte la documentación de *Solución de problemas de vSphere*.

Registrar proveedores de almacenamiento de Virtual Volumes

El entorno de Virtual Volumes debe incluir proveedores de almacenamiento, también llamados proveedores VASA. Por lo general, los distribuidores independientes desarrollan proveedores

de almacenamiento a través de VMware API for Storage Awareness (VASA). Los proveedores de almacenamiento facilitan la comunicación entre vSphere y el lado de almacenamiento. Debe registrar el proveedor de almacenamiento en vCenter Server para poder trabajar con Virtual Volumes.

Después del registro, el proveedor de Virtual Volumes se comunica con vCenter Server e informa de las características del almacenamiento subyacente. Las características aparecen en la interfaz de las directivas de almacenamiento de máquina virtual y pueden usarse para crear una directiva de almacenamiento de máquina virtual compatible con el almacén de datos virtual. Después de aplicar esta directiva de almacenamiento a una máquina virtual, la directiva se aplica al almacenamiento de Virtual Volumes. Esta directiva aplica una selección óptima de la máquina virtual dentro del almacenamiento de Virtual Volumes y garantiza que el almacenamiento pueda satisfacer los requisitos de la máquina virtual.

Requisitos previos

Compruebe que el componente del proveedor de almacenamiento esté instalado en el lado del almacenamiento y solicítele las credenciales correspondientes al administrador de almacenamiento. Para obtener más información, póngase en contacto con el proveedor.

Procedimiento

- 1 Desplácese hasta vCenter Server en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar** y, a continuación, en **Proveedores de almacenamiento**.
- 3 Haga clic en el icono **Register a new storage provider** (Registrar un nuevo proveedor de almacenamiento).
- 4 (opcional) Para dirigir vCenter Server al certificado del proveedor de almacenamiento, seleccione la opción **Use storage provider certificate** (Usar certificado de proveedor de almacenamiento) y especifique la ubicación del certificado.

Si no selecciona esta opción, aparecerá la huella digital del certificado. Revise la huella digital y apruébela.

- 5 Haga clic en **OK** (Aceptar) para completar el registro.

Resultados

vCenter Server detecta y registra el proveedor de almacenamiento de Virtual Volumes.

Crear un almacén de datos virtual

Puede utilizar el asistente **New Datastore** (Nuevo almacén de datos) para crear un almacén de datos virtual.

Procedimiento

- 1 En el navegador de vSphere Web Client, seleccione **Listas de inventario global > Almacenes de datos**.

- 2 Haga clic en el icono **Nuevo almacén de datos**.
- 3 Escriba el nombre del almacén de datos y, si es necesario, seleccione la ubicación en la que colocará el almacén de datos.

Asegúrese de utilizar un nombre que no duplique el de otro almacén de datos en el entorno del centro de datos.

Si monta el mismo almacén de datos virtual en varios hosts, el nombre del almacén de datos debe ser uniforme entre todos los hosts.
- 4 Seleccione **VVOL** como tipo de almacén de datos.
- 5 En la lista de contenedores de almacenamiento, seleccione un contenedor de almacenamiento de respaldo.
- 6 Seleccione los hosts que requieren acceso al almacén de datos.
- 7 Revise las opciones de configuración y haga clic en **Finish** (Finalizar).

Pasos siguientes

Después de crear el almacén de datos virtual, puede realizar operaciones de almacenes de datos como cambiar el nombre del almacén de datos, explorar los archivos del almacén de datos, desmontar el almacén de datos, etc.

No puede agregar el almacén de datos virtual a un clúster de almacenes de datos.

Revisar y administrar extremos de protocolo

Los hosts ESXi utilizan un proxy de E/S lógico, denominado extremo de protocolo, para comunicarse con volúmenes virtuales y archivos de discos virtuales que los volúmenes virtuales encapsulan. A través de un proveedor de almacenamiento, el sistema de almacenamiento exporta los extremos de protocolo junto con los contenedores de almacenamiento asociados. Los extremos de protocolo se vuelven visibles en vSphere Web Client después de asignar un contenedor de almacenamiento a un almacén de datos virtual. Es posible revisar las propiedades de los extremos de protocolo y modificar opciones especiales.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Protocol Endpoints** (Extremos de protocolo).
- 4 Para ver los detalles de un elemento específico, selecciónelo en la lista.

- 5 Utilice las pestañas en Protocol Endpoint Details (Detalles del extremo de protocolo) para acceder a información adicional y modificar las propiedades del extremo de protocolo seleccionado.

Pestaña	Descripción
Properties (Propiedades)	Muestra las propiedades y las características del elemento. Para los elementos SCSI (en bloque), muestra directivas de múltiples rutas y permite editarlas.
Paths (SCSI protocol endpoints only) (Rutas de acceso [solo extremos de protocolo SCSI])	Muestra las rutas de acceso disponibles para el extremo de protocolo. Permite deshabilitar o habilitar una ruta de acceso seleccionada. Permite cambiar la directiva de selección de rutas de acceso.
Almacenes de datos	Muestra el almacén de datos virtual correspondiente. Permite realizar operaciones de administración de almacenes de datos.

Cambiar la directiva de selección de rutas de acceso para un extremo de protocolo

Si el host ESXi utiliza transporte basado en SCSI para comunicarse con extremos de protocolo que representan a una matriz de almacenamiento, se pueden modificar las directivas de múltiples rutas asignadas a los extremos de protocolo. Utilice el cuadro de diálogo **Edit Multipathing Policies** (Editar directivas de múltiples rutas) para cambiar una directiva de selección de rutas de acceso.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 Haga clic en **Protocol Endpoints** (Extremos de protocolo).
- 4 Seleccione el extremo de protocolo cuyas rutas de acceso desea cambiar y haga clic en la pestaña **Properties** (Propiedades).
- 5 En Multipathing Policies (Directivas de múltiples rutas), haga clic en **Edit Multipathing** (Editar múltiples rutas).
- 6 Seleccione una directiva de ruta de acceso.
 - Fixed (Fija) (VMware)
 - Most Recently Used (Utilizados más recientemente) (VMware)
 - Round robin (VMware)
- 7 Para la directiva fija, especifique la ruta de acceso preferida.
- 8 Haga clic en **OK** (Aceptar) para guardar la configuración y salir del cuadro de diálogo.

Aprovisionar máquinas virtuales en almacenes de datos virtuales

Puede aprovisionar máquinas virtuales en un almacén de datos virtual.

Nota Todos los discos virtuales que aprovisione en un almacén de datos virtual deben ser un múltiplo par de 1 MB.

Una máquina virtual que se ejecute en un almacén de datos virtual necesita una directiva de almacenamiento de máquina virtual apropiada.

Después de aprovisionar la máquina virtual, es posible realizar las tareas de administración de máquina virtual típicas. Para obtener información, consulte la documentación de *Administración de máquinas virtuales de vSphere*.

Para obtener información sobre solución de problemas, consulte la documentación de *Solución de problemas de vSphere*.

Procedimiento

1 Definir una directiva de almacenamiento de máquina virtual para Virtual Volumes

Puede crear una directiva de almacenamiento de máquina virtual compatible con un almacén de datos virtual.

2 Asignar la directiva de almacenamiento de Virtual Volumes a máquinas virtuales

Para garantizar que el almacén de datos virtual cumpla con los requisitos de almacenamiento específicos cuando asigne una máquina virtual, asocie la directiva de almacenamiento de Virtual Volumes con la máquina virtual.

3 Cambiar la directiva de almacenamiento predeterminada de un almacén de datos virtual

Para máquinas virtuales aprovisionadas en almacenes de datos virtuales, VMware ofrece una directiva sin requisitos predeterminada. No es posible editar esta directiva, pero se puede designar una directiva recién creada como la predeterminada.

Definir una directiva de almacenamiento de máquina virtual para Virtual Volumes

Puede crear una directiva de almacenamiento de máquina virtual compatible con un almacén de datos virtual.

Requisitos previos

Compruebe que el proveedor de almacenamiento de Virtual Volumes esté disponible y activo. Consulte [Registrar proveedores de almacenamiento de Virtual Volumes](#).

Procedimiento

- 1 En la página de inicio de vSphere Web Client, haga clic en **Directivas y perfiles > Directivas de almacenamiento de máquina virtual**.

- 2 Haga clic en el icono **Crear una nueva directiva de almacenamiento de máquina virtual**.
- 3 Seleccione la instancia de vCenter Server.
- 4 Escriba un nombre y una descripción para la directiva de almacenamiento y haga clic en **Siguiente**.

- 5 En la página Conjunto de reglas, seleccione el proveedor de almacenamiento de Virtual Volumes en el menú desplegable **Reglas basadas en servicios de datos**.

La página se expande para mostrar los servicios de datos que proporciona el recurso de almacenamiento de Virtual Volumes.

- 6 Seleccione el servicio de datos que desea incluir y especifique su valor.

Asegúrese de que los valores que proporciona estén dentro del rango de los valores anunciados por el perfil de Virtual Volumes.

Según lo que introduzca, el mecanismo de consumo de almacenamiento calcula la cantidad de espacio necesario para un disco virtual que residirá en el almacén de datos virtual.

- 7 Complete la creación de la directiva de almacenamiento y haga clic en **Finalizar**.

Resultados

La nueva directiva de almacenamiento de máquina virtual compatible con Virtual Volumes aparecerá en la lista.

Pasos siguientes

Ahora es posible asociar esta directiva con una máquina virtual o designarla como predeterminada.

Asignar la directiva de almacenamiento de Virtual Volumes a máquinas virtuales

Para garantizar que el almacén de datos virtual cumpla con los requisitos de almacenamiento específicos cuando asigne una máquina virtual, asocie la directiva de almacenamiento de Virtual Volumes con la máquina virtual.

Es posible asignar la directiva de almacenamiento de Virtual Volumes durante una implementación inicial de una máquina virtual, o cuando se realicen otras operaciones de máquina virtual, como una clonación o una migración. Este tema describe cómo asignar la directiva de almacenamiento de Virtual Volumes cuando se crea una máquina virtual nueva. Para obtener información sobre otros métodos de aprovisionamiento de máquina virtual, consulte la documentación de *Administración de máquinas virtuales de vSphere*.

Se puede aplicar la misma directiva de almacenamiento al archivo de configuración de máquina virtual y a todos los discos virtuales. Si los requisitos de almacenamiento para los discos virtuales y el archivo de configuración son diferentes, se pueden asociar distintas directivas de almacenamiento con el archivo de configuración de máquina virtual y los discos virtuales seleccionados.

Procedimiento

- 1 En vSphere Web Client, inicie el proceso de aprovisionamiento de máquina virtual y siga los pasos adecuados.
- 2 Asigne la misma directiva de almacenamiento a todos los discos y archivos de máquina virtual.
 - a En la página Select Storage (Seleccionar almacenamiento), seleccione la directiva de almacenamiento compatible con Virtual Volumes, por ejemplo VVols Silver, en el menú desplegable **VM Storage Policy** (Directiva de almacenamiento de máquina virtual).
 - b Seleccione el almacén de datos virtual en la lista de almacenes de datos disponibles y haga clic en **Next** (Siguiente).

El almacén de datos se transforma en el recurso de almacenamiento de destino del archivo de configuración de la máquina virtual y de todos los discos virtuales.

- 3 Cambie la directiva de almacenamiento del disco virtual.

Utilice esta opción si los requisitos de selección de almacenamiento son distintos para los discos virtuales.

- a En la página Customize Hardware (Personalizar hardware), expanda el panel New hard disk (Nuevo disco duro).
 - b En el menú desplegable **VM storage policy** (Directiva de almacenamiento de máquina virtual), seleccione la directiva de almacenamiento adecuada, por ejemplo VVols Gold, que desea asignar al disco virtual.
- 4 Complete el proceso de aprovisionamiento de máquina virtual.

Resultados

Una vez creada la máquina virtual, la pestaña **Summary** (Resumen) muestra las directivas de almacenamiento asignadas y su estado de cumplimiento.

Pasos siguientes

Si los requisitos de selección de almacenamiento del archivo de configuración o los discos virtuales cambian, se puede modificar la asignación de la directiva virtual posteriormente. Consulte [Cambiar la asignación de directivas de almacenamiento para archivos y discos de máquinas virtuales](#).

Cambiar la directiva de almacenamiento predeterminada de un almacén de datos virtual

Para máquinas virtuales aprovisionadas en almacenes de datos virtuales, VMware ofrece una directiva sin requisitos predeterminada. No es posible editar esta directiva, pero se puede designar una directiva recién creada como la predeterminada.

Requisitos previos

Cree una directiva de almacenamiento compatible con Virtual Volumes.

Procedimiento

- 1 Desplácese hasta el almacén de datos virtual para el que desea cambiar la directiva de almacenamiento.
- 2 Haga clic en la pestaña **Manage** (Administrar) y, a continuación, en **Settings** (Configuración).
- 3 Haga clic en **General** y, a continuación, haga clic en **Edit** (Editar) en el panel Default Storage Policy (Directiva de almacenamiento predeterminada).
- 4 En la lista de directivas de almacenamiento disponibles, seleccione la que desee designar como predeterminada y haga clic en **OK** (Aceptar).

Resultados

La directiva de almacenamiento seleccionada se convertirá en la predeterminada para el almacén de datos virtual. vSphere asigna esta directiva a todos los objetos de máquinas virtuales que aprovisionen en el almacén de datos virtual cuando no se selecciona explícitamente otra directiva.

Directivas de almacenamiento de máquinas virtuales

20

Las directivas de almacenamiento de las máquinas virtuales son fundamentales para el aprovisionamiento de las máquinas virtuales. Estas directivas ayudan a definir los requisitos de almacenamiento para la máquina virtual y a controlar qué tipo de almacenamiento se proporciona para la máquina virtual, cómo se coloca la máquina virtual en el almacenamiento y qué servicios de datos se ofrecen para la máquina virtual.

Cuando se define una directiva de almacenamiento, se especifican los requisitos de almacenamiento para las aplicaciones que se ejecutan en máquinas virtuales. Después de aplicar esta directiva de almacenamiento a una máquina virtual, la máquina virtual se coloca en un almacén de datos específico que puede satisfacer los requisitos de almacenamiento. En los entornos de almacenamiento definidos por software, como Virtual SAN y Virtual Volumes, la directiva de almacenamiento también determina cómo los objetos de almacenamiento de máquina virtual se aprovisionan y asignan dentro del recurso de almacenamiento para garantizar el nivel de servicio requerido. En entornos con filtros de E/S externos instalados, es posible utilizar directivas de almacenamiento para habilitar un nivel adicional de servicios de datos, como almacenamiento en caché y replicación, para discos virtuales.

Este capítulo incluye los siguientes temas:

- [Actualizar perfiles de almacenamiento heredados](#)
- [Descripción de las directivas de almacenamiento de máquinas virtuales](#)
- [Trabajar con directivas de almacenamiento de máquinas virtuales](#)
- [Crear y administrar directivas de almacenamiento de máquina virtual](#)
- [Directivas de almacenamiento y máquinas virtuales](#)

Actualizar perfiles de almacenamiento heredados

En vSphere 5.x, las directivas de almacenamiento de máquina virtual se denominaban perfiles de almacenamiento y tenían un formato diferente. Cuando se actualiza el entorno vSphere de la versión 5.x a vSphere 6.x, los perfiles de almacenamiento creados en las versiones anteriores se convierten a directivas de almacenamiento.

Todos los componentes de los perfiles de almacenamiento heredados se transforman en formatos u objetos nuevos. Cualquier funcionalidad de almacenamiento definida por el sistema se convierte a servicios de datos específicos del almacenamiento en función de los metadatos. Las funcionalidades definidas por el usuario se convierten en etiquetas de almacén de datos.

Tabla 20-1. Formatos antiguos y nuevos de directivas de almacenamiento

vSphere 5.x	vSphere 6.x
Perfil de almacenamiento de máquina virtual	Directiva de almacenamiento de la máquina virtual
Funcionalidades definidas por el sistema	Servicios de datos específicos del almacenamiento
Funcionalidades definidas por el usuario	Etiquetas de almacén de datos
N/C	Servicios de datos comunes

Descripción de las directivas de almacenamiento de máquinas virtuales

Las directivas de almacenamiento de máquinas virtuales almacenan características que requieren los archivos de inicio y los discos virtuales de las máquinas virtuales para ejecutar aplicaciones dentro de la máquina virtual. Puede crear varias directivas de almacenamiento para definir los tipos y las clases de requisitos de almacenamiento.

Cada directiva de almacenamiento no es solo un conjunto de limitaciones que se aplican simultáneamente. Una sola directiva puede incluir conjuntos alternativos de subdirectivas, o conjuntos de reglas, que son específicos del almacén de datos y representan requisitos de almacenamiento igualmente aceptables. Si se utiliza vSphere API para los filtros de E/S, la directiva de almacenamiento puede incluir reglas que sean comunes para todos los tipos de almacenamiento. La directiva puede contener solo reglas comunes, conjuntos de reglas específicos de un almacén de datos solamente, o bien ambos.

Cuando crea, clona o migra una máquina virtual, puede aplicar la directiva de almacenamiento a la máquina virtual. Puede colocar la máquina virtual en uno de los almacenes de datos que coincida con los requisitos de la directiva. Para cumplir con el requisito de la directiva, el almacén de datos debe cumplir estas directrices:

- Cuando los filtros de E/S y las reglas comunes no estén disponibles, el almacén de datos debe cumplir con todas las reglas en al menos uno de los conjuntos de reglas específicos del almacén de datos.
- Con las reglas comunes habilitadas, el almacén de datos debe cumplir con todas las reglas comunes y todas las reglas en al menos uno de los conjuntos de reglas.

Los archivos de inicio (.vmx, .vmsd, .nvram, .log, etc.) y los discos virtuales (.vmdk) de la máquina virtual pueden tener directivas de almacenamiento individuales.

Tabla 20-2. Ejemplo de directiva de almacenamiento de una máquina virtual

Ejemplo de archivos de una máquina virtual	Ejemplo de una directiva de almacenamiento	Ejemplo de un almacén de datos que cumple con la directiva de almacenamiento
<i>windows_2008r2_test.vmx</i>		
<i>windows_2008r2_test.vmxfs</i>		
<i>windows_2008r2_test.log</i>		
<i>windows_2008r2_test.nvram</i>	Directiva de almacenamiento 2	datastore02, datastore05, datastore10
<i>windows_2008r2_test.vmem</i>		
<i>windows_2008r2_test.vmsd</i>		
<i>windows_2008r2_test.vmdk</i>	Directiva de almacenamiento 3	datastore05
<i>windows_2008r2_test_1.vmdk</i>	Directiva de almacenamiento 5	datastore10
k		

Directivas y reglas de almacenamiento

Las reglas que se incluyen en una directiva de almacenamiento pueden basarse en etiquetas o servicios de datos específicos del almacenamiento, o bien las reglas pueden ser comunes.

■ Reglas comunes

Las reglas comunes se basan en los servicios de datos que son genéricos para todo tipo de almacenamiento y no dependen del almacén de datos. Estos servicios adicionales aparecen disponibles en la interfaz de directivas de almacenamiento de máquina virtual cuando se instalan filtros de E/S de terceros desarrollados mediante vSphere API para el filtrado de E/S. Es posible hacer referencia a estos servicios de datos en una directiva de almacenamiento de máquina virtual.

■ Reglas basadas en servicios de datos específicos de almacenamiento

Estas reglas se basan en servicios de datos que anuncian entidades de almacenamiento, como Virtual SAN y Virtual Volumes.

■ Reglas basadas en etiquetas

Las reglas basadas en etiquetas hacen referencia a etiquetas de almacenes de datos asociadas con almacenes de datos específicos. Es posible aplicar más de una etiqueta a un almacén de datos.

Reglas comunes

Las reglas comunes se basan en los servicios de datos que son genéricos para todo tipo de almacenamiento y no dependen del almacén de datos. Estos servicios adicionales aparecen disponibles en la interfaz de directivas de almacenamiento de máquina virtual cuando se instalan filtros de E/S de terceros desarrollados mediante vSphere API para el filtrado de E/S. Es posible hacer referencia a estos servicios de datos en una directiva de almacenamiento de máquina virtual.

A diferencia de las reglas específicas del almacenamiento, las reglas comunes no definen la selección de almacenamiento ni los requisitos de almacenamiento para una máquina virtual, pero garantizan que esos servicios de datos adicionales, como los filtros de E/S, se habiliten para la máquina virtual. Independientemente del almacén de datos en que se ejecute la máquina virtual, los filtros habilitados pueden proporcionar los siguientes servicios:

- Almacenamiento en caché. Configura una memoria caché para los datos de disco virtual. El filtro puede utilizar una memoria caché local o un dispositivo de almacenamiento flash para almacenar los datos en caché y aumentar las operaciones de entrada/salida por segundo y las tasas de utilización de hardware del disco virtual.
- Replicación. Replica la máquina virtual o los discos virtuales en destinos externos como otro host o clúster.

Para obtener más información sobre los filtros de entrada/salida, consulte [Capítulo 21 Filtrar E/S de máquinas virtuales](#).

Reglas basadas en servicios de datos específicos de almacenamiento

Estas reglas se basan en servicios de datos que anuncian entidades de almacenamiento, como Virtual SAN y Virtual Volumes.

Para ofrecer información sobre el almacenamiento subyacente a vCenter Server, Virtual SAN y Virtual Volumes utilizan proveedores de almacenamiento, también denominados proveedores VASA. La información de almacenamiento y las características del almacén de datos aparecen en la interfaz de las directivas de almacenamiento de máquina virtual de vSphere Web Client como servicios de datos ofrecidos por el tipo de almacén de datos específico.

Un solo almacén de datos puede ofrecer varios servicios. Los servicios de datos se agrupan en un perfil de almacén de datos que describe la calidad de servicio que puede ofrecer el almacén de datos.

Cuando se crean reglas para una directiva de almacenamiento de máquina virtual, se hace referencia a servicios de datos que anuncia un almacén de datos específico. Para la máquina virtual que utiliza esta directiva, el almacén de datos garantiza que pueda satisfacer los requisitos de almacenamiento de la máquina virtual. El almacén de datos también puede ofrecerle a la máquina virtual un conjunto de características específicas de capacidad, rendimiento, disponibilidad, redundancia, entre otras.

Para obtener más información sobre proveedores de almacenamiento, consulte [Capítulo 25 Usar proveedores de almacenamiento](#).

Reglas basadas en etiquetas

Las reglas basadas en etiquetas hacen referencia a etiquetas de almacenes de datos asociadas con almacenes de datos específicos. Es posible aplicar más de una etiqueta a un almacén de datos.

Por lo general, las etiquetas sirven para lo siguiente:

- Asocian una definición de nivel de almacenamiento amplio a almacenes de datos que no están representados por ningún proveedor de almacenamiento, por ejemplo, almacenes de datos de VMFS y NFS.
- Codifican información importante para la directiva que no se anuncia a través de vSphere API for Storage Awareness (VASA), como la ubicación geográfica o el grupo administrativo.

De manera similar a los servicios específicos de almacenamiento, todas las etiquetas asociadas con almacenes de datos aparecen en la interfaz de las directivas de almacenamiento de máquina virtual. Puede utilizar las etiquetas cuando define reglas para directivas de almacenamiento.

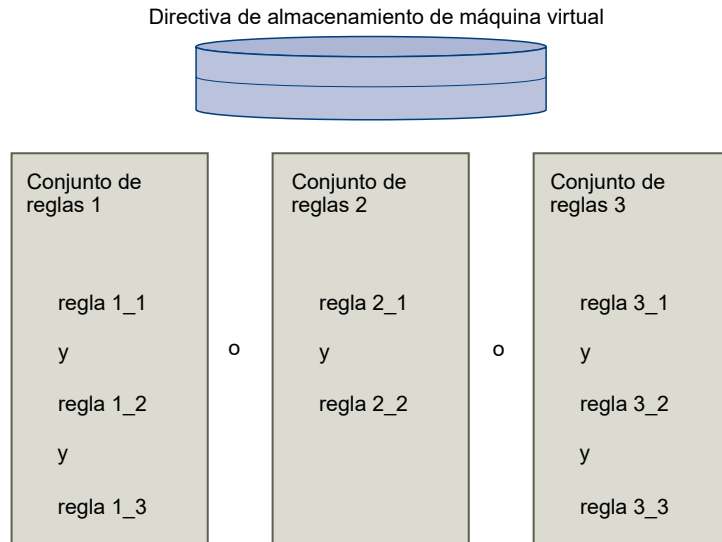
Acerca de los conjuntos de reglas específicos y comunes de los almacenes de datos

Una directiva de almacenamiento puede incluir uno o varios conjuntos de reglas que describen los requisitos de los recursos de almacenamiento de máquinas virtuales. También puede incluir reglas comunes.

Si las reglas comunes no están disponibles en el entorno o no se definen, es posible crear una directiva que incluya conjuntos de reglas específicos de un almacén de datos. Para definir una directiva, se requiere un conjunto de reglas. Los conjuntos de reglas adicionales son opcionales. Varios conjuntos de reglas permiten que una sola directiva defina parámetros de selección alternativos, con frecuencia de distintos proveedores de almacenamiento.

Un conjunto de reglas individual contiene una o varias reglas. Cada regla puede basarse en un servicio de datos subyacente individual garantizado por una entidad de almacenamiento. La regla describe una calidad o cantidad específicas que el recurso de almacenamiento debe proporcionar. En las reglas, también se puede hacer referencia a etiquetas de almacenes de datos definidas por el usuario. Un conjunto de reglas específico de un almacén de datos puede incluir reglas de una sola entidad de almacenamiento.

La relación entre todos los conjuntos de reglas dentro de una directiva se define por medio del operador booleano OR, mientras que la relación entre todas las reglas dentro de un solo conjunto de reglas se define por medio de AND. Cumplir con todas las reglas de cualquier conjunto de reglas es suficiente para cumplir toda la directiva. Cada conjunto de reglas representa un conjunto de limitaciones igualmente aceptables.



Si las reglas comunes se encuentran habilitadas, la directiva debe incluir reglas comunes o al menos un conjunto de reglas específico de un almacén de datos. Si se definen las reglas comunes y las reglas específicas de un almacén de datos, la directiva de almacenamiento busca coincidencias con almacenes de datos que cumplan con todas las reglas comunes y todas las reglas en al menos uno de los conjuntos de reglas.

Trabajar con directivas de almacenamiento de máquinas virtuales

El proceso completo de creación y administración de directivas de almacenamiento generalmente incluye varios pasos. Según el tipo de servicios de datos o almacenamiento que ofrezca el entorno, es posible que deba realizar algún paso específico.

- 1 Si utiliza directivas de almacenamiento con proveedores de almacenamiento, compruebe que se registre un proveedor de almacenamiento adecuado. Las entidades que requieren proveedores de almacenamiento son Virtual SAN, Virtual Volumes y filtros de E/S que ofrecen servicios de datos de software adicional a máquinas virtuales.

Consulte [Capítulo 25 Usar proveedores de almacenamiento](#).
- 2 Aplique las etiquetas de almacenamiento a los almacenes de datos. Consulte [Asignar etiquetas a almacenes de datos](#).
- 3 Cree directivas de almacenamiento mediante la definición de requisitos para las aplicaciones que se ejecutan en una máquina virtual. Consulte [Definir una directiva de almacenamiento para una máquina virtual](#).
- 4 Aplique la directiva de almacenamiento de máquina virtual a una máquina virtual. Puede aplicar la directiva de almacenamiento al implementar la máquina virtual o configurar sus discos virtuales. Consulte [Asignar directivas de almacenamiento a máquinas virtuales](#).

- 5 Cambie la directiva de almacenamiento de los discos virtuales o los archivos de inicio de la máquina virtual. Consulte [Cambiar la asignación de directivas de almacenamiento para archivos y discos de máquinas virtuales](#).
- 6 Compruebe que las máquinas virtuales y los discos virtuales utilicen almacenes de datos que cumplan con la directiva de almacenamiento asignada. Consulte [Comprobar el cumplimiento de una directiva de almacenamiento de máquina virtual](#).

Crear y administrar directivas de almacenamiento de máquina virtual

Para habilitar, crear y administrar directivas de almacenamiento de máquinas virtuales, por lo general, se puede utilizar la interfaz de directivas de almacenamiento de máquina virtual de vSphere Web Client.

Si utiliza directivas de almacenamiento de Virtual SAN, Virtual Volumes o filtros de entrada/salida, consulte la documentación para obtener más información:

- *Administración de VMware Virtual SAN*
- [Capítulo 19 Trabajar con Virtual Volumes](#)
- [Capítulo 21 Filtrar E/S de máquinas virtuales](#)

Asignar etiquetas a almacenes de datos

Cuando el almacén de datos no está representado por un proveedor de almacenamiento y no muestra sus capacidades y servicios de datos en la interfaz de directivas de almacenamiento de máquina virtual, use las etiquetas para codificar información sobre el almacén de datos. Puede hacer referencia a estas etiquetas cuando define una directiva de almacenamiento para una máquina virtual.

Puede aplicar una etiqueta nueva que contiene información de almacenamiento en un almacén de datos. Para obtener información sobre estas etiquetas, sus categorías y cómo administrar las etiquetas, consulte la documentación sobre la *administración de vCenter Server y hosts*.

Procedimiento

- 1 Desplácese hasta un almacén de datos en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Manage** (Administrar) y en **Tags** (Etiquetas).
- 3 Haga clic en el icono **New Tag** (Etiqueta nueva).
- 4 En el menú desplegable **vCenter Server**, seleccione la instancia de vCenter Server en la que se creará la etiqueta.
- 5 Escriba un nombre y una descripción para la etiqueta.

Por ejemplo, puede especificar una definición de nivel de almacenamiento amplia, como Gold Storage (Almacenamiento dorado), o indicar una propiedad que no se comunique a través de un proveedor de almacenamiento, como una ubicación geográfica o un grupo administrativo.

Propiedad de etiqueta	Ejemplo
Name (Nombre)	Fault Tolerance
Descripción	El almacenamiento tiene una capacidad superior a 2 TB y tolera errores

- 6 En el menú desplegable **Category** (Categoría), seleccione una categoría existente o cree una nueva.
- 7 (opcional) Cree una categoría:
 - a Seleccione **New Category** (Nueva categoría).
 - b Especifique las opciones de la categoría.

Propiedad de la categoría	Ejemplo
Nombre de la categoría	Categoría de almacenamiento
Descripción	Categoría de etiquetas relacionada con el almacenamiento
Cardinalidad	Many tags per object (Muchas etiquetas por objeto)
Tipos de objeto que se pueden asociar	Datastore (Almacén de datos) y Datastore Cluster (Clúster de almacenes de datos)

- 8 Haga clic en **OK** (Aceptar).

Resultados

La etiqueta nueva se asigna al almacén de datos y aparece en la pestaña **Summary** (Resumen) del panel Tags (Etiquetas).

Pasos siguientes

Puede hacer referencia a la etiqueta cuando agregue reglas basadas en etiquetas a la directiva de almacenamiento. Consulte [Agregar o editar reglas basadas en etiquetas](#). El almacén de datos aparece en una lista de recursos de almacenamiento compatibles de las máquinas virtuales que usan la directiva.

Definir una directiva de almacenamiento para una máquina virtual

Cuando se definen directivas de almacenamiento para las máquinas virtuales, se especifican los requisitos de almacenamiento para las aplicaciones que se ejecutarán en las máquinas virtuales.

Una directiva de almacenamiento puede basarse en los servicios de datos anunciados por una entidad de almacenamiento o en etiquetas de almacén de datos. La directiva también puede hacer referencia a servicios de datos comunes que proporciona el marco de filtros de E/S.

Requisitos previos

- Si utiliza directivas de almacenamiento de máquina virtual con proveedores de almacenamiento, compruebe que se registre un proveedor de almacenamiento adecuado. Consulte [Capítulo 25 Usar proveedores de almacenamiento](#).

- Privilegios necesarios: **Directivas de almacenamiento de máquina virtual.Actualizar y Directivas de almacenamiento de máquina virtual.Ver.**

Procedimiento

1 Iniciar proceso de creación de directivas de almacenamiento de máquina virtual

Para definir una directiva de almacenamiento de máquina virtual, utilice el asistente **Create New VM Storage Policy** (Crear nueva directiva de almacenamiento de máquina virtual).

2 Definir reglas comunes para una directiva de almacenamiento de máquina virtual

Las reglas comunes se basan en los servicios de datos que son genéricos para todo tipo de almacenamiento y no dependen del almacén de datos. Estos servicios de datos pasan a estar disponibles en la interfaz de directivas de almacenamiento de máquina virtual cuando se instalan filtros de E/S de terceros desarrollados mediante vSphere API para los filtros de E/S. Es posible hacer referencia a estos servicios de datos en una directiva de almacenamiento.

3 Crear reglas específicas de almacenamiento para una directiva de almacenamiento de máquina virtual

Las reglas específicas de los almacenes de datos se basan en servicios de datos que anuncian entidades de almacenamiento como Virtual SAN y Virtual Volumes. Para la máquina virtual que utiliza esta directiva, el almacén de datos garantiza que pueda satisfacer los requisitos de almacenamiento de la máquina virtual. El almacén de datos también garantiza que puede ofrecer un conjunto de características específicas de capacidad, rendimiento, disponibilidad, redundancia, entre otras.

4 Agregar o editar reglas basadas en etiquetas

Cuando se define o edita una directiva de almacenamiento para máquinas virtuales, se puede crear o modificar una regla que haga referencia a las etiquetas que se usaron para almacenes de datos específicos. Los almacenes de datos pasan a ser compatibles con ese tipo de directiva de almacenamiento.

5 Finalizar la creación de directivas de almacenamiento de máquina virtual

Es posible revisar la lista de almacenes de datos que son compatibles con la directiva de almacenamiento de máquina virtual y cambiar cualquier configuración de directivas de almacenamiento.

Pasos siguientes

Esta directiva de almacenamiento se puede aplicar a las máquinas virtuales. Si se utiliza el almacenamiento basado en objetos, como Virtual SAN y Virtual Volumes, se puede designar esta directiva de almacenamiento como la predeterminada.

Iniciar proceso de creación de directivas de almacenamiento de máquina virtual

Para definir una directiva de almacenamiento de máquina virtual, utilice el asistente **Create New VM Storage Policy** (Crear nueva directiva de almacenamiento de máquina virtual).

Procedimiento

- 1 Desde la página de inicio de vSphere Web Client, haga clic en **Policies and Profiles (Directivas y perfiles) > VM Storage Policies (Directivas de almacenamiento de máquina virtual)**.
- 2 Haga clic en el icono **Create a New VM Storage Policy** (Crear una nueva directiva de almacenamiento de máquina virtual).
- 3 Seleccione la instancia de vCenter Server.
- 4 Escriba un nombre y una descripción para la directiva de almacenamiento.

Definir reglas comunes para una directiva de almacenamiento de máquina virtual

Las reglas comunes se basan en los servicios de datos que son genéricos para todo tipo de almacenamiento y no dependen del almacén de datos. Estos servicios de datos pasan a estar disponibles en la interfaz de directivas de almacenamiento de máquina virtual cuando se instalan filtros de E/S de terceros desarrollados mediante vSphere API para los filtros de E/S. Es posible hacer referencia a estos servicios de datos en una directiva de almacenamiento.

Procedimiento

- 1 En la página Common Rules (Reglas comunes), seleccione **Use common rules in the storage policy** (Usar reglas comunes en la directiva de almacenamiento) para habilitar este tipo de reglas.
- 2 En el menú desplegable **Add rule** (Agregar regla), seleccione el servicio de datos que desea incluir en la regla.
- 3 Seleccione un proveedor de servicio de datos.

Si distintos proveedores ofrecen el mismo servicio de datos, por ejemplo, replicación, no es posible agregar más de una regla que haga referencia a ese servicio de datos.
- 4 Especifique los valores de la regla y haga clic en **Next** (Siguiente).

Crear reglas específicas de almacenamiento para una directiva de almacenamiento de máquina virtual

Las reglas específicas de los almacenes de datos se basan en servicios de datos que anuncian entidades de almacenamiento como Virtual SAN y Virtual Volumes. Para la máquina virtual que utiliza esta directiva, el almacén de datos garantiza que pueda satisfacer los requisitos de almacenamiento de la máquina virtual. El almacén de datos también garantiza que puede ofrecer un conjunto de características específicas de capacidad, rendimiento, disponibilidad, redundancia, entre otras.

Un conjunto de reglas específico de un almacén de datos puede incluir reglas de una sola entidad de almacenamiento.

Requisitos previos

Si el entorno incluye entidades de almacenamiento como Virtual SAN o Virtual Volumes, revise estas funcionalidades. Para obtener información, consulte la documentación de *Administración de VMware Virtual SAN* y [Capítulo 19 Trabajar con Virtual Volumes](#).

Procedimiento

- 1 En la página Rule Set (Conjunto de reglas), seleccione un proveedor de almacenamiento, por ejemplo, Virtual SAN o Virtual Volumes, del menú desplegable **Rules based on data services** (Reglas basadas en servicios de datos).

La página se expande para mostrar los servicios de datos que provee el recurso de almacenamiento.

- 2 Seleccione el servicio de datos que desea incluir y especifique su valor.

Compruebe que los valores que proporciona estén dentro del rango de los valores que anuncia el perfil de servicios de datos del recurso de almacenamiento.

Según lo que introduzca, el mecanismo de consumo de almacenamiento calcula la cantidad de espacio necesaria para un disco virtual que residirá en esta entidad de almacenamiento.

- 3 (opcional) Agregue reglas basadas en etiquetas.
- 4 Haga clic en **Next** (Siguiente).

Agregar o editar reglas basadas en etiquetas

Cuando se define o edita una directiva de almacenamiento para máquinas virtuales, se puede crear o modificar una regla que haga referencia a las etiquetas que se usaron para almacenes de datos específicos. Los almacenes de datos pasan a ser compatibles con ese tipo de directiva de almacenamiento.

Puede agregar reglas basadas en etiquetas a un conjunto de reglas que incluye reglas específicas del almacenamiento o crear un conjunto de reglas separado solamente con reglas basadas en etiquetas. Cuando utilice etiquetas en las directivas, siga estas instrucciones:

- Si el conjunto de reglas contiene otras reglas específicas del almacenamiento, el almacén de datos con la etiqueta asignada debe cumplir con todas las reglas del conjunto de reglas.
- Si se agregan varias etiquetas de la misma categoría dentro de la misma regla, las etiquetas se tratan como restricciones alternativas. Se puede cumplir con cualquiera de las etiquetas.
- Si se agregan las etiquetas en reglas distintas dentro del mismo conjunto de reglas, se debe cumplir con todas las etiquetas.

Requisitos previos

Cree etiquetas de almacenamiento y aplíquelas a los almacenes de datos. Consulte [Asignar etiquetas a almacenes de datos](#).

Procedimiento

- 1 En la página Rule Set (Conjunto de reglas), agregue o edite una regla basada en etiquetas:
 - Para agregar una regla, haga clic en el botón **Add tag-based rule** (Agregar regla basada en etiquetas).
 - Para modificar una regla existente, seleccione la regla y haga clic en el icono **Modify rule** (Modificar regla).
- 2 Especifique una categoría.
- 3 Seleccione etiquetas o edite una selección actual.

Resultados

Los almacenes de datos que utilizan las etiquetas que seleccionó son compatibles con la directiva de almacenamiento.

Finalizar la creación de directivas de almacenamiento de máquina virtual

Es posible revisar la lista de almacenes de datos que son compatibles con la directiva de almacenamiento de máquina virtual y cambiar cualquier configuración de directivas de almacenamiento.

Procedimiento

- 1 En la página Storage Compatibility (Compatibilidad de almacenamiento), revise la lista de almacenes de datos que coinciden con esta directiva y haga clic en **Next** (Siguiente).
Para cumplir los requisitos, el almacén de datos debe satisfacer al menos un conjunto de reglas y todas las reglas dentro de este conjunto.
- 2 Revise la configuración de la directiva de almacenamiento y realice cambios; para ello, haga clic en **Back** (Atrás) para volver a la página correspondiente.
- 3 Haga clic en **Finish** (Finalizar).

Resultados

La directiva de almacenamiento de máquina virtual aparece en la lista.

Eliminar una directiva de almacenamiento de una máquina virtual

Puede eliminar una directiva de almacenamiento si no la está utilizando para ninguna máquina virtual o ningún disco virtual.

Procedimiento

- 1 En la página de inicio de vSphere Web Client, haga clic en **Directivas y perfiles > Directivas de almacenamiento de máquina virtual**.
- 2 En la interfaz de directivas de almacenamiento de máquina virtual, seleccione una directiva para eliminarla y haga clic en el icono **Delete a VM Storage Policy** (Eliminar una directiva de almacenamiento de máquina virtual) (✖).

3 Haga clic en **Yes** (Sí).

Resultados

Esta directiva se quita del inventario.

Editar o clonar una directiva de almacenamiento de máquina virtual

Si cambian los requisitos de almacenamiento de las máquinas virtuales y los discos virtuales, se puede modificar la directiva de almacenamiento existente. También se puede crear una copia de una directiva de almacenamiento de máquina virtual existente mediante su clonación. Durante la clonación, se puede seleccionar la personalización de la directiva de almacenamiento original.

Requisitos previos

Privilegios necesarios: **Perfil de almacenamiento.Ver**

Procedimiento

- 1 En la página de inicio de vSphere Web Client, haga clic en **Directivas y perfiles > Directivas de almacenamiento de máquina virtual**.
- 2 Seleccione una directiva de almacenamiento y haga clic en uno de los iconos siguientes:
 - **Edit a VM storage policy (Editar una directiva de almacenamiento de máquina virtual)**
 - **Clone a VM storage policy (Clonar una directiva de almacenamiento de máquina virtual)**
- 3 (opcional) Modifique la directiva y haga clic en **OK** (Aceptar).
- 4 Si edita la directiva de almacenamiento que utiliza una máquina virtual, vuelva a aplicar la directiva a la máquina virtual.

Opción	Descripción
Manually later (Manualmente más adelante)	Si selecciona esta opción, el estado de cumplimiento de todos los discos virtuales y los objetos de inicio de máquina virtual asociados con la directiva de almacenamiento cambia a Out of Date (Desactualizado). Para actualizar la configuración y el cumplimiento, vuelva a aplicar manualmente la directiva de almacenamiento a todas las entidades asociadas. Consulte Volver a aplicar una directiva de almacenamiento de máquinas virtuales .
Now (Ahora)	Actualice el estado de cumplimiento y de la máquina virtual inmediatamente después de editar la directiva de almacenamiento.

Directivas de almacenamiento y máquinas virtuales

Después de definir una directiva de almacenamiento de máquina virtual, puede aplicarla a una máquina virtual. La directiva de almacenamiento se aplica al aprovisionar la máquina virtual o configurar sus discos virtuales. Según el tipo y la configuración, la directiva puede servir para diferentes usos. Puede seleccionar el almacén de datos más adecuado para la máquina virtual y aplicar el nivel requerido de servicio o puede habilitar servicios de datos específicos para la máquina virtual y sus discos.

Si no se especifica la directiva de almacenamiento, el sistema utilizará la directiva de almacenamiento predeterminada asociada con el almacén de datos. Si cambian los requisitos de almacenamiento de las aplicaciones en la máquina virtual, puede modificar la directiva de almacenamiento que se aplicó originalmente a la máquina virtual.

Directivas de almacenamiento predeterminadas

Cuando aprovisiona una máquina virtual en un almacén de datos basado en objetos, como Virtual SAN o Virtual Volumes, debe asignarle a la máquina virtual una directiva de almacenamiento de máquina virtual adecuada que sea compatible con el almacén de datos. Esta asignación garantiza una selección óptima de los objetos de máquina virtual dentro del almacenamiento basado en objetos. Si no asigna explícitamente una directiva de almacenamiento a la máquina virtual, el sistema utiliza la directiva de almacenamiento predeterminada que está asociada con el almacén de datos. La directiva predeterminada también se usa cuando la directiva asignada no incluye reglas específicas para Virtual Volumes o Virtual SAN.

Las directivas de almacenamiento predeterminadas para Virtual SAN y Virtual Volumes pueden ser proporcionadas por VMware y definidas por el usuario. Los almacenes de datos VMFS y NFS no tienen directivas predeterminadas.

Directivas predeterminadas proporcionas por VMware

VMware proporciona directivas de almacenamiento predeterminadas para los almacenes de datos virtuales y de Virtual SAN.

Directiva de almacenamiento predeterminada de Virtual SAN

La directiva de almacenamiento predeterminada que proporciona VMware se aplica a todos los objetos de máquina virtual que se aprovisionan en un almacén de datos de Virtual SAN cuando no se selecciona ninguna otra directiva de Virtual SAN.

La directiva que proporciona VMware tiene las características siguientes:

- No se puede eliminar la directiva.
- La directiva puede editarse. Para editar la directiva, se deben tener privilegios de directiva de almacenamiento que incluyan los de visualización y actualización.
- Cuando se edita la directiva, no se puede cambiar el nombre de la directiva ni la especificación del proveedor de almacenamiento de Virtual SAN. Todos los demás parámetros, incluidas las reglas, pueden editarse.
- Puede clonar la directiva predeterminada y usarla como plantilla para crear una directiva de almacenamiento.
- La directiva predeterminada de Virtual SAN solo es compatible con almacenes de datos de Virtual SAN.
- Puede crear una directiva de almacenamiento de máquina virtual para Virtual SAN y designarla como predeterminada.

Directiva de almacenamiento predeterminada de Virtual Volumes

Para Virtual Volumes, VMware proporciona una directiva de almacenamiento predeterminada que no contiene reglas ni requisitos de almacenamiento. Al igual que con Virtual SAN, esta directiva se aplica a los objetos de máquina virtual cuando no se especifica otra directiva para la máquina virtual que se coloca en el almacén de datos virtual. Con la directiva sin requisitos, las matrices de almacenamiento pueden determinar la selección óptima de los objetos de la máquina virtual.

La directiva de Virtual Volumes predeterminada que proporciona VMware tiene las características siguientes:

- No puede eliminar, editar ni clonar esta directiva.
- La directiva predeterminada de Virtual Volumes es compatible solo con los almacenes de datos virtuales.
- Puede crear una directiva de almacenamiento de máquina virtual para Virtual Volumes y designarla como predeterminada.

Directivas predeterminadas definidas por el usuario para el almacenamiento de máquinas virtuales

Puede crear una directiva de almacenamiento de máquina virtual que sea compatible con Virtual SAN o con Virtual Volumes y designar esta directiva como la predeterminada para Virtual SAN y los almacenes de datos virtuales. La directiva predeterminada definida por el usuario reemplaza a la directiva de almacenamiento predeterminada que proporcionó VMware.

Cada Virtual SAN y almacén de datos virtual puede tener una sola directiva predeterminada a la vez. Sin embargo, puede crear una sola directiva de almacenamiento que coincida con varios almacenes de datos de Virtual Volumes y Virtual SAN como la directiva predeterminada para todos los almacenes de datos.

Cuando la directiva de almacenamiento de máquina virtual se convierta en la directiva predeterminada de un almacén de datos, no podrá eliminarla a menos que la separe del almacén de datos.

Cambiar la directiva de almacenamiento predeterminada de un almacén de datos

Para los almacenes de datos de Virtual SAN y Virtual Volumes, VMware proporciona directivas de almacenamiento que se utilizan como las predeterminadas durante el aprovisionamiento de una máquina virtual. Es posible cambiar la directiva de almacenamiento predeterminada para un almacén de datos de Virtual Volumes o Virtual SAN.

Requisitos previos

Cree una directiva de almacenamiento que sea compatible con Virtual Volumes o Virtual SAN. Puede crear una directiva que coincida con ambos tipos de almacenamiento.

Procedimiento

- 1 En el navegador de vSphere Web Client, seleccione **Listas de inventario global > Almacenes de datos**.

- 2 Haga clic en el almacén de datos.
- 3 Haga clic en la pestaña **Manage** (Administrar) y en **Settings** (Configuración).
- 4 Haga clic en **General** y, a continuación, haga clic en **Edit** (Editar) en el panel Default Storage Policy (Directiva de almacenamiento predeterminada).
- 5 En la lista de directivas de almacenamiento disponibles, seleccione una directiva para designarla como la predeterminada y haga clic en **OK** (Aceptar).

Resultados

La directiva de almacenamiento seleccionada se convierte en la directiva predeterminada del almacén de datos. vSphere asigna esta directiva a cualquier objeto de máquina virtual que se aprovisiona en el almacén de datos cuando no hay ninguna otra directiva seleccionada.

Asignar directivas de almacenamiento a máquinas virtuales

Es posible asignar una directiva de almacenamiento de máquina virtual en una implementación inicial de una máquina virtual o cuando realiza otras operaciones de máquina virtual, como la clonación o la migración.

Este tema describe cómo asignar la directiva de almacenamiento de máquina virtual cuando crea una máquina virtual. Para obtener información sobre otros métodos de implementación, incluidas la clonación, la implementación a partir de una plantilla, etc., consulte la documentación *Administración de máquinas virtuales de vSphere*.

Se puede aplicar la misma directiva de almacenamiento al archivo de configuración de máquina virtual y a todos los discos virtuales. Si los requisitos de almacenamiento para los discos virtuales y el archivo de configuración son diferentes, se pueden asociar distintas directivas de almacenamiento con el archivo de configuración de máquina virtual y los discos virtuales seleccionados.

Procedimiento

- 1 En vSphere Web Client, inicie el proceso de aprovisionamiento de máquina virtual y siga los pasos adecuados.
- 2 Asigne la misma directiva de almacenamiento a todos los discos y archivos de máquina virtual.
 - a En la página Select Storage (Seleccionar almacenamiento), seleccione una directiva de almacenamiento en el menú desplegable **VM Storage Policy** (Directiva de almacenamiento de máquina virtual).

De acuerdo con la configuración, la directiva de almacenamiento separa todos los almacenes de datos en conjuntos compatibles e incompatibles. Si la directiva hace referencia a servicios de datos que ofrece una entidad de almacenamiento específica, por ejemplo, Virtual Volumes, la lista compatible incluye almacenes de datos que representan solo ese tipo de almacenamiento.
 - b Seleccione un almacén de datos adecuado de la lista de almacenes de datos compatibles y haga clic en **Next** (Siguiente).

El almacén de datos se transforma en el recurso de almacenamiento de destino del archivo de configuración de la máquina virtual y de todos los discos virtuales.

3 Cambie la directiva de almacenamiento de máquina virtual del disco virtual.

Utilice esta opción si los requisitos de selección de almacenamiento son distintos para los discos virtuales. También puede usar esta opción si debe habilitar servicios de datos de software, como el almacenamiento en caché y la replicación, para los discos virtuales.

- a En la página **Customize Hardware** (Personalizar hardware), expanda el panel **New hard disk** (Nuevo disco duro).
- b En el menú desplegable **VM storage policy** (Directiva de almacenamiento de máquina virtual), seleccione la directiva de almacenamiento para asignar al disco virtual.
- c (opcional) Cambie la ubicación de almacenamiento del disco virtual.

Use esta opción para almacenar el disco virtual en un almacén de datos distinto del almacén de datos en el que reside el archivo de configuración de máquina virtual.

4 Complete el proceso de aprovisionamiento de máquina virtual.

Resultados

Una vez creada la máquina virtual, la pestaña **Summary** (Resumen) muestra las directivas de almacenamiento asignadas y su estado de cumplimiento.

Pasos siguientes

Si los requisitos de selección de almacenamiento del archivo de configuración o los discos virtuales cambian, se puede modificar la asignación de la directiva virtual posteriormente.

Cambiar la asignación de directivas de almacenamiento para archivos y discos de máquinas virtuales

Si cambian los requisitos de almacenamiento para las aplicaciones en la máquina virtual, puede editar la directiva de almacenamiento que se aplicó originalmente a la máquina virtual.

Puede editar la directiva de almacenamiento de una máquina virtual encendida o apagada.

Cuando cambia la asignación de una directiva de almacenamiento de máquina virtual, puede aplicar la misma directiva de almacenamiento al archivo de configuración de la máquina virtual y a todos sus discos virtuales. Si los requisitos de almacenamiento para los discos virtuales y el archivo de configuración son diferentes, se pueden asociar distintas directivas de almacenamiento con el archivo de configuración de máquina virtual y los discos virtuales seleccionados.

Procedimiento

- 1 En vSphere Web Client, desplácese hasta la máquina virtual.
- 2 Haga clic en la pestaña **Manage** (Administrar) y en **Policies** (Directivas).
- 3 Haga clic en **Storage** (Almacenamiento).

- 4 Haga clic en **Edit VM Storage Policies** (Editar directivas de almacenamiento de máquina virtual).
- 5 Especifique la directiva de almacenamiento de máquina virtual para la máquina virtual.

Opción	Descripción
Aplique la misma directiva de almacenamiento a todos los objetos de la máquina virtual.	<ol style="list-style-type: none"> a Seleccione la directiva en el menú desplegable VM storage policy (Directiva de almacenamiento de máquina virtual). b Haga clic en Apply to all (Aplicar a todo).
Aplique distintas directivas de almacenamiento al objeto de inicio de la máquina virtual y a los discos virtuales.	<ol style="list-style-type: none"> a Seleccione el objeto. b Seleccione la directiva en el menú desplegable VM storage policy (Directiva de almacenamiento de máquina virtual) del objeto.

- 6 Haga clic en **OK** (Aceptar).

Resultados

La directiva de almacenamiento se asigna a la máquina virtual y a sus discos.

Supervisar cumplimiento del almacenamiento en máquinas virtuales

Cuando asocia una directiva con objetos de máquinas virtuales y selecciona en qué máquinas virtuales y discos virtuales se ejecutan los almacenes de datos, puede comprobar si las máquinas virtuales y los discos virtuales utilizan almacenes de datos que cumplen con la directiva.

Si comprueba el cumplimiento de una máquina virtual cuyo host o clúster posee directivas de almacenamiento deshabilitadas, el resultado de la comprobación será Noncompliant (Incumplimiento), ya que la característica está deshabilitada.

Requisitos previos

Para realizar una comprobación de cumplimiento de una directiva de almacenamiento, asocie la directiva al menos con una máquina virtual o un disco virtual.

Procedimiento

- 1 En la página de inicio de vSphere Web Client, haga clic en **Directivas y perfiles > Directivas de almacenamiento de máquina virtual**.
- 2 Haga doble clic en una directiva de almacenamiento.
- 3 Haga clic en la pestaña **Monitor** (Supervisar) y, a continuación, haga clic en **VMs and Virtual Disks** (Máquinas virtuales y discos virtuales).
- 4 Haga clic en **Trigger VM Storage Policy Compliance Check** (Activar comprobación de cumplimiento de la directiva de almacenamiento de máquina virtual).

La columna Compliance Status (Estado de cumplimiento) muestra el estado de cumplimiento del almacenamiento de las máquinas virtuales y sus directivas.

Estado de cumplimiento	Descripción
Compliant (Compatible)	El almacén de datos que utiliza la máquina virtual o el disco virtual posee las capacidades de almacenamiento requeridas por la directiva.
Noncompliant (No compatible)	El almacén de datos cumple con los requisitos de almacenamiento especificados, pero actualmente no puede satisfacer la directiva de almacenamiento de la máquina virtual. Por ejemplo, el estado puede pasar a ser Not Compliant (Incumplimiento) si los recursos físicos que respaldan al almacén de datos no están disponibles o están agotados. Puede lograr que el almacén de datos cumpla con los requisitos si realiza cambios en la configuración física; por ejemplo, si agrega hosts o discos al clúster. Si los recursos adicionales satisfacen la directiva de almacenamiento de la máquina virtual, el estado pasará a ser Compliant (Cumplimiento).
Desactualizado	El estado indica que se editó la directiva, pero los nuevos requisitos no se han comunicado al almacén de datos donde residen los objetos de la máquina virtual. Para comunicar los cambios, vuelva a aplicar la directiva a los objetos desactualizados.
Not Applicable (No aplicable)	Esta directiva de almacenamiento hace referencia a capacidades de los almacenes de datos no compatibles con el almacén de datos donde reside la máquina virtual.

Pasos siguientes

Si no puede lograr que un almacén de datos cumpla con los requisitos, migre los archivos o los discos virtuales a un almacén de datos compatible. Consulte [Encontrar un recurso de almacenamiento compatible para máquinas virtuales no compatibles](#).

Si el estado es Out of Date (Desactualizado), vuelva a aplicar la directiva a los objetos. Consulte [Volver a aplicar una directiva de almacenamiento de máquinas virtuales](#).

Comprobar el cumplimiento de una directiva de almacenamiento de máquina virtual

Se puede comprobar si una máquina virtual utiliza un almacén de datos compatible con los requisitos de almacenamiento especificados en la directiva de almacenamiento de máquina virtual.

Requisitos previos

Compruebe que haya una directiva de almacenamiento asociada con la máquina virtual.

Procedimiento

- 1 En vSphere Web Client, desplácese hasta la máquina virtual.
- 2 En el menú contextual, seleccione **VM Políticas (Directivas de máquina virtual) > Check VM Storage Policy Compliance (Comprobar el cumplimiento de la directiva de almacenamiento de máquina virtual)**.

El sistema verificará el cumplimiento.

- 3 Haga clic en la pestaña **Summary** (Resumen) que corresponde a la máquina virtual.

- 4 Vea el estado de cumplimiento en el panel VM Storage Policies (Directivas de almacenamiento de máquina virtual).

Estado de cumplimiento	Descripción
Compliant (Compatible)	El almacén de datos que utiliza la máquina virtual o el disco virtual posee las capacidades de almacenamiento requeridas por la directiva.
Noncompliant (No compatible)	El almacén de datos cumple con los requisitos de almacenamiento especificados, pero actualmente no puede satisfacer la directiva de almacenamiento de la máquina virtual. Por ejemplo, el estado puede pasar a ser Not Compliant (Incumplimiento) si los recursos físicos que respaldan al almacén de datos no están disponibles o están agotados. Puede lograr que el almacén de datos cumpla con los requisitos si realiza cambios en la configuración física; por ejemplo, si agrega hosts o discos al clúster. Si los recursos adicionales satisfacen la directiva de almacenamiento de la máquina virtual, el estado pasará a ser Compliant (Cumplimiento).
Desactualizado	El estado indica que se editó la directiva, pero los nuevos requisitos no se han comunicado al almacén de datos donde residen los objetos de la máquina virtual. Para comunicar los cambios, vuelva a aplicar la directiva a los objetos desactualizados.
Not Applicable (No aplicable)	Esta directiva de almacenamiento hace referencia a capacidades de los almacenes de datos no compatibles con el almacén de datos donde reside la máquina virtual.

Pasos siguientes

Si no puede lograr que un almacén de datos cumpla con los requisitos, migre los archivos o los discos virtuales a un almacén de datos compatible. Consulte [Encontrar un recurso de almacenamiento compatible para máquinas virtuales no compatibles](#).

Si el estado es Out of Date (Desactualizado), vuelva a aplicar la directiva a los objetos. Consulte [Volver a aplicar una directiva de almacenamiento de máquinas virtuales](#).

Encontrar un recurso de almacenamiento compatible para máquinas virtuales no compatibles

Determine qué almacén de datos es compatible con la directiva de almacenamiento que está asociada con la máquina virtual.

Ocasionalmente, una directiva de almacenamiento asignada a una máquina virtual puede tener el estado de incumplimiento. Este estado indica que la máquina virtual o sus discos utilizan almacenes de datos que son incompatibles con la directiva. En este caso, se pueden migrar los archivos y los discos virtuales de la máquina virtual a almacenes de datos compatibles.

Utilice esta tarea para determinar qué almacenes de datos satisfacen los requisitos de la directiva.

Requisitos previos

Compruebe que el campo **VM Storage Policy Compliance** (Conformidad con la directiva de almacenamiento de máquina virtual) en la pestaña **Summary** (Resumen) de la máquina virtual muestre el estado Not Compliant (No compatible).

Procedimiento

- 1 En vSphere Web Client, desplácese hasta la máquina virtual.

- 2 Haga clic en la pestaña **Summary** (Resumen).

El panel VM Storage Policy Compliance (Conformidad con la directiva de almacenamiento de máquina virtual), en el panel VM Storage Policies (Directivas de almacenamiento de máquina virtual), muestra el estado Not Compliant (No compatible).

- 3 En el panel **VM Storage Policies** (Directivas de almacenamiento de máquina virtual), haga clic en el vínculo de la directiva.
- 4 Haga clic en la pestaña **Monitor** (Supervisar) y, a continuación, haga clic en **VMs and Virtual Disks** (Máquinas virtuales y discos virtuales) para determinar qué archivos de la máquina virtual no son compatibles.
- 5 Haga clic en **Storage Compatibility** (Compatibilidad de almacenamiento).

Aparecerá una lista de almacenes de datos que coinciden con los requisitos de la directiva.

Pasos siguientes

Es posible migrar la máquina virtual o sus discos a uno de los almacenes de datos incluidos en la lista.

Volver a aplicar una directiva de almacenamiento de máquinas virtuales

Después de editar una directiva de almacenamiento que ya está asociada con un objeto de máquina virtual, la directiva se debe volver a aplicar. Al hacerlo, los nuevos requisitos de almacenamiento se comunican al almacén de datos donde reside el objeto de máquina virtual.

Requisitos previos

El estado de cumplimiento de una máquina virtual es Out of Date (Desactualizado). El estado indica que la directiva se editó, pero los nuevos requisitos no se han comunicado al almacén de datos.

Procedimiento

- 1 En vSphere Web Client, desplácese hasta la máquina virtual.
- 2 Haga clic en la pestaña **Manage** (Administrar) y en **Policies** (Directivas).
- 3 Compruebe que el estado de cumplimiento sea Out of Date (Desactualizado).
- 4 Haga clic en el icono **Reapply VM Storage Policy** (Volver a aplicar directiva de almacenamiento de máquina virtual).

- 5 Vea el estado de cumplimiento en el panel VM Storage Policies (Directivas de almacenamiento de máquina virtual).

Estado de cumplimiento	Descripción
Compliant (Compatible)	El almacén de datos que utilizan la máquina virtual o el disco virtual tiene las capacidades de almacenamiento que requiere la directiva.
Noncompliant (No compatible)	<p>El almacén de datos que utilizan la máquina virtual o el disco virtual no tiene las capacidades de almacenamiento que requiere la directiva. Es posible migrar los archivos de la máquina virtual y los discos virtuales a los almacenes de datos compatibles.</p> <p>Si no puede lograr que un almacén de datos cumpla con los requisitos, migre los archivos o los discos virtuales a un almacén de datos compatible. Consulte Encontrar un recurso de almacenamiento compatible para máquinas virtuales no compatibles.</p>
Not Applicable (No aplicable)	Este nivel de servicio de almacenamiento hace referencia a capacidades de almacenes de datos no compatibles con el almacén de datos donde reside la máquina virtual.

Filtrar E/S de máquinas virtuales

21

vSphere API para los filtros de E/S (VAIO) ofrece un marco que permite que terceros creen componentes de software denominados filtros de E/S.

Los filtros pueden instalarse en hosts ESXi y pueden ofrecer servicios de datos adicionales a las máquinas virtuales al procesar solicitudes de E/S que se transfieren entre el sistema operativo invitado de una máquina virtual y los discos virtuales.

Este capítulo incluye los siguientes temas:

- [Acerca de los filtros de E/S](#)
- [Utilizar dispositivos de almacenamiento flash con filtros de E/S de memoria caché](#)
- [Implementar y configurar filtros de E/S en el entorno de vSphere](#)
- [Administrar filtros de E/S](#)
- [Directrices y prácticas recomendadas para los filtros de E/S](#)

Acerca de los filtros de E/S

Los filtros de E/S que están asociados a los discos virtuales obtienen acceso directo a la ruta de acceso de E/S de la máquina virtual, independientemente de la topología de almacenamiento subyacente.

Otros proveedores crean los filtros de E/S, los cuales están distribuidos como paquetes que proporcionan un instalador para implementar componentes de filtros en clústeres de host vCenter Server y ESXi.

Una vez instalados los filtros de E/S e implementados sus componentes en el clúster de ESXi, vCenter Server automáticamente configura y registra un proveedor de almacenamiento de filtros de E/S, también denominado proveedor VASA, para cada host en el clúster. Los proveedores de almacenamiento se comunican con vCenter Server y hacen que los servicios de datos ofrecidos por el filtro de E/S estén visibles en la interfaz de directivas de almacenamiento de máquina virtual. Es posible hacer referencia a estos servicios de datos al crear reglas comunes para una directiva de máquina virtual. Después de asociar discos virtuales con esta directiva, los filtros de E/S se habilitan en los discos virtuales.

Tipos de filtros de E/S

Por lo general, los partners de VMware crean los filtros de E/S a través del programa de desarrolladores de vSphere API para los filtros de E/S (VAIO). El desarrollo de los filtros de E/S para varios propósitos puede estar a cargo de proveedores externos.

En esta versión, los tipos compatibles de filtros incluyen lo siguiente:

- **Almacenamiento en caché.** Implementa una memoria caché para los datos del disco virtual. El filtro puede usar un dispositivo de almacenamiento flash local para almacenar en caché los datos y aumentar las tasas de utilización de hardware e IOPS para el disco virtual. Si utiliza el filtro de almacenamiento en caché, es posible que deba configurar un recurso flash virtual.
- **Replicación.** Replica todas las operaciones de E/S en una ubicación objetivo externa, como otro host o clúster.

Nota Puede instalar muchos filtros de la misma categoría, como el almacenamiento en caché, en el host ESXi. No obstante, puede tener un filtro de la misma categoría por disco virtual.

Componentes de los filtros de E/S

En el proceso de filtrado de E/S están involucrados varios componentes.

Algunos de los componentes de los filtros de E/S son:

Marco de filtros de VAIO

Una combinación del ámbito del usuario y de la infraestructura VMkernel que ESXi proporciona y que permite que los partners de VMware agreguen complementos de filtro a la ruta de acceso de E/S desde y hacia discos virtuales.

Complemento de filtro de E/S

Un componente de software desarrollado por partners de VMware que intercepta y filtra los datos de E/S en tránsito entre los discos virtuales y los sistemas operativos invitados.

Proveedor de CIM

Un componente opcional desarrollado por los partners de VMware que configura y administra los complementos de filtro de E/S.

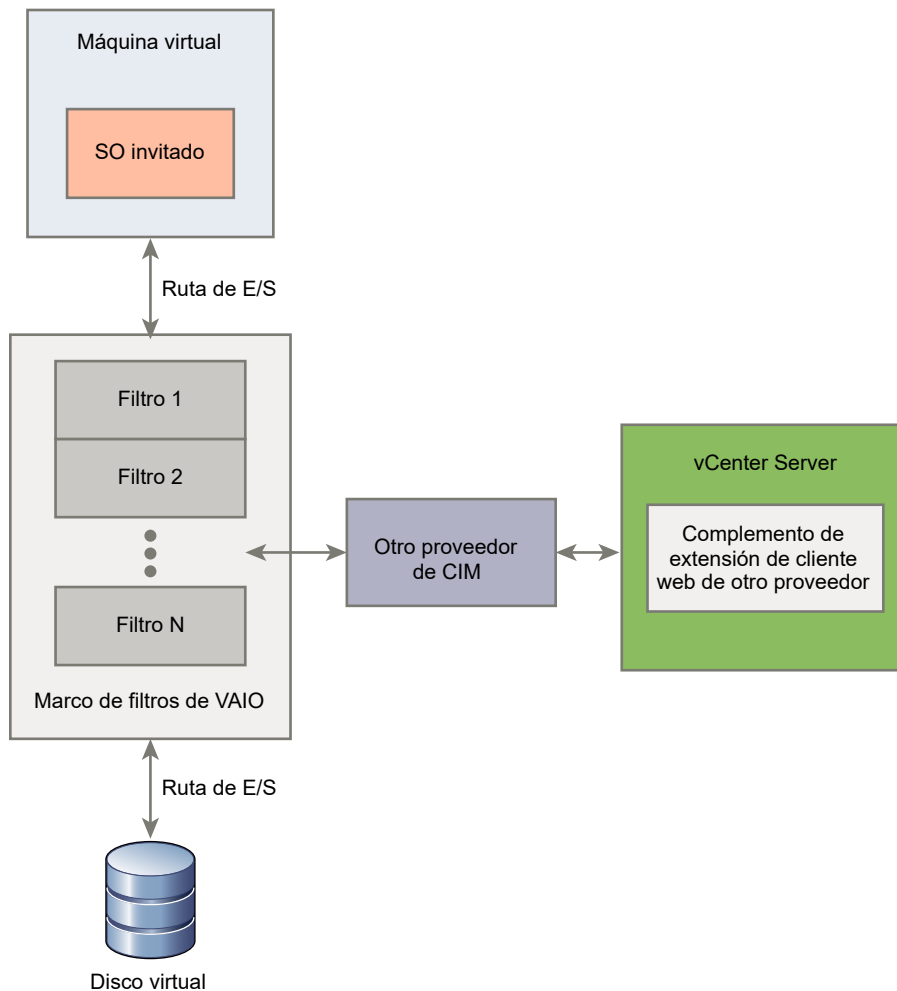
Complemento de vSphere Web Client

Un componente opcional desarrollado por los partners de VMware. Proporciona a los administradores de vSphere métodos de comunicación con un proveedor de CIM de filtro de E/S para recibir información de supervisión sobre el estado del filtro de E/S, así como para enviar comandos de configuración al proveedor de CIM a fin de configurar sus filtros de E/S.

Daemon de filtro de E/S

Un componente opcional desarrollado por los partners de VMware. Puede usarse como servicio adicional que interactúa con las instancias de filtro individual que se ejecutan en un host. El servicio puede establecer canales de comunicación de red entre hosts.

La siguiente imagen muestra los componentes de los filtros de E/S y el flujo de E/S entre los sistemas operativos invitados y el disco virtual.



Cada componente ejecutable de máquina virtual (VMX) contiene un marco de filtro que administra los complementos de filtro de E/S conectados al disco virtual. El marco de filtro invoca los filtros cuando las solicitudes de E/S se transfieren entre el sistema operativo invitado y el disco virtual. Asimismo, el filtro intercepta cualquier acceso de E/S hacia el disco virtual que ocurra fuera de una máquina virtual en ejecución.

Los filtros se ejecutan de forma secuencial en un orden específico. Por ejemplo, un filtro de replicación se ejecuta antes que un filtro de memoria caché. Varios filtros pueden filtrar el disco virtual, pero solo uno por cada categoría.

Una vez que todos los filtros hayan filtrado la solicitud de E/S para un disco en particular, la solicitud de E/S se traslada a su destino, ya sea la máquina virtual o el disco virtual.

Dado que los filtros se ejecutan en un espacio de usuario, cualquier error de filtro solamente afecta a la máquina virtual, pero no afecta al host ESXi.

Proveedores de almacenamiento para filtros VAIO

Después de instalar los filtros de E/S e implementarlos en hosts ESXi, el marco de filtros de E/S configura y registra un proveedor de almacenamiento, también llamado proveedor VASA, para cada host del clúster.

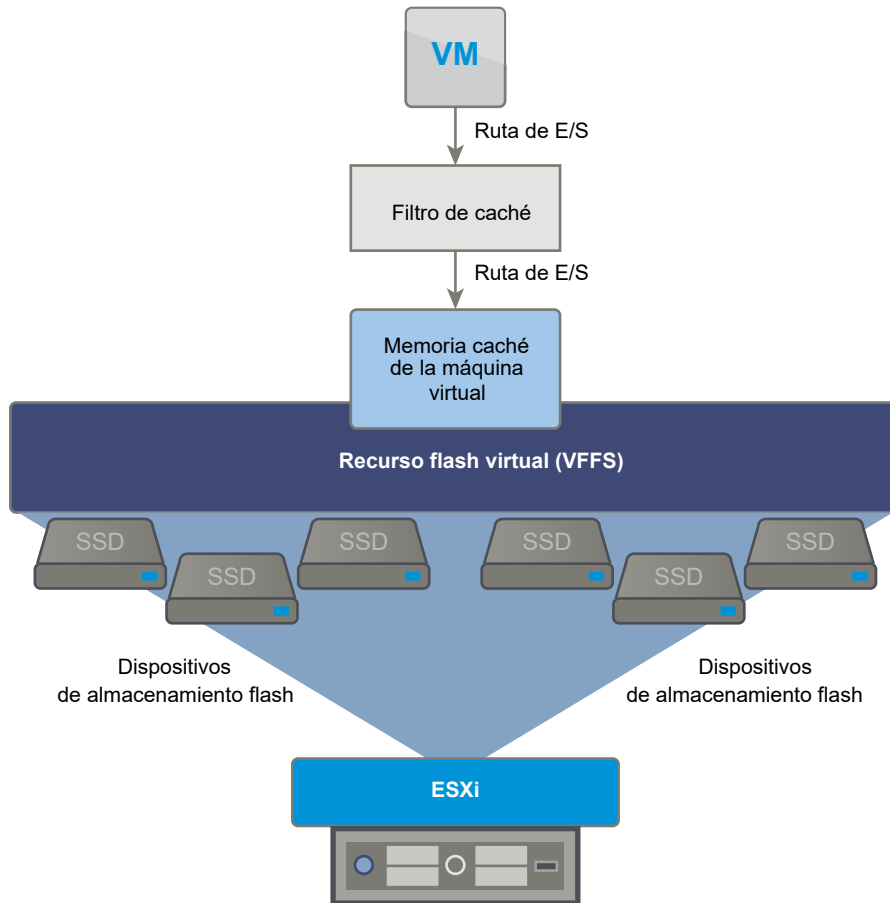
Los proveedores de almacenamiento de filtrado de E/S son componentes de software que ofrece vSphere. Estos se integran con los filtros de E/S e indican las capacidades de servicio de datos que los filtros de E/S admiten en vCenter Server.

Estos servicios de datos se hacen visibles en la interfaz de directivas de almacenamiento de máquina virtual y se puede hacer referencia a ellos en una directiva de máquina virtual. A continuación, puede aplicar esta directiva a los discos virtuales, de modo que los filtros puedan procesar la E/S de los discos.

Utilizar dispositivos de almacenamiento flash con filtros de E/S de memoria caché

Un filtro de E/S de memoria caché puede utilizar dispositivos de almacenamiento flash local para almacenar en caché los datos de la máquina virtual.

Si el filtro de E/S de almacenamiento en caché utiliza dispositivos flash locales, antes de activar el filtro, es necesario configurar un recurso flash virtual, también conocido como volumen VFFS, en el host ESXi. Mientras se procesan las operaciones de E/S de lectura de la máquina virtual, el filtro crea una memoria caché de la máquina virtual y la coloca en el volumen VFFS.



Para configurar un recurso flash virtual, se deben utilizar dispositivos flash conectados al host. Para aumentar la capacidad del recurso flash virtual, puede agregar más unidades flash. Una unidad flash individual debe estar asignada exclusivamente al recurso flash virtual, y no puede compartirse con ningún otro servicio de vSphere, como Virtual SAN o VMFS.

Flash Read Cache y los filtros de E/S de memoria caché son mutuamente excluyentes porque ambas funciones utilizan el recurso flash virtual en el host. No puede habilitar Flash Read Cache en un disco virtual con los filtros de E/S de memoria caché. De forma similar, si una máquina virtual tiene Flash Read Cache configurado, no puede utilizar los filtros de E/S de memoria caché.

Implementar y configurar filtros de E/S en el entorno de vSphere

Es posible instalar filtros de E/S en el entorno de vSphere y después habilitar los servicios de datos que los filtros ofrecen en las máquinas virtuales.

Requisitos previos

Los partners de VMware crean filtros de E/S mediante el programa de desarrolladores de vSphere API para los filtros de E/S (VAIO) y los distribuyen como paquetes de filtro. Los paquetes que se ofrecen como paquetes de instalación de vSphere (VIB) incluyen daemons para filtros de E/S, proveedores CIM y otros componentes asociados. Para obtener información, comuníquese con el proveedor o el representante de VMware.

Procedimiento

1 Instalar filtros de E/S en un clúster

Para instalar filtros de E/S en un clúster de hosts ESXi, ejecute los instaladores que ofrecen los proveedores.

2 Ver proveedores de almacenamiento para filtros de E/S

Después de implementar filtros de E/S, se registra automáticamente el proveedor de almacenamiento, también denominado proveedor VASA, para cada host ESXi en el clúster. Se puede comprobar si los proveedores de almacenamiento de filtros de E/S aparecen según lo esperado y si están activos.

3 Revisar las capacidades de los filtros de E/S

Después de instalar un filtro de E/S en el entorno de vSphere, las capacidades y los servicios de datos que el filtro proporciona se registran y pueden verse en la interfaz de directivas de almacenamiento de máquina virtual. Es posible revisar estos servicios y capacidades, además de los valores predeterminados.

4 Configurar el recurso flash virtual para almacenar en caché los filtros de E/S

Si el filtro de E/S de almacenamiento en caché utiliza dispositivos flash locales, antes de activar el filtro, es necesario configurar un recurso flash virtual, también conocido como volumen VFFS, en el host ESXi.

5 Habilitar servicios de datos de filtros de E/S en discos virtuales

Habilitar los servicios de datos que ofrecen los filtros de E/S es un proceso bidireccional. Puede crear una directiva de máquina virtual en función de las funciones de servicio de datos que ofrecen los filtros de E/S; y, a continuación, asociar esta directiva a una máquina virtual.

Pasos siguientes

Para obtener información sobre la solución de problemas de filtros de E/S, consulte la documentación de *Solución de problemas de vSphere*.

Instalar filtros de E/S en un clúster

Para instalar filtros de E/S en un clúster de hosts ESXi, ejecute los instaladores que ofrecen los proveedores.

Requisitos previos

- Privilegios necesarios: **Host.Configuración.Consultar revisión.**

- Compruebe si la solución de filtros de E/S se integra con vSphere ESX Agent Manager y si está certificada por VMware.
- Compruebe si el clúster incluye hosts ESXi 6.0 Update 1.
- Habilite DRS en el clúster.

Procedimiento

- 1 Ejecute el instalador que proporcionó el proveedor.

Con él, se instalará la extensión de filtros de E/S adecuada en vCenter Server y se implementarán componentes de filtro en todos los hosts de un clúster. No es posible instalar el filtro en los hosts seleccionados.

- 2 Compruebe si los componentes de filtro de E/S se instalaron correctamente en los hosts ESXi:

```
esxcli --server=nombre_del_servidor software vib list
```

El filtro aparecerá en la lista de paquetes de VIB.

Ver proveedores de almacenamiento para filtros de E/S

Después de implementar filtros de E/S, se registra automáticamente el proveedor de almacenamiento, también denominado proveedor VASA, para cada host ESXi en el clúster. Se puede comprobar si los proveedores de almacenamiento de filtros de E/S aparecen según lo esperado y si están activos.

El registro automático correcto del proveedor de almacenamiento de filtros de E/S activa un evento en el nivel del host. Si el proveedor de almacenamiento no logra registrarse automáticamente, el sistema emite una alarma en el host.

Procedimiento

- 1 Desplácese hasta vCenter Server en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar** y, a continuación, en **Proveedores de almacenamiento**.
- 3 Revise los proveedores de almacenamiento para comprobar los filtros de E/S.

Revisar las capacidades de los filtros de E/S

Después de instalar un filtro de E/S en el entorno de vSphere, las capacidades y los servicios de datos que el filtro proporciona se registran y pueden verse en la interfaz de directivas de almacenamiento de máquina virtual. Es posible revisar estos servicios y capacidades, además de los valores predeterminados.

Procedimiento

- 1 En la página de inicio de vSphere Web Client, haga clic en **Directivas y perfiles > Directivas de almacenamiento de máquina virtual**.
- 2 Haga clic en el icono **Create a new VM storage policy** (Crear una nueva directiva de almacenamiento de máquina virtual).

- 3 Seleccione la instancia de vCenter Server.
- 4 Escriba un nombre, por ejemplo, Filtro de E/S de memoria caché, y una descripción para la directiva y, a continuación, haga clic en **Next** (Siguiente).
- 5 En la página Common Rules (Reglas comunes), seleccione **Use common rules in the storage policy** (Usar reglas comunes en la directiva de almacenamiento).
- 6 En el menú desplegable **Add rule** (Agregar regla), seleccione una categoría de filtro de E/S, por ejemplo, memoria caché.
- 7 En el menú desplegable **Select Value** (Seleccionar valor), seleccione el filtro cuyas capacidades desea revisar.

El panel se expandirá para mostrar los servicios de datos que el filtro de E/S ofrece y los valores predeterminados correspondientes.

Configurar el recurso flash virtual para almacenar en caché los filtros de E/S

Si el filtro de E/S de almacenamiento en caché utiliza dispositivos flash locales, antes de activar el filtro, es necesario configurar un recurso flash virtual, también conocido como volumen VFFS, en el host ESXi.

Requisitos previos

Consulte con el proveedor de filtros de E/S para determinar si el recurso flash virtual debe estar habilitado.

Procedimiento

- 1 En vSphere Web Client, desplácese hasta el host.
- 2 Haga clic en la pestaña **Manage** (Administrar) y en **Settings** (Configuración).
- 3 En Virtual Flash (Flash virtual), seleccione **Virtual Flash Resource Management** (Administración de recursos flash virtuales) y haga clic en **Add Capacity** (Agregar capacidad).
- 4 En la lista de unidades flash disponibles, seleccione una o más unidades que desea usar para el recurso flash virtual y haga clic en **OK** (Aceptar).

Resultados

Se crea el recurso flash virtual. El área Device Backing (Copia de seguridad de los dispositivos) enumera todas las unidades que se utilizan para el recurso flash virtual.

Habilitar servicios de datos de filtros de E/S en discos virtuales

Habilitar los servicios de datos que ofrecen los filtros de E/S es un proceso bidireccional. Puede crear una directiva de máquina virtual en función de las funciones de servicio de datos que ofrecen los filtros de E/S; y, a continuación, asociar esta directiva a una máquina virtual.

Requisitos previos

Para los filtros de E/S de almacenamiento en caché, configure el recurso flash virtual en el host ESXi.

Procedimiento

1 Definir una directiva de máquina virtual en función de las capacidades de los filtros de E/S

Para habilitar los filtros de E/S para las máquinas virtuales, primero es necesario crear una directiva de máquina virtual que enumere las capacidades de servicio de datos que los filtros de E/S proporcionan.

2 Asignar la directiva de filtros de E/S a máquinas virtuales

Para activar los servicios de datos que proporcionan los filtros de E/S, asocie la directiva de filtros de E/S con los discos virtuales. Puede asignar la directiva cuando crea o edita una máquina virtual.

Definir una directiva de máquina virtual en función de las capacidades de los filtros de E/S

Para habilitar los filtros de E/S para las máquinas virtuales, primero es necesario crear una directiva de máquina virtual que enumere las capacidades de servicio de datos que los filtros de E/S proporcionan.

Las capacidades de filtro de E/S aparecen en la página Common Rules (Reglas comunes) del asistente VM Storage Policies (Directivas de almacenamiento de máquina virtual).

Requisitos previos

- Compruebe que el proveedor de almacenamiento de filtros de E/S esté disponible y activo. Consulte [Ver proveedores de almacenamiento para filtros de E/S](#).

Procedimiento

- 1 En la página de inicio de vSphere Web Client, haga clic en **Directivas y perfiles > Directivas de almacenamiento de máquina virtual**.

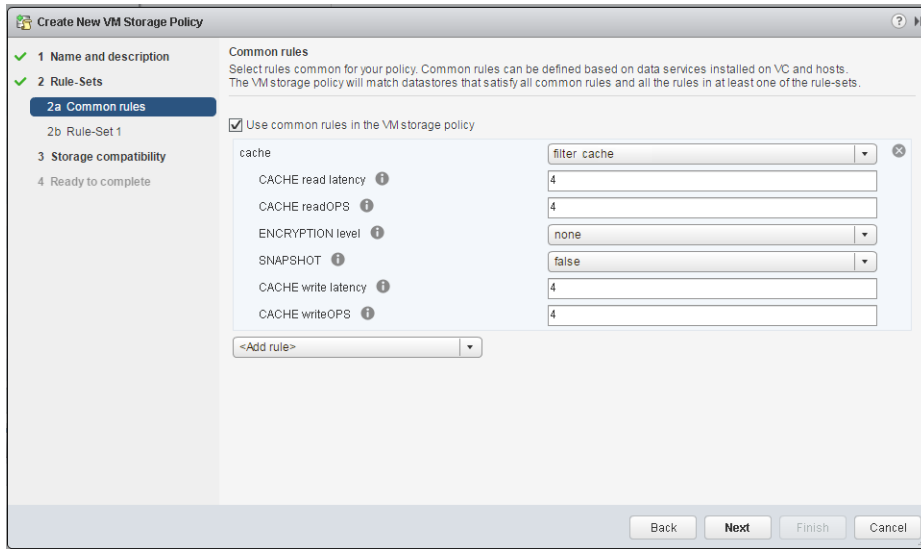
- 2 Haga clic en el icono **Create a new VM storage policy** (Crear una nueva directiva de almacenamiento de máquina virtual).

- 3 Seleccione la instancia de vCenter Server.

- 4 Escriba un nombre, por ejemplo, Filtros de E/S, y una descripción para la directiva de máquina virtual y, a continuación, haga clic en **Next** (Siguiente).

- 5 En la página Common Rules (Reglas comunes), especifique los servicios de filtro de E/S que desea activar para la máquina virtual.

Puede combinar los filtros de E/S de diferentes categorías, como replicación y almacenamiento en caché, en una directiva de almacenamiento. O bien cree directivas diferentes para cada categoría. También puede usar solo un filtro de la misma categoría, por ejemplo, almacenamiento en caché, por directiva de almacenamiento.



- a Seleccione **Use common rules in the storage policy** (Usar reglas comunes en la directiva de almacenamiento).
- b En el menú desplegable **Add rule** (Agregar regla), seleccione una categoría de filtro de E/S.

Opción	Descripción
Replication (Replicación)	Replica todas las operaciones de E/S de escritura entre un sistema operativo invitado de máquina virtual y discos virtuales a una ubicación objetivo externa, como otro host o clúster.
Caching (Almacenamiento en caché)	Configura una memoria caché para los datos de disco virtual. Usa un dispositivo de almacenamiento flash local para almacenar en caché los datos y aumentar las IOPS y las tasas de utilización de hardware del disco virtual.

- c En el menú desplegable **Select Value** (Seleccionar valor), seleccione el filtro.
La página se expande para mostrar las capacidades de servicio de datos y los valores predeterminados que el filtro admite.
 - d Especifique los valores de la regla y haga clic en **Next** (Siguiente).
- 6 En la página Rule Set (Conjunto de reglas), especifique los requisitos de selección de almacenamiento y haga clic en **Next** (Siguiente).

Nota Si planifica migrar la máquina virtual con filtros de E/S en diferentes tipos de almacenes de datos, por ejemplo, entre VMFS y Virtual Volumes, asegúrese de que la directiva de almacenamiento de máquina virtual incluya conjuntos de reglas para cada tipo de almacén de datos que desea usar. Por ejemplo, si migra la máquina virtual entre almacenes de datos de VMFS y Virtual Volumes, cree una directiva de almacenamiento de máquina virtual mixta que incluya una regla basada en etiquetas para el almacén de datos de VMFS y reglas para el almacén de datos de Virtual Volumes.

- 7 En la página Storage Compatibility (Compatibilidad de almacenamiento), revise la lista de almacenes de datos disponibles y haga clic en **Next** (Siguiente).

Para que sean compatibles con la directiva de filtros de E/S, los almacenes de datos deben conectarse al host con filtros de E/S y satisfacer los requisitos de almacenamiento de la directiva.

- 8 Complete la creación de la directiva de almacenamiento y haga clic en **Finish** (Finalizar).

Resultados

La nueva directiva se agrega a la lista.

Asignar la directiva de filtros de E/S a máquinas virtuales

Para activar los servicios de datos que proporcionan los filtros de E/S, asocie la directiva de filtros de E/S con los discos virtuales. Puede asignar la directiva cuando crea o edita una máquina virtual.

Puede asignar la directiva de filtros de E/S durante la implementación inicial de una máquina virtual. Este tema describe cómo asignar la directiva cuando se crea una máquina virtual nueva. Para obtener información sobre los métodos de implementación, consulte la documentación de *Administración de máquinas virtuales de vSphere*.

Nota No puede cambiar ni asignar la directiva de filtro de E/S cuando migra o clona una máquina virtual.

Requisitos previos

Compruebe que los filtros de E/S estén instalados en el host ESXi donde se va a ejecutar la máquina virtual.

Procedimiento

- 1 En vSphere Web Client, inicie el proceso de aprovisionamiento de máquina virtual y siga los pasos adecuados.
- 2 En la página Select Storage (Seleccionar almacenamiento), seleccione la directiva de filtros de E/S desde el menú desplegable **VM Storage Policy** (Directiva de almacenamiento de máquina virtual).
- 3 Seleccione el almacén de datos en la lista de almacenes de datos disponibles y haga clic en **Next** (Siguiente).

El almacén de datos se transforma en el recurso de almacenamiento de destino del archivo de configuración de la máquina virtual y de todos los discos virtuales. La directiva también activa los servicios de filtros de E/S para los discos virtuales.
- 4 Complete el proceso de aprovisionamiento de máquina virtual.

Resultados

Una vez creada la máquina virtual, la pestaña **Summary** (Resumen) muestra las directivas de almacenamiento asignadas y su estado de cumplimiento.

Pasos siguientes

Posteriormente, puede cambiar la asignación de directiva virtual. Consulte [Cambiar la asignación de directivas de almacenamiento para archivos y discos de máquinas virtuales](#).

Administrar filtros de E/S

Es posible ejecutar el instalador que el proveedor ofrece para instalar, desinstalar o actualizar los filtros de E/S.

Al trabajar con filtros de E/S, se deben tener en cuenta las siguientes consideraciones:

- vCenter Server utiliza ESX Agent Manager (EAM) para instalar y desinstalar filtros de E/S. Como administrador, nunca se debe invocar las API de EAM directamente para agencias de EAM que vCenter Server crea o utiliza. Todas las operaciones relacionadas con los filtros de E/S deben pasar por las API de VIM. Si se modifica de forma accidental una agencia de EAM que vCenter Server creó, se deben revertir los cambios. Si se destruye por accidente la agencia de EAM que utilizan los filtros de E/S, se debe llamar a `Vim.IoFilterManager#uninstallIoFilter` para que se desinstalen los filtros de E/S afectados. Cuando finalice la desinstalación, vuelva a reinstalar.
- Cuando un host nuevo se une al clúster que tiene filtros de E/S, los filtros instalados en el clúster se implementan en el host. vCenter Server registra el proveedor de almacenamiento de filtros de E/S del host. Todos los cambios que se realicen en el clúster se verán en la interfaz de directivas de almacenamiento de máquina virtual de vSphere Web Client.
- Al sacar un host de un clúster o al quitarlo de vCenter Server, se desinstalan los filtros de E/S del host. vCenter Server cancela el registro del proveedor de almacenamiento de filtros de E/S del host una vez que se desinstalan los filtros.
- Al utilizar un host ESXi sin estado, es posible que el host pierda su VIB de filtros de E/S durante el reinicio. vCenter Server comprueba los paquetes instalados en el host después del reinicio y envía los VIB de filtros de E/S al host, de ser necesario.

Desinstalar filtros de E/S de un clúster

Puede desinstalar filtros de E/S implementados en un clúster de hosts ESXi.

Requisitos previos

- Privilegios necesarios: **Host.Config.Revisión**.

Procedimiento

- 1 Para desinstalar el filtro de E/S, ejecute el instalador que le proporcione su proveedor.

Durante la desinstalación, vSphere ESX Agent Manager coloca los hosts de forma automática en el modo de mantenimiento.

Si la desinstalación se realiza correctamente, el filtro y los componentes relacionados se quitan de los hosts.

- 2 Compruebe que los componentes del filtro de E/S se desinstalaron correctamente de los hosts ESXi:

```
esxcli --server=server_name software vib list
```

El filtro desinstalado ya no aparece en la lista.

Actualizar filtros de E/S en un clúster

Utilice los instaladores que proporcionan los proveedores de filtros de E/S para actualizar ese tipo de filtros implementados en un clúster de hosts ESXi.

La actualización consiste en desinstalar los componentes de filtro anteriores y reemplazarlos por los nuevos componentes de filtro. Para determinar si una instalación es una actualización, vCenter Server comprueba los nombres y las versiones de los filtros existentes. Si los nombres de los filtros existentes coinciden con los nombres de los filtros nuevos, pero tienen versiones diferentes, se considera que la instalación es una actualización.

Requisitos previos

- Privilegios necesarios: **Host.Config.Revisión**.

Procedimiento

- 1 Ejecute el instalador del proveedor para actualizar el filtro.

Durante la actualización, vSphere ESX Agent Manager coloca automáticamente los hosts en modo de mantenimiento.

El instalador identifica todos los componentes de filtro existentes y los quita antes de instalar los nuevos componentes de filtro.

- 2 Compruebe que los componentes del filtro de E/S se desinstalaron correctamente de los hosts ESXi:

```
esxcli --server=server_name software vib list
```

Resultados

Después de la actualización, vSphere ESX Agent Manager vuelve a colocar los hosts en modo operativo.

Directrices y prácticas recomendadas para los filtros de E/S

Al utilizar filtros de E/S en el entorno, siga las instrucciones y las prácticas recomendadas específicas.

- Los filtros de E/S no admiten RDM en el modo de compatibilidad física.

- Flash Read Cache y los filtros de E/S de memoria caché son mutuamente excluyentes porque ambas funciones utilizan el recurso flash virtual en el host. No puede habilitar Flash Read Cache en un disco virtual con los filtros de E/S de memoria caché. De forma similar, si una máquina virtual tiene Flash Read Cache configurado, no puede utilizar los filtros de E/S de memoria caché.
- No puede cambiar ni asignar la directiva de filtro de E/S cuando migra o clona una máquina virtual.
- La clonación o la migración de una máquina virtual con la directiva de filtro de E/S de un host a otro requieren que el host de destino tenga un filtro compatible instalado. Este requisito se aplica a las migraciones que inician un administrador o funciones como HA o DRS.
- Al convertir una plantilla en una máquina virtual, si la plantilla está configurada con una directiva de filtro de E/S, el host de destino debe tener el filtro de E/S compatible instalado.
- Si utiliza vCenter Site Recovery Manager para replicar discos virtuales, los discos que se obtienen en el sitio de recuperación no tienen directivas de filtro E/S. Debe crear directivas de filtro E/S en el sitio de recuperación y volver a asociarlas a los discos replicados.
- Si la máquina virtual tiene un árbol de instantáneas asociado, no se puede agregar, cambiar ni quitar la directiva de filtro de E/S para la máquina virtual.

Para obtener información sobre la solución de problemas de filtros de E/S, consulte la documentación de *Solución de problemas de vSphere*.

Migrar máquinas virtuales con filtros de E/S

Al migrar una máquina virtual con filtros de E/S, existen consideraciones específicas que se deben tener en cuenta.

Si se utiliza Storage vMotion para migrar una máquina virtual con filtros de E/S, debe conectarse un almacén de datos de destino a los hosts con filtros de E/S compatibles instalados.

Es posible que deba migrar una máquina virtual con filtros de E/S en distintos tipos de almacenes de datos, por ejemplo, entre VMFS y Virtual Volumes, VMFS y Virtual SAN, entre otros. Si lo hace, asegúrese de que además de las reglas comunes que describen la directiva de filtros de E/S, la directiva de almacenamiento de máquina virtual incluya conjuntos de reglas para cada tipo de almacén de datos que planea utilizar. Por ejemplo, si se migra la máquina virtual entre almacenes de datos de VMFS y Virtual Volumes, cree una directiva de almacenamiento de máquina virtual mixta que incluya lo siguiente:

- Reglas comunes para los filtros de E/S.
- Conjunto de reglas 1 para el almacén de datos de VMFS. Debido a que la administración de almacenamiento basada en directivas no ofrece una directiva de VMFS explícita, el conjunto de reglas debe incluir las reglas basadas en etiquetas para el almacén de datos de VMFS.
- Conjunto de reglas 2 para el almacén de datos de Virtual Volumes.

Cuando Storage vMotion migra la máquina virtual, se selecciona el conjunto de reglas correcto que corresponde al almacén de datos de destino. Las reglas de filtros de E/S se mantienen iguales.

Si no se especifican reglas para los almacenes de datos y únicamente se definen reglas comunes para los filtros de E/S, se seleccionarán directivas de almacenamiento predeterminadas para los almacenes de datos de Virtual SAN, Virtual Volumes y VMFS/NFS.

El VMkernel es un sistema operativo de alto rendimiento que se ejecuta directamente en el host ESXi. El VMkernel administra la mayoría de los recursos físicos del hardware, incluidos la memoria, los procesadores físicos, el almacenamiento y las controladoras de redes.

Para administrar el almacenamiento, el VMkernel tiene un subsistema de almacenamiento que admite varios adaptadores de bus de host (HBA), incluidos SCSI paralelos, SAS, de canal de fibra, FCoE e iSCSI. Estos HBA conectan una amplia variedad de matrices de almacenamiento ALUA, de tipo activo-pasivo y activo-activo, que están certificadas para el uso con el VMkernel. Consulte *Guía de compatibilidad de vSphere* para ver una lista de los HBA y las matrices de almacenamiento compatibles.

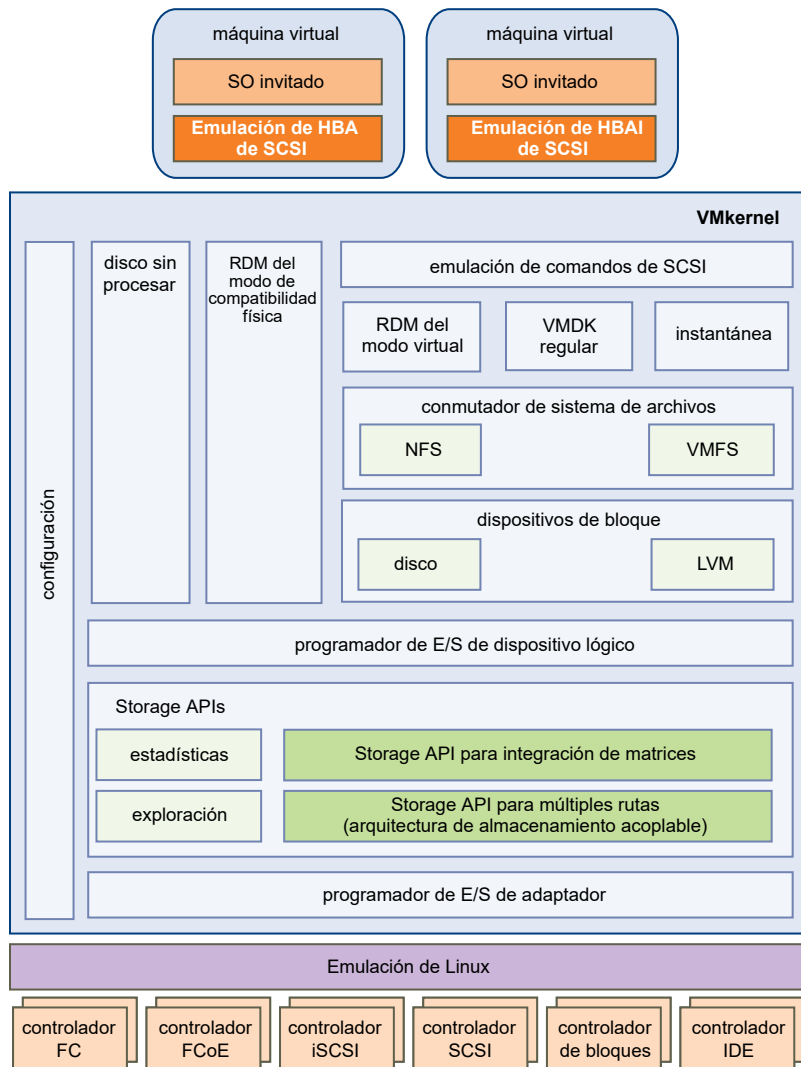
El sistema de archivos principal que usa el VMkernel es VMware Virtual Machine File System (VMFS). VMFS es un sistema de archivos de clúster diseñado y optimizado para admitir archivos grandes, como discos virtuales y archivos de intercambio. El VMkernel también admite el almacenamiento de discos virtuales en sistemas de archivos NFS.

La ruta de acceso de E/S de almacenamiento brinda a las máquinas virtuales acceso a los dispositivos de almacenamiento mediante la emulación de dispositivos. La emulación de dispositivos permite a una máquina virtual acceder a archivos en un sistema de archivos NFS o VMFS como si fueran dispositivos SCSI. El VMkernel ofrece funciones de virtualización de almacenamiento, como la programación de solicitudes de E/S desde varias máquinas virtuales y la funcionalidad de múltiples rutas.

Además, el VMkernel ofrece varias API de almacenamiento que permiten a los partners de almacenamiento integrar y optimizar sus productos para vSphere.

El gráfico siguiente ilustra los conceptos básicos del núcleo del VMkernel, con especial atención en la pila de almacenamiento. Los módulos relacionados con el almacenamiento residen entre las capas del programador de E/S del dispositivo lógico y del programador de E/S del adaptador.

Figura 22-1. VMkernel y almacenamiento



Este capítulo incluye los siguientes temas:

- [Storage APIs](#)

Storage APIs

Storage APIs es una familia de API utilizada por proveedores de hardware, software y almacenamiento externos con el fin de desarrollar componentes que mejoren distintas características y soluciones de vSphere.

En esta publicación, se describen los siguientes conjuntos de Storage APIs y se explica cómo contribuyen al entorno de almacenamiento. Para obtener información sobre otras API de esta familia, incluidas Storage API - Data Protection y Storage API - Site Recovery Manager, visite el sitio web de VMware.

- Storage APIs - Multipathing, también denominada Pluggable Storage Architecture (PSA). PSA es una recopilación de API del VMkernel que les permite a los partners de almacenamiento habilitar y certificar sus matrices de manera asíncrona con los cronogramas de las versiones de ESXi, y también ofrecer comportamientos que mejoran el rendimiento y permiten acceder a funciones de múltiples rutas y equilibrio de carga optimizadas para cada matriz. Para obtener más información, consulte [Administrar varias rutas de acceso](#).
- Storage APIs - Array Integration, anteriormente conocida como VAAI, incluye las siguientes API:
 - API de aceleración de hardware. Permite que las matrices se integren con vSphere para descargar de manera transparente ciertas operaciones de almacenamiento en la matriz. Esta integración reduce significativamente la sobrecarga de CPU en el host. Consulte [Capítulo 23 Aceleración de hardware de almacenamiento](#).
 - API de aprovisionamiento fino de matrices. Ayudan a supervisar la utilización del espacio en matrices de almacenamiento de aprovisionamiento fino para evitar condiciones de falta de espacio y realizar tareas de recuperación de espacio. Consulte [Aprovisionamiento fino de matrices y almacenes de datos de VMFS](#).
- Storage APIs - Storage Awareness. Estas API basadas en vCenter Server permiten que las matrices de almacenamiento informen a vCenter Server acerca de sus opciones de configuración, capacidades, estados de almacenamiento y eventos. Consulte [Capítulo 25 Usar proveedores de almacenamiento](#).

Aceleración de hardware de almacenamiento

23

La funcionalidad de aceleración de hardware permite que el host ESXi se integre con las matrices de almacenamiento compatibles, y asigne operaciones de administración de máquinas virtuales y almacenamiento al hardware de almacenamiento. Con la asistencia de hardware de almacenamiento, el host realiza estas operaciones más rápidamente y consume menos CPU, memoria y ancho de banda de tejido de almacenamiento.

La aceleración de hardware es compatible con los dispositivos de almacenamiento en bloque, el canal de fibra e iSCSI, y dispositivos NAS.

Para obtener detalles adicionales, consulte el artículo de la base de conocimientos de VMware en <http://kb.vmware.com/kb/1021976>.

Este capítulo incluye los siguientes temas:

- [Beneficios de la aceleración de hardware](#)
- [Requisitos de aceleración de hardware](#)
- [Estado de compatibilidad con la aceleración de hardware](#)
- [Aceleración de hardware para dispositivos de almacenamiento en bloque](#)
- [Aceleración de hardware en dispositivos NAS](#)
- [Consideraciones sobre la aceleración de hardware](#)

Beneficios de la aceleración de hardware

Cuando se admite la funcionalidad de aceleración de hardware, el host puede obtener asistencia de hardware y realizar varias tareas de forma más rápida y eficaz.

El host puede obtener asistencia en las actividades siguientes:

- Migrar máquinas virtuales con Storage vMotion
- Implementar máquinas virtuales desde plantillas
- Clonar máquinas virtuales o plantillas
- Bloquear clústeres de VMFS y operaciones de metadatos para archivos de máquina virtual
- Aprovisionar discos virtuales gruesos
- Crear máquinas virtuales con tolerancia a errores

- Crear y clonar discos gruesos en almacenes de datos de NFS

Requisitos de aceleración de hardware

La funcionalidad de aceleración de hardware solo funciona si se utiliza una combinación adecuada de host y matriz de almacenamiento.

Tabla 23-1. Requisitos de almacenamiento de aceleración de hardware

ESXi	Dispositivos de almacenamiento en bloque	Dispositivos NAS
ESXi versión 6.0	Compatibilidad con el estándar T10 SCSI o complementos de almacenamiento en bloque para integración de matrices (VAAI)	Compatibilidad con complementos NAS para integración de matrices Nota NFS 4.1 no admite la aceleración de hardware.

Nota Si el tejido de almacenamiento SAN o NAS utiliza un dispositivo intermedio frente a un sistema de almacenamiento compatible con la aceleración de hardware, este dispositivo también debe ser compatible con la aceleración de hardware y contar con las certificaciones apropiadas. El dispositivo intermedio puede ser un dispositivo de virtualización de almacenamiento, de aceleración de E/S, de cifrado, etc.

Estado de compatibilidad con la aceleración de hardware

vSphere Web Client muestra el estado de compatibilidad con aceleración de hardware de cada dispositivo de almacenamiento y almacén de datos.

Los valores de estado son Unknown (Desconocido), Supported (Compatible) y Not Supported (No compatible). El valor inicial es Unknown.

En el caso de los dispositivos en bloque, el estado cambia a Supported después de que el host finaliza correctamente la operación de descarga. Si la operación de descarga genera errores, el estado cambia a Not Supported. El estado permanece como Unknown si el dispositivo ofrece una compatibilidad parcial con la aceleración de hardware.

Con NAS, el estado cambia a Supported cuando el almacenamiento puede realizar al menos una operación de descarga de hardware.

Cuando los dispositivos de almacenamiento no son compatibles u ofrecen compatibilidad parcial con las operaciones del host, el host vuelve a los métodos nativos para realizar las operaciones no admitidas.

Aceleración de hardware para dispositivos de almacenamiento en bloque

Con la aceleración de hardware, el host puede integrarse con dispositivos de almacenamiento en bloque, canal de fibra o iSCSI, y utilizar ciertas operaciones de matriz de almacenamiento.

La aceleración de hardware de ESXi admite las siguientes operaciones de matriz:

- Copia completa, también conocida como bloques de clonación o descarga de copias. Permite a las matrices de almacenamiento realizar copias completas de datos dentro de la matriz sin hacer que el host lea y escriba la información. Esta operación disminuye el tiempo y la carga de red cuando se clonan máquinas virtuales, se ejecuta el aprovisionamiento desde una plantilla o se realizan migraciones con vMotion.
- Puesta a cero de bloques, que también se conoce como escribir lo mismo. Permite que las matrices de almacenamiento pongan a cero una gran cantidad de bloques para proporcionar almacenamiento asignado recientemente, libre de datos escritos anteriormente. Esta operación disminuye el tiempo y la carga de red cuando crea máquinas virtuales y da formato a discos virtuales.
- Bloqueo asistido por hardware, también denominado prueba y configuración atómica (ATS). Admite el bloqueo discreto de máquinas virtuales sin utilizar reservas de SCSI. Esta operación permite el bloqueo de discos por sector, en lugar del LUN completo como con reservas de SCSI.

Compruebe con el proveedor la compatibilidad con la aceleración de hardware. Ciertas matrices de almacenamiento requieren que se active la compatibilidad del lado del almacenamiento.

En el host, la aceleración de hardware está habilitada de forma predeterminada. Si el almacenamiento no admite la aceleración de hardware, es posible deshabilitarla.

Además de la compatibilidad con la aceleración de hardware, ESXi admite el aprovisionamiento fino de matrices. Para obtener información, consulte [Aprovisionamiento fino de matrices y almacenes de datos de VMFS](#).

Deshabilitar la aceleración de hardware para dispositivos de almacenamiento en bloque

En el host, la aceleración de hardware para dispositivos de almacenamiento en bloque está habilitada de forma predeterminada. Se puede utilizar la configuración avanzada de vSphere Web Client para deshabilitar las operaciones de aceleración de hardware.

Como con cualquier opción de configuración avanzada, antes de deshabilitar la aceleración de hardware, consulte al equipo de soporte de VMware.

Procedimiento

- 1 Diríjase al host en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar**.
- 3 En **Sistema**, haga clic en **Configuración avanzada del sistema**.
- 4 Cambie el valor de cualquiera de las opciones a 0 (deshabilitado):
 - VMFS3.HardwareAcceleratedLocking
 - DataMover.HardwareAcceleratedMove

- DataMover.HardwareAcceleratedInit

Administrar aceleración de hardware en dispositivos de almacenamiento en bloque

Para lograr una integración con las matrices de almacenamiento en bloque y aprovechar las operaciones de hardware de la matriz, vSphere utiliza las extensiones de ESXi denominadas Storage APIs - Array Integration, anteriormente conocidas como VAAI.

En vSphere 5.x y versiones posteriores, estas extensiones se implementan como comandos basados en T10 SCSI. En consecuencia, en dispositivos compatibles con el estándar T10 SCSI, el host ESXi puede comunicarse directamente y no requiere los complementos de VAAI.

Si el dispositivo no es compatible con T10 SCSI u ofrece compatibilidad parcial, ESXi vuelve a utilizar los complementos de VAAI instalados en el host, o bien utiliza una combinación de comandos T10 SCSI y complementos. Los complementos de VAAI son específicos de cada proveedor y pueden ser desarrollados por VMware o por un partner. Para administrar el dispositivo compatible con VAAI, el host asocia al dispositivo el filtro VAAI y el complemento VAAI específico del proveedor.

Para saber si el almacenamiento requiere complementos de VAAI o es compatible con la aceleración de hardware a través de los comandos T10 SCSI, consulte la *Guía de compatibilidad de VMware* o comuníquese con el proveedor de almacenamiento.

Es posible utilizar varios comandos `esxcli` para consultar dispositivos de almacenamiento y acceder a la información de compatibilidad de aceleración de hardware. Para los dispositivos que requieren los complementos de VAAI, también están disponibles los comandos de reglas de notificación. Para obtener información sobre los comandos `esxcli`, consulte *Introducción a vSphere Command-Line Interface*.

Mostrar los complementos y el filtro de aceleración de hardware

Para comunicarse con los dispositivos que no admiten SCSI T10 estándar, el host utiliza una combinación de un solo filtro VAAI y un complemento VAAI específico del proveedor. Utilice el comando `esxcli` para ver el filtro de aceleración de hardware y los complementos cargados actualmente en el sistema.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Ejecute el comando **esxcli --server=*server_name* storage core plugin list --plugin-class=*value***.

En *value*, escriba una de las opciones siguientes:

- Escriba **VAAI** para mostrar los complementos.

El resultado de este comando es similar al ejemplo siguiente:

```
#esxcli --server=server_name storage core plugin list --plugin-class=VAAI
Plugin name      Plugin class
VMW_VAAIP_EQL    VAAI
VMW_VAAIP_NETAPP VAAI
VMW_VAAIP_CX     VAAI
```

- Escriba **Filter** para mostrar el filtro.

El resultado de este comando es similar al ejemplo siguiente:

```
esxcli --server=server_name storage core plugin list --plugin-class=Filter
Plugin name  Plugin class
VAAI_FILTER  Filter
```

Comprobar el estado de compatibilidad de la aceleración de hardware

Use el comando **esxcli** para comprobar el estado de compatibilidad de la aceleración de hardware de un determinado dispositivo de almacenamiento.

En el procedimiento, **--server=*server_name*** especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de **esxcli** en ESXi Shell.

Procedimiento

- ◆ Ejecute el comando **esxcli --server=*server_name* storage core device list -d=*device_ID***.

La salida mostrará el estado de aceleración de hardware, o VAAI, que puede ser desconocido, compatible o no compatible.

```
# esxcli --server=server_name storage core device list -d naa.XXXXXXXXXXXXX4c
naa.XXXXXXXXXXXXX4c
Display Name: XXXX Fibre Channel Disk(naa.XXXXXXXXXXXXX4c)
Size: 20480
Device Type: Direct-Access
```



```

Multipath Plugin: NMP
XXXXXXXXXXXXXXXXXX
Attached Filters: VAAI_FILTER
VAAI Status: compatible
XXXXXXXXXXXXXXXXXX

```

Comprobar los detalles de compatibilidad con la aceleración de hardware

Use el comando `esxcli` para comprobar la compatibilidad del dispositivo de almacenamiento en bloque con la aceleración de hardware.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Ejecute el comando `esxcli --server=server_name storage core device vaai status get -d=device_ID`.

Si el dispositivo se administra con un complemento VAAI, la salida muestra el nombre del complemento asociado al dispositivo. La salida también muestra el estado de compatibilidad de cada T10 SCSI primitivo, si están disponibles. En el siguiente ejemplo se muestra una salida:

```

# esxcli --server=server_name storage core device vaai status get -d naa.XXXXXXXXXXX4c
naa.XXXXXXXXXXX4c
VAAI Plugin Name: VMW_VAAIP_SYMM
ATS Status: compatible
Clone Status: compatible
Zero Status: compatible
Delete Status: unsupported

```

Lista de reglas de notificación de aceleración de hardware

Cada dispositivo de almacenamiento en bloque administrado por un complemento VAAI necesita dos reglas de notificación: una que especifique el filtro de aceleración de hardware y otra que especifique el complemento de aceleración de hardware del dispositivo. Se pueden utilizar los comandos `esxcli` para generar una lista de las reglas de notificación del filtro y del complemento de aceleración de hardware.

Procedimiento

- 1 Para generar una lista de las reglas de notificación, ejecute el comando **esxcli --server=*server_name* storage core claimrule list --claimrule-class=Filter**.

En este ejemplo, las reglas de notificación del filtro especifican dispositivos que debe reclamar el filtro VAAI_FILTER.

```
# esxcli --server=server_name storage core claimrule list --claimrule-class=Filter
Rule Class Rule Class Type Plugin Matches
Filter 65430 runtime vendor VAAI_FILTER vendor=EMC model=SYMMETRIX
Filter 65430 file vendor VAAI_FILTER vendor=EMC model=SYMMETRIX
Filter 65431 runtime vendor VAAI_FILTER vendor=DGC model=*
Filter 65431 file vendor VAAI_FILTER vendor=DGC model=*
```

- 2 Para generar una lista de las reglas de notificación del complemento, ejecute el comando **esxcli --server=*server_name* storage core claimrule list --claimrule-class=VAAI**.

En este ejemplo, las reglas de notificación de VAAI especifican dispositivos que debe reclamar un complemento VAAI específico.

```
esxcli --server=server_name storage core claimrule list --claimrule-class=VAAI
Rule Class Rule Class Type Plugin Matches
VAAI 65430 runtime vendor VMW_VAAIP_SYMM vendor=EMC model=SYMMETRIX
VAAI 65430 file vendor VMW_VAAIP_SYMM vendor=EMC model=SYMMETRIX
VAAI 65431 runtime vendor VMW_VAAIP_CX vendor=DGC model=*
VAAI 65431 file vendor VMW_VAAIP_CX vendor=DGC model=*
```

Agregar reglas de notificación de aceleración de hardware

Para configurar la aceleración de hardware de una matriz nueva, es necesario agregar dos reglas de notificación, una para el filtro VAAI y otra para el complemento VAAI. Para que las reglas de notificación nuevas estén activas, primero se deben definir las reglas y, a continuación, se las debe cargar en el sistema.

Este procedimiento es para aquellos dispositivos de almacenamiento en bloque que no admiten comandos SCSI T10 y, en su lugar, utilizan los complementos VAAI.

En el procedimiento, **--server=*server_name*** especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de **esxcli** en ESXi Shell.

Procedimiento

- 1 Defina una regla de notificación nueva para el filtro VAAI ejecutando el comando `esxcli --server=server_name storage core claimrule add --claimrule-class=Filter --plugin=VAAI_FILTER`.
- 2 Defina una regla de notificación nueva para el complemento VAAI ejecutando el comando `esxcli --server=server_name storage core claimrule add --claimrule-class=VAAI`.
- 3 Cargue ambas reglas de notificación ejecutando los comandos siguientes:


```
esxcli --server=server_name storage core claimrule load --claimrule-class=Filter
esxcli --server=server_name storage core claimrule load --claimrule-class=VAAI
```
- 4 Ejecute la regla de notificación de filtro VAAI con el comando `esxcli --server=server_name storage core claimrule run --claimrule-class=Filter`.

Nota Solo es necesario ejecutar las reglas de clase de filtro. Cuando el filtro VAAI reclama un dispositivo, encuentra automáticamente el complemento VAAI adecuado para asociar.

Ejemplo: Definir reglas de notificación de aceleración de hardware

En este ejemplo se muestra cómo configurar la aceleración de hardware para las matrices IBM con el complemento VMW_VAAIP_T10. Utilice la secuencia de comandos siguiente. Para obtener información sobre las opciones que acepta el comando, consulte [Agregar reglas de notificación de múltiples rutas](#).

```
# esxcli --server=server_name storage core claimrule add --claimrule-class=Filter --plugin=VAAI_FILTER --type=vendor --vendor=IBM --autoassign
# esxcli --server=server_name storage core claimrule add --claimrule-class=VAAI --plugin=VMW_VAAIP_T10 --type=vendor --vendor=IBM --autoassign
# esxcli --server=server_name storage core claimrule load --claimrule-class=Filter
# esxcli --server=server_name storage core claimrule load --claimrule-class=VAAI
# esxcli --server=server_name storage core claimrule run --claimrule-class=Filter
```

Eliminar reglas de notificación de aceleración de hardware

Utilice el comando `esxcli` para eliminar las reglas de notificación de aceleración de hardware existentes.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Ejecute los siguientes comandos:

```
esxcli --server=server_name storage core claimrule remove -r claimrule_ID
--claimrule-class=Filter
```

```
esxcli --server=server_name storage core claimrule remove -r claimrule_ID
--claimrule-class=VAAI
```

Aceleración de hardware en dispositivos NAS

La aceleración de hardware permite a los hosts ESXi integrarse con dispositivos NAS y usar varias operaciones de hardware que proporciona el almacenamiento NAS. La aceleración de hardware utiliza VMware vSphere Storage APIs para la integración de matrices (VAAI) para habilitar la comunicación entre los hosts y los dispositivos de almacenamiento.

Las API definen un conjunto de primitivos de almacenamiento que habilitan al host a descargar ciertas operaciones de almacenamiento a la matriz. La lista siguiente muestra las operaciones NAS admitidas:

- Clonación de archivo completo. Permite al dispositivo NAS clonar archivos del disco virtual. Esta operación es similar a la clonación en bloque de VMFS, a excepción de que los dispositivos NAS clonan archivos completos en lugar de segmentos de archivos.
- Reserva de espacio. Habilita a las matrices de almacenamiento a asignar espacio para un archivo de disco virtual en formato grueso.

Generalmente, cuando crea un disco virtual en un almacén de datos de NFS, el servidor NAS determina la directiva de asignación. La directiva de asignación predeterminada en la mayoría de los servidores NAS es de formato fino y no garantiza la copia de seguridad del almacenamiento en el archivo. Sin embargo, la operación de reserva de espacio puede indicar al dispositivo NAS que utilice mecanismos específicos del proveedor para reservar espacio para un disco virtual. Como resultado, es posible crear discos virtuales gruesos en el almacén de datos de NFS.

- Compatibilidad nativa con instantáneas. Permite que la creación de instantáneas de máquina virtual se descargue en la matriz.

- Estadísticas ampliadas. Habilita la visibilidad del uso del espacio en dispositivos NAS y es útil para el aprovisionamiento fino.

Con los dispositivos de almacenamiento NAS, la integración con la aceleración de hardware se implementa a través de complementos NAS específicos del proveedor. Generalmente, los proveedores crean estos complementos y se distribuyen como paquetes de VIB a través de una página web. No se necesitan reglas de notificación para que funcionen los complementos NAS.

Existen varias herramientas disponibles para instalar y actualizar los paquetes de VIB. Incluyen los comandos `esxcli` y vSphere Update Manager. Para obtener más información, consulte la documentación sobre *Actualización de vSphere* y *Instalación y administración de VMware vSphere Update Manager*.

Instalar el complemento de NAS

Instale complementos de NAS de aceleración de hardware distribuidos por el proveedor en el host.

En este tema se ofrece un ejemplo de instalación de un paquete VIB con el comando `esxcli`. Para obtener más detalles, consulte la documentación de *Actualización de vSphere*.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- 1 Coloque el host en modo de mantenimiento.
- 2 Establezca el nivel de aceptación del host:

```
esxcli --server=server_name software acceptance set --level=value
```

El comando controla qué paquete VIB se permite en el host. La variable *value* puede ser una de las siguientes:

- VMwareCertified
- VMwareAccepted
- PartnerSupported
- CommunitySupported

- 3 Instale el paquete VIB:

```
esxcli --server=server_name software vib install -v|--viburl=URL
```

La variable *URL* especifica la URL del paquete VIB que se va a instalar; http:, https:, ftp: y file: y file:.

- 4 Compruebe que se haya instalado el complemento:

```
esxcli --server=server_name software vib list
```

- 5 Reinicie el host para que la instalación se aplique.

Desinstalar los complementos de NAS

Para desinstalar un complemento de NAS, quite el paquete de VIB del host.

En este tema se analiza cómo desinstalar un paquete de VIB con el comando `esxcli`. Para obtener más detalles, consulte la documentación de *Actualización de vSphere*.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- 1 Desinstale el complemento:

```
esxcli --server=server_name software vib remove -n|--vibname=name
```

La variable *name* es el nombre del paquete de VIB que desea quitar.

- 2 Compruebe que se haya eliminado el complemento:

```
esxcli --server=server_name software vib list
```

- 3 Reinicie el host para que se apliquen los cambios.

Actualizar los complementos de NAS

Actualice los complementos de NAS de aceleración de hardware en el host cuando un proveedor de almacenamiento publique una nueva versión del complemento.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

En este tema se analiza cómo actualizar un paquete de VIB con el comando `esxcli`. Para obtener más detalles, consulte la documentación de *Actualización de vSphere*.

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- 1 Actualice el complemento a una versión nueva:

```
esxcli --server=server_name software vib update -v|--viburl=URL
```

La variable *URL* especifica la URL del paquete de VIB que se desea actualizar. Se admiten las opciones `http:`, `https:`, `ftp:` y `file:`.

- 2 Compruebe que se haya instalado la versión correcta:

```
esxcli --server=server_name software vib list
```

- 3 Reinicie el host.

Comprobar el estado de aceleración de hardware para NAS

Además del cliente, puede utilizar el comando `esxcli` para comprobar el estado de aceleración del hardware del dispositivo NAS.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Ejecute el comando **`esxcli --server=server_name storage nfs list`**.

La columna Hardware Acceleration (Aceleración de hardware) en los resultados muestra el estado.

Consideraciones sobre la aceleración de hardware

Cuando se utiliza la funcionalidad de aceleración de hardware, aplican ciertas consideraciones.

Varios motivos pueden causar errores en una operación acelerada por hardware.

Por cada primitivo que la matriz no implementa, la matriz devuelve un error. El error activa el host ESXi para intentar la operación con los métodos nativos.

El administrador de transferencia de datos de VMFS no aprovecha las descargas de hardware, en su lugar, utiliza el movimiento de los datos de software cuando ocurre una de las situaciones siguientes:

- Los almacenes de datos de VMFS de origen y destino tienen distintos tamaños de bloques.
- El tipo de archivo de origen es RDM y el tipo de archivo de destino no lo es (archivo normal).
- El tipo VMDK de origen es grueso con todos los bloques puestos a cero y el tipo de VMDK de destino es fino.
- El VMDK de origen o destino está en formato disperso o alojado.
- La máquina virtual de origen tiene una instantánea.
- La dirección lógica y la longitud de transferencia en la operación solicitada no están alineadas con la alineación mínima que requiere el dispositivo de almacenamiento. Todos los almacenes de datos creados con vSphere Web Client se alinean automáticamente.
- VMFS tiene varios LUN o extensiones, y se encuentran en distintas matrices.

La clonación de hardware entre matrices, incluso dentro del mismo almacén de datos de VMFS, no funciona.

Aprovisionamiento fino y grueso de almacenamiento

24

vSphere admite dos modelos de aprovisionamiento de almacenamiento: aprovisionamiento grueso y aprovisionamiento fino.

Aprovisionamiento grueso

Es un modelo tradicional de aprovisionamiento de almacenamiento. Con el aprovisionamiento grueso, se proporciona por adelantado una gran cantidad de espacio de almacenamiento para anticipar necesidades de almacenamiento futuras. Sin embargo, el espacio puede permanecer inutilizado, lo que genera la infrautilización de la capacidad de almacenamiento.

Aprovisionamiento fino

Este método se opone al aprovisionamiento grueso y ayuda a eliminar problemas de infrautilización del almacenamiento al asignar el espacio de almacenamiento de manera flexible y a petición. Con ESXi, puede utilizar dos modelos de aprovisionamiento fino, en el nivel de la matriz y en el nivel del disco virtual.

Este capítulo incluye los siguientes temas:

- [Sobresuscripción del almacenamiento](#)
- [Aprovisionamiento fino de discos virtuales](#)
- [Aprovisionamiento fino de matrices y almacenes de datos de VMFS](#)

Sobresuscripción del almacenamiento

El aprovisionamiento fino permite informar más espacio de almacenamiento virtual que la capacidad física real. Esta discrepancia puede llevar a una sobresuscripción de almacenamiento, también denominada sobreaprovisionamiento.

Cuando usa aprovisionamiento fino, debe supervisar el uso real del almacenamiento para evitar condiciones en las que se quede sin espacio de almacenamiento físico.

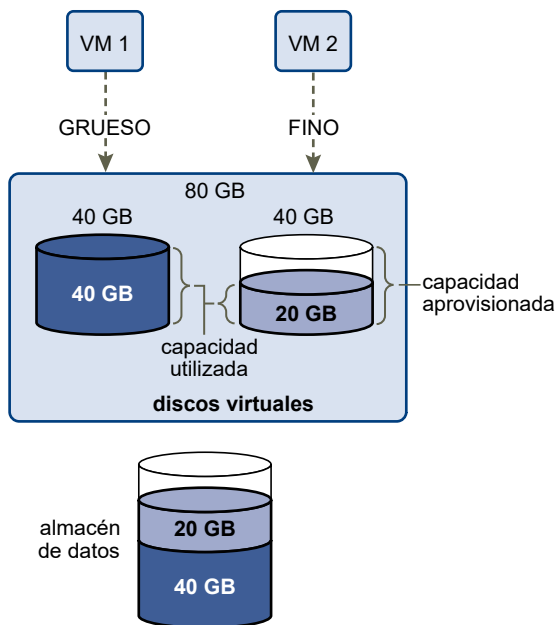
Aprovisionamiento fino de discos virtuales

Cuando se crea una máquina virtual, se aprovisiona una cierta cantidad de espacio de almacenamiento de un almacén de datos a archivos de disco virtual.

De forma predeterminada, ESXi ofrece un método de aprovisionamiento de almacenamiento tradicional para las máquinas virtuales. Con este método, primero se estima cuánto espacio de la máquina virtual se necesitará para el ciclo de vida completo. A continuación, se aprovisiona una cantidad de espacio de almacenamiento fija para el disco virtual por adelantado, por ejemplo, 40 GB, y se confirma todo el espacio aprovisionado en el disco virtual. Un disco virtual que inmediatamente ocupa todo el espacio aprovisionado es un disco grueso.

ESXi admite el aprovisionamiento fino de discos virtuales. Con la característica de aprovisionamiento fino en el nivel del disco, se pueden crear discos virtuales en un formato fino. En un disco virtual fino, ESXi aprovisiona el espacio completo necesario para las actividades actuales y futuras del disco, por ejemplo, 40 GB. Sin embargo, el disco fino utiliza solo la cantidad de espacio que necesita el disco para las operaciones iniciales. En este ejemplo, el disco de aprovisionamiento fino ocupa solo 20 GB de almacenamiento. Dado que el disco requiere más espacio, puede utilizar hasta el total de 40 GB aprovisionados.

Figura 24-1. Discos virtuales finos y gruesos



Acerca de las directivas de aprovisionamiento de discos virtuales

Al realizar ciertas operaciones de administración de máquinas virtuales, como crear un disco virtual, clonar una máquina virtual a una plantilla o migrar una máquina virtual, se puede especificar la directiva de aprovisionamiento para el archivo del disco virtual.

Los almacenes de datos de NFS con aceleración de hardware y los almacenes de datos de VMFS admiten las siguientes directivas de aprovisionamiento de discos. En los almacenes de datos de NFS que se no admite la aceleración de hardware, solo está disponible el formato fino.

Puede utilizar Storage vMotion o bien Storage vMotion entre hosts para pasar los discos virtuales de un formato a otro.

Thick Provision Lazy Zeroed (Puesta a cero lenta con aprovisionamiento grueso)

Crea un disco virtual en un formato grueso predeterminado. El espacio necesario para el disco virtual se asigna en el momento en que se crea el disco. Los datos que quedan en el dispositivo físico no se borran durante la creación, sino que se ponen a cero a petición más adelante, en la primera escritura de la máquina virtual. Las máquinas virtuales no leen datos obsoletos del dispositivo físico.

Thick Provision Eager Zeroed (Puesta a cero rápida con aprovisionamiento grueso)

Un tipo de disco virtual grueso que admite características de clúster, como Fault Tolerance. El espacio necesario para el disco virtual se asigna en el momento de la creación. A diferencia del formato de puesta a cero lenta de aprovisionamiento grueso, los datos que quedan en el dispositivo físico se ponen a cero cuando se crea el disco virtual. Es posible que la creación de discos virtuales en este formato demore más que la creación de otros tipos de disco.

Thin Provision (Aprovisionamiento fino)

Utilice este formato para ahorrar espacio de almacenamiento. Para el disco fino, aprovisione tanto espacio de almacén de datos como lo requiera el disco, en función del valor que introduzca para el tamaño del disco virtual. Sin embargo, el disco fino comienza siendo pequeño y, al principio, utiliza solo el espacio de almacén de datos que necesita para las operaciones iniciales. Si posteriormente el disco fino necesita más espacio, puede aumentar su tamaño hasta la capacidad máxima y ocupar todo el espacio del almacén de datos aprovisionado para él.

El aprovisionamiento fino es el método más rápido para crear un disco virtual, ya que crea un disco solo con la información del encabezado. No asigna ni pone a cero los bloques de almacenamiento. Los bloques de almacenamiento se asignan y se ponen a cero la primera vez que se accede a ellos.

Nota Si un disco virtual admite soluciones de agrupación en clústeres, como Fault Tolerance, ese disco no debe tener aprovisionamiento fino.

Puede expandir manualmente el disco fino para que ocupe todo el espacio aprovisionado. Si el espacio de almacenamiento físico se agotó y el disco con aprovisionamiento fino no puede ampliarse, la máquina virtual se volverá inutilizable.

Crear discos virtuales con aprovisionamiento fino

Para ahorrar espacio de almacenamiento, se puede crear un disco virtual en formato de aprovisionamiento fino. El disco virtual con aprovisionamiento fino que se crea es pequeño y aumenta a medida que se requiere más espacio en disco. Es posible crear discos finos únicamente en almacenes de datos compatibles con aprovisionamiento fino en el nivel de disco.

Este procedimiento da por sentado que se está creando una máquina virtual nueva. Para obtener más información, consulte la documentación de *Administración de máquinas virtuales de vSphere*.

Procedimiento

- 1 Haga clic con el botón derecho en cualquier objeto de inventario que sea un objeto primario válido de una máquina virtual, como un centro de datos, una carpeta, un clúster, un grupo de recursos o un host y seleccione **New Virtual Machine** (Nueva máquina virtual).
- 2 Seleccione **Create a new virtual machine** (Crear una nueva máquina virtual) y haga clic en **Next** (Siguiente).
- 3 Siga los pasos necesarios para crear una máquina virtual.
- 4 En la página Customize Hardware (Personalizar hardware), haga clic en la pestaña **Virtual Hardware** (Hardware virtual).
- 5 Haga clic en el triángulo **New Hard Disk** (Nuevo disco duro) para expandir las opciones del disco duro.
- 6 (opcional) Ajuste el tamaño de disco predeterminado.

Con un disco virtual fino, el valor de tamaño de disco muestra cuánto espacio está aprovisionado y garantizado para el disco. Al principio, es posible que el disco virtual no utilice todo el espacio aprovisionado, por lo que el valor de utilización de almacenamiento real puede ser menor al tamaño del disco virtual.

- 7 En Disk Provisioning (Aprovisionamiento de disco), seleccione **Thin Provision** (Aprovisionamiento fino).
- 8 Finalice la creación de la máquina virtual.

Resultados

Creó una máquina virtual con un disco en formato fino.

Pasos siguientes

Si se creó un disco virtual en el formato fino, más tarde se podrá expandir hasta su tamaño completo.

Ver los recursos de almacenamiento de una máquina virtual

Es posible ver cómo el espacio de almacenamiento del almacén de datos se asigna a las máquinas virtuales.

Storage Usage (Uso del almacenamiento) muestra cuánto espacio del almacén de datos ocupan los archivos de máquina virtual, incluidos los archivos de registro y configuración, las instantáneas, los discos virtuales, etc. Cuando la máquina virtual está en ejecución, el espacio de almacenamiento utilizado también incluye archivos de intercambio.

En las máquinas virtuales con discos finos, el valor de uso del almacenamiento real puede ser inferior al tamaño del disco virtual.

Procedimiento

- 1 En vSphere Web Client, desplácese hasta la máquina virtual.
- 2 Haga doble clic en la máquina virtual y haga clic en la pestaña **Summary** (Resumen).
- 3 Revise la información de uso del almacenamiento en el área superior derecha de la pestaña **Summary** (Resumen).

Determinar el formato de disco de una máquina virtual

Puede determinar si el disco virtual tendrá formato grueso o fino.

Procedimiento

- 1 En vSphere Web Client, desplácese hasta la máquina virtual.
- 2 Haga clic con el botón derecho en la máquina virtual y seleccione **Edit Settings** (Editar configuración).
- 3 Haga clic en la pestaña **Virtual Hardware** (Hardware virtual).
- 4 Haga clic en el triángulo **Hard Disk** (Disco duro) para expandir las opciones de disco duro.

El cuadro de texto **Type** (Tipo) muestra el formato del disco virtual.

Pasos siguientes

Si el disco virtual tiene formato fino, puede expandirlo a su tamaño completo.

Expandir discos virtuales finos

Si creó un disco virtual en formato fino, puede convertir el disco fino a un disco virtual con formato de aprovisionamiento grueso.

Puede utilizar el explorador del almacén de datos para expandir el disco virtual.

Requisitos previos

- Asegúrese de que el almacén de datos donde se encuentra la máquina virtual tenga espacio suficiente.
- Asegúrese de que el disco virtual sea fino.
- Quite las instantáneas.
- Apague la máquina virtual.

Procedimiento

- 1 Desplácese hasta la carpeta del disco virtual que desea expandir.
 - a En vSphere Web Client, desplácese hasta la máquina virtual.
 - b Haga doble clic en la máquina virtual para mostrar la información.

- c Haga clic en la pestaña **Objetos relacionados** y haga clic en **Almacenes de datos**.

Se enumera el almacén de datos que almacena los archivos de la máquina virtual.

- d Seleccione el almacén de datos y haga clic en el icono **Desplazarse hasta el explorador de archivos en el almacén de datos**.

El explorador del almacén de datos muestra el contenido del almacén de datos.

- 2 Abra la carpeta de la máquina virtual y desplácese hasta el archivo del disco virtual que desea convertir.

El archivo tiene la extensión `.vmdk` y está marcado con el icono de disco virtual (.

- 3 Haga clic con el botón derecho en el archivo de disco virtual y seleccione **Inflar**.

Nota Es posible que la opción no esté disponible si el disco virtual es grueso o si la máquina virtual está en ejecución.

Resultados

El disco virtual inflado ocupa el espacio del almacén de datos completo que se le aprovisionó originalmente.

Manejar la sobresuscripción del almacén de datos

Debido a que el espacio aprovisionado para los discos finos puede ser mayor que el espacio establecido, puede producirse una sobresuscripción del almacén de datos. En consecuencia, el espacio aprovisionado total para los discos de máquinas virtuales en el almacén de datos es mayor que la capacidad real.

La sobresuscripción puede ocurrir debido a que, por lo general, no todas las máquinas virtuales con discos finos necesitan simultáneamente todo el espacio del almacén de datos aprovisionado. Sin embargo, si desea evitar una sobresuscripción del almacén de datos, puede configurar una alarma que notifique el momento en el que espacio aprovisionado llega a un determinado umbral.

Para obtener información sobre la configuración de alarmas, consulte la documentación de *Administración de vCenter Server y hosts*.

Si las máquinas virtuales requieren más espacio, el espacio del almacén de datos se asigna por orden de llegada. Cuando el almacén de datos se queda sin espacio, puede agregar más almacenamiento físico y aumentar el almacén de datos.

Consulte [Aumentar la capacidad de un almacén de datos de VMFS](#).

Aprovisionamiento fino de matrices y almacenes de datos de VMFS

Puede utilizar matrices de almacenamiento de aprovisionamiento fino con ESXi.

Los LUN tradicionales que las matrices presentan al host ESXi son de aprovisionamiento grueso. Todo el espacio físico necesario para respaldar a cada LUN se asigna por adelantado.

ESXi también admite LUN de aprovisionamiento fino. Cuando un LUN es de aprovisionamiento fino, la matriz de almacenamiento informa del tamaño lógico del LUN, que puede ser mayor que la capacidad física real que respalda a ese LUN.

Un almacén de datos de VMFS que se implementa en el LUN de aprovisionamiento fino puede detectar solo el tamaño lógico del LUN. Por ejemplo, si la matriz informa de 2 TB de almacenamiento cuando en realidad la matriz ofrece solo 1 TB, el almacén de datos considera que el tamaño del LUN es 2 TB. A medida que el almacén de datos crece, no puede determinar si la cantidad real de espacio físico es suficiente para sus necesidades.

Sin embargo, cuando se utiliza Storage APIs - Array Integration, el host puede integrarse con el almacenamiento físico y detectar los LUN de aprovisionamiento fino subyacentes con su correspondiente utilización de espacio.

Al utilizar la integración de aprovisionamiento fino, el host puede realizar las siguientes tareas:

- Supervisar la utilización de espacio en LUN de aprovisionamiento fino para no quedarse sin espacio físico. A medida que el almacén de datos crece, o si se utiliza Storage vMotion para migrar máquinas virtuales a un LUN de aprovisionamiento fino, el host se comunica con el LUN y emite advertencias sobre las infracciones de espacio físico y las condiciones de falta de espacio.
- Informar a la matriz sobre el espacio liberado en el almacén de datos cuando Storage vMotion elimina o borra archivos del almacén de datos. De ese modo, la matriz puede recuperar los bloques de espacio liberados.

Nota ESXi no admite la habilitación y deshabilitación de aprovisionamiento fino en un dispositivo de almacenamiento.

Requisitos

Para utilizar la característica de informes de aprovisionamiento fino, el host y la matriz de almacenamiento deben cumplir los siguientes requisitos:

- ESXi versión 5.0 o posteriores.
- La matriz de almacenamiento tiene firmware apropiado que admite Storage APIs - Array Integration (aprovisionamiento fino) basado en T10. Para obtener información, póngase en contacto con el proveedor de almacenamiento y compruebe el HCL.

Supervisar la utilización del espacio

La funcionalidad de integración de aprovisionamiento fino ayuda a supervisar el uso del espacio en los LUN con aprovisionamiento fino y a evitar quedarse sin espacio.

El flujo de muestra siguiente demuestra cómo el host ESXi y la matriz de almacenamiento interactúan para generar advertencias por infracción del espacio y falta de espacio de un almacén de datos con LUN con aprovisionamiento fino subyacente. Se aplica el mismo mecanismo cuando se utiliza Storage vMotion para migrar máquinas virtuales al LUN con aprovisionamiento fino.

- 1 Mediante herramientas específicas de almacenamiento, el administrador de almacenamiento aprovisiona un LUN fino y establece un límite de umbral flexible que, cuando se alcanza, activa una alerta. Este paso es específico del proveedor.
- 2 Con vSphere Web Client, puede crear un almacén de datos de VMFS en el LUN con aprovisionamiento fino. El almacén de datos abarca el tamaño lógico completo que informa el LUN.
- 3 A medida que el espacio que utiliza el almacén de datos aumenta y se alcanza el umbral flexible especificado, se realizan las acciones siguientes:
 - a La matriz de almacenamiento informa la infracción al host.
 - b El host activa una alarma de advertencia para el almacén de datos.

Puede ponerse en contacto con el administrador de almacenamiento para solicitar más espacio físico o utilizar Storage vMotion para evacuar las máquinas virtuales antes de que los LUN se queden sin capacidad.
- 4 Si no queda espacio para asignar al LUN con aprovisionamiento fino, se realizan las acciones siguientes:
 - a La matriz de almacenamiento informa la condición de falta de espacio al host.

Precaución En ciertos casos, cuando un LUN se llena, puede desconectarse o desasignarse del host.

- b El host pausa las máquinas virtuales y genera una alarma por falta de espacio.

Para solucionar la condición de falta de espacio permanente, solicite más espacio físico al administrador de almacenamiento.

Identificar dispositivos de almacenamiento de aprovisionamiento fino

Use el comando `esxcli` para comprobar si un dispositivo de almacenamiento particular es de aprovisionamiento fino.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Ejecute el comando `esxcli --server=server_name storage core device list -d=device_ID`.

Resultados

El estado de aprovisionamiento fino siguiente indica que el dispositivo de almacenamiento es de aprovisionamiento fino.

```
# esxcli --server=server_name storage core device list -d naa.XXXXXXXXXXX4c
naa.XXXXXXXXXXX4c
Display Name: XXXX Fibre Channel Disk(naa.XXXXXXXXXXX4c)
Size: 20480
Device Type: Direct-Access
Multipath Plugin: NMP
-----
Thin Provisioning Status: yes
Attached Filters: VAAI_FILTER
VAAI Status: compatible
-----
```

Un estado desconocido indica que el dispositivo de almacenamiento es grueso.

Nota Algunos sistemas de almacenamiento presentan todos los dispositivos como de aprovisionamiento fino, sin importar si los dispositivos son finos o gruesos. El estado de aprovisionamiento fino siempre es `yes`. Para obtener más información, consulte al proveedor de almacenamiento.

Recuperar espacio de almacenamiento acumulado

Cuando hay almacenes de datos de VMFS que residen en LUN de aprovisionamiento fino, puede usar el comando `esxcli` para recuperar bloques de almacenamiento no utilizados.

En el procedimiento, `--server=server_name` especifica el servidor de destino. El servidor de destino especificado solicita un nombre de usuario y una contraseña. Se admiten otras opciones de conexión, como un archivo de configuración o un archivo de sesión. Para obtener una lista de opciones de conexión, consulte *Introducción a vSphere Command-Line Interface*.

Requisitos previos

Instale vCLI o implemente la máquina virtual de vSphere Management Assistant (vMA). Consulte *Introducción a vSphere Command-Line Interface*. Para solucionar problemas, ejecute los comandos de `esxcli` en ESXi Shell.

Procedimiento

- ◆ Para recuperar bloques de almacenamiento no utilizados en el almacén de datos VMFS5 para el dispositivo de aprovisionamiento delgado, ejecute el siguiente comando:

```
esxcli --server=server_name storage vmfs unmap --volume-label=volume_label|--volume-uuid=volume_uuid --reclaim-unit=number
```

Este comando toma estas opciones:

Opción	Descripción
-l --volume-label=volume_label	La etiqueta del volumen VMFS cuya asignación se desea anular. Este es un argumento obligatorio. Si especifica este argumento, no use -u --volume-uuid=volume_uuid .
-u --volume-uuid=volume_uuid	El UUID del volumen VMFS cuya asignación se desea anular. Este es un argumento obligatorio. Si especifica este argumento, no use -l --volume-label=volume_label .
-n --reclaim-unit=number	Cantidad de bloques VMFS cuya asignación se desea anular por iteración. Este es un argumento opcional. Si no se especifica, el comando utiliza el valor predeterminado de 200.

Pasos siguientes

Importante Para obtener detalles adicionales, consulte el artículo de la base de conocimientos de VMware en <http://kb.vmware.com/kb/2014849>.

Usar proveedores de almacenamiento

25

Un proveedor de almacenamiento es un componente de software que ofrece vSphere o que desarrolla un tercero a través de vSphere API for Storage Awareness (VASA). Los proveedores de almacenamiento se integran con una variedad de entidades de almacenamiento que incluyen almacenamiento físico externo y abstracciones de almacenamiento, como Virtual SAN y Virtual Volumes. Los proveedores de almacenamiento también pueden admitir soluciones de software, por ejemplo, filtros de E/S desarrollados a través de vSphere API para los filtros de E/S.

Generalmente, vSphere usa proveedores de almacenamiento para obtener información sobre la topología del almacenamiento, el estado y los servicios de datos de almacenamiento que se ofrecen en su entorno. Esta información aparece en vSphere Web Client. La información ayuda a tomar las decisiones adecuadas sobre la selección de máquinas virtuales y a supervisar el entorno de almacenamiento.

El proveedor de almacenamiento de terceros generalmente se instala del lado del almacenamiento y actúa como un servicio de reconocimiento de almacenamiento en el entorno de vSphere.

Para saber si el almacenamiento es compatible con los complementos del proveedor de almacenamiento, póngase en contacto con el distribuidor de almacenamiento. Si el almacenamiento es compatible con proveedores de almacenamiento de terceros, use vSphere Web Client para registrar y administrar cada componente del proveedor de almacenamiento.

Los proveedores de almacenamiento integrados generalmente se ejecutan en los hosts ESXi y no requieren registro. Por ejemplo, el proveedor de almacenamiento compatible con Virtual SAN se registra automáticamente cuando se habilita Virtual SAN. Para obtener más información, consulte la documentación sobre *Administración de VMware Virtual SAN*.

Este capítulo incluye los siguientes temas:

- [Proveedores de almacenamiento y representación de datos de almacenamiento](#)
- [Consideraciones y requisitos del proveedor de almacenamiento](#)
- [Informe de estado de almacenamiento](#)
- [Registrar proveedores de almacenamiento](#)
- [Proteger la comunicación con proveedores de almacenamiento](#)
- [Ver información sobre el proveedor de almacenamiento](#)

- [Cancelar el registro de proveedores de almacenamiento](#)
- [Actualizar proveedores de almacenamiento](#)

Proveedores de almacenamiento y representación de datos de almacenamiento

vCenter Server y ESXi se comunican con el proveedor de almacenamiento para obtener información que el proveedor de almacenamiento recopila del almacenamiento físico subyacente y del almacenamiento definido por software, o bien de los filtros de E/S disponibles. De ese modo, vCenter Server puede mostrar los datos de almacenamiento en vSphere Web Client.

La información que proporciona el proveedor de almacenamiento puede dividirse en las siguientes categorías:

- Capacidades y servicios de datos de almacenamiento. Este tipo de información es esencial para funcionalidades como Virtual SAN, Virtual Volumes y los filtros de E/S. El proveedor de almacenamiento recopila información sobre servicios de datos que ofrecen entidades de almacenamiento subyacentes o filtros de E/S disponibles.

Se hace referencia a estos servicios de datos cuando se definen los requisitos de almacenamiento para máquinas virtuales y discos virtuales en una directiva de almacenamiento. Según el entorno, la directiva de almacenamiento garantiza una selección adecuada del almacenamiento para una máquina virtual o habilita servicios de datos específicos para discos virtuales. Para obtener información detallada, consulte [Descripción de las directivas de almacenamiento de máquinas virtuales](#).

- Estado de almacenamiento. Esta categoría incluye informes sobre el estado de distintas entidades de almacenamiento. También incluye alarmas y eventos para notificar acerca de cambios de configuración.

Este tipo de información puede ayudar a resolver problemas de rendimiento y conectividad de almacenamiento. También puede ser útil para facilitar la correlación de eventos y alarmas generados por la matriz con los correspondientes cambios de rendimiento y carga de esa matriz.

- Información de Storage DRS. Para programación de recursos distribuidos (DRS) en dispositivos en bloque o sistemas de archivos. Los proveedores de almacenamiento ofrecen información adicional sobre el sistema de almacenamiento, para que las decisiones tomadas por Storage DRS sean compatibles con las decisiones de administración de recursos internas de los sistemas de almacenamiento.

Consideraciones y requisitos del proveedor de almacenamiento

Cuando se utiliza la funcionalidad del proveedor de almacenamiento, se aplican ciertos requisitos y consideraciones.

Por lo general, los distribuidores son responsables de suministrar los proveedores de almacenamiento que se integran con vSphere. Los proveedores de almacenamiento se implementan a través de VMware API for Storage Awareness (VASA). La arquitectura de VASA extiende el servicio de supervisión de almacenamiento (SMS) que se ofrece con vSphere, y define un conjunto de funciones que vCenter Server y los hosts ESXi pueden utilizar para comunicarse con los proveedores de VASA.

Para utilizar los proveedores de almacenamiento, cumpla estos requisitos:

- Asegúrese de que cada proveedor de almacenamiento esté certificado por VMware y correctamente implementado. Para obtener información sobre la implementación de proveedores de almacenamiento, póngase en contacto con el distribuidor de almacenamiento o revise la *Guía de compatibilidad de VMware*.
- Asegúrese de que el proveedor de almacenamiento sea compatible con la versión de vSphere. Consulte *Guía de compatibilidad de VMware*.

Cuando utiliza proveedores de almacenamiento, se aplican las consideraciones siguientes:

- Tanto los dispositivos de almacenamiento del sistema de archivos como los de almacenamiento en bloque pueden utilizar proveedores de almacenamiento.
- Los proveedores de almacenamiento pueden ejecutarse en todos lados, menos en vCenter Server. Por lo general, el proveedor de almacenamiento de terceros se ejecuta en un procesador de servicio de matriz de almacenamiento o en un host independiente.
- Varios vCenter Server pueden conectarse simultáneamente a una misma instancia de un proveedor de almacenamiento.
- Un solo vCenter Server puede conectarse simultáneamente a varios proveedores de almacenamiento diferentes. Es posible tener un proveedor de almacenamiento diferente para cada tipo de dispositivo de almacenamiento físico disponible para el host.

Informe de estado de almacenamiento

Si utiliza proveedores de almacenamiento, vCenter Server puede recopilar características de estado para dispositivos de almacenamiento físicos y mostrar esta información en vSphere Web Client.

La información de estado incluye eventos y alarmas.

- Los eventos indican cambios importantes en la configuración del almacenamiento. Entre estos cambios pueden encontrarse la creación y la eliminación de un LUN, o la imposibilidad de acceder a un LUN debido al enmascaramiento de LUN.
- Las alarmas indican un cambio en la disponibilidad del sistema de almacenamiento. Por ejemplo, cuando se usa la administración de almacenamiento basada en perfiles, se pueden especificar requisitos de almacenamiento de máquinas virtuales. Cuando se producen cambios en el almacenamiento subyacente que pueden infringir los requisitos de la máquina virtual, se dispara una alarma.

Para obtener más información sobre eventos y alarmas, consulte la documentación de *Supervisión y rendimiento de vSphere*.

Los LUN de aprovisionamiento delgado tienen requisitos de informe especiales. Para obtener información sobre la supervisión de espacio en LUN de aprovisionamiento delgado, consulte [Aprovisionamiento fino de matrices y almacenes de datos de VMFS](#).

Registrar proveedores de almacenamiento

Para establecer una conexión entre vCenter Server y un proveedor de almacenamiento, se debe registrar al proveedor de almacenamiento. Asegúrese de registrar un proveedor de almacenamiento distinto para cada host en un clúster.

Nota Si se utiliza Virtual SAN, los proveedores de almacenamiento de Virtual SAN se registran y aparecen en la lista de proveedores de almacenamiento automáticamente. Virtual SAN no admite el registro manual de proveedores de almacenamiento. Consulte la documentación de *Administración de VMware Virtual SAN*.

Requisitos previos

Compruebe que el componente del proveedor de almacenamiento esté instalado en el lado del almacenamiento y solicítele las credenciales correspondientes al administrador de almacenamiento.

Procedimiento

- 1 Desplácese hasta vCenter Server en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar** y, a continuación, en **Proveedores de almacenamiento**.
- 3 Haga clic en el icono **Registrar un nuevo proveedor de almacenamiento**.
- 4 Escriba la información de conexión del proveedor de almacenamiento, incluidos el nombre, la URL y las credenciales.
- 5 (opcional) Para dirigir vCenter Server al certificado del proveedor de almacenamiento, seleccione la opción **Usar certificado de proveedor de almacenamiento** y especifique la ubicación del certificado.

Si no selecciona esta opción, aparecerá la huella digital del certificado. Revise la huella digital y apruébela.
- 6 Haga clic en **Aceptar** para completar el registro.

Resultados

vCenter Server registró el proveedor de almacenamiento y estableció una conexión SSL segura con él.

Pasos siguientes

Si el proveedor de almacenamiento no puede registrarse, consulte el artículo de la base de conocimientos de VMware <http://kb.vmware.com/kb/2079087>. Si tiene problemas con el registro del proveedor de almacenamiento de Virtual SAN, consulte <http://kb.vmware.com/kb/2105018>.

Proteger la comunicación con proveedores de almacenamiento

Para comunicarse con un proveedor de almacenamiento, vCenter Server utiliza una conexión SSL segura. El mecanismo de autenticación SSL requiere que ambas partes, vCenter Server y el proveedor de almacenamiento, intercambien certificados SSL y los agreguen a sus almacenes de confianza.

vCenter Server puede agregar el certificado del proveedor de almacenamiento al almacén de confianza como parte de la instalación del proveedor de almacenamiento. Si el certificado no se agrega durante la instalación, utilice uno de los métodos siguientes para agregarlo en el momento de registrar el proveedor de almacenamiento:

- Dirija vCenter Server al certificado del proveedor de almacenamiento. En el cuadro de diálogo **New Storage Provider** (Nuevo proveedor de almacenamiento), seleccione la opción **Use storage provider certificate** (Utilizar certificado de proveedor de almacenamiento) y especifique la ubicación del certificado.
- Utilice una huella digital del certificado del proveedor de almacenamiento. Si no dirige vCenter Server para que utilice el certificado del proveedor, se muestra la huella digital del certificado. Revise la huella digital y apruébela. vCenter Server agrega el certificado al almacén de confianza y procede con la conexión.

El proveedor de almacenamiento agrega el certificado de vCenter Server al almacén de confianza cuando vCenter Server se conecta por primera vez al proveedor.

Ver información sobre el proveedor de almacenamiento

Luego de registrar un componente del proveedor de almacenamiento con vCenter Server, el proveedor de almacenamiento aparece en la lista de proveedores de almacenamiento.

Vea la información general del proveedor de almacenamiento y los detalles de cada componente de almacenamiento.

Procedimiento

- 1 Desplácese hasta vCenter Server en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar** y, a continuación, en **Proveedores de almacenamiento**.

- 3 En la lista Storage Providers (Proveedores de almacenamiento), vea los componentes del proveedor de almacenamiento registrados con vCenter Server.

En la lista aparece información general sobre el proveedor, por ejemplo, nombre, URL y la hora de actualización de la última visualización.

- 4 Para ver detalles adicionales, seleccione un proveedor de almacenamiento específico en la lista.

Los detalles incluyen distribuidores de matrices de almacenamiento y modelos de matrices que admite el proveedor.

Nota Un único proveedor de almacenamiento puede admitir matrices de almacenamiento de varios distribuidores diferentes.

Cancelar el registro de proveedores de almacenamiento

Cancele el registro de los proveedores de almacenamiento que no necesita.

Precaución No puede cancelar manualmente el registro de los proveedores de almacenamiento proporcionados por VMware, como los proveedores de almacenamiento de Virtual SAN.

Procedimiento

- 1 Desplácese hasta vCenter Server en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar** y, a continuación, en **Proveedores de almacenamiento**.
- 3 De la lista de proveedores de almacenamiento, seleccione uno del que desee cancelar el registro y haga clic en el icono **Unregister the storage provider** (Cancelar el registro del proveedor de almacenamiento).

Resultados

vCenter Server finaliza la conexión y quita al proveedor de almacenamiento de la configuración.

Actualizar proveedores de almacenamiento

vCenter Server actualiza los datos de almacenamiento de su base de datos de forma periódica. Las actualizaciones son parciales y reflejan solo los cambios de almacenamiento que los proveedores de almacenamiento comunican a vCenter Server. Cuando sea necesario, puede realizar una sincronización total de la base de datos para el proveedor de almacenamiento seleccionado.

Procedimiento

- 1 Desplácese hasta vCenter Server en el navegador de vSphere Web Client.
- 2 Haga clic en la pestaña **Configurar** y, a continuación, en **Proveedores de almacenamiento**.

- 3 En la lista, seleccione el proveedor de almacenamiento con el que desea sincronizarse y haga clic en el icono **Rescan the storage provider** (Volver a examinar proveedor de almacenamiento).

Resultados

vSphere Web Client actualiza los datos de almacenamiento del proveedor.

`vmkfstools` es uno de los comandos de ESXi Shell para administrar volúmenes VMFS y discos virtuales. Es posible realizar muchas operaciones de almacenamiento con el comando `vmkfstools`. Por ejemplo, puede crear y administrar almacenes de datos de VMFS en una partición física, o manipular archivos de disco virtual, almacenados en almacenes de datos de NFS o VMFS.

Nota Después de hacer un cambio con `vmkfstools`, es posible que vSphere Web Client no se actualice inmediatamente. Se debe utilizar una operación para actualizar o volver a examinar desde el cliente.

Para obtener más información sobre ESXi Shell, consulte *Introducción a vSphere Command-Line Interface*.

Este capítulo incluye los siguientes temas:

- [Sintaxis del comando vmkfstools](#)
- [Opciones de vmkfstools](#)

Sintaxis del comando vmkfstools

Por lo general, no debe iniciar sesión como usuario raíz para ejecutar los comandos `vmkfstools`. Sin embargo, algunos comandos, como los comandos del sistema de archivos, pueden requerir un inicio de sesión con el usuario raíz.

El comando `vmkfstools` admite la siguiente sintaxis de comandos:

`vmkfstools conn_options options target.`

El destino especifica una partición, un dispositivo o una ruta de acceso donde aplicar la opción de comando.

Tabla 26-1. Argumentos del comando `vmkfstools`

Argumento	Descripción
opciones	<p>Una o varias opciones de la línea de comandos y los argumentos asociados que usa para especificar la actividad para que <code>vmkfstools</code> realice, por ejemplo, la selección del formato de disco al crear un nuevo disco virtual.</p> <p>Después de introducir la opción, especifique el destino en el cual se realizará la operación. El destino puede indicar una partición, un dispositivo o una ruta de acceso.</p>
partition	<p>Especifica particiones de discos. Este argumento usa un formato <code>disk_ID:P</code>, donde <code>disk_ID</code> es el identificador del dispositivo que arroja la matriz de almacenamiento, y <code>P</code> es un número entero que representa el número de partición. El dígito de la partición debe ser mayor que (0) y debe corresponder a una partición VMFS válida.</p>
device	<p>Especifica dispositivos o volúmenes lógicos. Este argumento utiliza una ruta de acceso en el sistema de archivos del dispositivo ESXi. El nombre de la ruta de acceso comienza con <code>/vmfs/devices</code>, que es el punto de montaje del sistema de archivos del dispositivo.</p> <p>Use los siguientes formatos al especificar diferentes tipos de dispositivos:</p> <ul style="list-style-type: none"> ■ <code>/vmfs/devices/disks</code> para discos locales o basados en SAN. ■ <code>/vmfs/devices/lvm</code> para volúmenes lógicos de ESXi. ■ <code>/vmfs/devices/generic</code> para dispositivos SCSI genéricos.
path	<p>Especifica un sistema de archivos o archivo VMFS. Este argumento es una ruta de acceso absoluta o relativa que nombra a un vínculo simbólico de directorio, una asignación de dispositivo sin formato o un archivo en <code>/vmfs</code>.</p> <ul style="list-style-type: none"> ■ Para especificar un sistema de archivos VMFS, use este formato: <div data-bbox="646 1123 1042 1152" data-label="Text"> <pre>/vmfs/volumes/file_system_UUID</pre> </div> <p>o</p> <div data-bbox="646 1245 1053 1274" data-label="Text"> <pre>/vmfs/volumes/file_system_label</pre> </div> ■ Para especificar un archivo en un almacén de datos de VMFS, use este formato: <div data-bbox="646 1388 1366 1442" data-label="Text"> <pre>/vmfs/volumes/file_system_label file_system_UUID/[dir]/myDisk.vmdk</pre> </div> <p>No es necesario introducir la ruta de acceso completa si el directorio de trabajo actual es el directorio principal de <code>myDisk.vmdk</code>.</p>

Opciones de `vmkfstools`

El comando `vmkfstools` tiene varias opciones. Algunas de las opciones se recomiendan solo para usuarios avanzados.

Las formas largas y de letras únicas de las opciones son equivalentes. Por ejemplo, los siguientes comandos son idénticos.

```
vmkfstools --createfs vmfs5 --blocksize 1m disk_ID:P
vmkfstools -C vmfs5 -b 1m disk_ID:P
```

Subopción -v

La subopción `-v` indica el nivel de detalle del resultado del comando.

El formato de esta subopción es el siguiente:

```
-v --verbose number
```

Especifica el valor *number* como un valor entero de 1 a 10.

Puede especificar la subopción `-v` con cualquier opción `vmkfstools`. Si el resultado de la opción no es adecuado para su uso con la subopción `-v`, `vmkfstools` ignora `-v`.

Nota Dado que puede incluir la subopción `-v` en cualquier línea de comando `vmkfstools`, `-v` no se incluye como una subopción en las descripciones de las opciones.

Opciones del sistema de archivos

Las opciones del sistema de archivos permiten crear y administrar almacenes de datos de VMFS. Estas opciones no se aplican a NFS. Puede realizar varias de estas tareas a través de vSphere Web Client.

Mostrar atributos de un volumen VMFS

Utilice el comando `vmkfstools` para enumerar los atributos de un volumen VMFS.

```
-P --queryfs
    -h --humanreadable
```

Cuando utiliza esta opción en cualquier archivo o directorio que resida en un volumen VMFS, la opción enumerará los atributos del volumen especificado. Entre los atributos enumerados, se encuentran la etiqueta del sistema de archivos (si existe), la cantidad de extensiones que comprende el volumen VMFS especificado, el UUID y un listado de los nombres de los dispositivos donde reside cada extensión.

Nota Si cualquier dispositivo que respalda el sistema de archivos VMFS se queda sin conexión, la cantidad de extensiones y de espacio disponible cambiará de manera acorde.

Puede especificar la subopción `-h` con la opción `-P`. Si lo hace, `vmkfstools` enumerará la capacidad del volumen de manera más legible, por ejemplo, 5k, 12.1M o 2.1G.

Crear un almacén de datos de VMFS

Utilice el comando `vmkfstools` para crear un almacén de datos de VMFS.

```
-C --createfs [vmfs5]
-S --setfsname datastore
```

Esta opción crea un almacén de datos de VMFS5 en la partición de SCSI especificada, por ejemplo, `disk_ID:P`. La partición se convierte en la partición principal del sistema de archivos.

Nota No puede crear un nuevo almacén de datos de VMFS3, pero puede utilizar los existentes. Actualice sus almacenes de datos de VMFS3 a VMFS5.

Puede especificar las siguientes subopciones con la opción `-c`:

- `-S --setfsname`: define la etiqueta de volumen en el almacén de datos de VMFS creado. Utilice esta subopción solo junto con la opción `-c`. La etiqueta que especifica puede tener un máximo de 128 caracteres y no puede contener ningún espacio en blanco al principio o al final.

Nota vCenter Server admite un límite de 80 caracteres para todas sus entidades. Si el nombre de un almacén de datos supera ese límite, el nombre se acorta cuando se agrega este almacén de datos a vCenter Server.

Después de definir una etiqueta de volumen puede utilizarla siempre que especifique el almacén de datos de VMFS para el comando `vmkfstools`. La etiqueta de volumen aparece en listados generados por el comando `ls -l` y como vínculo simbólico al volumen de VMFS en el directorio `/vmfs/volumes`.

Para cambiar la etiqueta de volumen de VMFS, utilice el comando `ln -sf`. Utilice lo siguiente como ejemplo:

```
ln -sf /vmfs/volumes/UUID /vmfs/volumes/datastore
```

datastore es la nueva etiqueta de volumen que se utilizará para el VMFS del *UUID*.

Nota Si el host está registrado en vCenter Server, vCenter Server sobrescribirá todos los cambios que realice a la etiqueta de volumen de VMFS. Esto garantiza que la etiqueta de VMFS sea coherente en todos los hosts de vCenter Server.

Ejemplo de creación de un sistema de archivos VMFS

Este ejemplo ilustra la creación de un almacén de datos VMFS5 con el nombre `my_vmfs` en la partición `naa.ID:1`. El tamaño del bloque de archivos es de 1 MB.

```
vmkfstools -C vmfs5 -S my_vmfs /vmfs/devices/disks/naa.ID:1
```

Extender un volumen VMFS actual

Use el comando `vmkfstools` para agregar una extensión a un volumen VMFS.

```
-Z --spanfs span_partitionhead_partition
```

Esta opción amplía el sistema de archivos VMFS con la partición principal especificada al expandirlo por toda la partición especificada por *span_partition*. Debe especificar el nombre de ruta de acceso completo, por ejemplo `/vmfs/devices/disks/disk_ID:1`. Cada vez que se utiliza esta opción, se amplía un volumen VMFS con una nueva extensión para que el volumen se expanda en varias particiones.

Precaución Cuando se ejecuta esta opción, se pierden todos los datos que existían previamente en el dispositivo SCSI que se especificó en *span_partition*.

Ejemplo para extender un volumen de VMFS

En este ejemplo, se extiende el sistema de archivos lógico al permitir su expansión a una partición nueva.

```
vmkfstools -Z /vmfs/devices/disks/naa.disk_ID_2:1 /vmfs/devices/disks/naa.disk_ID_1:1
```

El sistema de archivos extendido abarca dos particiones: `naa.disk_ID_1:1` y `naa.disk_ID_2:1`. En este ejemplo, `naa.disk_ID_1:1` es el nombre de la partición principal.

Aumentar el tamaño de una extensión existente

En lugar de agregar una extensión nueva a un almacén de datos de VMFS, se puede aumentar el tamaño de una extensión existente con el comando `vmkfstools -G`.

Use la siguiente opción para aumentar el tamaño de un almacén de datos de VMFS cuando la capacidad del almacenamiento subyacente haya aumentado.

```
-G --growfs devicedevice
```

Esta opción aumenta el tamaño de un almacén de datos de VMFS existente o su extensión. Por ejemplo,

```
vmkfstools --growfs /vmfs/devices/disks/disk_ID:1 /vmfs/devices/disks/disk_ID:1
```

Actualizar un almacén de datos de VMFS

Si usa un almacén de datos VMFS3, debe actualizarlo a VMFS5.

Precaución La actualización es un proceso unidireccional. Una vez que haya convertido un almacén de datos VMFS3 a VMFS5, no podrá revertirlo.

Cuando actualice el almacén de datos, use el comando siguiente: `vmkfstools -T|--upgradelvms /vmfs/volumes/UUID`

Nota Todos los hosts que acceden al almacén de datos deben admitir VMFS5. Si cualquier host ESX/ESXi versión 4.x o anterior usa el almacén de datos VMFS3, se producirá un error en la actualización y se mostrará la dirección Mac del host que utiliza el almacén de datos activamente.

Opciones de discos virtuales

Las opciones de discos virtuales permiten configurar, migrar y administrar discos virtuales almacenados en sistemas de archivos VMFS y NFS. También se pueden realizar la mayoría de estas tareas mediante vSphere Web Client.

Formatos de disco compatibles

Cuando se crea o clona un disco virtual, se puede utilizar la subopción `-d --diskformat` para especificar el formato del disco.

Elija entre los formatos siguientes:

- `zeroedthick` (predeterminado): el espacio necesario para el disco virtual se asigna durante la creación. Los datos que quedan en el dispositivo físico no se borran durante la creación, sino que se ponen a cero a petición más adelante, en la primera escritura de la máquina virtual. La máquina virtual no lee los datos obsoletos del disco.
- `eagerzeroedthick`: el espacio necesario para el disco virtual se asigna en el momento de la creación. En contraposición con el formato `zeroedthick`, los datos que quedan en el dispositivo físico se ponen a cero durante la creación. Es posible que la creación de discos en este formato demore mucho más que la creación de otros tipos de discos.
- `thin`: disco virtual de aprovisionamiento fino. A diferencia del formato `thick`, el espacio requerido para el disco virtual no se asigna durante la creación, pero se proporciona, puesto a cero, a pedido posteriormente.
- `rdm: device`: asignación de disco sin formato de modo de compatibilidad virtual.
- `rdmp: device`: asignación de disco sin formato (de transmisión) de modo de compatibilidad física.
- `2gbsparse`: un disco disperso con tamaño de extensión máximo de 2 GB. Se pueden utilizar discos en este formato con productos VMware en host, como VMware Fusion, Player, Server o Workstation. Sin embargo, no se puede encender un disco disperso en un host ESXi a menos que primero se vuelva a importar el disco con `vmkfstools` en un formato compatible, como `thick` o `thin`.

Consulte [Migrar máquinas virtuales entre distintos productos de VMware](#).

Formatos de disco NFS

Los únicos formatos de disco que se pueden utilizar para NFS son `thin`, `thick`, `zeroedthick` y `2gbsparse`.

Los formatos `Thick`, `zeroedthick` y `thin`, por lo general, se comportan igual dado que el servidor NFS, y no el host ESXi, determina la directiva de asignación. La directiva de asignación predeterminada en la mayoría de los servidores NFS es `thin`. Sin embargo, en los servidores NFS que admiten Storage APIs - Array Integration, se pueden crear discos virtuales en formato `zeroedthick`. La operación de reserva de espacio habilita los servidores NFS para asignar y garantizar espacio.

Para obtener más información sobre las API de integración de matrices, consulte [Capítulo 23 Aceleración de hardware de almacenamiento](#).

Crear un disco virtual

Utilice el comando `vmkfstools` para crear un disco virtual.

```
-c --createvirtualdisk size[kK|mM|gG]
-a --adaportype [buslogic|lsilogic|ide|lsisas|pvscsi] srcfile
-d --diskformat [thin|zeroedthick|eagerzeroedthick]
-W --objecttype [file|vsan|vvol]
--policyFile fileName
```

Esta opción crea un disco virtual en la ruta de acceso especificada en un almacén de datos. Especifique el tamaño del disco virtual. Al introducir el valor de *size*, puede indicar el tipo de unidad agregando el sufijo `k` (kilobytes), `m` (megabytes) o `g` (gigabytes). El tipo de unidad no distingue entre mayúsculas y minúsculas. `vmkfstools` interpreta `k` o `K` como kilobytes. Si no se especifica un tipo de unidad, `vmkfstools` toma los bytes como valor predeterminado.

Es posible especificar las siguientes subopciones con la opción `-c`.

- `-a` especifica la controladora que utiliza una máquina virtual para comunicarse con los discos virtuales. Las opciones disponibles son BusLogic, LSI Logic, IDE, LSI Logic SAS y VMware Paravirtual SCSI.
- `-d` especifica los formatos de disco.
- `-W` especifica si el disco virtual es un archivo de un almacén de datos de VMFS o NFS, o bien un objeto de un almacén de datos de Virtual SAN o Virtual Volumes.
- `--policyFile fileName` especifica la directiva de almacenamiento de máquina virtual del disco.

Ejemplo para crear un disco virtual

En este ejemplo se ilustra la creación de un archivo de disco virtual de dos gigabytes llamado `rh6.2.vmdk` en el sistema de archivos VMFS llamado `myVMFS`. Este archivo representa un disco virtual vacío al que pueden acceder las máquinas virtuales.

```
vmkfstools -c 2048m /vmfs/volumes/myVMFS/rh6.2.vmdk
```


Inicializar un disco virtual

Use el comando `vmkfstools` para inicializar un disco virtual.

```
-w --writezeros
```

Esta opción limpia el disco virtual sobrescribiendo con ceros todos sus datos. Según el tamaño del disco virtual y el ancho de banda de E/S del dispositivo que aloja el disco virtual, es posible que la ejecución de este comando tarde mucho tiempo.

Precaución Si usa este comando, perderá todos los datos que tenga el disco virtual.

Expandir un disco virtual fino

Utilice el comando `vmkfstools` para expandir un disco virtual fino.

```
-j --inflatedisk
```

Esta opción convierte un disco virtual `thin` en un disco `eagerzeroedthick`, y conserva todos los datos existentes. Esta opción asigna y llena con ceros todos los bloques que aún no están asignados.

Quitar bloques puestos a cero

Utilice el comando `vmkfstools` para convertir cualquier disco virtual fino, disco virtual grueso con algunos bloques puestos a cero o disco virtual grueso con todos los bloques puestos a cero a un disco fino sin bloques puestos a cero.

```
-K --punchzero
```

Esta opción desasigna todos los bloques puestos a cero y deja solo aquellos asignados previamente y con datos válidos. El disco virtual resultante tiene formato fino.

Convertir un disco virtual grueso con algunos bloques puestos a cero a un disco virtual grueso con todos los bloques puestos a cero

Use el comando `vmkfstools` para convertir todos los discos virtuales gruesos con algunos bloques puestos a cero a discos gruesos con todos los bloques puestos a cero.

```
-k --eagerzero
```

Al realizar esta conversión, esta opción preserva todos los datos presentes en el disco virtual.

Eliminar un disco virtual

Esta opción elimina un archivo de disco virtual en la ruta de acceso especificada en el volumen VMFS.

```
-U --deletevirtualdisk
```

Cambiar nombre de un disco virtual

Esta opción asigna un nuevo nombre a un archivo de disco virtual en la ruta de acceso especificada en el volumen VMFS.

Debe especificar el nombre del archivo o la ruta de acceso del archivo original *oldName* y el nombre del archivo o la ruta de acceso del archivo nuevo *newName*.

```
-E --renamevirtualdisk oldName newName
```

Clonar convertir un disco virtual o un RDM

Use el comando `vmkfstools` para crear una copia de un disco virtual o un disco sin formato que especifique.

Un usuario no raíz no tiene permitido clonar un disco virtual o un RDM. Debe especificar el nombre del archivo o la ruta de acceso del archivo original *oldName* y el nombre del archivo o la ruta de acceso del archivo nuevo *newName*.

```
-i|--clonevirtualdisk oldName newName
-d|--diskformat [thin|zeroedthick|eagerzeroedthick|rdm:device|rdmp:device]
-W|--objecttype [file|vsan|vvol]
--policyFile fileName
-N|--avoidnativeclone
```

Use las siguientes subopciones si desea cambiar los parámetros correspondientes para la copia que va a crear.

- `-d|--diskformat` especifica los formatos de disco.
- `-W|--objecttype` especifica si el disco virtual es un archivo de un almacén de datos de VMFS o NFS, o bien un objeto de un almacén de datos de Virtual SAN o Virtual Volumes.
- `--policyFile fileName` especifica la directiva de almacenamiento de máquina virtual para el disco.

De manera predeterminada, ESXi usa sus métodos nativos para realizar las operaciones de clonación. Si la matriz admite las tecnologías de clonación, puede descargar las operaciones para la matriz. Especifique la opción `-N|--avoidnativeclone` para evitar la clonación nativa de ESXi.

Ejemplo: Ejemplo de clonación o conversión de un disco virtual

En este ejemplo, se ilustra la clonación de contenido de un disco virtual oro del repositorio `templates` a un archivo de disco virtual llamado `myOS.vmdk` en el sistema de archivos `myVMFS`.

```
vmkfstools -i /vmfs/volumes/myVMFS/templates/gold.vmdk /vmfs/volumes/myVMFS/myOS.vmdk
```

Es posible configurar una máquina virtual para que utilice este disco virtual agregando líneas al archivo de configuración de la máquina virtual, como se muestra en el siguiente ejemplo:

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/myOS.vmdk
```

Si quiere convertir el formato del disco, use la subopción `-d|--diskformat`.

Esta subopción resulta útil cuando importa discos virtuales en un formato que no es compatible con ESXi, por ejemplo, el formato 2gbparse. Después de convertir el disco, puede asociarlo a una nueva máquina virtual que cree en ESXi.

Por ejemplo:

```
vmkfstools -i /vmfs/volumes/myVMFS/templates/gold.vmdk /vmfs/volumes/myVMFS/myOS.vmdk -d thin
```

Migrar máquinas virtuales entre distintos productos de VMware

Por lo general, utiliza VMware Converter para migrar máquinas virtuales desde otros productos de VMware al sistema ESXi. Sin embargo, puede utilizar el comando `vmkfstools -i` para importar discos virtuales con formato 2gbparse a ESXi y, a continuación, conectar este disco a una máquina virtual nueva que cree en ESXi.

Debe importar primero el disco virtual porque no puede encender discos con formato 2gbparse en el host ESXi.

Procedimiento

- 1 Importe un disco con formato 2gbparse al host ESXi con el comando siguiente. Asegúrese de seleccionar el formato de disco compatible con ESXi.

```
vmkfstools -i <input> <output> -d <format>
```

- 2 Utilice vSphere Web Client para conectar el disco que importó a la máquina virtual en ESXi.

Para obtener información, consulte *Administración de máquinas virtuales de vSphere*.

Extender un disco virtual

Esta opción amplía el tamaño de un disco asignado a una máquina virtual una vez creada la máquina virtual.

```
-X --extendvirtualdisk newSize [kK|mM|gG]
```

Debe apagar la máquina virtual que usa este archivo de disco antes de escribir este comando. Es posible que deba actualizar el sistema de archivos en el disco para que el sistema operativo invitado pueda reconocer y utilizar el tamaño nuevo del disco y aprovechar el espacio adicional.

Nota No puede ampliar en caliente los discos SATA virtuales o cualquier disco virtual si la capacidad después de la ampliación es igual o superior a 2 TB.

Especifica el parámetro `newSize` en kilobytes, megabytes o gigabytes agregando los sufijos `k` (kilobytes), `m` (megabytes) o `g` (gigabytes). El tipo de unidad no distingue entre mayúsculas y minúsculas. `vmkfstools` interpreta `k` o `K` como kilobytes. Si no se especifica un tipo de unidad, `vmkfstools` toma los kilobytes como valor predeterminado.

El parámetro `newSize` define el tamaño nuevo completo, no solo el incremento que se agrega al disco.

Por ejemplo, para ampliar un disco virtual de 4 g con 1 g, escriba: `vmkfstools -X 5g disk name`.

Puede ampliar el disco virtual al formato grueso con todos los bloques puestos a cero con la opción `-d eagerzeroedthick`.

Nota No amplíe el disco base de una máquina virtual con instantáneas asociadas. Si lo hace, ya no podrá confirmar la instantánea ni revertir el disco base al tamaño original.

Actualizar discos virtuales

Esta opción convierte el archivo de disco virtual especificado del formato de ESX Server 2 al formato de ESXi.

```
-M --migratevirtualdisk
```

Crear un modo de compatibilidad virtual con asignación de dispositivos sin formato

Esta opción crea un archivo de asignación de dispositivos sin formato (RDM) en un volumen VMFS y asigna un LUN sin formato a este archivo. Una vez establecida esta asignación, se puede acceder al LUN del mismo modo que se accede a un disco virtual VMFS normal. La longitud de archivo de la asignación es igual al tamaño del LUN sin formato al que se apunta.

```
-r --createrdm device
```

Cuando especifique el parámetro *device*, utilice el siguiente formato:

```
/vmfs/devices/disks/disk_ID:P
```

Ejemplo para crear un RDM de modo de compatibilidad virtual

En este ejemplo, se crea un archivo RDM denominado *my_rdm.vmdk* y se asigna el disco sin formato *disk_ID* a ese archivo.

```
vmkfstools -r /vmfs/devices/disks/disk_ID my_rdm.vmdk
```

Para configurar la máquina virtual para que utilice el archivo de asignación *my_rdm.vmdk*, agregue las líneas siguientes al archivo de configuración de la máquina virtual:

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/my_rdm.vmdk
```

Crear una asignación de dispositivo sin formato de modo de compatibilidad física

Esta opción permite asignar un dispositivo sin formato de acceso directo a un archivo en un volumen VMFS. Esta asignación permite a una máquina virtual omitir el filtrado del comando SCSI de ESXi cuando accede al disco virtual. Este tipo de asignación resulta útil cuando la

máquina virtual debe enviar comandos SCSI de propiedad, por ejemplo, cuando software con reconocimiento de SAN se ejecuta en la máquina virtual.

```
-z --createrdmpassthru device
```

Una vez que se establece este tipo de asignación, se la puede utilizar para acceder al disco sin formato del mismo modo que a cualquier otro disco virtual VMFS.

Cuando especifique el parámetro *device*, utilice el siguiente formato:

```
/vmfs/devices/disks/disk_ID
```

Mostrar atributos de un RDM

Esta opción permite enumerar los atributos de una asignación de discos sin formato.

```
-q --queryrdm
```

Esta opción imprime el nombre del RDM del disco sin formato. La opción también imprime otra información de identificación, como el identificador de disco, del disco sin formato.

Mostrar la geometría del disco virtual

Esta opción obtiene información sobre la geometría del disco virtual.

```
-g --geometry
```

La salida adopta la siguiente forma: `Geometry information C/H/S`, donde *c* representa la cantidad de cilindros, *H* representa la cantidad de cabezales y *s* representa la cantidad de sectores.

Nota Cuando se importan discos virtuales de los productos VMware alojados en el host ESXi, es posible que aparezca un mensaje de error de falta de coincidencia con la geometría del disco. Una falta de coincidencia con la geometría del disco también puede ser la causa de problemas para cargar un sistema operativo invitado o ejecutar una máquina virtual recientemente creada.

Comprobar y reparar discos virtuales

Utilice esta opción para comprobar o reparar un disco virtual en caso de producirse un apagado incorrecto.

```
-x , --fix [check|repair]
```

Comprobar la consistencia de la cadena de discos

Con esta opción, puede comprobar la cadena de discos completa. Puede determinar si alguno de los eslabones de la cadena está corrupto o si existe alguna relación de elementos primarios y secundarios no válida.

```
-e --chainConsistent
```

Opciones de dispositivos de almacenamiento

Las opciones de dispositivos permiten realizar una tarea administrativa para dispositivos de almacenamiento físico.

Administrar reservas de SCSI de LUN

La opción `-L` permite reservar un LUN de SCSI para utilización exclusiva del host ESXi, libera una reserva para que los otros hosts puedan acceder al LUN y restablece una reserva forzando la liberación de todas las reservas del destino.

```
-L --lock [reserve|release|lunreset|targetreset|busreset] device
```

Precaución Utilizar la opción `-L` puede interrumpir las operaciones de otros servidores en una SAN. Utilice esta opción `-L` solo durante la solución de problemas de configuración de agrupación en clústeres.

A menos que VMware lo recomiende específicamente, jamás utilice esta opción en un LUN que aloje un volumen VMFS.

Puede especificar la opción `-L` de varias maneras:

- `-L reserve`: reserva el LUN especificado. Después de la reserva, solo el servidor que reservó ese LUN puede acceder a él. Si otros servidores intentan acceder a ese LUN, se produce un error de reserva.
- `-L release`: libera la reserva en el LUN especificado. Otros servidores pueden volver a acceder al LUN.
- `-L lunreset`: restablece el LUN especificado borrando todas las reservas en el LUN y permitiendo que vuelva a estar disponible para todos los servidores. Esto no afecta a ningún otro LUN del dispositivo. Si otro LUN del dispositivo está reservado, lo seguirá estando.
- `-L targetreset`: restablece todo el destino. Esta acción borra todas las reservas en todos los LUN asociados con ese destino y hace que los LUN vuelvan a estar disponibles para todos los servidores.
- `-L busreset`: restablece todos los destinos accesibles en el bus. Esta acción borra todas las reservas en los LUN accesibles a través del bus y hace que vuelvan a estar disponibles para todos los servidores.

Al introducir el parámetro *device*, utilice el siguiente formato:

```
/vmfs/devices/disks/disk_ID:P
```

Romper el bloqueo de dispositivos

La opción `-B` permite romper por la fuerza el bloqueo de un dispositivo en una determinada partición.

```
-B --breaklock device
```

Al introducir el parámetro *device*, utilice el siguiente formato:

```
/vmfs/devices/disks/disk_ID:P
```

Puede utilizar este comando cuando un host genera errores en el medio de una operación del almacén de datos, por ejemplo, aumentar una extensión, agregar una extensión o volver a firmar. Al emitir este comando, asegúrese de que ningún otro host mantiene el bloqueo.