Dell EMC Data Domain® Operating System

Versión 6.2

Guía de administración

302-005-407
REV. 01

DELL EMC

Copyright © 2010-2018 Dell Inc. o sus filiales Todos los derechos reservados.

Publicado en Diciembre de 2018

Dell considera que la información de este documento es precisa en el momento de su publicación. La información está sujeta a cambios sin previo aviso.

LA INFORMACIÓN DE ESTA PUBLICACIÓN SE PROPORCIONA “TAL CUAL”. DELL NO SE HACE RESPONSABLE NI OFRECE GARANTÍA DE NINGÚN TIPO CON RESPECTO A LA INFORMACIÓN DE ESTA PUBLICACIÓN Y, ESPECÍFICAMENTE, RENUNCIA A TODA GARANTÍA IMPLÍCITA DE COMERCIABILIDAD O CAPACIDAD PARA UN PROPÓSITO DETERMINADO. EL USO, LA COPIA Y LA DISTRIBUCIÓN DE CUALQUIER SOFTWARE DE DELL DESCRITO EN ESTA PUBLICACIÓN REQUIEREN LA LICENCIA DE SOFTWARE CORRESPONDIENTE.

Dell, EMC y otras marcas comerciales pertenecen a Dell Inc. o sus filiales. Las demás marcas comerciales pueden ser propiedad de sus respectivos dueños. Publicado en México.

Dirección local de EMC
EMC Argentina (Cono Sur) Tel. +54-11-4021-3622 http://www.emc.com/es-ar/index.htm
EMC México Tel. +52-55-5080-3700 http://www.emc.com/es-mx/index.htm
EMC Venezuela (Norte de Latinoamérica) Tel. +58-212-206-6911 http://www.emc.com/es-ve/index.htm

CONTENIDO

Prefacio **17**

Capítulo 1 **Integración y funciones del sistema Data Domain** **21**
Historial de revisiones....22
Descripción general del sistema Data Domain....22
Funciones del sistema Data Domain....22
Integridad de los datos....23
Deduplicación de datos....24
Operaciones de restauración....24
Data Domain Replicator....24
Balanceo de carga y múltiples rutas....25
Alta disponibilidad....25
Manejo de I/O aleatorias....27
Acceso de administrador del sistema....28
Funciones con licencia....28
Integración de ambientes de almacenamiento....30

Capítulo 2 **Introducción** **33**
Descripción general de Dell EMC Data Domain System Manager....34
Inicio y cierre de sesión de DD System Manager....35
Inicio de sesión con un certificado....37
Interfaz de DD System Manager....38
Elementos de la página....38
Anuncio....38
Panel de navegación....39
Panel de información....39
Pie de página....40
Botones de ayuda....40
Acuerdo de licencia para el usuario final....40
Configuración del sistema con el asistente de configuración....40
Página License....41
Red....41
Sistema de archivos....44
Configuración del sistema....48
Protocolo de DD Boost....50
Protocolo CIFS....51
Protocolo NFS....52
Protocolo de DD VTL....53
Interfaz de la línea de comandos de Data Domain....54
Inicio de sesión en la CLI....55
Reglas de ayuda en línea de la CLI....56

Capítulo 3 **Administración de sistemas Data Domain** **57**
Descripción general de administración del sistema....58
Descripción general de la administración del sistema de alta disponibilidad....58
Mantenimiento planificado del sistema de alta disponibilidad....59
Reinicio de un sistema....59

Encendido o apagado de un sistema 59
Encendido del sistema..... 60
Administración de actualizaciones del sistema..... 61
Descripción general y listas de verificación previas a la actualización 62
Visualización de paquetes de actualización en el sistema..... 67
Obtención y verificación de paquetes de actualización..... 68
Actualización de un sistema Data Domain..... 69
Eliminación de un paquete de actualización..... 71
Administración de licencias electrónicas..... 71
Administración de licencias de sistemas de alta disponibilidad..... 72
Administración de almacenamiento del sistema..... 72
Visualización de información de almacenamiento del sistema..... 73
Ubicación física de un gabinete..... 78
Ubicación física de un disco..... 78
Configurar el almacenamiento..... 79
Expansión de capacidad de DD3300..... 80
Discos en estado fallido y discos que estaban en estado fallido y se pasaron a estado normal..... 81
Administración de conexiones de red..... 81
Administración de conexiones de red de sistemas de alta disponibilidad..... 82
Administración de interfaces de redes..... 82
Administración de configuración general de red..... 98
Administración de rutas de redes..... 102
Administración de contraseñas del sistema..... 105
Configuración de la contraseña del sistema..... 105
Cambio de la contraseña del sistema..... 106
Administración de acceso al sistema..... 106
Control de acceso basado en funciones..... 107
Administración de acceso para protocolos IP..... 109
Administración de la cuenta de usuario local..... 116
Administración de usuarios y grupos de directorio..... 124
Diagnóstico de problemas de autenticación..... 139
Cambio del método de autenticación del sistema..... 140
Configuración de ajustes del servidor de correo..... 141
Administración de configuración de fecha y hora..... 142
Administración de propiedades del sistema..... 143
Administración de SNMP..... 143
Visualización del estado y la configuración de SNMP..... 144
Activación y desactivación de SNMP..... 145
Descarga de SNMP MIB..... 145
Configuración de las propiedades de SNMP..... 146
Administración de usuarios SNMP V3..... 146
Administración de comunidades SNMP V2C..... 148
Administración de hosts de SNMP trap..... 150
Administración de informes de soporte automático..... 152
Capacidad de administración de paquetes de soporte y soporte automático de sistemas de alta disponibilidad..... 152
Habilitación y deshabilitación de la creación de informes de soporte automático para Data Domain..... 153
Revisión de informes de soporte automático generados..... 153
Configuración de la lista de distribución de correo de soporte automático..... 153
Verificar si Data Domain puede enviar correos electrónicos de ASUP y alertas a los destinatarios externos..... 154

Administración de paquetes de soporte....156
Generación de un paquete de soporte....156
Visualización de la lista de paquetes de soporte....156
Administración de coredump....157
Administración de notificación de alerta....158
Administración de notificación de alerta de sistemas de alta disponibilidad....158
Visualización de la lista de grupos de notificación....159
Creación de un grupo de notificación....160
Administrar la lista de suscriptores para un grupo....161
Modificación de un grupo de notificación....162
Eliminación de un grupo de notificación....163
Restablecimiento de la configuración del grupo de notificación....163
Configuración del calendario de resumen diario y la lista de distribución....163
Habilitación y deshabilitación de las notificaciones de alerta a Data Domain....165
Pruebas de la función de correo electrónico de alertas....165
Administración de la entrega de servicio de soporte....166
Selección de entrega de correo electrónico estándar a Data Domain....166
Selección y configuración de entrega de Secure Remote Services....166
Pruebas de funcionamiento de ConnectEMC....167
Administración de archivos de registro....167
Visualización de archivos de registro en DD System Manager....169
Visualización de un archivo de registro en la CLI....169
Más información acerca de los mensajes de registro....170
Guardado de una copia de archivos de registro....171
Transmisión de mensajes de registro a sistemas remotos....171
Administración de la alimentación de sistemas remotos con IPMI....173
Limitaciones de IPMI y SOL....174
Cómo agregar o eliminar usuarios de IPMI con DD System Manager....174
Cambio de la contraseña de un usuario de IPMI....175
Configuración de un puerto IPMI....175
Preparación para la administración remota de la alimentación y el monitoreo de la consola con la CLI....176
Administración de la alimentación con DD System Manager....178
Administración de alimentación con la CLI....179

Capítulo 4 Monitoreo de sistemas Data Domain 181

Visualización del estado del sistema en forma individual y la información de identidad....182
Área Dashboard Alerts....182
Área Dashboard File System....183
Área Dashboard Services....183
Área de preparación de alta disponibilidad de tablero....184
Área Dashboard Hardware....184
Área Maintenance System....184
Panel de alertas de estado....185
Visualización y borrado de alertas actuales....185
Pestaña de Current Alerts....186
Visualización del historial de alertas....187
Pestaña de Alerts History....187

Visualización del estado de los componentes de hardware..... 188
Estado del ventilador..... 188
Estado de la temperatura..... 189
Estado del panel Management..... 190
Estado del disco SSD (solo DD6300)..... 190
Estado de la fuente de alimentación..... 190
Estado del slot de PCI..... 190
Estado de NVRAM..... 190
Visualización de estadísticas del sistema..... 191
Gráfico de estadísticas del rendimiento..... 192
Visualización de usuarios activos..... 193
Administración de informe del historial..... 193
Tipos de informes..... 194
Visualización del registro de tareas..... 198
Visualización del estado de alta disponibilidad del sistema..... 199
Estado de alta disponibilidad..... 199

Capítulo 5 Sistema de archivos 203
Descripción general del sistema de archivos..... 204
Cómo almacena datos el sistema de archivos..... 204
Cómo el sistema de archivos informa sobre el uso del espacio..... 204
Cómo usa la compresión el sistema de archivos 205
Cómo el sistema de archivos implementa la integridad de los datos... 206
Cómo el sistema de archivos recupera el espacio de almacenamiento mediante la limpieza del sistema de archivos..... 207
Interfaces compatibles 208
Software de respaldo compatible..... 208
Flujos de datos enviados a un sistema Data Domain 208
Limitaciones del sistema de archivos..... 211
Monitoreo del uso del sistema de archivos..... 212
Acceso a la vista del sistema de archivos..... 212
Administración de las operaciones del sistema de archivos..... 221
Ejecución de operaciones básicas..... 221
Ejecución de la limpieza..... 223
Ejecutar saneamiento..... 226
Modificación de la configuración básica..... 228
Operaciones de copia rápida..... 230
Ejecución de una operación de copia rápida..... 230

Capítulo 6 MTree 233
Descripción general de MTrees..... 234
Límites de MTrees..... 234
Cuotas..... 235
Acerca del panel de MTree..... 235
Acerca de la vista resumida..... 236
Acerca de la vista de utilización del espacio (MTrees)..... 240
Acerca de la vista de escritura diaria (MTrees)..... 241
Monitoreo de uso de MTree..... 242
Comprensión de la medición de la capacidad física..... 242
Administración de las operaciones en MTree..... 245
Creación de un MTree..... 246
Configuración y habilitación/deshabilitación de las cuotas de MTree 247

Eliminación de un MTree....248
Restauración de un MTree....248
Cambiar el nombre de un MTree....249

Capítulo 7 Snapshots 251
Descripción general de snapshots....252
Monitoreo de snapshots y sus programas....253
Acerca de la vista de snapshots....253
Administración de snapshots....254
Creación de un snapshot....254
Modificación de la fecha de vencimiento de una snapshot....255
Cambiar el nombre de un snapshot....255
Crear vencimiento para una snapshot....256
Administración de calendarios de instantáneas....256
Creación de calendarios de snapshots....256
Modificación de un calendario de snapshots....257
Eliminación de un calendario de snapshots....258
Recuperar datos desde un snapshots....258

Capítulo 8 CIFS 259
Descripción general de la CIFS....260
Configuración de firmas de SMB....260
Ejecución de configuración de CIFS....261
Sistemas de alta disponibilidad y CIFS....261
Preparación de clientes para acceder a sistemas Data Domain....261
Activación de los servicios CIFS....262
Asignación de nombre al servidor CIFS....262
Configuración de parámetros de autenticación....262
Desactivación de los servicios CIFS....263
Trabajar con recursos compartidos....263
Creación de recursos compartidos en el sistema Data Domain....263
Modificación de un recurso compartido en un sistema Data Domain....266
Creación de un recurso compartido a partir de un recurso compartido existente....267
Desactivación de un recurso compartido en un sistema Data Domain....267
Activación de un recurso compartido en un sistema Data Domain....267
Eliminación de un recurso compartido en un sistema Data Domain....267
Ejecución de la administración de MMC....268
Conexión de un sistema Data Domain desde un cliente CIFS....268
Información de CIFS en pantalla....270
Administración del control de acceso....270
Acceso a recursos compartidos desde un cliente de Windows....270
Proporcionar acceso administrativo a los usuarios de dominio....271
Permiso de acceso administrativo a un sistema Data Domain para usuarios de dominios....271
Restricción del acceso administrativo desde Windows....272
Acceso a archivos....272
Monitoreo de operación de CIFS....275
Visualización del estado de CIFS....275
Configuración de pantalla CIFS....276

Visualización de las estadísticas CIFS..... 278
Ejecución de la solución de problemas de CIFS.....279
Visualización de actividad en curso de clientes..... 279
Configuración del máximo de archivos abiertos para una conexión.... 279
Reloj del sistema Data Domain.....280
Sincronización desde un controlador de dominio de Windows..... 280
Sincronizar desde un servidor NTP..... 281

Capítulo 9 NFS 283
Descripción general de NFS.....284
Sistemas de alta disponibilidad y NFS.....284
Administración del acceso de clientes NFS al sistema Data Domain..... 285
Activación de servicios NFS..... 285
Deshabilitación de servicios NFS..... 285
Creación de una exportación..... 285
Modificación una exportación..... 287
Creación de una exportación a partir de una exportación existente... 288
Eliminación de una exportación.....289
Visualización de la información de NFS.....289
Visualización del estado de NFS..... 289
Visualización de exportaciones de NFS.....289
Visualización de clientes NFS activos..... 290
Integración de un DDR en un dominio Kerberos.....290
Agregar y eliminar servidores KDC después de la configuración inicial.....292

Capítulo 10 NFSv4 295
Introducción a NFSv4.....296
NFSv4 comparado con NFSv3 en sistemas Data Domain.....296
Puertos NFSv4..... 297
Descripción general de mapeos de ID.....297
Formatos externos..... 298
Formatos de identificadores estándar.....298
Identificadores extendidos de ACE..... 298
Formatos alternativos.....298
Formatos de identificadores internos..... 299
Cuando se produce el mapeo de ID.....299
Mapeo de entrada.....299
Mapeo de salida.....300
Mapeo de credenciales..... 300
Interoperabilidad de NFSv4 y CIFS/SMB..... 301
Integración con Active Directory de CIFS/SMB..... 301
DACL predeterminada para NFSv4.....301
SID predeterminados del sistema..... 301
Identificadores comunes en SID y ACL de NFSv4.....302
Referencias de NFS.....302
Ubicaciones de referencia.....302
Nombres de ubicación de referencia.....302
Sistemas de escalamiento horizontal y referencias.....303
NFSv4 y alta disponibilidad.....303
Espacios de nombres globales de NFSv4.....304
Espacios de nombres globales de NFSv4 y submontajes de NFSv3... 304

Configuración de NFSv4.....305
Habilitación del servidor NFSv4.....305
Configuración del servidor predeterminado para incluir NFSv4....305
Actualización de exportaciones existentes.....306
Kerberos y NFSv4.....306
Configuración de Kerberos con un KDC basado en Linux.....307
Configuración del sistema Data Domain para utilizar la autenticación de Kerberos.....308
Configuración de clientes.....309
Habilitación de Active Directory.....309
Configuración de Active Directory.....310
Configuración de clientes en Active Directory.....310

Capítulo 11 Migración de almacenamiento 311
Descripción general de la migración de almacenamiento.....312
Consideraciones de planificación de migración.....313
Consideraciones de la bandeja DS60.....314
Visualización del estado de migración.....314
Evaluación de la preparación para la migración.....315
Migración de almacenamiento mediante DD System Manager.....316
Descripciones de cuadros de diálogo de migración de almacenamiento.....317
Cuadro de diálogo Select a Task.....317
Cuadro de diálogo Select Existing Enclosures.....317
Cuadro de diálogo Select New Enclosures.....317
Cuadro de diálogo Review Migration Plan.....317
Cuadro de diálogo Verify Migration Preconditions.....318
Cuadros de diálogo de progreso de migración.....319
Migración de almacenamiento mediante la CLI.....320
Ejemplo de migración de almacenamiento de CLI.....321

Capítulo 12 Metadatos en flash 327
Descripción general de los metadatos en flash (MDoF).....328
Licencias y capacidad de MDoF.....329
Nivel de caché de disco SSD.....330
Nivel de caché de disco SSD de MDoF: administración del sistema.....330
Administración del nivel de caché de disco SSD.....330
Alertas de discos SSD.....333

Capítulo 13 Destino SCSI 335
Descripción general del destino de SCSI.....336
Vista Fibre Channel.....337
Habilitación de NPIV.....337
Deshabilitación de NPIV.....340
Pestaña Resources.....341
Pestaña Access Groups.....348
Diferencias entre el monitoreo de vínculos de FC entre las versiones de SO de DD.....348

Capítulo 14 Trabajo con DD Boost 351
Acerca de Data Domain Boost.....352
Administración de DD Boost con DD System Manager.....353
Especificación de nombres de usuario de DD Boost.....353
Cambio de contraseñas de usuario de DD Boost.....354

Eliminación de un nombre de usuario de DD Boost....354
Activación de DD Boost....354
Configuración de Kerberos....355
Desactivación de DD Boost....355
Visualización de unidades de almacenamiento de DD Boost....356
Creación de una unidad de almacenamiento....357
Visualización de información de unidades de almacenamiento....358
Modificación de una unidad de almacenamiento....361
Cambio de nombre de una unidad de almacenamiento....362
Eliminación de una unidad de almacenamiento....362
Cómo revertir la eliminación de una unidad de almacenamiento....363
Selección de opciones de DD Boost....363
Administración de certificados para DD Boost....365
Administración de cifrado y acceso de clientes de DD Boost....367
Acerca de los grupos de interfaces....369
Interfaces....370
Clientes....371
Creación de grupos de interfaces....371
Activación y desactivación de grupos de interfaces....372
Modificación del nombre y de las interfaces de un grupo de interfaces....372
Eliminación de un grupo de interfaces....373
Cómo agregar un cliente a un grupo de interfaces....373
Modificación del nombre o del grupo de interfaces de un cliente....374
Eliminación de un cliente del grupo de interfaces....374
Uso de grupos de interfaces para la replicación de archivos administrados (MFR)....375
Destrucción de DD Boost....377
Configuración de DD Boost-over-Fibre Channel....377
Habilitación de usuarios de DD Boost....377
Configuración de DD Boost....378
Verificación de conectividad y creación de grupos de acceso....379
Uso de DD Boost en sistemas de alta disponibilidad....382
Acerca de las pestañas de DD Boost....382
Configuración....382
Conexiones activas....383
Red IP....384
Fibre Channel....384
Unidades de almacenamiento:....384

Capítulo 15 Librería de cintas virtuales DD 387
Descripción general de librerías de cintas virtuales de DD....388
Planificación de una DD VTL....389
Límites de DD VTL....389
Cantidad de unidades admitidas por una DD VTL....392
Códigos de barras de cintas....393
Compatibilidad con unidades de cinta LTO....394
Configuración de una DD VTL....395
Sistemas de alta disponibilidad y DD VTL....395
Transferencia de cintas de DD VTL a la nube....395
Administración de una DD VTL....396
Habilitación de DD VTL....397
Deshabilitación de DD VTL....398
Valores predeterminados de opción de DD VTL....398
Configuración de las opciones predeterminadas de DD VTL....398

Trabajo con librerías..... 400
Creación de librerías..... 400
Eliminación de librerías..... 403
Búsqueda de cintas.....403
Uso de una librería seleccionada..... 404
Creación de cintas..... 404
Eliminación de cintas..... 405
Importación de cintas..... 406
Exportación de cintas..... 408
Transferencia de cintas entre dispositivos dentro de una librería. 409
Cómo agregar slots.....411
Eliminación de slots.....411
Cómo agregar CAP..... 411
Eliminación de CAP..... 412
Visualización de información del convertidor.....412
Trabajo con unidades..... 413
Creación de unidades..... 414
Eliminación de unidades.....414
Trabajo con una unidad seleccionada..... 415
Trabajo con cintas.....415
Cambio del estado de bloqueo de retención o escritura de una cinta 416
Trabajo con el vault..... 417
Trabajar con vault en la nube.....418
Preparación del pool de la VTL para el movimiento de datos..... 418
Quitar cintas del inventario de aplicaciones de respaldo..... 420
Selección de volúmenes de cintas para la transferencia de datos 420
Restaurar datos que se encuentran en la nube.....423
Recuperación manual de un volumen de cinta del almacenamiento de nube.....423
Trabajo con grupos de acceso..... 425
Creación de un grupo de acceso..... 425
Eliminación del grupo de acceso..... 429
Trabajo con un grupo de acceso seleccionado..... 429
Selección de extremos para un dispositivo.....430
Configuración del grupo TapeServer en dispositivos con NDMP..430
Trabajo con recursos..... 432
Trabajo con iniciadores..... 433
Trabajo con terminales.....434
Trabajo con un punto final seleccionado..... 435
Trabajo con pools..... 436
Creación de pools..... 437
Eliminación de pools.....438
Trabajo con un pool seleccionado..... 439
Conversión de un pool de directorio en un pool MTree 441
Transferencia de cintas entre pools..... 442
Copiado de cintas entre pools.....443
Cambio de nombres de pools..... 444

Capítulo 16 DD Replicator 445
Descripción general de VNX Replicator..... 446
Requisitos previos para la configuración de replicaciones..... 447
Compatibilidad de versiones de replicación.....450
Tipos de replicación.....454
Replicación administrada de archivos 455

Replicación de directorios....456
Replicación de MTree.... 457
Replicación de recopilaciones 459
Uso de DD Encryption con DD Replicator....460
Topologías de replicación.... 461
Replicación de uno a uno.... 462
Replicación bidireccional....463
Replicación de uno a muchos....463
Replicación de muchos a uno....464
Replicación en cascada....465
Administración de la replicación....466
Estado de replicación....466
Vista Summary.... 466
Vista de DD Boost.... 477
Vista Performance.... 479
Vista Advanced Settings....479
Monitoreo de la replicación 482
Visualización del tiempo de finalización estimado para trabajos de respaldo....482
Comprobación del rendimiento de contextos de replicación..... 483
Rastreo del estado de un proceso de replicación.... 483
Retraso de replicación.... 483
Replicación con HA....484
Replicación de un sistema con cuotas a uno sin ellas.... 484
Replication Scaling Context 485
Migración de replicación de directorio a MTree.... 485
Ejecución de migración de la replicación de directorio a la replicación de MTree.... 485
Visualización del progreso de la migración de directorio a MTree.487
Comprobación del estado de la migración de replicación de directorio a MTree.... 487
Anulación de la replicación de D2M 488
Solución de problemas de D2M....488
Solución de problemas de D2M adicionales....489
Uso de la replicación de recopilaciones para la recuperación ante desastres con SMT....490

Capítulo 17 Multiusuario seguro de DD 493
Descripción general de multiusuario seguro de Data Domain.... 494
Aspectos básicos de la arquitectura de SMT.... 494
Terminología utilizada en multiusuario seguro (SMT).... 495
Aislamiento de red y ruta de control.... 496
Comprensión de RBAC en SMT.... 497
Aprovisionamiento de una unidad de grupos de usuario.... 498
Activación del modo Tenant Self-Service....502
Acceso a datos por protocolo.... 502
DD Boost para varios usuarios y unidades de almacenamiento en SMT.... 502
Configuración del acceso para CIFS.... 503
Configuración del acceso a NFS.... 503
Configuración de acceso para DD VTL....504
Uso de NDMP TapeServer de DD VTL 504
Operaciones de administración de datos.... 504
Obtención de estadísticas de rendimiento.... 505
Modificación de cuotas....505

SMT y replicación....506
Alertas de grupos de usuarios de SMT....507
Administración de snapshots....508
Creación de una copia rápida del sistema de archivos....508

Capítulo 18 DD Cloud Tier 509
Descripción general de DD Cloud Tier....510
Plataformas compatibles....510
Rendimiento de DD Cloud Tier....512
Configuración de Cloud Tier....514
Configuración del almacenamiento para DD Cloud Tier....514
Configuración de unidades de nube....516
Configuración de firewall y proxy....516
Importación de certificados de CA....517
Adición de una unidad de nube a Elastic Cloud Storage (ECS)....518
Adición de una unidad de nube para Virtustream....519
Agregar una unidad de nube para Alibaba....520
Adición de una unidad de nube para Amazon Web Services S3....522
Adición de una unidad de nube para Azure....524
Agregar una unidad de nube para el proveedor de Google Cloud. 525
Adición de una unidad de nube de un proveedor de S3 Flexible....527
Modificación de una unidad de nube o un perfil en la nube....528
Eliminación de una unidad de nube....529
Transferencia de datos....530
Adición de políticas de transferencia de datos a MTrees....530
Transferencia manual de datos....531
Transferencia automática de datos....531
Recuperación de un archivo desde el nivel de nube....532
Uso de la CLI para recuperar un archivo desde el nivel de nube...533
Restauración directa desde el nivel de nube....534
Uso de la interfaz de la línea de comandos (CLI) para configurar DD Cloud Tier....535
Configuración del cifrado de unidades de nube DD....539
Información necesaria en caso de pérdida del sistema....540
Uso de DD Replicator con Cloud Tier....540
Uso de la biblioteca de cintas virtuales (VTL) de DD con Cloud Tier....541
Visualización de gráficos de consumo de capacidad para DD Cloud Tier....541
Registros de DD Cloud Tier....542
Uso de la interfaz de la línea de comandos (CLI) para eliminar DD Cloud Tier....542

Capítulo 19 DD Extended Retention 545
Descripción general de DD Extended Retention....546
Protocolos compatibles con DD Extended Retention....548
Alta disponibilidad y Extended Retention....548
Uso de DD Replicator con DD Extended Retention....548
Replicación de recopilación con DD Extended Retention....549
Replicación de directorio con DD Extended Retention....549
Replicación de MTree con DD Extended Retention....549
Replicación de archivos administrada con DD Extended Retention....550
Hardware y licencias para DD Extended Retention....550
Hardware compatible para DD Extended Retention....550
Licencias para DD Extended Retention....554

Agregar licencias de capacidad de bandejas para DD Extended Retention....554
Configuración del almacenamiento para DD Extended Retention.554
Infraestructura proporcionada por el cliente para DD Extended Retention.... 555
Administración de DD Extended Retention....555
Activación de sistemas DD para DD Extended Retention....555
Creación de un sistema de archivos en dos niveles para DD Extended Retention....557
Panel del sistema de archivos para DD Extended Retention.... 558
Pestañas del sistema de archivos para DD Extended Retention...560
Actualizaciones y recuperación con DD Extended Retention....566
Actualización al DD OS 5.7 con DD Extended Retention....566
Actualización de hardware con DD Extended Retention.... 566
Recuperación de un sistema habilitado para DD Extended Retention 567
Migrar datos de nivel de archiving a DD Cloud Tier....568
Planificación de la capacidad.... 569
Detener el movimiento de datos en el nivel de archiving....571
Comprobar ubicaciones de archivos....572
Aplicar la licencia de replicación de Data Domain.... 572
Iniciar la replicación desde el sistema de origen al sistema de destino 573
Monitorear el progreso de la replicación.... 575
Confirme que la inicialización de la replicación esté completa o sincronizada....575
Interrumpir el contexto de replicación....576
Replanificar el sistema de origen....576
Configurar DD Cloud Tier en el sistema de destino....577

Capítulo 20 DD Retention Lock 583
Descripción general del DD Retention Lock.... 584
Protocolo de DD Retention Lock.... 585
Flujo de DD Retention Lock.... 586
Protocolos de acceso a datos admitidos....586
Activación de DD Retention Lock en un MTree....587
Habilitación de DD Retention Lock Governance en un MTree..... 587
Activación de DD Retention Lock Compliance en un MTree..... 589
Control de archivo Retention Lock del lado del cliente.... 590
Configuración de bloqueo de retención sobre un archivo....592
Extensión del bloqueo de retención en un archivo.... 593
Identificación de un archivo Retention-Locked....595
Especificación de un directorio e intervenir solo en esos archivos.... 595
Leer de una lista de archivos y tocar solo aquellos archivos.....595
Eliminar o marcar un archivo como expirado....595
Utilización de ctime o mtime en archivos Retention-Locked.....596
Comportamiento del sistema con DD Retention Lock....596
DD Retention Lock Governance....596
DD Retention Lock Compliance.... 598

Capítulo 21 DD Encryption 609
Descripción general del cifrado de DD....610
Configuración del cifrado....611

Acerca de la administración de claves..... 612
Rectificación de claves perdidas o dañadas..... 612
Compatibilidad con el administrador de claves..... 613
Trabajo con RSA DPM Key Manager..... 613
Trabajo con Embedded Key Manager..... 616
Trabajar con el administrador de claves de KeySecure..... 617
Uso de DD System Manager para configurar y administrar el administrador de claves KeySecure..... 617
Uso de la CLI de Data Domain para administrar el administrador de claves KeySecure..... 620
Cómo funcionan las operaciones de limpieza..... 624
Configuración del administrador de claves..... 624
Configuración de cifrado de RSA DPM Key Manager..... 624
Configuración del administrador de claves del KMIP..... 627
Cambio de administradores de claves después de la configuración..... 629
Administración de certificados para RSA Key Manager..... 630
Comprobación de la configuración del cifrado de datos inactivos..... 631
Activación y desactivación del cifrado de datos inactivos..... 631
Activación del cifrado de datos inactivos..... 631
Cómo desactivar el cifrado de datos inactivos..... 632
Bloqueo y desbloqueo del sistema de archivos..... 632
Bloqueo del sistema de archivos..... 632
Desbloqueo del sistema de archivos..... 633
Cambio del algoritmo de cifrado..... 634

Prefacio

Como parte de un esfuerzo por mejorar sus líneas de productos, Data Domain lanza revisiones periódicas de su hardware y software. Por lo tanto, es posible que no todas las versiones de hardware y software admitan algunas funciones que se describen en este documento. Las notas de la versión del producto proporcionan la información más actualizada sobre las características del producto, las actualizaciones de software y las guías de compatibilidad de software, y detalles acerca de productos, licencias y servicio Data Domain.

En caso de que un producto no funcione correctamente o no funcione según se describe en este documento, póngase en contacto con un profesional de soporte técnico de .

Nota

La información de este documento era precisa en el momento de la publicación. Consulte el soporte en línea (https://support.emc.com) para asegurarse de utilizar la versión más reciente de este documento.

Propósito

Esta guía explica cómo administrar los sistemas Data Domain® con un énfasis en los procedimientos utilizando el administrador de sistemas Data Domain (DD System Manager), una interfaz gráfica del usuario basada en web (GUI). Si no se admite una tarea administrativa importante en DD System Manager, se describen los comandos de la interfaz de la línea de comandos (CLI).

Nota

- DD System Manager anteriormente se denominaba Enterprise Manager.
- En algunos casos, un comando de la CLI puede ofrecer más opciones que las que ofrece la función de DD System Manager correspondiente. Consulte la *Guía de referencia de comandos de Data Domain Operating System* para obtener una descripción completa de un comando y sus opciones.

Público de destino

Esta guía está destinada a los administradores del sistema que están familiarizados con paquetes de software de respaldo estándar y administración de respaldo en general.

Documentación relacionada

En los siguientes documentos del sistema Data Domain, se proporciona información adicional:

- Guía de instalación y configuración del sistema, por ejemplo, *Guía de instalación del sistema Data Domain DD9300*
- *Guía de especificaciones y funciones del hardware de Data Domain*
- *Guía de instalación en USB de Data Domain Operating System*
- *Guía de instalación en DVD de Data Domain Operating System*
- *Notas de la versión de Data Domain Operating System*
- *Guía de configuración inicial de Data Domain Operating System*

- *Guía de configuración de seguridad de Data Domain*
- *Informe técnico de alta disponibilidad de Data Domain Operating System*
- *Guía de referencia de comandos de Data Domain Operating System*
- *Guía de referencia rápida de MIB de Data Domain Operating System*
- *Guía del usuario de la suite de diagnósticos offline de Data Domain Operating System*
- Guías de reemplazo de campo de los componentes del sistema, por ejemplo, *Field Replacement Guide, Data Domain DD4200, DD4500, and DD7200 Systems, IO Module and Management Module Replacement or Upgrade*
- *Guía de actualización de la controladora del sistema de Data Domain*
- *Guía de hardware de la bandeja de expansión de Data Domain* (para modelos de bandeja ES30/FS15 o DS60)
- *Guía de administración para integración de partners de Data Domain Boost*
- *Guía de administración de Data Domain Boost para OpenStorage*
- *Guía de administración de administrador de recuperación de Data Domain Boost para Oracle*
- *Statement of Volatility for the Data Domain DD2500 System*
- *Statement of Volatility for the Data Domain DD4200, DD4500, or DD7200 System*
- *Statement of Volatility for the Data Domain DD6300, DD6800, or DD9300 System*
- *Statement of Volatility for the Data Domain DD9500 or DD9800 System*

Si tiene el RSA Data Protection (DPM) Key Manager opcional, consulte la versión más reciente de la guía *RSA Data Protection Manager Server Administrator's Guide*, disponible con el producto RSA Key Manager.

Convenciones para avisos especiales utilizadas en este documento
Data Domain utiliza las siguientes convenciones en las notificaciones especiales:

AVISO

Un aviso identifica el contenido que advierte sobre la posibilidad de pérdida de negocios o datos.

Nota

Una nota identifica la información que es incidental, pero no esencial, para el tema. Las notas pueden proporcionar una explicación, un comentario, un refuerzo de un punto en el texto o simplemente un punto relacionado.

Convenciones tipográficas
Data Domain utiliza las siguientes convenciones de estilo de letras en este documento:

Tabla 1 Tipografía

Negrita	Indica nombres de elementos de la interfaz, como los nombres de las ventanas, los cuadros de diálogo, los botones, los campos, los nombres de las pestañas, los nombres de las teclas y las rutas de acceso de menú (los elementos que el usuario selecciona o en los que hace clic específicamente)
Cursiva	Resalta los títulos de publicaciones que se incluyen en el texto
`Monospace`	Indica la información del sistema, tal como:

Tabla 1 Tipografía (continuación)

	• Código del sistema • Salida del sistema, como un mensaje de error o script • Nombres de ruta, nombres de archivos, indicadores y sintaxis. • Comandos y opciones
Fuente monoespaciada en cursiva	Destaca el nombre de una variable que debe reemplazarse por el valor de la variable
`Fuente monoespaciada en negrita`	Indica el texto para la entrada del usuario
[ ]	Los corchetes encierran valores opcionales
|	La barra vertical indica selecciones alternativas; la barra significa “o”
{ }	Las llaves encierran contenido que debe especificar el usuario, como x, y o z
...	Los puntos suspensivos indican información no esencial omitida en el ejemplo

Dónde obtener ayuda

La información sobre soporte, productos y licencias de Data Domain puede obtenerse de la siguiente manera:

Información de productos

Para obtener documentación, notas de la versión, actualizaciones de software o información acerca de los productos Data Domain, visite el soporte en línea en https://support.emc.com.

Soporte técnico

Visite el soporte en línea y haga clic en Centro de servicios. Podrá ver varias opciones para comunicarse con el soporte técnico. Tenga en cuenta que para abrir una solicitud de servicio, debe contar con un acuerdo de soporte válido. Póngase en contacto con un representante de ventas para conocer detalles acerca de cómo obtener un acuerdo de soporte válido o si tiene dudas sobre su cuenta.

Sus comentarios

Sus sugerencias nos ayudarán a continuar mejorando la exactitud, organización y calidad general de la documentación para usuarios. Envíe sus opiniones sobre este documento a: DPAD.Doc.Feedback@emc.com.

CAPÍTULO 1

Integración y funciones del sistema Data Domain

Este capítulo incluye:

- Historial de revisiones 22
- Descripción general del sistema Data Domain 22
- Funciones del sistema Data Domain 22
- Integración de ambientes de almacenamiento 30

Historial de revisiones

El historial de revisiones muestra los cambios principales de este documento para respaldar la versión del SO DD 6.2.

Tabla 2 Historial de revisiones del documento

Revisión	Fecha	Descripción
01 (6.2.0)	Diciembre de 2018	Esta revisión incluye información acerca de estas nuevas funciones: • Configurar las credenciales del servidor de correo como parte del asistente de configuración de DD SM. • Capacidad de expansión de DD300 de 8 TB a 16 TB. • Autenticación con LDAP segura. • Herramienta de diagnóstico de conexión de Active Directory. • Guardar archivos de coredump en una unidad USB. • Notificación de cambio de SMB. • Acceso sin conexión a dominio de confianza. • Compatibilidad de DD Cloud Tier con proveedores de nube de Alibaba y Google Cloud Platform.

Descripción general del sistema Data Domain

Los sistemas Data Domain son dispositivos de deduplicación en línea basados en discos que proporcionan protección de datos y recuperación ante desastres (DR) en el ambiente empresarial.

Todos los sistemas ejecutan Data Domain Operating System (DD OS), que proporciona una interfaz de la línea de comandos (CLI) para realizar todas las operaciones del sistema y la interfaz gráfica del usuario (GUI) de Data Domain System Manager (DD System Manager) para la configuración, la administración y el monitoreo.

Nota

DD System Manager anteriormente se denominaba Enterprise Manager.

Los sistemas constan de dispositivos que varían en capacidad de almacenamiento y rendimiento de datos. Los sistemas generalmente están configurados con gabinetes de expansión que agregan espacio de almacenamiento.

Funciones del sistema Data Domain

Las funciones del sistema Data Domain garantizan la integridad de los datos, una restauración confiable, el uso eficiente de recursos y la facilidad de administración. Las

funciones con licencia le permiten escalar el conjunto de funciones del sistema para que se ajuste a sus necesidades y presupuesto.

Integridad de los datos

DD OS Data Invulnerability Architecture™ protege contra pérdida de datos por fallas de hardware y software.

- Cuando se escribe un disco, el SO DD crea y almacena sumas de comprobación y metadatos autodescriptivos de todos los datos recibidos. Después de escribir los datos en el disco, el SO DD vuelve a procesar y verifica las sumas de comprobación y los metadatos.
- Una política de escritura de solo anexo protege contra la sobrescritura de datos válidos.
- Después de que se completa un respaldo, un proceso de validación examina qué se escribió en el disco y verifica que todos los segmentos de archivos sean lógicamente correctos dentro del sistema de archivos, así como que los datos sean idénticos antes y después de la escritura en el disco.
- En segundo plano, la operación de verificación en línea comprueba constantemente que los datos en los discos sean correctos y no se hayan modificado desde el proceso de validación anterior.
- El almacenamiento en la mayoría de los sistemas Data Domain está configurado con paridad doble RAID 6 (dos unidades de paridad). Además, la mayoría de las configuraciones incluyen un hot spare en cada gabinete, excepto los sistemas serie DD1xx, que usan ocho discos. Cada fracción de paridad usa sumas de comprobación en bloques para garantizar que los datos sean correctos. Las sumas de comprobación se usan constantemente durante la operación de verificación en línea y mientras los datos se leen desde el sistema Data Domain. Con paridad doble, el sistema puede solucionar errores simultáneos en dos discos como máximo.
- Para mantener los datos sincronizados durante una falla de hardware o de alimentación, el sistema Data Domain usa NVRAM (RAM no volátil) para rastrear las operaciones de I/O pendientes. Una tarjeta NVRAM con baterías completamente cargadas (el estado normal) puede retener datos durante un período de horas, lo que se determina según el hardware en uso.
- Cuando se vuelven a leer los datos en una operación de restauración, el SO DD usa varias capas de comprobaciones de coherencia para verificar que los datos restaurados sean correctos.
- Al escribir en la caché de SSD, DD OS:
  - Crea una suma de verificación de SL para todos los registros almacenados en la caché para detectar los daños de datos de la caché. Esta suma de verificación está validada para cada caché de lectura.
  - Trata los daños de datos de la caché como un error de caché y no tiene como resultado la pérdida de datos. Por lo tanto, los clientes de caché no pueden almacenar la copia más reciente de los datos sin algún otro mecanismo de respaldo, como la NVRAM o el disco duro.
  - Elimina la necesidad de verificación en línea de escrituras en caché, ya que los clientes de caché pueden detectar y manejar escrituras perdidas o mal direccionadas. Esto también ahorra ancho de banda de I/O.

- Elimina la necesidad de limpieza de discos SSD del sistema de archivos, ya que los datos en la caché cambian con frecuencia y ya fueron limpiados por el análisis de medios en segundo plano (BMS) de SAS.

Deduplicación de datos

La deduplicación de datos del SO DD identifica datos redundantes durante cada respaldo y almacena datos únicos una sola vez.

El almacenamiento de datos únicos es invisible para el software de respaldo e independiente del formato de los datos. Los datos pueden ser estructurados, como las bases de datos, o no estructurados, como los archivos de texto. Los datos se pueden derivar de sistemas de archivos o de volúmenes crudos.

Las proporciones de deduplicación típicas son de 20 a 1, en promedio, en muchas semanas. Esta proporción supone que hay respaldos completos semanales y respaldos incrementales diarios. Un respaldo que incluye muchos archivos duplicados o similares (archivos copiados varias veces con cambios menores) se beneficia más de la deduplicación.

Según el volumen, el tamaño, el período de retención y la velocidad de cambio del respaldo, puede variar la cantidad de deduplicación. La mejor deduplicación ocurre con tamaños de volúmenes de respaldo de al menos 10 MiB (MiB es el equivalente de base 2 de MB).

Para aprovechar completamente varios sistemas Data Domain, un sitio con más de un sistema Data Domain debe respaldar continuamente el mismo conjunto de datos o sistema del cliente en el mismo sistema Data Domain. Por ejemplo, si un respaldo completo de todos los datos de ventas va al sistema Data Domain A, se logra la deduplicación máxima cuando los respaldos incrementales y los respaldos completos futuros de los datos de ventas también van al sistema Data Domain A.

Operaciones de restauración

Las operaciones de restauración de archivos no crean contención, o crean poca, con las operaciones de respaldo u otras.

Cuando se realizan respaldos en discos en un sistema Data Domain, los respaldos incrementales siempre son confiables y se puede acceder fácilmente a ellos. Con los respaldos en cinta, una operación de restauración puede depender de que varias cintas tengan respaldos incrementales. Además, cuantos más respaldos incrementales almacena un sitio en varias cintas, más tiempo consume y más riesgoso es el proceso de restauración. Una cinta defectuosa puede interrumpir la restauración.

Al usar un sistema Data Domain, puede realizar respaldos completos con más frecuencia sin la penalidad de almacenar datos redundantes. A diferencia de los respaldos de unidades de cinta, varios procesos pueden acceder a un sistema Data Domain simultáneamente. Un sistema Data Domain permite que su sitio ofrezca operaciones de restauración seguras, dirigidas por los usuarios y de un solo archivo.

Data Domain Replicator

Data Domain Replicator configura y administra la replicación de datos de respaldo entre dos sistemas Data Domain.

Un par de DD Replicator consta de un sistema de origen y uno de destino, y replica un conjunto de datos o un directorio completo del sistema de origen en el sistema de destino. Un sistema Data Domain individual puede ser parte de varios pares de replicación y puede funcionar como el origen de uno o más pares y el destino de uno o

más pares. Después de que se inicia la replicación, el sistema de origen envía automáticamente todos los datos de respaldo nuevos al sistema de destino.

Balanceo de carga y múltiples rutas

En una configuración de múltiples rutas de Fibre Channel, se establecen múltiples rutas entre un sistema Data Domain y un servidor de respaldo o un arreglo de destino de respaldo. Cuando hay múltiples rutas presentes, el sistema balancea automáticamente la carga de respaldo entre las rutas disponibles.

Se requieren al menos dos puertos HBA para crear una configuración de múltiples rutas. Cuando se conecta a un servidor de respaldo, cada uno de los puertos HBA en las múltiples rutas se conecta a un puerto independiente en el servidor de respaldo.

Alta disponibilidad

La función de alta disponibilidad (HA) le permite configurar dos sistemas Data Domain como un par activo-en espera, lo que proporciona redundancia en caso de una falla del sistema. La alta disponibilidad mantiene sincronizados los sistemas activos y en espera, de modo que, si el nodo activo falla debido a problemas de hardware o software, el nodo en espera puede ocuparse de servicios y continuar donde se detuvo el nodo con fallas.

La función de alta disponibilidad:

- Es compatible con la conmutación por error de los servicios de respaldo, restauración, replicación y administración en un sistema de dos nodos. La conmutación por error automática no requiere ninguna intervención del usuario.
- Proporciona un diseño completamente redundante sin puntos únicos de falla dentro del sistema cuando se configura según las recomendaciones.
- Proporciona un sistema activo-standby sin pérdida de rendimiento en caso de conmutación por error.
- Proporciona conmutación por error en un plazo de 10 minutos para la mayoría de las operaciones. CIFS, DD VTL y NDMP se deben reiniciar manualmente.

  Nota

  La recuperación de aplicaciones de DD Boost puede tardar más de 10 minutos, ya que la recuperación de aplicaciones de Boost no puede comenzar mientras no finalice la conmutación por error del servidor DD. Además, la recuperación de aplicaciones de Boost no puede comenzar hasta que la aplicación invoca la biblioteca de Boost. De manera similar, es posible que NFS requiera tiempo adicional para recuperar.

- Es compatible con la facilidad de administración y configuración por medio de las CLI de DD OS.
- Proporciona alertas de hardware que funciona incorrectamente.
- Conserva escalabilidad y el rendimiento de un solo nodo dentro de una configuración de alta disponibilidad en el modo normal y degradado.
- Es compatible con el mismo conjunto de funciones que los sistemas DD independientes.

  Nota

  No se admite vDisk ni DD Extended Retention.

- Es compatible con sistemas con todos los discos SAS. Esto incluye sistemas heredados actualizados a sistemas con todos los discos SAS.

  Nota

  La guía de la descripción general de hardware y la de instalación de sistemas Data Domain que admiten alta disponibilidad describen cómo instalar un nuevo sistema de alta disponibilidad. La *Actualización de un solo nodo de Data Domain a la alta disponibilidad* describe cómo actualizar un sistema existente a un par de alta disponibilidad.

- No afecta la capacidad de escalar el producto.
- Es compatible con actualizaciones de software no disruptivas.

La alta disponibilidad se admite en los siguientes sistemas Data Domain:

- DD6800
- DD9300
- DD9500
- DD9800

Arquitectura de alta disponibilidad

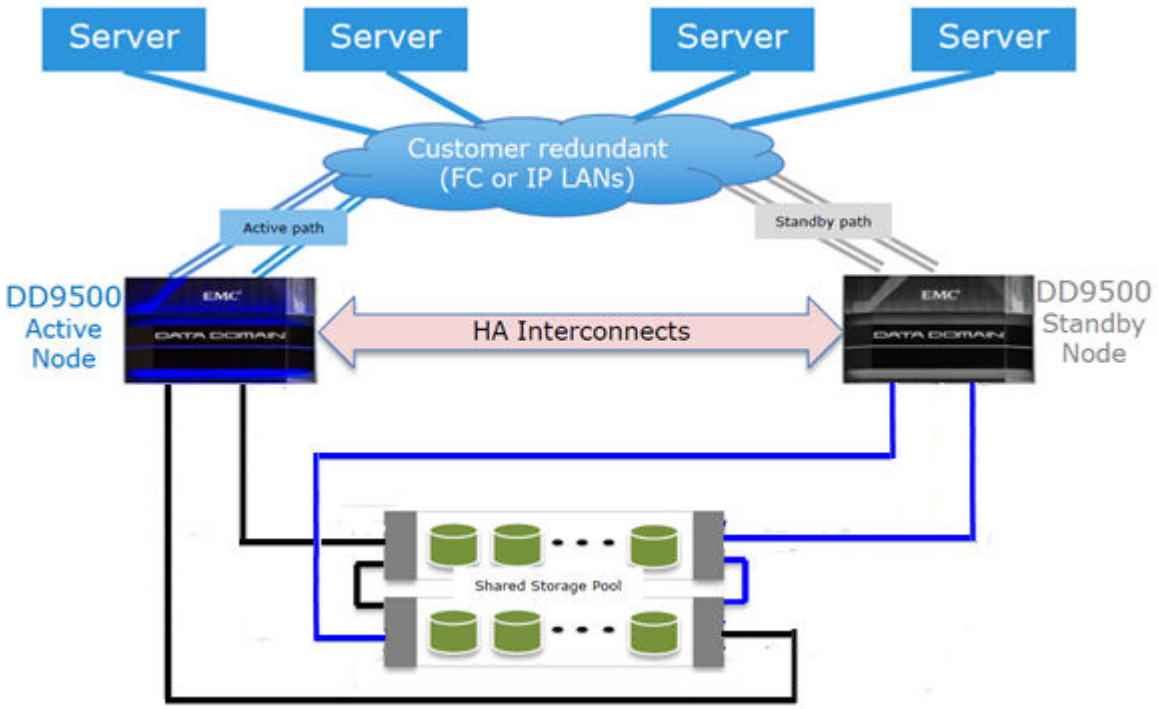
La función de alta disponibilidad está disponible para las conexiones IP y FC. Ambos nodos deben tener acceso a las mismas redes IP, SAN FC y hosts a fin de lograr alta disponibilidad para el ambiente.

Mediante redes IP, la alta disponibilidad usa una dirección IP flotante para proporcionar acceso a los datos al par de alta disponibilidad de Data Domain, independientemente de qué nodo físico sea el nodo activo.

A través de las SAN FC, la alta disponibilidad usa NPIV para trasladar los WWN entre nodos, lo que permite que los iniciadores de FC vuelvan a establecer conexiones después de un failover.

La Figura 1 en la página 27 muestra la arquitectura de la alta disponibilidad.

Figura 1 Arquitectura de alta disponibilidad



Manejo de I/O aleatorias

Las optimizaciones de I/O aleatorias incluidas en DD OS brindan un mejor rendimiento para aplicaciones y casos de uso que generan mayores cantidades de operaciones de lectura y escritura aleatorias que de operaciones de lectura y escritura secuenciales.

DD OS está optimizado para manejar cargas de trabajo que constan de operaciones de lectura y escritura aleatorias, como acceso instantáneo y restauración instantánea de máquinas virtuales, y respaldos eternos incrementales generados por aplicaciones, como Avamar. Estas optimizaciones:

- Mejoran las latencias de lectura aleatoria y escritura aleatoria.
- Mejoran los IOPS de usuario con tamaños de lectura más pequeños.
- Admiten operaciones de I/O concurrentes dentro de un solo flujo.
- Proporcionan rendimiento de lectura y escritura pico con flujos menores.

Nota

El conteo de flujos de I/O aleatorio máximo se limita al conteo máximo de flujos de restauración de un sistema Data Domain.

Las mejoras de I/O aleatorias permiten que el sistema Data Domain admita la funcionalidad de acceso instantáneo / restauración instantánea para aplicaciones de respaldo, como Avamar y Networker.

Acceso de administrador del sistema

Los administradores del sistema pueden acceder al sistema para la configuración y la administración a través de una interfaz de la línea de comandos o mediante una interfaz gráfica del usuario.

- CLI de DD OS: una interfaz de la línea de comandos que está disponible a través de una consola en serie o a través de conexiones Ethernet con SSH o Telnet. Los comandos de la CLI permiten la configuración inicial del sistema, cambios en opciones de configuración individuales y la visualización del estado operativo del sistema.
- DD System Manager: una interfaz gráfica del usuario basada en web que está disponible a través de conexiones Ethernet. Puede usar DD System Manager para realizar la configuración inicial del sistema, realizar cambios después de la configuración inicial, visualizar el estado del sistema y los componentes, y generar informes y gráficos.

Nota

Algunos sistemas admiten el acceso mediante un teclado y un monitor conectados directamente al sistema.

Funciones con licencia

Las funciones con licencia le permiten comprar solo las funciones que desea usar. Algunos ejemplos de funciones que requieren licencia son DD Extended Retention, DD Boost y los aumentos en la capacidad de almacenamiento.

Consulte a su representante de ventas para obtener información sobre la compra de funciones con licencia.

Tabla 3 Funciones que requieren licencias

Nombre de la característica	Nombre de la licencia en software	Descripción
Data Domain ArchiveStore	ARCHIVESTORE	Otorga licencia para sistemas Data Domain para el uso de archivos, como archiving de correo electrónico y archivos, almacenamiento en niveles de archivos, y archiving de contenido y bases de datos.
Data Domain Boost	DDBOOST	Permite el uso de un sistema Data Domain con las siguientes aplicaciones: Avamar, NetWorker, Oracle RMAN, Quest vRanger, Symantec Veritas NetBackup (NBU) y Backup Exec. La función de replicación administrada de archivos (MFR) de DD Boost también requiere la licencia de DD Replicator.
Data Domain Capacity on Demand	CONTROLLER-COD	Permite un aumento de capacidad a petición para sistemas DD2200 de 4 TB a 7.5 TB o 13.18 TB. Un aumento a 13.18 TB también requiere la licencia EXPANDED-STORAGE.

Tabla 3 Funciones que requieren licencias (continuación)

Nombre de la característica	Nombre de la licencia en software	Descripción
Data Domain Cloud Tier	CLOUDTIER-CAPACITY	Permite que un sistema Data Domain transfiera datos del nivel activo al almacenamiento de objetos de bajo costo y alta capacidad en la nube pública, privada o híbrida para retención a largo plazo.
Data Domain Encryption	ENCRYPTION	Permite el cifrado de datos en unidades del sistema o en un almacenamiento externo, mientras se guardan y bloquean, antes de su traslado a otra ubicación.
Data Domain Expansion Storage	EXPANDED-STORAGE	Permite la expansión del almacenamiento de sistemas Data Domain más allá del nivel proporcionado en el sistema de base.
Data Domain Extended Retention (anteriormente DD Archiver)	EXTENDED-RETENTION	Otorga licencia para la función de almacenamiento DD Extended Retention.
Data Domain I/OS (para ambientes operativos IBM i)	I/OS	Una licencia I/OS se requiere cuando DD VTL se usa para respaldar sistemas en un ambiente operativo IBM i. Aplique esta licencia antes de agregar unidades de cintas virtuales a las librerías.
Data Domain Replicator	REPLICACIÓN	Agrega DD Replicator para la replicación de datos de un sistema Data Domain a otro. Se requiere una licencia en cada sistema.
Data Domain Retention Lock Compliance Edition	RETENTION-LOCK-COMPLIANCE	Cumple con los requisitos de retención de datos más estrictos de estándares de cumplimiento de normas como SEC17a-4.
Data Domain Retention Lock Governance Edition	RETENTION-LOCK-GOVERNANCE	Protege archivos seleccionados contra modificación y eliminación antes de que venza un período de retención seleccionado.
Data Domain Shelf Capacity-Active Tier	CAPACITY-ACTIVE	Permite que un sistema Data Domain expanda la capacidad de almacenamiento del nivel activo a un gabinete adicional o un paquete de discos dentro de un gabinete.
Data Domain Shelf Capacity-Archive Tier	CAPACITY-ARCHIVE	Permite que un sistema Data Domain expanda la capacidad de almacenamiento del nivel de archivo a un gabinete adicional o un paquete de discos dentro de un gabinete.
Data Domain Storage Migration	STORAGE-MIGRATION-FOR-DATADOMAIN-SYSTEMS	Permite la migración de datos de un gabinete de a otro para admitir el reemplazo de los gabinetes antiguos y de menor capacidad.
Data Domain Virtual Tape Library (DD VTL)	Librería de cintas virtuales	Permite el uso de un sistema Data Domain como una librería de cintas virtual en una red Fibre Channel. Esta licencia también permite la función

Tabla 3 Funciones que requieren licencias (continuación)

Nombre de la característica	Nombre de la licencia en software	Descripción
		de servidor de cintas NDMP, que anteriormente requería una licencia independiente.
Alta disponibilidad	HA-ACTIVE-PASSIVE	Activa la función de alta disponibilidad en una configuración de activo-standby. Solo debe adquirir una licencia de alta disponibilidad; la licencia se ejecuta en el nodo activo y se espejea en el nodo en espera.

Integración de ambientes de almacenamiento

Los sistemas Data Domain se integran fácilmente con centros de datos existentes.

- Todos los sistemas Data Domain se pueden configurar como destinos de almacenamiento para aplicaciones de respaldo y archiving líder que usan protocolos NFS, CIFS, DD Boost o DD VTL.
- Busque los *documentos de compatibilidad* en https://support.emc.com para obtener información sobre las aplicaciones que pueden funcionar con las diferentes opciones de configuración.
- Varios servidores de respaldo pueden compartir un sistema Data Domain.
- Un sistema Data Domain puede manejar varias operaciones de respaldo y restauración simultáneas.
- Se pueden conectar varios sistemas Data Domain con uno o más servidores de respaldo.

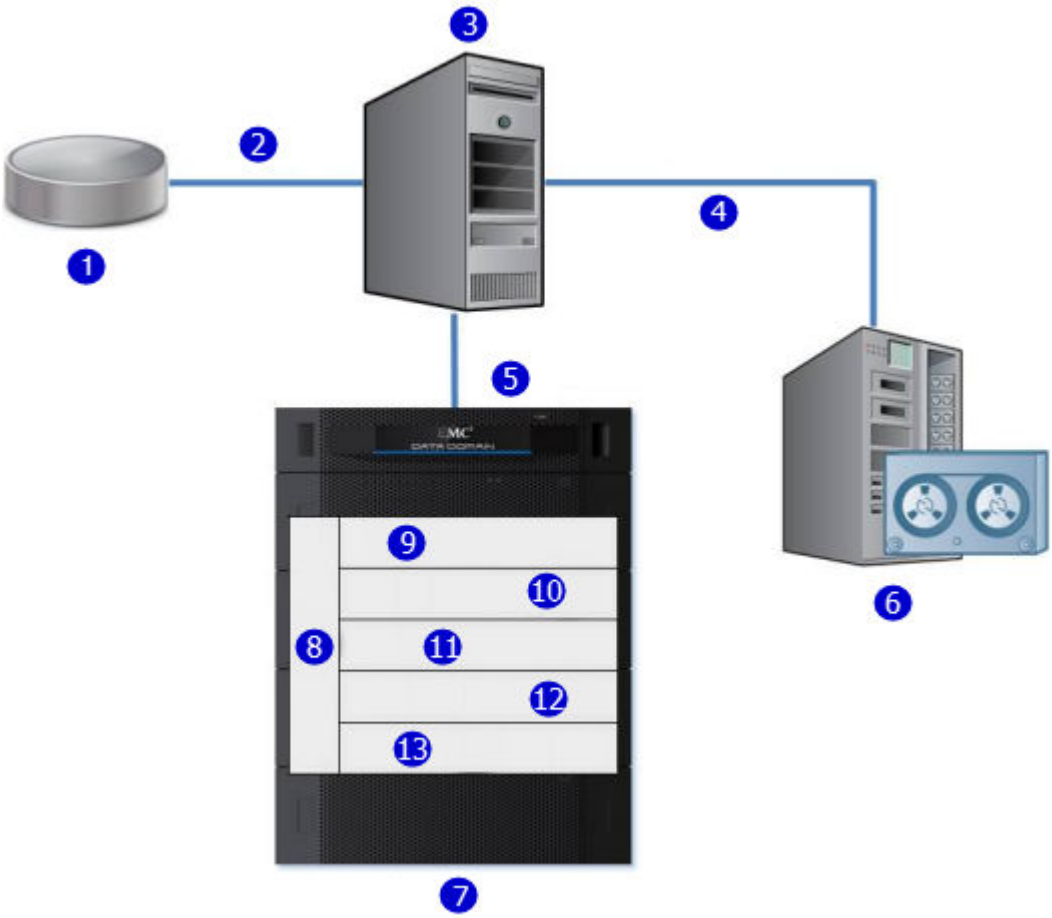
Para usarlo como destino de respaldo, un sistema Data Domain puede configurarse como una unidad de almacenamiento en disco con un sistema de archivos al que se accede a través de una conexión Ethernet o como una librería de cintas virtuales a la que se accede por medio de una conexión de Fibre Channel. La función de DD VTL permite que los sistemas Data Domain se integren en ambientes donde ya hay software de respaldo configurado para respaldos de cintas, lo que minimiza la interrupción.

La configuración se realiza en DD OS, como se describe en las secciones relevantes de esta guía, y en la aplicación de respaldo, como se describe en las guías para administradores de la aplicación de respaldo y en las notas técnicas y en las guías relacionadas con la aplicación de Data Domain.

Todas las aplicaciones de respaldo pueden acceder a un sistema Data Domain como un sistema de archivos NFS o CIFS en el dispositivo de disco Data Domain.

En la siguiente figura se muestra un sistema Data Domain integrado en una configuración de respaldo básica existente.

Figura 2 Sistema Data Domain integrado en un ambiente de almacenamiento



1. Almacenamiento primario
2. Ethernet
3. Servidor de respaldo
4. SCSI/Fibre Channel
5. Gigabit Ethernet o Fibre Channel
6. Sistema de cintas
7. Sistema Data Domain
8. Administración
9. NFS/CIFS/DD VTL/DD Boost
10. Verificación de datos
11. Sistema de archivos
12. Deduplicación y compresión globales
13. RAID

Como se muestra en la Figura 2 en la página 31, los datos se transfieren a un sistema Data Domain por medio de una conexión Ethernet o Fibre Channel. Los procesos de verificación de datos comienzan de inmediato y continúan mientras los datos residen en el sistema Data Domain. En el sistema de archivos, los algoritmos de DD OS Global Compression™ deduplican y comprimen los datos para el almacenamiento. A continuación, los datos se envían al subsistema RAID de disco. Cuando se requiere una operación de restauración, los datos se recuperan del almacenamiento de Data

Domain, se descomprimen, se verifica su coherencia y se transfieren a través de Ethernet a los servidores de respaldo mediante Ethernet (para NFS, CIFS, DD Boost) o mediante Fiber Channel (para DD VTL y DD Boost).

DD OS se adapta a flujos de datos secuenciales relativamente grandes del software de respaldo y está optimizado para alto rendimiento, verificación de datos continua y alta compresión. También se adapta a las grandes cantidades de archivos pequeños en el almacenamiento nearline (DD ArchiveStore).

El rendimiento del sistema Data Domain es mejor cuando se almacenan datos de aplicaciones que no son específicamente software de respaldo bajo las siguientes circunstancias.

- Los datos se envían al sistema Data Domain como escrituras secuenciales (no como sobrescrituras).
- Los datos no se comprimen ni se cifran antes de enviarse al sistema Data Domain.

CAPÍTULO 2

Introducción

Este capítulo incluye:

- Descripción general de Dell EMC Data Domain System Manager 34
- Inicio y cierre de sesión de DD System Manager 35
- Interfaz de DD System Manager 38
- Configuración del sistema con el asistente de configuración 40
- Interfaz de la línea de comandos de Data Domain 54
- Inicio de sesión en la CLI 55
- Reglas de ayuda en línea de la CLI 56

Descripción general de Dell EMC Data Domain System Manager

DD System Manager es una interfaz del usuario basada en un navegador, que está disponible mediante conexiones Ethernet, para administrar un solo sistema desde cualquier ubicación. DD System Manager ofrece una única interfaz de administración consolidada que permite la configuración y el monitoreo de muchas funciones y opciones de configuración del sistema.

Nota

Data Domain Management Center le permite administrar múltiples sistemas desde una sola ventana del navegador.

DD System Manager proporciona gráficos y tablas en tiempo real que le permiten monitorear el estado de los componentes de hardware y las funciones configuradas del sistema.

Además, hay un conjunto de comandos disponible que lleva a cabo todas las funciones del sistema para los usuarios en la interfaz de la línea de comandos (CLI). Los comandos establecen las opciones de configuración del sistema y proporcionan visualizaciones del estado del hardware, la configuración de funciones y el funcionamiento del sistema.

La interfaz de la línea de comandos está disponible a través de una consola en serie o a través de una conexión Ethernet con SSH o Telnet.

Nota

Algunos sistemas admiten el acceso mediante un teclado y un monitor conectados directamente al sistema.

Versiones de software de DD OS

Las versiones de software DD OS tienen tres estados públicos, que indican la cantidad de sistemas instalados que ejecutan la versión.

- Las versiones de **disponibilidad general** han completado las pruebas de control de calidad internas de Data Domain y se pueden instalar en ambientes de producción.
- Las versiones de **disponibilidad dirigida y controlada (disponibilidad dirigida)** son versiones de acceso controladas cuidadosamente, que se dirigen a un pequeño número de instalaciones. Los clientes pueden solicitar ser calificados para el acceso a estas versiones.
- **Código de destino**: Se recomienda que todos los sistemas se actualicen al código de destino del SO de Data Domain dentro de una familia de versiones tan pronto como resulte práctico.

Nota

Solo hay una versión de código de destino en una familia determinada. Las versiones de código de destino han cumplido las horas de instalación y tiempo de ejecución, así como las métricas de calidad que indican que son estables y no tienen problemas que puedan afectar a la mayoría de los clientes. Para algunas familias, es posible que no haya ningún código de destino identificado, debido a la aceptación limitada de los clientes, los problemas de calidad u otras consideraciones.

Cuando se realiza una actualización entre familias, se debe tener en cuenta la compatibilidad entre los productos y se debe realizar un análisis cuidadoso de la compatibilidad del producto antes de cualquier actualización a una nueva familia de versiones.

Inicio y cierre de sesión de DD System Manager

Use un navegador para iniciar sesión en DD System Manager.

Cuando se conecte con DD System Manager desde un navegador web, todas las conexiones HTTP se redireccionarán automáticamente a HTTPS.

Procedimiento

1. Abra un navegador web e ingrese la dirección IP o el nombre de host para conectarse a DD System Manager. Debe ser:
   - Un nombre de dominio calificado (por ejemplo, `http://dd01.emc.com`)
   - Un nombre de host (`http://dd01`)
   - Una dirección IP (`http://10.5.50.5`)

   Nota

   DD System Manager usa el puerto HTTP 80 y el puerto HTTPS 443. Si su sistema Data Domain está protegido con firewall, es posible que deba habilitar el puerto 80 si usa HTTP o el puerto 443 si usa HTTPS para acceder al sistema. Los números de puerto se pueden cambiar fácilmente si los requisitos de seguridad lo exigen.

Nota

Si Data Domain System Manager no puede iniciarse desde cualquier navegador web, el mensaje de error que se muestra es “The GUI Service is temporarily unavailable. Please refresh your browser. If the problem persists, please contact Data Domain support for assistance”. SSH se puede utilizar para iniciar sesión en el sistema Data Domain y puede ejecutar todos los comandos.
Si no ha actualizado DD OS, pero todavía encuentra este error de GUI, utilice el siguiente procedimiento:

a. Cierre la sesión del navegador web en el sistema Data Domain con el error informado.

b. Ejecute estos comandos en secuencia:

- `adminaccess disable http`
- `adminaccess disable https`
- `adminaccess enable http`
- `adminaccess enable https`

c. Espere 5 minutos para permitir que los servicios HTTP y HTTPS se inicien por completo.

d. Abra un navegador web y conéctese a Data Domain System Manager.

Si ve este problema de GUI después de una actualización de DD OS, utilice el siguiente procedimiento:

a. Cierre la sesión del navegador web en el sistema Data Domain con el error informado.

b. Ejecute estos comandos en secuencia:

- `adminaccess disable http`
- `adminaccess disable https`
- `adminaccess certificate generate self-signed-cert`
- `adminaccess enable http`
- `adminaccess enable https`

a. Espere 5 minutos para permitir que los servicios HTTP y HTTPS se inicien por completo.

b. Abra un navegador web y conéctese a Data Domain System Manager.

2. Para el inicio de sesión seguro con HTTPS, haga clic en **Secure Login**.

   El inicio de sesión seguro con HTTPS requiere un certificado digital para validar la identidad del sistema DD OS y para admitir cifrado bidireccional entre DD System Manager y un navegador. DD OS incluye un certificado autofirmado y le permite importar su propio certificado.

3. Escriba su nombre de usuario y contraseña asignados.

Nota

El nombre de usuario inicial es *sysadmin* y la contraseña inicial es el número de serie del sistema. Para obtener información sobre cómo configurar un sistema nuevo, consulte la *Guía de configuración inicial de Data Domain Operating System*.

4. Haga clic en **Log In**.

   Si esta es la primera vez que ha iniciado sesión, se mostrará la vista Home en el panel Information.

   Nota

   Si introduce una contraseña incorrecta cuatro veces consecutivas, el sistema bloquea el nombre de usuario especificado durante 120 segundos. El tiempo entre el inicio de sesión y período de bloqueo puede configurarse y puede ser diferente en su sistema.

   Nota

   Si esta es la primera vez que inicia sesión, es posible que deba necesario para cambiar la contraseña. Si el administrador del sistema ha configurado su nombre de usuario para solicitar un cambio de contraseña, deberá cambiar la contraseña para poder obtener acceso a DD System Manager.

5. Para cerrar sesión, haga clic en el botón Log Out en el anuncio de DD System Manager.

   Cuando cierre sesión, el sistema mostrará la página de inicio de sesión con un mensaje indicando que se completó el cierre de sesión.

Inicio de sesión con un certificado

Como una alternativa al inicio de sesión con un nombre de usuario y una contraseña, puede iniciar sesión en DD System Manager con un certificado emitido por una autoridad de certificación (CA).

Para iniciar sesión con un certificado, debe tener privilegios de autorización en el sistema Data Domain, y el sistema Data Domain debe confiar en el certificado de la CA. Se debe especificar el nombre de usuario en el campo common-name en el certificado.

Procedimiento

1. Asegúrese de que tiene una cuenta de usuario en el sistema Data Domain.

   Puede ser un usuario local o un usuario de servicio de nombre (NIS/AD). Si es un usuario de servicio de nombre, la asignación de grupo a función debe configurarse en el sistema Data Domain.

2. Utilice el siguiente comando de la CLI para importar la clave pública de la CA que emitió el certificado: `adminaccess certificate import ca application login-auth`.

3. Cargue el certificado en formato PKCS12 en su navegador.

   Una vez que el certificado de la CA se marque como de confianza en el sistema Data Domain, se mostrará un vínculo **Log in with certificate** en la pantalla de inicio de sesión del HTTPS.

4. Haga clic en **Log in with certificate** y seleccione el certificado en la lista de certificados que aparece en el navegador.

Resultados

El sistema Data Domain valida el certificado de usuario en comparación con el almacén de confianza. En función de los privilegios de autorización asociados a su cuenta, se crea una sesión de administrador del sistema para usted.

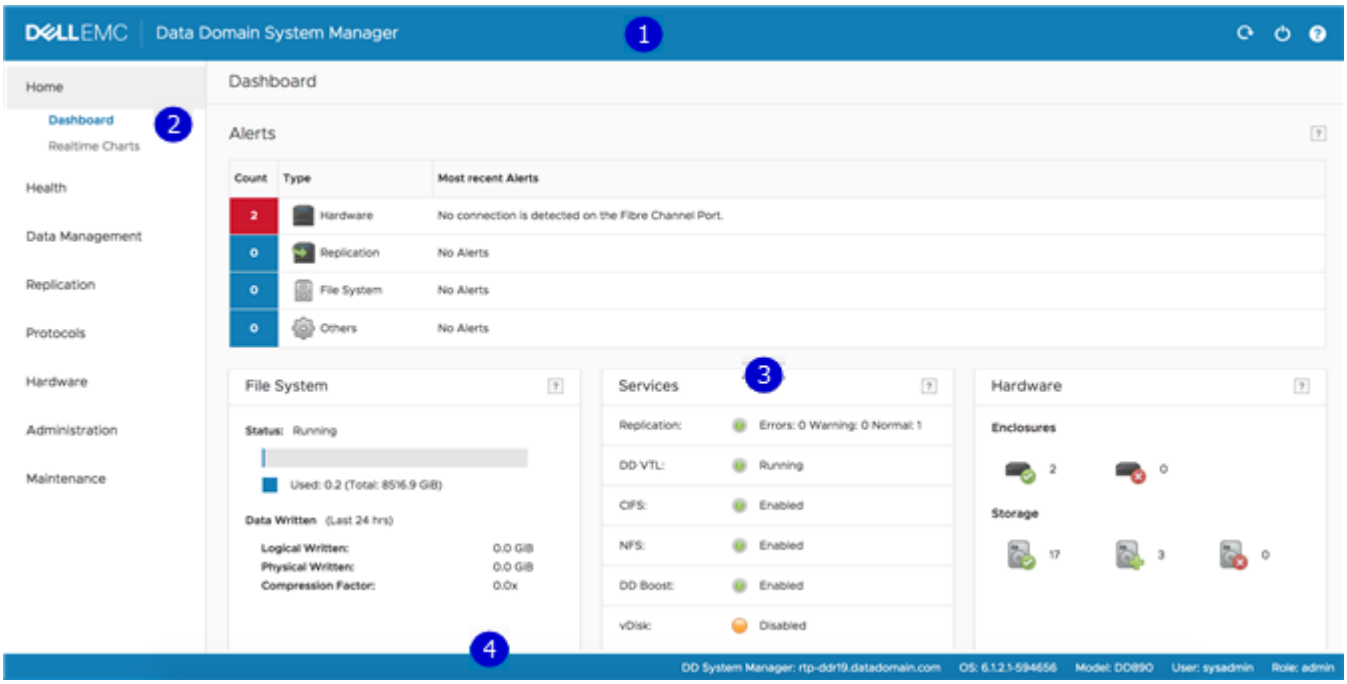
Interfaz de DD System Manager

La interfaz de DD System Manager proporciona elementos comunes en la mayoría de las páginas, que le permiten desplazarse por las opciones de configuración y ver ayuda contextual.

Elementos de la página

Los elementos de la página principal son la barra del encabezado, el panel de navegación, los paneles de información y el pie de página.

Figura 3 Componentes de la página de DD System Manager



1. Anuncio
2. Panel de navegación
3. Paneles de información
4. Pie de página

Anuncio

El anuncio de DD System Manager muestra el nombre del programa y los botones para las opciones **Refresh**, **Log Out** y **Help**.

Panel de navegación

El panel de navegación muestra las selecciones de menú de nivel más alto que puede utilizar para identificar el componente del sistema o la tarea que desea administrar.

El panel de navegación muestra los dos niveles superiores del sistema de navegación. Haga clic en cualquier título de nivel superior para mostrar los títulos de segundo nivel. Las pestañas y los menús del panel de información proporcionan controles de navegación adicionales.

Panel de información

El panel de información muestra información y controles relacionados con el elemento seleccionado en el panel de navegación. El panel de información es donde puede encontrar información acerca del estado del sistema y configurar un sistema.

Según la función o la tarea seleccionada en el panel de navegación, el panel de información puede mostrar de una barra de pestañas, áreas de temas, controles de vista de tabla y el menú More Tasks.

Barra de pestañas
Las pestañas proporcionan acceso a distintos aspectos del tema seleccionado en el panel de navegación.

Áreas de temas
Las áreas de temas dividen el panel de información en las secciones que representan los distintos aspectos del tema seleccionado en la pestaña principal o en panel de navegación.

Para sistemas de alta disponibilidad (HA), la pestaña HA Readiness en el tablero System Manager indica si el sistema de alta disponibilidad está listo para realizar una conmutación por error del nodo activo al nodo en espera. Puede hacer clic en **HA Readiness** para navegar a la sección **High Availability** en **HEALTH**.

Uso de las opciones de la vista de tabla
Muchas de las vistas con tablas de elementos contienen controles para filtrar, explorar y ordenar información en la tabla.

Cómo usar controles de tabla comunes:

- Haga clic en el ícono de diamante en el encabezado de una columna para invertir el orden de los elementos de la columna.
- Haga clic en las flechas **<** y **>** en la parte inferior derecha de la vista para moverse hacia atrás o hacia adelante por las páginas. Para ir hasta el comienzo de una secuencia de páginas, haga clic en **|<**. Para ir hasta el final, haga clic en **>|**.
- Use la barra de desplazamiento para ver todos los elementos de una tabla.
- Ingrese texto en el cuadro **Filter By** para buscar o priorizar la visualización de elementos.
- Haga clic en **Update** para actualizar la lista.
- Haga clic en **Reset** para volver a la lista predeterminada.

Menú More Tasks
Algunas páginas proporcionan un menú More Tasks en la parte superior derecha de la vista, que contiene comandos relacionados con la vista actual.

Pie de página

El pie de página de DD System Manager muestra información importante sobre la sesión de administración.

El anuncio muestra la información y los controles que se indican a continuación.

- Nombre de host del sistema.
- DD OS version
- Número de modelo del sistema seleccionado.
- Nombre de usuario y función del usuario actualmente conectado.

Botones de ayuda

Los botones de ayuda muestran un signo ? y aparecen en el anuncio, en el título de muchas áreas del panel de información y en muchos cuadros de diálogo. Haga clic en el botón de ayuda para que se muestre una ventana de ayuda relacionada con la función actual que está usando.

La ventana de ayuda proporciona un botón de contenido y un botón de navegación arriba de la ayuda. Haga clic en el botón de contenido para que se muestre el contenido de la guía y un botón de búsqueda que puede usar para buscar la ayuda. Use los botones de flechas direccionales para avanzar o retroceder en las páginas de los temas de ayuda en orden secuencial.

Acuerdo de licencia para el usuario final

Para ver el Acuerdo de licencia para el usuario final (EULA), seleccione **Maintenance** > **System** > **View EULA**.

Configuración del sistema con el asistente de configuración

Hay dos asistentes, un asistente de configuración de DD System Manager y un asistente de configuración de la interfaz de la línea de comandos (CLI). Los asistentes de configuración lo guían para realizar una configuración simplificada del sistema, para que el sistema esté en funcionamiento rápidamente.

Después de completar la configuración básica con un asistente, puede usar controles de configuración adicionales de DD System Manager y de la CLI para continuar la configuración del sistema.

Nota

En el siguiente procedimiento se describe cómo iniciar y ejecutar el asistente de configuración de DD System Manager después de la configuración inicial del sistema. Para obtener instrucciones acerca de cómo ejecutar los asistentes de configuración durante el arranque del sistema, consulte la *Guía de configuración inicial de Data Domain Operating System*.

Nota

Si desea configurar el sistema para alta disponibilidad (HA), debe ejecutar esta operación mediante el asistente de configuración de la CLI. Para obtener más información, consulte la *Guía de instalación y descripción general de hardware de Data Domain DD9500/DD9800* y la *Guía de configuración inicial de Data Domain Operating System*.

Procedimiento

1. Seleccione **Maintenance** > **System** > **Configure System**.
2. Use los controles que aparecen en la parte inferior del cuadro de diálogo Configuration Wizard para seleccionar qué funciones desea configurar y para avanzar por el asistente. Para ver ayuda sobre una función, haga clic en el ícono de ayuda (signo de interrogación) que se encuentra en la esquina inferior izquierda del cuadro de diálogo.

Página License

La página License muestra todas las licencias instaladas. Haga clic en **Yes** para agregar, modificar o eliminar una licencia, o en **No** para omitir la instalación de licencias.

Configuración de licencia

La sección **Licenses Configuration** permite la adición, modificación y eliminación de licencias de un archivo de licencia. Data Domain Operating System 6.0 y las versiones posteriores son compatibles con licencias de ELMS, lo que permite incluir varias funciones en una carga de archivo de licencia único.

Cuando use el asistente de configuración en un sistema sin licencias configuradas en él, seleccione el tipo de licencia en la lista desplegable y haga clic en el botón **...**. Navegue hasta el directorio donde reside el archivo de licencia y selecciónelo para cargarlo en el sistema.

Tabla 4 Valores de página License Configuration

Elemento	Descripción
Add Licenses	Seleccione esta opción para agregar licencias desde un archivo de licencia.
Replace Licenses	Si las licencias ya están configuradas, la selección **Add Licenses** cambia a **Replace Licenses**. Seleccione esta opción para reemplazar las licencias ya agregadas.
Delete Licenses	Seleccione esta opción para eliminar las licencias que ya están configuradas en el sistema.

Red

La sección **Network** le permite configurar los ajustes de red. Haga clic en **Yes** para configurar los ajustes de red o haga clic en **No** para omitir la configuración de red.

Página General de la red

La página General le permite ajustar opciones de configuración de red que definen cómo participa el sistema en una red IP.

Para configurar estos ajustes fuera del asistente de configuración, seleccione **Hardware** > **Ethernet**.

Tabla 5 Configuración de la página General

Elemento	Descripción
Obtain Settings using DHCP	Seleccione esta opción para especificar que el sistema recopila la configuración de la red de un servidor de protocolos de control dinámico de hosts (DHCP). Cuando configura las interfaces de red, al menos una de las interfaces debe estar configurada para usar DHCP.
Manually Configure	Seleccione esta opción para usar la configuración de red definida en el área Settings de esta página.
Nombre del host	Especifica el nombre de host de la red para este sistema. **Nota** Si elige obtener la configuración de red por medio de DHCP, puede configurar manualmente el nombre de host en **Hardware** > **Ethernet** > **Settings** o con el comando `net set hostname`. Debe configurar manualmente el nombre de host cuando se usa DHCP mediante IPv6.
Nombre del dominio	Especifica el dominio de red al que pertenece el sistema.
Default IPv4 Gateway	Especifica la dirección IPv4 del gateway al que el sistema enviará las solicitudes de red cuando no haya entradas de ruta para el sistema de destino.
Default IPv6 Gateway	Especifica la dirección IPv6 del gateway al que el sistema enviará las solicitudes de red cuando no haya entradas de ruta para el sistema de destino.

Página Network Interfaces

La página Interfaces le permite ajustar opciones de configuración de red que definen cómo participa cada interfaz en una red IP.

Para configurar estos ajustes fuera del asistente de configuración, seleccione select **Hardware** > **Ethernet** > **Interfaces**.

Tabla 6 Configuración de la página Interfaces

Elemento	Descripción
Interfaz	Muestra las interfaces disponibles en el sistema.
Activado	Muestra si cada interfaz está habilitada (casilla de verificación seleccionada) o deshabilitada (no seleccionada). Haga clic en la casilla de verificación para alternar la interfaz entre habilitada y deshabilitada.

Tabla 6 Configuración de la página Interfaces (continuación)

Elemento	Descripción
DHCP	Muestra la configuración de protocolos de control dinámico de hosts (DHCP) de cada interfaz. Seleccione **v4** para conexiones DHCP IPv4, **v6** para conexiones IPv6 o **no** para deshabilitar DHCP.
Dirección IP	Especifica una dirección IPv4 o IPv6 para este sistema. Para configurar la dirección IP, debe configurar DHCP en **No**. **Nota** Los sistemas DD140, DD160, DD610, DD620 y DD630 no admiten IPv6 en la interfaz eth0a (eth0 en sistemas que usan nombres de puertos existentes) o en VLAN creadas en esa interfaz.
Netmask	Especifica la máscara de red para este sistema. Para configurar la máscara de red, debe establecer DHCP en **No**.
Enlace	Muestra si la conexión Ethernet está activa (Yes) o no (No).

Página DNS de la red

La página DNS le permite configurar cómo obtiene direcciones IP el sistema para servidores DNS en un sistema de nombre de dominio (DNS).

Para configurar estos ajustes fuera del asistente de configuración, seleccione **Hardware** > **Ethernet** > **Settings**.

Tabla 7 Configuración de la página DNS

Elemento	Descripción
Obtención de DNS mediante DHCP.	Seleccione esta opción para especificar que el sistema recopila direcciones IP de DNS de un servidor de protocolos de control dinámico de hosts (DHCP). Cuando configura las interfaces de red, al menos una de las interfaces debe estar configurada para usar DHCP.
Manually configure DNS list	Seleccione esta opción cuando desee ingresar manualmente las direcciones IP del servidor DNS.
Botón Add (+)	Haga clic en este botón para que se muestre un cuadro de diálogo en el que puede agregar una dirección IP de DNS a la lista DNS IP Address. Debe seleccionar **Manually configure DNS list** list antes de poder agregar o eliminar direcciones IP de DNS.
Botón Delete (X)	Haga clic en este botón para eliminar una dirección IP de DNS de la lista DNS IP Address. Debe seleccionar la dirección IP que desea eliminar para que se habilite este botón. También debe seleccionar **Manually configure DNS list** antes de poder agregar o eliminar direcciones IP de DNS.
IP Address Checkboxes	Seleccione una casilla de verificación para una dirección IP de DNS que desee eliminar. Seleccione la casilla de verificación

Tabla 7 Configuración de la página DNS (continuación)

Elemento	Descripción
	DNS IP Address cuando desee eliminar todas las direcciones IP. Debe seleccionar **Manually configure DNS list** list antes de poder agregar o eliminar direcciones IP de DNS.

Sistema de archivos

La sección **File System** le permite configurar el almacenamiento para los niveles activo y de nube. Cada nivel tiene una página de asistente propia. También puede crear el sistema de archivos dentro de esta sección. No se puede acceder a las páginas de configuración si el sistema de archivos ya se ha creado.

Cada vez que se muestra la sección **File System** cuando no se ha creado el sistema de archivos, el sistema muestra un mensaje de error. Continúe con el procedimiento para crear el sistema de archivos.

Configuración de las páginas de nivel de almacenamiento

Las páginas de configuración de nivel de almacenamiento le permiten configurar el almacenamiento para cada nivel con licencia en el sistema: Active Tier, Archive Tier y DD Cloud Tier. Cada nivel tiene una página de asistente propia. No se puede acceder a las páginas de configuración de nivel de almacenamiento si el sistema de archivos ya se ha creado.

Configuración del nivel activo

La sección Configuración del nivel activo le permite configurar los dispositivos de nivel de almacenamiento activo. El nivel activo es donde residen los datos de respaldo. Para agregar almacenamiento al nivel activo, seleccione uno o más dispositivos y agréguelos al nivel. La cantidad de dispositivos de almacenamiento que puede agregar está limitada por la cantidad de licencias de capacidad instaladas.

El sistema DD3300 requiere dispositivos de 4 TB para el nivel activo.

Tabla 8 Almacenamiento que se puede agregar

Elemento	Descripción
ID (dispositivo en DD VE)	El identificador del disco, que puede ser cualquiera de los siguientes. • El gabinete y el número de disco (con el formato Enclosure Slot o Enclosure Pack para bandejas DS60) • Un número de dispositivo para un dispositivo lógico, como los que utilizan DD VTL y vDisk. • Un LUN
Disks	Los discos que comprenden el paquete de discos o LUN. Esto no se aplica a las instancias de DD VE.
Modelo	El tipo de bandeja de discos. Esto no se aplica a las instancias de DD VE.
Disk Count	La cantidad de discos en el paquete de discos o LUN. Esto no se aplica a las instancias de DD VE.

Tabla 8 Almacenamiento que se puede agregar (continuación)

Elemento	Descripción
Tamaño del disco (el tamaño en DD VE)	La capacidad de almacenamiento de datos del disco cuando se utiliza en un sistema Data Domain.[a]
Licencias necesarias	La capacidad con licencia necesaria para agregar el almacenamiento al nivel.
Discos fallidos	Los discos fallidos en el paquete de discos o LUN. Esto no se aplica a las instancias de DD VE.
Tipo	SCSI. Esto solo se aplica a instancias de DD VE.

a. La convención de Data Domain para procesar el espacio en disco define un gibibyte como 230 bytes, lo que da como resultado una capacidad de disco diferente que la clasificación del fabricante.

Tabla 9 Valores del nivel activo

Elemento	Descripción
ID (dispositivo en DD VE)	El identificador del disco, que puede ser cualquiera de los siguientes. • El número de disco y gabinete (con el formato Enclosure Slot o Enclosure Pack para bandejas DS60). Esto no se aplica a las instancias de DD VE. • Un número de dispositivo para un dispositivo lógico, como los que utilizan DD VTL y vDisk. • Un LUN
Disks	Los discos que comprenden el paquete de discos o LUN. Esto no se aplica a las instancias de DD VE.
Modelo	El tipo de bandeja de discos. Esto no se aplica a las instancias de DD VE.
Disk Count	La cantidad de discos en el paquete de discos o LUN. Esto no se aplica a las instancias de DD VE.
Tamaño del disco (el tamaño en DD VE)	La capacidad de almacenamiento de datos del disco cuando se utiliza en un sistema Data Domain.[a]
Licencia usada	La capacidad con licencia consumida por el almacenamiento.
Failed Disks	Los discos fallidos en el paquete de discos o LUN. Esto no se aplica a las instancias de DD VE.
Configured	Almacenamiento nuevo o existente. Esto no se aplica a las instancias de DD VE.
Tipo	SCSI. Esto solo se aplica a instancias de DD VE.

a. La convención de Data Domain para procesar el espacio en disco define un gibibyte como 230 bytes, lo que da como resultado una capacidad de disco diferente que la clasificación del fabricante.

Configuración del nivel de archiving

La sección Configuración del nivel de archiving le permite configurar los dispositivos de nivel de almacenamiento para archivo. El nivel de archiving es donde residen los

datos archivados con la función DD Extended Retention. Para agregar almacenamiento al nivel de archiving, seleccione uno o más dispositivos y agréguelos al nivel. La cantidad de dispositivos de almacenamiento que puede agregar está limitada por la cantidad de licencias de capacidad instaladas.

El almacenamiento en niveles de archiving no está disponible en el sistema DD3300 ni en instancias de DD VE.

Tabla 10 Almacenamiento que se puede agregar

Elemento	Descripción
ID	El identificador del disco, que puede ser cualquiera de los siguientes. • El gabinete y el número de disco (con el formato Enclosure Slot o Enclosure Pack para bandejas DS60) • Un número de dispositivo para un dispositivo lógico, como los que utilizan DD VTL y vDisk. • Un LUN
Disks	Los discos que comprenden el paquete de discos o LUN.
Model	El tipo de bandeja de discos.
Disk Count	La cantidad de discos en el paquete de discos o LUN.
Tamaño del disco (el tamaño en DD VE)	La capacidad de almacenamiento de datos del disco cuando se utiliza en un sistema Data Domain. [a].
Licencias necesarias	La capacidad con licencia necesaria para agregar el almacenamiento al nivel.
Discos fallidos	Los discos fallidos en el paquete de discos o LUN.

a. La convención de Data Domain para computar el espacio en disco define un gibibyte como 230 bytes, lo que da como resultado una capacidad de disco diferente que la clasificación del fabricante

Tabla 11 Valores del nivel de archiving

Elemento	Descripción
ID	El identificador del disco, que puede ser cualquiera de los siguientes. • El número de disco y gabinete (con el formato Enclosure Slot o Enclosure Pack para bandejas DS60). Esto no se aplica a las instancias de DD VE. • Un número de dispositivo para un dispositivo lógico, como los que utilizan DD VTL y vDisk. • Un LUN
Disks	Los discos que comprenden el paquete de discos o LUN.
Model	El tipo de bandeja de discos.
Disk Count	La cantidad de discos en el paquete de discos o LUN.
Tamaño del disco (el tamaño en DD VE)	La capacidad de almacenamiento de datos del disco cuando se utiliza en un sistema Data Domain. [a].

Tabla 11 Valores del nivel de archiving (continuación)

Elemento	Descripción
Licencia usada	La capacidad con licencia consumida por el almacenamiento.
Failed Disks	Los discos fallidos en el paquete de discos o LUN.
Configured	Almacenamiento nuevo o existente.

a. La convención de Data Domain para computar el espacio en disco define un gibibyte como 230 bytes, lo que da como resultado una capacidad de disco diferente que la clasificación del fabricante

Configuración de Cloud Tier

La sección Configuración de Cloud Tier le permite configurar los dispositivos de nivel de almacenamiento de nube. Para agregar almacenamiento al nivel de nube, seleccione uno o más dispositivos y agréguelos al nivel. La cantidad de dispositivos de almacenamiento que puede agregar está limitada por la cantidad de licencias de capacidad instaladas.

El sistema DD3300 requiere dispositivos de 1 TB para DD Cloud Tier.

Tabla 12 Almacenamiento que se puede agregar

Elemento	Descripción
ID (dispositivo en DD VE)	El identificador del disco, que puede ser cualquiera de los siguientes. • El gabinete y el número de disco (con el formato Enclosure Slot o Enclosure Pack para bandejas DS60) • Un número de dispositivo para un dispositivo lógico, como los que utilizan DD VTL y vDisk. • Un LUN
Disks	Los discos que comprenden el paquete de discos o LUN. Esto no se aplica a las instancias de DD VE.
Modelo	El tipo de bandeja de discos. Esto no se aplica a las instancias de DD VE.
Disk Count	La cantidad de discos en el paquete de discos o LUN. Esto no se aplica a las instancias de DD VE.
Tamaño del disco (el tamaño en DD VE)	La capacidad de almacenamiento de datos del disco cuando se utiliza en un sistema Data Domain.[a]
Licencias necesarias	La capacidad con licencia necesaria para agregar el almacenamiento al nivel.
Discos fallidos	Los discos fallidos en el paquete de discos o LUN. Esto no se aplica a las instancias de DD VE.
Tipo	SCSI. Esto solo se aplica a instancias de DD VE.

a. La convención de Data Domain para procesar el espacio en disco define un gibibyte como 230 bytes, lo que da como resultado una capacidad de disco diferente que la clasificación del fabricante.

Tabla 13 Valores del nivel de nube

Elemento	Descripción
ID (dispositivo en DD VE)	El identificador del disco, que puede ser cualquiera de los siguientes. • El número de disco y gabinete (con el formato Enclosure Slot o Enclosure Pack para bandejas DS60). Esto no se aplica a las instancias de DD VE. • Un número de dispositivo para un dispositivo lógico, como los que utilizan DD VTL y vDisk. • Un LUN
Disks	Los discos que comprenden el paquete de discos o LUN. Esto no se aplica a las instancias de DD VE.
Modelo	El tipo de bandeja de discos. Esto no se aplica a las instancias de DD VE.
Disk Count	La cantidad de discos en el paquete de discos o LUN. Esto no se aplica a las instancias de DD VE.
Tamaño del disco (el tamaño en DD VE)	La capacidad de almacenamiento de datos del disco cuando se utiliza en un sistema Data Domain.[a]
Licencia usada	La capacidad con licencia consumida por el almacenamiento.
Failed Disks	Los discos fallidos en el paquete de discos o LUN. Esto no se aplica a las instancias de DD VE.
Configured	Almacenamiento nuevo o existente. Esto no se aplica a las instancias de DD VE.
Tipo	SCSI. Esto solo se aplica a instancias de DD VE.

a. La convención de Data Domain para procesar el espacio en disco define un gibibyte como 230 bytes, lo que da como resultado una capacidad de disco diferente que la clasificación del fabricante.

Página Create File System

La página Create File System muestra el tamaño permitido de cada nivel de almacenamiento en el sistema de archivos y le permite activar automáticamente el sistema de archivos después de su creación.

Configuración del sistema

La sección **System Settings** le permite configurar las contraseñas del sistema y la configuración de correo electrónico. Haga clic en **Yes** para configurar los ajustes del sistema o haga clic en **No** para omitir la configuración de ajustes del sistema.

Página System Settings Administrator

La página Administrator le permite configurar la contraseña del administrador y cómo se comunica el sistema con el administrador.

Tabla 14 Configuración de la página Administrator

Elemento	Descripción
Nombre de usuario	El nombre predeterminado del administrador es *sysadmin*. El usuario sysadmin no se puede eliminar ni se le puede cambiar el nombre.
Old Password	Introduzca la contraseña anterior para sysadmin.
Nueva contraseña	Introduzca la nueva contraseña para sysadmin.
Verify New Password	Vuelva a ingresar la nueva contraseña para sysadmin.
Admin Email	Especifique la dirección de correo electrónico a la cual DD System Manager envía los mensajes de correo electrónico de soporte automático y alerta.
Send Alert Notification Emails to this address	Seleccione esta casilla para configurar DD System Manager para que envíe notificaciones de alertas a la dirección de correo electrónico del administrador a medida que ocurran eventos de alerta.
Send Daily Alert Summary Emails to this address	Seleccione esta casilla para configurar DD System Manager para que envíe resúmenes de alertas a la dirección de correo electrónico del administrador al final de cada día.
Send Autosupport Emails to this address	Seleccione esta casilla para configurar DD System Manager para que envíe correos electrónicos de soporte automático del usuario admin, que son informes diarios que documentan la actividad y el estado del sistema.

Página System Settings Email/Location

La página Email/Location le permite configurar el nombre del servidor de correo, controlar qué información del sistema se envía a Data Domain y especificar el nombre de una ubicación para identificar el sistema.

Tabla 15 Configuración de la página Email/Location

Elemento	Descripción
Servidor de correo	Especifica el nombre del servidor de correo que administra los correos electrónicos que recibe y envía el sistema.
Credenciales	Seleccione si desea requerir credenciales para el servidor de correo electrónico.
User Name	Si las credenciales están habilitadas, especifique el nombre de usuario del servidor de correo electrónico.
Password	Si las credenciales están habilitadas, especifique la contraseña del servidor de correo electrónico.
Send Alert Notification Emails to Data Domain	Seleccione esta casilla para configurar DD System Manager para que envíe correos electrónicos de notificación de alertas a Data Domain.
Send Vendor Support Notification Emails to Data Domain	Seleccione esta casilla para configurar DD System Manager para que envíe correos electrónicos de notificación de soporte de proveedores a Data Domain.

Tabla 15 Configuración de la página Email/Location (continuación)

Elemento	Descripción
Location	Use este atributo opcional según sea necesario para registrar la ubicación del sistema. Si especifica una ubicación, esta información se almacena como la ubicación del sistema SNMP.

Protocolo de DD Boost

La sección de configuración de **DD Boost** le permite configurar los ajustes del protocolo de DD Boost. Haga clic en **Yes** para configurar los ajustes del protocolo de DD Boost o haga clic en **No** para omitir la configuración de DD Boost.

Página Storage Unit del protocolo DD Boost

La página Storage Unit le permite configurar unidades de almacenamiento de DD Boost.

Para configurar estas opciones fuera del asistente de configuración, seleccione Protocols DD Boost Storage Units + **Protocols** > **DD Boost** > **Storage Units** > **+ (signo más)** para agregar una unidad de almacenamiento, **el lápiz** para modificar una unidad de almacenamiento o **X** para eliminar una unidad de almacenamiento.

Tabla 16 Configuración de la página Storage Unit

Elemento	Descripción
Storage Unit	El nombre de la unidad de almacenamiento de DD Boost. Puede cambiar este nombre.
Usuario	Para el usuario de DD Boost predeterminado, seleccione un usuario existente o seleccione Create a new Local User e ingrese el nombre de usuario, la contraseña y la función de administración. La función puede ser una de las siguientes: • *Función admin*: Le permite configurar y supervisar todo el sistema Data Domain. • *Función user*: le permiten monitorear sistemas Data Domain y cambiar su propia contraseña. • *Función security*: además de los privilegios de la función user, le permite configurar opciones de directores de seguridad y administrar otros operadores de directores de seguridad. • *Función backup-operator*: Además de los privilegios de la función user, le permite crear instantáneas, importar y exportar cintas a una DD VTL, y mover cintas dentro de una DD VTL. • *Función none*: está diseñada solo para la autenticación de DD Boost, de modo que no podrá supervisar ni configurar un sistema Data Domain. None también es la función principal para las funciones SMT tenant-admin y tenant-user. None también es el tipo de usuario recomendado

Tabla 16 Configuración de la página Storage Unit (continuación)

Elemento	Descripción
	para los propietarios de almacenamiento de DD Boost. La creación de un usuario local nuevo aquí solo permite que ese usuario tenga la función “none”.

Página Fibre Channel del protocolo DD Boost

La página Fibre Channel le permite configurar grupos de acceso de DD Boost mediante Fibre Channel.

Para configurar estas opciones fuera del asistente de configuración, seleccione **Protocols** > **DD Boost** > **Fibre Channel** > **+ (signo más)** para agregar un grupo de acceso, **el lápiz** para modificar un grupo de acceso o **X** para eliminar un grupo de acceso.

Tabla 17 Configuración de la página Fibre Channel

Elemento	Descripción
Configure DD Boost over Fibre Channel	Seleccione la casilla de verificación si desea configurar DD Boost over Fibre Channel.
Nombre del grupo (de 1 a 128 caracteres)	Cree un grupo de acceso. Escriba un nombre único. No se admiten grupos de acceso duplicados.
Initiators	Seleccione uno o más iniciadores. De manera opcional, reemplace el nombre del iniciador introduciendo uno nuevo. Un iniciador es un cliente de respaldo que se conecta al sistema para leer y escribir datos con el protocolo FC (Fibre Channel). Un iniciador específico puede admitir DD Boost mediante FC o DD VTL, pero no ambos.
Dispositivos	Se enumeran los dispositivos que se usarán. Están disponibles en todos los terminales. Un terminal es el destino lógico en el sistema Data Domain con el que se conecta el iniciador.

Protocolo CIFS

La sección de configuración **CIFS Protocol** le permite configurar los ajustes del protocolo CIFS. Haga clic en **Yes** para configurar los ajustes del protocolo CIFS o haga clic en **No** para omitir la configuración de CIFS.

Los sistemas Data Domain utilizan el término MTree para describir directorios. Cuando configura una ruta de directorio, DD OS crea un MTree donde residirán los datos.

Página Authentication del protocolo CIFS

La página Authentication le permite configurar información de Active Directory y Workgroup para el sistema.

Para configurar estos ajustes fuera del asistente de configuración, seleccione **Administration** > **Access** > **Authentication**.

Tabla 18 Configuración de la página Authentication

Elemento	Descripción
Active Directory/Kerberos Authentication	Expanda este panel para habilitar, deshabilitar y configurar la autenticación Active Directory Kerberos.
Workgroup Authentication	Expanda este panel para configurar la autenticación Workgroup.
Autenticación LDAP	Expanda este panel para configurar la autenticación con LDAP.
NIS Authentication	Expanda este panel para configurar la autenticación de NIS.

Página Share del protocolo CIFS

La página Share le permite configurar un nombre de recurso compartido del protocolo CIFS y una ruta de directorio para el sistema.

Para configurar estos ajustes de red fuera del asistente de configuración, seleccione **Protocols** > **CIFS** > **Shares** > **Create**.

Tabla 19 Configuración de la página Share

Elemento	Descripción
Share Name	Escriba un nombre de recurso compartido para el sistema.
Ruta al directorio	Escriba una ruta de directorio para el sistema.
Botón Add (+)	Haga clic en + para ingresar un cliente, un usuario o un grupo del sistema.
el icono de lápiz	Modifique un cliente, un usuario o un grupo.
Botón Delete (X)	Haga clic en X para eliminar un cliente, usuario o grupo seleccionado.

Protocolo NFS

La sección de configuración **NFS Protocol** le permite configurar los ajustes del protocolo NFS. Haga clic en **Yes** para configurar los ajustes del protocolo NFS o haga clic en **No** para omitir la configuración de NFS.

Los sistemas Data Domain utilizan el término MTree para describir directorios. Cuando configura una ruta de directorio, DD OS crea un MTree donde residirán los datos.

Página Export del protocolo NFS

La página Export le permite configurar una ruta de directorio de exportación del protocolo NFS, clientes de red y derivaciones de NFSv4.

Para configurar estos ajustes fuera del asistente de configuración, seleccione **Protocols** > **NFS** > **Create**.

Tabla 20 Configuración de la página Export

Elemento	Descripción
Ruta al directorio	Introduzca un nombre de ruta para la exportación.
Botón Add (+)	Haga clic en + para ingresar un cliente del sistema o una derivación de NFSv4.
el icono de lápiz	Modifique un cliente o una derivación de NFSv4.
Botón Delete (X)	Haga clic en X para eliminar un cliente o una derivación de NFSv4 seleccionados.

Protocolo de DD VTL

La sección de configuración del **protocolo de DD VTL** le permite configurar los ajustes de Data Domain Virtual Tape Library. Haga clic en **Yes** para configurar los ajustes de DD VTL o haga clic en **No** para omitir la configuración de DD VTL.

Página Library del protocolo de VTL

La página Library le permite configurar opciones del protocolo de DD VTL para una biblioteca.

Para configurar estas opciones fuera del asistente de configuración, seleccione **PROTOCOLS** > **VTL** > **Virtual Tape Libraries** > **VTL Service** > **Libraries** > **More Tasks** > **Library** > **Create**.

Tabla 21 Configuración de la página Library

Elemento	Descripción
Library Name	Ingrese el nombre de entre 1 y 32 caracteres alfanuméricos.
Cantidad de unidades	Cantidad de unidades de cinta admitidas.
Drive Model	Seleccione el modelo deseado de la lista desplegable: • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5 (predeterminado) • HP-LTO-3 • HP-LTO-4
Cantidad de slots	Ingrese el número de slots por librería. • Hasta 32,000 slots por biblioteca • Hasta 64,000 slots por sistema • Esto debe ser igual o mayor que el número de unidades.
Number of CAPs	Ingrese el número de puertos de acceso a cartuchos (CAP) (opcional):

Tabla 21 Configuración de la página Library (continuación)

Elemento	Descripción
	• Hasta 100 CAP por biblioteca • Hasta 1000 CAP por sistema
Changer Model Name	Seleccione el modelo deseado de la lista desplegable: • L180 (predeterminado) • RESTORER-L180 • TS3500 • I2000 • I6000 • DDVTL
Starting Barcode	Ingrese el código de barras deseado para la primera cinta, con el formato A990000LA.
Tape Capacity	Ingrese la capacidad de la cinta (opcional). Si no se especifica, la capacidad de la cinta se deriva del último carácter del código de barras.

Página Access Group del protocolo de VTL

La página Access Group le permite configurar opciones del protocolo de DD VTL para un grupo de acceso.

Para configurar estas opciones fuera del asistente de configuración, seleccione **PROTOCOLS** > **VTL** > **Access Groups** > **Groups** > **More Tasks** > **Group** > **Create**.

Tabla 22 Configuración de la página Access Group

Elemento	Descripción
Group Name	Ingrese un nombre único entre uno y 128 caracteres. No se admiten grupos de acceso duplicados.
Initiators	Seleccione uno o más iniciadores. De manera opcional, reemplace el nombre del iniciador introduciendo uno nuevo. Un iniciador es un cliente de respaldo que se conecta a un sistema para leer y escribir datos usando el protocolo Fibre Channel (FC). Un iniciador específico puede admitir DD Boost mediante FC o DD VTL, pero no ambos.
Dispositivos	Se enumeran los dispositivos que se usarán (unidades y cambiador) Están disponibles en todos los terminales. Un terminal es el destino lógico en el sistema Data Domain con el que se conecta el iniciador.

Interfaz de la línea de comandos de Data Domain

La interfaz de la línea de comandos (CLI) es una interfaz guiada por texto que se puede usar en lugar de (o además de) DD System Manager. La mayoría de las tareas de administración se pueden realizar en DD System Manager o con la CLI. En algunos

casos, la CLI ofrece opciones de configuración e informes que todavía no son compatibles en DD System Manager.

Todos los comandos de los sistemas Data Domain que admiten una lista, como una lista de direcciones IP, aceptan entradas separadas por comas, por espacios, o ambos.

La tecla de tabulador puede usarse para realizar lo siguiente.

- Completar una entrada de comando cuando la entrada es única. La finalización con tabulador se admite para todas las palabras clave. Por ejemplo, al ingresar `syst` tabulador `sh` tabulador `st` tabulador se muestra el comando `system show stats`.
- Mostrar la siguiente opción disponible, si no ingresa ningún carácter antes de presionar la tecla de tabulador.
- Mostrar tokens con coincidencia parcial o completar una entrada única, si ingresa caracteres antes de presionar la tecla de tabulador.

La *Guía de referencia de comandos de Data Domain Operating System* proporciona información sobre cada uno de los comandos de la CLI. Hay ayuda en línea disponible que proporciona la sintaxis completa para cada comando.

Inicio de sesión en la CLI

Puede acceder a la CLI a través de una conexión directa al sistema o con una conexión Ethernet mediante SSH o Telenet.

Antes de comenzar

Para usar la CLI, debe establecer una conexión local o remota con el sistema a través de uno de los siguientes métodos.

- Si se está conectando a través de un puerto de la consola en serie del sistema, conecte una consola de terminal al puerto y use la configuración de comunicación: 9600 baudios, 8 bits de datos, sin paridad y 1 bit de parada.
- Si el sistema cuenta con puertos para teclado y monitor, conéctelos a esos puertos.
- Si se está conectando a través de Ethernet, conecte una computadora con software cliente SSH o Telnet a una red Ethernet que pueda comunicarse con el sistema.

Procedimiento

1. Si usa una conexión SSH o Telnet para acceder a la CLI, inicie el cliente SSH o Telnet y especifique la dirección IP o el nombre de host del sistema.

   Para obtener información sobre cómo iniciar la conexión, consulte la documentación del software cliente. El sistema le solicitará su nombre de usuario.

2. Cuando se le solicite, ingrese su nombre de usuario del sistema.
3. Cuando se le solicite, ingrese su contraseña del sistema.

En el siguiente ejemplo se muestra el inicio de sesión SSH a un sistema denominado *mysystem* con software cliente SSH.

```
# ssh -l sysadmin mysystem.mydomain.com
Data Domain OS 5.6.0.0-19899
```

```
Password:
```

Reglas de ayuda en línea de la CLI

La CLI muestra dos tipos de ayuda, ayuda de sintaxis únicamente y ayuda de descripción de comandos que incluye la sintaxis de los comandos. Ambos tipos de ayuda ofrecen funciones que le permiten reducir el tiempo necesario para encontrar la información que necesita.

En las siguientes reglas se describe cómo usar la ayuda de sintaxis únicamente.

- Para que se muestren los comandos de la CLI de nivel superior, escriba un signo de interrogación (`?`) o el comando `help` en la línea de comandos.
- Para que se muestren todas las formas de un comando de nivel superior, escriba el comando sin opciones en la línea o escriba *comando*`?`.
- Para que se muestren todos los comandos que usan una palabra clave específica, escriba `help`*palabra clave* o `?`*palabra clave*.
  Por ejemplo, `? password` muestra todos los comandos del sistema Data Domain que usan el argumento de palabra clave.

En las siguientes reglas se describe cómo usar la ayuda de descripción de comandos.

- Para que se muestren los comandos de la CLI de nivel superior, escriba un signo de interrogación (`?`) o el comando `help` en la línea de comandos.
- Para que se muestren todas las formas de un comando de nivel superior con una introducción, escriba `help`*comando* o `?`*comando*.
- El final de cada descripción de la ayuda se marca con `END`. Presione Intro para regresar a la línea de comandos de la CLI.
- Cuando la descripción completa de la ayuda no cabe en la pantalla, aparece el indicador de dos puntos (:) en la parte inferior de la pantalla. En las siguientes reglas se describe qué puede hacer cuando aparece este indicador.
  - Para desplazarse por la pantalla de ayuda, use las teclas de flecha arriba y abajo.
  - Para salir de la pantalla de ayuda actual y volver a la línea de comandos de la CLI, presione **q**.
  - Para ver la ayuda para explorar la pantalla de ayuda, presione **h**.
  - Para buscar texto en la pantalla de ayuda, escriba una barra (`/`) seguida de un patrón para usar como criterio de búsqueda y presione Intro. Las coincidencias aparecerán resaltadas.

CAPÍTULO 3

Administración de sistemas Data Domain

Este capítulo incluye:

- Descripción general de administración del sistema 58
- Reinicio de un sistema 59
- Encendido o apagado de un sistema 59
- Administración de actualizaciones del sistema 61
- Administración de licencias electrónicas 71
- Administración de almacenamiento del sistema 72
- Administración de conexiones de red 81
- Administración de contraseñas del sistema 105
- Administración de acceso al sistema 106
- Configuración de ajustes del servidor de correo 141
- Administración de configuración de fecha y hora 142
- Administración de propiedades del sistema 143
- Administración de SNMP 143
- Administración de informes de soporte automático 152
- Administración de paquetes de soporte 156
- Administración de coredump 157
- Administración de notificación de alerta 158
- Administración de la entrega de servicio de soporte 166
- Administración de archivos de registro 167
- Administración de la alimentación de sistemas remotos con IPMI 173

Descripción general de administración del sistema

DD System Manager le permite administrar el sistema en el que está instalado DD System Manager.

- Para respaldar la replicación, DD System Manager admite la incorporación de sistemas que ejecutan las dos versiones anteriores, la versión actual y las siguientes dos versiones cuando están disponibles. Para la versión 6.0, DD System Manager admite la incorporación de sistemas para la replicación de las versiones de DD OS 5.6 a 5.7, además de las dos versiones siguientes.

Nota

Al procesar una carga pesada, es posible que un sistema tenga menos respuesta que lo normal. En este caso, es posible que los comandos de administración de DD System Manager o de la CLI tomen más tiempo para completarse. Cuando la duración supera los límites permitidos, se devuelve un error de tiempo de espera agotado, incluso si la operación se ha completado.

En la siguiente tabla, se recomienda el número máximo de sesiones de usuario que admite DD System Manager:

Tabla 23 Cantidad máxima de usuarios que admite DD System Manager

Modelo de sistema	Máximo de usuarios activos	Máximo de usuarios registrados
Modelos de 4 GB[a]	5	10
Modelos de 8 GB[b]	10	15
Modelos de 16 GB y más[c]	10	20

a. Incluye DD140 y DD2200 (4 TB)
b. Incluye DD610 y DD630
c. Incluye DD670, DD860, DD890, DD990, DD2200 (más de 7.5 TB), DD4200, DD4500, DD6300, DD6800, DD7200, DD9300, DD9500 y DD9800

Nota

La configuración inicial de sistema de alta disponibilidad no se puede establecer desde DD System Manager, pero el estado de un sistema de alta disponibilidad ya configurado puede verse desde DD System Manager.

Descripción general de la administración del sistema de alta disponibilidad

La relación de alta disponibilidad entre los dos nodos, uno activo y uno en standby, se configura por medio de las CLI de DDSH.

La configuración inicial se puede ejecutar en cualquiera de los dos nodos, pero solo en uno por vez. Es un prerrequisito de la alta disponibilidad que la interconexión del sistema y el hardware idéntico se establezcan primero en ambos nodos.

Nota

Ambos DDR deben tener hardware idéntico, el cual se validará durante la configuración y el arranque del sistema.

Si la configuración es desde instalaciones nuevas de sistemas, el comando `ha create` debe ejecutarse en el nodo con la licencia instalada. Si la configuración es desde un sistema existente y un sistema de instalación nueva (actualización), entonces debe ejecutarse desde el sistema existente.

Mantenimiento planificado del sistema de alta disponibilidad

La arquitectura de alta disponibilidad proporciona una actualización gradual, lo que reduce el tiempo muerto de mantenimiento para una actualización de DD OS.

Con una actualización gradual, los nodos de alta disponibilidad se actualizan de a uno, de manera coordinada y automática. El nodo en espera se reinicia y se actualiza en primer lugar. El nodo actualizado recientemente asume la función activa por medio de una conmutación por error de alta disponibilidad. Después de la conmutación por error y una vez que se ejecuta la actualización en el segundo nodo, este se reinicia y toma la función del nodo en espera.

Las operaciones de actualización de sistemas que requieren conversión de datos no pueden iniciarse hasta que ambos sistemas se actualizan al mismo nivel y el estado de alta disponibilidad se restaura por completo.

Reinicio de un sistema

Reinicie un sistema cuando un cambio de configuración, como un cambio en la zona horaria, requiera que se reinicie el sistema.

Procedimiento

1. Seleccione **Maintenance** > **System** > **Reboot System**.
2. Haga clic en **OK** para confirmar.

Encendido o apagado de un sistema

Cuando enciende o apaga un sistema, es importante que siga el procedimiento adecuado para preservar el sistema de archivos y la integridad de la configuración.

No use el switch de alimentación del chasis para apagar el sistema. Si lo hace, se impide que el control de alimentación remota use IPMI. Use el comando `system poweroff` en su lugar. El comando `system poweroff` apaga el sistema y la alimentación.

La función IMPI Remote System Power Down no realiza ningún apagado ordenado de DD OS. Use esta función únicamente si el comando `system poweroff` no se ejecuta correctamente.

Para los sistemas de alta disponibilidad, se requiere una conexión a ambos nodos.

Complete los pasos siguientes para apagar un sistema Data Domain.

Procedimiento

1. Verifique que se hayan detenido las operaciones de I/O en el sistema.

   Ejecute los siguientes comandos:

   - `cifs show active`
   - `nfs show active`
   - `system show stats view sysstat interval 2`
   - `system show perf`

2. Para los sistemas de alta disponibilidad, verifique el estado de la configuración de alta disponibilidad.

   Ejecute el siguiente comando:
   `ha status`

```
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                  Node ID   Role      HA State
-------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com       0       active    online
apollo-ha3a-p1.emc.com       1       standby   online
-------------------------- --------- --------- --------
```

Nota

Este es un ejemplo de salida de un sistema en buen estado. Si se desea apagar el equipo para reemplazar un componente fallido, se degradará el estado del sistema de alta disponibilidad y uno o ambos nodos se mostrarán offline para el estado de alta disponibilidad.

3. Ejecute el comando `alerts show current`. Para los pares de alta disponibilidad, ejecute el comando en el nodo activo primero y, a continuación, en el nodo en espera.
4. Para los sistemas de alta disponibilidad, ejecute el comando `ha offline` si el sistema está en un estado de alta disponibilidad con ambos nodos en línea. Si el estado de alta disponibilidad está degradado, omita este paso.
5. Ejecute el comando `system poweroff`. Para los pares de alta disponibilidad, ejecute el comando en el nodo activo primero y, a continuación, en el nodo en espera.

```
# system poweroff

Continue? (yes|no|?) [no]: yes
```

   Este comando lleva a cabo automáticamente un apagado ordenado de los procesos del sistema operativo DD y está disponible para usuarios administrativos únicamente.
6. Quite los cables de alimentación de los suministros de energía en la controladora o las controladoras.
7. Verifique que el LED de alimentación azul esté apagado en la controladora o las controladoras para confirmar que el sistema esté apagado.

   Después de apagar la controladora, apague cualquier bandeja de expansión externa (ES30, DS60, FS15).

Encendido del sistema

Restaure la alimentación al sistema Data Domain una vez finalizado el tiempo de inactividad del sistema.

Procedimiento

1. Encienda las bandejas de expansión antes de encender la controladora Data Domain. Espere aproximadamente 3 minutos después de encender todas las bandejas de expansión.

Nota

Una controladora es el chasis y el almacenamiento interno. Un *sistema Data Domain* hace referencia a lcontroladoraor y cualquier almacenamiento externo opcional.

2. Conecte el cable de alimentación de la controladora y, si hay un botón de encendido en la controladora, presiónelo (como se muestra en la *Guía de instalación y configuración* del sistema Data Domain). En el caso de sistemas de alta disponibilidad, encienda primero el nodo activo y luego el nodo en espera.

Nota

Algunos dispositivos de Data Domain no tienen un botón de encendido tradicional, sino que están diseñados para estar "siempre encendidos" y se encenderán al conectarlos a la alimentación CA.

3. Para los sistemas de alta disponibilidad, verifique el estado de la configuración de alta disponibilidad.

   Ejecute el siguiente comando:
   `ha status`

```
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                  Node ID   Role      HA State
-------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com       0       active    online
apollo-ha3a-p1.emc.com       1       standby   offline
-------------------------- --------- --------- --------
```

4. Para los sistemas de alta disponibilidad, si uno de los nodos se muestra como offline, ejecute el comando `ha online` en ese nodo para restaurar la configuración de alta disponibilidad.
5. Verifique que el dispositivo Data Domain se haya iniciado completamente y que el sistema operativo se esté ejecutando. Esto se puede hacer con la consola del sistema o desde una sesión SSH al sistema Data Domain. El sistema está en marcha cuando se puede iniciar sesión en el sistema.
6. Ejecute el comando `alerts show current`. Para los pares de alta disponibilidad, ejecute el comando en el nodo activo primero y, a continuación, en el nodo en espera.

Administración de actualizaciones del sistema

Para actualizar un sistema DD OS, debe verificar que haya suficiente espacio para el software nuevo en el sistema de destino, transferir el software al sistema para que se actualice y, a continuación, iniciar la actualización. Para un sistema de alta disponibilidad, transfiera el software al nodo activo e inicie la actualización desde el nodo activo.

Para los sistemas de alta disponibilidad, utilice la dirección IP flotante para acceder a DD System Manager y realizar actualizaciones de software.

⚠ PRECAUCIÓN

DD OS 6.0 utiliza la versión 3 de Secure Remote Support (ESRSv3). La actualización de un sistema que ejecuta DD OS 5.X a DD OS 6.0 elimina la configuración de ConnectEMC existente del sistema. Una vez completada la actualización, vuelva a configurar ConnectEMC manualmente.

Si el sistema utiliza certificados firmados por MD5, vuelva a generar los certificados con un algoritmo hash más sólido durante el proceso de actualización.

Actualización con pocas interrupciones
La función de actualización con pocas interrupciones (MDU) le permite actualizar los componentes de software específicos o aplicar reparaciones de errores sin necesidad de realizar un reinicio del sistema. Se interrumpen solamente los servicios que dependen de los componentes que se están actualizando, por lo que la función MDU puede evitar tiempo fuera considerable durante determinadas actualizaciones de software.

No todos los componentes de software cumplen los requisitos para una actualización con pocas interrupciones; esos componentes se deben actualizar como parte de una actualización de software habitual del sistema DD OS. Una actualización de software DD OS utiliza un gran r/MIN (paquete de actualización), que lleva a cabo las acciones de actualización para todos los componentes de DD OS. MDU utiliza paquetes más pequeños de componentes, que actualizan componentes de software específicos de forma individual.

Verificación de firma de r/min
La verificación de firma de r/min valida los RPM de Data Domain que usted descarga para la actualización. Si no se ha manipulado el RPM, la firma digital es válida, y el RPM se puede usar de forma habitual. Si el RPM ha sido alterado, los daños invalidan la firma digital, y DD OS rechaza el RPM. Se muestra un mensaje de error adecuado.

Nota

Al actualizar de 5.6.0.x a 6.0, actualice el sistema de 5.6.0.x a 5.6.1.x (o posterior) antes de actualizar a 6.0.

Software de soporte
DD OS 6.1 presenta un tipo de paquete de software llamado software de soporte. El equipo de ingeniería de soporte de Data Domain proporciona el software de soporte para enfrentar problemas específicos. De forma predeterminada, el sistema Data Domain no permite que se instale software de soporte en el sistema. Para obtener más información acerca del software de soporte, póngase en contacto con el servicio de soporte.

Descripción general y listas de verificación previas a la actualización

Antes de realizar cualquier actualización de DD OS, debe revisar los elementos de estas listas de verificación. Si lo hace, puede simplificar el proceso de actualización y evitar posibles dificultades.

Tareas manuales previas a la actualización

⚠ PRECAUCIÓN

Si no se realizan las tareas de esta sección, puede producirse una falla durante la actualización.

Estas son las tareas que debe planear antes de la actualización. Estas tareas no se realizan automáticamente durante ningún proceso.

1. Reinicie el sistema Data Domain. En los sistemas de HA, siga las instrucciones de reinicio que se describen en Consideraciones de actualización para sistemas de alta disponibilidad en la página 64 después de realizar el resto de las comprobaciones en esta sección.
2. Compruebe las alertas actuales; esto puede revelar muchas fallas en los discos y otro hardware que se deben abordar antes de la actualización:

   ```
   # alert show current
   ```

3. Compruebe que las configuraciones de registro de `config.net.*`, las de `crontab` y las relacionadas con las redes sean válidas.

   Por ejemplo, utilice la operación `reg show config.net` y compruebe si `noauto.enabled`, `noauto.speed` y `noauto.full_duplex` se establecieron correctamente. Esto permitirá que la red negocie la velocidad. Además, compruebe si `.use_dhcp=true`, porque esto permitirá la configuración rápida no solo de la dirección IP y la máscara de red, sino también de la puerta de enlace.

   Esta comprobación es importante porque, si estos elementos están mal configurados, el reinicio puede causar que la red no esté disponible.
4. Compruebe si todas las interfaces de red están en funcionamiento y tienen direcciones IP apropiadas, y si se puede acceder al sistema Data Domain a través de Data Domain System Manager o cualquier otro cliente en uso:

   ```
   # net show
   ```

5. Compruebe los estados de disco y no realice la actualización si el sistema Data Domain no cuenta con suficientes repuestos o tiene discos que se muestran en estado ausente, fallido o de reconstrucción:

   ```
   # disk show state

   # disk show reliability-data
   ```

6. Compruebe la confiabilidad del disco y reemplace los discos que tengan más de 50 sectores reubicados:

   ```
   # disk show reliability-data
   ```

7. Compruebe el estado del gabinete:

   ```
   # enclosure show all
   ```

   Debe mostrar “OK” para todos los dispositivos.
8. Compruebe si la topología del gabinete es correcta:

   ```
   # enclosure show topology
   ```

   Compruebe también si aparece algún error con un asterisco (*) junto al campo **enc.ctrl.port**. Además, busque en el campo **Error Message** si aparecen errores como `"A possible problem was detected for this shelf controller or the cable connected to it."`.
9. Compruebe que la asignación de puertos del dispositivo sea correcta:

   ```
   # system show hardware
   ```

10. Compruebe la velocidad de vínculo de los puertos conectados:

    ```
    # system show ports
    ```

11. Compruebe el estado del sistema de archivos para determinar que el sistema de archivos esté habilitado y se ejecute normalmente:

    ```
    # filesys status
    ```

12. Compruebe si la limpieza del sistema de archivos se está ejecutando y, si es así, deténgala:

    ```
    # filesys clean status
    ```

    ```
    # filesys clean stop
    ```

13. Si la replicación está habilitada, compruebe su estado:

    ```
    # replication status
    ```

14. Si el sistema está en una configuración de clúster, compruebe si el clúster está en funcionamiento:

    ```
    # cluster show config
    ```

15. En un sistema habilitado con DD Cloud Tier, asegúrese de que no haya movimiento de datos:

    ```
    # data-movement status
    ```

    ```
    # data-movement stop all
    ```

16. Compruebe si la limpieza de la nube se está ejecutando y, si es así, deténgala:

    ```
    # cloud clean status
    ```

    ```
    # cloud clean stop
    ```

17. Compruebe si hay alguna actividad de respaldo y restauración en curso y, de ser así, deténgala:

    ```
    # system show stats
    ```

18. Compruebe el registro `kern.info` y, si observa fallas frecuentes en el hardware, póngase en contacto con el soporte de Data Domain para inspeccionar el sistema antes de realizar la actualización.

    ```
    # log view debug/platform/kern.info
    ```

19. Ejecute un informe de soporte automático justo antes de realizar la actualización de DD OS para determinar si es necesario abordar cualquier problema restante:

    ```
    # autosupport send <your_email_address>
    ```

Consideraciones de actualización para sistemas de alta disponibilidad

Los sistemas de alta disponibilidad requieren determinados pasos únicos antes de iniciar la operación de actualización y una verificación posterior única después de que se completa la actualización.

⚠ PRECAUCIÓN

Realice las comprobaciones manuales descritas en Tareas manuales previas a la actualización en la página 62 antes de reiniciar el sistema de HA.

Cuando actualice un sistema de HA, cargue el paquete RPM de actualización al nodo activo.

1. El sistema de alta disponibilidad debe estar en un estado de alta disponibilidad, con ambos nodos en línea antes de realizar la actualización de DD OS. Ejecute el comando `ha status` para verificar el estado del sistema de alta disponibilidad.

```
# ha status
HA System Name: apollo-ha3a.emc.com
```

```
HA System Status: highly available
Node Name                  Node ID   Role      HA State
-------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com       0       active    online
apollo-ha3a-p1.emc.com       1       standby   online
-------------------------- --------- --------- --------
```

2. Reinicie el nodo en espera (nodo 1).
3. Ejecute el comando `ha status` para verificar que el estado del sistema de HA se muestre como `highly available` después de que se reinicie el nodo en espera.
4. Ejecute el comando `ha failover` para iniciar una conmutación por error del nodo activo al nodo en espera.
5. Ejecute el comando `ha status` para verificar que el nodo 1 sea el nodo activo y el nodo 0 sea el nodo en espera.

```
# ha status
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                  Node ID   Role      HA State
-------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com       0       standby   online
apollo-ha3a-p1.emc.com       1       active    online
-------------------------- --------- --------- --------
```

6. Reinicie el nodo en espera (nodo 0).
7. Ejecute el comando `ha status` para verificar que el estado del sistema de HA se muestre como `highly available` después de que se reinicie el nodo en espera.
8. Ejecute el comando `ha failover` para iniciar una conmutación por error del nodo activo al nodo en espera.
9. Ejecute el comando `ha status` para verificar que el nodo 0 sea el nodo activo y el nodo 1 sea el nodo en espera.

```
# ha status
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                  Node ID   Role      HA State
-------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com       0       active    online
apollo-ha3a-p1.emc.com       1       standby   online
-------------------------- --------- --------- --------
```

Inicie la actualización desde el nodo activo. DD OS reconoce automáticamente el sistema de alta disponibilidad y lleva a cabo el procedimiento de actualización en ambos nodos. La actualización de HA se ejecuta en la siguiente secuencia:

1. El nodo en espera se actualiza y, a continuación, se reinicia.
2. Después de completar el reinicio, el sistema de HA inicia una conmutación por error y el nodo en espera asume la función del nodo activo.
3. Se actualiza el nodo activo original y, a continuación, se reinicia y permanece como el nodo en espera.

Después de actualizar ambos nodos, el sistema no realiza otra conmutación por error para devolver los nodos a su configuración original.

Una vez completado el procedimiento de actualización, ejecute el comando `ha status` nuevamente para verificar que el sistema esté en un estado de alta disponibilidad y que ambos nodos estén en línea.

Opcionalmente, ejecute el comando `ha failover` para devolver los nodos a las funciones que tenían antes de la actualización.

Tareas automáticas que se realizan antes de la actualización

Comprender estos aspectos de una actualización de DD OS asegura un proceso más fluido.

La versión de DD OS en su sistema Data Domain antes de la actualización realiza estas tareas:

1. Determinar si la inicialización de la replicación está en curso. Si es así, la actualización no continuará.
2. Inspeccionar todas las recopilaciones y firmas en el archivo .rpm para garantizar la integridad y el origen del paquete. Si la firma no es válida, la actualización no continuará.
3. Determinar si la actualización de la versión anterior de DD OS a la nueva es permisible. Los sistemas Data Domain que ejecutan DD OS 5.7.x o 6.0.x pueden actualizarse directamente a 6.1. Esta restricción se debe a la firma de RPM. Generalmente, no se permite una actualización en estas circunstancias:
   a. La actualización se realiza entre las mismas versiones, como de 6.0.0.1 a 6.0.0.4. (Esto se puede invalidar en algunas circunstancias específicas; consulte a su representante de soporte de Data Domain para obtener más detalles).
   b. La actualización se realiza a una versión inferior, como de 6.0 a 5.7.
   c. La actualización supera las dos familias de funciones, como de 5.5 a 6.0.
4. Determinar si se desconoce cualquier punto de montaje de NFS. Si se desconoce cualquier punto de montaje de NFS, la actualización no continuará.
5. Determinar si la actualización anterior, si hubo alguna, se completó correctamente. Si la actualización anterior no se realizó correctamente o no se completó, la actualización actual no continuará.

Tareas automáticas que realiza el script de actualización (en el archivo .rpm) antes de la actualización

Estas pruebas preceden al proceso de actualización real en el sistema Data Domain:

1. Determinar si hay dos tipos diferentes de tarjetas NVRAM presentes.
2. Comprobar el tamaño de la partición `/ddr` y de la partición `/` (raíz) para verificar la utilización del espacio.
3. Comprobar la versión de OST.
4. Determinar si está conformado el metagrupo de RAID. Si no lo está, no se inicia el proceso de actualización.
5. Determinar el espacio disponible para el sistema de archivos.
6. Determinar si hay suficiente espacio disponible para la actualización.
7. Comprobar la versión de la VTL, si hay una presente.
8. Determinar si el sistema de archivos está habilitado y, si no lo está, habilitarlo.
9. Determinar si la VTL está habilitada.
10. Verificar los pools de VTL para asegurar que se puedan convertir en MTrees.
11. Determinar si hay suficiente espacio disponible de VTL.
12. Asegurar que los números de pools de VTL y MTrees no superen los 100. (Esta comprobación se aplica desde la versión 5.0 de DD OS).

13. Determinar si todos los discos de dg0 están ubicados en la unidad principal. De lo contrario, el proceso de actualización no comienza y se debe solucionar el problema.
14. Comprobar si se ha configurado ConnectEMC. Si es así, se muestra un mensaje de advertencia que informa al cliente que debe reconfigurar ConnectEMC después de la actualización.

Además de estas comprobaciones, el sistema determina si el sistema de archivos se puede apagar correctamente y sin problemas. Si el sistema de archivos no se puede apagar de manera correcta, el proceso de actualización se detendrá.

Condiciones que impiden el proceso de actualización

Varias condiciones pueden provocar la detención del proceso de actualización:

- El sistema Data Domain no está en un estado funcional. Por ejemplo:
  - El almacenamiento es funcionalmente deficiente, por ejemplo, falta un gabinete.
  - El sistema de archivos no se apagó correctamente, lo que generó un volcado de core.
  - La actualización anterior no se completó correctamente.
- El uso del espacio es problemático. Por ejemplo:
  - La partición `/` (raíz) o la partición `/ddr` están llenas con archivos de registro, volcados de core, etc.
  - No hay suficiente espacio de almacenamiento disponible para realizar la actualización de datos.
- El sistema Data Domain no está configurado correctamente. Por ejemplo, los puntos de montaje de NFS se crearon manualmente en el directorio raíz.
- Los nombres de las unidades de almacenamiento no se pueden convertir en nombres de MTree. Para poder convertirse en nombres de MTree, los nombres de las unidades de almacenamiento deben contener solo letras mayúsculas y minúsculas (a-z, A-Z), dígitos (0-9) y guion bajo (_), y no deben tener más de 50 caracteres.

El objetivo de comprobar estas condiciones es evitar que se produzcan o propaguen anomalías del sistema de archivos o actualizaciones problemáticas. Las condiciones también se aplican en las actualizaciones que involucran a sistemas de partners de destino y de origen en la replicación. Una actualización fallida o una anomalía del sistema de archivos en un sistema Data Domain que funciona como origen de replicación no provocan daños en el sistema de archivos de un sistema Data Domain que actúa como destino de replicación.

Visualización de paquetes de actualización en el sistema

DD System Manager le permite ver y administrar hasta cinco paquetes de actualización en un sistema. Antes de poder actualizar un sistema, debe descargar un paquete de actualización del sitio de servicio de soporte en línea a una computadora local y, a continuación, cargarlo en el sistema de destino.

Procedimiento

1. Seleccione **Maintenance** > **System**.
2. De manera opcional, seleccione un paquete de actualización y haga clic en **View Checksum** para mostrar las sumas de comprobación MD5 y SHA256 del paquete de actualización.

Resultados

Para cada paquete almacenado en el sistema, DD System Manager muestra el nombre de archivo, el tamaño y la fecha de la última modificación en la lista titulada: Upgrade Packages Available on Data Domain System.

Obtención y verificación de paquetes de actualización

Puede usar DD System Manager para ubicar archivos de paquetes de actualización en el sitio web de servicio al cliente de Data Domain y cargar copias de esos archivos en un sistema.

Nota

Puede usar FTP o NFS para copiar un paquete de actualización en un sistema. DD System Manager se limita a la administración de 5 paquetes de actualización de sistemas, pero no hay restricciones más que limitaciones de espacio al administrar los archivos directamente en el directorio `/ddvar/releases`. FTP está deshabilitado de forma predeterminada. Para usar NFS, `/ddvar` se debe exportar y montar desde un host externo).

Procedimiento

1. Seleccione **Maintenance** > **System**.
2. Para obtener un paquete de actualización, haga clic en el vínculo **EMC Online Support**, haga clic en Downloads y use la función de búsqueda para ubicar el paquete que recomienda el personal de soporte para su sistema. Guarde el paquete de actualización en la computadora local.
3. Verifique que no haya más de cuatro paquetes en la lista Upgrade Packages Available on Data Domain System.

   DD System Manager puede administrar hasta cinco paquetes de actualización. Si aparecen cinco paquetes en la lista, elimine al menos uno antes de cargar el paquete nuevo.
4. Haga clic en **Upload Upgrade Package** para iniciar la transferencia del paquete de actualización al sistema de destino.
5. En el cuadro de diálogo Upload Upgrade Package, haga clic en **Browse** para abrir el cuadro de diálogo Choose File to Upload. Vaya a la carpeta donde se descargó el archivo, selecciónelo y haga clic en **Open**.
6. Haga clic en **OK**.

   Aparecerá un cuadro de diálogo del progreso de carga. Cuando se complete la carga, el archivo descargado (con una extensión .rpm) aparecerá en la lista titulada: Upgrade Packages Available on Data Domain System.
7. Para verificar la integridad del paquete de actualización, haga clic en **View Checksum** y compare la suma de comprobación calculada que se muestra en el cuadro de diálogo con la suma de comprobación autorizada en el sitio de soporte en línea.
8. Para iniciar manualmente una comprobación previa de actualización, haga clic en **Upgrade Precheck**.

Actualización de un sistema Data Domain

Cuando hay un archivo de paquete de actualización presente en un sistema, puede usar DD System Manager para realizar una actualización con ese archivo de paquete de actualización.

Antes de comenzar

Lea las notas de versión de DD OS para obtener instrucciones de actualización completas y cobertura de todos los problemas que pueden afectar la actualización.

El siguiente procedimiento describe cómo iniciar una actualización mediante DD System Manager. Cierre todas las sesiones de la CLI de Data Domain en el sistema donde se realizará la actualización antes de usar DD System Manager para actualizar el sistema.

Nota

Los archivos de actualización del sistema usan la extensión de archivo .rpm. En este tema se da por hecho que está actualizando el sistema operativo DD únicamente. Si realiza cambios de hardware, como agregar, reemplazar o mover tarjetas de interfaz, debe actualizar la configuración de DD OS para que se ajuste a los cambios de hardware.

Procedimiento

1. Inicie sesión en DD System Manager en el sistema donde se realizará la actualización.

   Nota

   En la mayoría de las versiones, se permiten actualizaciones desde hasta dos versiones principales anteriores. Para la versión 6.0, se permiten actualizaciones a partir de las versiones 5.6 y 5.7.

   Nota

   Según las recomendaciones de las notas de versión, reinicie el sistema Data Domain antes de realizar una actualización para verificar que el hardware esté en un estado limpio. Si se descubren problemas durante el reinicio, resuélvalos antes de comenzar la actualización. Para realizar una actualización MDU, es posible que no sea necesario reiniciar.

2. Seleccione **Data Management** > **File System** y verifique que el sistema de archivos esté habilitado y en funcionamiento.
3. Seleccione **Maintenance** > **System**.
4. En la lista Upgrade Packages Available on Data Domain System, seleccione el paquete que desee usar para la actualización.

   Nota

   Debe seleccionar un paquete de actualización para una versión más reciente del sistema operativo DD. DD OS no admite cambiar a versiones anteriores.

5. Haga clic en **Perform System Upgrade**.

Aparecerá el cuadro de diálogo System Upgrade y mostrará información acerca de la actualización y una lista de los usuarios que están conectados actualmente al sistema que se va a actualizar.

6. Verifique la versión del paquete de actualización y haga clic en **OK** para continuar con la actualización.

   El cuadro de diálogo System Upgrade mostrará el estado de actualización y el tiempo restante.

   Al realizar una actualización del sistema, debe esperar a que se complete la actualización para poder usar DD System Manager para administrar el sistema. Si se reinicia el sistema, la actualización puede continuar después del reinicio y DD System Manager mostrará el estado de actualización después del inicio de sesión. Si es posible, deje el cuadro de diálogo System Upgrade abierto hasta que se complete la actualización o se apague el sistema. Al realizar una actualización a la versión 5.5 de DD OS a una versión más reciente, y si la actualización del sistema no requiere un apagado, aparecerá un vínculo de inicio de sesión cuando se complete la actualización.

   Nota

   Para ver el estado de una actualización con la CLI, ingrese el comando `system upgrade status`. Los mensajes de registro de la actualización se almacenan en `/ddvar/log/debug/platform/upgrade-error.log` y `/ddvar/log/debug/platform/upgrade-info.log`.

7. Si se apaga el sistema, debe desconectar la alimentación AC del sistema para borrar la configuración anterior. Desconecte todos los cables de alimentación durante 30 segundos y, a continuación, vuelva a conectarlos. El sistema se encenderá y se reiniciará.
8. Si el sistema no se enciende automáticamente y hay un botón de encendido en el panel frontal, presiónelo.

Requistos posteriores

Los siguientes requisitos pueden aplicarse después de completar una actualización.

- Para ambientes que usan certificados autofirmados SHA-256, los certificados deben volver a generarse manualmente después de que se completa el proceso de actualización, y debe volver a establecerse la confianza con sistemas externos que se conectan al sistema Data Domain.
  1. Ejecute el comando **`adminaccess certificate generate self-signed-cert regenerate-ca`** para volver a generar los certificados autofirmados de host y CA. La regeneración de los certificados rompe las relaciones de confianza existentes con sistemas externos.
  2. Ejecute el comando **`adminaccess trust add host`** ***`hostname`*** **`type mutual`** para restablecer una relación de confianza mutua entre el sistema Data Domain y el sistema externo.
- Si el sistema muestra los puertos FC existentes o configurados con información de WWPN o WWNN incompleta, o informa que no se encuentra instalado ningún controlador para la HBA (Host Bus Adapter) de FC, ejecute el comando `scsitarget endpoint enable all`.

Notas sobre la replicación

Con la replicación de recopilaciones, ningún archivo está visible en el sistema Data Domain de destino si no se completa la replicación antes de iniciar la actualización.

Después de la actualización, espere hasta que se complete la replicación para ver los archivos en el destino.

Notas sobre ConnectEMC

En esta versión, ConnectEMC se ha modificado para admitir la puerta de enlace de Secure Remote Service Virtual Edition (Secure Remote Services VE). Este cambio requiere una reconfiguración del sistema Data Domain a ConnectEMC después de la actualización.

Nota

ConnectEMC solamente funciona con Service Remote Services VE (V3) y no permite enviar correos electrónicos con versiones anteriores de Service Remote Services o por su cuenta. Si ConnectEMC se ha utilizado con versiones anteriores de DD OS (por ejemplo, 5.7 o 5.6), se deberá volver a realizar la configuración del servidor de Service Remote Services VE, dado que se quitó durante el proceso de actualización debido a la actualización de la tecnología.

Nota

Si utiliza una puerta de enlace de Service Remote Services anterior, la puerta de enlace de Service Remote Services VE deberá implementarse para permitir comunicaciones seguras.

Durante la actualización, si ConnectEMC se detecta como configurado, la configuración existente se eliminará. Además, si el método de notificación de soporte se configura como ConnectEMC para enviar mensajes de eventos a la empresa, cambiará a correo electrónico. Después de la actualización, puede volver a configurar ConnectEMC con el nuevo comando de ConnectEMC: `support connectemc device register`.

Después de configurar ConnectEMC, habilite ConnectEMC con `support notification method set connectemc`.

Eliminación de un paquete de actualización

Es posible cargar un máximo de cinco paquetes de actualización a un sistema con DD System Manager. Si el sistema que está actualizando contiene cinco paquetes de actualización, debe eliminar al menos uno para poder actualizar el sistema.

Procedimiento

1. Seleccione **Maintenance** > **System**.
2. En la lista Upgrade Packages Available de este sistema Data Domain, seleccione el paquete que desee quitar. Se puede eliminar un paquete a la vez.
3. Haga clic en **Remove Upgrade Package**.

Administración de licencias electrónicas

Agregue y elimine licencias electrónicas desde el sistema Data Domain. Consulte las *Notas de la versión de Data Domain Operating System* correspondientes para obtener información más actualizada sobre las características del producto, las actualizaciones de software y las guías de compatibilidad de software, además de detalles acerca de los productos, las licencias y los servicios.

Administración de licencias de sistemas de alta disponibilidad

La alta disponibilidad es una función con licencia, y la clave de licencia del sistema se registra siguiendo los mismos pasos que se siguen para agregar cualquier otra licencia al sistema DD.

Un sistema se configurará como activo-standby, y un nodo se designará "en standby". Se requerirá un solo conjunto de licencias en lugar de licencias individuales para cada nodo. Durante el failover, las licencias en un nodo producirán un failover en el otro nodo.

Administración de almacenamiento del sistema

Las funciones de administración de almacenamiento del sistema le permiten ver el estado y la configuración del espacio de almacenamiento, hacer que una luz LED del disco parpadee para facilitar la identificación del disco y cambiar la configuración de almacenamiento.

Nota

Todo el almacenamiento conectado o que utiliza el sistema de HA de dos nodos tipo activo-en espera puede verse como un solo sistema.

Usar la CLI para calcular el espacio de almacenamiento utilizable

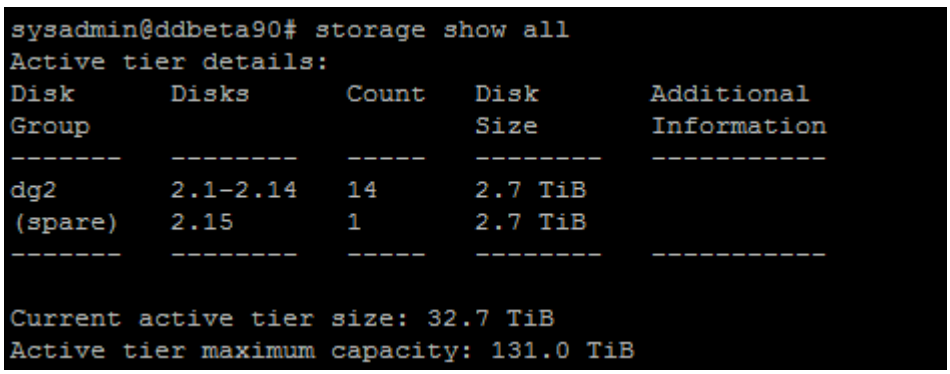
Los siguientes valores son necesarios para calcular el almacenamiento utilizable en un sistema Data Domain después de calcular la sobrecarga de RAID:

- *N* = cantidad de discos en uso en el grupo de discos (dg)
- *C* = capacidad de cada disco después del formateo
- *R* = 2 (cantidad de discos utilizados para la paridad de RAID 6)

Este cálculo no funciona para el almacenamiento de nivel de caché, ya que los discos de nivel de caché no cuentan con protección RAID.

Ejecute el comando `storage show all` para obtener los valores de *N* y *C*.

Figura 4 Ejemplo de comando `storage show all`



En este ejemplo, hay 14 discos en uso en dg2 y cada disco tiene una capacidad de 2,7 TIB, por lo tanto, *N* = 14 y *C* = 2,7 TIB.

Utilice la fórmula (*N* - *R*) x *C* para obtener la capacidad útil. En este ejemplo, la ecuación es (14 - 2) x 2,7 TiB.

12 x 2,7 TiB = 32,4 TiB o 35,6 TB.

Nota

Es posible que el valor calculado no coincida exactamente con la salida del comando `storage show all` debido a la forma en la que los valores de capacidad se redondean para la visualización. El comando `disk show hardware` muestra la capacidad del disco con lugares decimales adicionales.

Visualización de información de almacenamiento del sistema

El área Storage Status muestra el estado actual del almacenamiento (por ejemplo, Operational o Non-Operational) y el estado de la migración de almacenamiento. Debajo del área Status hay pestañas que organizan cómo se presenta el inventario de almacenamiento.

Procedimiento

1. Para mostrar el estado de almacenamiento, seleccione **Hardware** > **Storage**.
2. Si aparece un vínculo de alertas después el estado de almacenamiento, haga clic en él para ver las alertas de almacenamiento.
3. Si el estado de la migración de almacenamiento no tiene licencia, puede hacer clic en **Add License** para agregar la licencia para esta función.

Pestaña Overview

En la pestaña Overview se muestra información de todos los discos incluidos en el sistema Data Domain seleccionado, organizada por tipo. Las categorías que se muestran dependen del tipo de configuración de almacenamiento en uso.

En la sección Overview se muestra el almacenamiento descubierto en una o más de las siguientes secciones.

- Active Tier
  Los discos en el nivel activo están marcados como utilizables por el sistema de archivos. Los discos se enumeran en dos tablas: Disks in Use y Disks Not in Use.
- Nivel de retención
  Si está instalada la licencia opcional de Data Domain Extended Retention (anteriormente DD Archiver), esta sección muestra los discos que están configurados para el almacenamiento de DD Extended Retention. Los discos se enumeran en dos tablas: Disks in Use y Disks Not in Use.
- Nivel de caché
  Los discos SSD en el nivel de caché se utilizan para almacenar metadatos en caché. El sistema de archivos no puede usar los discos SSD. Los discos se enumeran en dos tablas: Disks in Use y Disks Not in Use.
- Cloud Tier
  Los discos en el nivel de nube se usan para almacenar los metadatos para los datos que residen en almacenamiento de nube. El sistema de archivos no puede usar los discos. Los discos se enumeran en dos tablas: Disks in Use y Disks Not in Use.
- Addable Storage
  Para los sistemas con gabinetes opcionales, esta sección muestra los discos y gabinetes que se pueden agregar al sistema.
- Failed/Foreign/Absent Disks (se excluyen los discos del sistema)
  Muestra los discos con estado de falla; estos no se pueden agregar a los niveles Active o Retention del sistema.
- Systems Disks

Muestra los discos donde reside DD OS cuando la controladora de Data Domain no contiene discos de almacenamiento de datos.

- Migration History
  Muestra el historial de migraciones.

El encabezado de cada sección muestra un resumen del almacenamiento configurado para esa sección. El resumen muestra cálculos del número total de discos, los discos en uso, los discos de repuesto, los discos de repuesto en reconstrucción, los discos disponibles y los discos conocidos.

Haga clic en un botón más (+) de la sección para ver información detallada, o bien, haga clic en el botón menos (-) para ocultar la información.

Tabla 24 Descripciones de etiquetas de la columna Disks In Use

Elemento	Descripción
Disk Group	El nombre del grupo de discos que creó el sistema de archivos (por ejemplo, dg1).
State	El estado del disco (por ejemplo, Normal, Warning).
Disks Reconstructing	Los discos que están en reconstrucción, por ID de disco (por ejemplo, 1.11).
Total Disks	El número total de discos utilizables (por ejemplo, 14).
Disks	Los ID de disco de los discos utilizables (por ejemplo, 2.1-2.14).
Size	El tamaño del grupo de discos (por ejemplo, 25.47 TiB).

Tabla 25 Descripciones de etiquetas de la columna Disks Not In Use

Elemento	Descripción
Disk	El identificador del disco, que puede ser cualquiera de los siguientes. • El gabinete y el número de disco (con el formato Enclosure Slot) • Un número de dispositivo para un dispositivo lógico, como los que utilizan DD VTL y vDisk. • Un LUN
Slot	El gabinete donde se encuentra el disco.
Pack	El paquete de discos, 1-4, dentro del gabinete donde se encuentra el disco. Este valor solo será 2-4 para bandejas de expansión DS60.
State	El estado del disco, por ejemplo, In Use, Available, Spare.
Size	La capacidad de almacenamiento de datos del disco cuando se utiliza en un sistema Data Domain. [a]
Type	La conectividad y el tipo de disco (por ejemplo, SAS).

a. La convención de Data Domain para procesar el espacio en disco define un gibibyte como 230 bytes, lo que da como resultado una capacidad de disco diferente que la clasificación del fabricante.

Pestaña Enclosures

La pestaña Enclosures muestra una tabla que resume los detalles de los gabinetes conectados al sistema.

La pestaña Enclosures proporciona los siguientes detalles.

Tabla 26 Descripciones de etiquetas de columna de la pestaña Enclosures

Elemento	Descripción
Enclosure	El número de gabinete. El gabinete 1 es la unidad principal.
Serial Number	El número de serie del gabinete.
Disks	Los discos incluidos en el gabinete, en el formato *<número-de-gabinete>*. 1:*<número-de-gabinete>*.*<N>*.
Model	El modelo de gabinete. Para el gabinete 1, el modelo es la unidad principal.
Disk Count	La cantidad de discos en el gabinete.
Disk Size	La capacidad de almacenamiento de datos del disco cuando se utiliza en un sistema Data Domain. [a].
Failed Disks	Los discos fallidos en el gabinete.
Temperature Status	El estado de la temperatura del gabinete.

a. La convención de Data Domain para computar el espacio en disco define un gibibyte como 230 bytes, lo que da como resultado una capacidad de disco diferente que la clasificación del fabricante

Pestaña Disks

En la pestaña Disks, se muestra información sobre cada uno de los discos del sistema. Puede filtrar los discos visualizados para mostrar todos los discos, discos en un nivel específico o discos en un grupo específico.

En la tabla Disk State se muestra una tabla de estado de resumen que muestra el estado de todos los discos del sistema.

Tabla 27 Descripciones de etiquetas de columna de la tabla Disks State

Elemento	Descripción
Total	El número total de discos en el inventario del sistema Data Domain.
In Use	El número de discos actualmente en uso en el sistema de archivos.
Spare	El número de discos de repuesto (disponibles para reemplazar discos con fallas).
Spare (reconstructing)	El número de discos que están en el proceso de reconstrucción de datos (discos de repuesto que reemplazan discos con fallas).
Available	El número de discos que están disponibles para asignación en un nivel de almacenamiento activo o de DD Extended Retention.

Tabla 27 Descripciones de etiquetas de columna de la tabla Disks State (continuación)

Elemento	Descripción
Known	El número de discos no asignados conocidos.
Unknown	El número de discos no asignados desconocidos.
Failed	El número de discos con fallas.
Foreign	El número de discos externos.
Absent	El número de discos ausentes.
Migrating	La cantidad de discos que sirve como el origen de una migración de almacenamiento.
Destination	La cantidad de discos que sirve como el destino de una migración de almacenamiento.
Powered Off	La cantidad de discos no encendidos.
Not Installed	La cantidad de slots de disco vacíos que puede detectar el sistema.

La tabla Disks muestra información específica acerca de cada disco instalado en el sistema.

Tabla 28 Descripciones de etiquetas de columna de la tabla Disks

Elemento	Descripción
Disk	El identificador del disco, que puede ser: • El gabinete y el número de disco (en el formato *Enclosure.Slot*). • Un número de dispositivo para un dispositivo lógico, como los que utilizan DD VTL y vDisk. • Un LUN.
Size	El tamaño del disco.
Slot	El gabinete donde se encuentra el disco.
Pack	El paquete de discos, 1-4, dentro del gabinete donde se encuentra el disco. Este valor solo será 2-4 para bandejas de expansión DS60.
State	El estado del disco, que puede ser uno de los siguientes. • Absent. No hay discos instalados en la ubicación indicada. • Available. Hay un disco disponible asignado al nivel activo o de retención, pero no está en uso actualmente. • Copy Recovery. El disco tiene una frecuencia de errores alta pero no falló. RAID está copiando actualmente el contenido en una unidad de repuesto y la unidad fallará una vez que se complete la reconstrucción de la copia. • Destination. El disco está en uso como destino para la migración de almacenamiento. • Error. El disco tiene una frecuencia de errores alta pero no falló. El disco está en la línea de espera de reconstrucción

Tabla 28 Descripciones de etiquetas de columna de la tabla Disks (continuación)

Elemento	Descripción
	de copia. El estado cambiará a Copy Recovery cuando comience la reconstrucción de la copia. • Foreign. El disco se ha asignado a un nivel, pero los datos del disco indican que el disco puede ser propiedad de otro sistema. • In-Use. El disco se está usando para el almacenamiento de datos de respaldo. • Known. El disco es un disco soportado que está listo para la asignación. • Migrating. El disco está en uso como origen para la migración de almacenamiento. • Powered Off. La alimentación del disco ha sido quitada por el servicio de soporte. • Reconstruction. El disco se está reconstruyendo en respuesta a un comando `disk fail` o por instrucción de RAID/SSM. • Spare. El disco está disponible para usar como repuesto. • System. Los discos del sistema almacenan DD OS y datos del sistema. No hay datos de respaldo almacenados en discos del sistema. • Unknown. No hay un disco desconocido asignado al nivel activo o de retención. Puede haber fallado de forma administrativa o por el sistema RAID.
Manufacturer/Model	La designación de modelo del fabricante. La visualización puede incluir un ID de modelo o un tipo de RAID u otra información, según la cadena del proveedor enviada por el arreglo de almacenamiento.
Firmware	El nivel de firmware usado por la controladora de almacenamiento del disco físico de otros fabricantes.
Serial Number	El número de serie del fabricante del disco.
Vida útil de disco utilizada	El porcentaje de la vida útil clasificada consumida de un disco SSD.
Type	La conectividad y el tipo de disco (por ejemplo, SAS).

Pestaña Reconstruction

La pestaña Reconstruction muestra una tabla que proporciona información adicional sobre discos de reconstrucción.

La siguiente tabla describe las entradas de la tabla Reconstructing.

Tabla 29 Descripciones de etiquetas de la columna de la tabla Reconstruction

Elemento	Descripción
Disco	Identifica los discos que se están reconstruyendo. Las etiquetas de disco tienen el formato *gabinete.disco*. El gabinete 1 es el sistema Data Domain y las bandejas externas comienzan numeración con el gabinete 2. Por ejemplo, la etiqueta 3.4 es el cuarto disco en la segunda bandeja.
Disk Group.	Muestra el grupo RAID (dg#) del disco en reconstrucción.
Nivel	El nombre del nivel donde se está reconstruyendo el disco con fallas.
Tiempo restante	La cantidad de tiempo antes de que se complete la reconstrucción.
Porcentaje de finalización	El porcentaje de la reconstrucción completada.

Cuando hay un disco de repuesto disponible, el sistema de archivos reemplaza automáticamente un disco fallido por uno de repuesto y comienza el proceso de reconstrucción para integrar el disco de repuesto al grupo de discos RAID. El uso de disco muestra `Spare` y el estado pasa a ser `Reconstructing`. La reconstrucción se realiza en un disco a la vez.

Ubicación física de un gabinete

Si tiene problemas para determinar qué gabinete físico corresponde a un gabinete que se muestra en DD System Manager, puede usar la función de señalización de la CLI para hacer parpadear los LED de IDENT del gabinete y los LED del disco que indican el funcionamiento normal.

Procedimiento

1. Establezca una sesión de la CLI con el sistema.
2. Escriba `enclosure beacon` *enclosure*.
3. Presione `Ctrl+C` para que el LED deje de parpadear.

Ubicación física de un disco

Si tiene problemas para determinar qué disco físico corresponde a un disco que se muestra en DD System Manager, puede usar la función de señalización para que parpadee un LED en el disco físico.

Procedimiento

1. Select **Hardware** > **Storage** > **Disks**.
2. Seleccione un disco en la tabla **Disks** y haga clic en **Beacon**.

   Nota

   Puede seleccionar solo un disco a la vez.

   Aparecerá el cuadro de diálogo Beaconing Disk y comenzará a parpadear la luz LED en el disco.

3. Haga clic en **Stop** para detener el parpadeo del LED.

Configurar el almacenamiento

Las funciones de configuración de almacenamiento le permiten agregar y eliminar gabinetes de expansión de almacenamiento de los niveles activo, de retención y de nube. El almacenamiento en un gabinete de expansión (que a veces se denomina bandeja de expansión) no está disponible para usarse hasta que se agrega a un nivel.

Nota

El almacenamiento adicional requiere las licencias adecuadas y suficiente memoria para admitir la nueva capacidad de almacenamiento. Los mensajes de error muestran si se necesitan más licencias o memoria.

Los sistemas DD6300 admiten la opción de usar gabinetes ES30 con unidades de 4 TB (43.6 TiB) al 50 % de utilización (21.8 TiB) en el nivel activo si la capacidad con licencia disponible es exactamente 21.8 TiB. Las siguientes reglas se aplican al uso de bandejas de capacidad parcial.

- No se admite ningún otro tipo de gabinetes o tamaño de unidades para usar en capacidad parcial.
- Una bandeja parcial solo puede existir en el nivel activo.
- Solo un ES30 parcial puede existir en el nivel activo.
- Una vez que una bandeja parcial existe en un nivel, no se pueden configurar ES30 adicionales en ese nivel hasta que la bandeja parcial se agrega en toda su capacidad.

  Nota

  Esto requiere otorgar licencias para capacidad adicional suficiente para utilizar los 21.8 TiB restantes de la bandeja parcial.

- Si la capacidad disponible es mayor de 21.8 TB, no se puede agregar una bandeja parcial.
- La eliminación de una licencia de 21 TiB no convertirá automáticamente una bandeja utilizada por completo en una bandeja parcial. La bandeja debe quitarse y agregarse de nuevo como una bandeja parcial.

Procedimiento

1. Seleccione **Hardware** > **Storage** > **Overview**.
2. Expanda el cuadro de diálogo para uno de los niveles de almacenamiento disponibles:
   - **Nivel activo**
   - **Nivel de retención ampliada**
   - **Nivel de caché**
   - **Nivel de nube**
3. Haga clic en **Configure**.
4. En el cuadro de diálogo Configure Storage, seleccione el almacenamiento que se debe agregar de la lista **Addable Storage**.
5. En la lista **Configure**, seleccione **Active Tier** o **Retention Tier**.

   La cantidad máxima de almacenamiento que se puede agregar al nivel activo depende del controlador DD que se use.

Nota

La barra de capacidad con licencia muestra la parte de la capacidad con licencia (utilizada y restante) para los gabinetes instalados.

6. Seleccione la casilla de verificación de la bandeja que desee agregar.
7. Haga clic en el botón **Add to Tier**.
8. Haga clic en **OK** para agregar el almacenamiento.

Nota

Para eliminar una bandeja agregada, selecciónela en la lista Tier Configuration, haga clic en **Remove from Configuration** y, a continuación, haga clic en **OK**.

Expansión de capacidad de DD3300

El sistema DD3300 está disponible en tres configuraciones de distinta capacidad. Se admiten expansiones de capacidad de una configuración a otra.

El sistema DD3300 está disponible en las siguientes configuraciones de capacidad:

- 4 TB
- 8 TB
- 16 TB
- 32 TB

Se aplican las siguientes consideraciones de actualización:

- Un sistema de 4 TB puede actualizarse a 16 TB.
- Un sistema de 8 TB se puede actualizar a uno de 16 TB, y uno de 16 TB se puede actualizar a uno de 32 TB.
- Un sistema de 16 TB puede actualizarse a 32 TB.
- No hay ninguna ruta de actualización de 4 TB a 32 TB.

Seleccione **Maintenance** > **System** para acceder a información sobre la expansión de la capacidad y para iniciar el proceso de expansión de capacidad.

La expansión de capacidad es un proceso único. El panel **Capacity Expansion History** muestra si ya se ha ampliado el sistema. Si el sistema no se ha expandido, haga clic en el botón **Capacity Expand** para iniciar la expansión de capacidad.

Todas las expansiones de capacidad requieren la instalación de memoria y discos adicionales en el sistema. No intente expandir la capacidad hasta que finalicen las actualizaciones de hardware. La siguiente tabla muestra los requisitos de actualización de hardware para la expansión de capacidad.

Tabla 30 Requisitos de actualización de DD3300 para la expansión de capacidad

Expansión de capacidad	Memoria adicional	Discos duros adicionales	Disco SSD adicional
De 4 TB a 16 TB	32 GB	6 discos duros de 4 TB	1 SSD de 480 GB
De 8 TB a 16 TB.	La expansión de 8 TB a 16 TB solo requiere cambios en la configuración y en la licencia. No se requieren actualizaciones de hardware.		

Tabla 30 Requisitos de actualización de DD3300 para la expansión de capacidad (continuación)

Expansión de capacidad	Memoria adicional	Discos duros adicionales	Disco SSD adicional
De 16 TB a 32 TB.	16 GB	6 discos duros de 4 TB	N/D

La *Guía de actualización y reemplazo de campo de Data Domain DD3300* proporciona instrucciones detalladas para expandir la capacidad del sistema.

Expansión de capacidad

Seleccione la capacidad de destino en la lista desplegable **Select Capacity**. Una expansión de capacidad se puede impedir por memoria insuficiente, por capacidad física insuficiente (HDD), porque ya se ha ampliado el sistema o porque el destino para expansión de capacidad no es compatible. Si no se puede completar la expansión de capacidad, el motivo aparecerá aquí.

Historial de expansión de capacidad

La tabla **Capactiy Expansion History** muestra los detalles acerca de la capacidad del sistema. La tabla proporciona la capacidad del sistema cuando se instaló el software por primera vez y la fecha de la instalación inicial del software. Si se expandió la capacidad, la tabla también proporciona la capacidad expandida y la fecha en que se realizó la expansión.

Discos en estado fallido y discos que estaban en estado fallido y se pasaron a estado normal

La funcionalidad de falla de disco le permite configurar manualmente un disco en un estado fallido para forzar la reconstrucción de los datos almacenados en el disco. La funcionalidad de pasar un disco con estado fallido a estado normal le permite tomar un disco en un estado fallido y regresarlo a funcionamiento.

Falla de un disco

Hacer fallar un disco y forzar la reconstrucción. Seleccione **Hardware** > **Storage** > **Disks** > **Fail**.

Seleccione un disco en la tabla y haga clic en **Fail**.

Pasar un disco de estado fallido a estado normal

Haga que un disco marcado con anterioridad como Failed o Foreign sea utilizable para el sistema. Seleccione **Hardware** > **Storage** > **Disks** > **Unfail**.

Seleccione un disco en la tabla y haga clic en **Unfail**.

Administración de conexiones de red

Las funciones de administración de conexiones de red le permiten ver y configurar interfaces de red, opciones generales de configuración de red y rutas de red.

Administración de conexiones de red de sistemas de alta disponibilidad

El sistema de alta disponibilidad usa dos tipos diferentes de direcciones IP: fijas y flotantes. Cada tipo tiene limitaciones y comportamientos específicos.

En un sistema de alta disponibilidad, las direcciones IP fijas tienen las siguientes características:

- Se usan para administración del nodo por medio de la CLI
- Se adjuntan (“fijan”) al nodo
- Pueden ser estáticas o DHCP, SLAAC de IPv6
- La configuración se realiza en el nodo específico con el argumento opcional `type fixed`

Nota

Todos los accesos al sistema de archivos deben ser por medio de una IP flotante.

Las direcciones IP flotantes solo existen en el sistema de alta disponibilidad de dos nodos; durante el failover, la dirección IP “flota” al nuevo nodo activo y tiene las siguientes características:

- Solo se configura en el nodo activo
- Se utiliza para acceso al sistema de archivos y la mayoría de la configuración
- Solo puede ser estática
- La configuración requiere el argumento `type floating`

Administración de interfaces de redes

Las funciones de administración de interfaces de redes le permiten administrar las interfaces físicas que conectan el sistema a una red y crean interfaces lógicas para admitir agregación de vínculos, balanceo de carga y failover de vínculos o nodos.

Visualización de información de interfaces

La pestaña Interfaces le permite administrar interfaces virtuales y físicas, VLAN, DHCP, DDNS y direcciones y alias de IP.

Tenga en cuenta las siguientes reglas al administrar interfaces IPv6.

- La interfaz de la línea de comandos (CLI) admite IPv6 para comandos de replicación y red de Data Domain básicos, pero no para comandos de respaldo y DD Extended Retention (`archive`). Los comandos de la CLI administran las direcciones IPv6. Puede ver direcciones IPv6 con DD System Manager, pero no puede administrar IPv6 con DD System Manager.
- Se admite replicación de MTree, replicación y colección en redes IPv6, lo que le permite aprovechar el espacio de direcciones IPv6. También se admite la replicación simultánea en redes IPv6 e IPv4, al igual que la replicación administrada de archivos con DD Boost.
- Hay algunas restricciones para interfaces con direcciones IPv6. Por ejemplo, la MTU mínima es 1280. Si intenta configurar la MTU inferior a 1280 en una interfaz con una dirección IPv6, aparece un mensaje de error y la interfaz se elimina del servicio. Una dirección IPv6 puede afectar a una interfaz aunque esté en una VLAN conectada a la interfaz y no directamente a la interfaz.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Interfaces**.

   En la tabla siguiente se describe la información disponible en la pestaña Interfaces.

   Tabla 31 Descripciones de etiquetas de la pestaña Interface

Elemento	Descripción
Interfaz	El nombre de cada interfaz asociada con el sistema seleccionado.
Activado	Si la interfaz está habilitada. • Seleccione **Yes** para habilitar la interfaz y conectarla a la red. • Seleccione **No** para deshabilitar la interfaz y desconectarla de la red.
DHCP	Indica si la interfaz está configurada manualmente (`no`), por un servidor IPv4 de DHCP (protocolo de configuración dinámica de host) (`v4`) o por un servidor IPv6 de DHCP (`v6`).
Dirección IP	Dirección IP asociada a la interfaz. La dirección utilizada por la red para identificar la interfaz. Si la interfaz está configurada a través de DHCP, aparece un asterisco después de este valor.
Netmask	La dirección de máscara de red asociada a la interfaz. Usa el formato de máscara de red IP estándar. Si la interfaz está configurada a través de DHCP, aparece un asterisco después de este valor.
Vínculo	Si la conexión Ethernet está activa (Yes/No).
Tipo de dirección	En un sistema de alta disponibilidad, el tipo de dirección indica Fija, Flotante o Interconexión.
Additional Info	Configuración adicional de la interfaz. Por ejemplo, el modo de vinculación.
Interfaces IPMI configuradas	Muestra Yes o No e indica si el monitoreo de estado de IPMI y la administración de energía están configurados para la interfaz.

2. Para filtrar la lista de interfaces por nombre de interfaz, ingrese un valor en el campo **Interface Name** y haga clic en **Update**.

   Los filtros admiten caracteres comodín, como eth*, veth* o eth0*

3. Para filtrar la lista de interfaces por tipo de interfaz, seleccione un valor del menú **Interface Type** y haga clic en **Update**.

   En un sistema de alta disponibilidad, hay una lista desplegable de filtro para filtrar por tipo de dirección IP (Fija, Flotante o Interconexión).

4. Para volver la tabla de interfaces a la lista predeterminada, haga clic en **Reset**.
5. Seleccione una interfaz de la tabla para rellenar el área Interface Details.

Tabla 32 Descripciones de etiquetas de Interface Details

Elemento	Descripción
Auto-generated Addresses	Muestra las direcciones IPv6 generadas automáticamente para la interfaz seleccionada.
Negociación automática	Cuando esta función muestra `Enabled`, la interfaz negocia automáticamente la configuración de las opciones Speed y Duplex. Cuando esta función muestra `Disabled`, los valores de las opciones Speed y Duplex deben establecerse manualmente.
Cable	Muestra si la interfaz es de cobre o de fibra. **Nota** Algunas interfaces deben estar activadas antes de que el estado de cable sea válido.
Duplex	Se usa junto con el valor de Speed para configurar el protocolo de transferencia de datos. Las opciones son Unknown, Full, Half.
Hardware Address	La dirección MAC de la interfaz seleccionada. Por ejemplo, 00:02:b3:b0:8a:d2.
Interface Name	El nombre de la interfaz seleccionada.
Detección de fallas latentes (LFD) (solo para sistemas de alta disponibilidad)	El campo LFD tiene un vínculo `View Configuration`, el cual muestra una lista emergente que enumera las direcciones e interfaces de LFD.
Unidad de trasmisión máxima (MTU)	El valor de MTU asignado a la interfaz.
Velocidad	Se usa junto con el valor de Duplex para configurar la velocidad de transferencia de datos. Las opciones son Unknown, 10 Mb/s, 100 Mb/s, 1000 Mb/s, 10 Gb/s. **Nota** Las interfaces negociadas automáticamente se deben configurar antes que la velocidad, el dúplex y la velocidad admitida estén visibles.
Supported Speeds	Muestra todas las velocidades que puede usar la interfaz.

6. Para ver opciones de configuración y administración de interfaces IPMI, haga clic en **View IPMI Interfaces**.

   Este vínculo muestra la información de **Maintenance** > **IPMI**.

Nombres y limitaciones de la interfaz física

El formato de los nombres de la interfaz física varía según los diferentes sistemas Data Domain y tarjetas de opción, y se aplican limitaciones a algunas interfaces.

- Para la mayoría de los sistemas, el formato de nombre de la interfaz física es `eth`*xy*, donde *x* es el número de slot de un puerto integrado o una tarjeta de opción e *y* es una cadena alfanumérica. Por ejemplo, eth0a.

- Para la mayoría de las interfaces verticales NIC integradas, la interfaz superior se denomina eth0a y la inferior es eth0b.
- Para la mayoría de las interfaces horizontales NIC integradas, la interfaz izquierda vista desde la parte trasera se denomina eth0a y la derecha es eth0b.
- Los sistemas DD990 proporcionan cuatro interfaces integradas: dos en la parte superior y dos en la parte inferior. La interfaz superior izquierda es eth0a, la superior derecha es eth0b, la inferior izquierda es eth0c y la inferior derecha es eth0d.
- Los sistemas DD2200 proporcionan cuatro puertos NIC 1G Base-T: ethMa (superior izquierdo), ethMb (superior derecho), ethMc (inferior izquierdo) y ethMd (inferior derecho).
- Los sistemas DD2500 proporcionan seis interfaces integradas. Los cuatro puertos NIC 1G Base-T integrados son ethMa (superior izquierdo), ethMb (superior derecho), ethMc (inferior izquierdo) y ethMd (inferior derecho). Los dos puertos NIC 10G Base-T integrados son ethMe (superior) y ethMf (inferior).
- Los sistemas DD4200, DD4500 y DD7200 proporcionan un puerto Ethernet integrado, que es ethMa.
- Para los sistemas que varían entre DD140 y DD990, los nombres de interfaz física para los módulos de I/O comienzan en la parte superior del módulo o del lado izquierdo. La primera interfaz es ethxa, la siguiente es ethxb, la siguiente es ethxc, y así sucesivamente.
- Los números de puerto en los módulos de I/O horizontales de DD2500 están etiquetados en secuencia desde el extremo opuesto al asa del módulo (lado izquierdo). El primer puerto está etiquetado como 0 y corresponde al nombre de interfaz física ethxa, el siguiente es 1/ethxb, el siguiente es 2/ethxc, y así sucesivamente.
- Los números de puerto de los módulos de I/O verticales de DD4200, DD4500 y DD7200 están etiquetados en secuencia desde el extremo opuesto al asa del módulo (parte inferior). El primer puerto está etiquetado como 0 y corresponde al nombre de interfaz física ethxa, el siguiente es 1/ethxb, el siguiente es 2/ethxc, y así sucesivamente.

Reglas generales de configuración de interfaces

Revise las reglas generales de configuración de interfaces antes de configurar interfaces del sistema.

- Cuando se admite tráfico de respaldo y de replicación, si es posible, se deben usar diferentes interfaces para cada tipo de tráfico a fin de que ningún tipo de tráfico tenga impacto en el otro.
- Cuando se espera que el tráfico de replicación sea inferior a 1 Gb/s, si es posible, no use interfaces de 10 GbE para el tráfico de replicación, dado que las interfaces de 10 GbE están optimizadas para tráfico más rápido.
- Si un servicio de Data Domain usa un puerto no estándar y el usuario desea actualizar a DD OS 6.0 o desea modificar un servicio para utilizar un puerto no estándar en un sistema DD OS 6.0, agregue una función de filtro de red para todos los clientes que usan ese servicio a fin de permitir que las direcciones IP del cliente usen el nuevo puerto.
- En sistemas DD4200, DD4500 y DD7200 que usan IPMI, si es posible, reserve la interfaz ethMa para tráfico IPMI y tráfico de administración del sistema (con

protocolos como HTTP, Telnet y SSH). El tráfico de datos de respaldo debe dirigirse a otras interfaces.

Configuración de interfaces físicas

Para que el sistema pueda conectarse a una red, debe configurar al menos una interfaz física.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Interfaces**.
2. Seleccione una interfaz para configurar.

   Nota

   Los sistemas DD140, DD160, DD610, DD620 y DD630 no admiten IPv6 en la interfaz eth0a (eth0 en sistemas que usan nombres de puertos heredados) o en VLAN creadas en esa interfaz.

3. Haga clic en **Configurar**.
4. En el cuadro de diálogo Configure Interface, determine cómo se establecerá la dirección IP de la interfaz:

   Nota

   En un sistema de alta disponibilidad, el cuadro de diálogo Configure Interface tiene un campo para designar o no la dirección IP flotante (Yes/No). Al seleccionar **Yes**, el botón de opción `Manually Configure IP Address` se selecciona de manera automática; las interfaces de IP flotante solo pueden configurarse de manera manual.

   - Use DHCP para asignar la dirección IP. En el área IP Settings, seleccione **Obtain IP Address using DHCP** y seleccione **DHCPv4** para acceso IPv4 o **DHCPv6** para acceso IPv6.
     Al configurar una interfaz física para usar DHCP, la interfaz se habilita automáticamente.

     Nota

     Si elige obtener la configuración de red por medio de DHCP, puede configurar manualmente el nombre de host en **Hardware** > **Ethernet** > **Settings** o con el comando `net set hostname`. Debe configurar manualmente el nombre de host cuando se usa DHCP mediante IPv6.

   - Especifique la configuración de IP manualmente. En el área IP Settings, seleccione **Manually configure IP Address**.
     Los campos **IP Address** y **Netmask** aparecerán activos.

5. Si decide ingresar manualmente la dirección IP, ingrese una dirección IPv4 o IPv6. Si ingresó una dirección IPv4, ingrese una dirección de máscara de red.

   Nota

   Puede asignar una sola dirección IP a una interfaz con este procedimiento. Si asigna otra dirección IP, la dirección nueva reemplaza a la anterior. Para conectar una dirección IP adicional con una interfaz, cree un alias de IP.

6. Especifique la configuración de velocidad/dúplex.

   La combinación de configuraciones de velocidad y dúplex define la velocidad de la transferencia de datos a través de la interfaz. Seleccione una de estas opciones:

   - **Autonegotiate Speed/Duplex**: seleccione esta opción para permitir que la tarjeta de interfaz de red negocie automáticamente la configuración de la velocidad de línea y dúplex para una interfaz. *No* se admite autonegociación en los siguientes módulos de I/O de DD2500, DD4200, DD4500 y DD7200:
     - Puerto doble óptico de 10 GbE SR con conectores LC (con SFP)
     - Puerto doble de cobre de 10 GbE con conexión directa (cables SFP+)
     - 2 puertos cuádruples de cobre de 1 GbE (RJ45)/2 puertos ópticos de 1 GbE SR
   - **Manually configure Speed/Duplex**: seleccione esta opción para configurar manualmente la velocidad de transferencia de datos de una interfaz. Seleccione la velocidad y el dúplex de los menús.
     - Las opciones de dúplex son semidúplex, dúplex completo y desconocido.
     - Las opciones de velocidad que se muestran están limitadas por las funcionalidades del dispositivo de hardware. Las opciones son 10 Mb, 100 Mb, 1000 Mb (1 Gb), 10 Gb y desconocido. El hardware de 10G Base-T admite solo las configuraciones de 100 Mb, 1000 Mb y 10 Gb.
     - Semidúplex está disponible para velocidades de 10 Mb y 100 Mb únicamente.
     - Las velocidades de línea 1000 Mb y 10 Gb requieren dúplex completo.
     - En los módulos de I/O de 10GbE de DD2500, DD4200, DD4500 y DD7200, las interfaces de cobre admiten solo la configuración de velocidad de 10 Gb.
     - La configuración predeterminada para interfaces de 10G Base-T es Autonegotiate Speed/Duplex. Si establece manualmente la velocidad en 1000 Mb o 10 Gb, debe establecer la configuración de dúplex en completa.

7. Especifique el tamaño de unidad de transferencia máxima (MTU) para la interfaz física (Ethernet).

   haga lo siguiente:

   - Haga clic en el botón **Default** para devolver la configuración al valor predeterminado.
   - Asegúrese de que todos los componentes de red sean compatibles con el tamaño configurado con esta opción.

8. Opcionalmente, seleccione **Dynamic DNS Registration**.

   Dynamic DNS (DDNS) es un protocolo que registra direcciones IP locales en un servidor de sistema de nombre de dominio (DNS). En esta versión, DD System Manager admite el modo de Windows DDNS. Para usar el modo de UNIX DDNS, use el comando de CLI `net ddns`.

   El DDNS debe estar registrado para habilitar esta opción.

Nota

Esta opción desactiva DHCP en esta interfaz.

9. Haga clic en **Next**.

   Aparecerá la página de resumen Configure Interface Settings. Los valores mostrados reflejan el estado de la interfaz y el sistema nuevo; estos se aplican cuando hace clic en Finish.

10. Haga clic en **Finish** y en **OK**.

Valores de tamaños de MTU

El tamaño de MTU se debe establecer correctamente para optimizar el rendimiento de una conexión de red. Un tamaño de MTU incorrecto puede afectar de manera negativa el rendimiento de una interfaz.

Los valores admitidos para configurar el tamaño de unidad de transferencia máxima (MTU) para la interfaz física (Ethernet) varían entre 350 y 9000. Para redes 100 Base-T y gigabit, 1500 es el valor predeterminado.

Nota

El tamaño de MTU mínimo para interfaces IPv6 es 1280. Si intenta establecer la MTU en un tamaño inferior a 1280, se genera un error en la interfaz.

Transferencia de una dirección IP estática

Una dirección IP estática específica se debe asignar para una sola interfaz de un sistema. Una dirección IP estática se debe eliminar correctamente de una interfaz antes de que se configure en otra interfaz.

Procedimiento

1. Si la interfaz que aloja la dirección IP estática es parte de un grupo de interfaces de DD Boost, elimine la interfaz del grupo.
2. Seleccione **Hardware** > **Ethernet** > **Interfaces**.
3. Elimine la dirección IP estática que desee transferir.
   a. Seleccione la interfaz que actualmente usa la dirección IP que desea transferir.
   b. En la columna Enabled, seleccione **No** para deshabilitar la interfaz.
   c. Haga clic en **Configure**.
   d. Establezca la dirección IP en 0.

      Nota

      Establezca la dirección IP en 0 cuando no haya otra dirección IP para asignar a la interfaz. No se debe asignar la misma dirección IP a varias interfaces.

   e. Haga clic en **Next** y en **Finish.**
4. Agregue la dirección IP estática eliminada a otra interfaz.
   a. Seleccione la interfaz a la que desea transferir la dirección IP.
   b. En la columna Enabled, seleccione **No** para deshabilitar la interfaz.

c. Haga clic en **Configure**.

d. Configure la dirección IP para que coincida con la dirección IP estática que eliminó.

e. Haga clic en **Next** y en **Finish.**

f. En la columna Enabled, seleccione **Yes** para habilitar la interfaz actualizada.

Reglas de configuración de interfaces virtuales

Las reglas de configuración de interfaces virtuales corresponden a interfaces virtuales de agregación y de conmutación por error. Hay otras reglas que corresponden a interfaces de agregación o de conmutación por error, pero no a ambas.

- El *nombre virtual* debe estar en formato `veth`*x* donde *x* es un número. El número máximo recomendado es 99 debido a las limitaciones de tamaño del nombre.
- Puede crear tantas interfaces virtuales como haya de interfaces físicas.
- Cada interfaz utilizada en una interfaz virtual primero se debe deshabilitar. Una interfaz que es parte de una interfaz virtual se ve como deshabilitada para otras opciones de configuración de red.
- Después de que se destruye una interfaz virtual, las interfaces físicas asociadas con ella permanecen deshabilitadas. Debe volver a habilitar manualmente las interfaces físicas.
- La cantidad y el tipo de tarjetas instaladas determinan el número de puertos Ethernet disponible.
- Cada interfaz física puede pertenecer a una interfaz virtual.
- Un sistema puede admitir varias interfaces virtuales de agregación y de conmutación por error combinadas, sujetas a las restricciones anteriores.
- Las interfaces virtuales se deben crear a partir de interfaces físicas idénticas. Por ejemplo, todas de cobre, todas ópticas, todas de 1 Gb o todas de 10 Gb. Sin embargo, las interfaces de 1 Gb admiten la vinculación de una combinación de interfaces ópticas y de cobre. Esto se aplica a interfaces virtuales en diferentes tarjetas con interfaces físicas idénticas, excepto para tarjetas Chelsio. Para las tarjetas Chelsio, solo se admite la conmutación por error, y solo en interfaces de la misma tarjeta.
- Los vínculos de conmutación por error y de agregación mejoran el rendimiento de la red y la resistencia mediante dos o más interfaces de red en paralelo, lo que aumenta la velocidad del vínculo para los vínculos agregados y la confiabilidad sobre eso de una sola interfaz.
- La funcionalidad de eliminación está disponible a través del botón **Configure**. Haga clic en una interfaz virtual en la lista de interfaces de la pestaña Interfaces y haga clic en **Configure**. En la lista de interfaces del cuadro de diálogo, desactive la casilla de verificación de la interfaz que desee eliminar de la vinculación (conmutación por error o agregación) y haga clic en **Next**.
- Para una interfaz vinculada, la interfaz vinculada se crea con los subordinados restantes si falla el hardware de una interfaz subordinada. Si no hay subordinados, se crea el ID de interfaz vinculada sin subordinados. Esta falla de hardware subordinada genera alertas administradas, una para cada subordinado fallido.

Nota

La alerta para un subordinado fallido desaparece después de que el subordinado fallido se extrae del sistema. Si se instala hardware nuevo, desaparecen las alertas, y la interfaz vinculada usa la nueva interfaz subordinada después del reinicio.

- En los sistemas DD3300, DD4200, DD4500 y DD7200, la interfaz ethMa no admite agregación de vínculos ni conmutación por error.

Reglas para la configuración de una interfaz virtual para agregación de vínculos

La agregación de vínculos proporciona rendimiento de red mejorado y resistencia mediante el uso de dos o más interfaces de red en paralelo, lo que aumenta la velocidad del vínculo y la confiabilidad sobre eso de una sola interfaz. Estas reglas se proporcionan para ayudarlo a optimizar el uso de agregación de vínculos.

- Los cambios en interfaces Ethernet deshabilitadas eliminan la tabla de enrutamiento. Se recomienda realizar cambios en la interfaz únicamente durante el tiempo fuera de mantenimiento programado. Después, vuelva a configurar las reglas de enrutamiento y los gateways.
- Habilite la agregación en una interfaz virtual existente; para ello, especifique las interfaces físicas y el modo, y asígnele una dirección IP.
- Las tarjetas Ethernet ópticas de 10 Gb de un solo puerto no admiten la agregación de vínculos.
- Las interfaces de 1 GbE y 10 GbE no se pueden agregar juntas.
- Las interfaces ópticas y de cobre no se pueden agregar juntas.
- En los sistemas DD4200, DD4500 y DD7200, la interfaz ethMA no admite agregación de vínculos.

Reglas para la configuración de una interfaz virtual para failover

El failover de vínculos proporciona rendimiento y estabilidad de red mejorados al identificar interfaces de respaldo que admitan tráfico de red cuando la interfaz primaria no está en funcionamiento. Estas reglas se proporcionan para ayudarlo a optimizar el uso de failover de vínculos.

- Una interfaz primaria debe ser parte del failover. Si se intenta la eliminación de una interfaz primaria de un failover, aparecerá un mensaje de error.
- Cuando se usa una interfaz primaria en una configuración de failover, se debe especificar explícitamente y también debe ser una interfaz vinculada a la interfaz virtual. Si la interfaz primaria deja de funcionar y hay varias interfaces disponibles, la siguiente interfaz se selecciona de forma aleatoria.
- Todas las interfaces de una interfaz virtual deben estar en la misma red física. Los switches de red utilizados por una interfaz virtual deben estar en la misma red física.
- El número recomendado de interfaces físicas para failover es superior a uno. Sin embargo, puede configurar una interfaz primaria y una o más interfaces de failover, excepto con lo siguiente:
  - Tarjetas de 10 Gb CX4 Ethernet, que están restringidas a una interfaz primaria y una interfaz de failover desde la misma tarjeta.
  - Tarjetas ópticas de 10 Gb de un solo puerto Ethernet, que no se pueden usar.

- En los sistemas DD4200, DD4500 y DD7200, la interfaz ethMA no admite failover de vínculos.

Creación de interfaces virtuales

Puede crear una interfaz virtual para admitir la agregación o el failover de vínculos. La interfaz virtual funciona como un contenedor para los vínculos que se agregarán o asociarán para failover.

Creación de una interfaz virtual para la agregación de vínculos

Cree una interfaz virtual para la agregación de vínculos a fin de que funcione como un contenedor para asociar los vínculos que participarán en la agregación.

Una interfaz de agregación de vínculos debe especificar un modo de vinculación y puede requerir una selección de hash. Por ejemplo, puede habilitar la agregación de vínculos en una interfaz virtual *veth1* a interfaces *eth1* y *eth2* en el modo LACP (protocolo de control de agregación de vínculos) y hash XOR-L2L3.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Interfaces**.
2. En la tabla Interfaces, deshabilite la interfaz física en la que se agregará la interfaz virtual al hacer clic en **No** en la columna **Enabled**.
3. En el menú **Create**, seleccione **Virtual Interface**.
4. En el cuadro de diálogo Create Virtual Interface, especifique un nombre de interfaz virtual en el cuadro **veth**.

   Ingrese un nombre de interfaz virtual en el formato *vethx*, donde *x* es un ID único (generalmente, uno o dos dígitos). Un nombre de interfaz virtual completo típico con VLAN y alias de IP es *veth56.3999:199*. La longitud máxima del nombre completo es de 15 caracteres. No se permiten caracteres especiales. Los números deben ser entre 0 y 4094, inclusive.

5. En **Bonding Type**, seleccione **Aggregate**.

   Nota

   La configuración del registro puede ser distinta a la configuración de la vinculación. Cuando se agregan interfaces a la interfaz virtual, la información no se envía al módulo de vinculación hasta que la interfaz virtual se activa y recibe una dirección IP. Hasta ese momento, el registro y la configuración del controlador de vinculación son diferentes.

6. En la lista **Mode**, seleccione un modo de vinculación.

   Seleccione el modo que sea compatible con los requisitos del sistema con el que las interfaces están conectadas directamente.

   - Round-robin
     Transmita paquetes en orden secuencial desde el primer vínculo disponible hasta el último en el grupo agregado.
   - Balanced
     Los datos se envían a través de las interfaces de acuerdo con lo que determina el método de hash seleccionado. Esto requiere que las interfaces asociadas en el switch estén agrupadas en un canal Ether (troncal) y reciban un hash a través del parámetro Load Balance.

- LACP
  El protocolo de control de agregación de vínculos es similar a Balanced, excepto que usa un protocolo de control que se comunica con el otro extremo y coordina qué vínculos dentro de la vinculación están disponibles para usarse. LACP proporciona un tipo de failover de latido y se debe configurar en ambos extremos del vínculo.

7. Si seleccionó el modo Balanced o LACP, especifique un tipo de hash de vinculación en la lista **Hash**.

   Las opciones son: XOR-L2, XOR-L2L3 o XOR-L3L4.

   XOR-L2 se transmite a través de una interfaz vinculada con un hash XOR de capa 2 (direcciones MAC de entrada y de salida).

   XOR-L2L3 se transmite a través de una interfaz vinculada con un hash XOR de capa 2 (direcciones MAC de entrada y de salida) y de capa 3 (direcciones IP de entrada y de salida).

   XOR-L3L4 se transmite a través de una interfaz vinculada con un hash XOR de capa 3 (direcciones IP de entrada y de salida) y de capa 4 (puertos de entrada y de salida).

8. Para seleccionar una interfaz a fin de agregarla a la configuración de agregación, seleccione la casilla de verificación que corresponda a la interfaz y, a continuación, haga clic en **Next**.

   Aparecerá el cuadro de diálogo Create virtual interface *veth_name*.

9. Especifique una dirección IP o escriba `0` para no especificar una dirección IP.
10. Ingrese una dirección de máscara de red o un prefijo.
11. Especifique las opciones de velocidad/dúplex.

    La combinación de configuraciones de velocidad y dúplex define la velocidad de la transferencia de datos a través de la interfaz. Seleccione:

    - **Autonegotiate Speed/Duplex**
      Seleccione esta opción para permitir que la interfaz de red negocie automáticamente la configuración de la velocidad de línea y dúplex para una interfaz.
    - **Manually configure Speed/Duplex**
      Seleccione esta opción para establecer manualmente una velocidad de transferencia de datos de la interfaz.
      - Las opciones de dúplex son semidúplex o dúplex completo.
      - Las opciones de velocidad que se muestran están limitadas por las funcionalidades del dispositivo de hardware. Las opciones son 10 Mb, 100 Mb, 1000 Mb y 10 Gb.
      - Semidúplex está disponible para velocidades de 10 Mb y 100 Mb únicamente.
      - Las velocidades de línea 1000 Mb y 10 Gb requieren dúplex completo.
      - Las interfaces ópticas requieren la opción Autonegotiate.
      - La opción predeterminada de NIC de cobre de 10 GbE es 10 Gb. Si la velocidad de línea de una interfaz de cobre se establece en 1000 Mb o 10 Gb, el dúplex debe ser completo.

12. Especifique la configuración de MTU.

- Haga clic en **Default** para seleccionar el valor predeterminado (1500).
- Para seleccionar una configuración diferente, ingrese la configuración en el cuadro **MTU**. Asegúrese de que todos los componentes de red sean compatibles con el tamaño configurado con esta opción.

13. Opcionalmente, seleccione Dynamic DNS Registration.

    Dynamic DNS (DDNS) es un protocolo que registra direcciones IP locales en un servidor de sistema de nombre de dominio (DNS). En esta versión, DD System Manager admite el modo de Windows DDNS. Para usar el modo de UNIX DDNS, use el comando de CLI `net ddns`.

    El DDNS debe estar registrado para habilitar esta opción.

14. Haga clic en **Next.**

    Aparecerá la página de resumen Configure Interface Settings. Los valores mostrados reflejan el estado de la interfaz y el sistema nuevo.

15. Haga clic en **Finish** y en **OK**.

Creación de una interfaz virtual para el failover de vínculos

Cree una interfaz virtual para el failover de vínculos a fin de que funcione como un contenedor para asociar los vínculos que participarán en el failover.

La interfaz virtual habilitada para el failover representa un grupo de interfaces secundarias, una de las cuales se puede especificar como principal. El sistema establece la interfaz principal como la interfaz activa cuando está en funcionamiento. Una opción de failover Down Delay configurable le permite configurar una demora de failover en intervalos de 900 milisegundos. La demora de failover brinda protección contra varios failovers cuando una red es inestable.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Interfaces**.
2. En la tabla de interfaces, deshabilite la interfaz física en la que se agregará la interfaz virtual haciendo clic en **No** en la columna **Enabled**.
3. En el menú **Create**, seleccione **Virtual Interface**.
4. En el cuadro de diálogo Create Virtual Interface, especifique un nombre de interfaz virtual en el cuadro **veth**.

   Ingrese un nombre de interfaz virtual en el formato `veth`*x*, donde *x* es un ID único (generalmente, uno o dos dígitos). Un nombre de interfaz virtual completo típico con VLAN y alias de IP es *veth56.3999:199*. La longitud máxima del nombre completo es de 15 caracteres. No se permiten caracteres especiales. Los números deben ser entre 0 y 4094, inclusive.

5. En la lista **Bonding Type**, seleccione **Failover**.
6. Seleccione una interfaz para agregar a la configuración de failover y haga clic en **Next**. Las interfaces de agregación virtuales pueden usarse para failover.

   Aparecerá el cuadro de diálogo Create virtual interface *veth_name*.

7. Especifique una dirección IP o escriba `0` para no especificar una dirección IP.
8. Ingrese una máscara de red o un prefijo.
9. Especifique las opciones de velocidad/dúplex.

La combinación de configuraciones de velocidad y dúplex define la velocidad de la transferencia de datos a través de la interfaz.

- Seleccione **Autonegotiate Speed/Duplex** para permitir que la tarjeta de interfaz de red negocie automáticamente la configuración de la velocidad de línea y dúplex de una interfaz.
- Seleccione **Manually configure Speed/Duplex** para establecer manualmente la velocidad de transferencia de datos de una interfaz.
  - Las opciones de dúplex son semidúplex o dúplex completo.
  - Las opciones de velocidad que se muestran están limitadas por las funcionalidades del dispositivo de hardware. Las opciones son 10 Mb, 100 Mb, 1000 Mb y 10 Gb.
  - Semidúplex está disponible para velocidades de 10 Mb y 100 Mb únicamente.
  - Las velocidades de línea 1000 Mb y 10 Gb requieren dúplex completo.
  - Las interfaces ópticas requieren la opción Autonegotiate.
  - La interfaz de cobre predeterminada es de 10 Gb. Si la velocidad de línea de una interfaz de cobre se establece en 1000 Gb o 10 Gb, el dúplex debe ser completo.

10. Especifique la configuración de MTU.
    - Haga clic en **Default** para seleccionar el valor predeterminado (1500).
    - Para seleccionar una configuración diferente, ingrese la configuración en el cuadro MTU. Asegúrese de que todos los componentes de ruta de la red sean compatibles con el tamaño configurado con esta opción.
11. Opcionalmente, seleccione Dynamic DNS Registration.

    Dynamic DNS (DDNS) es un protocolo que registra direcciones IP locales en un servidor de sistema de nombre de dominio (DNS). En esta versión, DD System Manager admite el modo de Windows DDNS. Para usar el modo de UNIX DDNS, use el comando de CLI `net ddns`.

    El DDNS debe estar registrado para habilitar esta opción.

    Nota

    Esta opción desactiva DHCP en esta interfaz.

12. Haga clic en **Next**.

    Aparecerá la página de resumen Configure Interface Settings. Los valores mostrados reflejan el estado de la interfaz y el sistema nuevo.

13. Complete la interfaz y haga clic en **Finish** y en **OK**.

Modificación de una interfaz virtual

Después de crear una interfaz virtual, puede actualizar la configuración para responder a cambios de red o resolver problemas.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Interfaces**.

2. En la columna Interfaces, seleccione la interfaz y deshabilite la interfaz virtual; para ello, haga clic en **No** en la columna **Enabled**. Haga clic en **OK** en el cuadro de diálogo de advertencia.
3. En la columna **Interfaces**, seleccione la interfaz y haga clic en **Configure.**
4. En el cuadro de diálogo **Configure Virtual Interface**, cambie la configuración.
5. Haga clic en **Next** y en **Finish**.

Configuración de una VLAN

Puede crear una nueva interfaz de VLAN a partir de una interfaz física o una virtual.

El conteo total recomendado de VLAN es 80. Puede crear hasta 100 interfaces (menos el número de alias e interfaces virtuales y físicas) antes de que el sistema le impida crear más.

Procedimiento

1. Seleccione**Hardware** > **Ethernet** > **Interfaces**.
2. En la tabla de interfaces, seleccione la interfaz a la que desea agregar la VLAN.

   La interfaz que seleccione debe estar configurada con una dirección IP antes de que pueda agregar una VLAN.
3. Haga clic en **Create** y seleccione **VLAN**.
4. En el cuadro de diálogo Create VLAN, escriba un número en el cuadro **VLAN Id** para especificar un ID de VLAN.

   El rango de un ID de VLAN es entre 1 y 4094.
5. Especifique una dirección IP o escriba `0` para no especificar una dirección IP.

   La dirección del protocolo de Internet (IP) es la etiqueta numérica asignada a la interfaz. Por ejemplo, 192.168.10.23.
6. Ingrese una máscara de red o un prefijo.
7. Especifique la configuración de MTU.

   La MTU de VLAN debe ser menor o igual que la MTU definida por la interfaz física o virtual a la que está asignada. Si la MTU definida para la interfaz física o virtual compatible se reduce por debajo del valor de VLAN configurado, el valor de VLAN se reduce automáticamente para coincidir con la interfaz compatible. Si el valor de MTU para la interfaz compatible aumenta por encima del valor de VLAN configurado, el valor de VLAN no cambia.

   - Haga clic en **Default** para seleccionar el valor predeterminado (1500).
   - Para seleccionar una configuración diferente, ingrese la configuración en el cuadro MTU. DD System Manager no acepta un tamaño de MTU que sea superior al definido para la interfaz física o virtual a la que está asignada la VLAN.
8. Especifique la opción Dynamic DNS Registration.

   Dynamic DNS (DDNS) es un protocolo que registra direcciones IP locales en un servidor de sistema de nombre de dominio (DNS). En esta versión, DD System Manager admite el modo de Windows DDNS. Para usar el modo de UNIX DDNS, use el comando de CLI `net ddns`.

   El DDNS debe estar registrado para habilitar esta opción.

9. Haga clic en **Next.**

   Aparecerá la página de resumen **Create VLAN**.

10. Analice la configuración; haga clic en **Finish** y luego haga clic en **OK**.

Modificación de una interfaz VLAN

Después de crear una interfaz VLAN, puede actualizar la configuración para responder a cambios de red o resolver problemas.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Interfaces**.
2. En la columna **Interfaces**, seleccione la casilla de verificación y deshabilite la interfaz VLAN; para ello, haga clic en **No** en la columna **Enabled**. Haga clic en **OK** en el cuadro de diálogo de advertencia.
3. En la columna Interfaces, seleccione la casilla de verificación de la interfaz y haga clic en **Configure**.
4. En el cuadro de diálogo **Configure VLAN Interface**, cambie la configuración.
5. Haga clic en **Next** y en **Finish**.

Configuración de un alias de IP

Un alias de IP asigna una dirección IP adicional a una interfaz física, una interfaz virtual o una VLAN.

El número total recomendado de IP, VLAN, alias e interfaces físicas y virtuales que puede existir en el sistema es 80. Aunque se admiten hasta 100 interfaces, a medida que se aproxime a la cantidad máxima, es posible que perciba lentitud en la visualización.

Nota

Cuando se utiliza un sistema Data Domain de alta disponibilidad, si se crea un usuario que inicia sesión en el nodo en standby sin iniciar sesión en el nodo activo primero, ese usuario no dispondrá de un alias predeterminado. Por lo tanto, para utilizar alias en el nodo en standby, el usuario debe iniciar sesión en el nodo activo primero.

Procedimiento

1. Seleccione**Hardware** > **Ethernet** > **Interfaces**.
2. Haga clic en **Create** y seleccione **IP Alias**.

   Aparecerá el cuadro de diálogo Create IP Alias.

3. Especifique un ID de alias de IP; para ello, escriba un número en el cuadro **IP ALIAS Id**.

   El rango es de 1 a 4094 inclusive.

4. Ingrese una dirección IPv4 o IPv6.
5. Si ingresó una dirección IPv4, ingrese una dirección de máscara de red.
6. Especifique la opción Dynamic DNS Registration.

   Dynamic DNS (DDNS) es un protocolo que registra direcciones IP locales en un servidor de sistema de nombre de dominio (DNS). En esta versión, DD System Manager admite el modo de Windows DDNS. Para usar el modo de UNIX DDNS, use el comando de CLI `net ddns`.

El DDNS debe estar registrado para habilitar esta opción.

7. Haga clic en **Next**.

   Aparecerá la página Create IP Alias.

8. Analice la configuración, haga clic en **Finish** y luego haga clic en **OK**.

Modificación de una interfaz de alias de IP

Después de crear un alias de IP, puede actualizar la configuración para responder a cambios de red o resolver problemas.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Interfaces**.
2. En la columna **Interfaces**, seleccione la casilla de verificación y deshabilite la interfaz de alias de IP; para ello, haga clic en **No** en la columna **Enabled**. Haga clic en **OK** en el cuadro de diálogo de advertencia.
3. En la columna **Interfaces**, seleccione la casilla de verificación de la interfaz y haga clic en **Configure**.
4. En el cuadro de diálogo Configure IP Alias, cambie la configuración como se describe en el procedimiento para crear un alias de IP.
5. Haga clic en **Next** y en **Finish**.

Registro de interfaces con DDNS

Dynamic DNS (DDNS) es un protocolo que registra direcciones IP locales en un servidor de sistema de nombre de dominio (DNS).

En esta versión, DD System Manager admite el modo de Windows DDNS. Para usar el modo de UNIX DDNS, use el comando de CLI `net ddns`. Puede realizar lo siguiente:

- Registrar manualmente (agregar) interfaces configuradas a la lista de registro de DDNS.
- Eliminar interfaces de la lista de registro de DDNS.
- Habilitar o deshabilitar las actualizaciones de DNS.
- Mostrar si el registro de DDNS está habilitado o no.
- Mostrar interfaces en la lista de registro de DDNS.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Interfaces** > **DDNS Registration**.
2. En el cuadro de diálogo DDNS Windows Mode Registration, haga clic en **Add** para agregar una interfaz al DDNS.

   Aparecerá el cuadro de diálogo Add Interface.

   a. Escriba un nombre en el campo **Interface**.

   b. Haga clic en **OK**.

3. Opcionalmente, para eliminar una interfaz del DDNS:

   a. Seleccione la interfaz que desee quitar y haga clic en **Remove**.

   b. En el cuadro de diálogo Confirm Remove, haga clic en **OK**.

4. Especifique el estado de DDNS.

- Seleccione **Enable** para habilitar actualizaciones para todas las interfaces registradas.
- Haga clic en **Default** para seleccionar la configuración predeterminada para las actualizaciones de DDNS.
- Desactive **Enable** para deshabilitar las actualizaciones de DDNS para las interfaces registradas.

5. Para completar el registro de DDNS, haga clic en **OK**.

Destrucción de una interfaz

Puede usar DD System Manager para destruir o eliminar interfaces virtuales, VLAN y de alias de IP.

Cuando se destruye una interfaz virtual, el sistema elimina la interfaz virtual, libera su interfaz física vinculada y elimina todos los alias o VLAN conectados a la interfaz virtual. Cuando elimina una interfaz VLAN, el SO elimina las interfaces de alias de IP y VLAN que se crean en él. Cuando destruye un alias de IP, el SO elimina solo esa interfaz de alias.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Interfaces**.
2. Haga clic en el cuadro que aparece junto a la interfaz que desea destruir (virtual, VLAN o de alias de IP).
3. Haga clic en **Destroy**.
4. Haga clic en **OK** para confirmar.

Visualización de una jerarquía de interfaz en la vista de árbol

El cuadro de diálogo Tree View muestra la asociación entre interfaces físicas y virtuales.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Interfaces** > **Tree View**.
2. En el cuadro de diálogo Tree View, seleccione los cuadros de los signos más o menos para expandir o contraer la vista de árbol que muestra la jerarquía.
3. Haga clic en **Close** para salir de esta vista.

Administración de configuración general de red

Las opciones de configuración de nombre de host, nombre de dominio, dominios de búsqueda, mapeo de hosts y lista de DNS se administran juntas en la pestaña Settings.

Visualización de información de configuración de red

En la pestaña Settings se muestra la configuración actual del nombre de host, nombre de dominio, dominios de búsqueda, mapeo de hosts y DNS.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Settings**.

Resultados

La pestaña Settings muestra la siguiente información.

Configuración de host

Nombre del host

El nombre de host del sistema seleccionado.

Nombre del dominio

El nombre de dominio calificado asociado con el sistema seleccionado.

Lista de dominios de búsqueda

Search Domain

Una lista de los dominios de búsqueda que usa el sistema seleccionado. El sistema aplica el dominio de búsqueda como un sufijo al nombre de host.

Mapeo de hosts

Dirección IP

La dirección IP del host para resolver.

Nombre del host

Los nombres de host asociados con la dirección IP.

Lista de DNS

DNS IP Address

Las direcciones IP de DNS actuales asociadas con el sistema seleccionado. Un asterisco (*) indica que las direcciones IP se asignaron a través de DHCP.

Configuración del nombre de host de DD System Manager

Puede configurar el nombre de host y el nombre de dominio de DD System Manager manualmente, o puede configurar DD OS para que reciba automáticamente los nombres de host y de dominio de un servidor protocolo de configuración dinámica de host (DHCP).

Una ventaja de configurar manualmente los nombres de host y de dominio es que elimina la dependencia del servidor DHCP y la interfaz que conduce al servidor DHCP. Para minimizar el riesgo de interrupción del servicio, si es posible, configure manualmente los nombres de host y de dominio.

Al configurar el nombre de host y el nombre de dominio, considere las siguientes reglas.

- No incluya un guion bajo en el nombre de host; no es compatible con algunos navegadores.
- La replicación y la autenticación CIFS se deben volver a configurar después de cambiar los nombres.
- Si un sistema se agregó anteriormente sin un nombre completo (sin nombre de dominio), un cambio de nombre de dominio requiere que elimine y agregue el sistema afectado o que actualice la lista Search Domain List para incluir el nombre de dominio nuevo.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Settings**.
2. Haga clic en **Edit** en el área **Host Settings**. Aparecerá el cuadro de diálogo Configure Host.

3. Para configurar manualmente los nombres de host y de dominio:
   a. Seleccione **Manually configure host**.
   b. Ingrese un nombre de host en el cuadro **Host Name**.

      Por ejemplo, `id##.suempresa.com`

   c. Ingrese un nuevo nombre de dominio en el cuadro **Domain Name**.

      Este es el nombre de dominio asociado con su sistema Data Domain y, generalmente, el nombre de dominio de su empresa. Por ejemplo, *suempresa.com*

   d. Haga clic en **OK**.

      El sistema muestra mensajes de progreso a medida que se aplican los cambios.
4. Para obtener los nombres de host y de dominio de un servidor DHCP, seleccione **Obtain Settings using DHCP** y haga clic en **OK**.

   Se debe configurar al menos una interfaz para usar DHCP.

Administración de la lista de búsqueda de dominios

Puede usar la lista de búsqueda de dominios para definir qué dominios puede buscar el sistema.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Settings**.
2. En la vista Settings, haga clic en **Edit** en el área Search Domain List.
3. Para agregar un dominio de búsqueda mediante el cuadro de diálogo Configure Search Domains:
   a. Haga clic en Add (**+**).
   b. En el cuadro de diálogo Add Search Domain, escriba un nombre en el cuadro **Search Domain**.

      Por ejemplo, `id##.suempresa.com`

   c. Haga clic en **OK**.

      El sistema agrega el dominio nuevo a la lista de dominios de búsqueda.

   d. Haga clic en **OK** para aplicar los cambios y volver a la vista Settings.
4. Para eliminar un dominio de búsqueda mediante el cuadro de diálogo Configure Search Domains:
   a. Seleccione el dominio de búsqueda que desee quitar.
   b. Hagaclic en Delete (**X**).

      El sistema quita el dominio seleccionado de la lista de dominios de búsqueda.

   c. Haga clic en **OK** para aplicar los cambios y volver a la vista Settings.

Cómo agregar y eliminar mapeos de host

Un mapeo de host vincula una dirección IP con un nombre de host, de manera que la dirección IP o el nombre de host puedan usarse para especificar el host.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Settings**.
2. Para agregar un mapeo de host, realice lo siguiente.
   a. En el área Hosts Mapping, haga clic en **Add**.
   b. En el cuadro de diálogo Add Hosts, escriba la dirección IP del host en el cuadro **IP Address**.
   c. Haga clic en Add (**+**).
   d. En el cuadro de diálogo Add Host, escriba un nombre de host, como `id##.suempresa.com`, en el cuadro **Host Name**.
   e. Haga clic en **OK** para agregar el nuevo nombre de host a la lista Host Name.
   f. Haga clic en **OK** para volver a la pestaña Settings.
3. Para eliminar un mapeo de host, haga lo siguiente:
   a. En el área Hosts Mapping, seleccione el mapeo de host que desee eliminar.
   b. Haga clic en Delete (**X**).

Configuración de direcciones IP de DNS

Las direcciones IP de DNS especifican los servidores DNS que el sistema puede usar para obtener direcciones IP para nombres de host que no están en la tabla de mapeo de hosts.

Puede configurar las direcciones IP de DNS manualmente o puede configurar DD OS para que reciba automáticamente direcciones IP de un servidor DHCP. Una ventaja de configurar manualmente las direcciones IP de DNS es que se elimina la dependencia en el servidor DHCP y la interfaz que conduce al servidor DHCP. Para minimizar el riesgo de interrupción del servicio, EMC recomienda que configure manualmente las direcciones IP de DNS.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Settings**.
2. Haga clic en **Edit** desde el área DNS List.
3. Para agregar manualmente una dirección IP de DNS:
   a. Seleccione **Manually configure DNS list**.
      Las casillas de verificación de direcciones IP de DNS aparecen activadas.
   b. Haga clic en Add (**+**).
   c. En el cuadro de diálogo Add DNS, especifique la dirección IP de DNS que desee agregar.
   d. Haga clic en **OK**.
      El sistema agrega la dirección IP nueva a la lista de direcciones IP de DNS.
   e. Haga clic en **OK** para aplicar los cambios.
4. Para eliminar una dirección IP de DNS de la lista:
   a. Seleccione **Manually configure DNS list**.
      Las casillas de verificación de direcciones IP de DNS aparecen activadas.
   b. Seleccione la dirección IP de DNS que desee eliminar y haga clic en Delete (**X**).

El sistema elimina la dirección IP de la lista de direcciones IP de DNS.

c. Haga clic en **OK** para aplicar los cambios.

5. Para obtener direcciones de DNS de un servidor DHCP, seleccione **Obtain DNS using DHCP** y haga clic en **OK**.

   Se debe configurar al menos una interfaz para usar DHCP.

Administración de rutas de redes

Las rutas determinan la ruta que se toma para transferir datos hacia y desde el host local (sistema Data Domain) a otra red o host.

Los sistemas Data Domain no generan ni responden a ningún protocolo de administración de enrutamiento de red (RIP, EGRP/EIGRP y BGP). El único tipo de enrutamiento implementado en un sistema Data Domain está basado en políticas de enrutamiento IPv4, lo cual permite solo una ruta en un gateway predeterminado por tabla de enrutamiento. Puede haber varias tablas de enrutamiento y varios gateways predeterminados. Se crea una tabla de enrutamiento para cada dirección que tenga la misma subred que un gateway predeterminado. Las reglas de enrutamiento envían los paquetes con la dirección IP de origen que coincide con la dirección IP utilizada para crear la tabla para esa tabla de enrutamiento. Todos los demás paquetes que no tienen direcciones IP de origen que coinciden con una tabla de enrutamiento se envían a la tabla de enrutamiento principal.

Dentro de cada tabla de enrutamiento, se pueden agregar rutas estáticas, pero debido a que el enrutamiento de origen se utiliza para hacer que los paquetes lleguen a la tabla, las únicas rutas estáticas que funcionan son aquellas que utilizan la interfaz que tiene la dirección de origen de cada tabla. De lo contrario, deben colocarse en la tabla principal.

Además del enrutamiento de origen de IPv4 utilizado para las otras tablas de enrutamiento, los sistemas Data Domain usan enrutamiento basado en origen para las tablas principales de enrutamiento IPv4 e IPv6, lo que significa que los paquetes de red de salida que coinciden con la subred de varias interfaces se enrutan únicamente mediante la interfaz física cuya dirección IP coincide con la dirección IP de origen de los paquetes, que es el lugar en el que se originaron.

Para IPv6, establezca rutas estáticas cuando varias interfaces contengan las mismas subredes IPv6 y las conexiones se realicen a direcciones IPv6 con esta subred. Normalmente, no se necesitan rutas estáticas con direcciones IPv4 con la misma subred, por ejemplo, para respaldos. Hay algunos casos en los que pueden requerirse direcciones estáticas para permitir que funcionen las conexiones, como conexiones del sistema Data Domain a sistemas remotos.

Las rutas estáticas pueden agregarse a tablas de enrutamiento individuales y eliminarse de ellas agregando la tabla a la especificación de ruta o eliminándola de esa especificación. Esto proporciona las reglas para dirigir los paquetes con direcciones de origen específicas a través de tablas de enrutamiento específicas. Si se requiere una ruta estática para paquetes con esas direcciones de origen, debe agregarse a las rutas la tabla específica donde se enruta la dirección IP.

Nota

El enrutamiento de conexiones iniciadas desde el sistema Data Domain, como para replicación, depende de la dirección de origen utilizada para las interfaces en la misma subred. Para forzar el tráfico para una interfaz determinada a un destino específico (incluso si la interfaz está en la misma subred que otras interfaces), configure una entrada de enrutamiento estático entre los dos sistemas: este enrutamiento estático reemplaza el enrutamiento de origen. Esto no es necesario si la dirección de origen es IPv4 y hay un gateway predeterminado asociado con ella. En ese caso, el enrutamiento de origen ya se maneja a través de su propia tabla de enrutamiento.

Visualización de información de la ruta

En la pestaña Routes se muestran los gateways predeterminados, las rutas estáticas y las rutas dinámicas.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Routes**.

Resultados

En el área Static Routes se muestra la especificación de ruta utilizada para configurar cada ruta estática. En la tabla Dynamic Routes se muestra información de cada una de las rutas asignadas de forma dinámica.

Tabla 33 Descripciones de etiquetas de la columna Dynamic Routes

Elemento	Descripción
Destino	La red/host de destino donde se envía el tráfico de red (datos).
Gateway	La dirección del enrutador en la red de DD, o 0.0.0.0 si no se establece un gateway.
Genmask	La máscara de red de la red de destino. Establézcala en 255.255.255.255 para un destino host y 0.0.0.0 para la ruta predeterminada.
Flags	Las marcas posibles incluyen: U: la ruta está activa; H: el destino es un host, G: usar gateway; R: restablecer ruta para enrutamiento dinámico; D: instalado dinámicamente por demonio o redireccionamiento; M: modificado desde demonio de enrutamiento o redireccionamiento; A: instalado por addrconf; C: entrada de caché y ! : rechazar ruta.
Métrica	La distancia al destino (generalmente se cuenta en saltos). El sistema operativo DD no la usa, pero puede ser necesaria para demonios de enrutamiento.
MTU	El tamaño de unidad de transferencia máxima (MTU) para la interfaz física (Ethernet).
Window	El tamaño de ventana predeterminado para conexiones TCP en esta ruta.
IRTT	El ciclo de ida y vuelta inicial (RTT) utilizado por el kernel para estimar los mejores parámetros del protocolo TCP sin esperar respuestas posiblemente lentas.
Interfaz	El nombre de interfaz asociado con la interfaz de enrutamiento.

Configuración del gateway predeterminado

Puede configurar el gateway predeterminado de forma manual o puede configurar DD OS para que reciba automáticamente direcciones IP del gateway predeterminado un servidor DHCP.

Una ventaja de configurar manualmente el gateway predeterminado es que elimina la dependencia en el servidor DHCP y la interfaz que conduce al servidor DHCP. Para minimizar el riesgo de interrupción del servicio, si es posible, configure manualmente la dirección IP del gateway predeterminado.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Routes**.
2. Haga clic en **Edit** junto al tipo de gateway predeterminado (IPv4 o IPv6) que desee configurar.
3. Para configurar manualmente la dirección del gateway predeterminado:
   a. Seleccione **Manually Configure**.
   b. Ingrese la dirección del gateway en el cuadro **Gateway**.
   c. Haga clic en **OK**.
4. Para obtener la dirección del gateway predeterminado de un servidor DHCP, seleccione **Use DHCP value** y haga clic en **OK**.

   Se debe configurar al menos una interfaz para usar DHCP.

Creación de rutas estáticas

Las rutas estáticas definen las redes o los hosts de destino con los que puede comunicarse el sistema.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Routes**.
2. Haga clic en **Create** en el área Static Routes.
3. En el cuadro de diálogo **Create Routes**, seleccione la interfaz en la que desee alojar la ruta estática y haga clic en **Next**.
4. Especifica el destino.
   - Para especificar una red de destino, seleccione **Network** e ingrese la dirección de red y la máscara de red de la red de destino.
   - Para especificar un host de destino, seleccione **Host** e ingrese el nombre de host o la dirección IP del host de destino.
5. Opcionalmente, puede especificar el gateway que desee usar para conectarse con la red o el host de destino.
   a. Seleccione **Specify a gateway for this route**.
   b. Ingrese la dirección del gateway en el cuadro **Gateway**.
6. Revise la configuración y haga clic en **Next**.

   Aparecerá la página Create Routes > Summary.
7. Haga clic en **Finish**.
8. Cuando finalice el proceso, haga clic en **OK**.

La nueva especificación de la ruta se enumera en la lista Route Spec.

Eliminación de rutas estáticas

Puede eliminar una ruta estática cuando ya no desea que el sistema se comunique con un host o una red de destino.

Procedimiento

1. Seleccione **Hardware** > **Ethernet** > **Routes**.
2. Seleccione la opción Route Spec de la especificación de ruta que desee eliminar.
3. Haga clic en **Delete**.
4. Haga clic en **Delete** para confirmar y, a continuación, haga clic en **Close**.

   La especificación de la ruta seleccionada se quitará de la lista Route Spec.

Administración de contraseñas del sistema

La contraseña del sistema es una clave que permite que un sistema Data Domain se transporte con claves de cifrado en el sistema. Las claves de cifrado protegen los datos, y la contraseña del sistema protege las claves de cifrado.

La contraseña del sistema es una clave legible por humanos (comprensible) (como una tarjeta inteligente) que se usa para generar una clave de cifrado AES 256 utilizable por máquinas. Si alguien roba el sistema en tránsito, el atacante no puede recuperar fácilmente los datos; como mucho, puede recuperar los datos cifrados del usuario y las claves cifradas.

La contraseña se almacena de forma interna en una parte oculta del subsistema de almacenamiento de Data Domain. Esto permite que el sistema Data Domain arranque y continúe brindando acceso a los datos sin intervención del administrador.

Configuración de la contraseña del sistema

La contraseña del sistema se debe configurar antes de que el sistema pueda admitir cifrado de datos o solicitar certificados digitales.

Antes de comenzar

No se configura una longitud de contraseña del sistema mínima cuando se instala DD OS, pero la CLI proporciona un comando para establecer una longitud mínima. Para determinar si hay una longitud mínima configurada para la contraseña, escriba el comando de CLI `system passphrase option show`.

Procedimiento

1. Seleccione **Administration** > **Access** > **Administrator Access**.

   Si la contraseña del sistema no está configurada, aparecerá el botón **Set Passphrase** en el área Passphrase. Si hay una contraseña del sistema configurada, aparecerá el botón **Change Passphrase** y la única opción que tendrá será cambiar la contraseña.

2. Haga clic en el botón **Set Passphrase**.

   Aparecerá el cuadro de diálogo Set Passphrase.

3. Escriba la contraseña del sistema en los cuadros y haga clic en **Next.**

   Si hay una longitud mínima configurada para la contraseña del sistema, la contraseña que escriba debe tener el número de caracteres mínimo.

Resultados

Se configurará la contraseña del sistema y el botón **Change Passphrase** reemplazará al botón **Set Passphrase**.

Cambio de la contraseña del sistema

El administrador puede cambiar la contraseña sin necesidad de manipular las claves de cifrado actuales. El cambio de la contraseña cambia el cifrado de las claves de forma indirecta, pero no afecta los datos del usuario ni la clave de cifrado subyacente.

El cambio de la contraseña requiere autenticación de dos usuarios para proteger contra destrucción de datos.

Procedimiento

1. Seleccione **Administration** > **Access** > **Administrator Access**.
2. Para cambiar la contraseña del sistema, haga clic en **Change Passphrase**.

   Aparecerá el cuadro de diálogo Change Passphrase.

   Nota

   El sistema de archivos debe estar deshabilitado para cambiar la contraseña. Si el sistema de archivos está en ejecución, se le pedirá que lo deshabilite.

3. En los campos de texto, proporcione lo siguiente:
   - El nombre de usuario y la contraseña de una cuenta de director de seguridad (un usuario autorizado en el grupo Security User de ese sistema Data Domain).
   - La contraseña actual en el momento del cambio de contraseña.
   - La contraseña nueva, que debe contener el número mínimo de caracteres configurados con el comando `system passphrase option set min-length`.
4. Haga clic en la casilla de verificación **Enable file system now**.
5. Haga clic en **OK**.

   AVISO

   Asegúrese de cuidar la contraseña. Si se pierde la contraseña, nunca podrá desbloquear el sistema de archivos ni obtener acceso a los datos; los datos se pierden de forma irreversible.

Administración de acceso al sistema

Las funciones de administración de acceso al sistema le permiten controlar el acceso al sistema para los usuarios en una base de datos local o en un directorio de red. Los controles adicionales definen niveles de acceso diferentes y controlan qué protocolos pueden acceder al sistema.

Control de acceso basado en funciones

El control de acceso basado en funciones (RBAC) es una política de autenticación que controla a qué comandos de la CLI y controles de DD System Manager puede acceder un usuario en un sistema.

Por ejemplo, los usuarios que tienen asignada la función *admin* pueden configurar y monitorear un sistema completo, mientras que los usuarios que tienen asignada la función *user* están limitados a monitorear un sistema. Cuando inician sesión en DD System Manager, los usuarios pueden ver únicamente las funciones del programa que se les permite usar según la función asignada al usuario. Las siguientes funciones están disponibles para administrar DD OS.

admin

Un usuario con función *admin* puede configurar y monitorear todo el sistema Data Domain. La mayoría de las características de configuración y los comandos están disponibles únicamente para usuarios con función *admin*. Sin embargo, algunos comandos y características requieren la aprobación de un usuario con función *security* antes de que se complete una tarea.

limited-admin

La función *limited-admin* puede configurar y monitorear el sistema Data Domain con algunas limitaciones. Los usuarios que tienen asignada esta función no pueden realizar operaciones de eliminación de datos, editar el registro ni ingresar bash o modo SE.

user

La función *user* permite a los usuarios monitorear sistemas y cambiar sus propias contraseñas. Los usuarios que tienen asignada la función de administración *user* pueden ver el estado del sistema, pero no pueden cambiar la configuración del sistema.

security (director de seguridad)

Un usuario con la función *security*, que puede denominarse director de seguridad, puede administrar a otros directores de seguridad, autorizar procedimientos que requieren su aprobación y realizar todas las tareas admitidas para usuarios con función user.

La función *security* se proporciona para cumplir con la normativa Write Once, Read Many (WORM). Esta normativa requiere que los datos corporativos almacenados electrónicamente se conserven en un estado original no alterado con fines como eDiscovery. Data Domain agregó funcionalidades de auditoría y registro para mejorar esta función. Como resultado de las normativas de cumplimiento de normas, la mayoría de las opciones de comandos para administrar operaciones confidenciales, como DD Encryption, DD Retention Lock Compliance y archiving, ahora requieren la aprobación de directores de seguridad.

En un escenario tradicional, un usuario con función *admin* emite un comando y, si se requiere la aprobación de un director de seguridad, el sistema muestra una solicitud de aprobación. Para continuar con la tarea original, el director de seguridad debe introducir su nombre de usuario y contraseña en la misma consola en la que se ejecutó el comando. Si el sistema reconoce la información de identificación del director de seguridad, se autoriza el proceso. Si no, se genera una alerta de seguridad.

A continuación se incluyen algunas reglas que corresponden a los usuarios con función security:

- Solo el usuario *sysadmin* (el usuario predeterminado creado durante la instalación de DD OS) puede crear el primer director de seguridad, después de lo cual se quitará el privilegio para crear directores de seguridad del usuario *sysadmin*.
- Una vez creado el primer director de seguridad, solo los directores de seguridad pueden crear otros directores de seguridad.
- La creación de un director de seguridad no habilita la política de autorización. Para habilitar la política de autorización, un director de seguridad debe iniciar sesión y habilitar la política de autorización.
- Los usuarios con función *admin* no pueden realizar tareas del director de seguridad, y los directores de seguridad no pueden realizar tareas de configuración del sistema.
- Durante una actualización, si la configuración del sistema contiene directores de seguridad, se crea un permiso de directores de seguridad predeterminados que incluye una lista de todos los directores de seguridad actuales.

backup-operator

Un usuario con función *backup-operator* puede realizar todas las tareas permitidas para usuarios con función *user*; crear instantáneas de MTrees; importar, exportar y transferir cintas en una biblioteca de cintas virtuales, y copiar cintas entre pools.

Un usuario con función *backup-operator* también puede agregar y eliminar claves públicas de SSH para inicios de sesión que no requieren contraseña. (Esta función se usa principalmente para script automatizado). Este usuario puede agregar, eliminar, restablecer y ver alias de comandos de la CLI; sincronizar archivos modificados; y esperar a que la replicación se complete en el sistema de destino.

none

La función *none* es para usuarios de unidades de grupos de usuarios y autenticación de DD Boost únicamente. Un usuario con función *none* puede iniciar sesión en un sistema Data Domain y puede cambiar su contraseña, pero no puede monitorear, administrar ni configurar el sistema primario. Cuando el sistema primario está particionado en unidades de grupos de usuarios, se usa la función *tenant-admin* o *tenant-user* para definir la función de un usuario con respecto a una unidad de grupos de usuarios específica. Al usuario de un grupo de usuarios primero se le asigna la función *none* para minimizar el acceso al sistema primario y, a continuación, se le agrega la función *tenant-admin* o *tenant-user*.

tenant-admin

Se puede agregar una función *tenant-admin* a otras funciones (que no sean de grupos de usuarios) cuando está habilitada la característica de multiusuario seguro (SMT). Un usuario *tenant-admin* puede configurar y monitorear una unidad de grupos de usuarios específica.

tenant-user

Se puede agregar una función *tenant-admin* a otras funciones (que no sean de grupos de usuarios) cuando la característica SMT está habilitada. La función *tenant-admin* permite que un usuario monitoree una unidad de grupos de usuarios específica y cambie la contraseña de usuarios. Los usuarios que tienen asignada la función de administración *tenant-admin* pueden ver el estado de la unidad de grupos de usuarios, pero no pueden cambiar la configuración de la unidad.

Administración de acceso para protocolos IP

Esta función administra el acceso a sistemas para los protocolos FTP, FTPS, HTTP, HTTPS, SSH, SCP y Telnet.

Visualización de la configuración de servicios de IP

La pestaña Administrator Access muestra el estado de configuración de los protocolos IP que se pueden usar para acceder al sistema. FTP y FTPS son los únicos protocolos que están restringidos a los administradores.

Procedimiento

1. Seleccione **Administration** > **Access** > **Administrator Access**.

Resultados

La página Access Management muestra las pestañas Administrator Access, Local Users, Authentication y Active Users tabs.

Tabla 34 Información de la pestaña Administrator Access

Elemento	Descripción
Frase de contraseña	Si no hay una frase de contraseña configurada, aparece el botón **Set Passphrase**. Si hay una frase de contraseña configurada, aparece el botón **Change Passphrase**.
Servicios	El nombre de un servicio/protocolo que puede acceder al sistema.
Enabled (Yes/No)	El estado del servicio. Si el servicio está deshabilitado, selecciónelo en la lista para habilitarlo y haga clic en **Configure**. Complete la pestaña General del cuadro de diálogo. Si el servicio está habilitado, selecciónelo en la lista para modificar su configuración y haga clic en **Configure**. Edite la configuración en la pestaña General del cuadro de diálogo.
Allowed Hosts	Los hosts que pueden acceder al servicio.
Service Options	El valor de tiempo de espera de la sesión o el puerto para el servicio seleccionado en la lista.
FTP/FTPS	Solo se puede establecer el tiempo de espera de la sesión.
HTTP port	El número de puerto abierto para el protocolo HTTP (puerto 80, de forma predeterminada).
HTTPS port	El número de puerto abierto para el protocolo HTTPS (puerto 443, de forma predeterminada).
SSH/SCP port	El número de puerto abierto para el protocolo SSH/SCP (puerto 22, de forma predeterminada).
Telnet	No se puede establecer un número de puerto.
Tiempo de espera de sesión agotado	La cantidad de tiempo inactivo que se permite antes de que se cierre una conexión. El valor predeterminado es Infinite, es decir, la conexión no se cierra. Si es posible, establezca un máximo de tiempo de espera de sesión de cinco minutos. Use la pestaña **Advanced** del cuadro de diálogo para establecer un tiempo de espera en segundos.

Administración de acceso a FTP

El protocolo de transferencia de archivos (FTP) les permite a los administradores acceder a archivos del sistema Data Domain.

Puede habilitar el acceso a FTP o FTPS para los usuarios que tienen asignada la función de administración admin. El acceso a FTP permite que los nombres de usuario admin y las contraseñas se transfieran por la red en texto no cifrado, lo que convierte a FTP en un método de acceso no seguro FTPS se recomienda como un método de acceso seguro. Cuando habilita el acceso a FTP o FTPS, el otro método de acceso se deshabilita.

Nota

Solo a los usuarios a los que se les asigna la función de administrador se les permite obtener acceso al sistema mediante FTP

Nota

Los clientes LFTP que se conectan a un sistema Data Domain por medio de FTPS o FTP se desconectan después de que se alcanza un límite de tiempo de espera establecido. Sin embargo, el cliente de LFTP usa su nombre de usuario y contraseña almacenados en caché para volver a conectarse después del tiempo de espera mientras ejecuta cualquier comando.

Procedimiento

1. Seleccione **Administration** > **Access** > **Administrator Access**.
2. Seleccione **FTP** y haga clic en **Configure**.
3. Para administrar el acceso a FTP y qué hosts pueden conectarse, seleccione la pestaña General y realice lo siguiente:
   a. Para habilitar el acceso a FTP, seleccione **Allow FTP Access**.
   b. Para permitir que se conecten todos los hosts, seleccione **Allow all hosts to connect**.
   c. Para restringir el acceso a determinados hosts, seleccione **Limit Access to the following systems** y modifique la lista Allowed Hosts.

      Nota

      Puede identificar un host con un nombre completo del host, una dirección IPv4 o una dirección IPv6.

      - Para agregar un host, haga clic en Add (**+**). Especifique el identificador de host y haga clic en **OK**.
      - Para modificar un ID de host, seleccione el host en la lista **Hosts** y haga clic en Edit (lápiz). Cambie el ID de host y haga clic en **OK**.
      - Para quitar un ID de host, seleccione el host en la lista **Hosts** y haga clic en (**X**).
4. Para configurar un tiempo de espera de sesión, seleccione la pestaña **Advanced** y especifique el valor de tiempo de espera en segundos.

Nota

El valor predeterminado de tiempo de espera de sesión es Infinite, es decir, la conexión no se cierra.

5. Haga clic en **OK**.

   Si FTPS está habilitado, aparecerá un mensaje de advertencia solicitándole que haga clic en **OK** para continuar.

Administración de acceso a FTPS

El protocolo FTP seguro (FTPS) les permite a los administradores acceder a archivos del sistema Data Domain.

FTPS proporciona seguridad adicional al uso de FTP, como compatibilidad con los protocolos criptográficos de Transport Layer Security (TLS) y capa de conexión segura (SSL). Tenga en cuenta las siguientes reglas al usar FTPS:

- Únicamente los usuarios que tienen asignada la función de administración admin pueden acceder al sistema a través de FTPS.
- Cuando habilita el acceso a FTPS, se deshabilita el acceso a FTP.
- FTPS no se muestra como un servicio para sistemas DD que ejecutan DD OS 5.2, administrados desde un sistema DD que ejecuta DD OS 5.3 o versiones posteriores.
- Cuando se emite el comando `get`, aparece el mensaje de error irrecuperable `SSL_read: wrong version number lftp` si no hay versiones coincidentes de SSL instaladas en el sistema Data Domain y compiladas en el cliente LFTP. Como solución alternativa, puede intentar volver a emitir el comando `get` en el mismo archivo.

Procedimiento

1. Seleccione **Administration** > **Access** > **Administrator Access**.
2. Seleccione **FTPS** y haga clic en **Configure**.
3. Para administrar el acceso a FTPS y qué hosts pueden conectarse, seleccione la pestaña General y realice lo siguiente:
   a. Para habilitar el acceso a FTPS, seleccione **Allow FTPS Access**.
   b. Para permitir que se conecten todos los hosts, seleccione **Allow all hosts to connect**.
   c. Para restringir el acceso a determinados hosts, seleccione **Limit Access to the following systems** y modifique la lista de hosts.

      Nota

      Puede identificar un host con un nombre completo del host, una dirección IPv4 o una dirección IPv6.

      - Para agregar un host, haga clic en Add (**+**). Especifique el identificador de host y haga clic en **OK**.
      - Para modificar un ID de host, seleccione el host en la lista **Hosts** y haga clic en Edit (lápiz). Cambie el ID de host y haga clic en **OK**.
      - Para quitar un ID de host, seleccione el host en la lista **Hosts** y haga clic en (**X**).

4. Para configurar un tiempo de espera de sesión, seleccione la pestaña **Advanced** y especifique el valor de tiempo de espera en segundos.

   Nota

   El valor predeterminado de tiempo de espera de sesión es Infinite, es decir, la conexión no se cierra.

5. Haga clic en **OK**. Si FTP está habilitado, aparecerá un mensaje de advertencia solicitándole que haga clic en **OK** para continuar.

Administración del acceso HTTP y HTTPS

Se requiere el acceso HTTP o HTTPS para respaldar el acceso del navegador a DD System Manager.

Procedimiento

1. Seleccione **Administration** > **Access** > **Administrator Access**.
2. Seleccione **HTTP** o **HTTPS** y haga clic en **Configure**.

   Aparecerá el cuadro de diálogo Configure HTTP/HTTPS Access y se mostrarán pestañas de configuración general, configuración avanzada y administración de certificados.
3. Para administrar el método de acceso y qué hosts pueden conectarse, seleccione la pestaña General y realice lo siguiente:
   a. Seleccione las casillas de verificación de los métodos de acceso que quiera permitir.
   b. Para permitir que se conecten todos los hosts, seleccione **Allow all hosts to connect**.
   c. Para restringir el acceso a determinados hosts, seleccione **Limit Access to the following systems** y modifique la lista de hosts.

      Nota

      Puede identificar un host con un nombre completo del host, una dirección IPv4 o una dirección IPv6.

      - Para agregar un host, haga clic en Add (**+**). Especifique el identificador de host y haga clic en **OK**.
      - Para modificar un ID de host, seleccione el host en la lista **Hosts** y haga clic en Edit (lápiz). Cambie el ID de host y haga clic en **OK**.
      - Para quitar un ID de host, seleccione el host en la lista **Hosts** y haga clic en Delete (**X**).
4. Para configurar puertos del sistema y valores de tiempo de espera de sesión, seleccione la pestaña **Advanced** y complete el formulario.
   - En el cuadro **HTTP Port**, ingrese el número de puerto. El puerto 80 está asignado de forma predeterminada.
   - En el cuadro **HTTP Port**, ingrese el número correspondiente. El puerto 443 está asignado de forma predeterminada.
   - En el cuadro **Session Timeout**, especifique el intervalo en segundos que debe transcurrir antes de que se cierre una conexión. El mínimo es 60 segundos y el máximo es 31536000 segundos (un año).

Nota

El tiempo de espera predeterminado es 10 800 segundos.

5. Haga clic en **OK**.

Administración de certificados de host para HTTP y HTTPS

Un certificado de host permite que los navegadores verifiquen la identidad del sistema cuando se establecen sesiones de administración.

Solicitud de un certificado de host para HTTP y HTTPS

Puede usar DD System Manager para generar una solicitud de certificado de host, que después puede reenviar a una autoridad de certificación (CA).

Nota

Debe configurar una contraseña del sistema (conjunto de contraseñas del sistema) antes de poder generar una CSR.

Procedimiento

1. Seleccione **Administration** > **Access** > **Administrator Access**.
2. En el área Services, seleccione **HTTP** o **HTTPS** y haga clic en **Configure**.
3. Seleccione la pestaña **Certificate**.
4. Haga clic en Add.

   Aparecerá un cuadro de diálogo para el protocolo que seleccionó antes en este procedimiento.

5. Haga clic en **Generate the CSR for this Data Domain system**.

   El cuadro de diálogo se expandirá para mostrar un formulario de CSR.

   Nota

   DD OS admite una CSR activa por vez. Después de que se genera una CSR, el vínculo **Generate the CSR for this Data Domain system** se reemplaza con el vínculo **Download the CSR for this Data Domain system**. Para eliminar una CSR, use el comando de la CLI `adminaccess certificate cert-signing-request delete`.

6. Complete el formulario de CSR y haga clic en **Generate and download a CSR**.

   El archivo de CSR se guarda en la siguiente ruta: `/ddvar/certificates/CertificateSigningRequest.csr`. Use SCP, FTP o FTPS para transferir el archivo de CSR desde el sistema a una computadora, desde la que puede enviar la CSR a una CA.

Cómo agregar un certificado de host para HTTP y HTTPS

Puede usar DD System Manager para agregar un certificado de host al sistema.

Procedimiento

1. Si no solicitó un certificado de host, solicítelo a una autoridad de certificación.
2. Cuando haya recibido un certificado de host, cópielo o muévalo a la computadora desde la que ejecuta DD Service Manager.

3. Seleccione **Administration** > **Access** > **Administrator Access**.
4. En el área Services, seleccione **HTTP** o **HTTPS** y haga clic en **Configure**.
5. Seleccione la pestaña **Certificate**.
6. Haga clic en **Add**.

   Aparecerá un cuadro de diálogo para el protocolo que seleccionó antes en este procedimiento.

7. Para agregar un certificado de host adjunto en un archivo .p12, realice lo siguiente:
   a. Seleccione **I want to upload the certificate as a .p12 file**.
   b. Escriba la contraseña en el cuadro **Password**.
   c. Haga clic en **Browse** y seleccione el certificado de host para cargarlo en el sistema.
   d. Haga clic en **Add**.
8. Para agregar un certificado de host adjunto en un archivo .pem, realice lo siguiente:
   a. Seleccione **I want to upload the public key as a .pem file and use a generated private key**.
   b. Haga clic en **Browse** y seleccione el certificado de host para cargarlo en el sistema.
   c. Haga clic en **Add**.

Eliminación de un certificado de host para HTTP y HTTPS

DD OS admite un certificado de host para HTTP y HTTPS. Si actualmente el sistema usa un certificado de host y usted quiere usar un certificado de host diferente, debe eliminar el certificado actual antes de agregar el nuevo.

Procedimiento

1. Seleccione **Administration** > **Access** > **Administrator Access**.
2. En el área Services, seleccione **HTTP** o **HTTPS** y haga clic en **Configure**.
3. Seleccione la pestaña **Certificate**.
4. Seleccione el certificado que desea eliminar.
5. Haga clic en **Delete** y en **OK**.

Administración del acceso de SSH y SCP

SSH es un protocolo seguro que permite el acceso de red a la CLI del sistema, con o sin SCP (copia segura). Puede usar DD System Manager para habilitar el acceso al sistema a través del protocolo SSH. SCP requiere SSH, de modo que cuando SSH está deshabilitado, SCP se deshabilita automáticamente.

Procedimiento

1. Seleccione **Administration** > **Access** > **Administrator Access**.
2. Seleccione **SSH** o **SCP** y haga clic en **Configure**.
3. Para administrar el método de acceso y qué hosts pueden conectarse, seleccione la pestaña **General**.
   a. Seleccione las casillas de verificación de los métodos de acceso que quiera permitir.

b. Para permitir que se conecten todos los hosts, seleccione **Allow all hosts to connect**.

c. Para restringir el acceso a determinados hosts, seleccione **Limit Access to the following systems** y modifique la lista de hosts.

Nota

Puede identificar un host con un nombre completo del host, una dirección IPv4 o una dirección IPv6.

- Para agregar un host, haga clic en Add (**+**). Especifique el identificador de host y haga clic en **OK**.
- Para modificar un ID de host, seleccione el host en la lista **Hosts** y haga clic en Edit (lápiz). Cambie el ID de host y haga clic en **OK**.
- Para quitar un ID de host, seleccione el host en la lista **Hosts** y haga clic en (**X**).

4. Para configurar puertos del sistema y valores de tiempo de espera de sesión, haga clic en la pestaña **Advanced**.
   - En el cuadro de entrada de texto **SSH/SCP**, especifique el número de puerto. El puerto 22 está asignado de forma predeterminada.
   - En el cuadro **Session Timeout**, especifique el intervalo en segundos que debe transcurrir antes de que se cierre la conexión.

Nota

El valor predeterminado de tiempo de espera de sesión es Infinite, es decir, la conexión no se cierra.

Nota

Haga clic en **Default** para volver al valor predeterminado.

5. Haga clic en **OK**.

Administración del acceso de Telnet

Telnet es un protocolo no seguro que permite a la CLI del sistema acceder a la red.

Nota

El acceso de Telnet permite que los nombres de usuario y las contraseñas se transfieran por la red en texto no cifrado, lo que convierte a Telnet en un método de acceso no seguro

Procedimiento

1. Seleccione **Administration** > **Access** > **Administrator Access**.
2. Seleccione **Telnet** y haga clic en **Configure**.
3. Para administrar el acceso de Telnet y qué hosts pueden conectarse, seleccione la pestaña **General**.
   a. Para habilitar el acceso de Telnet, seleccione **Allow Telnet Access**.

b. Para permitir que se conecten todos los hosts, seleccione **Allow all hosts to connect**.

c. Para restringir el acceso a determinados hosts, seleccione **Limit Access to the following systems** y modifique la lista de hosts.

Nota

Puede identificar un host con un nombre completo del host, una dirección IPv4 o una dirección IPv6.

- Para agregar un host, haga clic en Add (**+**). Especifique el identificador de host y haga clic en **OK**.
- Para modificar un ID de host, seleccione el host en la lista **Hosts** y haga clic en Edit (lápiz). Cambie el ID de host y haga clic en **OK**.
- Para quitar un ID de host, seleccione el host en la lista **Hosts** y haga clic en Delete (**X**).

4. Para configurar un tiempo de espera de sesión, seleccione la pestaña Advanced y especifique el valor de tiempo de espera en segundos.

Nota

El valor predeterminado de tiempo de espera de sesión es Infinite, es decir, la conexión no se cierra.

5. Haga clic en **Aceptar**.

Administración de la cuenta de usuario local

Un usuario local es una cuenta de usuario (nombre de usuario y contraseña) que está configurada en el sistema Data Domain en lugar de estar definida en un grupo de trabajo de Windows, Windows Active Directory o directorio de NIS.

Después de configurar un dominio de confianza, los usuarios que pertenezcan a ese dominio podrán iniciar sesión en el sistema Data Domain, incluso si ese dominio de confianza está desconectado.

Conflictos de UID: Cuentas de usuarios locales y de NIS

Cuando configura un sistema Data Domain en un ambiente NIS, tenga en cuenta que se pueden generar conflictos de UID entre las cuentas de usuarios locales y de NIS.

Las cuentas de usuarios locales en un sistema Data Domain comienzan con un UID de 500. Para evitar conflictos, considere el tamaño de las posibles cuentas locales al definir rangos de UID admisibles para usuarios de NIS.

Visualización de información del usuario local

Los usuarios locales son cuentas de usuario que están definidas en el sistema, en lugar de en Active Directory, un grupo de trabajo o UNIX. Puede mostrar el nombre de usuario, la función de administración, el estado de inicio de sesión y la fecha de deshabilitación de destino del usuario local. También puede mostrar los controles de contraseña del usuario y las unidades del grupo de usuarios a los que puede acceder el usuario.

Nota

El módulo de autenticación de usuario utiliza la hora del meridiano de Greenwich (GMT). Para garantizar que las cuentas y contraseñas de usuario venzan correctamente, establezca opciones de configuración para que se use la GMT que corresponde a la hora local de destino.

Procedimiento

1. Seleccione **Administration** > **Access** > **Local Users** .

   Aparecerá la vista Local Users y se mostrarán la tabla Local Users y el área Detailed Information.

   Tabla 35 Descripciones de etiquetas de columnas de la lista de usuarios locales

Elemento	Descripción
Name	El ID de usuario como se agregó al sistema.
Management Role	La función que se muestra es admin, user, security, backup-operator o none. En esta tabla, las funciones de usuarios de grupos de usuarios se muestran como *none*. Para ver una función de grupo de usuarios asignada, seleccione el usuario y visualice la función en el área Detailed Information.
Status	• Active: se permite el acceso del usuario a esta cuenta. • Disabled: el acceso del usuario a esta cuenta está denegado porque la cuenta está deshabilitada administrativamente, la fecha actual es posterior a la fecha de vencimiento de la cuenta o la contraseña de una cuenta bloqueada requiere renovación. • Locked: se deniega el acceso del usuario porque la contraseña venció.
Disable Date	La fecha establecida para que se deshabilite la cuenta.
Last Login From	La ubicación donde el usuario inició sesión por última vez.
Last Login Time	El momento en el que el usuario inició sesión por última vez.

   Nota

   Las cuentas de usuario configuradas con las funciones admin o security officer pueden ver todos los usuarios. Los usuarios con otras funciones solo pueden ver sus propias cuentas de usuario.

2. Seleccione el usuario que desee ver de la lista de usuarios.

   La información del usuario seleccionado se muestra en el área Detailed Information.

   Tabla 36 Información detallada del usuario, descripciones de etiquetas de filas

Elemento	Descripción
Password Last Changed	La fecha en que se modificó la contraseña por última vez.

Tabla 36 Información detallada del usuario, descripciones de etiquetas de filas (continuación)

Elemento	Descripción
Minimum Days Between Change	El número mínimo de días entre los cambios de contraseña que le otorga a un usuario. El valor predeterminado es 0.
Maximum Days Between Change	El número máximo de días entre los cambios de contraseña que le otorga a un usuario. El valor predeterminado es 90.
Warn Days Before Expire	El número de días para advertirles a los usuarios antes de que venza su contraseña. El valor predeterminado es 7.
Disable Days After Expire	El número de días después de que vence una contraseña para deshabilitar la cuenta de usuario. El valor predeterminado es Never.

Nota

Los valores predeterminados son los valores iniciales de la política de contraseña predeterminada. Un administrador del sistema (función de administrador) puede cambiarlos seleccionando **More Tasks** > **Change Login Options**.

Creación de usuarios locales

Puede crear usuarios locales cuando desea administrar el acceso en el sistema local en lugar de a través de un directorio externo. Los sistemas Data Domain admiten un máximo de 500 cuentas de usuarios locales.

Procedimiento

1. Seleccione **Administration** > **Access** > **Local Users**.

   Aparecerá la vista Local Users.

2. Haga clic en el botón **Create** para crear un usuario nuevo.

   Aparecerá el cuadro de diálogo Create User.

3. Escriba la información del usuario en la pestaña General.

   Tabla 37 Cuadro de diálogo Create User, controles generales

Elemento	Descripción
Usuario	El nombre o ID de usuario.
Contraseña	La contraseña del usuario. Establezca una contraseña predeterminada; el usuario puede cambiarla más adelante.
Verify Password	La contraseña del usuario, nuevamente.
Función de administración	La función asignada al usuario, que puede ser admin, user, security, backup-operator o none.

Tabla 37 Cuadro de diálogo Create User, controles generales (continuación)

Elemento	Descripción
	Nota Solo el usuario sysadmin (el usuario predeterminado creado durante la instalación de DD OS) puede crear el primer usuario con función security. Después de que se crea el primer usuario con función security, solo los usuarios con función security pueden crear otros.
Forzar cambio de contraseña	Seleccione esta casilla de verificación para exigir al usuario cambiar la contraseña durante el primer inicio de sesión al iniciar sesión en DD System Manager o en la CLI con SSH o Telnet.

El valor predeterminado para la longitud mínima de una contraseña es 6 caracteres. El valor predeterminado para el número mínimo de clases de caracteres necesario para una contraseña de usuario es 1. Entre las clases de caracteres admitidos se incluyen:

- Letras en minúscula (a-z)
- Letras en mayúscula (A-Z)
- Números (0-9)
- Caracteres especiales ($, %, #, +, etc.)

Nota

La función sysadmin pertenece al usuario con función admin y no se puede eliminar ni modificar.

4. Para administrar el vencimiento de la cuenta y la contraseña, seleccione la pestaña Advanced y use los controles que se describen en la siguiente tabla.

Tabla 38 Cuadro de diálogo Create User, controles avanzados

Elemento	Descripción
Minimum Days Between Change	El número mínimo de días entre los cambios de contraseña que le otorga a un usuario. El valor predeterminado es 0.
Maximum Days Between Change	El número máximo de días entre los cambios de contraseña que le otorga a un usuario. El valor predeterminado es 90.
Warn Days Before Expire	El número de días para advertirles a los usuarios antes de que venza su contraseña. El valor predeterminado es 7.
Disable Days After Expire	El número de días después de que vence una contraseña para deshabilitar la cuenta de usuario. El valor predeterminado es Never.
Disable account on the following date	Marque esta casilla e ingrese una fecha (mm/dd/aaaa) cuando desee deshabilitar esta cuenta. Puede también hacer clic en el calendario para elegir una fecha.

5. Haga clic en **OK**.

Nota

Nota: La política de contraseña predeterminada puede cambiar si la cambia un usuario con función de administrador (**More Tasks** > **Change Login Options**). Los valores predeterminados son los valores iniciales de la política de contraseña predeterminada.

Modificación de un perfil de usuario local

Después de crear un usuario, puede usar DD System Manager para modificar la configuración del usuario.

Procedimiento

1. Seleccione **Administration** > **Access** > **Local Users**.

   Aparecerá la vista Local Users.

2. Haga clic en un nombre de usuario de la lista.
3. Haga clic en **Modify** para realizar cambios en una cuenta de usuario.

   Aparecerá el cuadro de diálogo Modify User.
4. Actualice la información en la pestaña General.

Nota

Si se habilita SMT y se solicita un cambio de la función de none a cualquier otra función, el cambio se acepta solamente si el usuario no está asignado a una unidad de grupos de usuarios como un usuario de administración, si no es un usuario de DD Boost con su conjunto de unidades predeterminadas de grupos de usuarios y si no es el propietario de una unidad de almacenamiento que esté asignada a una unidad de grupo de usuarios.

Nota

Si desea cambiar la función de un usuario de DD Boost que no sea propietario de ninguna unidad de almacenamiento, cancele su asignación como un usuario de DD Boost, cambie la función de usuario y vuelva a asignarlo como un usuario de DD Boost nuevamente.

Tabla 39 Cuadro de diálogo Modify User, controles generales

Elemento	Descripción
Usuario	El nombre o ID de usuario.
Role	Seleccione la función de la lista.

5. Actualice la información en la pestaña Advanced.

Tabla 40 Cuadro de diálogo Modify User, controles avanzados

Elemento	Descripción
Minimum Days Between Change	El número mínimo de días entre los cambios de contraseña que le otorga a un usuario. El valor predeterminado es 0.

Tabla 40 Cuadro de diálogo Modify User, controles avanzados (continuación)

Elemento	Descripción
Maximum Days Between Change	El número máximo de días entre los cambios de contraseña que le otorga a un usuario. El valor predeterminado es 90.
Warn Days Before Expire	El número de días para advertirles a los usuarios antes de que venza su contraseña. El valor predeterminado es 7.
Disable Days After Expire	El número de días después de que vence una contraseña para deshabilitar la cuenta de usuario. El valor predeterminado es Never.

6. Haga clic en **OK**.

Eliminación de un usuario local

Puede eliminar determinados usuarios según la función de usuario. Si uno de los usuarios seleccionados no se puede eliminar, el botón Delete estará deshabilitado.

El usuario sysadmin no se puede eliminar. Los usuarios administradores no pueden eliminar funcionarios de seguridad. Solo los funcionarios de seguridad pueden eliminar, habilitar y deshabilitar otros funcionarios de seguridad.

Procedimiento

1. Seleccione **Administration** > **Access** > **Local Users**.

   Aparecerá la vista Local Users.

2. Haga clic en uno o más nombres de usuario de la lista.
3. Haga clic en **Delete** para eliminar las cuentas de usuario.

   Aparecerá el cuadro de diálogo Delete User.

4. Haga clic en **OK** y **Close**.

Habilitación y deshabilitación de usuarios locales

Los usuarios administradores pueden habilitar o deshabilitar todos los usuarios excepto el usuario administrador del sistema y los usuarios con rol de seguridad. El usuario administrador del sistema no se puede deshabilitar. Solo los funcionarios de seguridad pueden habilitar y deshabilitar a otros funcionarios de seguridad.

Procedimiento

1. Seleccione **Administration** > **Access** > **Local Users**.

   Aparecerá la vista Local Users.

2. Haga clic en uno o más nombres de usuario de la lista.
3. Haga clic en **Enable** o en **Disable** para habilitar o deshabilitar cuentas de usuario.

   Aparecerá el cuadro de diálogo Enable or Disable User.

4. Haga clic en **OK** y **Close**.

Activación de autorización de seguridad

Puede usar la interfaz de la línea de comandos (CLI) del sistema Data Domain para habilitar y deshabilitar la política de autorización de seguridad.

Para obtener información sobre los comandos utilizados en este procedimiento, consulte la *Guía de referencia de comandos de Data Domain Operating System*.

Nota

La licencia de DD Retention Lock Compliance debe estar instalada. No puede deshabilitar la política de autenticación en sistemas de DD Retention Lock Compliance.

Procedimiento

1. Inicie sesión en la CLI con un nombre de usuario y contraseña de funcionario de seguridad.
2. Para habilitar la política de autorización de funcionario de seguridad, escriba: `# authorization policy set security-officer enabled`

Cambio de contraseñas de usuario

Después de crear un usuario, puede usar DD System Manager para cambiar la contraseña del usuario. Los usuarios individuales también pueden cambiar sus propias contraseñas.

Procedimiento

1. Haga clic en **Administration** > **Access** > **Local Users**.

   Se muestra la vista Local Users.

2. Haga clic en un nombre de usuario de la lista.
3. Haga clic en **Change Password** para cambiar la contraseña del usuario.

   Se muestra el cuadro de diálogo Change Password.

4. Escriba la contraseña anterior en el cuadro **Old Password**.
5. Escriba la contraseña nueva en el cuadro **New Password**.
6. Vuelva a escribir la contraseña nueva en el cuadro **Verify New Password**.
7. Haga clic en **OK**.

   Solo los usuarios con una función “admin” pueden cambiar la contraseña de otros usuarios. El administrador puede cambiar la contraseña de otros usuarios de la CLI ejecutando el comando `user change password [<user>] .`

   Nota

   Por motivos de seguridad, los usuarios con una función “admin” no pueden cambiar las contraseñas de otros usuarios “admin”. Si se debe cambiar la contraseña de un usuario “admin” iniciando sesión como otro usuario, póngase en contacto con el soporte de Dell EMC creando una solicitud de soporte o una solicitud de chat para recibir asistencia.

Modificación de la política de contraseñas y los controles de inicio de sesión

La política de contraseñas y los controles de inicio de sesión definen los requisitos de inicio de sesión para todos los usuarios. Los administradores pueden especificar con qué frecuencia se debe cambiar una contraseña, qué se requiere para crear una contraseña válida y cómo responde el sistema a intentos de inicio de sesión no válidos.

Procedimiento

1. Seleccione **Administration** > **Access**.
2. Seleccione **More Tasks** > **Change Login Options**.

   Aparecerá el cuadro de diálogo Change Login Options.

3. Especifique la configuración nueva en los cuadros de cada opción. Para seleccionar el valor predeterminado, haga clic en **Default** junto a la opción adecuada.
4. Haga clic en **OK** para guardar la configuración de contraseña.

Cuadro de diálogo Change Login Options

Puede usar este cuadro de diálogo para configurar la política de contraseñas y especificar el máximo de intentos de inicio de sesión y el período de bloqueo.

Tabla 41 Controles del cuadro de diálogo Change Login Options

Elemento	Descripción
Minimum Days Between Change	El número mínimo de días entre los cambios de contraseña que le otorga a un usuario. Este valor debe ser menor que el valor de **Maximum Days Between Change** menos el valor de **Warn Days Before Expire**. La configuración predeterminada es 0.
Maximum Days Between Change	El número máximo de días entre los cambios de contraseña que le otorga a un usuario. El valor mínimo es 1. El valor predeterminado es 90.
Warn Days Before Expire	El número de días para advertirles a los usuarios antes de que venza su contraseña. Este valor debe ser menor que el valor de **Maximum Days Between Change** menos el valor de **Minimum Days Between Change**. La configuración predeterminada es 7.
Disable Days After Expire	El sistema deshabilita la cuenta del usuario después del vencimiento de la contraseña de acuerdo con el número de días especificado en esta opción. Las entradas válidas son *never* o un número mayor o igual que 0. La configuración predeterminada es never.
Minimum Length of Password	Es la longitud de contraseña mínima requerida. El valor predeterminado es 6.
Minimum Number of Character Classes	El número mínimo de clases de caracteres obligatorio para una contraseña de usuario. El valor predeterminado es 1. Las clases de caracteres incluyen: • Letras en minúscula (a-z) • Letras en mayúscula (A-Z) • Números (0-9) • Caracteres especiales ($, %, #, +, etc.)
Lowercase Character Requirement	Habilita o deshabilita el requisito de al menos un carácter en minúscula. La configuración predeterminada es deshabilitado.
Uppercase Character Requirement	Habilita o deshabilita el requisito de al menos un carácter en mayúscula. La configuración predeterminada es deshabilitado.

Tabla 41 Controles del cuadro de diálogo Change Login Options (continuación)

Elemento	Descripción
One Digit Requirement	Habilita o deshabilita el requisito de al menos un carácter numérico. La configuración predeterminada es deshabilitado.
Special Character Requirement	Habilita o deshabilita el requisito de al menos un carácter especial. La configuración predeterminada es deshabilitado.
Max Consecutive Character Requirement	Habilita o deshabilita el requisito de un máximo de tres caracteres repetidos. La configuración predeterminada es deshabilitado.
Number of Previous Passwords to Block	Especifica el número de contraseñas recordadas. El rango es 0 a 24, y la configuración predeterminada es 1. **Nota** Si se reduce esta configuración, la lista de contraseñas recordadas permanece sin cambios hasta la próxima vez que se modifique la contraseña. Por ejemplo, si esta configuración cambia de 4 a 3, se recuerdan las últimas cuatro contraseñas hasta la próxima vez que se cambie la contraseña.
Maximum login attempts	Especifica el número máximo de intentos de inicio de sesión antes de que se aplique un bloqueo obligatorio a una cuenta de usuario. Este límite se aplica a todas las cuentas de usuario, incluso sysadmin. Un usuario bloqueado no puede iniciar sesión mientras la cuenta está bloqueada. El rango es 4 a 10, y el valor predeterminado es 4.
Unlock timeout (seconds)	Especifica durante cuánto tiempo está bloqueado un usuario después del número máximo de intentos de inicio de sesión. Cuando se alcanza el tiempo de espera de desbloqueo configurado, el usuario puede intentar iniciar sesión. El rango es 120 a 600 segundos, y el período predeterminado es 120 segundos.
Maximum active logins	Especifica el número máximo de inicios de sesión activos que se permitirán. El valor predeterminado es 100.

Administración de usuarios y grupos de directorio

Puede usar DD System Manager para administrar el acceso al sistema para usuarios y grupos en Windows Active Directory, Windows Workgroup y NIS. La autenticación de Kerberos es una opción para clientes CIFS y NFS.

Visualización de la información de Active Directory y Kerberos

La configuración de Active Directory/Kerberos determina los métodos que los clientes CIFS y NFS utilizan para autenticar. El panel Active Directory/Kerberos Authentication muestra esta configuración.

Procedimiento

1. Seleccione **Administration** > **Access** > **Authentication**.
2. Expanda el panel Active Directory/Kerberos Authentication.

Tabla 42 Descripción de etiquetas de Active Directory/ Kerberos Authentication

Elemento	Descripción
Mode	El tipo de modo de autenticación utilizado. En el modo Windows/ Active Directory, los clientes CIFS usan las autenticaciones Active Directory y Kerberos y clientes NFS utilizan la autenticación Kerberos. En el modo Unix, los clientes CIFS utilizan la autenticación de grupo de trabajo (sin Kerberos), y los clientes NFS utilizan la autenticación Kerberos. En el modo Disabled, la autenticación Kerberos está desactivada y los clientes CIFS utilizan la autenticación de grupo de trabajo.
Dominio	El nombre de dominio del grupo de trabajo o Active Directory.
DDNS	Si el Sistema de nombre de dominio está o no habilitado.
Controladores de dominio:	El nombre del controlador de dominio para el grupo de trabajo o Active Directory.
Unidad organizacional	El nombre de la unidad de las organizaciones para el grupo de trabajo o Active Directory.
Nombre del servidor CIFS	El nombre del servidor CIFS en uso (solo en modo Windows).
WINS Server	El nombre del servidor WINS en uso (solo en modo Windows).
Nombre abreviado de dominio	Un nombre abreviado para el dominio.
NTP	Habilitado/deshabilitado (solo en modo UNIX)
NIS	Habilitado/deshabilitado (solo en modo UNIX)
Centro de distribución de claves	Nombre(s) del host o IP(s) de los KDC en uso (solo en modo UNIX)
Acceso administrativo del Active Directory	Enabled/Disabled: Haga clic en Enable o deshabilite el acceso administrativo a los grupos de Active Directory (Windows).

Tabla 43 Grupos y funciones administrativas de Active Directory

Elemento	Descripción
Grupo de Windows	El nombre del grupo de Windows.
Función de administración	La función del grupo (administrador, usuario, etc.).

Configuración de autenticación de Active Directory y Kerberos

Configurar la autenticación de Active Directory hace que el sistema Data Domain sea un componente del dominio de Windows Active Directory. Los clientes CIFS y NFS utilizan la autenticación Kerberos.

Procedimiento

1. Seleccione **Administration** > **Access** > **Authentication**.
   Aparecerá la vista Authentication.
2. Expanda el panel Active Directory/Kerberos Authentication.
3. Haga clic en **Configure...** al costado de Mode para iniciar el asistente de configuración.
   Aparecerá el diálogo Active Directory/Kerberos Authentication.

4. Seleccione **Windows/Active Directory** y haga clic en **Next**.
5. Ingrese el nombre de dominio completo para el sistema (por ejemplo, domain1.local), el nombre de usuario y la contraseña para el sistema Data Domain. Luego, haga clic en **Next**.

   Nota

   Utilice el nombre de dominio completo. Asegúrese de que al usuario le sean asignados privilegios suficientes para unir el sistema al dominio. El nombre de usuario y la contraseña deben ser compatibles con los requisitos de Microsoft para dominios de Active Directory. A este usuario también se le debe asignar el permiso para crear cuentas en este dominio.

6. Seleccione el nombre del servidor CIFS predeterminada o seleccione **Manual** y escriba un nombre de servidor CIFS.
7. Para seleccionar los controladores de dominio, seleccione **Automatically assign**, o seleccione **Manual** y escriba hasta tres nombres de controladores de dominio.

   Puede ingresar nombres de dominio calificados, nombres del host o direcciones IP (IPv4 or IPv6).

8. Para seleccionar una unidad organizacional, seleccione **Use default Computers**, o seleccione **Manual** y escriba el nombre de unidad de la organización.

   Nota

   La cuenta se trasladará a la nueva unidad organizacional.

9. Haga clic en **Next**.

   Aparecerá la página Summary para esta configuración.
10. Haga clic en **Finish**.

    El sistema muestra la información de configuración en la vista Authentication.
11. Para habilitar el acceso administrativo, haga clic en **Enable** a la derecha de **Active Directory Administrative Access**.

Selecciones de modo de autenticación

La selección del modo de autenticación determina la forma de autenticación de los clientes CIFS y NFS mediante combinaciones compatibles de autenticación en Active Directory, grupo de trabajo y Kerberos.

DD OS es compatible con las siguientes opciones de autenticación.

- Desactivado: La autenticación Kerberos está deshabilitada para clientes CIFS y NFS. Los clientes CIFS utilizan la autenticación de grupo de trabajo.
- Windows/Active Directory: La autenticación Kerberos está habilitada para clientes CIFS y NFS. Los clientes CIFS utilizan la autenticación de Active Directory.
- Unix: La autenticación Kerberos está habilitada solo para clientes NFS. Los clientes CIFS utilizan la autenticación de grupo de trabajo.

Administración de grupos administrativos para Active Directory

Puede utilizar el panel de Active Directory/Kerberos Authentication para crear, modificar y eliminar grupos de Active Directory (Windows) y asignar funciones de administración (admin, operador de respaldo, etc.) a esos grupos.

Para la preparación de la administración de grupos, seleccione **Administration** > **Access** > **Authentication** , expanda el panel Active Directory/Kerberos Authentication y haga clic en el botón Enable **Enable** de Active Directory Administrative Access.

Creación de grupos administrativos para Active Directory

Cree un grupo administrativo cuando desee asignar una función de administración a todos los usuarios configurados en un grupo de Active Directory.

Antes de comenzar

Active el acceso administrativo de Active Directory en el panel de la autenticación de Active Directory/Kerberos, en la página **Administration** > **Access** > **Authentication**.

Procedimiento

1. Haga clic en **Create...**
2. Escriba el nombre del dominio y del grupo separado por una barra invertida. Por ejemplo: domainname\groupname.
3. Seleccione la función de administración para el grupo en el menú desplegable.
4. Haga clic en **OK**.

Modificación de los grupos administrativos para Active Directory

Modifique un grupo administrativo cuando desee cambiar el nombre de un grupo administrativo o la función administrativa configuradas para un grupo para Active Directory.

Antes de comenzar

Active el acceso administrativo de Active Directory en el panel de la autenticación de Active Directory/Kerberos, en la página **Administration** > **Access** > **Authentication** .

Procedimiento

1. Seleccione un grupo a modificar bajo el encabezado **Active Directory Administrative Access** heading.
2. Haga clic en **Modify...**.
3. Modifique el nombre de dominio y de grupo. Estos nombres deben estar separados por una barra invertida. Por ejemplo: domainname\groupname.
4. Modifique la función de administración para el grupo al seleccionar una función diferente en el menú desplegable.

Eliminación de grupos administrativos para Active Directory

Eliminar un grupo administrativo cuando desee cancelar el acceso al sistema para todos los usuarios configurados en un grupo de Active Directory.

Antes de comenzar

Active el acceso administrativo de Active Directory en el panel de la autenticación de Active Directory/Kerberos, en la página **Administration** > **Access** > **Authentication** .

Procedimiento

1. Seleccione un grupo a eliminar bajo el encabezado **Active Directory Administrative Access**.
2. Haga clic en **Delete**.

Configuración de la autenticación Kerberos en UNIX

La configuración de la autenticación Kerberos en UNIX permite que los clientes NFS utilicen la autenticación Kerberos. Los clientes CIFS utilizan la autenticación de grupo de trabajo.

Antes de comenzar

NIS debe estar ejecutándose en modo UNIX con autenticación Kerberos para la funcionar. Para obtener instrucciones acerca de cómo habilitar Kerberos, consulte la sección sobre habilitación de servicios NIS.

La configuración de Kerberos para UNIX permite que los clientes NFS utilicen la autenticación Kerberos. Los clientes CIFS utilizan la autenticación de grupo de trabajo.

Procedimiento

1. Seleccione **Administration** > **Access** > **Authentication**.

   Aparecerá la vista Authentication.

2. Expanda el panel Active Directory/Kerberos Authentication.
3. Haga clic en **Configure...** al costado de Mode para iniciar el asistente de configuración.

   Aparecerá el diálogo Active Directory/Kerberos Authentication.
4. Seleccione **Unix** y haga clic en **Next**.
5. Escriba el nombre de dominio (por ejemplo, domain1.local), y hasta tres nombres de host o direcciones IP (IPv4 o IPv6) para los centros de distribución de claves (KDC).
6. Si lo desea, haga clic en **Browse** para cargar un archivo keytab y haga clic en **Next**.

   The Summary page for the configuration appears.

   Nota

   Los archivos keytab se generan en los servidores de autenticación (KDC) y contienen una seña secreta compartida entre el servidor KDC y el DDR.

   AVISO

   Un archivo keytab debe ser cargado e importado para que la autenticación Kerberos opere correctamente.
7. Haga clic en **Finish**.

   El sistema muestra la información de configuración en el panel Active Directory/Kerberos Authentication.

Deshabilitación de la autenticación Kerberos

Deshabilitar de la autenticación Kerberos impide que los clientes CIFS y NFS utilicen la autenticación Kerberos. Los clientes CIFS utilizan la autenticación de grupo de trabajo.

Procedimiento

1. Seleccione **Administration** > **Access Management** > **Authentication**.

   Aparecerá la vista Authentication.

2. Expanda el panel Active Directory/Kerberos Authentication.
3. Haga clic en **Configure...** al costado de Mode para iniciar el asistente de configuración.

   Aparecerá el diálogo Active Directory/Kerberos Authentication.

4. Seleccione **Disabled** y haga clic en **Next**.

   El sistema muestra una página de resumen donde los cambios aparecen en negrita.

5. Haga clic en **Finish**.

   El sistema mostrará Disabled al costado de Mode en el panel Active Directory/ Kerberos Authentication.

Visualización de la información de autenticación del grupo de trabajo

Utilice el panel Workgroup Authentication para ver información de la configuración del grupo de trabajo.

Procedimiento

1. Seleccione **Administration** > **Access** > **Authentication**.
2. Expanda el panel Workgroup Authentication

Tabla 44 Descripción de etiquetas de Workgroup Authentication

Elemento	Descripción
Mode	El tipo de modo de autenticación (Workgroup or Active Directory)
Nombre de grupo de trabajo	El nombre especificado del grupo de trabajo
Nombre del servidor CIFS	El nombre del servidor CIFS en uso.
WINS Server	El nombre del servidor WINS en uso.

Configuración de parámetros de autenticación de grupos de trabajo

Los parámetros de autenticación de grupos de trabajo le permiten configurar un nombre de grupo de trabajo y un nombre de servidor CIFS.

Procedimiento

1. Seleccione **Administration** > **Access** > **Authentication**.

   Aparecerá la vista Authentication.

2. Expanda el panel Workgroup Authentication
3. Haga clic en **Configure**.

   Aparecerá el cuadro de diálogo Workgroup Authentication.

4. Para el nombre del grupo de trabajo, seleccione **Manual** y especifique un nombre de grupo de trabajo para la unión, o use el predeterminado.

El modo de grupo de trabajo une un sistema Data Domain a un dominio de grupo de trabajo.

5. Para el nombre de servidor CIFS, seleccione **Manual** y especifique un nombre de servidor (DDR), o use el predeterminado.
6. Haga clic en **OK**.

Ver la información de autenticación con LDAP

En el panel LDAP Authentication se muestran los parámetros de configuración de LDAP y si la autenticación LDAP está habilitada o deshabilitada.

Habilitar el LDAP le permite usar un servidor o una implementación OpenLDAP existente con el sistema Data Domain para la autenticación de usuarios de nivel de sistema, la asignación de ID de NFSv4, NFSv3 Kerberos con LDAP o NFSv4 Kerberos con LDAP.

Procedimiento

1. Seleccione **Administration** > **Access** > **Authentication**.

   Aparecerá la vista Authentication.

2. Expanda el panel LDAP Authentication.

Resultados

Tabla 45 Elementos del panel LDAP Authentication

Elemento	Descripción
LDAP Status	Enabled o Disabled.
Base Suffix	Sufijo de base de LDAP.
Bind DN	Nombre de la cuenta asociada al servidor de LDAP.
SSL	Enabled o Disabled.
Server	Servidor(es) de autenticación.
LDAP Group	El nombre del grupo de LDAP.
Management Role	La función del grupo (administrador, usuario, etc.).

Habilitar y deshabilitar la autenticación con LDAP

Puede usar el panel LDAP Authentication para habilitar y deshabilitar o restablecer la autenticación con LDAP.

Procedimiento

1. Seleccione **Maintenance** > **Access** > **Authentication**.

   Aparecerá la vista Authentication.

2. Expanda el panel LDAP Authentication.
3. Haga clic en **Enable** junto a LDAP Status para habilitar la autenticación con LDAP o en **Disable** para deshabilitarla.

   Aparecerá el cuadro de diálogo Enable or Disable LDAP Authentication.

Nota

Debe haber un servidor LDAP antes de habilitar la autenticación con LDAP.

4. Haga clic en **OK**.

Restablecer la autenticación con LDAP.

El botón **Reset** deshabilita la autenticación con LDAP y borra la información de configuración de LDAP.

Configuración de la autenticación LDAP

Utilice el panel de LDAP Authentication para configurar la autenticación con LDAP.

Procedimiento

1. Seleccione **Administration** > **Access** > **Authentication**.

   Aparecerá la vista Authentication.

2. Expanda el panel LDAP Authentication.
3. Haga clic en **Configure**.

   Aparecerá el cuadro de diálogo Configure LDAP Authentication.

4. Especifique el sufijo base en el campo **Base Suffix**.
5. Especifique el nombre de la cuenta que se asociará al servidor de LDAP en el campo **Bind DN**.
6. Especifique la contraseña de la cuenta de nombre de dominio de vinculación en el campo **Bind Password**.
7. Opcionalmente, seleccione **Enable SSL**.
8. Opcionalmente, seleccione **Demand server certificate** para requerir que el sistema Data Domain importe un certificado de CA desde el servidor LDAP.
9. Haga clic en **OK**.
10. Si es necesario en un momento posterior, haga clic en **Reset** para que la configuración de LDAP vuelva a sus valores predeterminados.

Especificar los servidores de autenticación con LDAP

Puede usar el panel LDAP Authentication para especificar los servidores de autenticación con LDAP.

Antes de comenzar

La autenticación con LDAP se debe deshabilitar antes de configurar un servidor LDAP.

Nota

El rendimiento de DD SM al iniciar sesión con LDAP disminuirá a medida que el número de saltos entre el sistema Data Domain y el servidor LDAP aumente.

Procedimiento

1. Seleccione **Administration** > **Access** > **Authentication**.

   Aparecerá la vista Authentication.

2. Expanda el panel LDAP Authentication.
3. Haga clic en el botón **+** para agregar un servidor.
4. Especifique el servidor LDAP en uno de los siguientes formatos:
   - Dirección IPv4:`10.26.16.250`
   - Dirección IPv6:`[::ffff:9.53.96.21]`
   - Hostname:`myldapserver`
5. Haga clic en **OK**.

Configurar grupos de LDAP

Utilice el panel de LDAP Authentication para configurar los grupos de LDAP.

La configuración de grupos de LDAP solo se aplica cuando se utiliza LDAP para la autenticación de usuarios en el sistema Data Domain.

Procedimiento

1. Seleccione **Administration** > **Access** > **Authentication**.

   Aparecerá la vista Authentication.
2. Expanda el panel LDAP Authentication.
3. Configure los grupos de LDAP en la tabla LDAP Group.
   - Para agregar un grupo de LDAP, haga clic en Add (**+**), escriba el nombre del grupo de LDAP y su función, y haga clic en **OK**.
   - Para modificar un grupo de LDAP, seleccione la casilla de verificación del nombre del grupo que aparece en la lista de grupos de LDAP y haga clic en Edit (lápiz). Cambie el nombre del grupo de LDAP y haga clic en **OK**.
   - Para quitar un nombre de grupo de LDAP, seleccione el grupo de LDAP en la lista y haga clic en Delete **X**.

Usar la interfaz de línea de comandos (CLI) para configurar la autenticación con LDAP

Puede utilizar la interfaz de línea de comandos de Data Domain para configurar un servidor o implementación existente de OpenLDAP con un sistema Data Domain para la autenticación de usuarios de nivel de sistema, la asignación de ID de NFSv4, NFSv3 Kerberos con LDAP o NFSv4 Kerberos con LDAP.

Configurar servidores LDAP

Puede configurar uno o más servidores LDAP al mismo tiempo.

Nota

LDAP debe estar deshabilitado cuando se realiza cualquier cambio a la configuración.

Especifique el servidor LDAP en uno de los siguientes formatos:

- Dirección IPv4: `10.<A>.<B>.<C>`
- Dirección IPv4 con número de puerto: `10.<A>.<B>.<C>:400`
- Dirección IPv6:`[::ffff:9.53.96.21]`
- Dirección IPv6 con número de puerto:`[::ffff:9.53.96.21]:400`

- Hostname:**myldapserver**
- Hostname con número de puerto:**myldapserver:400**

Cuando se configuran varios servidores:

- Separe cada servidor con un espacio.
- El primer servidor en la lista cuando se usa el comando `authentication ldap servers add` se convierte en el servidor principal.
- Si no se puede configurar alguno de los servidores, el comando falla para todos los servidores de la lista.

Procedimiento

1. Agregue uno o más servidores LDAP mediante el comando `authentication ldap servers add`:

```
# authentication ldap servers add 10.A.B.C 10.X.Y.Z:400
LDAP server(s) added
LDAP Server(s):        2
#     IP Address/Hostname
---   --------------------
1.    10.A.B.C (primary)
2.    10.X.Y.Z:400
---   --------------------
```

2. Quite uno o más servidores LDAP mediante el comando `authentication ldap servers del`:

```
# authentication ldap servers del 10.X.Y.Z:400
LDAP server(s) deleted.
LDAP Servers: 1
#   Server
-   ------------   ---------
1   10.A.B.C       (primary)
-   ------------   ---------
```

3. Quite todos los servidores LDAP mediante el comando `authentication ldap servers reset`:

```
# authentication ldap servers reset
LDAP server list reset to empty.
```

Configuración del sufijo base de LDAP

El sufijo base es el DN base de búsqueda y es donde comienza a buscar el directorio de LDAP.

Procedimiento

1. Configure el sufijo base de LDAP con el comando `authentication ldap base set`:

```
# authentication ldap base set "dc=anvil,dc=team"
LDAP base-suffix set to "dc=anvil,dc=team".
```

2. Restablezca el sufijo base de LDAP con el comando `authentication ldap base reset`:

```
# authentication ldap base reset
LDAP base-suffix reset to empty.
```

Configuración de autenticación de cliente LDAP

Configure la cuenta (nombre de dominio de vinculación) y la contraseña (contraseña de vinculación) que se utilizan para realizar la autenticación con el servidor LDAP y hacer consultas.

Siempre debe configurar el nombre de dominio y la contraseña de vinculación. Por lo general, los servidores LDAP requieren una vinculación autenticada de forma predeterminada. Si `client-auth` no se configura, se solicita el acceso anónimo y no se proporciona ningún nombre ni contraseña. El resultado de `authentication ldap show` es el siguiente:

```
# authentication ldap show
LDAP configuration
        Enabled:         yes (*)
        Base-suffix:     dc=u2,dc=team
        Binddn:          (anonymous)
        Server(s):       1
#   Server
-   -------------   ---------
1   10.207.86.160   (primary)
-   -------------   ---------

Secure LDAP configuration
        SSL Enabled:     no
        SSL Method:      off
        tls_reqcert:     demand

(*) Requires a filesystem restart for the configuration to take
effect.
```

Si se establece binddn mediante la CLI `client-auth`, pero bindpw no está disponible, se solicita acceso sin autenticar.

```
# authentication ldap client-auth set binddn
"cn=Manager,dc=u2,dc=team"
Enter bindpw:
** Bindpw is not provided. Unauthenticated access would be requested.
LDAP client authentication binddn set to "cn=Manager,dc=u2,dc=team".
```

Procedimiento

1. Configure el nombre de dominio y la contraseña de vinculación con el comando `authentication ldap client-auth set binddn`:

   ```
   # authentication ldap client-auth set binddn
   "cn=Administrator,cn=Users,dc=anvil,dc=team"
       Enter bindpw:
       LDAP client authentication binddn set to
   "cn=Administrator,cn=Users,dc=anvil,dc=team".
   ```

2. Restablezca el nombre de dominio y la contraseña de vinculación con el comando `authentication ldap client-auth reset`:

   ```
   # authentication ldap client-auth reset
   LDAP client authentication configuration reset to empty.
   ```

Activación de LDAP

Antes de comenzar

Una configuración de LDAP debe existir antes de activar LDAP. Además, debe deshabilitar NIS, asegurarse de que el servidor LDAP esté accesible y poder consultar el DSE raíz del servidor LDAP.

Procedimiento

1. Active LDAP con el comando `authentication ldap enable`:

```
# authentication ldap enable
```

   Se muestran los detalles de la configuración de LDAP para que los confirme antes de continuar. Para continuar, escriba **yes** y reinicie el sistema de archivos a fin de que se aplique la configuración de LDAP.

2. Puede ver la configuración de LDAP actual con el comando `authentication ldap show`:

```
# authentication ldap show
LDAP configuration
        Enabled:          no
        Base-suffix:      dc=anvil,dc=team
        Binddn:
cn=Administrator,cn=Users,dc=anvil,dc=team
        Server(s):        2
#   Server
-   ----------------   ---------
1   10.26.16.250       (primary)
2   10.26.16.251:400
-   ----------------   ---------

Secure LDAP configuration
        SSL Enabled:      no
        SSL Method:       off
        tls_reqcert:      demand
```

   Se muestran los detalles de configuración básica de LDAP y segura de LDAP.

3. Puede ver el estado de LDAP actual con el comando `authentication ldap status`:

```
# authentication ldap status
```

   Se muestra el estado de LDAP. Si el estado de LDAP no es `good`, el problema se identifica en la salida. Por ejemplo:

```
# authentication ldap status
Status: invalid credentials
```

   o

```
# authentication ldap status
Status: invalid DN syntax
```

4. Deshabilite LDAP con el comando `authentication ldap disable`:

```
# authentication ldap disable
LDAP is disabled.
```

Habilitación de LDAP seguro

Puede configurar DDR para utilizar LDAP seguro mediante la habilitación de SSL.

Antes de comenzar

Si no hay un certificado de CA de LDAP y `tls_reqcert` está configurado en `demand`, la operación falla. Importe un certificado de CA de LDAP y vuelva a intentarlo.

Si `tls_reqcert` está configurado en `never`, no se requiere un certificado de CA de LDAP. Para obtener más información, consulte Configuración de la verificación del certificado del servidor LDAP con certificados CA importados en la página 136.

Procedimiento

1. Habilite SSL con el comando `authentication ldap ssl enable`:

   ```
   # authentication ldap ssl enable
   Secure LDAP is enabled with 'ldaps' method.
   ```

   El método predeterminado es el LDAP seguro o *ldaps*. Puede especificar otros métodos, como el TLS:

   ```
   # authentication ldap ssl enable method start_tls
   Secure LDAP is enabled with 'start_tls' method.
   ```

2. Deshabilite SSL con el comando `authentication ldap ssl disable`:

   ```
   # authentication ldap ssl disable
   Secure LDAP is disabled.
   ```

Configuración de la verificación del certificado del servidor LDAP con certificados CA importados

Puede cambiar el comportamiento del certificado de solicitud de TLS.

Procedimiento

1. Cambie el comportamiento del certificado de solicitud de TLS con el comando `authentication ldap ssl set tls_reqcert`.

   No verifique el certificado:

   ```
   # authentication ldap ssl set tls_reqcert never
   "tls_reqcert" set to "never". LDAP server certificate will not
   be verified.
   ```

   Verifique el certificado:

   ```
   # authentication ldap ssl set tls_reqcert demand
   "tls_reqcert" set to "demand". LDAP server certificate will be
   verified.
   ```

2. Restablezca el comportamiento del certificado de solicitud de TLS con el comando `authentication ldap ssl reset tls_reqcert`. El comportamiento predeterminado es `demand`.

   ```
   # authentication ldap ssl reset tls_reqcert
   tls_reqcert has been set to "demand". LDAP Server certificate
   will be verified with imported CA certificate.Use "adminaccess"
   CLI to import the CA certificate.
   ```

Administración de certificados de CA para LDAP

Puede importar o eliminar certificados, y ver información del certificado actual.

Procedimiento

1. Importe un certificado de CA para la verificación del certificado de servidor LDAP con el comando `adminaccess certificate import`.

   Especifique `ldap` para `ca application`:

   ```
   # adminaccess certificate import{host application {all | aws-
   federal | ddboost | https| keysecure | rkm | <application-
   list>}| ca application { ldap }} [file <file-name>] Import host
   or ca certificate
   ```

2. Elimine un certificado de CA para la verificación del certificado del servidor LDAP con el comando `adminaccess certificate delete`.

   Especifique `ldap` para `application`:

```
# adminaccess certificate delete
{ subject <subject-name> | fingerprint <fingerprint>}
[application { ldap }]
```

Especifique `ldap` para `imported-ca application`:

```
# adminaccess certificate delete
{ imported-host application { all | aws-federal | ddboost |
https
| keysecure | rkm | <application-list>}
| imported-ca application { ldap }}
```

3. Vea la información actual del certificado de CA para la verificación del certificado del servidor LDAP con el comando `adminaccess certificate show`:

```
# adminaccess certificate show imported-ca ldap
```

Visualización de información de autenticación NIS

En el panel NIS Authentication se muestran los parámetros de configuración de NIS y si la autenticación NIS está habilitada o deshabilitada.

Procedimiento

1. Seleccione **Administration** > **Access** > **Authentication**.

   Aparecerá la vista Authentication.

2. Expanda el panel NIS Authentication.

Resultados

Tabla 46 Elementos del panel NIS Authentication

Elemento	Descripción
NIS Status	Activado o Desactivado.
Nombre del dominio	El nombre del dominio para este servicio.
Servidor	Servidor(es) de autenticación.
NIS Group	El nombre del grupo NIS.
Función de administración	La función del grupo (administrador, usuario, etc.).

Activación y desactivación de la autenticación NIS

Puede usar el panel NIS Authentication para habilitar y deshabilitar la autenticación NIS.

Procedimiento

1. Seleccione **Maintenance** > **Access** > **Authentication**.

   Aparecerá la vista Authentication.

2. Expanda el panel NIS Authentication.
3. Haga clic en **Enable** junto a NIS Status para habilitar o en **Disable** para deshabilitar NIS Authentication.

   Aparecerá el cuadro de diálogo Enable or Disable NIS.

4. Haga clic en **OK**.

Configuración del nombre de dominio NIS

Puede usar el panel NIS Authentication para configurar el nombre de dominio NIS.

Procedimiento

1. Seleccione **Administration** > **Access** > **Authentication**.

   Aparecerá la vista Authentication.

2. Expanda el panel NIS Authentication.
3. Haga clic en **Edit** junto a Domain Name para editar el nombre de dominio NIS.

   Aparecerá el cuadro de diálogo Configure NIS Domain Name.

4. Especifique el nombre de dominio en el cuadro **Domain Name**.
5. Haga clic en **OK**.

Especificación de servidores de autenticación NIS

Puede usar el panel NIS Authentication para especificar servidores de autenticación NIS.

Procedimiento

1. Seleccione **Administration** > **Access** > **Authentication**.

   Aparecerá la vista Authentication.

2. Expanda el panel NIS Authentication.
3. Debajo de Domain Name, seleccione una de las siguientes opciones:
   - **Obtain NIS Servers from DHCP**: el sistema obtiene automáticamente servidores NIS a través de DHCP.
   - **Manually Configure**: use los siguientes procedimientos para configurar manualmente los servidores NIS.

   - Para agregar un servidor de autenticación, haga clic en Add (**+**) en la tabla de servidores, escriba el nombre del servidor y haga clic en **OK**.
   - Para modificar un servidor de autenticación, seleccione el nombre del servidor de autenticación y haga clic en el ícono de edición (lápiz). Cambie el nombre del servidor y haga clic en **OK**.
   - Para quitar el nombre de un servidor de autenticación, seleccione un servidor, haga clic en el ícono X y, a continuación, haga clic en **OK**.
4. Haga clic en **OK**.

Configuración de los grupos NIS

Utilice el panel de NIS Authentication para configurar grupos NIS.

Procedimiento

1. Seleccione **Administration** > **Access** > **Authentication**.

   Aparecerá la vista Authentication.

2. Expanda el panel NIS Authentication.

3. Configure los grupos NIS en la tabla NIS Group.
   - Para agregar un grupo NIS, haga clic en Add (**+**), escriba el nombre del grupo NIS y su función, luego haga clic en **Validate**. Haga clic en **OK** para cerrar el cuadro de diálogo Agregar grupo NIS. Haga clic en **OK** de nuevo para cerrar el cuadro de diálogo **Configure Allowed NIS Groups**.
   - Para modificar un grupo NIS, seleccione la casilla de verificación del nombre del grupo NIS que aparece en la lista de grupos NIS y haga clic en Edit (lápiz). Cambie el nombre del grupo de NIS y haga clic en **OK**.
   - Para eliminar un nombre de grupo de NIS, seleccione el grupo de NIS en la lista y haga clic en Delete **X**.
4. Haga clic en **OK**.

Diagnóstico de problemas de autenticación

Data Domain Operating System proporciona la capacidad de diagnosticar problemas de autenticación de Active Directory desde la interfaz de Data Domain System Manager.

Procedimiento

1. Seleccione **Administration** > **Access** > **Authentication**
2. Expanda el panel Active Directory/Kerberos Authentication.
3. Haga clic en **Diagnose**.
4. Seleccione un problema para investigar y haga clic en **Diagnose**.
5. Proporcione la información solicitada.

   Para diagnosticar problemas al iniciar sesión como usuario de Active Directory, proporcione lo siguiente:
   - Dirección IP del servidor de Active Directory
   - FQDN del servidor de Active Directory
   - Nombre de usuario del servicio de Active Directory

     Nota

     La cuenta de usuario de Active Directory especificada aquí requiere los siguientes privilegios:
     - Acceso de solo lectura al DN base identificado por el nombre de dominio.
     - Acceso de solo lectura a los atributos de consulta de todos los usuarios del DN base.
     - Acceso de solo lectura a los atributos de consulta de la cuenta de equipo para el sistema Data Domain.
   - Contraseña de servicio de Active Directory
   - Nombre de usuario de Data Domain que experimenta el error al iniciar sesión

   Para diagnosticar problemas que unen el sistema Data Domain a un dominio de Active Directory, proporcione lo siguiente:
   - Dirección IP del servidor de Active Directory
   - FQDN del servidor de Active Directory

- Nombre de usuario del servicio Active Directory
- Contraseña de servicio de Active Directory

6. Haga clic en **Diagnose**.
7. Consulte el informe.
   - Haga clic en **View Report** para ver el informe en línea. Se puede hacer clic en cada elemento de la tabla Action Items para obtener más detalles.
   - Haga clic en **Download** para descargar una copia del informe.
8. Analice e implemente las reparaciones que se sugieren para el problema y reintente la operación.

Cambio del método de autenticación del sistema

El sistema Data Domain es compatible con la autenticación basada en contraseña o basada en certificado. La autenticación basada en contraseña es el método predeterminado.

Antes de comenzar

La autenticación basada en certificado requiere claves SSH, y los certificados de CA se importan para permitir a los usuarios autenticarse con el sistema cuando la autenticación basada en contraseña está deshabilitada.

Realice los siguientes pasos para cambiar el método de autenticación del sistema de autenticación basada en contraseña a autenticación basada en certificado.

Procedimiento

1. Seleccione **Administration** > **Access**.

   Aparecerá la vista Access Management.
2. Haga clic en **Manage CA Certificates**.
3. Haga clic en **Add** para crear un certificado nuevo.
4. Agregue el certificado.
   - Seleccione **I want to upload the certificate as a .pem file** y haga clic en **Choose File** para seleccionar el archivo de certificado y cargarlo al sistema.
   - Seleccione **I want to copy and paste the certificate text** para copiar y pegar el texto del certificado en el campo de texto.
5. Haga clic en **Add**.
6. Seleccione **More Tasks** > **Change Login Options**.
7. En el menú desplegable **Password Based Login**, seleccione **Disable**.

   Nota

   El menú desplegable está desactivado si las claves SSH requeridas y los certificados de CA no están configurados en el sistema.

8. Haga clic en **OK**.

   Si se configura una política de seguridad, el sistema solicita las credenciales del director de seguridad. Proporcione las credenciales y haga clic en **OK**.

Restablezca el método de autenticación del sistema a la autenticación basada en contraseña.

Realice los siguientes pasos para cambiar el método de autenticación del sistema de autenticación basada en certificado a autenticación basada en contraseña.

Procedimiento

1. Seleccione **Administration** > **Access**.

   Aparecerá la vista Access Management.

2. Seleccione **More Tasks** > **Change Login Options**.
3. En el menú desplegable **Password Based Login**, seleccione **Enable**.
4. Haga clic en **OK**.

   Si se configura una política de seguridad, el sistema solicita las credenciales del director de seguridad. Proporcione las credenciales y haga clic en **OK**.

Configuración de ajustes del servidor de correo

La pestaña Mail Server le permite especificar el servidor de correo al cual DD OS envía informes por correo electrónico.

Procedimiento

1. Seleccione **Administration** > **Settings** > **Mail Server**.
2. Seleccione **More Tasks** > **Set Mail Server**.

   Aparecerá el cuadro de diálogo Set Mail Server.

3. Especifique el nombre del servidor de correo electrónico en el campo **Mail Server**.
4. Utilice el botón **Credentials** para habilitar o deshabilitar el uso de credenciales para el servidor de correo electrónico.
5. Si las credenciales están habilitadas, especifique el nombre de usuario del servidor de correo electrónico en el campo **User Name**.
6. Si las credenciales están habilitadas, especifique la contraseña del servidor de correo electrónico en el campo **Password**.
7. Haga clic en **Set**.
8. Opcionalmente, utilice la CLI para verificar y solucionar problemas de la configuración del servidor de correo electrónico.
   a. Ejecute el comando `config show mailserver` para verificar que el servidor de correo electrónico esté configurado.
   b. Ejecute el comando `net ping <mailserver-hostname> count 4` para enviar un ping al servidor de correo electrónico.
   c. Si el servidor de correo electrónico no está configurado correctamente, ejecute el comando `config set mailserver <mailserver-hostname>` para establecer el servidor de correo electrónico e intente enviar un ping nuevamente.
   d. Ejecute el comando `net show dns` para verificar que el servidor DNS esté configurado.
   e. Ejecute el comando `net ping <DNS-hostname> count 4` para enviar un ping al servidor DNS.

f. Si el servidor DNS no está configurado correctamente, ejecute el comando `config set dns <dns-IP>` para establecer el servidor DNS e intente enviar un ping nuevamente.

g. Opcionalmente, ejecute el comando `net hosts add <IP-address> <hostname>` para agregar la dirección IP y el nombre de host del servidor de correo electrónico al archivo de hosts de Data Domain para la resolución local.

h. Ejecute el comando `net ping <mailserver-hostname> count 4` para enviar un ping al servidor de correo electrónico.

Administración de configuración de fecha y hora

La pestaña Time and Date Settings le permite ver y configurar la fecha y la hora del sistema o configurar el protocolo de hora de red para establecer la fecha y la hora.

Procedimiento

1. Para ver la configuración de fecha y hora actual, seleccione **Administration** > **Settings** > **Time and Date Settings**.

   La página Time and Date Settings presenta la fecha y la hora actuales del sistema, muestra si NTP está habilitado o no y muestra las direcciones IP o los nombres de host de los servidores NTP configurados.

2. Para cambiar la configuración, seleccione **More Tasks** > **Configure Time Settings**.

   Aparecerá el cuadro de diálogo Configure Time Settings.

3. En la lista desplegable **Time Zone**, seleccione la zona horaria donde reside el sistema Data Domain.
4. Para configurar manualmente la fecha y la hora, seleccione **None**, escriba la fecha en el cuadro Date**Date** y seleccione la hora en las listas desplegables **Time**.
5. Para usar NTP para sincronizar la hora, seleccione NTP y establezca cómo se accede al servidor NTP.
   - Para usar DHCP para seleccionar automáticamente un servidor, seleccione **Obtain NTP Servers using DHCP**.
   - Para configurar la dirección IP de un servidor NTP, seleccione **Manually Configure**, agregue la dirección IP del servidor y haga clic en **OK**.

   Nota

   El uso de sincronización de hora de un controlador de dominio de Active Directory puede provocar cambios de hora excesivos en el sistema si NTP y el controlador de dominio están modificando la hora.

6. Haga clic en **OK**.
7. Si cambió la zona horaria, debe reiniciar el sistema.
   a. Seleccione **Maintenance** > **System**.
   b. En el menú More Tasks, seleccione Reboot System.

c. Haga clic en OK para confirmar.

Administración de propiedades del sistema

La pestaña System Properties le permite ver y configurar propiedades del sistema que identifican la ubicación del sistema administrado, la dirección de correo electrónico del administrador y el nombre de host.

Procedimiento

1. Para ver la configuración actual, seleccione **Administration** > **Settings** > **System Properties**.

   La pestaña System Properties muestra la ubicación del sistema, la dirección de correo electrónico del administrador y el nombre de host del administrador.

2. Para cambiar la configuración, seleccione **More Tasks** > **Set System Properties**.

   Aparecerá el cuadro de diálogo Set System Properties.

3. En el cuadro **Location**, especifique información acerca de la ubicación del sistema Data Domain.
4. En el cuadro **Admin Email**, especifique la dirección de correo electrónico del administrador del sistema.
5. En el cuadro **Admin Host**, especifique el nombre del servidor del administrador.
6. Haga clic en **OK**.

Administración de SNMP

El Protocolo simple de administración de red (SNMP) es un protocolo estándar para intercambiar información de administración de redes. El protocolo SNMP forma parte de un conjunto de protocolos denominado Protocolo de control de transmisión/ Protocolo de Internet (TCP/IP). El protocolo SNMP es una herramienta que los administradores de red pueden usar para monitorear y administrar dispositivos conectados a la red, como los sistemas Data Domain, en busca de condiciones que justifiquen su atención.

Para monitorear sistemas Data Domain con SNMP, deberá instalar Data Domain MIB en el sistema de administración SNMP. El SO DD también admite MIB-II estándar para que también pueda consultar estadísticas de MIB-II de datos generales, como estadísticas de red. Para lograr cobertura completa de los datos disponibles, debe usar tanto Data Domain MIB como MIB-II MIB estándar.

El agente SNMP del sistema Data Domain acepta consultas de información específica de Data Domain desde sistemas de administración que usan SNMP v1, v2c y v3. SNMP V3 proporciona un mayor grado de seguridad que v2c y v1 mediante el reemplazo de cadenas de comunidad de texto no cifrado (como forma de autenticación), con autenticación basada en usuario mediante MD5 o SHA1. Asimismo, se pueden cifrar los paquetes de autenticación de usuario con SNMP v3, y se puede verificar su integridad con DES o AES.

Los sistemas Data Domain pueden enviar SNMP traps (que son mensajes de alerta) utilizando SNMP v2c y SNMP v3. Dado que no se admiten traps de SNMP v1, si es posible, utilice SNMP v2c o v3.

El puerto predeterminado que se abre al habilitar SNMP es el puerto 161. Los traps se envían a través del puerto 162.

- En la *Guía de configuración inicial de Data Domain Operating System* se describe cómo configurar el sistema Data Domain para usar monitoreo de SNMP.
- En la *Guía de referencia rápida de MIB de Data Domain Operating System* se describe el conjunto completo de parámetros de MIB incluido en la opción Data Domain MIB.

Visualización del estado y la configuración de SNMP

La pestaña SNMP muestra el estado y la configuración en curso de SNMP.

Procedimiento

1. Seleccione **Administration** > **Settings** > **SNMP**.

   La vista de SNMP muestra el estado de SNMP, las propiedades de SNMP y la configuración de SNMP V3 y de SNMP V2C.

Etiquetas de la pestaña SNMP

Las etiquetas de la pestaña SNMP identifican el estado general de SNMP, los valores de propiedad de SNMP y las opciones de configuración de SNMPv3 y SNMPv2.

Status
El área Status muestra el estado operativo del agente SNMP en el sistema, que está habilitado o deshabilitado.

Propiedades de SNMP

Tabla 47 Descripciones de las propiedades de SNMP

Elemento	Descripción
SNMP System Location	La ubicación del sistema Data Domain que se está monitoreando.
SNMP System Contact	La persona designada como contacto para la administración del sistema Data Domain.
SNMP System Notes	Datos de configuración de SNMP adicionales (opcional).
SNMP Engine ID	Un identificador hexadecimal único para el sistema Data Domain.

Configuración de SNMP V3

Tabla 48 Descripciones de la columna SNMP Users

Elemento	Descripción
Name	El nombre del usuario en SNMP Manager con acceso al agente para el sistema Data Domain.
Access	Los permisos de acceso para el usuario de SNMP, que pueden ser de solo lectura o de lectura y escritura.
Authentication Protocols	El protocolo de autenticación utilizado para validar al usuario de SNMP, que puede ser MD5, SHA1 o ninguno.
Privacy Protocol	El protocolo de cifrado utilizado durante la autenticación del usuario de SNMP, que puede ser AES, DES o ninguno.

Tabla 49 Descripciones de la columna Trap Hosts

Elemento	Descripción
Host	La dirección IP o el nombre de dominio del host de administración de SNMP.
Port	El puerto utilizado para la comunicación de SNMP trap con el host. Por ejemplo, 162 es el valor predeterminado.
User	El usuario en el host de trap autenticado para acceder a la información de Data Domain SNMP.

Configuración de SNMP V2C

Tabla 50 Descripciones de la columna Communities

Elemento	Descripción
Community	El nombre de la comunidad. Por ejemplo, Comunidad pública, privada o local.
Access	El permiso de acceso asignado, que puede ser de solo lectura o de lectura y escritura.
Hosts	Los hosts en esta comunidad.

Tabla 51 Descripciones de la columna Trap Hosts

Elemento	Descripción
Host	Los sistemas designados para recibir SNMP traps generados por el sistema Data Domain. Si este parámetro está configurado, los sistemas reciben mensajes de alerta, incluso si el agente SNMP está deshabilitado.
Port	El puerto utilizado para la comunicación de SNMP trap con el host. Por ejemplo, 162 es el valor predeterminado.
Community	El nombre de la comunidad. Por ejemplo, Comunidad pública, privada o local.

Activación y desactivación de SNMP

Use la pestaña SNMP para activar o desactivar SNMP.

Procedimiento

1. Seleccione **Administration** > **Settings** > **SNMP**.
2. En el área Status, haga clic en **Enable** o en **Disable**.

Descarga de SNMP MIB

Use la pestaña SNMP para descargar SNMP MIB.

Procedimiento

1. Seleccione **Administration** > **Settings** > **SNMP**.
2. Haga clic en **Download MIB file**.

3. En el cuadro de diálogo Opening DATA_DOMAIN.mib, seleccione **Open**.
4. Haga clic en **Browse** y seleccione un navegador para ver MIB en una ventana.

   Nota

   Si usa Microsoft Internet Explorer, active Automatic prompting para descargar el archivo.

5. Guarde el archivo MIB o salga del navegador.

Configuración de las propiedades de SNMP

Utilice la pestaña SNMP para configurar las entradas de texto para la ubicación y el contacto del sistema.

Procedimiento

1. Seleccione **Administration** > **Settings** > **SNMP**.
2. En el área SNMP Properties, haga clic en **Configure**.

   Aparecerá el cuadro de diálogo SNMP Configuration.

3. En los campos de texto, especifique la siguiente información:
   - SNMP System Location: Una descripción del lugar donde se encuentra el sistema Data Domain.
   - SNMP System Contact: La dirección de correo electrónico del administrador del sistema para el sistema Data Domain.
   - SNMP System Notes: Información de configuración de SNMP adicional (opcional).
   - SNMP Engine ID: Un identificador único para la entidad SNMP. El ID del motor debe constar de 5 a 34 caracteres hexadecimales (SNMPv3 solamente).

     Nota

     El sistema muestra un error si el ID de motor de SNMP no cumple con los requisitos de longitud o si se utilizan caracteres no válidos.

4. Haga clic en **OK**.

Administración de usuarios SNMP V3

Puede usar la pestaña SNMP para crear, modificar y eliminar usuarios SNMPv3 y hosts de traps.

Creación de usuarios SNMP V3

Cuando crea usuarios SNMPv3, puede definir un nombre de usuario, especificar acceso de solo lectura o de lectura y escritura, y seleccionar un protocolo de autenticación.

Procedimiento

1. Seleccione **Administration** > **Settings** > **SNMP**.
2. En el área SNMP Users, haga clic en **Create**.

   Aparecerá el cuadro de diálogo Create SNMP User.

3. En el campo de texto **Name**, especifique el nombre del usuario al que desea otorgarle acceso al agente del sistema Data Domain. El nombre debe tener un mínimo de ocho caracteres.
4. Seleccione acceso de solo lectura o de lectura y escritura para este usuario.
5. Para autenticar al usuario, seleccione **Authentication**.
   a. Seleccione el protocolo MD5 o SHA1.
   b. Especifique la clave de autenticación en el campo de texto **Key**.
   c. Para proporcionar cifrado a la sesión de autenticación, seleccione **Privacy**.
   d. Seleccione el protocolo AES o DES.
   e. Especifique la clave de cifrado en el campo de texto **Key**.
6. Haga clic en **OK**.

   La cuenta de usuario agregada recientemente aparecerá en la tabla SNMP Users.

Modificación de usuarios SNMP V3

Puede modificar el nivel de acceso (de solo lectura o de lectura y escritura) y el protocolo de autenticación para usuarios SNMPv3 existentes.

Procedimiento

1. Seleccione **Administration** > **Settings** > **SNMP**.
2. En el área **SNMP Users**, seleccione una casilla de verificación para el usuario y haga clic en **Modify**.

   Aparecerá el cuadro de diálogo Modify SNMP User. Agregue o cambie las siguientes configuraciones:

3. Seleccione acceso de solo lectura o de lectura y escritura para este usuario.
4. Para autenticar al usuario, seleccione **Authentication**.
   a. Seleccione el protocolo MD5 o SHA1.
   b. Especifique la clave de autenticación en el campo de texto Key.
   c. Para proporcionar cifrado a la sesión de autenticación, seleccione **Privacy**.
   d. Seleccione el protocolo AES o DES.
   e. Especifique la clave de cifrado en el campo de texto **Key**.
5. Haga clic en **OK**.

   La nueva configuración de esta cuenta de usuario aparecerá en la tabla SNMP Users.

Eliminación de usuarios SNMP V3

Puede usar la pestaña SNMP para eliminar usuarios SNMPv3 existentes.

Procedimiento

1. Seleccione **Administration** > **Settings** > **SNMP**.
2. En el área SNMP Users, seleccione una casilla de verificación para el usuario y haga clic en **Delete**.

   Aparecerá el cuadro de diálogo Delete SNMP User.

Nota

Si el botón **Delete** está deshabilitado, el usuario seleccionado está en uso en uno o más hosts de traps. Elimine los hosts de traps y, a continuación, elimine el usuario.

3. Verifique el nombre de usuario que se eliminará y haga clic en **OK**.
4. En el cuadro de diálogo Delete SNMP User Status, haga clic en **Close**.

   La cuenta de usuario se eliminará de la tabla SNMP Users.

Administración de comunidades SNMP V2C

Puede definir comunidades SNMP v2c (que funcionan como contraseñas) para controlar el acceso al sistema de administración del sistema Data Domain. Para restringir el acceso a determinados hosts que usan la comunidad especificada, asigne los hosts a la comunidad.

Nota

La cadena SNMP V2c Community se envía en texto no cifrado y es muy fácil de interceptar. Si esto ocurre, el interceptor puede recuperar información de dispositivos de la red, modificar su configuración y, posiblemente, apagarlos. SNMP V3 proporciona funciones de cifrado y autenticación para evitar la intercepción.

Nota

Las definiciones de comunidades SNMP no permiten la transmisión de SNMP traps a una estación administrada. Debe definir hosts de trap para permitir el envío de traps a estaciones administradas.

Creación de comunidades SNMP V2C

Cree comunidades para restringir el acceso al sistema DDR o para ser usadas en el envío de capturas a un host de captura. Debe crear una comunidad y asignarla a un host antes de que le sea posible seleccionar a esa misma comunidad para su uso con el host de capturas.

Procedimiento

1. Seleccione **Administration** > **Settings** > **SNMP**.
2. En el área Communities, haga clic en **Create**.

   Aparecerá el cuadro de diálogo Create SNMP V2C Community.

3. En el cuadro **Community**, escriba el nombre de una comunidad a la que desea que el agente de sistema Data Domain tenga acceso.
4. Seleccione acceso de solo lectura o de lectura y escritura para esta comunidad.
5. Si desea asociar la comunidad a uno o más hosts, agregue los hosts de la siguiente manera:

   a. Haga clic en **+** para agregar un host.

      Aparecerá el cuadro de diálogo Host.

   b. En el campo de texto **Host**, escriba la dirección IP o el nombre de dominio del host.

c. Haga clic en **OK**.

El Host será agregado a la lista de host.

6. Haga clic en **OK**.

La nueva entrada de la comunidad aparece en la tabla de **Communities** y enumera los hosts seleccionados.

Modificación de comunidades SNMP V2C

Procedimiento

1. Seleccione **Administration** > **Settings** > **SNMP**.
2. En el área Communities, seleccione la casilla de verificación de la comunidad y haga clic en **Modify**.

   Aparecerá el cuadro de diálogo Modify SNMP V2C Community.

3. Para cambiar el modo de acceso para esta comunidad, seleccione el acceso de **read-only** o de **read-write**.

   Nota

   Los botones de acceso de la comunidad seleccionada están deshabilitados cuando hay un host de trap del mismo sistema configurado como parte de esa comunidad. Para modificar la configuración de acceso, elimine el host de trap y vuélvalo a agregar después de que se modifique la comunidad.

4. Para agregar uno o más hosts a esta comunidad, realice lo siguiente:
   a. Haga clic en **+** para agregar un host.

      Aparecerá el cuadro de diálogo Host.

   b. En el campo de texto **Host**, escriba la dirección IP o el nombre de dominio del host.
   c. Haga clic en **Aceptar**.

      El Host será agregado a la lista de host.
5. Para eliminar uno o más hosts de la lista, realice lo siguiente:

   Nota

   DD System Manager no permite la eliminación de un host cuando hay un host de trap en el mismo sistema configurado como parte de esa comunidad. Para eliminar un host de trap de una comunidad, elimine el host de trap y vuélvalo a agregar después de que se modifique la comunidad.

   Nota

   Los botones de acceso de la comunidad seleccionada no están deshabilitados cuando el host de trap utiliza una dirección IPv6 y el sistema se administra con una versión anterior de DD OS que no es compatible con IPv6. Si es posible, seleccione siempre un sistema de administración que utilice la misma versión o una versión más reciente de DD OS que los sistemas que administra.

a. Seleccione la casilla de verificación para cada host o haga clic en la casilla de verificación Host en el encabezado de la tabla para seleccionar todos los hosts de la lista.

b. Haga clic en el botón Delete (X).

6. Para editar un nombre de host, realice lo siguiente:

a. Seleccione la casilla de verificación del host.

b. Haga clic en el botón Edit (ícono de lápiz).

c. Edite el nombre de host.

d. Haga clic en **Aceptar**.

7. Haga clic en **Aceptar**.

La entrada de la comunidad modificada aparecerá en la tabla Communities.

Eliminación de comunidades SNMP V2C

Puede usar la pestaña SNMP para eliminar comunidades SNMPv2 existentes.

Procedimiento

1. Seleccione **Administration** > **Settings** > **SNMP**.
2. En el área **Communities**, seleccione una casilla de verificación para la comunidad y haga clic en **Delete**.

   Aparecerá el cuadro de diálogo Delete SNMP V2C Communities.

Nota

Si el botón **Delete**está deshabilitado, la comunidad seleccionada está en uso en uno o más hosts de traps. Elimine los hosts de traps y, a continuación, elimine la comunidad.

---

3. Verifique el nombre de la comunidad que se eliminará y haga clic en **OK**.
4. En el cuadro de diálogo Delete SNMP V2C Communities Status, haga clic en **Close**. La entrada de la comunidad se eliminará de la tabla Communities.

Administración de hosts de SNMP trap

Las definiciones de hosts de trap permiten que el sistema Data Domain envíe mensajes de alerta en mensajes SNMP trap a una estación de administración SNMP.

Creación de hosts de traps SNMP V3 y V2C

Las definiciones de hosts de traps identifican hosts remotos que reciben mensajes de SNMP trap del sistema.

Antes de comenzar

Si tiene planeado asignar una comunidad SNMP v2c existente a un host de trap, primero debe usar el área Communities para asignar el host de trap a la comunidad.

Procedimiento

1. Seleccione **Administration** > **Settings** > **SNMP**.
2. En el área SNMP V3 Trap Hosts o SNMP V2C Trap Hosts, haga clic en **Create**.

   Aparecerá el cuadro de diálogo Create SNMP [V3 o V2C] Trap Hosts.

3. En el cuadro **Host**, especifique la dirección IP o el nombre de dominio del host SNMP que recibirá traps.
4. En el cuadro **Port**, especifique el número de puerto para enviar traps (el puerto 162 es un puerto común).
5. Seleccione el usuario (SNMP V3) o la comunidad (SNMP V2C) desde el menú desplegable.

   Nota

   En la lista Community se muestran únicamente las comunidades en las que ya está asignado el host de trap.

6. Para crear una comunidad nueva, realice lo siguiente:
   a. Seleccione **Create New Community** en el menú desplegable Community.
   b. Escriba el nombre para la comunidad nueva en el cuadro **Community**.
   c. Seleccione el tipo de acceso.
   d. Haga clic en el botón Add (+).
   e. Escriba el nombre del host de trap.
   f. Haga clic en **OK**.
   g. Haga clic en **OK**.
7. Haga clic en **OK**.

Modificación de hosts de SNMP trap V3 y V2C

Puede modificar el número de puerto y la selección de comunidad para configuraciones de hosts de trap existentes.

Procedimiento

1. Seleccione **Administration** > **Settings** > **SNMP**.
2. En las áreas **SNMP V3 Trap Hosts** o **SNMP V2C Trap Hosts**, seleccione una entrada de host de trap y haga clic en **Modify**.

   Aparecerá el cuadro de diálogo Modify SNMP [V3 o V2C] Trap Hosts.

3. Para modificar el número de puerto, especifique un número de puerto nuevo en el cuadro **Port** (el puerto 162 es un puerto común).
4. Seleccione el usuario (SNMP V3) o la comunidad (SNMP V2C) desde el menú desplegable.

   Nota

   En la lista Community se muestran únicamente las comunidades en las que ya está asignado el host de trap.

5. Para crear una comunidad nueva, realice lo siguiente:
   a. Seleccione **Create New Community** en el menú desplegable Community.
   b. Escriba el nombre para la comunidad nueva en el cuadro **Community**.
   c. Seleccione el tipo de acceso.

d. Haga clic en el botón Add (+).

e. Escriba el nombre del host de trap.

f. Haga clic en **OK**.

g. Haga clic en **OK**.

6. Haga clic en **OK**.

Eliminación de hosts de traps SNMP V3 y V2C

Puede usar la pestaña SNMP para eliminar configuraciones de hosts de traps existentes.

Procedimiento

1. Seleccione **Administration** > **Settings** > **SNMP**.
2. En el área **Trap Hosts** (ya sea para V3 o V2C), seleccione una casilla de verificación para el host de trap y haga clic en **Delete**.

   Aparecerá el cuadro de diálogo Delete SNMP [V3 o V2C] Trap Hosts.

3. Verifique el nombre del host que se eliminará y haga clic en **OK**.
4. En el cuadro de diálogo Delete SNMP [V3 o V2C] Trap Hosts Status, haga clic en **Close**.

   La entrada de host de trap se eliminará de la tabla **Trap Hosts**.

Administración de informes de soporte automático

La función de soporte automático genera un informe denominado ASUP. El ASUP muestra información de identificación del sistema, salidas consolidadas de un número de comandos del sistema Data Domain y entradas de diferentes archivos de registro. En la parte inferior del informe aparecen estadísticas internas detalladas y extensas. Este informe está diseñado para ayudar al departamento de soporte de Data Domain a depurar problemas del sistema.

Cada vez que se inicia el sistema, que generalmente es una vez por día, se genera un ASUP. Sin embargo, el sistema de archivos se puede iniciar más de una vez por día.

Puede configurar direcciones de correo electrónico para recibir los informes ASUP y puede habilitar o deshabilitar el envío de esos informes a Data Domain. La hora predeterminada para enviar el ASUP es a las 6:00, y es configurable. Cuando se envían informes ASUP a Data Domain, tiene la opción de seleccionar el método no seguro heredado o el método ConnectEMC, que cifra la información antes de la transmisión.

Capacidad de administración de paquetes de soporte y soporte automático de sistemas de alta disponibilidad

La configuración se realiza en el nodo activo y se espejea en el nodo en espera; por lo tanto, ambos nodos tienen la misma configuración, pero no hay un paquete de soporte y ASUP consolidado.

El paquete de soporte automático y soporte en el nodo activo también incluye información sobre alta disponibilidad completa, sistema de archivos, replicación, protocolo y nodo local. El paquete de soporte automático y soporte en el nodo en espera tiene solo información del nodo local y algunos detalles sobre la alta disponibilidad (configuración y estado), pero no incluye información de sistema de archivos, replicación ni protocolo. Los paquetes de soporte automático y soporte de ambos nodos se necesitarán para depurar problemas relacionados con el estado del

sistema de alta disponibilidad (sistema de archivos, replicación, protocolos y configuración de alta disponibilidad).

Habilitación y deshabilitación de la creación de informes de soporte automático para Data Domain

Puede habilitar o deshabilitar la creación de informes de soporte automático para Data Domain sin afectar el hecho de si se envían o no las alertas a Data Domain.

Procedimiento

1. Para ver el estado de una creación de informes autosupport, seleccione **Maintenance** > **Support** > **Autosupport**.

   El estado de la creación de informes de soporte automático se destaca junto a la etiqueta de soporte automático programado en el área Support. Según la configuración actual, aparece el botón **Enable** o **Disable** en la fila de soporte automático programado.
2. Para habilitar la creación de informes de soporte automático para Data Domain, haga clic en **Enable** en la fila de soporte automático programado.
3. Para deshabilitar la creación de informes de soporte automático para Data Domain, haga clic en **Disable** en la fila de soporte automático programado.

Revisión de informes de soporte automático generados

Puede revisar informes de soporte automático para ver estadísticas e información de configuración del sistema recopiladas en el pasado. El sistema almacena un máximo de 14 informes de soporte automático.

Procedimiento

1. Seleccione **Maintenance** > **Support** > **Autosupport**.

   La página Autosupport Reports muestra el nombre y el tamaño de archivo del informe de soporte automático, y la fecha en la que se generó el informe. Los nombres de los informes se asignan automáticamente. El informe más reciente es autosupport, el del día anterior es autosupport.1, y el número aumenta a medida que los informes retroceden en el pasado.

   Equivalente de la CLI

   ```
   # autosupport show history
   ```
2. Haga clic en el vínculo del nombre de archivo para ver el informe con un editor de texto. Si el navegador lo requiere, descargue el archivo primero.

Configuración de la lista de distribución de correo de soporte automático

Los suscriptores de la lista de distribución de correo de soporte automático reciben mensajes de soporte automático por correo electrónico. Puede usar la pestaña Autosupport para agregar, modificar y eliminar suscriptores.

Los correos electrónicos de soporte automático se envían a través del servidor de correo configurado a todos los suscriptores de la lista de correos electrónicos de soporte automático. Después de configurar el servidor de correo y la lista de correos electrónicos de soporte automático, se recomienda probar la configuración para garantizar que los mensajes de soporte automático lleguen a los destinos deseados.

Procedimiento

1. Seleccione **Maintenance** > **Support** > **Autosupport**.
2. Haga clic en **Configure**.

   Aparecerá el cuadro de diálogo Configure Autosupport Subscribers.

3. Para agregar un suscriptor, realice lo siguiente:
   a. Haga clic en **Add (+)**.

      Aparecerá el cuadro de diálogo Email.

   b. Especifique las direcciones de correo electrónico de los destinatarios en el cuadro Email.

   c. Haga clic en Aceptar.

   Equivalente de la CLI

   ```
    # autosupport add asup-detailed emails djones@company.com # autosupport add alert-summary emails djones@company.com
   ```

4. Para eliminar un suscriptor, realice lo siguiente:
   a. En el cuadro de diálogo Configure Autosupport Subscribers, seleccione el suscriptor que desea eliminar.

   b. Hagaclic en Delete (**X**).

   Equivalente de la CLI

   ```
    # autosupport del asup-detailed emails djones@company.com # autosupport del alert-summary emails djones@company.com
   ```

5. Para modificar la dirección de correo electrónico de un suscriptor, realice lo siguiente.
   a. En el cuadro de diálogo Configure Autosupport Subscribers, seleccione el nombre del suscriptor que desea editar.

   b. Haga clic en Modify (ícono de lápiz).

      Aparecerá el cuadro de diálogo Email.

   c. Modifique la dirección de correo electrónico según sea necesario.

   d. Haga clic en Aceptar.
6. Haga clic en **OK** para cerrar el cuadro de diálogo Configure Autosupport Subscribers.

   La lista de correos electrónicos de soporte automático revisada aparecerá en el área Autosupport Mailing List.

Verificar si Data Domain puede enviar correos electrónicos de ASUP y alertas a los destinatarios externos

Confirme que los destinatarios de correo electrónico externos puedan recibir los correos electrónicos de soporte automático (ASUP) y de alerta que envía desde su dispositivo de Data Domain.

Verifique que el servidor de Exchange retransmita los correos electrónicos de soporte automático (ASUP).

Procedimiento

1. Compruebe si los correos electrónicos de ASUP se pueden enviar a una dirección de correo electrónico local, una dirección de correo electrónico en el mismo servidor de correo electrónico.

   ```
   # autosupport send [internal-email-addr]
   ```

2. Compruebe si los correos electrónicos de ASUP se pueden enviar a una dirección de correo electrónico fuera del servidor de correo electrónico local.

   ```
   # autosupport send [external email-addr]
   ```

3. Si el correo electrónico no llega a la dirección de correo electrónico externa en el servidor de correo, es posible que reciba un error como:

   ```
   **** Unable to send message: (errno 51: Unrecoverable errors
   from server--giving up)
   ```

   En este caso, es probable que se deba habilitar el reenvío al sistema Data Domain en el servidor de correo electrónico local siguiendo los pasos descritos en el artículo de la base de conocimientos *Configure Email Relay on MS Exchange*, disponible en https://support.emc.com/kb/181900.

4. Si el ASUP se puede enviar a una dirección de correo electrónico externa, pero no llega a Data Domain, puede haber un problema con la configuración del firewall o los filtros de correo no deseado.
5. Si las alertas de ASUP llegan a Data Domain, pero no provocan un caso, puede deberse a caracteres no válidos en el asunto o el cuerpo del correo electrónico de alerta. Para verificarlo:

   a. Busque en un correo electrónico de soporte automático actual y compruebe HOSTNAME, SYSTEM_ID y LOCATION para buscar comillas simples o apóstrofos. Este es un carácter no válido y se debe quitar en las versiones de DD OS 4.9.2.0 y anteriores.

   ```
   Example:


   ==========  GENERAL INFO  ==========
   GENERATED_ON=Thu Apr 28 06:54:55 PDT 2011


   VERSION=Data Domain OS 4.9.2.6-226914
   SYSTEM_ID=7FP5105000


   MODEL_NO=DD510
   HOSTNAME=system.datadomain.com


   LOCATION=123 O Malley Lane
   ```

   b. Quite los caracteres no válidos de HOSTNAME o LOCATION del sistema. Los comandos son los siguientes:

   ```
   net set hostname <host>

   config set location "location"
   ```

   c. Pruebe la nueva configuración simulando una alerta. La manera más fácil es implementar una falla manualmente en una unidad de disco de repuesto,

verificar la alerta enviada e inmediatamente quitar la falla en la misma unidad para regresarla al estado de repuesto.

Administración de paquetes de soporte

Un paquete de soporte es un archivo que contiene información sobre la configuración y el funcionamiento del sistema. Una buena práctica es generar un paquete de soporte antes de una actualización de software o un cambio de topología del sistema (como la actualización de una controladora).

Con frecuencia, el departamento de soporte de Data Domain solicita un paquete de soporte cuando brinda asistencia.

El artículo de la base de conocimientos *How to collect/upload a support bundle (SUB) from a Data Domain Restorer (DDR)*, disponible en https://support.emc.com/kb/180563, proporciona información adicional sobre cómo trabajar con paquetes de soporte técnico.

Generación de un paquete de soporte

Cuando soluciona problemas, el servicio al cliente de Data Domain puede solicitar un paquete de soporte, que es una selección de archivos de registro comprimidos en tar-g-zip con un archivo LÉAME donde incluye la identificación de los encabezados de soporte automático.

Procedimiento

1. Seleccione **Maintenance** > **Support** > **Support Bundles**.
2. Haga clic en **Generate Support Bundle**.

   Nota

   El sistema admite un máximo de cinco paquetes de soporte. Si intenta generar un sexto paquete de soporte, el sistema elimina automáticamente el paquete de soporte más antiguo. También puede eliminar paquetes de soporte con el comando de la CLI `support bundle delete`.

   Además, si genera un paquete de soporte en un sistema actualizado que contiene un paquete de soporte con un nombre que sigue el formato antiguo, `support-bundle.tar.gz`, se cambia el nombre de ese archivo para usar el formato de nombre más reciente.

3. Envíe el archivo a servicio al cliente a la dirección support@emc.com.

   Nota

   Si el paquete es demasiado grande para enviar por correo electrónico, use el sitio del servicio de soporte en línea para cargar el paquete. (Vaya a https://support.emc.com.)

Visualización de la lista de paquetes de soporte

Puede usar la pestaña Support Bundles para ver los archivos de paquetes de soporte en el sistema.

Procedimiento

1. Seleccione **Maintenance** > **Support** > **Support Bundles**.

   Aparecerá la lista Support Bundles.

   En esta se incluyen el nombre de archivo, el tamaño de archivo y la fecha de generación de los paquetes de soporte. Los nombres de los paquetes se asignan automáticamente de la siguiente manera *hostname*-support-bundle-*datestamp*.tar.gz. Un nombre de archivo de ejemplo es localhost-support-bundle-1127103633.tar.gz, que indica que el paquete de soporte se creó en el sistema de host local el 27 de noviembre a las 10:36:33.

2. Haga clic en el vínculo del nombre de archivo y seleccione una herramienta de descompresión de gz/tar para ver el contenido ASCII del paquete.

Administración de coredump

Cuando DD OS se bloquea debido a un coredump, se crea un archivo principal que describe el problema en el directorio /ddvar/core. Este archivo puede ser grande y difícil de copiar del sistema Data Domain.

Si no se puede copiar el archivo principal del sistema Data Domain porque es demasiado grande, ejecute el comando **support coredump split *<filename>* by *<n>* {MiB|GiB}**, donde:

- *<filename>* es el nombre del archivo principal en el directorio /ddvar/core
- *<n>* es la cantidad de fragmentos más pequeños en los que se dividirá el archivo principal

Nota

Un archivo principal solo se puede dividir en 20 fragmentos como máximo. El comando fallará con un error si el tamaño especificado da como resultado más de 20 fragmentos.

Por ejemplo, dividir un archivo principal de 42.1 MB denominado cpmdb.core.19297.1517443767 en fragmentos de 10 MB daría como resultado cinco fragmentos.

```
# support coredump split cpmdb.core.19297.1517443767 10 MiB
cpmdb.core.19297.1517443767 will be split into 5 chunks.
Splitting...

The md5 and split chunks of cpmdb.core.19297.1517443767:
File                              Size       Time Created
--------------------------------  --------   ------------------------
cpmdb.core.19297.1517443767_5_01  10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_02  10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_03  10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_04  10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_05  2.1 MiB    Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767.md5   0 MiB      Mon Feb  5 11:50:58 2018
--------------------------------  --------   ------------------------
Download the files as soon as possible. Otherwise they will be automatically delete in 48
hours.
```

Ejecute el comando **support coredump save *<file-list>*** para guardar los archivos de coredump especificados en una unidad USB.

Administración de notificación de alerta

La función de alerta genera informes de evento e informes resumidos que pueden distribuirse a las listas de correo electrónico configurables y a Data Domain.

Los informes de evento se envían en forma inmediata y proporcionan información detallada sobre un evento del sistema. Las listas de distribución para alertas de eventos se llaman *notification groups*. Puede configurar un grupo de notificación para incluir una o más direcciones de correo electrónico y se puede configurar el tipo y el nivel de gravedad de los informes de evento enviados a esas direcciones. Por ejemplo, puede configurar un grupo de notificación para los individuos que necesiten saber acerca de eventos críticos y otro grupo para los que monitorean eventos menos críticos. Otra opción es configurar grupos para diferentes tecnologías. Por ejemplo, puede configurar un grupo de notificación para recibir mensajes por correo electrónico sobre todos los eventos de la red y otro grupo para recibir mensajes sobre los problemas de almacenamiento.

Los informes resumidos se envían en forma diaria y proporcionan un resumen de los eventos que surgieron durante las últimas 24 horas. Los informes resumidos no incluyen toda la información proporcionada en los informes de evento. La hora de generación predeterminada para el informe diario es 8 a.m., y puede ser modificada. Los informes resumidos se envían utilizando una lista de correo electrónico dedicada que está separada de los grupos de notificación de eventos.

Puede habilitar o deshabilitar la distribución de alertas a Data Domain. Cuando envía informes a Data Domain, tiene la opción de seleccionar el método inseguro heredado o Secure Remote Services para transmisiones seguras.

Administración de notificación de alerta de sistemas de alta disponibilidad

La función de alerta en un sistema de alta disponibilidad genera eventos e informes de resumen como en un sistema sin alta disponibilidad, pero la forma en que el sistema de alta disponibilidad administra estas alertas es diferente debido a la configuración de sistema de dos nodos.

La configuración de alerta inicial se completa en el nodo activo y se espejea en el que está en standby (es decir, ambos nodos tienen la misma configuración). Las alertas AM y locales se envían por correo electrónico según la configuración de notificación e incluyen información que indica que son de un sistema de alta disponibilidad y en qué nodo, ya sea activo o en standby, se generaron.

Si hay alertas activas en el sistema de archivos, la replicación o los protocolos cuando se produce un failover, estas alertas activas se siguen mostrando en el nuevo nodo activo después del failover si las condiciones de alerta no desaparecieron.

Las alertas históricas en el sistema de archivos, la replicación y los protocolos se conservan en el nodo donde se originaron en vez de realizar un failover en conjunto con el sistema de archivos en un failover. Esto significa que las CLI en el nodo activo no mostrarán una vista completa/continua de las alertas históricas para el sistema de archivos, la replicación y los protocolos

Durante un failover, las alertas históricas locales se conservan en el nodo desde el cual se generaron. Sin embargo, las alertas históricas para el sistema de archivos, la replicación y los protocolos (generalmente, denominadas “alertas lógicas”) realizan un failover junto con el sistema de archivos.

Nota

El panel **Health** > **High Availability** muestra solo las alertas que están relacionadas con alta disponibilidad. Esas alertas pueden filtrarse por componentes principales de alta disponibilidad, como administrador de alta disponibilidad, nodo, interconexión, almacenamiento y conexión SAS.

Visualización de la lista de grupos de notificación

Un grupo de notificación define un conjunto de tipos de alertas (clases) y un grupo de direcciones de correo electrónico (para los suscriptores). Siempre que el sistema genera un tipo de alerta seleccionado en una lista de notificación, esa alerta se envía a los suscriptores de la lista.

Procedimiento

1. Seleccione **Health** > **Alerts** > **Notification**.

   Equivalente de la CLI

   ```
   # alerts notify-list show
   ```

2. Para limitar (filtrar) las entradas de la lista Group Name, escriba un nombre de grupo en el cuadro Group Name o del correo electrónico un suscriptores en el cuadro Alert Email y haga clic en **Update**.

   Nota

   Haga clic en **Reset** para visualizar todos los grupos configurados.

3. Para visualizar información detallada para un grupo, seleccione el grupo en la lista Group Name.

Pestaña Notification

La pestaña Notification le permite configurar grupos de direcciones de correo electrónico que recibirán alertas del sistema para los tipos de alerta y los niveles de severidad que seleccione.

Tabla 52 Lista Group Name, descripciones de etiquetas de la columna

Elemento	Descripción
Group Name	El nombre configurado para el grupo.
Classes	El número de clases de alertas que se informan al grupo.
Subscribers	El número de suscriptores que están configurados para recibir notificaciones por correo electrónico.

Tabla 53 Información detallada, descripciones de etiquetas

Elemento	Descripción
Class	Un servicio o subsistema que puede reenviar alertas. Las clases incluidas son aquellas para las que el grupo de notificación recibe alertas.

Tabla 53 Información detallada, descripciones de etiquetas (continuación)

Elemento	Descripción
Severity	El nivel de severidad que desencadena un correo electrónico al grupo de notificación. Todas las alertas en el nivel de severidad especificado y superiores se envían al grupo de notificación.
Subscribers	El área de suscriptores muestra una lista de todas las direcciones de correo electrónico configuradas para el grupo de notificación.

Tabla 54 Controles de la pestaña Notification

Control	Descripción
Botón Add	Haga clic en el botón **Add** para comenzar a crear un grupo de notificación.
Botón Class Attributes Configure	Haga clic en el botón Configure para cambiar las clases y los niveles de severidad que generan alertas para el grupo de notificación seleccionado.
Botón Delete	Haga clic en el botón **Delete** para eliminar el grupo de notificación seleccionado.
Filter By: Cuadro Alert Email	Escriba texto en este cuadro para limitar las entradas de la lista de nombres de grupo a los grupos que incluyen una dirección de correo electrónico que contiene el texto especificado.
Filter By: Cuadro Group Name	Escriba texto en este cuadro para limitar las entradas de la lista de nombres de grupo a los nombres de grupos que contienen el texto especificado.
Botón Modify	Haga clic en el botón **Modify** para modificar la configuración del grupo de notificación seleccionado.
Botón Reset	Haga clic en este botón para eliminar las entradas de los cuadros Filter By y mostrar todos los nombres de grupos.
Botón Subscribers Configure	Haga clic en el botón Configure para cambiar la lista de correos electrónicos para el grupo de notificación seleccionado.
Botón Update	Haga clic en este botón para actualizar la lista de nombres de grupos después de escribir texto en un cuadro de filtro.

Creación de un grupo de notificación

Puede usar la pestaña Notification para agregar grupos de notificación y seleccionar el nivel de gravedad para cada grupo.

Procedimiento

1. Seleccione **Health** > **Alerts** > **Notification**.
2. Haga clic en **Add**.

   Aparecerá el cuadro de diálogo Add Group.

3. Especifique el nombre del grupo en el cuadro **Group Name**.
4. Seleccione la casilla de verificación de una o más clases de alertas de las que quiera recibir notificaciones.
5. Para cambiar el nivel de gravedad predeterminado (Advertencia) para una clase, seleccione otro nivel en el cuadro de lista asociado.

   Los niveles de gravedad se enumeran por nivel de gravedad en orden ascendente. *Emergency* es el nivel de gravedad más alto.

6. Haga clic en **Aceptar**.

   Equivalente de la CLI

   ```
   # alerts notify-list create eng_grp class hardwareFailure
   ```

Administrar la lista de suscriptores para un grupo

Utilice la pestaña Notification para agregar, modificar o eliminar direcciones de correo electrónico de una lista de notificaciones para suscriptores de un grupo

Procedimiento

1. Seleccione **Health** > **Alerts** > **Notification**.
2. Seleccione la casilla de verificación de un grupo en la lista de grupos Notifications y realice una de las siguientes acciones.
   - Haga clic en **Modify** y seleccione **Subscribers.**
   - Haga clic en **Configure** en la lista Subscribers.
3. Para agregar un suscriptor al grupo, haga lo siguiente.
   a. Haga clic en el ícono **+**.

      Aparecerá el cuadro de diálogo Email Address.

   b. Escriba la dirección de correo electrónico de un suscriptor.

   c. Haga clic en **Aceptar**.

      Equivalente de la CLI

      ```
       # alerts notify-list add eng_lab emails
      mlee@urcompany.com,bob@urcompany.com
      ```

4. Para modificar una dirección de correo electrónico, haga lo siguiente.
   a. Haga clic en la casilla de verificación de la dirección de correo electrónico en la lista **Subscriber Email**.

   b. Haga clic en el ícono de lápiz.

   c. Edite la dirección de correo electrónico en el cuadro de diálogo Email Address.

   d. Haga clic en **Aceptar**.

5. Para eliminar una dirección de correo electrónico, haga clic en la casilla de verificación de la lista **Subscriber Email** y haga clic en el ícono **X**.

   Equivalente de la CLI

   ```
   # alerts notify-list del eng_lab emails bob@urcompany.com
   ```

6. Haga clic en **Finish** o en **OK**.

Modificación de un grupo de notificación

Puede usar la tabla Notification para modificar las clases de atributos en un grupo existente.

Procedimiento

1. Seleccione **Health** > **Alerts** > **Notification**.
2. Seleccione la casilla de verificación del grupo que desee modificar en la lista de grupos.
3. Para modificar las clases de atributos para un grupo, realice lo siguiente.
   a. Haga clic en **Configure** en el área Class Attributes.

      Aparecerá el cuadro de diálogo Edit Group.

   b. Seleccione la casilla de verificación (o anule la selección de esta) de uno o más atributos de clase.

   c. Para cambiar el nivel de gravedad de un atributo de clase, seleccione un nivel del cuadro de lista correspondiente.

   d. Haga clic en **Aceptar**.

      Equivalente de la CLI

      ```
      # alerts notify-list add eng_lab class cloud severity warning
      # alerts notify-list del eng_lab class cloud severity notice
      ```

4. Para modificar la lista de suscriptores para un grupo, realice lo siguiente.
   a. Haga clic en **Configure** en el área Subscribers.

      Aparecerá el cuadro de diálogo Edit Subscribers.

   b. Para eliminar suscriptores de la lista de grupos, seleccione las casillas de verificación de los suscriptores que desee eliminar y haga clic en el ícono para eliminar (X).

   c. Para agregar un suscriptor, haga clic en el ícono para agregar (+), escriba la dirección de correo electrónico de un suscriptor y haga clic en OK.

   d. Haga clic en **Aceptar**.

      Equivalente de la CLI

      ```
      # alerts notify-list add eng_lab emails
      mlee@urcompany.com,bob@urcompany.com
      # alerts notify-list del eng_lab emails bob@urcompany.com
      ```

5. Haga clic en **Aceptar**.

Eliminación de un grupo de notificación

Puede usar la pestaña Notification para eliminar uno o más grupos de notificación existentes.

Procedimiento

1. Seleccione **Health** > **Alerts** > **Notification**.
2. Seleccione una o más casillas de verificación de los grupos en la lista de grupos Notifications y haga clic en **Delete**.

   Aparecerá el cuadro de diálogo Delete Group.

3. Verifique la eliminación y haga clic en **OK**.

   Equivalente de la CLI

   ```
   # alerts notify-list destroy eng_grp
   ```

Restablecimiento de la configuración del grupo de notificación

Puede usar la pestaña Notification para eliminar todos los grupos de notificación agregados y para eliminar los cambios realizados al grupo predeterminado.

Procedimiento

1. Seleccione **Health** > **Alerts** > **Notification**.
2. Seleccione **More Tasks** > **Reset Notification Groups**.
3. En el cuadro de diálogo Reset Notification Groups, haga clic en **Yes** en el diálogo de verificación.

   Equivalente de la CLI

   ```
   # alerts notify-list reset
   ```

Configuración del calendario de resumen diario y la lista de distribución

Todas las mañanas, cada sistema administrado envía un correo electrónico de resumen diario de alertas a los suscriptores configurados para el grupo de correo electrónico alertssummary.list. El correo electrónico de resumen diario de alertas contiene alertas actuales e históricas que muestran mensajes acerca de situaciones de hardware no críticas y números de uso de espacio en disco que podría querer tratar pronto.

La falla de un ventilador es un ejemplo de un problema no crítico que podría querer tratar tan pronto como sea razonablemente posible. Cuando el departamento de soporte recibe la notificación de la falla, se pone en contacto con usted para organizar el reemplazo del componente.

Procedimiento

1. Seleccione **Health** > **Alerts** > **Daily Alert Summary**.
2. Si la hora de envío predeterminada de 8 AM no es aceptable, realice lo siguiente.
   a. Haga clic en **Schedule**.

      Se abrirá el cuadro de diálogo Schedule Alert Summary.

   b. Use los cuadros de lista para seleccionar la hora, los minutos y AM o PM para el informe de resumen.

c. Haga clic en **Aceptar**.

Equivalente de la CLI

```
# autosupport set schedule alert-summary daily 1400
```

3. Para configurar la lista de suscriptores de alertas diarias, realice lo siguiente.

a. Haga clic en **Configure**.

Se abrirá el cuadro de diálogo Daily Alert Summary Mailing List.

b. Modifique la lista de suscriptores de alertas diarias de la siguiente manera.

- Para agregar un suscriptor, haga clic en el ícono **+**, escriba la dirección de correo electrónico y haga clic en **OK**.
  Equivalente de la CLI
  ```
  # autosupport add alert-summary emails djones@company.com
  ```
- Para modificar una dirección de correo electrónico, seleccione la casilla de verificación del suscriptor, haga clic en el ícono de lápiz, edite la dirección de correo electrónico y haga clic en **OK**.
- Para eliminar una dirección de correo electrónico, seleccione la casilla de verificación del suscriptor y haga clic en **X**.
  Equivalente de la CLI
  ```
  # autosupport del alert-summary emails djones@company.com
  ```

c. Haga clic en **Finalizar**.

Pestaña Daily Alert Summary

La pestaña de resumen diario de alertas permite configurar una lista de correos electrónicos de aquellos usuarios que quieren recibir un resumen de todas las alertas del sistema una vez por día. Las personas de esta lista no recibirán alertas individuales a menos que también estén agregadas a un grupo de notificación.

Tabla 55 Resumen diario de alertas, descripciones de etiquetas

Elemento	Descripción
Delivery Time	La hora de envío muestra la hora configurada para los correos electrónicos diarios.
Email List	Esta lista muestra las direcciones de correo electrónico de los usuarios que recibirán los correos electrónicos diarios.

Tabla 56 Controles de la pestaña Daily Alert Summary

Control	Descripción
Botón Configure	Haga clic en el botón **Configure** para editar la lista de correos electrónicos de suscriptores.
Botón Schedule	Haga clic en el botón **Schedule** para configurar la hora a la que se envía el informe diario.

Habilitación y deshabilitación de las notificaciones de alerta a Data Domain

Puede habilitar o deshabilitar las notificaciones de alerta que se envían a Data Domain sin afectar el hecho de si se envían o no los informes de soporte automático a Data Domain.

Procedimiento

1. Para ver el estado de una creación de informes de soporte automático, seleccione **Maintenance** > **Support** > **Autosupport**.

   El estado de las notificaciones de alerta se destaca en verde junto a la etiqueta de alerta en tiempo real en el área Support. Según la configuración actual, aparece el botón **Enable** o **Disable** en la fila de la alerta en tiempo real.
2. Para habilitar la creación de informes de alertas para Data Domain, haga clic en **Enable** en la fila de las alertas en tiempo real.
3. Para deshabilitar la creación de informes de alertas para Data Domain, haga clic en **Disable** en la fila de las alertas en tiempo real.

Pruebas de la función de correo electrónico de alertas

Puede usar la pestaña Notification para enviar un correo electrónico de prueba a direcciones de correo electrónico o grupos de notificación específicos. Esta función le permite determinar si el sistema está configurado correctamente para enviar mensajes de alerta.

Procedimiento

1. Para controlar si una alerta de prueba se envía o no a Data Domain, realice lo siguiente.
   a. Seleccione **Maintenance** > **Support** > **Autosupport**.
   b. En el área **Alert Support**, haga clic en **Enable** o **Disable** para controlar si el correo electrónico de prueba se envía o no.

      No puede cambiar la dirección de correo electrónico.
2. Seleccione **Health** > **Alerts** > **Notification**.
3. Seleccione **More Tasks** > **Send Test Alert**.

   Aparecerá el cuadro de diálogo Send Test Alert.
4. En la lista **Notification Groups**, seleccione grupos para que reciban el correo electrónico de prueba y haga clic en **Next**.
5. Opcionalmente, agregue direcciones de correo electrónico adicionales para que reciban el correo electrónico.
6. Haga clic en **Send Now** y en **OK**.

   Equivalente de la CLI

   ```
   # alerts notify-list test jsmith@yourcompany.com
   ```
7. Si deshabilitó el envío de la alerta de prueba a Data Domain y quiere habilitar esta función ahora, realice lo siguiente.
   a. Seleccione **Maintenance** > **Support** > **Autosupport**.
   b. En el área **Alert Support**, haga clic en **Enable**.

Resultados

Si desea probar correos electrónicos de alertas agregados recientemente para problemas de correo, escriba `autosupport test email`*dirección-de-correo-electrónico*

Por ejemplo, después de agregar la dirección de correo electrónico djones@suempresa.com a la lista, compruebe la dirección con el comando `autosupport test email`*djones@suempresa.com*

Administración de la entrega de servicio de soporte

La administración de la entrega define cómo se envían alertas e informes de soporte automático a Data Domain. De forma predeterminada, las alertas y los informes de soporte automático se envían diariamente al servicio al cliente de Data Domain utilizando el correo electrónico estándar (no seguro). El método ConnectEMC envía mensajes en un formato seguro mediante una puerta de enlace de Secure Remote Services Virtual Edition (VE).

Cuando se usa el método ConnectEMC con una puerta de enlace de Secure Remote Services, una ventaja es que dicha puerta de enlace puede reenviar mensajes de varios sistemas y esto le permite configurar la seguridad de red solos para la puerta de enlace de ESRS en lugar de para varios sistemas. Además, si se adoptan las licencias electrónicas, se genera y se envía un informe de inteligencia de uso.

Al configurar una puerta de enlace de Secure Remote Services, el sistema Data Domain admite el registro de varias puertas de enlace para proporcionar redundancia.

Selección de entrega de correo electrónico estándar a Data Domain

Cuando selecciona el método de entrega de correo electrónico estándar (no seguro), este método se aplica a la creación de informes de soporte automático y alertas.

Procedimiento

1. Seleccione **Maintenance** > **Support** > **Autosupport**.
2. Haga clic en **Configure** en la fila Channel del área Support.

   Aparece el cuadro de diálogo Configure EMC Support Delivery. El método de entrega se muestra después de la etiqueta de canal en el área Support.
3. En el cuadro de lista **Channel**, seleccione **Email to datadomain.com**.
4. Haga clic en **OK**.

   Equivalente de la CLI

   ```
   # support notification method set email
   ```

Selección y configuración de entrega de Secure Remote Services

La puerta de enlace de Secure Remote Services Virtual Edition (VE) proporciona actividades Connect Home y de soporte remoto automatizadas mediante una solución basada en IP mejorada por un sistema de seguridad integral.

Una puerta de enlace versión 3 de Secure Remote Services en las instalaciones ofrece la capacidad de monitorear los sistemas Data Domain en las instalaciones y las instancias de Data Domain Virtual Edition, y las instancias de Data Domain Virtual Edition basada en la nube.

Procedimiento

1. Seleccione **Maintenance** > **Support** > **Autosupport**.
2. Haga clic en **Configure** en la fila Channel del área Support.

   Aparecerá el cuadro de diálogo Configure Dell EMC Support Delivery. El método de entrega se muestra después de la etiqueta Channel en el área Support.
3. En el cuadro de lista **Channel**, seleccione **Secure Remote Services**.
4. Escriba el hostname de la puerta de enlace y seleccione la dirección IP local para el sistema Data Domain.
5. Haga clic en **OK**.
6. Escriba el nombre de usuario y la contraseña del vínculo de servicio.
7. Haga clic en **Register**.

   Los detalles de Secure Remote Services se muestran en el panel Autosupport.

   Equivalente de la CLI

```
# support connectemc device register ipaddr esrs-gateway [host-list] [ha-peer ipaddr]
```

⚠ PRECAUCIÓN

Cuando configure la prestación de Secure Remote Services en un par de HA de Data Domain:

- **El parámetro** `ha-peer` **es obligatorio cuando se configura Secure Remote Services en pares de alta disponibilidad de Data Domain para registrar ambos nodos.**
- **El cliente debe proporcionar las credenciales de vínculo de servicio para ejecutar el comando** `support connectemc device register` **en un par de HA, ya que no se podrá registrar el par de HA como un usuario y esto causará que el token de clave de RSA pierda la sincronización.**

Pruebas de funcionamiento de ConnectEMC

Un comando de la CLI le permite probar el funcionamiento de ConnectEMC mediante el envío de un mensaje de prueba al Soporte por medio de la puerta de enlace de Secure Remote Services.

Procedimiento

1. Para probar el funcionamiento de ConnectEMC, utilice la CLI.

```
#support connectemc test
Sending test message through ConnectEMC...
Test message successfully sent through ConnectEMC.
```

Administración de archivos de registro

El sistema Data Domain mantiene un conjunto de archivos de registro, que se pueden integrar y enviar al servicio de soporte para ayudar a solucionar problemas y errores del sistema que puedan surgir. Los archivos de registro no pueden ser eliminados ni modificados por ningún usuario con DD System Manager, pero pueden copiarse del directorio de registro y administrarse fuera del sistema.

Nota

Los mensajes de registro en un sistema de alta disponibilidad se conservan en el nodo donde se originó el archivo de registro.

Los archivos de registro se rotan semanalmente. Cada domingo a las 0:45 a.m., el sistema abre automáticamente archivos de registro nuevos para los registros existentes y cambia el nombre de los archivos anteriores con números anexados. Por ejemplo, después de la primera semana de funcionamiento, el archivo de la semana anterior `messages` recibe el nombre `messages.1` y los mensajes nuevos se almacenan en un archivo de mensajes nuevo. Cada archivo numerado pasa al siguiente número cada semana. Por ejemplo, después de la segunda semana, el archivo `messages.1` pasa a `messages.2`. Si ya existe un archivo `messages.2`, este pasa a `messages.3`. Al final del período de retención (que se muestra en la tabla a continuación), el registro vencido se elimina. Por ejemplo, un archivo `messages.9` existente se elimina cuando `messages.8` pasa a `messages.9`.

`audit.log` no rota semanalmente. En cambio, rota cuando el archivo alcanza 70 MB de tamaño.

A menos que se mencione en este tema, los archivos de registro se almacenan en `/ddvar/log`.

Nota

Los archivos en el directorio `/ddvar` se pueden eliminar con comandos de Linux si el usuario de Linux tiene permiso de *escritura* asignado para ese directorio.

El conjunto de archivos de registro en cada sistema se determina con las características configuradas en el sistema y los eventos que ocurran. En la siguiente tabla se describen los archivos de registro que el sistema puede generar.

Tabla 57 Archivos de registro del sistema

Archivo de registro	Descripción	Período de retención
audit.log	Mensajes acerca de eventos de inicio de sesión de usuarios.	15 semanas
cifs.log	Mensajes de registro del subsistema CIFS que se registran únicamente en `debug/cifs/cifs.log`. Límite de tamaño de 50 MiB.	10 semanas
mensajes	Mensajes acerca de eventos generales del sistema, incluidos los comandos ejecutados.	9 semanas
secure.log	Mensajes sobre eventos de usuarios, como inicios de sesión correctos y fallidos, incorporaciones y eliminaciones de usuarios, y cambios de contraseñas. Solo los usuarios con función de administrador pueden ver este archivo.	9 semanas
space.log	Mensajes acerca del uso de espacio en disco por componentes del sistema y mensajes del proceso de limpieza. Un mensaje de uso de espacio se genera cada hora. El proceso de limpieza crea alrededor de 100 mensajes cada vez que se ejecuta. Todos los mensajes tienen un formato de valores separados por coma con etiquetas que puede usar para separar los mensajes de espacio en disco y los mensajes del proceso de limpieza. Puede usar software de otros	Un solo archivo se conserva permanentemente. No hay rotación del archivo de

Tabla 57 Archivos de registro del sistema (continuación)

Archivo de registro	Descripción	Período de retención
	fabricantes para analizar cada conjunto de mensajes. El archivo de registro usa las siguientes etiquetas. • CLEAN para líneas de datos de operaciones de limpieza. • CLEAN_HEADER para líneas que contienen encabezados para las líneas de datos de operaciones de limpieza. • SPACE para líneas de datos de espacio en disco. • SPACE_HEADER para líneas que contienen encabezados para las líneas de datos de espacio en disco.	registro para este registro.

Visualización de archivos de registro en DD System Manager

Utilice la pestaña Logs para ver y abrir los archivos de registro del sistema en el DD System Manager.

Procedimiento

1. Seleccione **Maintenance** > **Logs**.

   La lista de Logs muestra los nombres de los archivos de registro y el tamaño y la fecha de creación de cada archivo de registro.

2. Haga clic en un nombre de archivo de registro para ver su contenido. Es posible que se le solicite que seleccione una aplicación, como Notepad.exe, para abrir el archivo.

Visualización de un archivo de registro en la CLI

Utilice el comando `log view` para ver un archivo de registro en la CLI.

Procedimiento

1. Para ver un archivo de registro en la CLI, utilice el comando `log view .`

   Sin argumento, el comando muestra el archivo de mensajes en curso.

2. Al ver el registro, utilice las flechas de arriba y abajo para desplazarse por el archivo; utilice la tecla "q" para salir; e escriba un carácter de barra (/) y un patrón para realizar una búsqueda a través del archivo.

La visualización del archivo de mensajes es similar a la siguiente. El último mensaje en el ejemplo es un mensaje de estado del sistema que el sistema Data Domain genera automáticamente cada hora. El uptime del sistema de informes de mensajes, el volumen de datos almacenados, las operaciones NFS y el volumen de espacio ocupado en el disco para el almacenamiento de datos (%). Los mensajes por hora se transfieren al registro del sistema y a la consola serie de haberse conectado a una.

```
# log view
Jun 27 12:11:33 localhost rpc.mountd: authenticated unmount
request from perfsun-g.emc.com:668 for /ddr/col1/segfs (/ddr/
col1/segfs)
```

```
Jun 27 12:28:54 localhost sshd(pam_unix)[998]: session opened
for user jsmith10 by (uid=0)

Jun 27 13:00:00 localhost logger: at 1:00pm up 3 days, 3:42,
52324 NFS ops, 84763 GiB data col. (1%)
```

Nota

GiB = Gibibytes = el equivalente binario de Gigabytes.

Más información acerca de los mensajes de registro

Busque mensajes de error en Error Message Catalog para su versión de SO DD.

En el archivo de registro el texto es similar a lo siguiente.

```
Jan 31 10:28:11 syrah19 bootbin: NOTICE: MSG-SMTOOL-00006: No
replication throttle schedules found: setting throttle to
unlimited.
```

Los componentes del mensaje son los siguientes.

```
DateTime Host Process [PID]: Severity: MSG-Module-MessageID: Mensaje
```

Los niveles de gravedad, en orden descendente, son: Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug.

Procedimiento

1. Vaya al sitio web de soporte en línea en https://support.emc.com, escriba *Error Message Catalog* en el cuadro de búsqueda y haga clic en el botón de búsqueda.
2. En la lista de resultados, ubique el catálogo de su sistema y haga clic en el vínculo.
3. Use la herramienta de búsqueda del navegador para buscar una cadena de caracteres única en el mensaje.

   La descripción del mensaje de error tiene un aspecto similar a la siguiente visualización.

   ```
   ID: MSG-SMTOOL-00006 - Severity: NOTICE - Audience:
   customerMessage: No replication throttle schedules found:
   setting throttle to unlimited.

   Description: The restorer cannot find a replication
   throttle schedule. Replication is running with throttle
   set to unlimited.

   Action: To set a replication throttle schedule, run the
   replication throttle add command.
   ```

4. Para resolver un problema, realice la acción recomendada.

   Según la descripción del mensaje de ejemplo, se podría ejecutar el comando `replication throttle add` para establecer la aceleración.

Guardado de una copia de archivos de registro

Puede guardar copias de archivos de registro en otro dispositivo cuando desea almacenar esos archivos.

Puede usar NFS, montaje CIFS o FTP para copiar los archivos en otra máquina. Si usa CIFS o NFS, monte /ddvar en el escritorio y copie los archivos desde el punto de montaje. El siguiente procedimiento describe cómo usar FTP para mover archivos a otra máquina.

Procedimiento

1. En el sistema Data Domain, use el comando `adminaccess show ftp` para ver si el servicio FTP está habilitado. Si el servicio está deshabilitado, use el comando `adminaccess enable ftp`.
2. En el sistema Data Domain, use el comando `adminaccess show ftp` para ver si la lista de acceso de FTP incluye la dirección IP de su máquina remota. Si la dirección no está en la lista, use el comando `adminaccess add ftp` *ipaddr*.
3. En la máquina remota, abra un navegador web.
4. En el cuadro **Address** que aparece en la parte superior del navegador web, use FTP para acceder al sistema Data Domain como se muestra en el siguiente ejemplo.

   `ftp://Data Domain system_name.yourcompany.com/`

   Nota

   Algunos navegadores web no solicitan automáticamente el inicio de sesión si una máquina no acepta inicios de sesión anónimos. En ese caso, agregue un nombre de usuario y una contraseña a la línea de FTP. Por ejemplo: **`ftp://sysadmin:your-pw@Data Domain system_name.yourcompany.com/`**

5. En el cuadro emergente de inicio de sesión, inicie sesión en el sistema Data Domain como usuario **`sysadmin`**.
6. En el sistema Data Domain, se encuentra en el directorio arriba del directorio de registro. Abra el directorio de registro para ver los archivos de mensajes.
7. Copie el archivo que desee guardar. Haga clic con el botón secundario en el ícono de archivo y seleccione **Copy To Folder** en el menú. Elija una ubicación para la copia del archivo.
8. Si quiere que el servicio FTP esté deshabilitado en el sistema Data Domain, después de completar la copia del archivo, use SSH para iniciar sesión en el sistema Data Domain como sysadmin e invoque el comando `adminaccess disable ftp`.

Transmisión de mensajes de registro a sistemas remotos

Es posible enviar algunos mensajes de registro desde el sistema Data Domain hacia otros sistemas. El sistema operativo DD utiliza syslog para publicar mensajes de registro en los sistemas remotos.

Un sistema Data Domain exporta los siguientes selectores de subsistema.prioridad para los archivos de registro. Para obtener información sobre la administración de selectores y la recepción de mensajes en un sistema de otros fabricantes, consulte la documentación suministrada por su proveedor para el sistema de recepción.

- *.notice: Envía todos los mensajes con la prioridad de aviso o un nivel superior.
- *.alert: Envía todos los mensajes con la prioridad de alerta o un nivel superior (las alertas se incluyen en *.notice).
- kern.*: Envía todos los mensajes de kernel (archivos de registro kern.info).

Los comandos de `log host` administran el proceso de envío de mensajes de registro a otro sistema.

Visualización de la configuración de transmisión del archivo de registro

Utilice el comando de CLI `log host show` para ver si la transmisión del archivo de registro está habilitada y qué hosts reciben archivos de registro.

Procedimiento

1. Para mostrar la configuración, introduzca el comando `log host show`.

```
# log host show
Remote logging is enabled.
Remote logging hosts
     log-server
```

Habilitación y deshabilitación de la transmisión de mensajes de registro

Debe utilizar comandos de la CLI para activar o desactivar la transmisión del mensaje de registro.

Procedimiento

1. Para habilitar el envío de mensajes de registro a otros sistemas, utilice el comando `log host enable`.
2. Para deshabilitar el envío de mensajes de registro a otros sistemas, utilice el comando `log host disable`.

Adición o eliminación de un host receptor

Debe utilizar los comandos de la CLI para agregar o quitar un host receptor.

Procedimiento

1. Para agregar un sistema a la lista que recibe los mensajes de registro del sistema Data Domain, utilice el comando `log host add`.
2. Para eliminar un sistema de la lista que recibe mensajes de registro del sistema, utilice el comando: `log host del`.

El siguiente comando agrega el sistema llamado *log-server* a los hosts que reciben los mensajes de registro.

```
log host add log-server
```

El siguiente comando quita el sistema llamado *log-server* a los hosts que reciben los mensajes de registro.

```
log host del log-server
```

El siguiente comando deshabilita el envío de registros y borra la lista de nombres de host de destino.

```
log host reset
```

Administración de la alimentación de sistemas remotos con IPMI

Determinados sistemas DD admiten la administración de la alimentación a través de Intelligent Platform Management Interface (IPMI), y admiten el monitoreo remoto de la secuencia de encendido con serie por medio de LAN (SOL).

La administración de alimentación de IPMI se lleva a cabo entre un iniciador IPMI y un host remoto de IPMI. El iniciador IPMI es el host que controla la energía en el host remoto. Para admitir la administración remota de la alimentación desde un iniciador, el host remoto debe configurarse con un nombre de usuario y una contraseña para IPMI. El iniciador debe proporcionar estos valores de nombre de usuario y contraseña cuando se intenta administrar la alimentación en un host remoto.

IPMI se ejecuta independientemente de DD OS y le permite a un usuario de IPMI administrar la alimentación del sistema siempre que el sistema remoto esté conectado a una fuente de alimentación y a una red. Se requiere una conexión de red IP entre un host de administración y un sistema remoto. Cuando está configurada y conectada correctamente, la administración de IPMI elimina la necesidad de estar presente físicamente para encender o apagar un sistema remoto.

Puede utilizar DD System Manager y la CLI para configurar los usuarios de IPMI en un sistema remoto. Después de configurar IPMI en un sistema remoto, puede usar funciones de iniciador IPMI en otro sistema para iniciar sesión y administrar la alimentación.

Nota

Si un sistema no admite IPMI debido a limitaciones de hardware o software, DD System Manager muestra un mensaje de notificación cuando intenta acceder a una página de configuración.

SOL se utiliza para visualizar la secuencia de encendido después de un reinicio en un sistema remoto. SOL permite que los datos de consola de texto, que normalmente se envían a un puerto en serie o a una consola conectada directamente, se envíen a través de LAN y se muestren mediante un host de administración.

La CLI de DD OS le permite configurar un sistema remoto para IPMI y SOL, además de ver la salida de la consola remota. Esta función es compatible solo en la CLI.

AVISO

La opción de eliminación de la alimentación de IPMI se proporciona para situaciones de emergencia durante las cuales fallan los intentos de apagar la alimentación con comandos de DD OS. La opción de eliminación de la alimentación de IPMI simplemente elimina la alimentación del sistema, no lleva a cabo un apagado en orden del sistema de archivos de DD OS. La forma correcta de eliminar y volver a aplicar alimentación es a través del comando `system reboot` de DD OS. La forma correcta de eliminar la alimentación del sistema es utilizar el comando `system poweroff` de DD OS y esperar a que el comando apague el sistema de archivos correctamente.

Limitaciones de IPMI y SOL

La compatibilidad con IPMI y SOL es limitada en algunos sistemas Data Domain.

- IPMI se admite en todos los sistemas compatibles con esta versión, excepto los siguientes sistemas: DD140, DD610 y DD630.
- La compatibilidad de usuarios de IPMI varía de la siguiente manera.
  - Modelo DD990: ID de usuario máximos = 15. Tres usuarios predeterminados (NULL, anonymous, root). ID de usuario máximas disponibles = 12.
  - Modelos DD640, DD4200, DD4500, DD7200 y DD9500: ID de usuario máximos = 10. Dos usuarios predeterminados (NULL, root). ID de usuario máximas disponibles = 8.
- SOL se admite en los siguientes sistemas: DD160, DD620, DD640, DD670, DD860, DD890, DD990, DD2200, DD2500 (requiere DD OS 5.4.0.6 o versiones posteriores), DD4200, DD4500, DD7200 y DD9500.

Nota

El usuario root no se admite para las conexiones de IPMI en sistemas DD160.

Cómo agregar o eliminar usuarios de IPMI con DD System Manager

Cada sistema contiene su propia lista de usuarios de IPMI configurados, que se usa para controlar el acceso a funciones de administración de alimentación local. Otro sistema operativo como iniciador de IPMI puede administrar la alimentación del sistema remoto solo después de proporcionar un nombre de usuario y una contraseña válidos.

Para darle a un usuario de IPMI la autoridad para administrar la alimentación en varios sistemas remotos, debe agregarlo a cada uno de los sistemas remotos.

Nota

La lista de usuarios de IPMI de cada sistema remoto es independiente de las listas de DD System Manager para acceso de administradores y usuarios locales. Los administradores y usuarios locales no heredan ninguna autorización de administración de alimentación de IPMI.

Procedimiento

1. Seleccione **Maintenance** > **IPMI**.
2. Para agregar un usuario, siga estos pasos.
   a. Arriba de la tabla Usuarios de IPMI, haga clic en **Add**.
   b. En el cuadro de diálogo Add User, escriba el nombre de usuario (16 caracteres como máximo) y la contraseña en los cuadros correspondientes (vuelva a escribir la contraseña en el cuadro **Verify Password**).
   c. Haga clic en **Create**.
   La entrada del usuario aparecerá en la tabla **IPMI Users**.
3. Para eliminar un usuario, siga estos pasos.
   a. En la lista de usuarios de IPMI, seleccione un usuario y haga clic en **Delete**.

b. En el cuadro de diálogo Delete User, haga clic en **OK** para verificar la eliminación del usuario.

Cambio de la contraseña de un usuario de IPMI

Cambiar la contraseña de usuario de IPMI para evitar el uso de la contraseña anterior para la administración de la alimentación.

Procedimiento

1. Seleccione **Maintenance** > **IPMI**.
2. En la tabla de usuarios de IPMI, seleccione un usuario y haga clic en **Change Password**.
3. En el cuadro de diálogo Change Password, escriba la contraseña en el cuadro de texto correspondiente y vuelva a escribirla en el cuadro **Verify Password**.
4. Haga clic en **Update**.

Configuración de un puerto IPMI

Al configura un puerto para un sistema administrado, puede seleccionar el puerto de una lista de puertos de red y especificar los parámetros de configuración de IP para ese puerto. El modelo del sistema Data Domain determina la selección de puertos IPMI que se muestran.

Algunos sistemas admiten uno o más puertos dedicados, que se pueden usar únicamente para el tráfico de IPMI. Otros sistemas admiten puertos que se pueden usar tanto para tráfico de IPMI como para todo el tráfico de IP admitido por las interfaces físicas de la vista **Hardware** > **Ethernet** > **Interfaces**. No se proporcionan puertos compartidos en sistemas que proporcionan puertos IPMI dedicados.

Los nombres de puerto en la lista IPMI Network Ports usan el prefijo bmc, que representa la controladora de administración de tarjeta madre. Para determinar si un puerto es dedicado o compartido, compare el resto del nombre del puerto con los puertos de la lista de interfaces de red. Si el resto del nombre del puerto IPMI coincide con una interfaz de la lista, es compartido. Si el resto del nombre del puerto IPMI es diferente de los nombres de la lista, es dedicado.

Nota

Los sistemas DD4200, DD4500 y DD7200 son una excepción a la regla de asignación de nombres que se describió anteriormente. En estos sistemas, el puerto IPMI, bmc0a, corresponde al puerto compartido ethMa en la lista de interfaces de red. Si es posible, reserve el puerto compartido ethMa para el tráfico de IPMI y el tráfico de administración del sistema (con protocolos como HTTP, Telnet y SSH). El tráfico de datos de respaldo debe dirigirse a otros puertos.

Cuando el tráfico de IP con IPMI y sin IPMI comparte un puerto Ethernet, si es posible, no utilice la función de agregación de vínculos en la interfaz compartida dado que los cambios en el estado de los vínculos pueden interferir con la conectividad de la IPMI.

Procedimiento

1. Seleccione **Maintenance** > **IPMI**.

   El área IPMI Configuration muestra la configuración de IPMI para el sistema administrado. La tabla Network Ports muestra los puertos en los que se puede habilitar y configurar IPMI. La tabla IPMI Users muestra los usuarios de IPMI que pueden acceder al sistema administrado.

Tabla 58 Descripciones de la columna de lista Network Ports

Elemento	Descripción
Puerto	El nombre lógico de un puerto que admite comunicaciones de IPMI.
Activado	Si el puerto está habilitado para IPMI (Yes o No).
DHCP	Si el puerto usa DHCP para configurar su dirección IP (Yes o No).
Dirección MAC	La dirección MAC de hardware para el puerto.
Dirección IP	La dirección IP del puerto.
Netmask	La máscara de subred para el puerto.
Gateway	La dirección IP de gateway del puerto.

Tabla 59 Descripciones de la columna de lista IPMI Users

Elemento	Descripción
Nombre de usuario	El nombre de un usuario con autoridad para administrar la alimentación del sistema remoto.

2. En la tabla **Network Ports**, seleccione un puerto para configurarlo.

   Nota

   Si el puerto IPMI también admite tráfico de IP (para acceso de administradores o tráfico de respaldo), el puerto de interfaz debe estar habilitado antes de configurar IPMI.

3. Arriba de la tabla **Network Ports**, haga clic en **Configure**.

   Aparecerá el cuadro de diálogo Configure Port.

4. Elija cómo se asigna la información de dirección de red.
   - Para recopilar la información de dirección IP, máscara de red y gateway de un servidor DHCP, seleccione **Dynamic (DHCP)**.
   - Para definir manualmente la configuración de red, seleccione **Static (Manual)** y escriba la dirección IP, la máscara de red y la dirección de gateway.
5. Para habilitar un puerto de red IPMI deshabilitado, seleccione el puerto de red en la tabla **Network Ports** y haga clic en **Enable.**
6. Para deshabilitar un puerto de red IPMI deshabilitado, seleccione el puerto de red en la tabla **Network Ports** y haga clic en **Disable.**
7. Haga clic en **Apply**.

Preparación para la administración remota de la alimentación y el monitoreo de la consola con la CLI

El monitoreo remoto de la consola usa la función de serie por medio de LAN (SOL) para permitir la visualización de la salida de la consola basada en texto sin un servidor

de serie. Debe usar la CLI para configurar un sistema para acceso remoto de monitoreo de la consola y administración de la energía.

El monitoreo remoto de la consola generalmente se usa en combinación con el comando `ipmi remote power cycle` para ver la secuencia de encendido del sistema remoto. Este procedimiento se debe usar en cada sistema para el que desee ver la consola de forma remota durante la secuencia de encendido.

Procedimiento

1. Conecte la consola al sistema de forma directa o remota.
   - Use los siguientes conectores para una conexión directa.
     - Conectores de tipo DIN para un teclado PS/2
     - Puerto de receptáculo USB-A para un teclado USB
     - Conector hembra DB15 para un monitor VGA

     Nota

     Los sistemas DD4200, DD4500 y DD7200 no admiten conexión directa, incluido KVM.

   - Para una conexión en serie, use un conector macho DB9 estándar o un conector hembra micro-DB9. Los sistemas DD4200, DD4500 y DD7200 proporcionan un conector micro-DB9 hembra. Se incluye un cable de módem nulo con conectores micro-DB9 macho y DB9 hembra estándar para una conexión de laptop tradicional.
   - Para una conexión de IPMI/SOL remota, use el receptáculo de RJ45 adecuado de la siguiente manera.
     - Para sistemas DD990, use el puerto eth0d predeterminado.
     - Para otros sistemas, use el puerto de servicio o mantenimiento. Para conocer las ubicaciones de los puertos, consulte la documentación del sistema, como una descripción general de hardware o la guía de instalación y configuración.
2. Para admitir el monitoreo remoto de la consola, use la configuración predeterminada de BIOS.
3. Para mostrar el nombre de puerto de IPMI, ingrese `ipmi show config`.
4. Para habilitar IPMI, escriba `ipmi enable {`*`port`* `| all}`.
5. Para configurar el puerto IPMI, escriba `ipmi config port { dhcp | ipaddress` *`ipaddr`* `netmask` *`mask`* `gateway` *`ipaddr`*`}`.

   Nota

   Si el puerto IPMI también admite tráfico de IP (para acceso de administradores o tráfico de respaldo), el puerto de interfaz debe estar habilitado con el comando `net enable` antes de configurar IPMI.

6. Si es la primera vez que usa IPMI, ejecute `ipmi user reset` para borrar los usuarios de IPMI que podrían estar desincronizados entre los dos puertos y para deshabilitar los usuarios predeterminados.
7. Para agregar un nuevo usuario de IPMI, escriba `ipmi user add`*`user`*.
8. Para configurar SOL, haga lo siguiente:

a. Ingrese `system option set console lan`.

b. Si se le solicita, ingrese `y` para reiniciar el sistema.

Administración de la alimentación con DD System Manager

Después de que IPMI se configure correctamente en un sistema remoto, puede usar DD System Manager para iniciar sesión en el sistema remoto, ver el estado de alimentación y cambiarlo.

Procedimiento

1. Seleccione **Maintenance** > **IPMI**.
2. Haga clic en **Login to Remote System**.

   Se abrirá el cuadro de diálogo IPMI Power Management.

3. Ingrese la dirección IP o el nombre de host de IPMI del sistema remoto y el nombre de usuario y la contraseña de IPMI y, a continuación, haga clic en **Connect**.
4. Visualice el estado de IPMI.

   Aparecerá el cuadro de diálogo IPMI Power Management y se mostrará la identificación del sistema de destino y el estado de alimentación actual. El área Status siempre muestra el estado actual.

   Nota

   El ícono de actualización (las flechas azules) que aparece junto al estado puede usarse para actualizar el estado de configuración (por ejemplo, si la dirección IP de IPMI o la configuración del usuario se modificaron en los últimos 15 minutos con los comandos de CLI).

5. Para cambiar el estado de alimentación de IPMI, haga clic en el botón correspondiente.
   - **Power Up**: aparece cuando el sistema remoto está apagado. Haga clic en este botón para encender el sistema remoto.
   - **Power Down**: aparece cuando el sistema remoto está encendido. Haga clic en este botón para apagar el sistema remoto.
   - **Power Cycle**: aparece cuando el sistema remoto está encendido. Haga clic en este botón para reiniciar el sistema remoto.
   - **Manage Another System**: haga clic en este botón para iniciar sesión en otro sistema remoto para la administración de alimentación de IPMI.
   - **Done**: haga clic aquí para cerrar el cuadro de diálogo IPMI Power Management.

   AVISO

   La función IPMI Power Down no lleva a cabo un apagado ordenado de DD OS. Esta opción se puede usar si DD OS no responde y no se puede utilizar para apagar un sistema correctamente.

Administración de alimentación con la CLI

Puede administrar la alimentación en un sistema remoto e iniciar el monitoreo de la consola remota a través de la CLI.

Nota

El sistema remoto debe estar configurado correctamente antes de que pueda administrar la alimentación o monitorear el sistema.

Procedimiento

1. Establezca una sesión de CLI en el sistema desde el que desea monitorear un sistema remoto.
2. Para administrar la alimentación en el sistema remoto, especifique `ipmi remote power {on | off | cycle | status} ipmi-target <`*ipaddr* | *hostname*`> user` *user*.
3. Para iniciar el monitoreo de la consola remota, especifique `ipmi remote console ipmi-target <`*ipaddr* | *hostname*`> user` *user*.

   Nota

   El nombre de usuario es un nombre de usuario de IPMI definido para IPMI en el sistema remoto. IPMI no admite automáticamente los nombres de usuario del SO DD.

4. Para desconectarse de una sesión de monitoreo de una consola remota y volver a la línea de comandos, escriba el símbolo arroba (@).
5. Para finalizar el monitoreo de la consola remota, escriba el símbolo de tilde de ñ (~).

CAPÍTULO 4

Monitoreo de sistemas Data Domain

Este capítulo incluye:

- Visualización del estado del sistema en forma individual y la información de identidad 182
- Panel de alertas de estado 185
- Visualización y borrado de alertas actuales 185
- Visualización del historial de alertas 187
- Visualización del estado de los componentes de hardware 188
- Visualización de estadísticas del sistema 191
- Visualización de usuarios activos 193
- Administración de informe del historial 193
- Visualización del registro de tareas 198
- Visualización del estado de alta disponibilidad del sistema 199

Visualización del estado del sistema en forma individual y la información de identidad

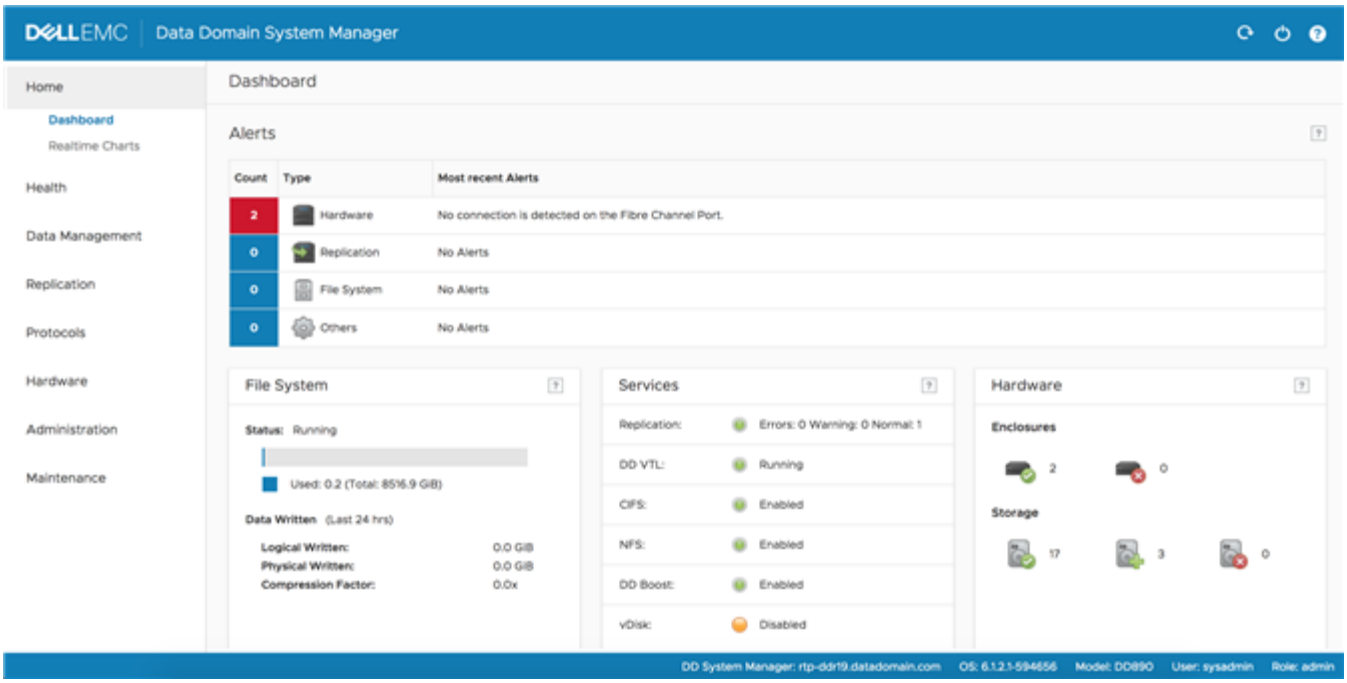
El área **Dashboard** muestra información de resumen y el estado de las alertas, el sistema de archivos, los servicios con licencia y los gabinetes del hardware. El área **Maintenance** muestra información adicional del sistema, incluidos los números de serie del sistema y del chasis, y el tiempo de actividad del sistema.

El nombre del sistema, la versión de software y la información del usuario aparecen en el pie de página en todo momento.

Procedimiento

1. Para ver el tablero del sistema, seleccione **Home** > **Dashboard**.

   Figura 5 Tablero del sistema



2. Para visualizar información sobre el tiempo de funcionamiento y la identidad del sistema, seleccione **Maintenance** > **System**.

   La información de tiempo de actividad e identificación del sistema aparece en el área System.

Área Dashboard Alerts

El área Dashboard Alerts muestra el conteo, el tipo y el texto de las alertas más recientes en el sistema para cada subsistema (ya sea hardware, replicación, sistema de archivos, y otros). Haga clic en cualquier parte del área de alertas para visualizar más información sobre las alertas en curso

Tabla 60 Descripciones de la columna Dashboard Alerts

Columna	Descripción
Conteo	Un conteo de las alertas en curso para el tipo de subsistema especificado en la columna adyacente. El color de fondo indica la gravedad de la alerta.
Tipo	El subsistema de almacenamiento que generó la alerta.
Alertas más recientes	El texto de la alerta más reciente para el tipo de subsistema especificado en la columna adyacente

Área Dashboard File System

El área Dashboard File System muestra estadísticas para la totalidad del sistema de archivos. Haga clic en cualquier parte del área File System para visualizar más información sobre el sistema de archivos.

Tabla 61 Descripción de las etiquetas del área File System

Columna	Descripción
Status	El estado actual del sistema de archivos.
X.Xx	El factor promedio de compresión de reducción para el sistema de archivos.
Utilizado	El total del espacio utilizado del sistema de archivos.
Datos escritos: Pre-compression	El volumen de datos recibidos por el sistema previo a la compresión.
Datos escritos: Post-compression	El volumen de datos almacenados en el sistema posterior a la compresión.

Área Dashboard Services

El área Dashboard Services muestra el estado de los servicios de replicación, DD VTL, CIFS, NFS, DD Boost y vDisk. Haga clic en un servicio para poder ver información detallada acerca de ese servicio.

Tabla 62 Descripción de columnas del área Services

Columna	Descripción
Columna izquierda	La columna de la izquierda enumera los servicios que pueden ser usados en el sistema. Estos servicios pueden incluir servicios de replicación, DD VTL, CIFS, NFS, DD Boost y vDisk.
Right column	La columna derecha muestra el estado operacional del servicio. Para la mayoría de los

Tabla 62 Descripción de columnas del área Services (continuación)

Columna	Descripción
	servicios, el estado está habilitado, deshabilitado, o no tiene licencia. La fila de servicio de replicación muestra el volumen de contextos de replicación que se encuentran en los estados normal, advertencia y error. Un cuadro de código de color aparecerá en verde en caso de operación normal, amarillo para las situaciones que requieran advertencia o rojo cuando se presentan errores).

Área de preparación de alta disponibilidad de tablero

En los sistemas de alta disponibilidad (HA), el panel de alta disponibilidad indica si el sistema puede realizar un failover del nodo activo al nodo en standby si es necesario.

Puede hacer clic en el **panel de HA** para navegar a la sección **High Availability** en **HEALTH**.

Área Dashboard Hardware

El área Dashboard Hardware muestra el estado de los gabinetes y las unidades del sistema. Haga clic en cualquier parte del área Hardware para visualizar más información sobre estos componentes.

Tabla 63 Descripción de etiquetas de área Hardware

Etiqueta	Descripción
Unidades	Los íconos del gabinete muestran la cantidad de gabinetes que operan en estados normal (marca de verificación verde) y degradado (X roja).
Almacenamiento	Los íconos de almacenamiento muestran el volumen de unidades de disco que operan en estado normal (marca de verificación verde), repuesto (+ verde), o fallado (X roja).

Área Maintenance System

El área Maintenance System muestra el número de modelo del sistema, la versión de DD OS, el tiempo de funcionamiento del sistema y los números de serie del chasis y del sistema.

Tabla 64 Descripción de las etiquetas del área System

Etiqueta	Descripción
Número de modelo	El número de modelo es el número asignado al sistema Data Domain.

Tabla 64 Descripción de las etiquetas del área System (continuación)

Etiqueta	Descripción
Versión	La versión es la versión del DD OS y el número de compilación del software que se ejecuta en el sistema.
Uptime del sistema	El uptime del sistema muestra el tiempo que el sistema estuvo ejecutándose desde el su último arranque. La hora entre paréntesis indica el momento en que el sistema se actualizó por última vez.
Nro. de serie del sistema	El número de serie del sistema es el número de serie asignado al sistema. En los sistemas más recientes, como DD4500 y DD7200 , el número de serie del sistema es independiente del número de serie del chasis y continúa siendo el mismo durante muchos tipos de eventos de mantenimiento, incluyendo los reemplazos de chasis. En los sistemas heredados, como DD990 y anteriores, el número de serie del sistema se establece en el número de serie del chasis.
Nro. de serie de chasis	El número de serie del chasis es el número de serie del chasis del sistema en curso.

Panel de alertas de estado

Las alertas son mensajes de los servicios del sistema y del subsistema que informan eventos del sistema. El panel Health > Alerts muestra pestañas que permiten visualizar alertas que estén o no estén en curso, los grupos de notificación de alertas configurados, y la configuración para quienes deseen recibir informes de resumen de alertas a diario.

Las alertas también se envían como capturas SNMP. Consulte la *Guía de referencia rápida de MIB* o el SNMP MIB para obtener una lista completa de capturas.

Visualización y borrado de alertas actuales

La pestaña Current Alerts muestra una lista de todas las alertas en curso y puede mostrar información detallada de una alerta seleccionada. Un alerta se elimina automáticamente de la lista de Current Alerts cuando la situación subyacente es corregida o cuando es borrada en forma manual.

Procedimiento

1. Para ver todas las alertas actuales, seleccione **Health** > **Alerts** > **Current Alerts**.
2. Para limitar la cantidad de entradas en la lista de alertas en curso, haga lo siguiente.
   a. En el área Filter By, seleccione un valor de **Severity** y **Class** para ver solo las alertas que pertenecen a esas elecciones.
   b. Haga clic en **Update**.

Todas las alertas que no concuerden con la severidad y la clase se eliminan de la lista.

3. Para visualizar información adicional sobre una alerta específica en el área **Details**, haga clic en la alerta de la lista.
4. Para borrar un alerta, seleccione la casilla de verificación de alerta en la lista y haga clic en **Clear**.

   Una alerta borrada dejará de aparecer en la lista de alertas en curso, pero se puede ser encontrada en la lista del historial de alertas.

5. Para quitar el filtrado y volver a la lista completa de las alertas en curso, haga clic en **Reset**.

Pestaña de Current Alerts

La pestaña Current Alert muestra una lista de alertas e información detallada acerca de una alerta seleccionada.

Tabla 65 Lista de Alerts, descripción de etiquetas de columna

Elemento	Descripción
Mensaje	El texto del mensaje de alerta.
Severidad	El nivel de severidad del alerta. Por ejemplo, advertencia, crítica, info o emergencia.
Fecha	Fecha y hora en que apareció el alerta.
Clase	El subsistema en donde apareció el alerta.
Objetos	El componente físico donde está ocurriendo el alerta.

Tabla 66 Área Details, descripción de etiquetas de fila

Elemento	Descripción
Nombre	Un identificador textual para el alerta.
Mensaje	El texto del mensaje de alerta.
Severidad	El nivel de severidad del alerta. Por ejemplo, advertencia, crítica, info, emergencia.
Clase	El subsistema y dispositivo en el que se apareció el alerta.
Fecha	Fecha y hora en que apareció el alerta.
ID de objeto	El componente físico donde está ocurriendo el alerta.
ID del evento	Un identificador de evento.
Unidades del grupo de usuarios	Listas afectadas por grupos de usuarios
Descripción	Información más descriptiva sobre el alerta.
Acción	Una sugerencia para remediar el alerta.
Object Info	Proporciona información adicional sobre el objeto afectado.
SNMP OID	ID del objeto SNMP

Visualización del historial de alertas

La pestaña Alerts History muestra una lista de todas las alertas borradas y puede mostrar información detallada de una alerta seleccionada.

Procedimiento

1. Para ver todo el historial de alertas, seleccione **Health** > **Alerts** > **Alerts History**.
2. Para limitar la cantidad de entradas en la lista de alertas en curso, haga lo siguiente.
   a. En el área Filter By, seleccione un valor de **Severity** y **Class** para ver solo las alertas que pertenecen a esas elecciones.
   b. Haga clic en **Update**.
   Todas las alertas que no concuerden con la severidad y la clase se eliminan de la lista.
3. Para visualizar información adicional sobre una alerta específica en el área **Details**, haga clic en la alerta de la lista.
4. Para quitar el filtrado y volver a la lista completa de las alertas borradas, haga clic en **Reset**.

Pestaña de Alerts History

La pestaña Alerts History muestra una lista de alertas borradas y de detalles acerca de una alerta seleccionada.

Tabla 67 Lista de Alerts, descripción de etiquetas de columna

Elemento	Descripción
Mensaje	El texto del mensaje de alerta.
Severidad	El nivel de severidad del alerta. Por ejemplo, advertencia, crítica, info o emergencia.
Fecha	Fecha y hora en que apareció el alerta.
Clase	El subsistema en donde apareció el alerta.
Objetos	El componente físico donde está ocurriendo el alerta.
Status	Si el estado se publica o se borra. Una alerta publicada no es borrada.

Tabla 68 Área Details, descripción de etiquetas de fila

Elemento	Descripción
Nombre	Un identificador textual para el alerta.
Mensaje	El texto del mensaje de alerta.
Severidad	El nivel de severidad del alerta. Por ejemplo, advertencia, crítica, info, emergencia,
Clase	El subsistema y dispositivo en el que se apareció el alerta.

Tabla 68 Área Details, descripción de etiquetas de fila (continuación)

Elemento	Descripción
Fecha	Fecha y hora en que apareció el alerta.
ID de objeto	El componente físico donde está ocurriendo el alerta.
ID del evento	Un identificador de evento.
Unidades del grupo de usuarios	Listas afectadas por grupos de usuarios
Información adicional	Información más descriptiva sobre el alerta.
Status	Si el estado se publica o se borra. Una alerta publicada no es borrada.
Descripción	Información más descriptiva sobre el alerta.
Acción	Una sugerencia para remediar el alerta.

Visualización del estado de los componentes de hardware

El panel Hardware Chassis muestra una imagen de bloque de cada gabinete en un sistema, que incluye el número de serie Del chasis y el estado del gabinete. Dentro de cada imagen de bloque se encuentran los componentes del gabinete, tales como discos, ventiladores, fuentes de alimentación, NVRAM, CPU y memoria. Los componentes que se muestran dependen del sistema modelo.

En los sistemas que ejecutan DD OS 5.5.1 y posteriores, también se mostrará el número de serie del sistema. En los sistemas más recientes, como DD4500 y DD7200 , el número de serie del sistema es independiente del número de serie del chasis y continúa siendo el mismo durante muchos tipos de eventos de mantenimiento, incluyendo los reemplazos de chasis. En los sistemas antiguos, como DD990 y anteriores, el número de serie del sistema se establece en el número de serie del chasis.

Procedimiento

1. Seleccione **Hardware** > **Chassis**.

   La vista Chassis muestra los gabinetes del sistema. Enclosure 1 es el controlador del sistema, y el resto de los gabinetes aparecen debajo del Enclosure 1.

   Los componentes que presentan problemas se muestran amarillo (advertencia) o rojo (error); de lo contrario, el componente muestra un OK.

2. Pase el cursor sobre un componente para ver una versión detallada de su estado.

Estado del ventilador

La numeración de los ventiladores corresponde a su ubicación en el chasis. Posicione el cursor sobre un ventilador del sistema para mostrar un mensaje de globo para ese dispositivo.

Tabla 69 Mensaje de globo de ventilador, descripción de etiquetas de columna

Elemento	Descripción
Descripción	El nombre del ventilador.
Nivel	El rango de velocidad de la operación en curso (Baja, Media, Alta). Los cambios en la velocidad de operación según la temperatura en el interior del chasis.
Estado	La condición en que se encuentra el ventilador.

Estado de la temperatura

Los sistemas Data Domain y algunos componentes están configurados para operar dentro de un rango de temperatura específico que está definida por un perfil de temperatura que no puede ser configurado. Posicione el cursor sobre el cuadro de la temperatura para ver el mensaje de globo de temperatura.

Tabla 70 Mensaje de globo de temperatura, descripción de etiquetas de columna

Elemento	Descripción
Descripción	La ubicación dentro del chasis a medirse. Los componentes enumerados dependen del modelo y, por lo general, se muestran como abreviaturas. Algunos ejemplos incluyen: • CPU 0 Temp (Unidad de procesamiento central) • MLB Temp 1 (placa lógica principal) • BP middle temp (backplane) • LP temp (bajo perfil de I/O en aumento FRU) • FHFL temp (altura completa longitud completa de I/O en aumento FRU) • FP temp (panel frontal)
C/F	La columna C/F muestra la temperatura en grados Celsius y Fahrenheit. Cuando la descripción de una CPU especifica *relativa* (CPU *n* Relative), esta columna muestra la cantidad grados por debajo de la temperatura máxima admisible se encuentra cada CPU y la temperatura del momento en el interior del chasis (chassis ambient).
Estado	Muestra el estado de la temperatura: • OK: la temperatura es aceptable • Critical: la temperatura es superior a la temperatura de apagado. • Warning: la temperatura es superior a la temperatura de advertencia (pero inferior a la temperatura de apagado). • Guión (-): No hay rangos de temperatura configurados para este componente, por lo que no se puede informar ningún estado.

Estado del panel Management

Los sistemas DD6300, DD6800 y DD9300 tienen un panel de administración fijo con un puerto Ethernet para la red de administración en la parte posterior del chasis. Coloque el cursor sobre el puerto Ethernet para que aparezca un mensaje de globo.

Tabla 71 Descripciones de etiquetas de la columna del mensaje de globo del panel Management

Elemento	Descripción
Descripción	El tipo de tarjeta NIC instalada en el panel Management.
Proveedor	El fabricante de la tarjeta NIC de administración.
Puertos	El nombre de la red de administración (Ma).

Estado del disco SSD (solo DD6300)

El DD6300 es compatible con hasta dos discos SSD en los slots en la parte posterior del chasis. Los slots de los discos SSD están numerados y corresponden a su ubicación en el chasis. Posicione el cursor sobre discos SSD para mostrar un mensaje de globo para ese dispositivo.

Tabla 72 Descripción de etiquetas de columna del mensaje de globo del disco SSD

Elemento	Descripción
Descripción	El nombre del disco SSD.
Status	El estado del disco SSD:
Life Used	El porcentaje de la vida útil operativa clasificada que el disco SSD usa.

Estado de la fuente de alimentación

El mensaje de globo muestra el estado de la fuente de alimentación (OK o DEGRADED si una fuente de alimentación se encuentra ausente o fallida). También puede ver en el panel posterior del gabinete y verificar el LED de cada fuente de alimentación para identificar las que necesiten ser reemplazadas.

Estado del slot de PCI

Los slots de PCI que se muestran en la vista de chasis indican la cantidad de slots de PCI y el número de cada ranura. Los mensajes de globo proporcionan el estado del componente para cada tarjeta en un slot de PCI. Por ejemplo, el mensaje de globo de un modelo de tarjeta NVRAM muestra el tamaño de la memoria, los datos de la temperatura y los niveles de la batería.

Estado de NVRAM

Posicione el cursor sobre NVRAM para visualizar información sobre la memoria RAM no volátil, baterías y otros componentes.

Tabla 73 Mensaje de globo del NVRAM, descripción de etiquetas de columna

Elemento	Descripción
Componente	Los elementos de la lista de componentes dependen del NVRAM instalado en el sistema y pueden incluir los siguientes elementos. • Versión de firmware • Memory size • Recuentos de errores • Recuentos de errores del controlador flash • Temperatura de la placa • Temperatura del CPU • Número de la batería (la cantidad de baterías depende del tipo de sistema.) • Número de slot actual para el NVRAM
C/F	Muestra la temperatura para los componentes seleccionados en formato Celsius/Fahrenheit.
Valor	Los valores se proporcionan para los componentes seleccionados y describen lo siguiente. • El número de versión del firmware • El valor del tamaño de la memoria en las unidades que se muestran • Recuentos de errores para la memoria, el PCI y el controlador • Recuentos de errores del controlador flash ordenados en los siguientes grupos: errores de configuración (Cfg Err), condiciones de pánico (Panic), Bus Hang, advertencias de bloques malos (Bad Blk Warn), errores de respaldo (Bkup Err), y errores de restauración (Rstr Err) • Información de la batería, como el porcentaje de carga y el estado (activado o desactivado)

Visualización de estadísticas del sistema

El panel Realtime Charts presenta hasta cinco gráficos que muestran las estadísticas de rendimiento del subsistema en tiempo real, como el uso de CPU y el tráfico de disco.

Procedimiento

1. Seleccione **Home** > **Realtime Charts**.

   El área Performance Graphs muestra los gráficos que estén seleccionados en ese momento.
2. Para cambiar la selección de gráficos que desea visualizar, seleccione y desactive las casillas de verificación para los gráficos en el cuadro de lista.
3. Para ver información específica de punto de datos, posicione el cursor sobre un punto del gráfico.

4. Cuando un gráfico que contiene varios datos, podrá utilizar las casillas de verificación en la esquina superior derecha del gráfico para seleccionar lo que desee visualizar. Por ejemplo, si Read no está seleccionada en la parte superior derecha del gráfico de actividad del disco, solamente aparecerán los datos de escritura.

Resultados

Cada gráfico muestra el uso de los últimos 200 segundos. Haga clic en **Pause** para detener temporalmente el gráfico. Haga clic en **Resume** para reiniciarlo y ver los puntos que se perdieron durante la pausa.

Gráfico de estadísticas del rendimiento

Los gráficos de estadísticas del rendimiento muestran las estadísticas para los componentes y funciones claves del sistema.

Conexiones activas de DD Boost

El gráfico DD Boost Active Connections muestra la cantidad de conexiones activas de DD Boost para cada uno de los últimos 200 segundos. Las líneas separadas del gráfico muestran los conteos para las conexiones de lectura (recuperación) y de escritura (de respaldo).

Rendimiento de datos de DD Boost

El gráfico DD Boost Data Throughput muestra los bytes transferidos por segundo para cada uno de los últimos 200 segundos. Las líneas separadas dentro del gráfico muestran las tasas de datos leídos desde el sistema por los clientes DD Boost y los datos escritos en el sistema por los clientes DD Boost.

Disco

El gráfico Disk muestra el volumen de datos en la unidad de medida adecuada en base a los datos recibidos, como KiB o MiB por segundo, que son transferidos desde y hacia todos los discos en el sistema.

Operaciones del sistema de archivos

El gráfico File System Operations muestra el volumen de operaciones por segundo que se produjeron para cada uno en los últimos 200 segundos. Las líneas separadas dentro del gráfico muestran las operaciones NFS y CIFS por segundo.

Red

El gráfico Network muestra el volumen de datos en la unidad de medida adecuada según los datos recibidos, como KiB o MiB por segundo, que se transfieren a través de cada conexión Ethernet. Aparece una línea por cada puerto Ethernet.

Uso reciente del CPU

El gráfico Recent CPU Usage muestra el porcentaje de uso del CPU para cada uno de los últimos 200 segundos.

Replicación (el DD Replicator debe contar con licencia)

El gráfico Replication muestra el volumen de replicación de datos que se transfieren a través de la red en cada uno de los últimos 200 segundos. Las líneas separadas muestran los datos de entrada y salida de la siguiente manera:

- In: La cantidad total de unidades de medida, tales como kilobytes por segundo, recibida por este lado desde el otro lado del par de DD Replicator. Para el destino, el valor incluye los datos de respaldo, la sobrecarga de la

replicación y la sobrecarga de la red. Para el origen, el valor incluye la sobrecarga de la replicación y la sobrecarga de la red.

- Out: La cantidad total de unidades de medida, tales como kilobytes por segundo, enviada por este lado hacia el otro lado del par de DD Replicator. Para el origen, el valor incluye los datos de respaldo, la sobrecarga de la replicación y la sobrecarga de la red. Para el destino, el valor incluye la sobrecarga de la replicación y de la red.

Visualización de usuarios activos

La pestaña Active Users muestra los nombres de los usuarios que se encuentran con la sesión iniciada en el sistema y las estadísticas sobre las sesiones en curso de los usuarios.

Procedimiento

1. Seleccione **Administration** > **Access** > **Active Users**.

   La lista Active Users aparecerá y mostrará la información de cada usuario.

Tabla 74 Lista Active Users, descripción de etiquetas de columna

Elemento	Descripción
Nombre	Nombre de usuario del usuario que inició sesión.
Idle	Tiempo transcurrido desde la última actividad del usuario.
Último inicio de sesión desde	Sistema del que el usuario inició sesión.
Hora de último inicio de sesión	Marca de fecha de cuando el usuario inició sesión.
TTY	Anotación de terminales para iniciar sesión. El GUI aparece para los usuarios de DD System Manager.

Nota

Para administrar usuarios locales, haga clic en **Go to Local Users**.

Administración de informe del historial

DD System Manager le permite generar informes para rastrear el uso del espacio en un sistema Data Domain de hasta dos años atrás. También puede generar informes para ayudarlo a comprender el progreso de la replicación y ver informes diarios y acumulativos sobre el sistema de archivos.

La vista Reports se divide en dos secciones. La sección superior le permite crear los distintos tipos de informes. La sección inferior le permite ver y administrar los informes guardados.

Los informes se muestran en un formato de tabla y como gráficos, según el tipo de informe. Puede seleccionar un informe para un sistema Data Domain específico y proporcionar un período de tiempo específico.

Los informes muestran datos históricos, no datos en tiempo real. Luego de que el informe se haya generado, los gráficos permanecen estáticos y no se actualizan. Los ejemplos de los tipos de información que puede obtener de los informes incluyen:

- El volumen de datos que se respaldaron en el sistema y el volumen de deduplicación logrado.
- Las estimaciones del momento en que el sistema Data Domain estará lleno, basadas en las tendencias semanales de uso del espacio
- La utilización de respaldos y compresión basada en intervalos seleccionados
- El rendimiento de limpieza histórico, incluyendo la duración del ciclo de limpieza, el volumen de espacio que puede limpiarse y la cantidad de espacio recuperado
- El volumen de ancho de banda WAN utilizada por la replicación, por tanto el origen como el destino y si el ancho de banda es suficiente como para cumplir con los requisitos de la replicación
- Rendimiento del sistema y utilización de recursos

Tipos de informes

El área de New Report enumera los tipos de informes que puede generar en su sistema.

Nota

Los informes de replicación solo pueden ser creados si el sistema contiene una licencia de replicación y si hay un contexto de replicación configurado.

Informe de File System Cumulative Space Usage

El informe File System Cumulative Space Usage muestra tres gráficos en los que se detalla el uso del espacio en el sistema a lo largo de la duración especificada. Este informe se utiliza para analizar el volumen de datos que son respaldados, el volumen de deduplicación ejecutado y la cantidad de espacio consumido.

Tabla 75 File System: descripción de las etiquetas del gráfico de uso

Elemento	Descripción
Datos escritos (GiB)	El volumen de datos escritos previo a la compresión. Esto se indica a través de un área del en el informe sombreada en púrpura
Hora	La línea de tiempo para los datos que fueron escritos. La hora que se muestra en este informe se modifica según la duración seleccionada al momento de crearse el gráfico.
Total Compression Factor	El factor de compresión total informa la relación de compresión.

Tabla 76 File System: descripción de las etiquetas del gráfico de consumo

Elemento	Descripción
Utilizado (GiB)	El volumen de espacio utilizado posterior a la compresión.
Hora	La fecha en que se escribieron los datos. La hora que se muestra en este informe se modifica según la duración seleccionada al momento de crearse el gráfico.
Used (Post Comp)	El volumen de almacenamiento utilizado posterior a la compresión.

Tabla 76 File System: descripción de las etiquetas del gráfico de consumo (continuación)

Elemento	Descripción
Tendencia de uso	La línea de puntos negros muestra la tendencia del uso del almacenamiento. Cuando la línea alcance el nivel de la línea roja en la parte superior, el almacenamiento estará casi lleno.
Capacidad	La capacidad total en un sistema Data Domain.
Cleaning	Cleaning es el ciclo de limpieza (hora de inicio y finalización de cada ciclo de limpieza). Los administradores pueden utilizar esta información para elegir el mejor momento para ejecutar la limpieza mediante la mejor configuración de aceleración.

Tabla 77 Descripción de etiquetas del gráfico File System Weekly Cumulative Capacity

Elemento	Descripción
Fecha (u hora para el informe de 24 horas)	El último día de cada semana, según el criterio establecido para el informe. En los informes, un período de 24 horas es de mediodía a mediodía.
Datos Escrito (Pre-Comp)	Los datos escritos acumulados antes de la compresión para el período de tiempo especificado.
Utilizado (Post-Comp)	Los datos escritos acumulados luego de la compresión para el período de tiempo especificado.
Compression Factor	El factor de compresión total. Esto se indica mediante una línea negra en el informe.

Informe File System Daily Space Usage

El informe File System Daily Space Usage muestra cinco gráficos en lo que se detalla el uso del espacio a lo largo de la duración especificada. Este informe se utiliza para analizar las actividades diarias.

Tabla 78 Descripción de las etiquetas del gráfico File System Daily Space Usage

Elemento	Descripción
Espacio utilizado (GiB)	La cantidad de espacio utilizado. Post-comp es el área sombreada de rojo. Pre-Comp es el área sombreada de púrpura.
Time	La fecha en que se escribieron los datos.
Compression Factor	El factor de compresión total. Esto se indica a través de un cuadrado negro en el informe.

Tabla 79 Descripción de las etiquetas del gráfico File System Daily Capacity Utilization

Elemento	Descripción
Fecha	La fecha en que se escribieron los datos.
Datos Escrito (Pre-Comp)	El volumen de datos escritos previo a la compresión.

Tabla 79 Descripción de las etiquetas del gráfico File System Daily Capacity Utilization (continuación)

Elemento	Descripción
Utilizado (Post-Comp)	El volumen de almacenamiento utilizado posterior la compresión.
Total Compression Factor	El factor de compresión total.

Tabla 80 Descripción de las etiquetas del gráfico File System Weekly Capacity Utilization

Elemento	Descripción
Fecha de inicio	El primer día de la semana para este resumen.
Fecha final	El último día de la semana para este resumen.
Available	El volumen total de almacenamiento disponible.
Consumida	El volumen total de almacenamiento utilizado.
Datos (Post -Comp)	Los datos acumulados escritos previo a la compresión para el período de tiempo especificado.
Replicación (Post-Comp)	Los datos acumulados escritos posterior a la compresión para el período de tiempo especificado.
Sobrecarga	Espacio extra utilizado para el almacenamiento, pero que no sea de datos.
Recuperado por Limpieza	El espacio total recuperado después de la limpieza.

Tabla 81 Descripción de las etiquetas del gráfico File System Compression Summary

Elemento	Descripción
Time	El período de recolección de datos para este informe.
Datos Escrito (Pre-Comp)	El volumen de datos escritos previo a la compresión.
Utilizado (Post-Comp)	El volumen de almacenamiento utilizado posterior la compresión.
Total Compression Factor	El factor de compresión total.

Tabla 82 Descripción de las etiquetas del gráfico File System Cleaning Activity

Elemento	Descripción
Hora de inicio	La hora de inicio de la actividad de limpieza.
Fecha final	La hora de finalización de la actividad de limpieza.
Duración (horas)	El tiempo total requerido para la limpieza en horas.
Espacio recuperado	El espacio recuperado en Gibibytes (GiB).

Informe de estado de la replicación

El informe Replication Status muestra tres gráficos que proporcionan el estado del trabajo de replicación que se está ejecutando en el sistema. Este informe se utiliza

para proporcionar un snapshot de lo que está sucediendo en todos los contextos de replicación para ayudar a entender el estado general de la replicación en un sistema Data Domain.

Tabla 83 Descripción de las etiquetas del gráfico Replication Context Summary

Elemento	Descripción
ID	Identificación de contexto de replicación
Origen	Nombre del sistema de origen.
Destino	Nombre del sistema de destino.
Tipo	Tipo de contexto de replicación: MTree, Directory, Collection o Pool.
Estado	Los tipos de estado de replicación incluyen: Error, Normal.
Sync as of Time	Hora y fecha de la última sincronización.
Estimated Completion	El tiempo estimado para que se completa la replicación.
Pre-Comp Remaining:	El volumen de datos comprimidos previamente para ser replicados. Esto sólo se aplica al tipo Collection.
Post-Comp Remaining:	El volumen de datos comprimidos posteriormente para ser replicados. Esto sólo aplica a los tipos Directory y Pool.

Tabla 84 Descripción de las etiquetas del gráfico Replication Context Error Status

Elemento	Descripción
ID	Identificación de contexto de replicación
Origen	Nombre del sistema de origen.
Destino	Nombre del sistema de destino.
Tipo	Tipo de contexto de replicación Directory o Pool.
Estado	Los tipos de estado de replicación incluyen: Error, Normal o Warning.
Descripción	Descripción del error.

Tabla 85 Descripción de las etiquetas del gráfico Replication Destination Space Availability

Elemento	Descripción
Destino	Nombre del sistema de destino.
Disponibilidad de espacio (GiB)	El volumen total de almacenamiento disponible.

Informe Replication Summary

El informe Replication Summary proporciona información del rendimiento sobre el uso general de entrada y salida en la red de un sistema para su replicación, así como por los niveles de contexto durante un lapso especificado. Deberá seleccionar los contextos para ser analizados mediante una lista.

Tabla 86 Descripción de etiquetas del informe Replication Summary

Elemento	Descripción
Network In (MiB)	El volumen de datos que ingresan al sistema. Network In se indica con una línea verde fina.
Network Out (MiB)	La cantidad de datos enviados desde el sistema. Network In se indica con una línea naranja fina.
Time	La fecha en que se escribieron los datos.
Pre-Comp Remaining (MiB)	El volumen de datos comprimidos previamente para ser replicados. Pre-Comp Remaining se indica con una línea azul.

Visualización del registro de tareas

El Task Log muestra una lista de los trabajos que se están ejecutando, tal como la replicación o las actualizaciones del sistema. El DD System Manager puede administrar múltiples sistemas y puede iniciar tareas en esos mismos sistemas. Si se inicia una tarea en un sistema remoto, se realiza un seguimiento de su progreso en el registro de tareas de la estación de administración, y no en el registro de tareas del sistema remoto.

Procedimiento

1. Seleccione **Health** > **Jobs**.

   Aparecerá la vista Tasks.

2. Seleccione un filtro por el cual visualizar el registro de tareas desde el cuadro de lista Filter By. Puede seleccionar **All**, **In Progress**, **Failed** o **Completed**.

   La vista Tasks muestra el estado de todas las tareas basadas en el filtro seleccionado y se actualiza cada 60 segundos.

3. Para actualizar en forma manual la lista Tasks, realice alguna de las siguientes indicaciones.
   - Haga clic en **Update** para actualizar el registro de tareas.
   - Haga clic en **Reset** para visualizar todas las tareas y borrar todos los filtros previamente establecidos.

4. Para visualizar información detallada acerca de una tarea, selecciónela en la lista de tareas.

   Tabla 87 Información detallada, descripción de etiquetas

Elemento	Descripción
Sistema	El nombre del sistema.
Descripción de la tarea	Una descripción de la tarea.
Status	El estado de la tarea (completado, fallido, o en curso).
Hora de inicio	La fecha y hora local de inicio de la tarea.
Fecha final	La fecha y hora local de finalización de la tarea.

Tabla 87 Información detallada, descripción de etiquetas (continuación)

Elemento	Descripción
Mensaje de error	Un mensaje de error aplicable, si los hubiere.

Visualización del estado de alta disponibilidad del sistema

Puede usar el panel **High Availability** para ver información detallada sobre el estado de alta disponibilidad del sistema y si el sistema puede realizar una conmutación por error de ser necesario.

Procedimiento

1. Seleccione **Health > High Availability** en DD System Manager.

   Aparece la pantalla **Health High Availability**.
   Una marca de verificación verde indica que el sistema está funcionando normalmente y está listo para la conmutación por error.

   La pantalla muestra el nodo activo, que generalmente es el nodo 0.

2. Coloque el cursor sobre un nodo para ver su estado.

   El nodo está resaltado en azul si está activo.

3. Si desea cambiar la vista del nodo activo al nodo en espera, que generalmente es el nodo 1, haga clic en el menú desplegable en la barra del encabezado.

Estado de alta disponibilidad

La vista **Health High Availability** (HA) brinda información sobre el estado del sistema mediante un diagrama de los nodos y su almacenamiento conectado. Además, también se pueden ver todas las alertas actuales y datos detallados sobre el sistema.

Puede determinar si el nodo activo y el almacenamiento son operacionales colocando el cursor sobre ellos. Cuando funcionan con normalidad, están resaltados en azul. El nodo en standby debe aparecer en color gris.

También puede filtrar la tabla de alertas haciendo clic en un componente. Solo se mostrarán las alertas relacionadas con los componentes seleccionados.

Figura 6 Indicadores de estado/alta disponibilidad

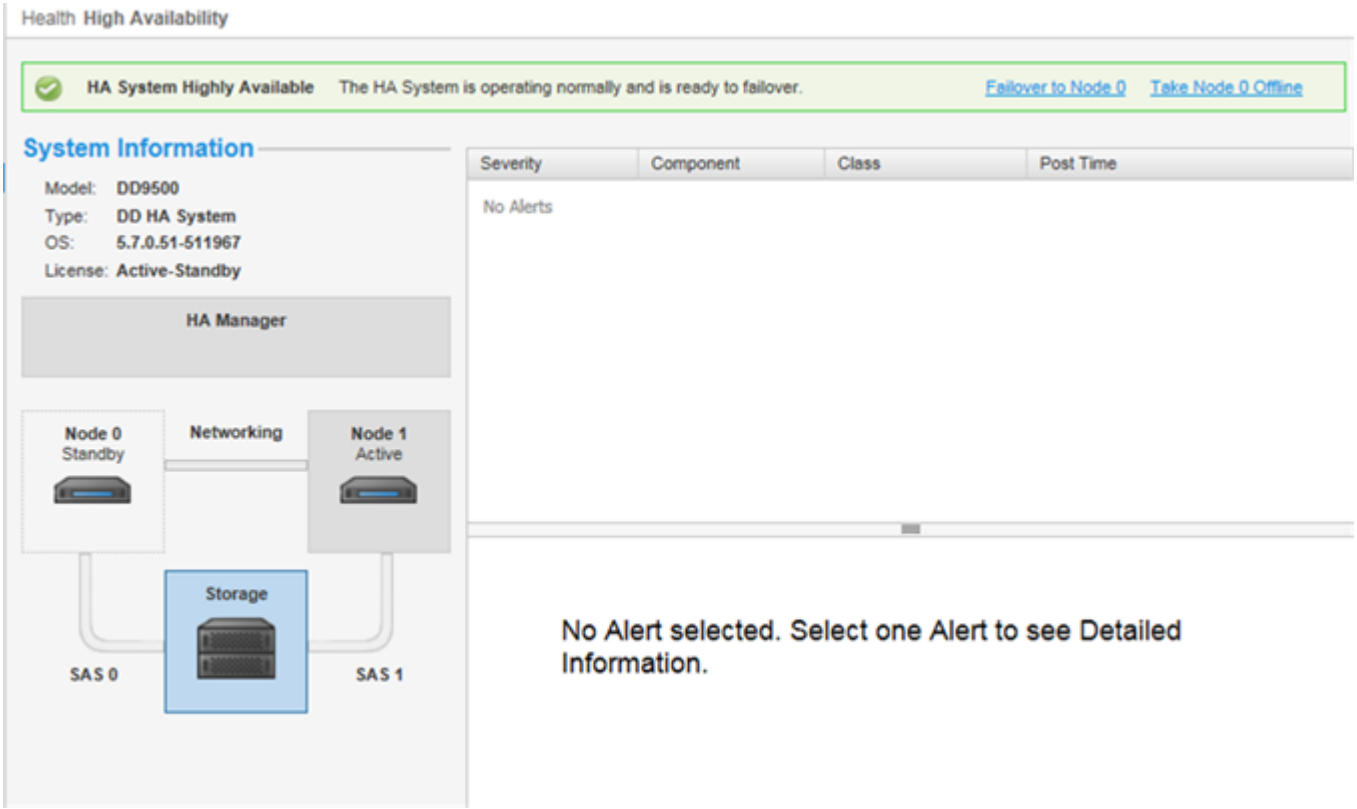


Tabla 88 Indicadores de alta disponibilidad

Elemento	Descripción
Barra de sistema de alta disponibilidad	Muestra una marca de verificación verde cuando el sistema está funcionando normalmente y está listo para el failover.
Failover al nodo 0	Le permite realizar un failover manual al nodo en standby.
Poner el nodo 1 offline	Le permite poner el nodo activo offline si es necesario.
Información del sistema	Detalla el modelo del sistema Data Domain, el tipo de sistema, la versión de la versión del sistema operativo de Data Domain en uso y la licencia de alta disponibilidad aplicada.
Administrador de alta disponibilidad	Muestra los nodos, el almacenamiento conectado, la interconexión de alta disponibilidad y el cableado.
Severidad	Indica la severidad de las alertas que podrían afectar el estado de alta disponibilidad del sistema.
Componente	Indica qué componente está afectado.

Tabla 88 Indicadores de alta disponibilidad (continuación)

Elemento	Descripción
Clase	Indica la clase de la alerta recibida, como hardware y ambiente, entre otras.
Tiempo de publicación	Indica la hora y la fecha en las que se publicó la alerta.

CAPÍTULO 5

Sistema de archivos

Este capítulo incluye:

- Descripción general del sistema de archivos 204
- Monitoreo del uso del sistema de archivos 212
- Administración de las operaciones del sistema de archivos 221
- Operaciones de copia rápida 230

Descripción general del sistema de archivos

Aprenda cómo utilizar el sistema de archivos.

Cómo almacena datos el sistema de archivos

La capacidad de almacenamiento de Data Domain se administra mejor si se realizan múltiples respaldos y se mantiene el 20% de espacio vacío para almacenar los respaldos hasta la próxima limpieza. El uso del espacio se ve afectado principalmente por el tamaño y compresión de datos y por el período de retención.

Un sistema Data Domain está diseñado como un sistema en línea muy confiable para realizar respaldos y archivar datos. A medida que se añaden nuevos respaldos al sistema, los respaldos antiguos vencen. Esta eliminación se realizan por lo general bajo el control de un software de respaldo o de archivado basado en el período de retención configurado.

Cuando el software de respaldo vence o elimina un respaldo antiguo de un sistema Data Domain, el espacio en el sistema Data Domain estará disponible solo luego de que el sistema Data Domain limpie los datos de los respaldos vencidos en el disco. Una buena manera de administrar el espacio en un sistema Data Domain es conservar la mayor cantidad de respaldos en línea conservando un poco de espacio vacío (alrededor del 20% del espacio total disponible) para alojar respaldos sin problemas hasta la próxima limpieza calendarizada, que se ejecuta predeterminadamente una vez a la semana.

Un segmento de la capacidad de almacenamiento es utilizado por los sistemas Data Domain para los índices internos y otros metadatos. El volumen de almacenamiento utilizado con el pasar del tiempo para los metadatos depende del tipo de datos almacenados y del tamaño de los archivos almacenados. Al contar con dos sistemas idénticos, un sistema puede, con el pasar del tiempo, reservar más espacio para metadatos y tener menos espacio para respaldos calendarizados que el otro, esto es posible si se envían diferentes conjuntos de datos a cada sistema.

La utilización del espacio en un sistema Data Domain se ve principalmente afectada por:

- El tamaño y la capacidad de compresión de los datos del respaldo.
- El período de retención especificado en el software de respaldo.

Los altos niveles de resultado de compresión al respaldarse conjuntos de datos con una gran cantidad de duplicados y reteniéndolos por prolongados períodos de tiempo.

Cómo el sistema de archivos informa sobre el uso del espacio

Todas las ventanas del DD System Manager y del sistema de comandos muestran la capacidad de almacenamiento utilizando cálculos en base 2. Por ejemplo, un comando que muestra que se utiliza 1 GiB de espacio en disco informa 2^{30} bytes = 1,073,741,824 bytes.

- 1 KiB = 2^{10} = 1,024 bytes
- 1 MiB = 2^{20} = 1,048,576 bytes
- 1 GiB = 2^{30} = 1,073,741,824 bytes
- 1 TiB = 2^{40} = 1,099,511,627,776 bytes

Cómo usa la compresión el sistema de archivos

El sistema de archivos utiliza la compresión para optimizar el espacio en disco disponible cuando almacena datos; de ese modo, el espacio en disco se calcula de dos maneras: física y lógica. (Consulte la sección sobre los tipos de compresión). El espacio físico es el espacio en disco que se utiliza en el sistema Data Domain. El espacio lógico es el volumen de datos no comprimidos escritos en el sistema.

Las herramientas de creación de informes de espacio del sistema de archivos (gráficos del DD System Manager y el comando `filesys show space` o el alias `df`) muestran tanto el espacio físico como el lógico. Estas herramientas también informan el tamaño y el volumen de espacio utilizado y disponible.

Cuando se monta un sistema de Data Domain, se pueden utilizar las herramientas más comunes para mostrar el uso físico del espacio en un sistema de archivos.

El sistema Data Domain genera mensajes de advertencia a medida que el sistema de archivos se acerca al 90 %, al 95 % y al 100 % de su capacidad. La información a continuación acerca de la compresión de datos brinda pautas para el uso del disco con el paso del tiempo.

El volumen de espacio en el disco que se utilizó con el paso del tiempo por un sistema Data Domain depende de:

- El tamaño del primer respaldo completo.
- El número de respaldos adicionales (incrementales y completos) conservados con el paso del tiempo.
- La tasa de crecimiento del conjunto de datos del respaldo.
- La tasa de cambios de los datos.

Para conjuntos de datos con las tasas típicas de cambio y crecimiento, la compresión de datos por lo general coincide con las siguientes pautas:

- En el primer respaldo completo a un sistema Data Domain, el factor de compresión es generalmente 3:1.
- Cada respaldo incremental para el respaldo inicial completo tiene un factor de compresión que por lo general se encuentran en un rango de 6:1.
- El próximo respaldo completo tiene un factor de compresión de aproximadamente 60:1.

Con el paso del tiempo, mediante una programación semanal de respaldos completos y una diaria de respaldos incrementales, el factor de compresión agregada de todos los datos será de aproximadamente 20:1. El factor de compresión es menor para los datos únicamente incrementales o para los respaldos con menos datos duplicados. La compresión es mayor cuando todos los respaldos son del tipo completo.

Tipos de compresión

Data Domain comprime datos en dos niveles: global y local. La compresión global compara los datos recibidos con los datos ya almacenados en los discos. Los datos duplicados no necesitan ser almacenados de nuevo, mientras que los datos nuevos son comprimidos localmente antes de ser escritos en el disco.

Compresión local

Un sistema Data Domain utiliza un algoritmo de compresión local desarrollado específicamente para maximizar el rendimiento mientras los datos son escritos en el disco. El algoritmo predeterminado (lz) permite que las ventanas de respaldo sean más cortas para trabajos de respaldo, pero utiliza más espacio. Otros dos tipos de compresión local están disponibles: gzfast y gz. Ambos ofrecen una mayor compresión

mediante lz, pero al costo de la carga de CPU adicional. Las opciones de compresión locales son una desventaja con respecto al rendimiento (más lento) y el uso del espacio. También es posible desactivar la compresión local. Para cambiar la compresión, consulte Cambio de la compresión local en la página 228.

Después de cambiar la compresión, todas las nuevas escrituras utilizarán el nuevo tipo de compresión. Los datos existentes serán convertidos al nuevo tipo de compresión durante la limpieza. Volver a comprimir todos los datos existentes previos al cambio de compresión puede demorar varias rondas de limpieza.

La limpieza inicial posterior al cambio de compresión puede demorar más de lo acostumbrado. Cada vez que cambie el tipo de compresión, debe monitorear cuidadosamente el sistema por una o dos semanas para verificar que funcione correctamente.

Cómo el sistema de archivos implementa la integridad de los datos

Múltiples capas de verificación de datos se ejecutan por el sistema de archivos DD OS en los datos recibidos desde las aplicaciones de respaldo para garantizar que los datos se escriban a los discos del sistema Data Domain en forma correcta. Esto asegura que los datos se pueden recuperar sin errores.

El DD OS fue especialmente diseñado para la protección de datos y está diseñado arquitectónicamente para evitar la invulnerabilidad de datos. Hay cuatro puntos críticos, los mismos se describen en las siguientes secciones.

Verificación de punto a punto

La comprobación de punto a punto protege todos los datos y metadatos del sistema de archivos. Ya que los datos ingresan en el sistema, una importante suma de verificación es calculada. Los datos se deduplican y son almacenados en el sistema de archivos. Después de que todos los datos son vaciados en el disco, los lee de nuevo, y vuelve a realizar la suma de comprobación. Las sumas de comprobación se comparan para verificar que tanto los datos como los metadatos del sistema de archivos sean almacenan en forma correcta.

Evitar y contener fallas

Data Domain utiliza un sistema de archivos de estructura de registro que nunca se sobrescribe o actualiza datos existentes. Los datos nuevos son siempre escritos en contenedores nuevos y se adjuntan a los contenedores antiguos existentes. Las referencias y los contenedores antiguos permanecen en su lugar y están seguros, incluso, de errores de software o hardware que puedan producirse durante el almacenamiento de los respaldos nuevos.

Detección de fallas y reparación continuas

La funcionalidad de detección y reparación continuas de fallas brinda protección contra fallas del sistema de almacenamiento. El sistema vuelve a comprobar periódicamente la integridad de las fracciones RAID, y utiliza la redundancia del sistema RAID para solucionar cualquier falla que se produzca. Durante una lectura, se vuelve a verificar la integridad de los datos y se repara cualquier error de manera inmediata.

Capacidad de recuperación del sistema de archivos

Los datos se escriben en un formato autodescriptivo. Si es necesario, se puede volver a crear el sistema de archivos mediante el análisis del log y la reconstrucción a partir de los metadatos almacenados con los datos.

Cómo el sistema de archivos recupera el espacio de almacenamiento mediante la limpieza del sistema de archivos

Cuando una aplicación de respaldo (como NetBackup o NetWorker) determina el vencimiento de datos, el sistema Data Domain marca estos datos para su eliminación. De todas formas, los datos no se eliminan de inmediato, lo hacen durante una operación de limpieza.

- Durante la operación de limpieza, el sistema de archivos se encuentra disponible para todas las operaciones habituales, incluidas la creación de respaldos (escritura) y la restauración (lectura).
- Si bien la limpieza consume un volumen significativo de recursos del sistema, este proceso cuenta con la capacidad de autorregularse y dejar libres los recursos del sistema en presencia de tráfico de usuario.
- Data Domain recomienda ejecutar una operación de limpieza después del primer respaldo completo de un sistema Data Domain. La compresión local inicial en un respaldo completo generalmente usa un factor de 1.5 a 2.5. Una operación de limpieza inmediata aporta una compresión adicional con un factor de 1.15 a 1.2 y permite recuperar el espacio en disco correspondiente.
- Una vez finalizada a la operación de limpieza, se envía un mensaje al registro del sistema con el porcentaje de espacio de almacenamiento que fue recuperado.

Un calendario predeterminado ejecuta la operación de limpieza todos los martes a las 6 am (tue 0600). Puede modificar el calendario puede ejecutar la operación de forma manual (consulte la sección sobre la modificación de un calendario de limpieza).

Data Domain recomienda ejecutar la operación de limpieza una vez por semana.

Cualquier operación que deshabilite el sistema de archivos o apague un sistema Data Domain durante una operación de limpieza (tal como un sistema de apagado o reinicio) anula la operación de limpieza. La operación de limpieza no se reinicia en forma inmediata tras el reinicio del sistema. Puede reiniciar la operación de limpieza manualmente o esperar hasta la próxima operación de limpieza programada.

Con la replicación de recopilaciones, no se pueden procesar datos que no se hayan replicado para la limpieza del sistema de archivos en un contexto de replicación en el sistema de origen. Si la limpieza del sistema de archivos no puede completarse debido a que los sistemas de origen y destino no están sincronizados, el sistema informa el estado de la operación de limpieza como `partial` y solo las estadísticas limitadas del sistema están disponibles para la operación de limpieza. Si la replicación de recopilaciones está deshabilitada, la cantidad de datos que no se pueden procesar para la limpieza del sistema de archivos aumenta porque la fuente de replicación y los sistemas de destino sigue sin estar sincronizados. El artículo de la base de conocimientos *Data Domain: An overview of Data Domain File System (DDFS) clean/ garbage collection (GC) phases*, disponible en el sitio de soporte en línea en https:// support.emc.com, proporciona más información.

Con la replicación del MTree, si se crea y elimina un archivo durante la replicación de una instantánea, la instantánea siguiente no tendrá ninguna información sobre este archivo, y el sistema no replicará ningún contenido asociado con este archivo. La replicación de un directorio replicará tanto la creación como la eliminación, incluso aunque ocurran en un breve lapso.

Con el registro de replicación que utiliza la replicación de directorios, se permite que las operaciones tales como la eliminación, el cambio de nombre, y otras, se ejecuten como un solo flujo. Esto puede reducir el rendimiento de la replicación. El uso de instantáneas mediante la replicación del MTree evita este problema.

Interfaces compatibles

Interfaces compatibles con el sistema de archivos.

- NFS
- CIFS
- DD Boost
- DD VTL

Software de respaldo compatible

La guía para configurar el software y los servidores de respaldo en un sistema de Data Domain se encuentra disponible en support.emc.com.

Flujos de datos enviados a un sistema Data Domain

Para lograr un rendimiento óptimo, Data Domain recomienda límites en los flujos simultáneos entre sistemas Data Domain y sus servidores de respaldo.

Un flujo de datos, en el contexto de la siguiente tabla, hace referencia a un flujo de bytes grande asociado con el acceso secuencial a archivos, como un flujo de escritura en un archivo de respaldo o un flujo de lectura de una imagen de restauración. Un flujo de origen o destino de replicación hace referencia a una operación de replicación de directorios o a un flujo de replicación de archivos de DD Boost asociado con una operación de replicación de archivos.

Tabla 89 Flujos de datos enviados a un sistema Data Domain

Modelo	RAM/ NVRAM	Flujos de escritura de respaldo	Flujos de lectura de respaldo	Flujos de origen de replicación [a]	Flujos de destino[a] de replicación	Mixto
DD140, DD160, DD610	4 GB o 6 GB/0.5 GB	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20
DD620, DD630, DD640	8 GB/0.5 GB o 1 GB	20	16	20	20	w<=20; r<=16; ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; Total<=30
DD640, DD670	16 GB o 20 GB/1 GB	90	30	60	90	w<=90; r<=30; ReplSrc<=60; ReplDest<=90; ReplDest+w<=90; Total<=90
DD670, DD860	36 GB/1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90

Tabla 89 Flujos de datos enviados a un sistema Data Domain (continuación)

Modelo	RAM/ NVRAM	Flujos de escritura de respaldo	Flujos de lectura de respaldo	Flujos de origen de replicación [a]	Flujos de destino[a] de replicación	Mixto
DD860	72 GB[b] / 1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD890	96 GB/2 GB	180	50	90	180	w<=180; r<=50; ReplSrc <=90;ReplDest<=180; ReplDest +w<=180; Total<=180
DD990	128 o 256 GB[b] / 4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD2200	8 GB	20	16	16	20	w<=20; r<=16; ReplSrc<=16; ReplDest<=20; ReplDest+w<=20; Total<=20
DD2200	16 GB	60	16	30	60	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest+w<=60; Total<=60
DD2500	32 o 64 GB/2 GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD4200	128 GB[b] / 4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD4500	192 GB[b] / 4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD7200	128 o 256 GB[b] / 4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD9500	256/512 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest+w<=1080; Total<=1885
DD9800	256/768 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest+w<=1080; Total<=1885
DD6300	De 48 a 96 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD6800	192 GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest +w<=400; Total<=400

Tabla 89 Flujos de datos enviados a un sistema Data Domain (continuación)

Modelo	RAM/ NVRAM	Flujos de escritura de respaldo	Flujos de lectura de respaldo	Flujos de origen de replicación [a]	Flujos de destino[a] de replicación	Mixto
DD9300	De 192 a 384 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest +w<=800; Total<=800
DD VE (8 TB)	8 GB / 512 MB	20	16	20	20	w<= 20 ; r<= 16 ReplSrc<=20; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=20;Total<=20
DD VE (16 TB)	16 GB / 512 MB o 24 GB / 1 GB	45	30	45	45	w<= 45 ; r<= 30 ReplSrc<=45; ReplDest<=45; ReplDest+w<=45; w+r+ReplSrc <=45;Total<=45
DD VE (32 TB)	24 GB/1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE (48 TB)	36 GB/1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE (64 TB)	48 GB/1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE (96 TB)	64 GB/2 GB	180	50	90	180	w<= 180 ; r<= 50 ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; w+r+ReplSrc <=180;Total<=180
DD3300 (4 TB)	12 GB (memoria virtual) / 512 MB	20	16	30	20	w<= 20 ; r<= 16 ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=30;Total<=30
DD3300 (8 TB)	32 GB (memoria virtual) / 1536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 (16 TB)	32 GB (memoria virtual) / 1536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 (32 TB)	46 GB (memoria virtual) / 1536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=140

a. DirRepl, OptDup, MTreeRepl
b. La opción de software Data Domain Extended Retention está disponible solo para estos dispositivos con memoria extendida (máxima)

Limitaciones del sistema de archivos

Limitaciones del sistema de archivos, que incluyen: límites de la cantidad de archivos, la batería, etc.

Límites en el número de archivos en un sistema Data Domain

Las consecuencias y consideraciones para el almacenamiento de más de mil millones de archivos.

Data Domain recomienda no almacenar más de mil millones de archivos en un sistema. El almacenamiento de un número mayor de archivos pueden afectar en forma negativa tanto el rendimiento como el tiempo de duración de la limpieza, al igual que algunos procesos, como la limpieza del sistema de archivos, pueden ejecutarse por un tiempo más extenso de haber una gran cantidad de archivos. Por ejemplo, la fase de enumeración de limpieza puede tardar desde unos pocos minutos a varias horas según la cantidad de archivos en el sistema.

Nota

El rendimiento general del sistema Data Domain bajará a niveles inaceptables si el sistema debe ejecutarse en compatibilidad con el volumen máximo de archivos y la carga de trabajo de las máquinas cliente no se encuentra controlada en forma cuidadosa.

Cuando el sistema de archivos pasa el límite de mil millones de archivos, varios procesos u operaciones podrían verse afectadas en forma negativa, por ejemplo:

- La limpieza puede demorar mucho tiempo en completarse, varios días quizás.
- Las operaciones AutoSupport pueden demorar más tiempo.
- Cualquier proceso o comando que necesite enumerar todos los archivos.

Si hay muchos archivos pequeños, debe considerar lo siguiente:

- La cantidad de archivos separados que pueden crearse por segundo, (incluso si los archivos son muy pequeños) puede ser una mayor limitación que la cantidad de MB/s que pueden moverse a un sistema Data Domain. Cuando los archivos son grandes, la tasa de creación de archivos no es significativa, pero cuando son pequeños, la tasa de creación de archivos gana relevancia y puede llegar a ser un factor desfavorable. La tasa de creación del archivo es de aproximadamente 100 a 200 archivos por segundo, según el número de MTrees y conexiones CIFS. Esta tasa debe tenerse en el dimensionamiento del sistema cuando un ambiente del cliente requiere una inclusión de gran volumen de una gran cantidad archivos.
- Las latencias de acceso a archivos resultan afectadas por la cantidad de archivos en un directorio. En la medida en que sea posible, recomendamos tamaños de directorio de menos de 250,000. Los directorios de tamaños más grandes experimentarán respuestas más lentas para las operaciones de metadatos como la enumeración de archivos en el directorio y la apertura o la creación de archivos.

Límites de la batería

Para los sistemas que utilizan NVRAM, el sistema operativo crea una alerta de batería baja en caso de que la carga de la batería baje del 80 % de su capacidad, y el sistema de archivos se desactiva.

AVISO

El sistema Data Domain DD2200 no utiliza NVRAM para que los cálculos de firmware decidan si la carga de la batería es suficiente para guardar los datos y desactivar el sistema de archivos en caso de una pérdida de alimentación de CA.

Cantidad máxima de inodos compatibles

Una solicitud NFS o CIFS de cliente provoca que un sistema Data Domain informe una capacidad de alrededor de dos mil millones de inodos (archivos y directorios). Un sistema Data Domain puede superar ese volumen, pero la creación de informes en el cliente puede ser incorrecta.

Longitud máxima del nombre de ruta

La longitud máxima de un nombre de ruta de acceso completa (que incluye los caracteres en `/data/col1/backup`) es de 61 caracteres. La longitud máxima de un vínculo simbólico también es de 61 caracteres.

Acceso limitado durante el failover de alta disponibilidad

El acceso a archivos puede interrumpirse por hasta 10 minutos durante el failover en los sistemas de alta disponibilidad. (DD Boost y NFS requieren tiempo adicional).

Monitoreo del uso del sistema de archivos

Vea las estadísticas del almacenamiento de datos en tiempo real.

La vista File System tiene pestañas y controles que proporcionan acceso a estadísticas de almacenamiento de datos en tiempo real, información de la unidad de nube, información de cifrado y gráficos de volúmenes de uso de espacio, factores de consumo y tendencias de datos escritos. También hay controles para administrar la limpieza, la expansión, la copia y la destrucción del sistema de archivos.

Acceso a la vista del sistema de archivos.

En esta sección se describe la funcionalidad del sistema de archivos.

Procedimiento

- Seleccione **Data Management** > **File System**.

Acerca del panel File System Status

Muestra el estado de los servicios del sistema de archivos.

Para acceder al panel File System Status, haga clic en **File System Status** > **File System** > **Show Status of File System Services**.

Sistema de archivos
El campo **File System** contiene un vínculo **Enable/Disable** y muestra el estado de funcionamiento del sistema de archivos:

- Enabled and running: la última longitud de tiempo consecutiva que el sistema de archivos fue habilitado y ejecutado.
- Disabled and shutdown.
- Enabling and disabling: en proceso de activarse o desactivarse.

- Destroyed: si se elimina el sistema de archivos.
- Error: si hay una condición de error, tal como un problema al inicializar el sistema de archivos

Cloud File Recall
El campo **Cloud File Recall** contiene un vínculo **Recall** para iniciar una recuperación de archivos desde el nivel de nube. Un vínculo **Details** está disponible si hay recuperaciones activas en curso. Para obtener más información, consulte el tema "Recuperación de un archivo desde el nivel de nube".

Medición de la capacidad física
El campo **Physical Capacity Measurement** contiene el botón **Enable** cuando el estado de medición de la capacidad física está deshabilitado. Cuando está habilitado, el sistema muestra los botones **Disable** y **View**. Haga clic en **View** para ver las mediciones de capacidad física en ejecución actualmente: MTree, prioridad, hora de envío, hora de inicio y duración.

Transferencia de datos
El campo **Data Movement** contiene los botones **Start/Stop** y muestra la fecha de la última operación de transferencia de datos finalizada, la cantidad de archivos copiados y la cantidad de datos copiados. El sistema muestra el botón **Start** cuando la operación de transferencia de datos está disponible y el botón **Stop** cuando se está ejecutando una operación de transferencia de datos.

Limpieza de nivel activo
El campo **Active Tier Cleaning** contiene un botón **Start/Stop** y muestra la fecha en que se ejecutó la última operación de limpieza o el estado de limpieza actual si la operación de limpieza está en curso. Por ejemplo:

```
Cleaning finished at 2009/01/13 06:00:43
```

o, si el sistema de archivos está deshabilitado, muestra:

```
No disponible
```

Limpieza de nivel de nube
El campo **Cloud Tier Cleaning** contiene un botón **Start/Stop** y muestra la fecha en que se ejecutó la última operación de limpieza o el estado de limpieza actual si la operación de limpieza está en curso. Por ejemplo:

```
Cleaning finished at 2009/01/13 06:00:43
```

o, si el sistema de archivos está deshabilitado, muestra:

```
No disponible
```

Acerca de la pestaña Summary

Haga clic en la pestaña Summary para mostrar estadísticas de uso de espacio de niveles activos y de nube, y para acceder a los controles de visualización del estado del sistema de archivos, la configuración del sistema de archivos, la ejecución de una operación de copia rápida, la expansión de la capacidad y la destrucción del sistema de archivos.

Para cada nivel, las estadísticas de uso de espacio incluyen lo siguiente:

- **Size**: La cantidad total de espacio del disco físico disponible para los datos.
- **Used**: El espacio físico utilizado para los datos comprimidos en ese momento. Los mensajes de advertencia son enviados al registro del sistema y se generará un

correo electrónico de alerta cuando el uso alcance el 90%, 95% y 100%. De alcanzar el 100%, el sistema Data Domain no aceptará más datos de los servidores de respaldo.
Si la cantidad utilizada es siempre alta, verifique el calendario de limpieza para consultar la frecuencia en la que se ejecuta la operación de limpieza en forma automática. Luego utilice el procedimiento de modificación del calendario de limpieza para ejecutar la operación con más frecuencia. También considere reducir el período de retención de datos o dividir una porción de los datos de respaldo a otro sistema Data Domain.

- **Available** (GiB): La cantidad total de espacio disponible para el almacenamiento de datos. Esta cifra puede cambiar ya que un índice interno puede expandirse a medida que el sistema Data Domain se rellena de datos. La expansión del índice toma el espacio del volumen disponible de Available (GiB).
- **Pre-Compression** (GiB): Los datos por escrito antes de la compresión.
- **Total Compression Factor (Reduction %)**: Antes o después de la compresión.
- **Cleanable** (GiB): La cantidad de espacio que podría ser recuperada si se ejecutara una limpieza.

Para el nivel de nube, el campo **Cloud File Recall** contiene un vínculo **Recall** para iniciar una recuperación de archivos desde el nivel de nube. Un vínculo **Details** está disponible si hay recuperaciones activas en curso. Para obtener más información, consulte el tema "Recuperación de un archivo desde el nivel de nube".

Los paneles separados proporcionan las siguientes estadísticas de las últimas 24 horas para cada nivel:

- **Pre-Compression** (GiB): los datos escritos antes de la compresión.
- **Post-Compression** (GiB): almacenamiento usado después de la compresión.
- **Global Compression Factor**: (antes de la compresión / (el tamaño después de la compresión global).
- **Local Compression Factor**: (el tamaño después de la compresión global) / después de la compresión).
- **Total Compression Factor (Reduction %)**: [(antes de la compresión - después de la comprensión) / antes de la compresión] * 100.

Acerca de los ajustes del sistema de archivos

Visualice y cambie tanto el sistema de opciones así como el calendario de limpieza en curso.

Para acceder al cuadro de diálogo File System Settings, haga clic en **Data Management** > **File System** > **Settings**.

Tabla 90 Ajustes generales

Ajustes generales	Descripción
Tipo de compresión local	El tipo de compresión local en uso. • Consulte la sección sobre tipos de compresión para una descripción general. • Consulte la sección sobre cómo cambiar la compresión local
Compresión local de nivel de nube	El tipo de compresión que se usa para el nivel de nube.

Tabla 90 Ajustes generales (continuación)

Ajustes generales	Descripción
	• Consulte la sección sobre tipos de compresión para una descripción general. • Consulte la sección sobre cómo cambiar la compresión local
Informar que la réplica puede escribirse	Cómo ven las aplicaciones a una réplica. • Consulte la sección sobre cómo cambiar la configuración de solo lectura.
Reserva de almacenamiento provisional	Administración de almacenamiento provisional • Consulte la sección sobre cómo trabajar con almacenamiento provisional en disco • Consulte la sección sobre la configuración de almacenamiento provisional en disco
Marker Type	Los marcadores del software de respaldo (puede utilizarse marcadores de cinta, encabezados de etiqueta, u otros nombres) en los flujos de datos. Consulte la sección relacionada con la configuración del marcador de cinta
Regular	Consulte la sección sobre la configuración de la regulación de la medición de la capacidad física.
Caché	Las inicialización de la memoria caché de capacidad física limpia las memorias caché y mejora la velocidad de medición.

Puede ajustar el balanceo de carga de trabajo del sistema de archivos para aumentar el rendimiento en función del uso.

Tabla 91 Ajustes de balanceo de carga de trabajo

Ajustes de balanceo de carga de trabajo	Descripción
Cargas de trabajo aleatorias (%)	Las restauraciones y el acceso instantáneos tienen un mejor rendimiento con cargas de trabajo aleatorias.
Cargas de trabajo secuenciales (%)	Las restauraciones y los respaldos tradicionales tienen un mejor rendimiento con cargas de trabajo secuenciales.

Tabla 92 Configuración de la transferencia de datos

Configuración de políticas de transferencia de datos	Descripción
Umbral de antigüedad de archivos	Cuando comienza la transferencia de datos, todos los archivos que no se han modificado para la cantidad de días del umbral especificado se transferirán del nivel activo al nivel de retención.
Calendario	Los datos se días y horas de transfieren.
Regular	El porcentaje de los recursos disponibles que el sistema usa para transferencia de datos. Un valor de aceleración del 100 %

Tabla 92 Configuración de la transferencia de datos (continuación)

Configuración de políticas de transferencia de datos	Descripción
	es la regulación predeterminada y significa que no se regula la transferencia de datos.

Tabla 93 Configuración de limpieza

Configuración del calendario de limpieza	Descripción
Hora	La fecha y hora en que se ejecutan las operaciones de limpieza. • Consulte la sección sobre la modificación de un calendario de limpieza
Regular	La asignación de recursos del sistema. • Consulte la sección sobre la regulación de la operación de limpieza

Acerca de la pestaña Cloud Units

Visualice información de resumen de las unidades de nube, agregue y modifique las unidades de nube, y administre certificados.

La pestaña Cloud Units en la página File System aparece solo cuando se habilita la licencia opcional de DD Cloud Tier. Esta vista muestra información de resumen (estado, ancho de banda de red, acceso de lectura, compresión local, transferencia y estado de datos), el nombre del proveedor de nube, la capacidad utilizada y la capacidad con licencia. Se proporcionan controles para la edición de la unidad de nube, la administración de certificados y la adición de una nueva unidad de nube.

Acerca de la pestaña Retention Units

Visualice la unidad de retención y su condición, su estado y su tamaño.

La pestaña Retention Units en la página File System aparece solo cuando se habilita la licencia opcional de DD Extended Retention. Esta vista enumera la unidad de retención y muestra su condición (nuevo, sellado u objetivo), su estado (deshabilitado o listo) y su tamaño. Si la unidad fue sellada, es decir, que no se pueden agregar más datos, podrá ver la fecha en que fue sellada.

Seleccione el símbolo de diamante ubicado la derecha del encabezado de una columna para ordenar los valores en sentido inverso.

Acerca de la pestaña DD Encryption

Visualice el estado de cifrado, su progreso, algoritmos, y más.

Tabla 94 Configuración de DD Encryption

Configuración	Descripción
Sistema DD	El estado puede ser uno de los siguientes:

Tabla 94 Configuración de DD Encryption (continuación)

Configuración	Descripción
	• Not licensed: ninguna proporciona ninguna otra información. • Not configured: el cifrado tiene licencia pero no está configurado. • Enabled: el cifrado está habilitado y ejecutándose. • Disabled: el cifrado está deshabilitado
Nivel activo	Visualice el estado de cifrado para el nivel activo: • Enabled: el cifrado está habilitado y ejecutándose. • Disabled: el cifrado está deshabilitado
Unidad de nube	Visualice el estado de cifrado por unidad de nube: • Enabled: el cifrado está habilitado y ejecutándose. • Disabled: el cifrado está deshabilitado
Progreso del cifrado	Visualice detalles del estado del cifrado para el nivel activo en cuanto a la aplicación de los cambios y de nuevo cifrado de datos. El estado puede ser uno de los siguientes: • Ninguno • Pending • Running • Done Haga clic en View Details para visualizar el cuadro de diálogo Encryption Status Details que incluye la siguiente información para el Nivel activo: • Type (ejemplo: Apply Changes una vez que el cifrado se haya iniciado o Re-encryption cuando el cifrado original sea resultado de datos que fueron comprometidos, posiblemente por una clave destruida anteriormente). • Status (ejemplo: Pending) • Detalles: (ejemplo: Solicitado en diciembre xx/xx/xx y se retomará después de la próxima limpieza del sistema).
Algoritmo de cifrado	El algoritmo utilizado para cifrar los datos: • AES de 256 bits (CBC) (predeterminado) • AES de 256 bits (GCM) (más seguro pero más lento) • AES de 128 bits (CBC) (no tan seguro como el de 256 bits) • AES de 128 bits (GCM) (no tan seguro como el de 256 bits) Consulte Modificación del algoritmo de cifrado para obtener más detalles.
Frase de contraseña de cifrado	Una vez configurado, se muestra como "*****." Para cambiar la frase de contraseña, consulte Administración de la frase de contraseña del sistema
Bloqueo del sistema de archivos	

Tabla 94 Configuración de DD Encryption (continuación)

Configuración	Descripción
Status	El estado del File System Lock puede ser: • Unlocked: la función no está habilitada. • Locked: la función está habilitada.
Administración de claves	
Administrador de claves	Ya sea el Administrador de claves incorporado de Data Domain interno o el Administrador de claves de Data Protection Manager (DPM) de RSA opcional. Haga clic en **Configure** para alternar entre los administradores de clave (si ambos están configurados), o para modificar las opciones del administrador de claves.
Servidor	El nombre del servidor del administrador de claves del RSA
Estado del servidor	En línea u offline, o los mensajes de error generados por el servidor del administrador de claves del RSA
Clase de clave	Un tipo especializado de clase de seguridad es utilizado por el Data Protection Manager (DPM) de RSA opcional, el mismo junta claves criptográficas en grupos con características similares. El sistema Data Domain recupera una clave desde el servidor RSA mediante la clase de clave. Una clase debe configurarse para que devuelva la clave en curso o para que cada vez genere una nueva clave. **Nota** El sistema Data Domain sólo admite clases de clave configurados para devolver la clave en curso.
Puerto	El número de puerto del servidor RSA.
Modo FIPS	Si el certificado de host importado es o no es compatible con FIPS. En modo predeterminado se encuentra activado.
Claves de cifrado	Enumera las clave de números de ID. Muestra la hora de creación de una clave, cuánto tiempo es válida, su tipo (DPM Key Manager de RSA o la clave interna de Data Domain), su estado (consulte Trabajar con el RSA DPM Key Manager, estados de claves de cifrado de DPM compatibles con Data Domain), y el volumen de datos cifrados con la clave. El sistema mostrará la última hora de actualización de información de la clave en la parte superior de la columna derecha. Las claves seleccionadas en la lista pueden estar: • Sincronizados para que la lista muestre las claves nuevas agregadas al servidor RSA (pero no se pueden utilizar hasta que el sistema de archivos sea reiniciado) • Eliminado. • Destruido.

Acerca de la vista del uso del espacio (sistema de archivos)

Se muestra una representación visual (pero estática) de uso de datos para el sistema de archivos en determinados momentos.

Haga clic en **Data Management** > **File System** > **Charts**. Seleccione **Space Usage** en la lista desplegable Chart.

Haga clic en un punto de una línea del gráfico para visualizar los datos de ese punto. Las líneas del gráfico indican las mediciones en los siguientes campos:

- Pre-comp Written: El volumen total de datos enviados al MTree por los servidores de respaldo. Los datos pre-comprimidos en un MTree es lo que un servidor de respaldo ve como la totalidad de datos sin comprimir almacenados en un MTree como unidad de almacenamiento, se muestra con el Espacio utilizado (a la izquierda) del eje vertical del gráfico.
- Post-comp Utilizado—El volumen total de almacenamiento en disco en uso en el MTree, se muestra con el Espacio utilizado (a la izquierda) del eje vertical del gráfico.
- Comp Factor—El volumen de la compresión ejecutada en el sistema Data Domain con los datos que recibió (relación de compresión), que se muestra con el Factor de compresión (a la derecha) en el eje vertical del gráfico.

Verificación de historial de uso de espacio
Si en el gráfico Space Usage se hace clic en un intervalo (1w, 1m, 3m, 1y, All) arriba de la línea del gráfico, se puede modificar la cantidad de días de datos que aparecen en el gráfico, de una semana a todo.

Acerca de la vista de consumo

Visualice el espacio que se utilizó con el paso del tiempo, en relación a la capacidad total del sistema.

Haga clic en **Data Management** > **File System** > **Charts**. En la lista desplegable Chart, seleccione **Consumption**.

Haga clic en un punto de una línea del gráfico para visualizar los datos de ese punto. Las líneas del gráfico indican las mediciones en los siguientes campos:

- Capacity: es el volumen total de almacenamiento en disco disponible para almacenar datos en el sistema Data Domain. El volumen se muestra con el eje vertical Space Used (izquierdo) del gráfico. Al hacer clic en la casilla de verificación Capacity alternará la visualización de esta línea.
- Post-comp Used: la cantidad total de almacenamiento en disco usado en el sistema Data Domain. Se muestra con el eje vertical Space Used (izquierdo) del gráfico.
- Comp Factor: es el grado de compresión que el sistema Data Domain aplicó a los datos que recibió (factor de compresión). Se muestra con el eje vertical Compression Factor (derecho) del gráfico.
- Cleaning: visualizará un diamante gris se muestra en el gráfico cada vez que se inicia una operación de limpieza de sistema de archivos.
- Data Movement: el volumen de espacio de disco que se movió al área de almacenamiento de archivado (si la licencia Archive está habilitada).

Verificación de uso del consumo histórico
Si en el gráfico Consumption se hace clic en un intervalo (1w, 1m, 3m, 1y, All) arriba de la línea del gráfico, se puede modificar la cantidad de días de datos que aparecen en el gráfico, de una semana a todo.

Acerca de la vista de escritura diaria (sistema de archivos)

Visualice el flujo de datos con el tiempo. Se muestra el volumen de datos a través del paso del tiempo, con los volúmenes previos y posteriores a la compresión.

Haga clic en **Data Management** > **File System** > **Charts**. Seleccione **Daily Written** en la lista desplegable Chart.

Haga clic en un punto de una línea del gráfico para visualizar un cuadro con los datos de ese punto. Las líneas del gráfico indican las mediciones en los siguientes campos:

- Pre-Comp Written: el volumen total de datos escritos en el sistema de archivos por los servidores de respaldo. Los datos precomprimidos en un sistema de archivos es lo que un servidor de respaldo ve como la totalidad de datos que el sistema de archivos almacena sin comprimir.
- Post-Comp Written: el volumen total de datos escritos en el sistema de archivos posterior a la ejecución de la compresión, en GiBs.
- Total Comp Factor: el volumen total de la compresión ejecutada en el sistema Data Domain con los datos que recibió (relación de compresión), que se muestra con el Total Compression Factor (a la derecha) en el eje vertical del gráfico.

Verificación del historial de los datos escritos
Si en el gráfico de Daily Written se hace clic en un intervalo (1w, 1m, 3m, 1y, All) arriba de la línea del gráfico, se puede modificar la cantidad de días de datos que aparecen en el gráfico, de una semana a todo.

Cuando el sistema de archivos esté lleno o casi lleno

Los sistemas Data Domain tienen tres niveles de capacidad completa progresivos. A medida que se alcanza cada nivel, se cancelan más operaciones en forma progresiva. En cada nivel, si se eliminan datos y luego se ejecuta una operación de limpieza de sistema de archivos se crea mayor disponibilidad en el espacio del disco.

Nota

El proceso de eliminación de archivos y borrado de snapshots no recupera el espacio de disco en forma inmediata, la siguiente operación de limpieza lo hace.

- Nivel 1: en el primer nivel de capacidad llena, no se pueden escribir más datos nuevos al sistema de archivos. Se genera una alerta informativa de poco espacio disponible.
  Solución: elimine datos innecesarios, reduzca el período de retención, elimine snapshots y ejecute una operación de limpieza del sistema de archivos.
- Nivel 2: en el segundo nivel de capacidad llena, los archivos no se pueden eliminar. Esto se debe a que la eliminación de archivos también requiere espacio libre, pero el sistema tiene tan poco espacio libre disponible que ni siquiera le es posible eliminar archivos.
  Solución: Expirar las snapshots y ejecutar una operación de limpieza del sistema de archivos.
- Nivel 3: en el tercer y último nivel de capacidad llena intentará hacer expirar las snapshots, eliminar archivos, o escribir nuevos fallos en datos
  Solución: ejecutar una operación de limpieza del sistema de archivos para liberar espacio suficiente para, al menos, eliminar algunos archivos o expirar algunas snapshots y luego volver a ejecutar la limpieza.

Monitorea el uso del espacio mediante alertas por correo electrónico

Se generan alertas cuando el sistema de archivos está lleno en un 90%, 95% y 100%. Para enviar estas alertas, agregue al usuario a la lista de correo electrónico de alerta.

Nota

Para unirse a la lista de correo electrónico de alerta, consulte Visualización y borrado de alertas.

Administración de las operaciones del sistema de archivos

En esta sección se describe la limpieza, el saneamiento, y la ejecución de operaciones básicas en el sistema de archivos.

Ejecución de operaciones básicas

Las operaciones básicas del sistema de archivos incluyen la activación y desactivación del sistema de archivos y, en raras ocasiones, la destrucción de un sistema de archivos.

Creación del sistema de archivos

Cree un sistema de archivos desde la página Data Management > File System usando la pestaña Summary.

Hay tres razones para crear un sistema de archivos:

- Para un nuevo sistema Data Domain.
- Cuando se inicia un sistema después de una instalación limpia.
- Luego de la destrucción de un sistema de archivos.

Para crear el sistema de archivos:

Procedimiento

1. Verifique que el almacenamiento se haya instalado y configurado (consulte la sección sobre la visualización de la información de almacenamiento del sistema para obtener más información) . Si el sistema no cumple con este requisito previo, aparecerá un mensaje de advertencia. Instale y configure el almacenamiento previo al intentar crear el sistema de archivos.
2. Seleccione **Data Management** > **File System** > **Summary** > **Create**.

   Se inicia el asistente de creación de sistema de archivos Siga las instrucciones proporcionadas.

Habilitación o deshabilitación del sistema de archivos

La opción para habilitar o deshabilitar el sistema de archivos depende del estado actual del archivo de sistema-si se encuentra habilitado, puede deshabilitarlo y viceversa.

- La habilitación del sistema de archivos permite que inicien las operaciones del sistema Data Domain. Esta capacidad se encuentra disponible sólo para usuarios administrativos.
- La deshabilitación del sistema de archivos detiene todas las operaciones del sistema Data Domain, incluyendo la limpieza. Esta capacidad se encuentra disponible sólo para usuarios administrativos.

⚠ PRECAUCIÓN

Deshabilitar el sistema de archivos cuando una aplicación de respaldo se encuentre enviando datos al sistema puede causar fallos en el proceso de respaldo. Algunas aplicaciones de software de respaldo son capaces de recuperarse al reiniciarlas en el mismo punto en que dejaron de ejecutarse y cuando sea capaz de reanudar la copia de archivos exitosamente; otras podrían fracasar, dejando al usuario con un respaldo incompleto.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Summary**.
2. Para **File System**, haga clic en **Enable** o en **Disable**.
3. Haga clic en **Close** en el cuadro de diálogo de confirmación.

Ampliación del sistema de archivos

Puede que tenga que ampliar el tamaño de un sistema de archivos si las sugerencias de "When the File System Is Full or Nearly Full" no liberan el espacio suficiente para ejecutar las operaciones habituales.

Sin embargo, puede que un sistema de archivos no pueda ampliarse por estas razones:

- El sistema de archivos no está habilitado.
- No hay discos o gabinetes sin utilizar en los niveles activo, de retención o de nube.
- Falta instalar una licencia de ampliación del almacenamiento.
- No hay suficientes licencias de capacidad instalada.

Los sistemas DD6300 admiten la opción de usar gabinetes ES30 con unidades de 4 TB (43.6 TiB) al 50 % de utilización (21.8 TiB) en el nivel activo si la capacidad con licencia disponible es exactamente 21.8 TiB. Las siguientes reglas se aplican al uso de bandejas de capacidad parcial.

- No se admite ningún otro tipo de gabinetes o tamaño de unidades para usar en capacidad parcial.
- Una bandeja parcial solo puede existir en el nivel activo.
- Solo un ES30 parcial puede existir en el nivel activo.
- Una vez que una bandeja parcial existe en un nivel, no se pueden configurar ES30 adicionales en ese nivel hasta que la bandeja parcial se agrega en toda su capacidad.

  Nota

  Esto requiere otorgar licencias para capacidad adicional suficiente para utilizar los 21.8 TiB restantes de la bandeja parcial.

- Si la capacidad disponible es mayor de 21.8 TB, no se puede agregar una bandeja parcial.
- La eliminación de una licencia de 21 TiB no convertirá automáticamente una bandeja utilizada por completo en una bandeja parcial. La bandeja debe quitarse y agregarse de nuevo como una bandeja parcial.

Para ampliar el sistema de archivos:

Procedimiento

1. Seleccione **Data Management** > **File System** > **Summary** > **Expand Capacity**.

Se inicia el asistente de expansión de la capacidad del sistema de archivos. La lista desplegable **Storage Tier** siempre contiene el nivel activo y puede contener el nivel de retención extendida o el nivel de nube como una opción secundaria. El asistente muestra la capacidad actual del sistema de archivos para cada nivel, así como la cantidad de espacio de almacenamiento adicional disponible para la ampliación.

Nota

La capacidad del sistema de archivos se puede ampliar solo si los discos físicos son instalados en el sistema y el sistema de archivos se encuentra habilitado.

2. Desde la lista desplegable **Storage Tier**, seleccione un nivel.
3. En el área **Addable Storage**, seleccione los dispositivos de almacenamiento que se utilizarán y haga clic en **Add to Tier**.
4. Siga las instrucciones del asistente. Cuando aparezca la página de confirmación, haga clic en **Close**.

Destrucción del sistema de archivos

La destrucción del sistema de archivos debe hacerse solo bajo la recomendación del Servicio al cliente. Esta acción elimina todos los datos del sistema de archivos, incluidas las cintas virtuales. Los datos eliminados podrán recuperarse. Esta operación también elimina los ajustes de configuración de replicación.

Esta operación se utiliza cuando sea necesario borrar los datos existentes, ya sea para crear un nuevo destino de replicación de colección, o para reemplazar el origen de una colección, o por razones de seguridad ya que el sistema puede estar siendo retirado para dejar de operar.

⚠ PRECAUCIÓN

La operación opcional Write zeros to disk escribe ceros en todos los discos del sistema de archivos, eliminando todos los rastros de datos eficazmente. Si el sistema Data Domain contiene un gran volumen de datos, esta operación puede demorar muchas horas, o un día, hasta completarse.

Nota

Ya que este es un procedimiento destructivo, esta operación está habilitada solo para usuarios administrativos.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Summary** > **Destroy**.
2. En el cuadro de diálogo Destroy File System, escriba la contraseña del administrador de sistemas (es la única contraseña que será aceptada).
3. Si lo desea, puede hacer clic en la casilla de verificación **Write zeros to disk** para eliminar los datos de forma completa.
4. Haga clic en **Aceptar**.

Ejecución de la limpieza

En esta sección, se proporciona información sobre la limpieza y se describe cómo iniciar, detener y modificar las programaciones de limpieza.

DD OS intenta mantener un contador denominado “Cleanable GiB” para el nivel activo. Este número es una estimación de cuánto espacio físico (después de la compresión)

podría recuperarse en el nivel activo mediante la ejecución de la limpieza/recolección de elementos no utilizados. Este contador se muestra con los comandos `filesys show space` y `df`.

```
Active Tier:
Resource Size GiB Used GiB Avail GiB Use% Cleanable GiB*
---------------- -------- --------- --------- ----
--------------
/data: pre-comp - 7259347.5 - - -
/data: post-comp 304690.8 251252.4 53438.5 82% 51616.1 <=== NOTE
/ddvar 29.5 12.5 15.6 44% -
---------------- -------- --------- --------- ----
--------------
```

Ejecute la limpieza del nivel activo si:

- El valor de “Cleanable GiB” es elevado
- DDFS está totalmente completo (y, por lo tanto, es de solo lectura)

Puede que la limpieza no recupere todo el espacio posible en una sola ejecución. En los sistemas Data Domain que contienen conjuntos de datos muy grandes, la limpieza funciona en la parte del sistema de archivos que contiene los datos más superfluos y es posible que deba ejecutarse varias veces antes de recuperar todo el espacio posible.

Inicio de la limpieza

Para iniciar en forma inmediata una operación de limpieza.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Summary** > **Settings** > **Cleaning**.

   La pestaña **Cleaning** del cuadro de diálogo **File System Setting** muestra los ajustes de configuración de cada nivel.

2. Para el nivel activo:

   a. En el cuadro de texto Throttle %, escriba un volumen para la regulación del sistema. Este es el porcentaje de uso de CPU dedicada a la limpieza. El valor predeterminado es 50 por ciento.

   b. En la lista desplegable Frequency, seleccione una de estas frecuencias: Never, Daily, Weekly, Biweekly y Monthly. El valor predeterminado es Weekly.

   c. Para At, configure una hora específica.

   d. Para On, seleccione un día de la semana.

3. Para el nivel de nube:

   a. En el cuadro de texto Throttle %, escriba un volumen para la regulación del sistema. Este es el porcentaje de uso de CPU dedicada a la limpieza. El valor predeterminado es 50 por ciento.

   b. En la lista desplegable Frequency, seleccione una de estas frecuencias: Never, After every 'N' Active Tier cleans.

Nota

Si una unidad de nube no está accesible cuando se ejecuta la limpieza de nivel de nube, se omite la unidad de nube en esa ejecución. La limpieza en esa unidad de nube se produce en la siguiente ejecución si la unidad de nube está disponible. La programación de limpieza determina la duración entre dos ejecuciones. Si la unidad de nube está disponible y usted no puede esperar a la siguiente ejecución programada, puede iniciar la limpieza manualmente.

4. Haga clic en **Save**.

Nota

Para iniciar la operación de limpieza mediante la CLI, utilice el comando `filesys clean start`.

```
# filesys clean start
Cleaning started. Use 'filesys clean watch' to monitor progress.
```

Para confirmar que la limpieza esté en curso, utilice el comando `filesys status`.

```
# filesys status
The filesystem is enabled and running.
Cleaning started at 2017/05/19 18:05:58: phase 1 of 12 (pre-merge)
50.6% complete, 64942 GiB free; time: phase 0:01:05, total 0:01:05
```

Si la limpieza ya está en ejecución, se muestra el siguiente mensaje cuando se intenta iniciar.

```
**** Cleaning already in progress. Use 'filesys clean watch' to monitor
progress.
```

Nota

Si la limpieza no se puede iniciar, póngase en contacto con el proveedor de soporte contratado para obtener más ayuda. Este problema puede indicar que el sistema ha encontrado un `error de segmento faltante`, que causa que la limpieza se deshabilite.

Programar o interrumpir la limpieza

Para interrumpir o programar en forma inmediata una operación de limpieza.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Summary** > **Settings** > **Cleaning**.

   La pestaña Cleaning del cuadro de diálogo File System Setting muestra los ajustes de configuración de cada nivel.

2. Para el nivel activo:

   a. En la lista desplegable Frequency, seleccione la frecuencia deseada.

3. Para el nivel de nube:

   a. En la lista desplegable Frequency, seleccione la frecuencia deseada.

4. Haga clic en **Save**.

Nota

El CLI se puede utilizar para comprobar que se haya establecido una programación de limpieza.

```
# filesys clean show schedule
```

Si es necesario, establezca una programación de limpieza de nivel activo. El siguiente ejemplo establece que la limpieza se ejecute todos los martes a las 6 h:

```
# filesys clean set schedule Tue 0600
Filesystem cleaning is scheduled to run "Tue" at "0600".
```

En los sistemas configurados con retención extendida (ER), es posible que se establezca que la limpieza se ejecute después de completar el movimiento de datos y que no tenga una programación separada.

Ejecutar saneamiento

Para cumplir con las normas gubernamentales, el saneamiento del sistema, también conocida como la trituración de datos, debe ejecutarse cuando se escribe información clasificada o confidencial en cualquier sistema que no se encuentre aprobado para almacenar tales datos.

Cuando se produce un incidente, el administrador del sistema debe tomar medidas inmediatas para erradicar la totalidad de los datos escritos por error. El objetivo es restablecer, de forma eficaz, el dispositivo de almacenamiento a un estado como si el evento nunca hubiera ocurrido. Si la filtración de datos ocurrió con datos confidenciales, la totalidad del almacenamiento deberá sanearse con la práctica de eliminación de datos confidenciales de Data Domain Professional Services.

El comando de saneamiento de Data Domain existe para que el administrador pueda borrar archivos a nivel lógico, ya sea de un respaldo establecido o de archivos individuales. La eliminación de un archivo en la mayoría de los sistemas de archivos consiste en simplemente marcar el archivo o en eliminar las referencias a los datos en el disco, liberando el espacio físico que será utilizado más adelante. De todas formas, esta sencilla acción introduce el problema de poder dejar una representación residual de datos subyacente en los discos en forma física. Los ambientes de almacenamiento deduplicados no son inmunes a este problema.

La trituración de datos en un sistema implica que se elimine la representación residual de los datos y por lo tanto la posibilidad de que el archivo pueda ser accesible luego de ser triturado. El enfoque de saneamiento de Data Domain asegura que cumple con las siguientes especificaciones de las versiones de 2007 de la norma 5220.22 del Departamento de Defensa (DoD):

- *Departamento de Defensa de EE.UU. 5220.22-M Matriz de saneamiento y borrado*
- *Instituto Nacional de Sistemas y Tecnología (NIST) Publicación Especial 800-88 Guía esencial para saneamiento de medios*

Desinfección de datos deduplicados

Los sistemas Data Domain desinfectan los datos presentes, en su estado deduplicado original.

Los sistemas de almacenamiento con deduplicación extraen patrones comunes de datos de los archivos enviados al sistema y almacena solo copias únicas de estos patrones, haciendo referencia a todas las instancias redundantes. Debido a que estos patrones o segmentos de datos pueden potencialmente compartirse entre muchos archivos en el sistema, el proceso de desinfección debe primero determinar si cada uno de los segmentos del archivo contaminado se encuentran compartidos junto con

un archivo limpio y luego borrar solo aquellos segmentos que no son compartidos, junto con cualquier metadato contaminado.

Todos los niveles de almacenamiento, cachés, capacidad no utilizada y espacio libre son borrados para erradicar todas las copias de cada segmento que pertenece en forma exclusiva a los archivos borrados. El sistema recupera y sobrescribe todo el almacenamiento ocupado por estos segmentos para restaurar en forma eficaz el dispositivo de almacenamiento a un estado que refleje que los archivos contaminados nunca existieron en ese sistema.

Nivel 1 de saneamiento: o destrucción de datos

Si los datos que necesita eliminar no están clasificados, como se define en la "Matriz de saneamiento y limpieza 5220.22-M del Departamento de Defensa de los Estados Unidos", el saneamiento de nivel 1 se puede usar para sobrescribir el almacenamiento afectado una vez. Esto proporciona la base para la administración de la mayoría de los casos de destrucción de datos y saneamiento del sistema.

La función de saneamiento del sistema Data Domain garantiza que cada copia de cada segmento que corresponde solo a los archivos borrados se sobrescriban usando el mecanismo de puesta en cero de un único paso. Los datos limpios en el sistema que se está limpiando están en línea y disponibles para los usuarios.

Procedimiento

1. Elimine los archivos o respaldos contaminados con el software de respaldo o el cliente correspondiente. En el caso de las copias de seguridad, asegúrese de administrar el software de respaldo de forma adecuada para garantizar que los archivos relacionados en la imagen se concilien, los registros de los catálogos se administren como se requiera, etc.
2. Ejecute el comando `system sanitize start` en el sistema Data Domain contaminado para que todo el espacio previamente utilizado en este se sobrescriba una vez (consulte la figura siguiente).
3. Espere a que el sistema afectado sea saneado. El saneamiento se puede monitorear usando el comando `system sanitize watch`.

   Si el sistema Data Domain afectado tiene la replicación habilitada, todos los sistemas que contienen réplicas deben procesarse de una manera similar. Según cuántos datos existan en el sistema y cómo están distribuidos, el comando `system sanitize` puede tardar bastante tiempo. Sin embargo, durante este tiempo, todos los datos limpios en el sistema están disponibles para los usuarios.

Nivel 2 de saneamiento: saneamiento del sistema completo

Si los datos que necesita eliminar están clasificados, como se define en la "Matriz de saneamiento y limpieza 5220.22-M del Departamento de Defensa de los Estados Unidos", se requiere el saneamiento de nivel 2, o el saneamiento total del sistema.

Data Domain recomienda a Blancco para la sobrescritura multipass con cualquier patrón de sobrescritura y un certificado. Esto proporciona la base para la administración de los requisitos universales del Departamento de Defensa donde se requiere el saneamiento del sistema. Para obtener más información, visite:

https://www.emc.com/auth/rcoll/servicekitdocument/cp_datadomaindataerase_psbasddde.pdf

Modificación de la configuración básica

Modifique el tipo de compresión utilizada, los tipos de marcadores, el estado de réplica de escritura, y el porcentaje de la reserva de almacenamiento provisional, tal como se describe en esta sección.

Cambio de la compresión local

Utilice la pestaña General del cuadro de diálogo File System Settings para configurar el tipo de compresión local.

Nota

No cambie el tipo de compresión local a menos que sea necesario.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Summary** > **Settings** > **General**.
2. En la lista desplegable Local Compression Type, seleccione el tipo de compresión.

Tabla 95 Tipo de compresión

Opción	Descripción
NONE	No comprima los datos.
LZ	El algoritmo predeterminado que da el mejor rendimiento Data Domain recomienda la opción lz.
GZFAST	Una compresión con técnicas de descompresión que usa menos espacio para los datos comprimidos, pero más ciclos de CPU (el doble que lz). Gzfast es la alternativa recomendada para los sitios que requieren más compresión al costo de un rendimiento más bajo.
GZ	Una compresión con técnicas de descompresión que usa la menor cantidad de espacio para el almacenamiento de datos (un 10 a 20 % menos que lz en promedio; sin embargo, algunos conjuntos de datos obtienen compresión más alta). También usa más ciclos de CPU (hasta cinco veces más que lz). El tipo de compresión gz se usa comúnmente para las aplicaciones de almacenamiento nearline en que los requisitos de rendimiento son bajos.

3. Haga clic en **Save**.

Cambio de la configuración de solo lectura

Cambie la réplica para que incluya capacidad de escritura. Algunas aplicaciones de respaldo deben ver la réplica con capacidad de escritura para realizar una operación de restauración o de vault desde esta.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Summary** > **Settings** > **General**.
2. En el área Report Replica as Writable, elija alternativamente **Disabled** o **Enabled** según corresponda.

3. Haga clic en **Save**.

Trabajar con almacenamiento provisional en disco

El almacenamiento provisional en disco permite que un sistema Data Domain pueda utilizarse como un dispositivo de almacenamiento provisional, donde el sistema es tomado como un disco básico a través de un recurso compartido de CIFS o punto de montaje de NFS.

El almacenamiento provisional en disco se puede utilizar en combinación con el software de respaldo, como NetWorker y NetBackup (NBU) de Symantec, que no requiere de una licencia y se encuentra deshabilitado de manera predeterminada.

Nota

La función DD VTL no es necesaria ni se admite cuando el sistema Data Domain se utiliza como un dispositivo de almacenamiento provisional en disco.

La razón por la que algunas aplicaciones de respaldo utilizan dispositivos de almacenamiento provisional en disco es para permitir que las unidades de cinta puedan transmitir en forma continua. Luego de que los datos se copien a la cinta, serán almacenados en el disco hasta que el espacio deje de estar disponible. En caso de necesitar la restauración de algún dato almacenado en un respaldo reciente, es muy probable que el mismo continúe almacenado en el disco y puede resultar conveniente restaurarlo del disco mismo antes que de la unidad de cinta. Cuando el disco se llene, pueden eliminase los respaldos antiguos para hacer espacio. Esta política de delete-on-demand maximiza el uso del disco.

En funcionamiento normal, el sistema Data Domain no recupera el espacio de los archivos borrados hasta que se realice una operación de limpieza. Esto no es compatible con el software de respaldo que opera en un modo de almacenamiento provisional, el cual aguarda a que el espacio se utilice nuevamente cuando se eliminen los archivos . Al configurar el almacenamiento provisional en disco, está reservando un porcentaje del total de espacio (por lo general, del 20 al 30 por ciento) para permitir que el sistema simule la liberación inmediata del espacio.

El volumen de espacio disponible se reducirá al volumen de la reserva para el almacenamiento intermedio. Cuando el volumen de datos almacenado utiliza todo el espacio disponible, el sistema se encontrará lleno. De todas formas, cada vez que se elimina un archivo, el sistema calcula el volumen de espacio que será recuperado por la limpieza y toma prestado ese mismo volumen de la reserva de almacenamiento provisional para incrementar el espacio disponible. Cuando se ejecuta una operación de limpieza, el espacio se recupera y la reserva se restaura a su tamaño inicial. Dado que el volumen del nuevo espacio disponible se genera con la eliminación de archivos es solo una estimación, el espacio real a disponer por la limpieza puede no coincidir con el estimado. El objetivo de almacenamiento provisional en disco es configurar suficiente reserva para evitar quedarse sin espacio antes de que se ejecute la operación de limpieza programada.

Configuración de almacenamiento provisional del disco

Active el almacenamiento provisional del disco y especifique el porcentaje de reserva para el mismo.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Summary** > **Settings** > **General**.
2. En el área de Staging Reserve, elija alternativamente **Disabled** o **Enabled** según corresponda.

3. Si Staging Reserve está activada, ingrese un valor en el cuadro % of Total Space.

   Este valor representa el porcentaje del espacio total del disco que se va reservar para el almacenamiento provisional del disco (por lo general, entre el 20 % y el 30 %).

4. Haga clic en **Save**.

Configuración del marcador de cinta

El software de respaldo de algunos proveedores inserta marcadores (marcadores de cintas, encabezados de etiquetas u otros nombres) en todos los flujos de datos (respaldos de DD VTL y de sistemas de archivos) enviados a un sistema Data Domain.

Los marcadores pueden degradar significativamente la compresión de datos en un sistema Data Domain. De esta forma, se configura como automático el tipo de marcador predeterminado y no puede ser modificado por el usuario. Si esta configuración no es compatible con el software de respaldo, póngase en contacto con su proveedor de servicios de soporte contratado.

Nota

Para obtener información acerca de cómo las aplicaciones funcionan en un ambiente de Data Domain, consulte *Cómo los sistemas EMC Data Domain se integran en el ambiente de almacenamiento*. Puede usar estas matrices y guías de integración para resolver problemas relacionados con proveedores.

Uso compartido de cargas de trabajo aleatorias de discos SSD

El valor del umbral en el que se establece el máximo de I/O aleatorias en el sistema Data Domain se puede ajustar desde el valor predeterminado para dar cabida a los requisitos cambiantes y los patrones de I/O.

De forma predeterminada, el sistema Data Domain establece el uso compartido de cargas de trabajo aleatorias de discos SSD en 40 %. Este valor se puede ajustar hacia arriba o hacia abajo según sea necesario. Seleccione **Data Management** > **File System** > **Summary** > **Settings** > **Workload Balance** y ajuste el control deslizante.

Haga clic en **Save**.

Operaciones de copia rápida

Una operación de copia rápida copia archivos y árboles de directorios de un directorio de origen a uno de destino en un sistema Data Domain.

La opción `force` permite sobrescribir el directorio de destino, si existe. Al ejecutar la operación de copia rápida, se muestra el cuadro de diálogo de estado del progreso.

Nota

La operación de copia rápida hace que un destino sea igual al origen, pero no en un punto específico en el tiempo. No hay garantías de que ambos sean o hayan sido alguna vez iguales si cambia la carpeta durante la operación.

Ejecución de una operación de copia rápida

Copie un archivo o un árbol de directorios desde un directorio de origen del sistema Data Domain a otro destino en el sistema Data Domain

Procedimiento

1. Seleccione **Data Management** > **File System** > **Summary** > **Fast Copy**.

   Se mostrará el cuadro de diálogo Fast Copy.

2. En el cuadro de texto Source escriba el nombre de la ruta del directorio donde se guardan los datos de las copias. Por ejemplo, `/data/col1/backup/.snapshot/`*nombre-de-instantánea*`/dir1`.

   Nota

   col1 utiliza una L minúscula seguida por el número 1.

3. En el cuadro de texto Destination, escriba la ruta del directorio en que se copiarán los datos. Por ejemplo, `/data/col1/backup/dir2`. Este directorio de destino debe estar vacío, o la operación dará error.

   - Si existe el directorio de destino, haga clic en la casilla **Overwrite existing destination if it exists**.

4. Haga clic en **Aceptar**.
5. En el cuadro de diálogo del progreso que se muestra, haga clic en **Close** para salir.

CAPÍTULO 6

MTree

Este capítulo incluye:

- Descripción general de MTrees 234
- Monitoreo de uso de MTree 242
- Administración de las operaciones en MTree 245

Descripción general de MTrees

Un MTree es una partición lógica del sistema de archivos.

Puede utilizar MTrees para unidades de almacenamiento DD Boost, pools de DD VTL o un recurso compartido NFS/CIFS. Los MTrees permiten la administración granular de instantáneas, cuotas y DD Retention Lock. Para los sistemas que tienen DD Extended Retention y administración granular de las políticas de migración de datos del nivel activo al nivel de retención, las operaciones de MTrees se pueden realizar en un MTree específico en oposición al sistema de archivos completo.

Nota

Puede haber hasta el valor máximo configurable de MTrees designados para contextos de replicación de MTree.

No coloque archivos de usuario en el directorio de nivel superior de un MTree.

Límites de MTrees

Límites de MTrees para sistemas Data Domain

Tabla 96 MTrees compatibles

Sistema Data Domain	Versión de DD OS	MTrees configurables compatibles	MTrees activos simultáneos compatible
DD9800	6.0 y posterior	256	256
DD9500	5.7 y posterior	256	256
DD6800, DD9300	6.0 y posterior	128	128
DD6300	6.0 y posterior	100	32
DD990, DD4200, DD4500, DD7200	5.7 y posterior	128	128
Todos los demás sistemas DD	5.7 y posterior	100	Hasta 32, según el modelo
DD9500	5.6	100	64
DD990, DD890	5.3 y posterior	100	Hasta 32, según el modelo
DD7200, DD4500, DD4200	5.4 y posterior	100	Hasta 32, según el modelo
Todos los demás sistemas DD	5.2 y posterior	100	Hasta 14, según el modelo

Cuotas

Las cuotas de MTree se aplican solo a los datos lógicos por escrito a la MTree.

Un administrador puede definir una restricción de espacio de almacenamiento en un MTree, unidad de almacenamiento o pool de DD VTL para evitar el consumo excesivo de espacio. Existen dos tipos de límites de cuota: los límites máximos y los límites de advertencia. Puede establecer un límite, ya sea blando o dura o ambos, un límite blando y uno duro. Ambos valores deben ser enteros y el valor del blando debe ser menor que el valor del duro.

Cuando se establece un límite blando, se envía una alerta cuando el tamaño del MTree supera el límite, pero sin embargo los datos aún pueden escribirse en el mismo. Cuando se establece un límite duro, los datos no se pueden escribir en el MTree una vez que se alcance el límite duro. Por lo tanto, todas las operaciones de escritura fallan hasta que los datos sean eliminados del MTree.

Consulte Configure MTree quotas en la página 247 para obtener más información.

Imposición de cuotas

Habilite o deshabilite la imposición de cuotas

Acerca del panel de MTree

Enumera todos los MTrees activos en el sistema y muestra las estadísticas de almacenamiento de datos en tiempo real. La información en el área de descripción general es útil para visualizar las tendencias de uso del espacio.

Seleccione **Data Management** > **MTree**.

- Haga clic en una casilla de verificación de un MTree en la lista para ver los detalles y ejecutar la configuración en la vista Summary.
- Escriba el texto (son compatibles los comodines) en el campo Filter By MTree Name y haga clic en **Update** para agregar nombres MTrees específicos en la lista.
- Eliminar el texto del filtro y haga clic en **Reset** para volver a la lista predeterminada.

Tabla 97 Información de descripción general del MTree

Elemento	Descripción
MTree Name	The pathname of the MTree.
Quota Hard Limit	Porcentaje límite duro de la cuota utilizado.
Last 24 Hr Pre-Comp (antes de la compresión)	El volumen de datos crudos de la aplicación de respaldo que fueron escritos en las últimas 24 horas.
Last 24 Hr Post-Comp (después de la compresión)	El volumen de almacenamiento utilizado posterior la compresión en las últimas 24 horas.
Last 24 hr Comp Ratio	La proporción de compresión de las últimas 24 horas.
Weekly Avg Post-Comp	El volumen promedio de almacenamiento comprimido utilizado en las últimas cinco semanas.
Last Week Post-Comp	El volumen promedio de almacenamiento comprimido utilizado en los últimos siete días.

Tabla 97 Información de descripción general del MTree (continuación)

Elemento	Descripción
Weekly Avg Comp Ratio	La proporción de compresión promedio de las últimas cinco semanas.
Last Week Comp Ratio	La proporción de compresión promedio de los últimos siete días.

Acerca de la vista resumida

Visualice estadísticas importantes del sistema de archivos.

Ver información detallada

Seleccione un MTree para ver la información.

Tabla 98 Información detallada de MTree para un MTree seleccionado

Elemento	Descripción
Full Path	El nombre de ruta del MTree
Pre-Comp Used	El volumen actual de datos crudos de la aplicación de respaldo que fue escrita en el MTree.
Status	El estado actual del MTree (se admiten combinaciones). El estado puede ser: • D: Eliminado • RO: Solo lectura • RW: Lectura/escritura • RD: Destino de replicación • RLCE: DD Retention Lock Compliance habilitado • RLCD: DD Retention Lock Compliance deshabilitado • RLGE: DD Retention Lock Governance habilitado • RLGD: DD Retention Lock Governance deshabilitado
Cuota	
Quota Enforcement	Enabled o Disabled.
Pre-Comp Soft Limit	Valor actual. Haga clic en Configure para revisar los límites de la cuota.
Pre-Comp Hard Limit	Valor actual. Haga clic en Configure para revisar los límites de la cuota.
Quota Summary	Porcentaje de límite duro utilizado.
Protocolos	
CIFS Shared	El estado de recursos compartidos de CIFS. El estado puede ser: • Yes—El MTree o su directorio principal es compartido. • Partial—El subdirectorio bajo este MTree es compartido.

Tabla 98 Información detallada de MTree para un MTree seleccionado (continuación)

Elemento	Descripción
	• No: Este MTree y sus directorios principales o secundarios no son compartidos. Haga clic en el vínculo de CIFS para ir a la vista CIFS.
NFS exportado	El estado de exportación de NFS. El estado puede ser: • Yes—El MTree o su directorio principal es exportado. • Partial—El subdirectorio bajo este MTree es exportado. • No: Este MTree y sus directorios principales o secundarios no son exportados. Haga clic en el vínculo de NFS para ir a la vista NFS.
Unidad de Almacenamiento de DD Boost	El estado de exportación de DD Boost . El estado puede ser: • Yes—El MTree es exportado. • No—El MTree no es exportado. • Unknown—No brinda más información. Haga clic en el vínculo DD Boost para ir a la vista de DD Boost.
DD VTL Pool	Estado del informe del pool VTL. El estado puede ser: • Yes: El MTree es un pool de MTree de DD VTL. • No: El MTree no es un pool de MTree de DD VTL. • Unknown: No se brinda más información.
Pool de VDisk	Estado de informe de vDisk. El estado puede ser: • Unknown: no está habilitado el servicio de vDisk. • No: el servicio de vDisk está habilitado, pero el MTree no es un pool de vDisk. • Yes: el servicio de vDisk está habilitado y el MTree es un pool de vDisk.
Mediciones de capacidad física	
Used (Post-Comp)	Espacio de MTree utilizado después de la recopilación de los datos comprimidos.
Compression	Factor de compresión global.
Last Measurement Time	Última vez que el sistema midió el MTree.
Schedules	Cantidad de la programaciones asignadas. Haga clic en **Assign** para ver programaciones y asignarlas al MTree. • Name: El nombre de la programación. • Status: Enabled o Disabled. • Priority:

Tabla 98 Información detallada de MTree para un MTree seleccionado (continuación)

Elemento	Descripción
	▪ Normal: Envía una tarea de medición a la línea de espera de procesamiento. ▪ Urgent: Envía una tarea de medición al primer lugar de la línea de espera de procesamiento. • Schedule: Hora a la que se ejecuta la tarea. • MTree Assignments: Cantidad de MTrees asignados a la programación.
Submitted Measurements	Muestra el estado después de la compresión para el MTree. Haga clic en **Measure Now** para enviar un trabajo manual después de la compresión para el MTree y seleccione una prioridad para el trabajo. • 0: No se envía ningún trabajo de medición. • 1: Un trabajo de medición en ejecución. • 2: Dos trabajos de medición en ejecución.
Instantáneas	Muestra las siguientes estadísticas: • Total Snapshots • Expired • Unexpired • Oldest Snapshot • Newest Snapshot • Next Scheduled • Assigned Snapshot Schedules Haga clic en **Total Snapshots** para ir a la vista **Data Management** > **Snapshots**. Haga clic en **Assign Schedules** para configurar los programas de instantáneas.

Ver información de replicación de MTree

Visualizar configuración de replicación de MTree.

Si el MTree seleccionado está configurado para su replicación, se mostrará un resumen de la configuración en esta área. De lo contrario, esta área muestra `No Record Found`.

- Haga clic en el vínculo Replication para ir a la página de replicación para su configuración y ver detalles adicionales.

Tabla 99 Información de replicación de MTree

Elemento	Descripción
Source	El nombre de ruta del MTree de origen.

Tabla 99 Información de replicación de MTree (continuación)

Elemento	Descripción
Destino	El nombre de ruta del MTree de destino.
Status	El estado del par de replicación de MTree. Los estados pueden ser Normal, Error o Warning.
Sync As Of	El último día y hora en que el par de replicación fue sincronizado.

Visualización de información de la instantánea de MTree

Si el MTree seleccionado está configurado para instantáneas, se mostrará un resumen de la información sobre configuración de la instantánea.

- Haga clic en el vínculo **Instantáneas** para ir a la página de Instantáneas para ejecutar la configuración o ver detalles adicionales.
- Haga clic en **Assign Schedules** para asignar una programación de instantáneas al MTree seleccionado. Seleccione la casilla de verificación de la programación y luego haga clic en **OK** y **Close**. Para crear una programación de instantáneas, haga clic en **Create Snapshot Schedule** (consulte la sección sobre la creación de una programación de instantáneas para obtener instrucciones).

Tabla 100 Información de la instantánea de MTree

Elemento	Descripción
Total Snapshots	El número total de instantáneas creados para este MTree. Se puede crear un total de 750 instantáneas para cada MTree.
Expired	El número de instantáneas en este MTree que se han marcado para su eliminación, pero que todavía no se han quitado con la operación de borrado.
Unexpired	El número de instantáneas en este MTree que están marcados para conservarse.
Oldest Snapshot	La fecha de la instantánea más antigua para este MTree.
Newest Snapshot	La fecha de la instantánea más reciente para este MTree.
Next Scheduled	La fecha de la próxima instantánea programado.
Assigned Snapshot Schedules	El nombre de la programación de instantáneas asignada a este MTree.

Visualizar información del bloqueo de retención del MTree

Si el MTree seleccionado está configurado para una de las opciones de software de DD Retention Lock, se mostrará información resumida sobre la configuración de DD Retention Lock.

Nota

Para obtener información sobre cómo administrar DD Retention Lock para un MTree, consulte la sección acerca de cómo trabajar con DD Retention Lock.

Tabla 101 Información de DD Retention Lock

Elemento	Descripción
Status	Indica si DD Retention Lock está habilitado o deshabilitado.
Mode	Indica si MTree está configurado para DD Retention Lock Compliance o DD Retention Lock Governance.
Use	Indica el uso del MTree.
Retention period min	Indica los períodos de tiempo mínimos y máximos de DD Retention Lock.
Retention period max	Indica el período de tiempo máximo de DD Retention Lock.

Habilitación y administración de configuración de DD Retention Lock

Utilice el área DD Retention Lock de la interfaz gráfica del usuario para modificar los períodos de bloqueo de retención.

Procedimiento

1. Seleccione **Data Management** > **MTree** > **Summary**.
2. En el área Retention Lock, haga clic en **Edit**.
3. En el cuadro de diálogo Modify Retention Lock, seleccione **Enable** para habilitar DD Retention Lock en el sistema Data Domain.
4. Modifique el período de retención mínimo o máximo (la función debe estar previamente habilitada), en el panel Retention Period.
5. Seleccione un intervalo (minutos, horas, días, años). Haga clic en **Default** para visualizar los valores predeterminados.
6. Haga clic en **Aceptar**.

Resultados

Después de cerrar el cuadro de diálogo Modify Retention Lock, se mostrará la información actualizada del MTree en el área de resumen de DD Retention Lock.

Acerca de la vista de utilización del espacio (MTrees)

Mostrar una representación visual de la utilización de datos en un MTree en diferentes momentos.

Seleccione **Data Management** > **MTree** > **Space Usage**.

- Haga clic en un punto de una línea del gráfico para visualizar un cuadro con los datos de ese punto.
- Al hacer clic en **Print**(en la parte inferior del gráfico), se abre el cuadro de diálogo Print.
- Al hacer clic en **Show in new window**, se muestra el gráfico en una nueva ventana del navegador.

Las líneas del gráfico indican las mediciones en los siguientes campos:

- Pre-comp Escrito—El volumen total de datos enviados a el MTree por los servidores de respaldo. Los datos pre-comprimidos en un MTree es lo que un servidor de respaldo ve como la totalidad de datos sin comprimir almacenados en un MTree como unidad de almacenamiento, se muestra con el Espacio utilizado (a la izquierda) del eje vertical del gráfico.

- En uso después de la compresión: La cantidad total de espacio de almacenamiento en uso en el MTree después de la compresión, que se muestra con el eje vertical Space Used (izquierda) del gráfico.
- Factor de compresión: La tasa de compresión de los datos almacenados en el MTree, que se muestra con el eje vertical Comp Factor (derecha) del gráfico.

Nota

Para la vista del Espacio utilizado por MTrees, el sistema muestra solo la información comprimida previamente. Los datos pueden ser compartidos entre Mtrees por lo tanto no se puede proporcionar el uso de los datos comprimidos para un único Mtree.

Verificación de historial de uso de espacio

En el gráfico Space Usage, si hace clic en un intervalo (por ejemplo, 1w, 1m, 3m o 1y) en la línea Duration en la parte superior del gráfico, podrá modificar la cantidad de días de datos que se muestran en el gráfico, de 7 a 120 días.

Para ver el uso del espacio para los intervalos de más de 120 días, utilice el siguiente comando:

```
# filesys show compression [summary | daily | daily-detailed] {[last n
{hours | days | weeks | months}] | [start date [end date]]}
```

Acerca de la vista de escritura diaria (MTrees)

Visualice el flujo de datos de las últimas 24 horas. Se muestra el volumen de datos con el paso del tiempo, con los montos previos y posteriores a la compresión.

También se ofrecen los valores totales del volumen de compresión global y local, y los volúmenes previos y posteriores a la compresión.

- Haga clic en un punto de una línea del gráfico para visualizar un cuadro con los datos de ese punto.
- Al hacer clic en **Print** (en la parte inferior del gráfico), se abre el cuadro de diálogo Print.
- Al hacer clic en **Show in new window**, se muestra el gráfico en una nueva ventana del navegador.

Las líneas en gráfico indican las mediciones en los siguientes campos:

- Pre-Comp Written—El volumen total de datos escritos en el MTree por los servidores de respaldo. Los datos pre-comprimidos en un MTree es lo que un servidor de respaldo ve como la totalidad de datos sin comprimir almacenada en un Mtree como unidad de almacenamiento.
- Post-Comp Written—El volumen total de datos escritos en el MTree posterior a la ejecución de la compresión, en GiBs.
- Total Comp Factor—El volumen total de la compresión ejecutada en el sistema Data Domain con los datos que recibió (relación de compresión), que se muestran con el Factor de compresión total (a la derecha) en el eje vertical del gráfico.

Verificación del historial de los datos escritos

Si en el gráfico de Escrituras diarias se hace clic en un intervalo (por ejemplo, 7d , 30d , 60d o 120d) en la línea de Duración en la parte superior del gráfico, podrá modificar la cantidad de días de datos que aparecen en el gráfico, de 7 a 120 días .

En la parte inferior del gráficos de Escrituras diarias, podrán verse los siguientes totales para el valor de duración actual

- Pre-Comp escrito
- Post-Comp escrito
- Factor de Global-Comp
- Factor de Local-Comp
- Factor de Total-Comp

Monitoreo de uso de MTree

Visualice el uso del espacio y las tendencias de datos escritos para un MTree.

Procedimiento

- Seleccione **Data Management** > **MTree**.

  La vista MTree muestra una lista de MTrees configurados, y si se selecciona un MTree en la lista podrán verse detalles del mismo en la pestaña Summary. Las pestañas Space Usage y Daily Written muestran los gráficos que despliegan en forma visual los volúmenes de uso del espacio y la tendencia de los datos escritos para un MTree seleccionado. La vista también contiene opciones que permiten configurar un MTree para CIFS, NFS y DD Boost, además de secciones de administración de instantáneas y DD Retention Lock para un MTree.

  La vista MTree tiene un panel de descripción general del MTree y tres pestañas que se describen en forma detallada en estas secciones.

  - Acerca del panel de MTree en la página 235
  - Acerca de la vista resumida en la página 236
  - Acerca de la vista de utilización del espacio (MTrees) en la página 240
  - Acerca de la vista de escritura diaria (MTrees) en la página 241

  Nota

  La medición de la capacidad física (PCM) proporciona información de uso de espacio de un MTree. Para obtener más información acerca de PCM, consulte la sección sobre la comprensión de la medición de la capacidad física.

Comprensión de la medición de la capacidad física

La medición de la capacidad física (PCM) proporciona información de uso de espacio para un subconjunto de espacio de almacenamiento Desde DD System Manager, PCM proporciona información de uso de espacio para los MTrees, pero desde la interfaz de línea de comandos se puede ver información de uso de espacio para los MTrees, los grupos de usuarios, las unidades de grupos de usuarios y los conjuntos de rutas.

Una vez que se selecciona una ruta para PCM, todas las rutas debajo de ella se incluyen automáticamente. No seleccione una ruta secundaria después de que la ruta principal ya esté seleccionada. Por ejemplo, si `/data/col1/mtree3` está seleccionada, no seleccione ningún subdirectorio debajo de mtree3.

La *Guía de referencia de comandos de Data Domain Operating System* proporciona más información sobre el uso de PCM desde la línea de comandos.

Habilitación, deshabilitación y visualización de medición de la capacidad física

La medición de la capacidad física proporciona información de uso de espacio de un MTree.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Summary**.

   El sistema muestra la pestaña Summary en el panel File System.
2. Haga clic en **^** en la esquina inferior derecha para ver el panel de estado.
3. Haga clic en **Enable** a la derecha de **Physical Capacity Measurement Status** para habilitar PCM.
4. Haga clic en **Details** a la derecha de **Physical Capacity Measurement Status** para ver los trabajos de PCM que están actualmente en ejecución.
   - **MTree**: El MTree que PCM está midiendo.
   - **Priority**: La prioridad (normal o urgente) para la tarea.
   - **Submit Time**: La hora a la que se solicitó la tarea.
   - **Duration**: La cantidad de tiempo que se ejecutó PCM a fin de lograr la tarea.
5. Haga clic en **Disable** a la derecha de **Physical Capacity Measurement Status** para cancelar los trabajos de PCM actualmente en ejecución.

Inicialización de la medición de la capacidad física

La inicialización de la medición de la capacidad física (PCM) es una acción de un solo uso que se pueda llevar a cabo solo si PCM está habilitada y no se hay inicializado la caché. Limpia las memorias caché y mejora la velocidad de medición. Durante el proceso de inicialización, aún puede administrar y ejecutar trabajos de PCM.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Configuration**.
2. En Physical Capacity Measurement, a la derecha de la Cache, haga clic en **Initialize**.
3. Haga clic en **Yes**.

Administración de calendarios de medición de la capacidad física

Cree, edite, elimine y vea calendarios de medición de la capacidad física. Este cuadro de diálogo muestra solamente los calendarios creados para MTrees y calendarios que actualmente no tienen asignaciones.

Procedimiento

1. Seleccione **Data Management** > **MTree** > **Manage Schedules**.
   - Haga clic en **Add** (+) para crear el calendario.
   - Seleccione un calendario y haga clic en **Modify** (lápiz) para editarlo.
   - Seleccione un calendario y haga clic en **Delete** (X) para eliminarlo.
2. De manera opcional, haga clic en los nombres de encabezado para ordenar por calendario: **Name**, **Status** (Enabled o Disabled) **Priority** (Urgent or Normal), **Schedule** (sincronización de calendario) y **MTree Assignments** (la cantidad de MTrees a los que se asigna el calendario).

Creación de calendarios de medición de la capacidad física

Cree calendarios de medición de la capacidad física y asígnelos a MTrees.

Procedimiento

1. Seleccione **Data Management** > **MTree** > **Manage Schedules**.
2. Haga clic en **Add** (+) para crear el calendario.
3. Especifique el nombre del calendario.
4. Seleccione el estado:
   - **Normal**: Envía una tarea de medición a la línea de espera de procesamiento.
   - **Urgent**: Envía una tarea de medición al primer lugar de la línea de espera de procesamiento.
5. Seleccione la frecuencia con la que calendario desencadena una instancia de medición: **todos los días**, **todas las semanas** o **todos los meses**.
   - Para **días**, seleccione la hora.
   - Para **semanas**, seleccione la hora y el día de la semana.
   - Para **meses**, seleccione la hora y los días durante el mes.
6. Seleccione las asignaciones de MTrees para el calendario (los MTrees a los que se aplicará el calendario):
7. Haga clic en **Create**.
8. De manera opcional, haga clic en los nombres de encabezado para ordenar por calendario: **Name**, **Status** (Enabled o Disabled) **Priority** (Urgent or Normal), **Schedule** (sincronización de calendario) y **MTree Assignments** (la cantidad de MTrees a los que se asigna el calendario).

Edición de calendarios de medición de la capacidad física

Editar un calendario de medición de la capacidad física.

Procedimiento

1. Seleccione **Data Management** > **MTree** > **Manage Schedules**.
2. Seleccione un calendario y haga clic en **Modify** (lápiz).
3. Modifique el calendario y haga clic en **Save**.

   Las opciones de calendarización se describen en el tema Creación de calendarios de medición de la capacidad física.
4. De manera opcional, haga clic en los nombres de encabezado para ordenar por calendario: **Name**, **Status** (Enabled o Disabled) **Priority** (Urgent or Normal), **Schedule** (sincronización de calendario) y **MTree Assignments** (la cantidad de MTrees a los que se asigna el calendario).

Asignación de calendarios de medición de la capacidad física a un MTree

Conecte calendarios a un MTree.

Antes de comenzar

Se deben crear calendarios de medición de la capacidad física (PCM).

Nota

Los administradores pueden asignar hasta tres calendarios PCM a un MTree.

Procedimiento

1. Seleccione **Data Management** > **MTree** > **Summary**.
2. Seleccione MTrees a los cuales asignar calendarios.
3. Desplácese hacia abajo hasta el área Physical Capacity Measurements y haga clic en **Assign** a la derecha de Schedules.
4. Seleccione calendarios para asignar al MTree y haga clic en **Assign**.

Inicio inmediato de medición de la capacidad física

Inicie el proceso de medición tan pronto como sea posible.

Procedimiento

1. Seleccione **Data Management** > **MTree** > **Summary**.
2. Desplácese hacia abajo hasta el área Physical Capacity Measurements y haga clic en **Measure Now** a la derecha de Submitted Measurements.
3. Seleccione **Normal** (envía una tarea de medición a la línea de espera de procesamiento), o **Urgent** (envía una tarea de medición al primer lugar de la línea de espera de procesamiento).
4. Haga clic en **Enviar**.

Configuración de la regulación de medición de la capacidad física

Configure el porcentaje de los recursos del sistema dedicados a la medición de la capacidad física.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Settings**.
2. En el área Physical Capacity Measurement, haga clic en **Edit** a la izquierda de Throttle.
3.

Opción	Descripción
Haga clic en Default	Ingresa el valor predeterminado del sistema del 20 %.
Type throttle percent	El porcentaje de los recursos del sistema dedicados a la medición de la capacidad física.

4. Haga clic en **Save**.

Administración de las operaciones en MTree

En esta sección se describe la creación y configuración de un MTree, cómo habilitar y deshabilitar cuotas de MTree, y mucho más.

Creación de un MTree

Un MTree es una partición lógica del sistema de archivos. Utilice MTrees en unidades de almacenamiento de DD Boost, pools de DD VTL o un recurso compartido NFS/CIFS.

MTrees se crean en el área /data/col1/*mtree_name*.

Procedimiento

1. Seleccione **Data Management** > **MTree**.
2. En el área de descripción general de MTree, haga clic en **Create**.
3. Escriba el nombre del MTree en el cuadro de texto MTree Name. Los nombres de MTree pueden tener hasta 50 caracteres. Puede utilizar los siguientes caracteres:
   - Caracteres del alfabeto en mayúsculas y minúsculas: A-Z, a-z
   - Números 0-9
   - Espacio incorporado
   - coma (,)
   - punto (.), siempre y cuando no preceda al nombre.
   - signo de exclamación (!)
   - signo de número (#)
   - signo de dólar ($)
   - signo de porcentaje (%)
   - signo más (+)
   - arroba (@)
   - signo de igual (=)
   - Y comercial (&)
   - punto y coma (;)
   - paréntesis [(y)]
   - corchetes ([y])
   - llaves ({ y })
   - signo de intercalación (^)
   - tilde (~)
   - apóstrofe (comilla simple recta)
   - comilla inclinada (‘)
4. Establezca restricciones para el espacio de almacenamiento del MTree para evitar que se consuma espacio en exceso. Establezca el límite blando o duro de la cuota, o ambos. Con un límite blando, se envía una alerta cuando el tamaño MTree supera el límite, pero los datos aún pueden escribirse en el MTree. Los datos no se pueden escribir en el MTree una vez que se alcanza el límite duro.

Nota

Los límites de cuota son valores pre-comprimido.
Para establecer límites de cuota para el MTree, seleccione **Set to Specific value** y escriba el valor. Seleccione la unidad de medida: MiB, GiB, TiB o PiB.

Nota

Cuando establece límites flexibles y estrictos, el límite flexible de una cuota no puede superar el límite estricto.

5. Haga clic en **Aceptar**.

   La nueva MTree se muestra en la página de MTrees.

Nota

Puede ser necesario ampliar el ancho de la columna MTree Name para ver el nombre de ruta completo.

Configuración y habilitación/deshabilitación de las cuotas de MTree

Establezca la restricción del espacio de almacenamiento para un MTree, unidad de almacenamiento o pool de DD VTL.

La página **Data Management** > **Quota** le permite al administrador ver la cantidad de MTrees sin cuotas blandas o duras establecidas. Para MTrees con cuotas establecidas, la página muestra el porcentaje de límites blandos y duros utilizados que fueron previamente comprimidos.

Tenga en cuenta la siguiente información para la administración de las cuotas.

- Las cuotas de MTree aplican para la recopilación de operaciones. Estas cuotas pueden aplicarse a los datos en sistemas que tengan el software DD Extended Retention, sin importar en qué nivel resida, así como también DD VTL, DD Boost, CIFS y NFS.
- Los snapshots no son contados.
- Las cuotas no pueden establecerse en el directorio `/data/col1/backup`.
- El valor máximo permitido para la cuota es de 4096 PiB.

Configure MTree quotas

Utilice la pestaña de MTree o la de Quota para configurar cuotas de MTree.

Procedimiento

1. Seleccione una de las siguientes rutas de menú:
   - Seleccione **Data Management** > **MTree**.
   - Seleccione **Data Management** > **Quota**.
2. Seleccione solo una MTree en la pestaña MTree, o una o más MTrees en la pestaña Quota.

Nota

Las cuotas no pueden establecerse en el directorio `/data/col1/backup`.

3. En la pestaña MTree, haga clic en la pestaña **Summary** y luego haga clic en el botón **Configure** en el área Quota.
4. En la pestaña Quota, haga clic en el botón **Configure Quota**.

Configuración de cuotas de MTree

Escriba los valores de las cuotas duras y blandas y seleccione la unidad de medida.

Procedimiento

1. En el cuadro de diálogo Configure Quota for MTrees, escriba los valores de las cuotas duras y blandas y seleccione la unidad de medida: MiB, GiB, TiB o PiB.
2. Haga clic en **OK**.

Eliminación de un MTree

Elimina el MTree de la tabla de MTrees. Los datos de MTree se eliminarán en la próxima limpieza.

Nota

Debido a que el MTree y sus datos asociados no se eliminarán hasta que se ejecute la limpieza de archivos, no es posible crear un nuevo MTree con el mismo nombre que un MTree eliminado hasta que el MTree borrado sea eliminado del sistema de archivos en forma completa mediante la operación de limpieza.

Procedimiento

1. Seleccione **Data Management** > **MTree**.
2. Seleccione un MTree.
3. En el área de descripción general de MTree, haga clic en **Delete**.
4. Haga clic en **OK** en el cuadro de diálogo Warning.
5. Haga clic en **Close** en el cuadro de diálogo Delete MTree Status luego de ver el progreso.

Restauración de un MTree

La restauración recupera un MTree eliminado junto con sus datos y lo coloca nuevamente en su respectiva tabla del MTree.

Una restauración de un MTree recupera un MTree eliminado junto con sus datos y lo coloca nuevamente en su respectiva tabla del MTree.

Una restauración solo es posible si no se ejecutó la limpieza de archivos luego de haber marcado el MTree para ser eliminado.

Nota

También puede utilizar este procedimiento para restaurar una unidad de almacenamiento.

Procedimiento

1. Seleccione **Data Management** > **MTree** > **More Tasks** > **Undelete**.

2. Seleccione las casillas de verificación de los MTrees que desea recuperar y haga clic en **OK**.
3. Haga clic en **Close** en el cuadro de diálogo Undelete MTree Status luego de ver el progreso.

   El MTree recuperado aparecerá en la tabla del MTree

Cambiar el nombre de un MTree

Utilice la GUI del MTree de Data Management para cambiar el nombre de los MTrees.

Procedimiento

1. Seleccione **Data Management** > **MTree**.
2. Seleccione una MTree en la tabla MTree.
3. Seleccione la pestaña Summary.
4. En el área Detailed Information Overview, haga clic en **Rename**.
5. Escriba el nombre del MTree en el cuadro de texto New MTree Name.

   Consulte la sección acerca de la creación de un MTree para obtener una lista de caracteres permitidos.

6. Haga clic en **OK**.

   El MTree con el nombre nuevo aparecerá en la tabla del MTree

CAPÍTULO 7

Snapshots

Este capítulo incluye:

- Descripción general de snapshots 252
- Monitoreo de snapshots y sus programas 253
- Administración de snapshots 254
- Administración de calendarios de instantáneas 256
- Recuperar datos desde un snapshots 258

Descripción general de snapshots

En este capítulo se indica cómo utilizar la función snapshot con MTrees.

Un snapshot guarda una copia de solo lectura (conocido como *snapshot*) de un MTree designado en un momento específico. Puede utilizar un snapshot como punto de restauración, y puede administrar los calendarios y los snapshots de MTrees, y mostrar información acerca del estado de los snapshots existentes.

Nota

Los snapshots creados en el sistema Data Domain de origen se replican en el destino con la replicación de la colección y del MTree. No es posible crear snapshots en un sistema Data Domain que sea una réplica de la replicación de la colección. Tampoco es posible crear un snapshot en el MTree de destino de la replicación del MTree. La replicación del directorio no replica las snapshots, y requiere de la creación de snapshots por separado en el sistema de destino.

Las snapshots del MTree llamado `backup` se crean en el directorio del sistema `/data/col1/backup/.snapshot`. Cada directorio bajo `/data/col1/backup` también tiene un directorio `.snapshot` con el nombre de cada snapshot incluido en el directorio. Todos los MTrees presentan el mismo tipo de estructura, es por eso que un MTree denominado SantaClara puede tener un directorio del sistema `/data/col1/SantaClara/.snapshot`, y cada subdirectorio en `/data/col1/SantaClara` puede tener también un directorio `.snapshot`.

Nota

El directorio `.snapshot` no está visible si solamente `/data` esté montado. Al montarse el MTree, el directorio .snapshot podrá visualizarse.

Una snapshot vencida sigue encontrándose disponible hasta la próxima operación de limpieza del sistema de archivos.

La cantidad máxima de snapshots permitidos por MTree es de 750. Se envían advertencias cuando el número de snapshots por MTree alcanza el 90 % de la cantidad máxima permitida (de 675 a 749 snapshots), y se genera una alerta cuando se llega a la cantidad máxima. Para borrar la advertencia, debe expirar las snapshots y luego ejecutar la operación de limpieza del sistema de archivos.

Nota

Para identificar un MTree que esté llegando a la cantidad máxima de instantáneas, consulte el Panel de Snapshots en la página del MTree para mayor información sobre la visualización de la snapshot de un MTree.

La retención de snapshots para un MTree no ocupa espacio extra, pero si existe una snapshot y el archivo original ya no se encuentra allí, el espacio puede ser reclamado.

Nota

Protocolo de snapshots y CIFS: A partir de DD OS 5.0, el directorio `.snapshot` deja de estar visible en la lista de directorios del Explorador de Windows o el shell de comandos de DOS CMD. Puede acceder al directorio `.snapshot` escribiendo su nombre en la barra de direcciones del Explorador de Windows o el shell de comandos de DOS CMD. Por ejemplo, `\\dd\backup\.snapshot` o `Z:\.snapshot` cuando `Z:` se mapea como `\\dd\backup`).

Monitoreo de snapshots y sus programas

En esta sección, se proporciona información detallada y resumida acerca del estado de los snapshots y sus programas.

Acerca de la vista de snapshots

En los temas de esta sección, se describe la vista de Snapshot.

Descripción general del panel de snapshots

Visualice el cantidad total de las snapshots, la de snapshots vencidas, snapshots no vencidas, y el horario de la próxima limpieza.

Seleccione **Data Management** > **Snapshots**.

Tabla 102 Información general del panel de snapshots

Campo	Descripción
Total Snapshots (Across all MTrees)	El número total de snapshots, tanto activos y vencidos, en todos los MTrees en el sistema.
Expired	La cantidad de snapshots marcados para su eliminación, pero que no se eliminaron aún mediante la operación de limpieza.
Unexpired	La cantidad de snapshots marcados para mantenerse.
Calendario de próxima limpieza del sistema de archivos	La fecha en que se ejecutará la próxima operación de limpieza calendarizada del sistema de archivos.

Vista de snapshots

Visualice información de snapshots por nombre, por MTree, hora de creación, si se encuentra activo, y su vencimiento.

La pestaña de Snapshots muestra una lista de las snapshots y contiene la siguiente información.

Tabla 103 Información del snapshot

Campo	Descripción
MTree seleccionado	Una lista desplegable que selecciona el MTree en que opera el snapshot.

Tabla 103 Información del snapshot (continuación)

Campo	Descripción
Filtrar por	Elementos a buscar en la lista de snapshots que se visualiza. Las opciones son: • **Name**—Nombre de la snapshot (los comodines son aceptados). • **Year**—Lista desplegable para seleccionar el año.
Nombre	El nombre de la imagen del snapshot.
Hora de creación	La fecha de creación del snapshot.
Expira	La fecha en que expira el snapshot.
Estado	El estado del snapshot, que puede estar vencido o en blanco si está activo.

Vista de calendarios

Vea los días en que se tomarán los snapshots, los horarios, la hora en que serán conservados, y la convención de asignación de nombres.

Tabla 104 Información del calendario de snapshots

Campo	Descripción
Nombre	El nombre del calendario del snapshot.
Días	Los días en se tomarán los snapshot
Horario	La hora del día en se tomarán los snapshot
Período de retención	La cantidad de tiempo que se conservará el snapshot.
Patrón de asignación de nombres a Snapshots	Una cadena de caracteres y variables que se traduce al nombre del snapshot (por ejemplo, `scheduled-%Y-%m-%d-%H-%M`, se traduce a “scheduled-2010-04-12-17-33”).

1. Seleccione un calendario en la pestaña Schedules. El área de Detailed Information aparece una lista de los MTrees que comparten el mismo calendario con el MTree seleccionado.
2. Haga clic en el botón **Add/Remove** para agregar o quitar MTrees de lista de del calendario.

Administración de snapshots

En esta sección, se describe cómo administrar snapshots.

Creación de un snapshot

Cree un snapshot cuando se requiere un snapshot no programado.

Procedimiento

1. Seleccione **Data Management** > **Snapshots** para abrir la vista Snapshots.

2. En la Vista de snapshots, haga clic en **Create**.
3. En el campo de texto Name, escriba el nombre de la snapshot.
4. En el área de MTrees, seleccione la casilla de verificación de uno o más MTrees en el panel de Available MTrees y haga clic en **Add**.
5. En el área Expiration, seleccione una de estas opciones de vencimiento:
   a. **Never Expire**.
   b. Escriba un número para el campo de texto In y seleccione **Days**, **Weeks**, **Month** o **Years** en la lista desplegable. El snapshot se conservará hasta la misma hora del día tal como se establece en su creación.
   c. Escriba una fecha (con el formato *mm/dd/yyyy*) en el campo de texto On, o haga clic en **Calendar** y luego en una fecha.. El snapshot será conservado hasta la medianoche (00:00, el primer minuto del día) de la fecha determinada.
6. Haga clic en **OK** y **Close**.

Modificación de la fecha de vencimiento de una snapshot

Modifique la fecha de vencimiento de una snapshot ya sea para eliminarlos o para extender su vida útil para fines de auditoría o de cumplimiento de normas.

Procedimiento

1. Seleccione **Data Management**>**Snapshots** para abrir la vista Snapshots.
2. Haga clic en la casilla de verificación de la entrada del snapshot en la lista y haga clic en **Modify Expiration Date**.

   Nota

   Más de una Snapshot puede seleccionarse si hace clic en las casillas de verificación adicionales.

3. En el área Expiration, seleccione una de las siguientes fechas de vencimiento:
   a. **Never Expire**.
   b. En el campo de texto In, escriba un número y seleccione **Days**, **Weeks**, **Month** o **Years** en la lista desplegable.. El snapshot se conservará hasta la misma hora del día tal como se establece en su creación.
   c. En el campo de texto **On**, escriba una fecha (con el formato *mm/dd/yyyy*) o haga clic en Calendar**Calendar** y luego en una fecha. El snapshot será conservado hasta la medianoche (00:00, el primer minuto del día) de la fecha determinada.
4. Haga clic en **OK**.

Cambiar el nombre de un snapshot

Use la pestaña Snapshot para cambiar el nombre de un snapshot.

Procedimiento

1. Seleccione **Data Management** > **Snapshots** para abrir la vista Snapshots.
2. Seleccione la casilla de verificación de la entrada del snapshot en la lista y haga clic en **Rename**.

3. En el campo de texto Name, ingrese un nuevo nombre.
4. Haga clic en **OK**.

Crear vencimiento para una snapshot

Las snapshots no se pueden eliminar. Para liberar espacio en disco, deben vencer las snapshots, lo que sucederá en el próximo ciclo de limpieza posterior a su fecha de vencimiento.

Procedimiento

1. Seleccione **Data Management** > **Snapshots** para abrir la vista Snapshots.
2. Haga clic en la casilla de verificación al costado de la entrada del snapshot en la lista y haga clic en **Expire**.

Nota

Más de un Snapshot puede seleccionarse si selecciona las casillas adicionales de verificación.
El Snapshot se marca como Expired en la columna Status y se eliminará en la próxima operación de limpieza.

Administración de calendarios de instantáneas

Configure y administre una serie de instantáneas que se tomarán automáticamente en intervalos regulares (un calendario de instantáneas).

Múltiples calendarios de instantáneas pueden encontrase activos al mismo tiempo.

Nota

Si se programan múltiples instantáneas con el mismo nombre para que ocurran al mismo tiempo, solo se conserva una. No es posible determinar cuál será la que se conserve, por lo tanto debería programarse solo una instantánea con ese nombre para una hora determinada.

Creación de calendarios de snapshots

Cree un calendario de snapshots semanal o mensual mediante el GUI de Data Management.

Procedimiento

1. Seleccione **Data Managment** > **Snapshots** > **Schedules** para abrir la vista Schedules.
2. Haga clic en **Create**.
3. En el campo de texto **Name**, escriba el nombre del calendario.
4. En el cuadro de texto **Snapshot Name Pattern**, escriba el nombre del patrón.

   Escriba una cadena de caracteres y variables que se traduzca a un nombre del snapshot (por ejemplo, `scheduled-%Y-%m-%d-%H-%m`, se traduce como "scheduled-2012-04-12-17-33"). Utilice caracteres alfabéticos, números,_, - y las variables que se traducen en valores actuales.

5. Haga clic en **Validate Pattern & Update Sample**.

6. Haga clic en **Next**.
7. Seleccione la fecha en que se ejecutará el calendario:
   a. Semanal: Haga clic en las casillas al costado de los días de la semana o seleccione **Every Day**.
   b. Mensual: Haga clic en la opción **Selected Days** y luego en las fechas en el calendario, o seleccione el opción **Last Day of the Month**.
   c. Haga clic en **Next**.
8. Seleccione el horario del día en que se ejecutará el calendario:
   a. En un horario específico: Haga clic en **Add** y en el cuadro de horario que aparece, escriba la hora en el formato *hh:mm* y haga clic en **OK**.
   b. En Intervalos: Haga clic en las flechas desplegables para seleccionar el horario de inicio y final en *hh:mm* y si es AM o PM. Haga clic en las flechas desplegables de **Interval** para seleccionar un número y luego las horas o los minutos de intervalo.
   c. Haga clic en **Next**.
9. En el campo de texto de Retention Period, escriba un número y haga clic en la flecha desplegable para seleccionar los días, meses o años y haga clic en **Next**.

   Los calendarios programados deben especificar en forma explícita un horario de retención.
10. Revise los parámetros en el resumen del calendario y haga clic en **Finish** para completar la calendarización o **Back** para modificar alguna entrada.
11. Si un MTree no está asociado con el calendario, aparecerá un cuadro de diálogo de advertencia preguntándole si desea añadir un MTree al calendario. Haga clic en **OK** para continuar (o en **Cancel** para salir).
12. Para asignar un MTree al calendario, en el área de MTree, haga clic en la casilla de uno o más MTrees en el panel de MTrees disponibles, luego haga clic en **Add** y en **OK**.

Convenciones de asignación de nombres para snapshots creados por un calendario

La convención de nombrado para los snapshots calendarizados en un calendario se rige por la palabra scheduled seguida por la fecha de aparición del snapshot, en el formato `scheduled-`*`aaaa-mm-dd-hh-mm`*. Por ejemplo, `scheduled-2009-04-27-13-30`.

El nombre “mon_thurs” es el nombre del calendario del snapshot. Los snapshots generados por ese calendario pueden tener los nombres `scheduled-2008-03-24-20-00`, `scheduled-2008-03-25-20-00`, etc.

Modificación de un calendario de snapshots

Cambie el nombre, hora, fecha y período de retención del calendario de snapshots

Procedimiento

1. En la lista de calendarios, seleccione el calendario y haga clic en **Modify**.
2. En el campo de texto Name, escriba el nombre del calendario y haga clic en **Next**.

   Utilice caracteres alfanuméricos y el _ y el -.

3. Seleccione la fecha en que se ejecutará el calendario:
   a. Semanal: Haga clic en las casillas al costado de los días de la semana o seleccione **Every Day**.
   b. Mensual: Haga clic en la opción **Selected Days** y luego en las fechas en el calendario, o seleccione el opción **Last Day of the Month**.
   c. Haga clic en **Next**.
4. Seleccione el horario del día en que se ejecutará el calendario:
   a. En horario determinado: Haga clic en la casilla de verificación de la hora calendarizada en la lista Times y haga clic en **Edit**. En el cuadro de diálogo Times que aparece, escriba una nueva hora en el formato *hh:mm* y haga clic en **OK**. Haga clic en **Delete** para eliminar la hora calendarizada.
   b. En Intervalos: Haga clic en las flechas desplegables para seleccionar el horario de inicio y final en *hh:mm* y si es AM o PM. Haga clic en las flechas desplegables de Interval para seleccionar un número y luego las horas o los minutos de intervalo.
   c. Haga clic en **Next**.
5. En el campo de texto de Retention Period, escriba un número y haga clic en la flecha desplegable para seleccionar los días, meses o años y haga clic en **Next**.
6. Revise los parámetros en el resumen del calendario y haga clic en **Finish** para completar la calendarización o **Back** para modificar alguna entrada.

Eliminación de un calendario de snapshots

Elimine un calendario de snapshots de la lista Schedule.

Procedimiento

1. En la lista Schedule, haga clic en la casilla de verificación para seleccionar el calendario y luego haga clic en **Delete**.
2. En el cuadro de diálogo Verification, haga clic en **OK** y luego en **Close**.

Recuperar datos desde un snapshots

Utilice la operación de copia rápida para recuperar los datos almacenados en un snapshot. Consulte la sección sobre las operaciones de copia rápida.

CAPÍTULO 8

CIFS

Este capítulo incluye:

- Descripción general de la CIFS 260
- Configuración de firmas de SMB 260
- Ejecución de configuración de CIFS 261
- Trabajar con recursos compartidos 263
- Administración del control de acceso 270
- Monitoreo de operación de CIFS 275
- Ejecución de la solución de problemas de CIFS 279

Descripción general de la CIFS

Los clientes CIFS disponen de acceso a los directorios de un sistema Data Domain.

- El directorio `/data/col1/backup` es el directorio de destino para los datos comprimidos de los servidores de respaldo.
- El directorio `/ddvar/core` contiene los archivos core y de registro del sistema Data Domain (elimine los archivos core y de registro antiguos para liberar espacio en esta área).

Nota

También puede eliminar archivos core de `/ddvar` o del directorio `/ddvar/ext` si existe.

Los clientes, como los servidores de respaldo que ejecutan las operaciones de respaldo y restauración con un sistema Data Domain, necesitan, como mínimo, acceso al directorio `/data/col1/backup`. Los clientes con acceso administrativo necesitan ser capaces de acceder al directorio `/ddvar/core` para recuperar los archivos de registro y core.

Como componente de la configuración inicial del sistema Data Domain, los clientes CIFS fueron configurados para acceder a estos directorios. Este capítulo describe cómo modificar esta configuración y la forma de administrar el acceso a datos utilizando el Data DD Manager y el comando `cifs`.

Nota

- La página DD System Manager **Protocols** > **CIFS** le permite ejecutar las principales operaciones de CIFS, como habilitar y deshabilitar CIFS, establecer la autenticación, administrar recursos compartidos y visualizar la información de configuración y de recursos compartidos.
- El comando `cifs` contiene todas las opciones para la administración del respaldo y restauración de CIFS entre clientes de Windows y de los sistemas Data Domain, y para visualizar las estadísticas y el estado de los CIFS. Para obtener más información sobre el comando `cifs`, consulte la *Guía de referencia de comandos de Data Domain Operating System*.
- Para obtener información acerca de la configuración inicial del sistema, consulte la *Guía de configuración inicial de Data Domain Operating System*.
- Para obtener información sobre la configuración de clientes para usar el sistema Data Domain como un servidor, consulte la guía de ajuste relacionada, como la *CIFS Tuning Guide*, que está disponible desde el sitio web support.emc.com. Busque el nombre completo del documento utilizando el campo Search.

Configuración de firmas de SMB

En una versión de DD OS compatible, puede configurar la función de firma SMB usando la opción CIFS denominada firma de servidor.

Esta función de deshabilita de forma predeterminada debido a que degrada el rendimiento. Cuando se habilita, la firma de SMB puede causar una caída en el

rendimiento del 29 % (lecturas) al 50 % (escrituras), aunque el rendimiento individual del sistema puede variar. Hay tres valores posibles para la firma de SMB: disabled, auto y mandatory:

- Cuando la firma de SMB se define como deshabilitada, esta se deshabilita, de forma predeterminada.
- Cuando la firma de SMB se define como obligatoria, esta se requiere, y ambas computadoras en la conexión SMB deben tener la firma habilitada.

Comandos de la CLI de SMB

`cifs option set "server-signing" required`
Configura la firma de servidor como obligatoria.

`cifs option reset "server-signing"`
Restablece la firma del servidor a la predeterminada (deshabilitada).

Como una mejor práctica, cada vez que cambia las opciones de firma de SMB, deshabilite y luego habilite (reinicie) el servicio de CIFS usando los siguientes comandos de la CLI:

```
cifs disable
cifs enable
```

La interfaz de DD System Manager muestra si la opción de firma de SMB está deshabilitada o definida como automática u obligatoria. Para ver esta configuración en la interfaz, navegue hacia la siguiente pestaña: Pestaña **Protocols** > **CIFS** > **Configuration**. En el área Options, se deshabilitará el valor para la opción de firma de SMB , y automático u obligatorio reflejará el valor establecido usando los comandos de CLI.

Ejecución de configuración de CIFS

En esta sección, se proporcionan instrucciones acerca de cómo habilitar los servicios de CIFS, como el servidor CIFS, etc.

Sistemas de alta disponibilidad y CIFS

Los sistemas de alta disponibilidad son compatibles con CIFS. Sin embargo, si un trabajo CIFS está en curso durante un failover, el trabajo deberá reiniciarse.

“/ ddvar es un sistema de archivos ext3 y no puede compartirse como un recurso compartido basado en Mtrees normal. La información en /ddvar será obsoleta cuando el nodo activo produzca un failover en el nodo en standby porque los identificadores de archivos son diferentes en los dos nodos. Si /ddvar se monta para acceder a los archivos de registro o actualizar el sistema, desmonte y vuelva a montar /ddvar si se produjo un failover desde la última vez que se montó el /ddvar”.

Preparación de clientes para acceder a sistemas Data Domain

Busque documentación en línea.

Procedimiento

1. Inicie sesión en el sitio web de soporte en línea (support.emc.com).
2. En el campo Search, escriba el nombre del documento que está buscando.
3. Seleccione el documento adecuado, como la *Nota técnica de los sistemas CIFS y Data Domain*.

4. Siga las instrucciones en el documento.

Activación de los servicios CIFS

Habilitar el acceso del cliente al sistema utilizando el protocolo CIFS.

Luego de haberle configurado al cliente el acceso al sistema Data Domain, es posible activar los servicios CIFS para permitir que el cliente obtenga acceso al sistema mediante el protocolo CIFS.

Procedimiento

1. Para el sistema Data Domain que se encuentra seleccionado en el árbol de DD System Manager Navigation, haga clic en **Protocols** > **CIFS**.
2. En el área de estado CIFS, haga clic en **Enable**.

Asignación de nombre al servidor CIFS

El nombre de host para el sistema Data Domain que funciona como servidor CIFS se establece durante la configuración inicial del sistema.

Para cambiar un nombre de servidor CIFS, consulte los procedimientos de la sección sobre la configuración de parámetros de autenticación.

El nombre de host de un sistema Data Domain debe coincidir con el nombre asignado a sus direcciones IP en la tabla de DNS. De lo contrario, tanto la autenticación como los intentos de unirse a un dominio pueden fallar. Si es necesario cambiar el nombre del host de un sistema Data Domain, utilice el comando `net set hostname` y modifique la entrada del sistema en la tabla de DNS también.

Cuando el sistema Data Domain actúa como un servidor CIFS, toma el nombre de host del sistema. Con el fin de mantener la compatibilidad, también crea un nombre de NetBIOS. El nombre de NetBIOS es el primer componente de un nombre de host completamente en mayúsculas. Por ejemplo, el nombre de `host jp9.oasis.local` se trunca con el nombre de NetBIOS `JP9`. El servidor CIFS responde a ambos nombres.

Puede hacer que el servidor CIFS responda a diferentes nombres en los niveles de NetBIOS cambiando el nombre de host de NetBIOS.

Cómo cambiar los nombres del host de los NetBIOS

Cambie los nombres del host de los NetBIOS con la CLI.

Procedimiento

1. Visualice el nombre del NetBIOS en curso al escribir:

   ```
   # cifs show config
   ```

2. Use el comando
   `cifs set nb-hostname`*`nb-hostname`*
   .

Configuración de parámetros de autenticación

Configure los parámetros de autenticación de Data Domain para trabajar con CIFS.

Haga clic en el vínculo Configure a la izquierda de la etiqueta Authentication en la pestaña Configuration. El sistema navegará a la pestaña **Administration** > **Access** > **Authentication**, donde puede configurar la autenticación para Active Directory, Kerberos, grupos de trabajo y NIS.

Opciones de configuración de CIFS

Visualice la configuración de CIFS, restrinja las conexiones anónimas.

Procedimiento

1. Seleccione **Protocols** > **CIFS** > **Configuration**.
2. En el área Options, haga clic en **Configure Options**.
3. Para restringir las conexiones anónimas, haga clic en la casilla de la opción **Enable** en el área de Restrict Anonymous Connections.
4. En el área Log Level, haga clic en la lista desplegable para seleccionar el número de nivel.

   El nivel es un número entero de 1 (cero) a 5 (cinco). El primer uno es el nivel predeterminado del sistema, que envía los mensajes de registro menos detallados relacionados con CIFS, mientras que el nivel cinco proporciona el máximo nivel de detalle. Los mensajes de registro se almacenan en el archivo `/ddvar/log/debug/cifs/cifs.log`.

   Nota

   Un nivel de registro de 5 degrada el rendimiento del sistema. Haga clic en **Default** en el área Log Level luego de depurar un problema. Esto establece el nivel nuevamente en 1.

5. En el área Server Signing, seleccione:
   - **Enabled** para habilitar la firma de servidor
   - **Disabled** para deshabilitar la firma de servidor
   - **Required** cuando se requiera la firma de servidor

Desactivación de los servicios CIFS

Evite que los clientes accedan al sistema Data Domain.

Procedimiento

1. Seleccione **Protocols** > **CIFS**.
2. En el área Status, haga clic en **Disable**.
3. Haga clic en **OK**.

   Aun después de deshabilitar el acceso a CIFS, los servicios de autenticación de CIFS continuarán funcionando en el sistema Data Domain. Esta continuación se requiere para autenticar a los usuarios del dominio Active Directory para el acceso a la administración.

Trabajar con recursos compartidos

Para compartir datos, debe crear recursos compartidos en el sistema Data Domain.

Estos recursos son administrados en el sistema Data Domain y en los sistemas CIFS.

Creación de recursos compartidos en el sistema Data Domain

Al crear recursos compartidos, es necesario asignar el acceso de cliente a cada directorio por separado y eliminar el acceso desde cada directorio también por

separado. Por ejemplo, es posible quitar un cliente de `/ddvar` y que el cliente conserve el acceso a `/data/col1/backup`

Un sistema Data Domain admite un número máximo de 3000 recursos compartidos CIFS[1] y permite 600 conexiones simultáneas. Sin embargo, la cantidad máxima de conexiones compatibles se basa en la memoria del sistema. Consulte la sección sobre la configuración de la cantidad máxima de archivos abiertos en una conexión para obtener más información.

Nota

Si es necesario implementar la replicación, un solo sistema Data Domain puede recibir respaldos de clientes CIFS y clientes NFS, mientras se usen directorios por separado para cada uno. No combine datos de CIFS y NFS en el mismo directorio.

Procedimiento

1. Seleccione las pestañas **Protocols** > **CIFS** para desplazarse a la vista CIFS.
2. Asegúrese de que la autenticación se haya configurado, como se describe en la sección sobre la configuración de los parámetros de autenticación.
3. En el cliente CIFS, establezca los permisos de directorio compartido o las opciones de seguridad.
4. En la vista CIFS, haga clic en la pestaña Shares.
5. Haga clic en **Create**.
6. En el cuadro de diálogo Create Shares, introduzca la siguiente información:

Tabla 105 Información del cuadro de diálogo de Shares

Elemento	Descripción
Share Name	un nombre descriptivo para el recurso compartido.
Ruta al directorio	La ruta del directorio de destino (por ejemplo, `/data/col1/backup/dir1`). **Nota** col1 utiliza la letra en minúscula L seguida del número 1.
Comment	un comentario descriptivo acerca del recurso compartido.

Nota

El nombre del recurso compartido puede tener un máximo de 80 caracteres y no puede contener los siguientes caracteres: \ / : * ? " < > | + [ ] ; , = o caracteres ASCII extendidos.

7. Para agregar un cliente, haga clic en Add (**+**) en el área Clients. Se mostrará el cuadro de diálogo Client. Especifique el nombre del cliente en el cuadro de texto Client y haga clic en **OK**.

   Considere lo siguiente al escribir en el nombre del cliente.

   - No se permiten los espacios vacíos ni los caracteres de tabulación (espacios en blanco).

1. Puede resultar afectado por limitaciones de hardware.

- No se recomienda utilizar tanto un asterisco (*) y el nombre del cliente individual como también la dirección IP de un recurso compartido determinado. Cuando haya asterisco (*), no se utilizarán otras entradas del cliente para este recurso compartido.
- No es necesario utilizar el nombre del cliente y la dirección IP del cliente para el mismo cliente en un recurso compartido determinado. Utilice los nombres de cliente cuando estos se encuentren definidos en la tabla de DNS.
- Para hacer que el recurso compartido se encuentre disponible para todos los clientes, especifique el cliente mediante un asterisco (*). Todos los usuarios de la lista de clientes pueden acceder al recurso compartido, a menos que se especifiquen uno o más nombres de usuario, en cuyo caso solo los que aparecen en la lista pueden acceder al recurso compartido.

Repita este paso para cada cliente que sea necesario configurar.

8. En el área Max Connections, seleccione el cuadro de texto y escriba el número máximo de conexiones simultáneas para el recurso compartido. El valor predeterminado de cero (que también se puede configurar con el botón Unlimited) no impone ningún límite en el número de conexiones.
9. Haga clic en **OK**.

   El recurso compartido recién creado aparecerá al final de la lista de recursos compartidos, ubicada en el centro del panel Shares

Equivalente de la CLI

Procedimiento

1. Ejecute el comando `cifs status` para verificar que CIFS esté habilitado.
2. Ejecute el comando `filesys status` para verificar que el sistema de archivos esté habilitado.
3. Ejecute el comando `hostname` para determinar el nombre de host del sistema.
4. Cree el recurso compartido CIFS.

   `cifs share create <share> path <path> {max-connections <max connections> | clients <clients> | users <users> | comment <comment>}`

   ```
   # cifs share create backup path /backup
   ```

5. Conceda acceso de cliente al recurso compartido.

   `cifs share modify <share> {max-connections <max connections> | clients <clients> | browsing {enabled | disabled} | writeable {enabled | disabled} | users <users> | comment <comment>}`

   ```
   # cifs share modify backup clients
   "srvr24.yourdomain.com,srvr24,10.24.160.116
   ```

6. Opcionalmente, haga visible el recurso compartido.

   `cifs share <share> browsing enabled`

   ```
   # cifs share backup browsing enabled
   ```

7. Opcionalmente, permita que el recurso compartido se pueda escribir.

   `cifs share <share> writeable enabled`

   ```
   # cifs share backup writeable enabled
   ```

8. En el sistema de Windows, seleccione **Start** > **Run**, y escriba el nombre de host y el directorio del recurso compartido CIFS.

   <DDhostname>*.*<DDdomain.com>**<sharename>

9. Si existen problemas al conectarse al recurso compartido CIFS, ejecute el comando `cifs share show` para verificar el estado del recurso compartido.

   Se muestra la advertencia `WARNING: The share path does not exist!` si el recurso compartido no existe o se ha escrito mal en la creación.

   ```
   # cifs share show
   --------------- share backup ---------------

   enabled: yes
   path: /backup
   ```

10. Si todavía no se puede acceder al recurso compartido CIFS, verifique que toda la información del cliente esté en la lista de acceso y todas las conexiones de red sean funcionales.

Modificación de un recurso compartido en un sistema Data Domain

Modifique información y conexiones del recursos compartidos.

Procedimiento

1. Seleccione las pestañas **Protocols** > **CIFS** > **Shares** para desplazarse a la vista CIFS, pestaña Shares.
2. Haga clic en la casilla de verificación que aparece junto al recurso compartido que desea modificar en la lista de nombres de recursos compartidos.
3. Haga clic en **Modify**.
4. Información sobre la modificación de recurso compartido:
   a. Para modificar el comentario, escriba un texto nuevo en el campo de texto de Comment.
   b. Para modificar el nombre de un usuario o grupo, en la lista User/Group, seleccione la casilla de verificación de ese usuario o grupo y haga clic en **Edit** (lápiz) o **Delete** (X). Para agregar un usuario o grupo, haga clic en (**+**) y, en el cuadro de diálogo User/Group, seleccione Type para User o Group y escriba el nombre de usuario o de grupo.
   c. Para modificar el nombre de un cliente, en la lista Client, seleccione la casilla de verificación de ese cliente y haga clic en **Edit** (lápiz) o **Delete** (X). Para agregar un cliente, haga clic en el botón Add (**+**) y agregue el nombre en el cuadro de diálogo del Client.

      Nota

      Para hacer que el recurso compartido se encuentre disponible para todos los clientes, especifique el cliente mediante un asterisco (*). Todos los usuarios de la lista de clientes pueden acceder al recurso compartido, a menos que se especifiquen uno o más nombres de usuario, en cuyo caso solo los que aparecen en la lista pueden acceder al recurso compartido.

   d. Haga clic en **OK**.

5. En el área Max Connections, en el cuadro de texto, modifique el número máximo de conexiones simultáneas en el recurso compartido. O seleccione Unlimited para anular el límite de número de conexiones.
6. Haga clic en **OK**.

Creación de un recurso compartido a partir de un recurso compartido existente

Cree un recurso compartido a partir de recurso compartido existente y modifique el recurso nuevo de ser necesario.

Nota

Los permisos de usuario del recurso compartido existente se trasladarán al nuevo recurso compartido.

Procedimiento

1. En la pestaña CIFS Shares, haga clic en la casilla de verificación del recurso compartido que desea utilizar como el de origen.
2. Haga clic en **Create From**.
3. Modifique la información del recurso compartido, tal como se describe en la sección acerca de cómo modificar un recurso compartido en un sistema Data Domain .

Desactivación de un recurso compartido en un sistema Data Domain

Desactive uno o más recursos compartidos existentes.

Procedimiento

1. En la pestaña Shares, haga clic en la casilla del recurso compartido que desea deshabilitar en la lista de Nombres de recursos compartidos.
2. Haga clic en **Disable**.
3. Haga clic en **Close**.

Activación de un recurso compartido en un sistema Data Domain

Habilite uno o más recursos compartidos existentes.

Procedimiento

1. En la pestaña Shares, haga clic en la casilla de verificación de los recursos compartidos que desea habilitar en la lista Share Name.
2. Click **Enable**.
3. Haga clic en **Close**.

Eliminación de un recurso compartido en un sistema Data Domain

Elimine uno o más recursos compartidos existentes.

Procedimiento

1. En la pestaña Shares, haga clic en la casilla de verificación de los recursos compartidos que desea eliminar en la lista Share Name.
2. Haga clic en **Delete**.

   Aparece el cuadro de diálogo Warning.

3. Haga clic en **OK**.

   Se eliminarán los recursos compartidos.

Ejecución de la administración de MMC

Use Microsoft Management Console (MMC) para la administración.

El SO de DD es compatible con estas funciones de MMC:

- Administración de recurso compartido, excepto al navegar para agregar un recurso compartido o cambiar la configuración offline predeterminada, que es un procedimiento manual.
- Administración de sesiones
- Abra la administración de archivos, excepto para eliminarlos.

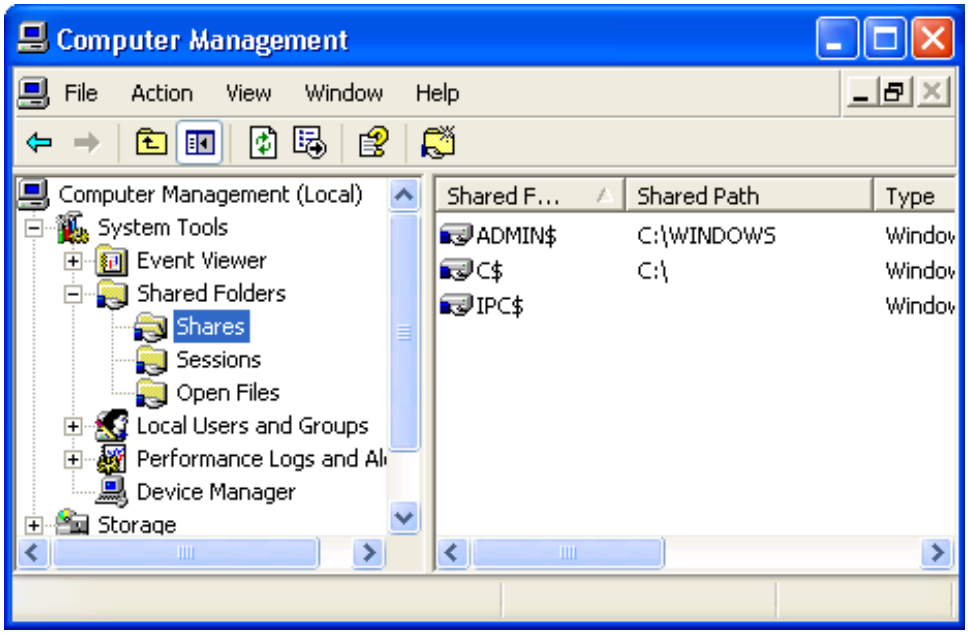
Conexión de un sistema Data Domain desde un cliente CIFS

Use CIFS para conectarse a un sistema Data Domain y crear una subcarpeta de respaldo de solo lectura.

Procedimiento

1. En la página de CIFS del sistema Data Domain, verifique que el estado de CIFS muestre que CIFS está habilitado y en funcionamiento.
2. En el panel de control, abra Administrative Tools y seleccione **Computer Management**.
3. En el cuadro de diálogo Computer Management, haga clic con el botón secundario en **Computer Management (Local)** y seleccione **Connect to another computer** del menú.
4. En el cuadro de diálogo Select Computer, seleccione **Another computer** e ingrese el nombre o la dirección IP para el sistema Data Domain.
5. Cree una subcarpeta de `\backup` que sea de solo lectura. Para obtener más información, consulte la sección acerca de cómo crear una subcarpeta /data/col1/backup de solo lectura.

Figura 7 Cuadro de diálogo Computer Management



Creación de una subcarpeta \data\col1\backup de solo lectura.

Escriba una ruta, nombre de recurso compartido y seleccione los permisos.

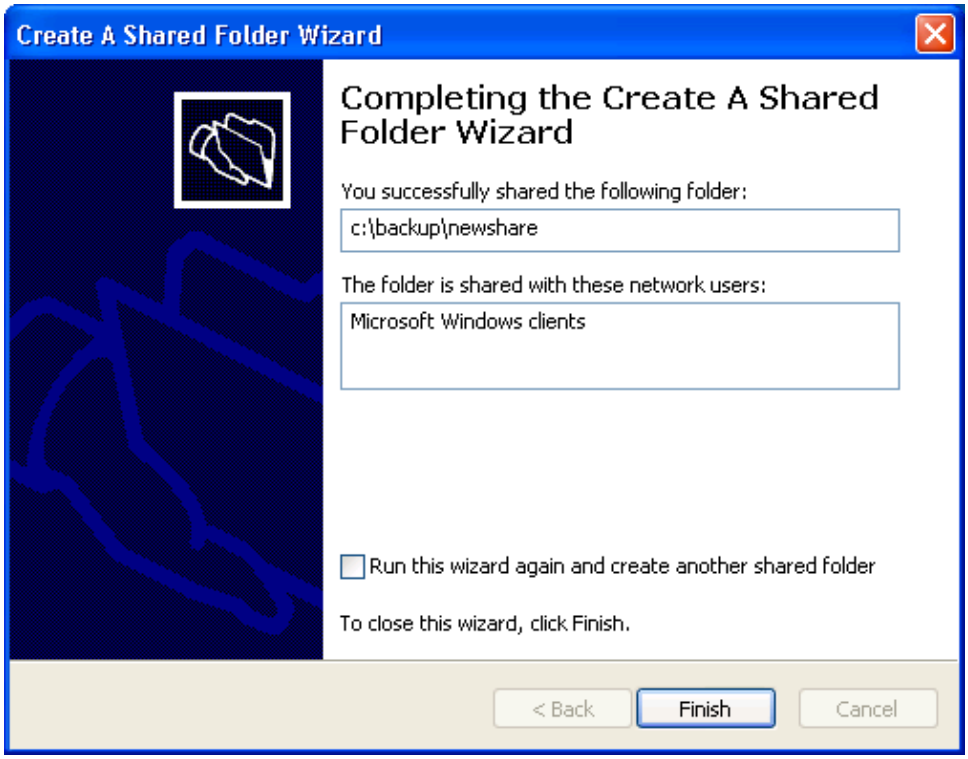
Procedimiento

1. En el Control Panel, abra Administrative Tools y seleccione **Computer Management**.
2. Haga clic con el botón secundario en **Shares** es el directorio de Shared Folders.
3. Seleccione **New File Share** desde el menú.

   Se abrirá el asistente para **Create a Shared Folder**. El nombre del equipo debe ser el nombre o la dirección IP del sistema de Data Domain

4. Escriba la ruta de la carpeta que va a compartir, por ejemplo, escriba `C:\data\col1\backup\newshare`.
5. Escriba el nombre del recurso compartido, por ejemplo, escriba **`newshare`**. Haga clic en **Next**.
6. Para los Share Folder Permissions, solo los administradores seleccionados cuentan con acceso completo. Otros usuarios tienen acceso de solo lectura. Haga clic en **Next**.

Figura 8 Completar el Asistente para Create a Shared Folder



7. El cuadro de diálogo Completing muestra que compartió la carpeta con todos los clientes de Microsoft Windows en la red en forma exitosa. Haga clic en **Finish**.

   La carpeta compartida recién creada se encuentra en el cuadro de diálogo Computer Management.

Información de CIFS en pantalla

Muestre información acerca de carpetas compartidas, sesiones y archivos abiertos.

Procedimiento

1. En el panel de control, abra Administrative Tools y seleccione **Computer Management**.
2. Seleccione una de las carpetas compartidas (**Shares**, **Sessions** u **Open Files**) en el directorio de herramientas del sistema.

   La información acerca de las carpetas compartidas, las sesiones y los archivos abiertos se muestra en el panel derecho.

Administración del control de acceso

Acceda a recursos compartidos desde un cliente Windows, proporcione acceso administrativo, y permita el acceso de usuarios del dominio que sean de confianza.

Acceso a recursos compartidos desde un cliente de Windows

Utilice la línea de comandos para asignar un recurso compartido.

Procedimiento

- En el cliente de Windows, utilice este comando de DOS:
  `net use`*drive*`:`*backup-location*

Por ejemplo, escriba:

```
# \\dd02\backup /USER:dd02\backup22
```

Este comando asigna el recurso compartido de respaldo para el sistema Data Domain dd02 a la unidad H en el sistema Windows y otorga al usuario con el nombre backup22 acceso al directorio `\\DD_sys\backup`.

DD OS admite la funcionalidad de notificación de cambios de SMB. Esto mejora el rendimiento de CIFS en el cliente de Windows permitiendo que el servidor CIFS notifique automáticamente al cliente de Windows sobre los cambios en el recurso compartido CIFS y elimine la necesidad de que el cliente sondee el sistema Data Domain para buscar cambios en el recurso compartido.

Proporcionar acceso administrativo a los usuarios de dominio

Utilice la línea de comandos para agregar CIFS e incluir el nombre de dominio en la instrucción ssh.

Procedimiento

- Escriba: **`adminaccess authentication add cifs`**

  El comando SSH, Telnet o FTP que accede al sistema Data Domain debe incluir el nombre de dominio, una barra invertida, y el nombre de usuario, todo entre comillas dobles. Por ejemplo:

  ```
  C:> ssh "domain2\djones" @dd22
  ```

Permiso de acceso administrativo a un sistema Data Domain para usuarios de dominios

Use la línea de comandos para asignar un número de grupo predeterminado del sistema DD y, luego, habilite el acceso administrativo de CIFS.

Procedimiento

1. Para asignar un número de grupo predeterminado del sistema Data Domain a un nombre de grupo de Windows distinto al nombre de grupo predeterminado, use el comando
   `cifs option set "dd admin group2" ["windows`*grp-name*`"]`
   .

   El nombre de grupo de Windows es un grupo (basado en una de las funciones de usuario: administrador, usuario u operador de respaldo) que existe en un controlador de dominio de Windows, y se pueden tener hasta 50 grupos (dd admin group1 a dd admin group50).

   Nota

   Para ver una descripción de las funciones de DD OS y de los grupos de Windows, consulte la sección acerca de la administración de sistemas Data Domain.

2. Habilite el acceso administrativo de CIFS ingresando lo siguiente:

`adminaccess authentication add cifs`

- El comando predeterminado group dd admin group1 del sistema Data Domain se asigna a los administradores de dominios de grupo de Windows.
- Puede asignar el comando predeterminado group dd admin group2 del sistema Data Domain a un grupo de Windows denominado Data Domain que crea en un controlador de dominios de Windows.
- El acceso está disponible a través de SSH, Telnet, FTP, HTTP y HTTPS.
- Después de configurar el acceso administrativo al sistema Data Domain desde `Data Domain`, del grupo de Windows, debe habilitar el acceso administrativo de CIFS usando el comando `adminaccess`.

Restricción del acceso administrativo desde Windows

Utilice la línea de comandos para prohibir el acceso a los usuarios que no tengan una cuenta de DD.

Procedimiento

- Escriba: `adminaccess authentication del cifs`

  Este comando prohíbe que los usuarios de Windows accedan al sistema Data Domain si no cuentan con una cuenta en el sistema Data Domain.

Acceso a archivos

Esta sección contiene información sobre las ACL, la configuración de permisos de DACL y SACL utilizando el Explorador de Windows, y así sucesivamente.

Listas de control de acceso NT

Las listas de control de acceso (ACL) están habilitadas de forma predeterminada en el sistema Data Domain.

⚠ PRECAUCIÓN

Data Domain recomienda que no deshabilite las ACL de NTFS una vez que se hayan habilitado. Póngase en contacto con el servicio de soporte de Data Domain antes de deshabilitar las ACL de NTFS.

Permisos de ACL predeterminados

Los permisos predeterminados, que se asignan a nuevos objetos creados a través del protocolo CIFS cuando están habilitadas las ACL, dependen del estado del directorio principal. Hay tres posibilidades diferentes:

- El directorio principal no tiene ACL porque se creó mediante el protocolo NFS.
- El directorio principal tiene un ACL heredable, porque se creó mediante el protocolo CIFS o porque las ACL se configuraron de forma explícita. La ACL existente se establece en objetos nuevos.
- El directorio principal tiene una ACL, pero no es heredable. Los permisos son los siguientes:

Tabla 106 Permisos

Tipo	Nombre	Permiso	Aplicar a
Permitir	SISTEMA	Control total	Solo esta carpeta
Permitir	CREATOR OWNER	Control total	Solo esta carpeta

Nota

CREATOR OWNER es reemplazado por el usuario que crea el archivo o la carpeta en el caso de los usuarios normales, y por los administradores en el caso de los usuarios administrativos.

Permisos para un objeto nuevo cuando el directorio principal no tiene ACL
Los permisos son los siguientes:

- BUILTIN\Administradores:(OI)(CI)F
- NT AUTHORITY\SYSTEM:(OI)(CI)F
- CREATOR OWNER:(OI)(CI)(IO)F
- BUILTIN\Usuarios:(OI)(CI)R
- BUILTIN\Usuarios:(CI)(acceso especial:)FILE_APPEND_DATA
- BUILTIN\Usuarios:(CI)(IO)(acceso especial:)FILE_WRITE_DATA
- Todos:(OI)(CI)R

Estos permisos se describen en más detalle a continuación:

Tabla 107 Detalles de permisos

Tipo	Nombre	Permiso	Aplicar a
Permitir	Administradores	Control total	Esta carpeta, subcarpetas y archivos
Permitir	SISTEMA	Control total	Esta carpeta, subcarpetas y archivos
Permitir	CREATOR OWNER	Control total	Solo subcarpetas y archivos
Permitir	Usuarios	Lectura y ejecución	Esta carpeta, subcarpetas y archivos
Permitir	Usuarios	Crear subcarpetas	Solo esta carpeta y subcarpetas
Permitir	Usuarios	Crear archivos	Solo subcarpetas
Permitir	Todos	Lectura y ejecución	Esta carpeta, subcarpetas y archivos

Configuración de permisos de ACL y seguridad
Las herramientas de restauración y respaldo basadas en Windows, como NetBackup, se pueden usar para respaldar archivos protegidos por DACL y SACL al sistema Data Domain, y para restaurarlos desde el sistema Data Domain.

Permisos granulares y complejos (DACL)
Puede configurar permisos granulares y complejos (DACL) en cualquier objeto de carpeta o archivo dentro del sistema de archivos, ya sea usando comandos de

Windows, como `cacls`, `xcacls`, `xcopy` y `scopy`, o a través del protocolo CIFS usando la GUI de Windows Explorer.

ACL de auditoría (SACL)
Puede configurar ACL de auditoría (SACL) en cualquier objeto en el sistema de archivos, ya sea mediante comandos o mediante el protocolo CIFS, usando la GUI de Windows Explorer.

Configuración de permisos de la DACL utilizando el Explorador de Windows

Utilice la configuración de propiedades del explorador para seleccionar los permisos de la DACL.

Procedimiento

1. Haga clic con el botón secundario en el archivo o la carpeta y seleccione **Properties**.
2. En el cuadro de diálogo Properties, haga clic en la pestaña Security.
3. Seleccione el nombre del grupo o usuario de la lista, como por ejemplo **Administrators**. Podrán verse los permisos, en este caso para `Administrators, Full Control`.
4. Haga clic en el botón **Advanced**, que le permitirá establecer permisos especiales.
5. En el cuadro de diálogo Advanced Security Settings for ACL, haga clic en la pestaña Permissions.
6. Seleccione la entrada del permiso en la lista.
7. Para obtener más información sobre una entrada de permiso, seleccione la entrada y haga clic en **Edit**.
8. Seleccione la opción Inherit from parent para obtener los permisos para las entradas principales existentes por sus objetos secundarios, y haga clic en **OK**.

Configuración de permisos de SACL con Windows Explorer

Use las configuraciones de propiedades de Explorer para seleccionar los permisos de SACL.

Procedimiento

1. Haga clic con el botón secundario en el archivo o la carpeta y seleccione **Properties** en el menú.
2. En el cuadro de diálogo Properties, haga clic en la pestaña Security.
3. Seleccione el nombre de grupo o usuario, como **Administrators**, de la lista, donde se muestran sus permisos, en este caso, `Full Control`.
4. Haga clic en el botón **Advanced**, que le permite configurar permisos especiales.
5. En el cuadro de diálogo Advanced Security Settings for ACL, haga clic en la pestaña Auditing.
6. Seleccione la entrada de auditoría en la lista,
7. Para ver más información acerca de las entradas de auditoría especiales, seleccione la entrada y haga clic en **Edit**.
8. Seleccione la opción Inherit from parent para obtener los permisos de las entradas principales existentes por los objetos secundarios y haga clic en **OK**.

Vista o cambio del ID de seguridad del propietario actual (SID del propietario)

Use el cuadro de diálogo de configuración de seguridad avanzada para ACL.

Procedimiento

1. En el cuadro de diálogo Advanced Security Settings for AC, haga clic en la pestaña Owner,
2. Para cambiar el propietario, seleccione un nombre de la lista Change owner y haga clic en **OK**.

Control de asignación de ID de cuentas

La opción idmap-type de CIFS controla el comportamiento de la asignación de los ID de las cuentas

Esta opción tiene dos valores: rid (el predeterminado) y none. Cuando la opción se establece en rid, la asignación de ID-a-id se ejecuta en forma interna. Cuando la opción se establece en none, todos los usuarios CIFS son asignados a un usuario UNIX local llamado “cifsuser” que pertenece a un grupo de usuarios UNIX local.

Tenga en cuenta la siguiente información al administrar esta opción.

- Para establecer esta opción, el CIFS debe estar desactivado. Si CIFS se encuentra ejecutándose, se deben desactivar los servicios CIFS.
- El tipo idmap-type puede establecerse a "ninguno" solo cuando la compatibilidad de ACL esté activado.
- Cada vez que se modifica idmap, puede que se requiera una conversión de metadatos del sistema de archivos para un correcto acceso al archivo. Sin ningún tipo de conversión, el usuario no podrá acceder a los datos. Para convertir los metadatos, consulte a su proveedor de soporte técnico contratado.

Monitoreo de operación de CIFS

Temas acerca del monitoreo de operaciones de CIFS

Visualización del estado de CIFS

Visualice y habilite/deshabilite los estados de CIFS.

Procedimiento

1. En DD System Manager, seleccione **Protocols** > **CIFS**.
   - El estado puede estar habilitado y ejecutándose, o deshabilitado pero con la autenticación CIFS ejecutándose.
     Para habilitar CIFS, consulte la sección sobre habilitación de los servicios CIFS Para deshabilitar CIFS, consulte la sección sobre deshabilitación de los servicios CIFS
   - La lista **Connections** muestra las conexiones y archivos abiertos.

Tabla 108 Información de detalles de conexiones

Elemento	Descripción
Open Connections	Conexiones CIFS abiertas
Límite de conexiones	Cantidad máxima de conexiones permitidas

Tabla 108 Información de detalles de conexiones (continuación)

Elemento	Descripción
Open Files	Archivos abiertos actuales
Max Open Files	Cantidad máxima de archivos abiertos en un sistema Data Domain

2. Haga clic en **Connection Details** para obtener más información sobre la conexión.

Tabla 109 Información de detalles de conexiones

Elemento	Descripción
Sessions	Sesiones activas de CIFS
Computadora	Nombre de la computadora o dirección IP conectada con DDR para la sesión
Usuario	Usuario que maneja la computadora conectada con el módulo DDR
Open Files	Cantidad de archivos abiertos para cada sesión
Connection Time	Duración de la conexión en minutos
Usuario	Nombre de dominio de la computadora
Mode	Permisos de archivos:
Bloqueos	Cantidad de bloqueos en el archivo
Archivos	Ubicación del archivo

Configuración de pantalla CIFS

Esta sección muestra la configuración de CIFS.

Configuración de autenticación

La información en el panel Authentication se modifica acorde al tipo de autenticación configurada.

Haga clic en el vínculo Configure a la izquierda de la etiqueta Authentication en la pestaña Configuration. El sistema navegará a la página **Administration** > **Access** > **Authentication**, donde puede configurar la autenticación para Active Directory, Kerberos, grupos de trabajo y NIS.

Configuración de Active Directory

Tabla 110 Información sobre la configuración de Active Directory

Elemento	Descripción
Mode	Se mostrará el modo de Active Directory.
Dominio	Se mostrará dominio configurado.
DDNS	El estado del servidor DDNS: enabled o disabled.

Tabla 110 Información sobre la configuración de Active Directory (continuación)

Elemento	Descripción
Controladores de dominio:	Se mostrará el nombre de los controladores de dominio configurado o una * si se permiten todos los controladores.
Unidad organizacional	Se mostrarán los nombres de las unidades organizacionales configuradas.
Nombre del servidor CIFS	Se mostrará el nombre del servidor CIFS configurado.
Nombre del servidor WINS	Se mostrará el nombre del servidor WINS configurado.
Nombre abreviado de dominio	Se mostrará el nombre resumido de dominio DNS

Configuración del grupo de trabajo

Tabla 111 Información de autenticación de la configuración del grupo de trabajo

Elemento	Descripción
Mode	Se mostrará el modo de grupo de trabajo
Nombre de grupo de trabajo	Se mostrará el nombre del grupo de trabajo
DDNS	El estado del servidor DDNS: enabled o disabled.
Nombre del servidor CIFS	Se mostrará el nombre del servidor CIFS configurado.
Nombre del servidor WINS	Se mostrará el nombre del servidor WINS configurado.

Pantalla de información de recursos compartidos

Esta sección muestra información de recursos compartidos

Visualización de los recursos compartidos configurados

Visualice la lista de recursos compartidos configurados

Tabla 112 Información de recursos compartidos configurados

Elemento	Descripción
Nombre de recurso compartido	El nombre de recurso compartido (por ejemplo, share1).
Estado del recurso compartido	El estado del recurso compartido: o activado o desactivado.
Ruta al directorio	La ruta al directorio del recurso compartido (por ejemplo, `/data/col1/backup/dir1`). **Nota** col1 utiliza la letra L minúscula seguida por el número 1
Estado de la ruta al directorio	El estado de la ruta al directorio.

- Para mostrar información sobre un recurso compartido específico, escriba el nombre del recurso compartido en el cuadro de texto "Filtrar por nombre del recurso compartido" y haga clic en **Update**.
- Haga clic en **Back** para volver a la lista predeterminada.
- Para desplazarse por la lista de recursos compartidos, haga clic en las flechas **<** y **>** en la parte inferior derecha de la vista para desplazarse hacia adelante o atrás. Para saltar al principio de la lista, haga clic en **|<** para ir directo hacia el final, haga clic en **>|**.
- Haga clic en la flecha desplegable **Items per Page** para modificar la cantidad de entradas de recursos compartidos en una página. Las elecciones son 15, 30 o 45 entradas.

Visualización de información detallada de recursos compartidos

Visualice información detallada acerca de un recurso compartido haciendo clic en un recurso compartido en la lista de recursos compartidos.

Tabla 113 Información de recursos compartidos

Elemento	Descripción
Share Name	El nombre de recurso compartido (por ejemplo, share1).
Ruta al directorio	La ruta del directorio del recurso compartido (por ejemplo, `/data/col1/backup/dir1`). **Nota** col1 utiliza la letra en minúscula L seguida del número 1.
Estado de la ruta al directorio	Indica si la ruta de directorio configurada existe en el módulo DDR. Los valores posibles son Path Exists o Path Does Not Exist, donde el último indica una configuración de CIFS incorrecta o incompleta.
Max Connections	La cantidad máxima de conexiones permitidas al recurso compartido al mismo tiempo. El valor predeterminado es Unlimited.
Comment	El comentario que se configuró al crearse el recurso compartido.
Estado del recurso compartido	El estado del servidor recurso compartido: enabled o disabled.

- El área Clients enumera los clientes que están configurados para acceder al recurso compartido, junto con un recuento de clientes en la parte inferior de la lista.
- El área User/Groups enumera los nombres y tipos de usuarios o grupos configurados para acceder al recurso compartido, junto con un recuento de usuarios o grupos en la parte inferior de la lista
- El área Options enumera el nombre y el valor de las opciones configuradas.

Visualización de las estadísticas CIFS

Utilice la línea de comandos para visualizar las estadísticas CIFS.

Procedimiento

- Escriba: `cifs show detailed-stats`

  El resultado muestra la cantidad de diversas solicitudes SMB recibidas y el tiempo requerido para procesarlas.

Ejecución de la solución de problemas de CIFS

En esta sección se presentan procedimientos para la solución de problemas básicos.

Nota

Los comandos `cifs troubleshooting` proporcionan información detallada acerca de los usuarios y grupos de CIFS.

Visualización de actividad en curso de clientes

Use la línea de comandos para mostrar la información de los archivos abiertos y las sesiones CIFS.

Procedimiento

- Ingrese: `cifs show active`

Resultados

Tabla 114 Sessions

Computadora	Usuario	Archivos abiertos	Tiempo de conexión (segundos)	Tiempo de inactividad (segundos)
::ffff:10.25.132.84	ddve-25179109\sysadmin	1	92	0

Tabla 115 Archivos abiertos

Usuario	Mode	Bloqueos	Archivo
ddve-25179109\sysadmin	1	0	C:\data\col1\backup

Configuración del máximo de archivos abiertos para una conexión

Utilice la línea de comandos para establecer el número máximo de archivos que pueden permanecer abiertos en forma simultánea.

Procedimiento

- Ingrese: `cifs option set max-global-open-files` *value*.

  El *value* para la cantidad máxima de archivos globales abiertos puede oscilar entre 1 y el límite máximo de archivos abiertos. El límite máximo se basa en la memoria DDR del sistema. Para los sistemas con más de 12 GB, el límite máximo de archivos abiertos es 30,000. Para los sistemas con 12 GB o menos, el límite máximo de archivos abiertos es 10,000.

Tabla 116 Límite de conexiones y límite máximo de archivos abiertos

Modelos de DDR	Memoria	Límite de conexiones	Límite máximo de archivos abiertos
DD620, DD630, DD640	8 GB	300	10,000
DD640	16 GB	600	30,000
DD640	20 GB	600	30,000
DD860	36 GB	600	30,000
DD860, DD860ArT	72 GB	600	30,000
	96 GB	600	30,000
	128 GB	600	30,000
	256 GB	600	30,000

Nota

El sistema tiene un límite máximo de 600 conexiones CIFS y 250,000 archivos abiertos. No obstante, si el sistema se queda sin archivos abiertos, la cantidad de archivos puede incrementarse.

Nota

Las latencias de acceso a archivos resultan afectadas por la cantidad de archivos en un directorio. En la medida en que sea posible, recomendamos tamaños de directorio de menos de 250,000. Los directorios de tamaños más grandes experimentarán respuestas más lentas para las operaciones de metadatos como la enumeración de archivos en el directorio y la apertura o la creación de archivos.

Reloj del sistema Data Domain

Cuando se utiliza el modo de Active Directory, para el acceso CIFS, la hora del reloj del sistema Data Domain puede diferir en no más de cinco minutos de la del controlador de dominio.

La pestaña **Administration** > **Settings** > **Time and Date Settings** del administrador del sistema DD sincroniza el reloj con un servidor de hora.

Ya que el controlador del dominio de Windows obtiene el tiempo desde una fuente externa, el NTP debe configurarse. Consulte la documentación de Microsoft sobre cómo configurar un NTP para la versión del sistema operativo o el service pack de Windows que se ejecuta en el controlador de dominio.

En el modo de autenticación de Active Directory, el sistema Data Domain sincroniza periódicamente el reloj con un Active Directory Domain Controller de Windows.

Sincronización desde un controlador de dominio de Windows

Utilice la línea de comandos en un controlador de dominio de Windows para sincronizar con un servidor NTP.

Nota

Este ejemplo aplica para Windows 2003 SP1; sustituya su servidor de dominio para el nombre del servidor NTP (*ntpservername*).

Procedimiento

1. En el sistema de Windows, escriba comandos similares al siguiente:

   ```
   C:\>w32tm /config /syncfromflags:manual /manualpeerlist: ntp-server-name C:\>w32tm /config /update C:\>w32tm /resync
   ```

2. Luego de que el NTP se encuentre configurado en el controlador del dominio, configure la sincronización del servidor de tiempo, tal como se describe en la sección sobre la configuración de la hora y la fecha.

Sincronizar desde un servidor NTP

Configurar la sincronización del servidor de tiempo, tal como se describe en la sección sobre la configuración de la hora y la fecha.

CAPÍTULO 9

NFS

Este capítulo incluye:

- Descripción general de NFS 284
- Administración del acceso de clientes NFS al sistema Data Domain 285
- Visualización de la información de NFS 289
- Integración de un DDR en un dominio Kerberos 290
- Agregar y eliminar servidores KDC después de la configuración inicial 292

Descripción general de NFS

Los clientes NFS disponen de acceso a los directorios del sistema o MTrees en el sistema Data Domain.

- El directorio `/backup` es el directorio de destino predeterminado para los datos comprimidos de los servidores de respaldo que no sean MTree.
- La ruta `/data/col1/backup` es el directorio de destino raíz cuando se utilizan MTrees para datos comprimidos de servidor de respaldo.
- El directorio `/ddvar/core` contiene los archivos principales y de registro del sistema Data Domain (elimine los archivos principales y de registro antiguos para liberar espacio en esta área).

Nota

En los sistemas Data Domain, el `/ddvar/core` está en una partición separada. Si monta solo `/ddvar`, no podrá navegar a `/ddvar/core` desde el punto de montaje `/ddvar`.

Los clientes, como los servidores de respaldo que ejecutan las operaciones de respaldo y restauración con un sistema Data Domain, necesitan acceso a las áreas `/backup` o `/data/col1/backup`. Los clientes con acceso administrativo necesitan ser capaces de acceder al directorio `/ddvar/core` para recuperar los archivos de registro y core.

Como parte de la configuración inicial del sistema Data Domain, los clientes NFS se configuraron para que tuvieran acceso a estas áreas. En este capítulo se describe cómo modificar esta configuración y cómo administrar el acceso a datos.

Nota

- Para obtener información acerca de la configuración inicial del sistema, consulte la *Guía de configuración inicial de Data Domain Operating System*.
- El comando `nfs` administra respaldos y restauraciones entre clientes NFS y sistemas Data Domain, y muestra estadísticas y estados de NFS. Para obtener más información sobre el comando `nfs`, consulte la *Guía de referencia de comandos de Data Domain Operating System*.
- Para obtener información acerca de la configuración de clientes de terceros para que usen el sistema Data Domain como servidor, consulte la guía de ajuste relacionada, como *Solaris System Tuning*, que está disponible desde el sitio web de soporte de Data Domain. En la página Documentation > Integration Documentation, seleccione el proveedor de la lista y haga clic en **OK**. Seleccione la guía de ajuste de la lista.

Sistemas de alta disponibilidad y NFS

Los sistemas de alta disponibilidad son compatibles con NFS. Si un trabajo NFS está en curso durante una conmutación por error, **no** será necesario reiniciar el trabajo.

Nota

/ddvar es un sistema de archivos ext3 y no puede compartirse como un recurso compartido basado en MTrees normal. La información en /ddvar será obsoleta cuando el nodo activo produzca una conmutación por error en el nodo en espera porque los identificadores de archivos son diferentes en los dos nodos. Si /ddvar se monta para acceder a los archivos de registro o actualizar el sistema, desmonte y vuelva a montar /ddvar si se produjo una conmutación por error desde la última vez que se montó el /ddvar.

Para crear exportaciones NFS válidas que realizarán una conmutación por error con alta disponibilidad, la exportación debe crearse desde el nodo activo de alta disponibilidad y, por lo general, debe compartirse mediante las interfaces de red de conmutación por error.

Administración del acceso de clientes NFS al sistema Data Domain

En los temas de esta sección se describe cómo administrar el acceso de clientes NFS a un sistema Data Domain.

El artículo de la base de conocimiento *NFS Best Practices for Data Domain and client OS*, disponible en https://support.emc.com/kb/180552, proporciona información adicional sobre las mejores prácticas para NFS.

Activación de servicios NFS

Puede habilitar servicios NFS para permitir que el cliente acceda al sistema a través del protocolo NFS.

Procedimiento

1. Seleccione **Protocols** > **NFS**.

   Se abre la vista NFS y muestra la pestaña Exports.

2. Haga clic en **Enable**.

Deshabilitación de servicios NFS

Puede deshabilitar servicios NFS para impedir el acceso de clientes al sistema a través del protocolo NFS.

Procedimiento

1. Seleccione las pestañas **Protocols** > **NFS**.

   Se abre la vista NFS y muestra la pestaña Exports.

2. Haga clic en **Disable**.

Creación de una exportación

Puede utilizar el botón Create del administrador de sistemas de Data Domain en la vista NFS o utilice el asistente de configuración para especificar los clientes NFS que pueden acceder a las áreas `/backup`, `/data/col1/backup`,`/ddvar`, `/ddvar/core`, o al área `/ddvar/ext` si existe.

Un sistema Data Domain admite un máximo de 2048 exportaciones[2] y el número de conexiones se escala en función de la memoria del sistema.

Nota

Debe asignar acceso de clientes a cada exportación por separado y eliminar el acceso de cada exportación por separado. Por ejemplo, un cliente puede ser eliminado de `/ddvar` y aun así tener acceso a `/data/col1/backup`.

⚠ PRECAUCIÓN

Si es necesario implementar la replicación, un solo sistema Data Domain de destino único puede recibir respaldos de clientes CIFS y clientes NFS, mientras se usen directorios o MTrees por separado para cada uno. No combine datos de CIFS y NFS en la misma área.

Procedimiento

1. Seleccione **Protocols > NFS**.

   Se abre la vista NFS y muestra la pestaña Exports.

2. Haga clic en **Create**.
3. Escriba el nombre de ruta en el cuadro de texto Directory Path (por ejemplo, `/data/col1/backup/dir1`).

   Nota

   `col1` usa la letra L en minúscula seguida del número 1.

4. En el área Clients, seleccione un cliente existente o haga clic en el ícono **+** para crear un cliente.

   Se mostrará el cuadro de diálogo Client.

   a. Ingrese un nombre de servidor en el cuadro de texto.

      Ingrese nombres de dominio calificados, nombres de host o direcciones IP. Un único asterisco (`*`) como comodín indica que todos los servidores de respaldo serán utilizados como clientes.

      Nota

      Los clientes a los que se otorga acceso al directorio `/data/col1/backup` tienen acceso a todo el directorio. Un cliente al que se le permitió el acceso al subdirectorio `/data/col1/backup` solo tiene acceso a ese subdirectorio.

      - Un cliente puede ser el nombre del host de un dominio totalmente calificado, una dirección IP IPv4 o IPv6, una dirección IPv4 con una máscara de red o longitud de prefijo, una dirección IPv6 con longitud de prefijo, el nombre de netgroup de NIS con el prefijo `@`, o un asterisco (`*`) como comodín con un nombre de dominio, por ejemplo, `*.yourcompany.com`.
      - Un cliente agregado a un subdirectorio bajo `/data/col1/backup` solo tiene acceso a ese subdirectorio.

2. Puede verse afectado por las limitaciones de hardware.

- Ingrese un asterisco (*) como la lista de clientes para dar acceso a todos los clientes de la red.

b. Seleccione las casillas de verificación de las opciones de NFS para el cliente.

General:

- Permiso de solo lectura (ro).
- Permitir conexiones desde puertos por debajo de 1024 (seguro) (predeterminado).

UID / GID anónimo:

- Solicitudes de mapeo desde UID (identificador de usuario) o GID (identificador de grupo) 0 a los UID/GID anónimos (root _squash).
- Mapear todas las solicitudes de usuario a UID/GID anónimo (all _squash).
- Use el UID o GID anónimo predeterminado.

Modos válidos de autenticación Kerberos:

- Conexiones no autenticadas (sec=sys). Seleccionar que no se utilice la autenticación.
- Conexiones autenticados (sec=krb5).

Nota

La integridad y la privacidad son compatibles, aunque podrían disminuir el rendimiento considerablemente.

c. Haga clic en **OK**.

5. Haga clic en **OK** para crear la exportación.

Modificación una exportación

Cambie la ruta al directorio, el nombre de dominio y otras opciones utilizando la GUI.

Procedimiento

1. Seleccione **Protocols** > **NFS**.

   Se abre la vista NFS y muestra la pestaña Exports.

2. Haga clic en la casilla de verificación de una exportación en la tabla NFS Exports.
3. Haga clic en **Modify**.
4. Modifique nombre de ruta en el cuadro de texto Directory Path.
5. En el área Clients, seleccione otro cliente y haga clic en el ícono de lápiz (modificación) o en el ícono **+** para crear un cliente

   a. Ingrese un nombre de servidor en el cuadro de texto Client.

   Ingrese nombres de dominio calificados, nombres de host o direcciones IP. Un único asterisco (*) como comodín indica que todos los servidores de respaldo serán utilizados como clientes.

Nota

Los clientes a los que se otorga acceso al directorio `/data/col1/backup` tienen acceso a todo el directorio. Un cliente al que se le permitió el acceso al subdirectorio `/data/col1/backup` solo tiene acceso a ese subdirectorio.

- Un cliente puede ser el nombre del host de un dominio totalmente calificado, una dirección IP IPv4 o IPv6, una dirección IPv4 con una máscara de red o longitud de prefijo, una dirección IPv6 con longitud de prefijo, el nombre de netgroup de NIS con el prefijo `@`, o un asterisco (`*`) como comodín con un nombre de dominio, por ejemplo, `*`.yourcompany.com.
  Un cliente agregado a un subdirectorio bajo `/data/col1/backup` solo tiene acceso a ese subdirectorio.
- Ingrese un asterisco (`*`) como la lista de clientes para dar acceso a todos los clientes de la red.

b. Seleccione las casillas de verificación de las opciones de NFS para el cliente.

General:

- Permiso de solo lectura (ro).
- Permitir conexiones desde puertos por debajo de 1024 (seguro) (predeterminado).

UID / GID anónimo:

- Solicitudes de mapeo desde UID (identificador de usuario) o GID (identificador de grupo) 0 a los UID/GID anónimos (root _squash).
- Mapear todas las solicitudes de usuario a UID/GID anónimo (all _squash).
- Use el UID o GID anónimo predeterminado.

Modos válidos de autenticación Kerberos:

- Conexiones no autenticadas (sec=sys). Seleccionar que no se utilice la autenticación.
- Conexiones autenticados (sec=krb5).

Nota

La integridad y la privacidad no son compatibles.

c. Haga clic en **Aceptar**.

6. Haga clic en **OK** para modificar la exportación.

Creación de una exportación a partir de una exportación existente

Cree una exportación a partir de una exportación existente y luego modifíquela según considere necesario.

Procedimiento

1. En la pestaña NFS Exports, haga clic en la casilla de verificación de la exportación que desea utilizar como origen.

2. Haga clic en **Create From**.
3. Modifique la información de exportación, tal como se describe en la sección sobre cómo modificar una exportación.

Eliminación de una exportación

Elimine una exportación desde la tabla NFS Exports.

Procedimiento

1. En la pestaña NFS Exports, haga clic en la casilla de verificación de la exportación que desea eliminar.
2. Haga clic en **Delete**.
3. Haga clic en **OK** y en **Close** para eliminar la exportación.

Visualización de la información de NFS

En los temas de esta sección se describe cómo usar DD System Manager para monitorear el estado de clientes NFS y la configuración de NFS.

Visualización del estado de NFS

Verifique si NFS está habilitado y si Kerberos también lo está.

Procedimiento

- Haga clic en **Protocols** > **NFS**.

  El panel superior muestra el estado del funcionamiento de NFS; por ejemplo, si NFS está actualmente habilitado y ejecutándose, y si el modo de Kerberos está habilitado.

  Nota

  Haga clic en Configure para ver la pestaña **Administration** > **Access** > **Authentication**, donde puede configurar la autenticación de Kerberos.

Visualización de exportaciones de NFS

Consulte la lista de clientes que tienen el acceso al Sistema de Data Domain permitido.

Procedimiento

1. Haga clic en **Protocols** > **NFS**.

   La vista de exportaciones muestra una tabla de las exportaciones de NFS que están configuradas para el sistema Data Domain y la ruta de montaje, el estado y las opciones de NFS para cada exportación.

2. Haga clic en una exportación en la tabla para rellenar el área Detailed Information, debajo de la tabla de exportaciones.

   Además de la ruta del directorio, las opciones configuradas, y el estado de la exportación, el sistema muestra una lista de clientes.

   Utilice cuadro de texto Filter By para ordenar por ruta de montaje.

   Haga clic en **Update** para que el sistema actualice la tabla y use los filtros suministrados.

Haga clic en **Reset** para que el sistema borre los filtros de ruta y de cliente.

Visualización de clientes NFS activos

Puede visualizar todos los clientes que se han conectado en los últimos 15 minutos y su ruta de montaje.

Procedimiento

- Seleccione la pestaña **Protocols** > **NFS** > **Active Clients** tab.

  Se mostrará la vista Active Clients, que incluye todos los clientes que se han conectado en los últimos 15 minutos y su ruta de montaje.

  Use los cuadros de texto Filter By para ordenar por ruta de montaje y nombre de cliente.

  Haga clic en **Update** para que el sistema actualice la tabla y use los filtros suministrados.

  Haga clic en **Reset** para que el sistema borre los filtros de ruta y de cliente.

Integración de un DDR en un dominio Kerberos

Establezca el nombre de dominio, el nombre de host y el servidor DNS para el DDR.

Habilite el DDR para utilizar el servidor de autenticación como un Key Distribution Center (para UNIX) y como Distribution Center (para Windows Active Directory).

⚠ PRECAUCIÓN

Los ejemplos proporcionados en esta descripción son específicos para el sistema operativo (OS) utilizado para desarrollar este ejercicio. Debe utilizar los comandos específicos de su sistema operativo.

Nota

Para el modo UNIX Kerberos, un archivo keytab debe ser transferido desde el servidor del Centro de distribución de claves (KDC), donde se genera, a la DDR. De utilizar más de un DDR, cada DDR requerirá un archivo keytab por separado. El archivo keytab contiene una seña secreta compartida entre el servidor KDC y el DDR.

Nota

Al utilizar un KDC de UNIX, el servidor DNS no tiene necesidad de ser el servidor KDC, puede ser un servidor separado.

Procedimiento

1. Establezca el nombre de host y el nombre de dominio para el DDR, utilizando comandos de DDR.

   ```
   net set hostname <host>
   ```

   ```
   net set {domainname <local-domain-name>}
   ```

   Nota

   El nombre de host es el nombre del DDR.

2. Configure el NFS principal (nodo) para el DDR en el Key Distribution Center (KDC).

   Ejemplo:
   addprinc nfs/hostname@realm

   Nota

   Hostname es el nombre para el DDR.

3. Verifique que haya entradas nfs agregadas como principales en el KDC.

   Ejemplo:
   listprincs
   ```
   nfs/hostname@realm
   ```

4. Añade el DDR principal a un archivo keytab.

   Ejemplo:
   ktadd <keytab_file> nfs/hostname@realm

5. Verifica que haya un archivo keytab de nfs configurado en el KDC.

   Ejemplo:
   klist -k <keytab_file>

   Nota

   El <keytab_file> es el archivo keytab utilizado para configurar las claves en un paso anterior.

6. Copie el archivo keytab desde la ubicación donde las claves para el NFS DDR son generadas para el DDR en el directorio /ddvar/.

   Tabla 117 Destino del keytab

Copiar archivos desde:	Copiar archivo a:
<keytab_file> (El archivo keytab configurado en un paso anterior).	/ddvar/

7. Establezca el dominio en el DDR, mediante el siguiente comando DDR:

   authentication kerberos set realm <home realm> kdc-type <unix, windows.> kdcs <IP address of server>

8. Cuando el kdc-type es UNIX, importe el archivo keytab desde /ddvar/ to /ddr/etc/, donde lo espera el archivo de configuración de Kerberos. Utilice el siguiente comando DDR siguiente para copiar el archivo:

   authentication kerberos keytab import

   AVISO

   Este paso es necesario solamente cuando el tipo de kdc es UNIX.

   Configuración de Kerberos acaba de finalizar.

9. Para agregar un punto de montaje de NFS para utilizar Kerberos, use el comando nfs para agregar.

Consulte la *Guía de referencia de comandos de Data Domain Operating System* para obtener más información.

10. Agregue principales de host, de NFS y de usuarios relevantes para cada cliente NFS en el Key Distribution Center (KDC).

    Ejemplo: **listprincs**

    ```
    host/hostname@realm
    nfs/hostname@realm
    root/hostname@realm
    ```

11. Para cada cliente NFS, importe todos sus principales en un archivo keytab en el cliente.

    Ejemplo:

    ktadd -k <keytab_file> host/hostname@realm

    ktadd -k <keytab_file> nfs/hostname@realm

Agregar y eliminar servidores KDC después de la configuración inicial

Después de haber integrado un DDR en un dominio Kerberos y, por lo tanto, permitiendo al DDR utilizar el servidor de autenticación como Key Distribution Center (para UNIX) y como Distribution Center (para Windows Active Directory), puede utilizar el siguiente procedimiento para agregar o eliminar servidores KDC.

Procedimiento

1. Una al DDR con un servidor de Windows Active Directory (AD) o Key Distribution Center de UNIX (KDC).

   authentication kerberos set realm <home-realm> kdc-type {windows [kdcs <kdc-list>] | unix kdcs <kdc-list>}

   Ejemplo: **authentication kerberos set realm krb5.test kdc-type unix kdcs nfskrb-kdc.krb5.test**

   Este comando une el sistema al dominio krb5.test y habilita la autenticación Kerberos para los clientes NFS.

   Nota

   Un keytab generado en este KDC debe existir en el DDR para poder autenticarse usando Kerberos.

2. Verifique la configuración de la autenticación Kerberos.

   authentication kerberos show config

   ```
   Home Realm:          krb5.test
   KDC List:            nfskrb-kdc.krb5.test
   KDC Type:            unix
   ```

3. Agregar un segundo servidor KDC

   authentication kerberos set realm <home-realm> kdc-type {windows [kdcs <kdc-list>] | unix kdcs <kdc-list>}

   Ejemplo: **authentication kerberos set realm krb5.test kdc-type unix kdcs ostqa-sparc2.krb5.test nfskrb-kdc.krb5.test**

Nota

Un keytab generado en este KDC debe existir en el DDR para poder autenticarse usando Kerberos.

4. Verifique que se agreguen dos servidores KDC.

   authentication kerberos show config

```
Home Realm:           krb5.test
KDC List:             ostqa-sparc2.krb5.test, nfskrb-
kdc.krb5.test
KDC Type:             unix
```

5. Visualice el valor de la clave de configuración de Kerberos.

   reg show config.keberos

```
config.kerberos.home_realm = krb5.test
config.kerberos.home_realm.kdc1 = ostqa-sparc2.krb5.test
config.kerberos.home_realm.kdc2 = nfskrb-kdc.krb5.test
config.kerberos.kdc_count = 2
config.kerberos.kdc_type = unix
```

6. Elimine un servidor KDC.

   Elimine un servidor KDC utilizando el comando **authentication kerberos set realm <home-realm> kdc-type {windows [kdcs <kdc-list>] | unix kdcs <kdc-list>}** sin enumerar el servidor KDC que desea eliminar. Por ejemplo, si los servidores KDC existentes son kdc1, kdc2 y kdc3, y desea eliminar kdc2 del dominio, puede utilizar el siguiente ejemplo:

   authentication kerberos set realm <realm-name> kdc-type <kdc_type> kdcs kdc1,kdc3

CAPÍTULO 10

NFSv4

Este capítulo incluye:

- Introducción a NFSv4 296
- Descripción general de mapeos de ID 297
- Formatos externos 298
- Formatos de identificadores internos 299
- Cuando se produce el mapeo de ID 299
- Interoperabilidad de NFSv4 y CIFS/SMB 301
- Referencias de NFS 302
- NFSv4 y alta disponibilidad 303
- Espacios de nombres globales de NFSv4 304
- Configuración de NFSv4 305
- Kerberos y NFSv4 306
- Habilitación de Active Directory 309

Introducción a NFSv4

Dado que los clientes NFS utilizan cada vez más NFSv4.x como el nivel predeterminado de protocolo NFS, los sistemas Data Domain ahora pueden emplear NFSv4 en vez de exigir al cliente que opere en un modo de compatibilidad con versiones anteriores.

En los sistemas Data Domain, los clientes pueden operar en ambientes combinados en los que NFSv4 y NFSv3 deben poder acceder a las mismas exportaciones NFS.

El servidor NFS Data Domain puede configurarse para admitir NFSv4 y NFSv3, según los requisitos del sitio. Se puede hacer que cada exportación NFS esté disponible solo para los clientes NFSv4, solo para los clientes NFSv3 o para ambos.

Varios factores pueden influir en la elección de NFSv4 o NFSv3:

- Compatibilidad con clientes de NFS
  Algunos clientes de NFS pueden admitir solamente NFSv3 o NFSv4, o pueden funcionar mejor con una versión.
- Requisitos de operacionales
  Es posible que una empresa utilice estrictamente NFSv4 o NFSv3 de manera estándar.
- Seguridad
  Si se requiere más seguridad, NFSv4 proporciona un mayor nivel de seguridad que NFSv3, incluidas las ACL y la configuración extendida de propietarios y de grupos.
- Requisitos de características
  Si necesita bloqueo de rango de bytes o archivos UTF-8, debe elegir NFSv4.
- Submontajes de NFSv3
  Si la configuración existente utiliza submontajes de NFSv3, es posible que NFSv3 sea la opción adecuada.

NFSv4 comparado con NFSv3 en sistemas Data Domain

NFSv4 proporciona funcionalidades y funciones mejoradas en comparación con NFSv3.

La siguiente tabla compara las funciones de NFSv3 con las de NFSv4.

Tabla 118 NFSv4 frente a NFSv3

Función	NFSv3	NFSv4
Sistema de archivos de red basado en estándares	Sí	Sí
Compatibilidad con Kerberos	Sí	Sí
Kerberos con LDAP	Sí	Sí
Informes de cuotas	Sí	Sí
Múltiples exportaciones con listas de acceso basadas en clientes	Sí	Sí
Mapeo de ID	Sí	Sí
Compatibilidad con caracteres UTF-8	No	Sí

Tabla 118 NFSv4 frente a NFSv3 (continuación)

Función	NFSv3	NFSv4
Listas de control de acceso (ACL) basadas en archivos/ directorios	No	Sí
Grupo/propietario extendido (OWNER@)	No	Sí
Bloqueo de recurso compartido de archivos	No	Sí
Bloqueo de rango de bytes	No	Sí
Integración de DD-CIFS (bloqueo, ACL, AD)	No	Sí
Aperturas y recuperación de archivos con información de estado	No	Sí
Espacio de nombres global y pseudosistemas de archivos	No	Sí
Espacio de nombres de varios sistemas mediante derivaciones	No	Sí

Puertos NFSv4

Puede habilitar o deshabilitar NFSv4 y NFSv3 de manera independiente. Además, puede transferir las versiones de NFS a distintos puertos; no es necesario que ambas versiones ocupen el mismo puerto.

Con NFSv4, no necesita reiniciar el sistema de archivos de Data Domain si cambias los puertos. Solo se requiere un reinicio de NFS en estos casos.

Al igual que NFSv3, NFSv4 funciona en el puerto 2049 de manera predeterminada si está habilitado.

NFSv4 no utiliza el asignador de puertos (puerto 111) ni mountd (puerto 2052).

Descripción general de mapeos de ID

NFSv4 identifica propietarios y grupos por un formato externo común, por ejemplo `joe@example.com`. Estos formatos comunes se conocen como identificadores, o ID.

Los identificadores se almacenan en un servidor NFS y utilizan representaciones internas como ID 12345 o ID S-123-33-667-2. La conversión entre identificadores internos y externos se conoce como mapeo de ID.

Los identificadores se asocian con lo siguiente:

- Propietarios de archivos y directorios
- Grupos de propietarios de archivos y directorios
- Entradas en listas de control de acceso (ACL)

Los sistemas Data Domain utilizan un formato interno común para los protocolos NFS y CIFS/SMB, lo que permite que los archivos y directorios se compartan entre NFS y CIFS/SMB. Cada protocolo convierte el formato interno en su propio formato externo con su propio mapeo de ID.

Formatos externos

El formato externo para identificadores de NFSv4 sigue estándares NFSv4 (por ejemplo, RFC-7530 para NFSv4.0). Además, se admiten formatos adicionales para fines de interoperabilidad.

Formatos de identificadores estándar

Los identificadores externos estándar para NFSv4 tienen el formato *identifier@domain*. Este identificador se utiliza para propietarios de NFSv4, grupos de propietarios y entradas de control de acceso (ACE). El dominio debe coincidir con el dominio NFSv4 configurado que se estableció usando el comando `nfs option`.

El siguiente ejemplo de CLI establece el dominio NFSv4 en `mycorp.com` para el servidor NFS Data Domain:

```
nfs option set nfs4-domain mycorp.com
```

Consulte la documentación específica del cliente que tiene para configurar al dominio NFS del cliente. Según el sistema operativo, tal vez necesite actualizar un archivo de configuración (por ejemplo, `/etc/idmapd.conf`) o utilizar una herramienta administrativa del cliente.

Nota

Si no establece el valor predeterminado, seguirá el nombre DNS para el sistema Data Domain.

Nota

El sistema de archivos debe reiniciarse después de cambiar el dominio DNS para que nfs4-domain se actualice automáticamente.

Identificadores extendidos de ACE

Para las entradas de ACE de la ACL, los servidores NFS Data Domain también soportan los siguientes identificadores extendidos de ACE NFSv4 estándar definidos por la RFC NFSv4:

- OWNER@: El propietario actual del archivo o directorio.
- GROUP@: El grupo del propietario actual del archivo o directorio.
- Los identificadores especiales INTERACTIVE@, NETWORK@, DIALUP@, BATCH@, ANONYMOUS@, AUTHENTICATED@, SERVICE@.

Formatos alternativos

Para permitir la interoperabilidad, los servidores NFSv4 en sistemas Data Domain admiten algunos formatos de identificadores alternativos para entrada y salida.

- Identificadores numéricos; por ejemplo, “12345”.
- Identificadores de seguridad (SID) compatibles con Windows expresados como “S-NNN-NNN-...”.

Consulte las secciones sobre mapeo de entrada y mapeo de salida para obtener más información acerca de las restricciones de estos formatos.

Formatos de identificadores internos

El sistema de archivos de Data Domain almacena identificadores con cada objeto (archivo o directorio) en el sistema de archivos. Todos los objetos tienen un ID de usuario (UID) y un ID de grupo (GID) numéricos. Estos, utilizados con un conjunto de bits de modo, permiten la identificación de UNIX/Linux y los controles de acceso tradicionales.

Los objetos creados por el protocolo CIFS/SMB (o por el protocolo NFSv4 cuando se habilitan las ACL NFSv4) también disponen de un descriptor de seguridad (SD) extendido. Cada SD contiene lo siguiente:

- Un identificador de seguridad (SID) de propietario
- Un SID de grupo de propietarios
- Una ACL discrecional (DACL)
- (Opcional) Un sistema ACL (SACL)

Cada SID contiene un ID relativo (RID) y un dominio distinto, de manera similar a los SID de Windows. Consulte la sección sobre la interoperabilidad de CIFS y NFSv4 para obtener más información sobre los SID y su mapeo.

Cuando se produce el mapeo de ID

El servidor NFSv4 Data Domain realiza el mapeo en las siguientes circunstancias:

- Mapeo de entrada
  El servidor NFS Data Domain recibe un identificador de un cliente NFSv4. Consulte Mapeo de entrada en la página 299.
- Mapeo de salida:
  Un identificador se envía desde el servidor NFS Data Domain al cliente NFSv4. Consulte Mapeo de salida en la página 300.
- Mapeo de credenciales
  Las credenciales de cliente RPC se mapean a una identidad interna para control de acceso y otras operaciones. Consulte Mapeo de credenciales en la página 300.

Mapeo de entrada

El mapeo de entrada se realiza cuando un cliente NFSv4 envía un identificador al servidor NFSv4 Data Domain, por ejemplo, para configurar el propietario o el grupo de propietarios de un archivo. El mapeo de entrada es distinto del mapeo de credenciales. Para obtener más información sobre el mapeo de credenciales, consulte xxxx.

Los identificadores de formato estándares, como `joe@mycorp.com`, se convierten en un UID/GID interno según las reglas de conversión configuradas. Si están habilitadas las ACL NFSv4, también se generará un SID basado en las reglas de conversión configuradas.

Los identificadores numéricos (por ejemplo, “12345”) se convierten directamente en el UID/GID correspondiente si el cliente no está utilizando la autenticación de Kerberos. Si se utiliza Kerberos, se generará un error de acuerdo con lo recomendado según el estándar NFSv4. Si están habilitadas las ACL NFSv4, se generará un SID basado en las reglas de conversión.

Los SID de Windows (por ejemplo, “S-NNN-NNN-...”) se validan y se convierten directamente en los SID correspondientes. Se generará un UID/GID basado en las reglas de conversión.

Mapeo de salida

El mapeo de salida se realiza cuando el servidor NFSv4 envía un identificador al cliente NFSv4; por ejemplo, si el servidor devuelve el propietario o el grupo de propietarios de un archivo.

1. Si ha configurado, la salida podría ser el identificador numérico.
   Esto puede ser útil para clientes NFSv4 que no están configurados para el mapeo de ID (por ejemplo, algunos clientes Linux).
2. Se intenta el mapeo utilizando los servicios de mapeo configurados, (por ejemplo, NIS o Active Directory).
3. La salida es una cadena numérica de ID o SID si el mapeo falla y la configuración está permitida.
4. De lo contrario, se devuelve nobody.

nfs option *nfs4-idmap-out-numeric* configura el mapeo de salida:

- Si **nfs option *nfs4-idmap-out-numeric*** se establece en **map-first**, se intentará el mapeo. En caso de error, la salida es una cadena numérica si está permitido. Este es el valor predeterminado.
- Si **nfs option *nfs4-idmap-out-numeric*** se establece en **always**, la salida siempre será una cadena numérica si está permitido.
- Si **nfs option *nfs4-idmap-out-numeric*** se establece en **never**, se intentará el mapeo. En caso de error, **nobody@nfs4-domain** es la salida.
  Si la conexión de RPC utiliza GSS/Kerberos, nunca se permite una cadena numérica y **nobody@nfs4-domain** es la salida.

En el siguiente ejemplo, se configura el servidor NFS Data Domain para que siempre intente que la salida sea una cadena numérica. Para Kerberos, se devuelve el nombre nobody:

```
nfs option set nfs4-idmap-out-numeric always
```

Mapeo de credenciales

El servidor NFSv4 proporciona credenciales para el cliente NFSv4.

Estas credenciales ejecutan las siguientes funciones:

- Determinar la política de acceso para la operación; por ejemplo, la capacidad de leer un archivo.
- Determinar el propietario predeterminado y grupo de propietarios para nuevos archivos y directorios.

Las credenciales enviadas desde el cliente pueden `john_doe@mycorp.com`, o credenciales del sistema, como `UID=1000, GID=2000`. Las credenciales del sistema especifican un UID/GID junto con ID de grupo auxiliares.

Si se deshabilitan las ACL de NFSv4, el UID/GID y los ID de grupo auxiliares se utilizan para las credenciales.

Si están habilitadas las ACL de NFSv4, los servicios de mapeo configurados se utilizan para crear un descriptor de seguridad extendido para las credenciales:

- Los SID para el propietario, el grupo de propietarios y el grupo auxiliar mapeados y agregados al descriptor de seguridad (SD).
- Los privilegios de credenciales, si corresponde, se agregan al SD.

Interoperabilidad de NFSv4 y CIFS/SMB

Si bien los descriptores de seguridad utilizados por NFSv4 y CIFS son similares desde el punto de vista de mapeo de ID, existen algunas diferencias.

Debe tener en cuenta lo siguiente para garantizar una interoperabilidad óptima:

- Active Directory debe estar configurado para CIFS y NFSv4, y el a mapeador de ID de NFS debe estar configurado para utilizar Active Directory para el mapeo de ID.
- Si está usando ACL de CIFS ampliamente, por lo general, puede mejorar la compatibilidad habilitando también ACL de NFSv4.
  - La habilitación de ACL de NFSv4 permite mapear credenciales NFSv4 a los SID apropiados durante la evaluación del acceso a DACL.
- El servidor CIFS recibe credenciales del cliente CIFS, incluidos los privilegios de usuario y la ACL predeterminada.
  - Por el contrario, el servidor NFSv4 recibe un conjunto más limitado de credenciales y crea credenciales en tiempo de ejecución mediante su mapeador de ID. Debido a esto, el sistema de archivos puede ver diferentes credenciales.

Integración con Active Directory de CIFS/SMB

El servidor NFSv4 Data Domain puede configurarse para utilizar la configuración de Windows Active Directory que se establece con el servidor CIFS Data Domain.

El sistema Data Domain se mapea para utilizar Active Directory si es posible. Esta funcionalidad está deshabilitada de forma predeterminada, pero puede habilitarla utilizando el siguiente comando:

```
nfs option set nfs4-idmap-active-directory enabled
```

DACL predeterminada para NFSv4

NFSv4 establece una DACL (lista de control de acceso discrecional) predeterminada diferente de la DACL predeterminada proporcionada por CIFS.

Solo OWNER@, GROUP@ y EVERYONE@ se definen en la DACL predeterminada de NFSv4. Puede utilizar la herencia de ACL para agregar automáticamente ACE de CIFS importantes de forma predeterminada si es adecuado.

SID predeterminados del sistema

Archivos y directorios creados por NFSv3 y NFSv4 sin ACL, usan el dominio predeterminado del sistema, a veces denominado el dominio de UNIX predeterminado:

- Los SID de usuario en el dominio del sistema tienen el formato `S-1-22-1-N`, donde N es el UID.
- Los SID de grupo en el dominio del sistema tienen el formato `S-1-22-2-N`, donde N es el GID.
  Por ejemplo, un usuario con `UID 1234` tendría un SID de propietario `S-1-22-1-1234`.

Identificadores comunes en SID y ACL de NFSv4

El identificador EVERYONE@ y otros identificadores especiales (por ejemplo, BATCH@) en ACL de NFSv4 usan los SID de CIFS equivalentes y son compatibles.

Los identificadores WNER@ y GROUP@ no tienen ninguna correspondencia directa en CIFS; aparecen como el propietario actual y el grupo actual de propietarios del archivo o directorio.

Referencias de NFS

La función de referencia permite que un cliente NFSv4 acceda a una exportación (o sistema de archivos) en una o varias ubicaciones. Las ubicaciones pueden ser en el mismo servidor NFS o en diferentes servidores NFS y pueden utilizar la misma ruta o una ruta diferente para llegar a la exportación.

Como las referencias son una función de NFSv4, se aplican solo a los montajes NFSv4.

Las referencias pueden hacerse a cualquier servidor que utilice NFSv4 o posterior, incluidos los siguientes:

- Un sistema Data Domain ejecuta NFS con NFSv4 habilitado
- Otros servidores que admiten NFSv4, incluidos sistemas VNX, dispositivos NAS y servidores Linux.

Una referencia puede utilizar un punto de exportación NFS con o sin una ruta subyacente actual en el sistema de archivos Data Domain.

Las exportaciones NFS con referencias pueden montarse mediante NFSv3, pero los clientes NFSv3 no se redireccionarán ya que las referencias son una función de NFSv4. Esta función es útil en sistemas de escalamiento horizontal para permitir el redireccionamiento de exportaciones en el nivel de administración de archivos.

Ubicaciones de referencia

Las referencias de NFSv4 siempre tienen una o más ubicaciones.

Estas ubicaciones incluyen lo siguiente:

- Una ruta en un servidor NFS remoto al sistema de archivos mencionado.
- Una o más direcciones de red del servidor que permiten que el cliente alcance al servidor NFS remoto.

Por lo general, cuando múltiples direcciones del servidor se asocian a la misma ubicación, esas direcciones se encuentran en el mismo servidor NFS.

Nombres de ubicación de referencia

Puede nombrar cada ubicación de referencia en una exportación de NFS. Puede utilizar el nombre para acceder a la referencia, así como modificarla o eliminarla.

Un nombre de referencia puede contener un máximo de 80 caracteres de los siguientes conjuntos de caracteres:

- a-z
- A-Z
- 0-9
- "."

- ","
- "_"
- "-"

Nota

Puede incluir espacios siempre que esos espacios estén integrados dentro del nombre. Si utiliza espacios incorporados, debe incluir el nombre completo entre comillas dobles.

Los nombres que comienzan con "." se reservan para la creación automática por parte del sistema Data Domain. Puede eliminar estos nombres, pero no puede crear ni modificar mediante la interfaz de la línea de comandos (CLI) o los servicios de administración del sistema (SMS).

Sistemas de escalamiento horizontal y referencias

Las ubicaciones y referencias de NFSv4 pueden mejorar el acceso si usted está realizando un escalamiento horizontal de sus sistemas Data Domain

Dado que su sistema Data Domain puede contener un espacio de nombres global o no, los dos escenarios siguientes describen cómo puede usar referencias de NFSv4:

- Su sistema Data Domain no contiene un espacio de nombres global.
  - Puede usar referencias de NFSv4 para crear ese espacio de nombres global. Los administradores del sistema pueden crear estos espacios de nombres globales, o usted puede utilizar referencias de creación de elementos del administrador del sistema inteligente según sea necesario.
- Su sistema Data Domain ya tiene un espacio de nombres global.
  - Si su sistema tiene un espacio de nombres global con MTrees ubicados en nodos específicos, pueden crearse referencias de NFS para redirigir el acceso a esos MTrees a los nodos agregados al sistema de escalamiento horizontal. Puede crear estas referencias o hacer que se realicen automáticamente en NFS si la información de administración de archivos o SM necesaria está disponible. Para obtener más información sobre MTrees, consulte la *Guía de administración de Data Domain Operating System*.

NFSv4 y alta disponibilidad

Con NFSv4, las exportaciones del protocolo, por ejemplo `/data/col1/<mtree>`, se espejean en una configuración de alta disponibilidad (HA). Sin embargo, las exportaciones de configuración como `/ddvar` no se espejean.

El sistema de archivos `/ddvar` es único para cada nodo de un par de alta disponibilidad. Como resultado, las exportaciones de `/ddvar` y sus listas de acceso de cliente asociadas no se espejean en el nodo en espera en un ambiente de alta disponibilidad.

La información en `/ddvar` se convierte en obsoleta cuando el nodo activo realiza una conmutación por error al nodo en espera. Todos los permisos de clientes otorgados a `/ddvar` en el nodo activo original deben recrearse en el nuevo nodo activo después de que se produce una conmutación por error.

También debe agregar cualquier exportación /ddvar adicional y sus clientes (por ejemplo, `/ddvar/core`) que se haya creado en el nodo activo original al nuevo nodo después de que se produce una conmutación por error.

Por último, cualquier exportación de `/ddvar` deseada debe desmontarse del cliente y volver a montarse después de que se produce una conmutación por error.

Espacios de nombres globales de NFSv4

El servidor NFSv4 proporciona un árbol de directorio virtual conocido como PseudoFS para conectar exportaciones NFS en un conjunto de rutas que permita hacer búsquedas.

El uso de PseudoFS distingue NFSv4 de NFSv3, que utiliza el protocolo auxiliar MOUNTD.

En la mayoría de las configuraciones, el cambio de NFSv3 MOUNTD al espacio de nombres global NFSv4 es transparente. El cliente y el servidor NFSv4 se encargan de realizar este cambio de manera automática.

Espacios de nombres globales de NFSv4 y submontajes de NFSv3

Si utiliza submontajes de exportación de NFSv3, es posible que la característica de los espacios de nombres globales de NFSv4 impidan que los submontajes se vean en el montaje de NFSv4.

Ejemplo 1 Exportaciones principales y exportaciones de submontajes de NFSv3

Si NFSv3 tiene una exportación principal y una exportación de submontaje, es posible que estas exportaciones usen los mismos clientes de NFSv3, pero tengan diferentes niveles de acceso:

Tabla 119 Exportaciones principales y exportaciones de submontajes de NFSv3

Exportación	Ruta	Cliente	Opciones
Mt1	`/data/col1/mt1`	cliente1.ejemplo.com	ro
Mt1-sub	`/data/col1/mt1/subdir`	cliente1.ejemplo.com	rw

En la tabla anterior, se aplica lo siguiente para NFSv3:

- Si cliente1.ejemplo.com monta /data/col1/mt1, el cliente obtiene acceso de solo lectura.
- Si cliente1.ejemplo.com monta /data/col1/mt1/subdir, el cliente obtiene acceso de lectura/escritura.

NFSv4 funciona de la misma manera con respecto a las rutas de exportación nivel superior. Para NFSv4, cliente1.ejemplo.com navega en NFSv4 PseudoFS hasta llegar a la ruta de exportación de nivel más alto, `/data/col1/mt1`, donde obtiene acceso de solo lectura.

Sin embargo, debido a que la exportación se seleccionó, la exportación de submontaje (Mt1-sub) no es parte de PseudoFS para el cliente, y no se proporciona acceso de lectura/escritura.

Mejor práctica
Si su sistema utiliza submontajes de exportaciones de NFSv3 para otorgar acceso de lectura/escritura al cliente según la ruta de montaje, debe tener en cuenta esto antes de usar NFSv4 con estas exportaciones de submontajes.

Con NFSv4, cada cliente tiene un PseudoFS individual.

Tabla 120 Exportaciones de submontajes de NFSv3

Exportación	Ruta	Cliente	Opciones
Mt1	`/data/col1/mt1`	cliente1.ejemplo.com	ro
Mt1-sub	`/data/col1/mt1/subdir`	cliente2.ejemplo.com	rw

Configuración de NFSv4

La configuración predeterminada del sistema Data Domain solo habilita NFSv3. Para utilizar NFSv4, primero debe habilitar el servidor NFSv4.

Habilitación del servidor NFSv4

Procedimiento

1. Entre a `nfs enable version 4` para habilitar NFSv4:

```
# nfs enable version 4
NFS server version(s) 3:4 enabled.
```

2. (Opcional) Si desea deshabilitar NFSv3, ingrese a `nfs disable version 3`.

```
# nfs disable version 3
NFS server version(s) 3 disabled.
NFS server version(s) 4 enabled.
```

Requistos posteriores

Después de habilitar el servidor NFSv4, es posible que deba realizar tareas adicionales de configuración de NFS específicamente para su sitio. Estas tareas pueden incluir la realización de las siguientes acciones en el sistema Data Domain:

- Establecimiento del dominio de NFSv4
- Configuración de la asignación de ID de NFSv4
- Configuración de las ACL (listas de Control de acceso)

Configuración del servidor predeterminado para incluir NFSv4

La opción de comando de NFS de Data Domain **`default-server-version`** controla qué versión de NFS se habilita cuando escribe el comando `nfs enable` sin especificar una versión.

Procedimiento

1. Escriba el comando `nfs option set default-server-version 3:4`:

```
# nfs option set default-server-version 3:4
NFS option 'default-server-version' set to '3:4'.
```

Actualización de exportaciones existentes

Puede actualizar las exportaciones existentes para cambiar la versión de NFS que utiliza su sistema Data Domain.

Procedimiento

1. Escriba el comando `nfs export modify all`:

   ```
   # nfs export modify all clients all options version=número de versión
   ```

   Para asegurar que todos los clientes existentes cuenten con la versión 3, 4 o ambas, puede modificar la versión de NFS con la cadena adecuada. En el siguiente ejemplo, se muestra el NFS modificado que incluye las versiones 3 y 4:

   ```
   #nfs export modify all clients all options version=3:4
   ```

   Para obtener más información acerca del comando `nfs export`, consulte la *Guía de referencia de comandos de Data Domain Operating System*.

Kerberos y NFSv4

Tanto NFSv4 como NFSv3 utilizan el mecanismo de autenticación de Kerberos para proteger la información de identificación.

Kerberos protege la información de identificación contra la suplantación de identidad en paquetes NFS y contra la alteración durante la transferencia al sistema Data Domain.

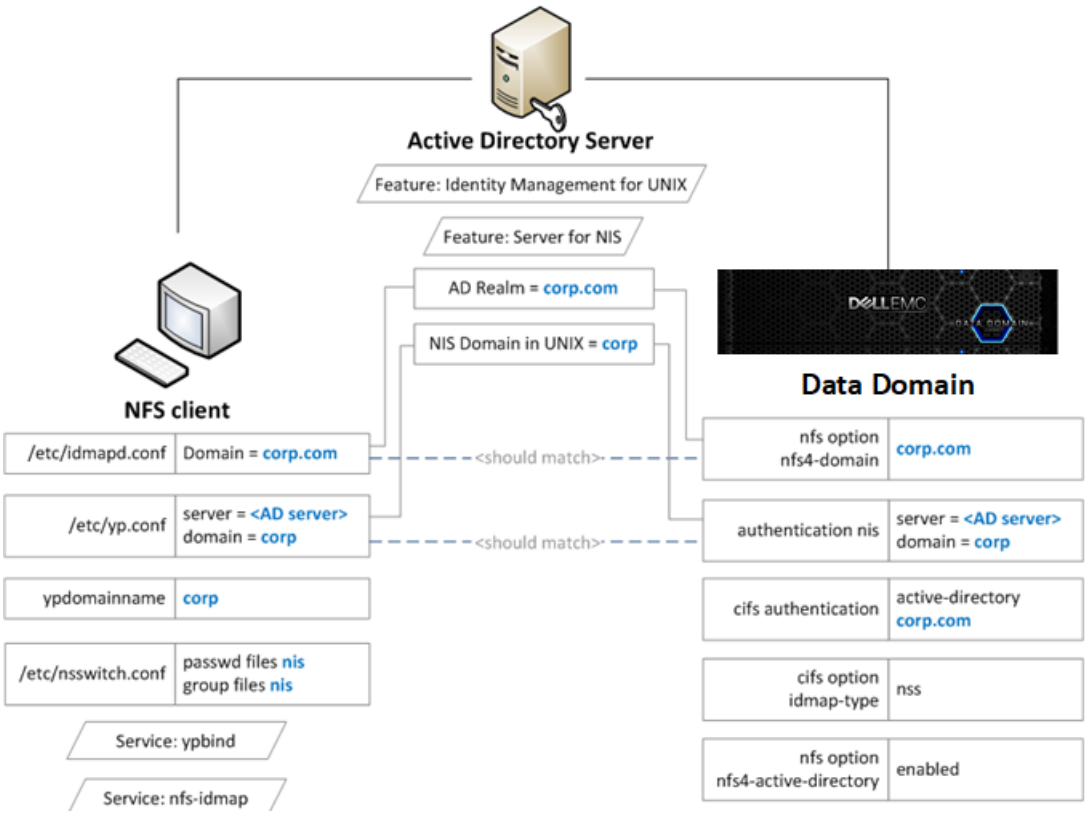
Hay distintos tipos de Kerberos mediante NFS:

- Kerberos 5 (**`sec=krb5`**)
  Use Kerberos para la información de identificación.
- Kerberos 5 con integridad (**`sec=krb5i`**)
  Use Kerberos y verifique la integridad de la carga útil de NFS utilizando una suma de comprobación cifrada.
- Kerberos 5 con seguridad (**`sec=krb5p`**)
  Use Kerberos 5 con integridad y cifre la carga útil completa de NFS.

Nota

Tanto **`krb5i`** como **`krb5p`** pueden causar degradación del rendimiento debido a la sobrecarga de procesamiento adicional en el cliente de NFS y en el sistema Data Domain.

Figura 9 Configuración de Active Directory



Se emplean los comandos existentes utilizados para NFSv3 al configurar el sistema para Kerberos. Consulte el capítulo sobre NFSv3 de la *Guía de referencia de comandos de Data Domain* para obtener más información.

Configuración de Kerberos con un KDC basado en Linux

Antes de comenzar

Debe asegurar que todos los sistemas puedan acceder al centro de distribución de claves (KDC).

Si los sistemas no pueden comunicarse con el KDC, compruebe la configuración del sistema de nombre de dominio (DNS).

Los pasos siguientes le permiten crear archivos keytab para el cliente y el sistema Data Domain:

- En los pasos 1 a 3, creará el archivo keytab para el sistema Data Domain.
- En los pasos 4 a 5, creará el archivo keytab para el cliente.

Procedimiento

1. Cree el principal del servicio de **nfs/<ddr_dns_name>@<realm>**.

   ```
   kadmin.local: addprinc -randkey nfs/ddr12345.<domain-
   name>@<domain-name>
   ```

2. Exporte **nfs/<ddr_dns_name>@<realm>** a un archivo keytab.

   ```
   kadmin.local: ktadd -k /tmp/ddr.keytab nfs/
   ddr12345.corp.com@CORP.COM
   ```

3. Copie el archivo keytab en el sistema Data Domain en la siguiente ubicación:

```
/ddr/var/krb5.keytab
```

4. Cree una de las siguientes entidades de seguridad para el cliente y exporte esa entidad de seguridad al archivo keytab:

```
nfs/<client_dns_name>@<REALM>
root/<client_dns_name>@<REALM>
```

5. Copie el archivo keytab al cliente en la siguiente ubicación:

```
/etc/krb5.keytab
```

Nota

Se recomienda que utilice un servidor NTP para mantener el tiempo sincronizado en todas las entidades.

Configuración del sistema Data Domain para utilizar la autenticación de Kerberos

Procedimiento

1. Configure el dominio de KDC y Kerberos en el sistema Data Domain con el comando `authentication`:

```
# authentication kerberos set realm <dominio> kdc-type unix
kdcs <kdc-server>
```

2. Importe el archivo keytab:

```
# authentication kerberos keytab import
```

3. (Opcional) Configure el servidor NIS introduciendo los siguientes comandos:

```
# authentication nis servers add <server>
# authentication nis domain set <domain-name>
# authentication nis enable
# filesys restart
```

4. (Opcional) Asegúrese de que **`nfs4-domain`** sea igual al dominio deKerberos con el comando `nfs option`:

```
nfs option set nfs4-domain <kerberos-realm>
```

5. Agregue un cliente a una exportación existente agregando **`sec=krb5`** al comando `nfs export add`:

```
nfs export add <export-name> clients * options
version=4,sec=krb5
```

Configuración de clientes

Procedimiento

1. Configure el servidor DNS y verifique que funcionen las búsquedas hacia delante y hacia atrás.
2. Configure el dominio de KDC y Kerberos editando el `/etc/krb5.conf` archivo de configuración.

   Es posible que necesite realizar este paso en función del sistema operativo de cliente que utiliza.
3. Configure el NIS u otro servicio de asignación de nombres externo.
4. (Opcional) Edite el archivo `/etc/idmapd.conf` para asegurar de que sea el mismo que el dominio de Kerberos.

   Es posible que necesite realizar este paso en función del sistema operativo de cliente que utiliza.
5. Verifique que el archivo keytab **`/etc/krb5.keytab`** contenga una entrada para el principal de servicio **`nfs/`** o el principal **`root/`**.

   ```
   [root@fc22 ~]# klist -k
   Keytab name: FILE:/etc/krb5.keytab
   KVNO Principal
   ----
   ----------------------------------------------------------------------
   ----------
   3 nfs/fc22.domain-name@domain-name
   ```
6. Monte la exportación con la opción **`sec=krb5`**.

   ```
   [root@fc22 ~]# mount ddr12345.<domain-name>:/data/col1/
   mtree1 /mnt/nfs4 -o sec=krb5,vers=4
   ```

Habilitación de Active Directory

Configurar la autenticación de Active Directory hace que el sistema Data Domain sea un componente del dominio de Windows Active Directory. Los clientes CIFS y NFS utilizan la autenticación Kerberos.

Procedimiento

1. Únase a un dominio de Active Directory con el comando `cifs set`:

   ```
   # cifs set authentication active-directory <dominio>
   ```

   Kerberos se configura automáticamente en el sistema Data Domain. El principal nfs/ service necesario se crea automáticamente en el KDC.
2. Configure el NIS con el comando `authentication nis`:

   ```
   # authentication nis servers add <windows-ad-server>
   # authentication nis domain set <ad-realm>
   # authentication nis enable
   ```
3. Configurar el CIFS para utilizar el NSS para la asignación de ID con los comandos `cifs`:

   ```
   # cifs disable
   # cifs option set idmap-type nss
   # cifs enable
   # filesys restart
   ```

4. Asegúrese de que **nfs4-domain** sea igual al dominio de Active Directory:

```
# nfs option set nfs4-domain <ad-realm>
```

5. Habilitar Active Directory para la asignación de ID de NFSv4 con el comando `nfs`:

```
# nfs option set nfs4-idmap-active-directory enabled
```

Configuración de Active Directory

Procedimiento

1. Instale la función Active Directory Domain Services (AD DS) en el servidor de Windows.
2. Instale los componentes de Identity Management for UNIX.

```
C:\Windows\system32>Dism.exe /online /enable-feature /
featurename:adminui /all
C:\Windows\system32>Dism.exe /online /enable-feature /
featurename:nis /all
```

3. Verifique que el dominio NIS se haya configurado en el servidor.

```
C:\Windows\system32>nisadmin
The following are the settings on localhost

Push Interval : 1 days
Logging Mode  : Normal

NIS Domains
NIS Domain in AD  Master server  NIS Domain in UNIX
----------------  -------------  ----------------
corp              win-ad-server  corp
```

4. Asigne los UID/GID de UNIX de los usuarios y los grupos de AD para el servidor NFSv4.
   a. Vaya a **Server Manager** > **Tools** > **Active Directory**.
   b. Abra **Properties** para acceder a un usuario o grupo de AD.
   c. En la pestaña ficha UNIX Atributes, rellene los campos NIS domain, UID y Primary GID.

Configuración de clientes en Active Directory

Procedimiento

1. Cree un nuevo usuario de AD en el servidor de AD para representar el principal de servicio de cliente de NFS.
2. Cree el principal de servicio nfs/ service para el cliente de NFS.

```
> ktpass -princ nfs/<client_dns_name>@<REALM> -mapuser nfsuser -
pass **** -out nfsclient.keytab
/crytp rc4-hmac-nt /ptype KRB5_NT_PRINCIPAL
```

3. (Opcional) Copie el archivo keytab a `/etc/krb5.keytab` en el cliente.

   La necesidad de realizar este paso depende del sistema operativo cliente que utiliza.

CAPÍTULO 11

Migración de almacenamiento

Este capítulo incluye:

- Descripción general de la migración de almacenamiento 312
- Consideraciones de planificación de migración 313
- Visualización del estado de migración 314
- Evaluación de la preparación para la migración 315
- Migración de almacenamiento mediante DD System Manager 316
- Descripciones de cuadros de diálogo de migración de almacenamiento 317
- Migración de almacenamiento mediante la CLI 320
- Ejemplo de migración de almacenamiento de CLI 321

Descripción general de la migración de almacenamiento

La migración de almacenamiento admite el reemplazo de los gabinetes de almacenamiento existentes con nuevos gabinetes que pueden ofrecer un rendimiento más alto, una mayor capacidad y menor espacio físico.

Después de la instalación de nuevos gabinetes, puede migrar los datos de los gabinetes anteriores a los gabinetes nuevos, mientras el sistema continúa siendo compatible con otros procesos, como el acceso a los datos, la expansión, la limpieza y la replicación. La migración de almacenamiento requiere recursos del sistema, pero puede controlar esto con los ajustes de regulación que le dan a la migración una prioridad relativamente mayor o menor. También puede suspender una migración a fin de que haya más recursos disponibles para otros procesos y luego reanudar la migración cuando la demanda de recursos sea más baja.

Durante la migración, el sistema utiliza los datos en los gabinetes de origen y destino. Los datos nuevos se escriben en los gabinetes nuevos. Los datos no migrados se actualizan en los gabinetes de origen y los datos migrados se actualizan en los gabinetes de destino. Si se interrumpe la migración, la operación puede reanudar la migración de los bloques que no se han marcado como migrados.

Durante la migración, se copia y se verifica cada bloque de datos, los bloques de origen se liberan y se marcan como migrados, y se actualiza el índice del sistema para utilizar la nueva ubicación. Los datos nuevos destinados a almacenarse en el bloque de origen ahora se redirigirán al bloque de destino. Todas las nuevas asignaciones de bloques de datos que se habrían asignado desde el origen se asignan desde el destino.

El proceso de copia de la migración se realiza en el nivel de la bandeja, no en el nivel de datos lógicos; por lo tanto, se accede a todos los sectores del disco en la bandeja de origen, y estos se copian independientemente de si hay datos en ellos. Por lo tanto, la utilidad de migración de almacenamiento no puede usarse para reducir un espacio físico de datos lógicos.

Nota

Debido a que el conjunto de datos se divide entre los gabinetes de origen y destino durante la migración, no puede detener una migración y reanudar el uso de solamente los gabinetes de origen. Una vez iniciada, la migración debe completarse. Si una falla, como una unidad de disco defectuosa, interrumpe la migración, enfrente el problema y reanude la migración.

Según la cantidad de datos para migrar y la configuración de regulación seleccionada, una migración de almacenamiento puede tardar días o semanas. Cuando se migran todos los datos, el proceso de finalización, que se debe iniciar manualmente con el comando `storage migration finalize`, reinicia el sistema de archivos. Durante el reinicio, los gabinetes de origen se eliminan de la configuración del sistema y los gabinetes de destino pasan a formar parte del sistema de archivos. Una vez completado el proceso de finalización, los gabinetes de origen se pueden eliminar del sistema.

Después de una migración de almacenamiento, los números de bandejas de discos informados por DD OS podrían no ser secuenciales. Esto es porque la numeración de la bandeja está vinculada con el número de serie de cada bandeja de discos individual. El artículo de la base de conocimientos 499019, *Data Domain: la numeración de gabinetes de almacenamiento no es secuencial*, disponible en https://support.emc.com, proporciona detalles adicionales. En DD OS, versión 5.7.3.0 y versiones posteriores, el

comando `enclosure show persistent-id` que se describe en el artículo de la base de conocimientos requiere acceso de administrador, no acceso de SE.

Consideraciones de planificación de migración

Considere las siguientes pautas antes de iniciar una migración de almacenamiento.

- La migración de almacenamiento requiere una licencia de un único uso y funciona en los modelos de sistema compatibles con DD OS versión 5.7 o superior.

  Nota

  Las operaciones de migración múltiple de almacenamiento requieren varias licencias. Sin embargo, se pueden migrar varios gabinetes de origen a varios gabinetes de destino durante una sola operación.

- La migración de almacenamiento se basa en la capacidad, no en el conteo de gabinetes. Por lo tanto:
  - Un gabinete de origen puede migrarse a un gabinete de destino.
  - Un gabinete de origen puede migrarse a varios gabinetes de destino.
  - Varios gabinetes de origen pueden migrarse a un gabinete de destino.
  - Varios gabinetes de origen pueden migrarse a varios gabinetes de destino.
- Los gabinetes de destino deben tener las siguientes características:
  - Ser bandejas nuevas, no asignadas y sin licencia.
  - Ser compatibles con el modelo del sistema DD.
  - Contener al menos tanta capacidad útil como los gabinetes que están reemplazando.

    Nota

    No es posible determinar la utilización de la bandeja de origen. El sistema Data Domain ejecuta todos los cálculos según la capacidad de la bandeja.
- El modelo del sistema DD debe tener suficiente memoria para soportar la capacidad de almacenamiento del nivel activo de los nuevos gabinetes.
- La migración de datos no es compatible con los discos de la controladora del sistema.
- **⚠ PRECAUCIÓN**

  No actualice DD OS hasta que finalice la migración de almacenamiento en curso.

- La migración de almacenamiento no puede iniciarse cuando el sistema de archivos está deshabilitado, ni mientras hay una actualización de DD OS en curso ni tampoco cuando está en curso una reconstrucción de RAID.

  Nota

  Si hay una migración de almacenamiento en curso, se requiere una licencia de migración de almacenamiento nueva para iniciar una nueva operación de migración de almacenamiento después de que finalice la migración en curso. La presencia o la ausencia de una licencia de migración de almacenamiento se informan como parte de la comprobación previa de la actualización.

- Todos los especifican gabinetes de origen especificados deben estar en el mismo nivel (activo o archivo).
- Puede haber solo un grupo de discos en cada gabinete de origen, y todos los discos deben estar instalados en el grupo de discos dentro del mismo gabinete.
- Todos los discos de cada gabinete de destino deben ser del mismo tipo (por ejemplo, deben ser todos SATA o todos SAS).
- Después de que comienza la migración, los gabinetes de destino no pueden eliminarse.
- Los gabinetes de origen no se pueden eliminar hasta que la migración está completa y ha finalizado.
- La duración de la migración de almacenamiento depende de los recursos del sistema (que difieren para distintos los modelos de sistemas), la disponibilidad de los recursos del sistema y la cantidad de datos que se migrarán. La migración de almacenamiento puede tardar días o semanas en completarse.

Consideraciones de la bandeja DS60

La bandeja densa DS60 puede contener 60 discos, lo que permite que el cliente use la cantidad total de espacio en el rack. Se accede a las unidades desde la parte superior de la bandeja, mediante la extensión de la bandeja del gabinete. Debido al peso de las bandejas, que es de aproximadamente 102 kg (225 lb) cuando están completamente cargadas, es recomendable que lea esta sección antes de continuar con una migración de almacenamiento a las bandejas DS60.

Tenga en cuenta las siguientes consideraciones durante el trabajo con la bandeja DS60:

⚠ PRECAUCIÓN

- **La carga de bandejas en la parte superior del rack puede provocar que la bandeja se vuelque.**
- **Confirme que el piso pueda soportar el peso total de las bandejas DS60.**
- **Confirme que los racks puedan proporcionar alimentación suficiente para las bandejas DS60.**
- **Cuando se agregan más de cinco DS60 en el primer rack o más de seis DS60 en el segundo rack, se requieren barras estabilizadores y una escalera para mantener las bandejas DS60.**

Visualización del estado de migración

DD System Manager proporciona dos maneras de ver el estado de la migración de almacenamiento.

Procedimiento

1. Seleccione **Hardware** > **Storage**.

   En el área Storage, revise la línea Storage Migration Status. Si el estado es Not Licensed, debe agregar una licencia antes de usar las funciones de migración de almacenamiento. Si se instaló la licencia de migración de almacenamiento, el estado puede ser uno de los siguientes: None, Starting, Migrating, Paused by User, Paused by System, Copy Completed - Pending Finalization, Finalizing, Failed during Copy o Failed during Finalize.

2. Si hay una migración de almacenamiento en curso, haga clic en **View Storage Migration** para ver los cuadros de diálogo de progreso.

   Nota

   El estado de migración muestra el porcentaje de bloques de transferencia. En un sistema con muchos bloques libres, los bloques libres no se migran, pero se incluyen en la indicación de progreso. En esta situación, la indicación de progreso ascenderá rápidamente y luego se ralentizará cuando se inicie la migración de datos.

3. Cuando hay una migración de almacenamiento en curso, también puede ver el estado seleccionando **Health** > **Jobs**.

Evaluación de la preparación para la migración

Puede usar el sistema a fin de evaluar la preparación para la migración de almacenamiento sin confirmar el inicio de la migración.

Procedimiento

1. Instale los gabinetes de destino con las instrucciones que se proporcionan en las guías de instalación del producto.
2. Seleccione **Administration** > **Licenses** y verifique que esté instalada la licencia de migración de almacenamiento.
3. Si no está instalada la licencia de migración de almacenamiento, haga clic en **Add Licenses** y agregue la licencia.
4. Seleccione **Hardware** > **Storage** y haga clic en **Migrate Data**.
5. En el cuadro de diálogo Select a Task, seleccione **Estimate** y haga clic en **Next**.
6. En el cuadro de diálogo Select Existing Enclosures, use las casillas de verificación para seleccionar cada uno de los gabinetes de origen para la migración de almacenamiento y, a continuación, haga clic en **Next**.
7. En el cuadro de diálogo Select New Enclosures, use las casillas de verificación para seleccionar cada uno de los gabinetes de destino para la migración de almacenamiento y, a continuación, haga clic en **Next**.

   El botón Add Licenses le permite agregar licencias de almacenamiento para los gabinetes nuevos según sea necesario, sin interrumpir la tarea actual.

8. En el cuadro de diálogo Review Migration Plan, revise el calendario de migración estimado y luego haga clic en **Next**.
9. Analice los resultados de la verificación previa en el cuadro de diálogo Verify Migration Preconditions y, a continuación, haga clic en Close.

Resultados

Si alguna de las pruebas de verificación previa falla, resuelva el problema antes de comenzar la migración.

Migración de almacenamiento mediante DD System Manager

El proceso de migración de almacenamiento evalúa la preparación del sistema, le solicita que confirme que desea iniciar la migración, migra los datos y, a continuación, le solicita finalizar el proceso.

Procedimiento

1. Instale los gabinetes de destino con las instrucciones que se proporcionan en las guías de instalación del producto.
2. Seleccione **Administration** > **Licenses** y verifique que esté instalada la licencia de migración de almacenamiento.
3. Si no está instalada la licencia de migración de almacenamiento, haga clic en **Add Licenses** y agregue la licencia.
4. Seleccione **Hardware** > **Storage** y haga clic en **Migrate Data**.
5. En el cuadro de diálogo Select a Task, seleccione **Migrate** y haga clic en **Next**.
6. En el cuadro de diálogo Select Existing Enclosures, use las casillas de verificación para seleccionar cada uno de los gabinetes de origen para la migración de almacenamiento y, a continuación, haga clic en **Next**.
7. En el cuadro de diálogo Select New Enclosures, use las casillas de verificación para seleccionar cada uno de los gabinetes de destino para la migración de almacenamiento y, a continuación, haga clic en **Next**.

   El botón Add Licenses le permite agregar licencias de almacenamiento para los gabinetes nuevos según sea necesario, sin interrumpir la tarea actual.
8. En el cuadro de diálogo Review Migration Plan, revise el calendario de migración estimado y luego haga clic en **Start**.
9. En el cuadro de diálogo Start Migration, haga clic en **Start**.

   El cuadro de diálogo Migrate aparece y se actualiza durante las tres fases de la migración: Starting Migration, Migration in Progress y Copy Complete.
10. Cuando el título del cuadro de diálogo Migrate muestre Copy Complete y un reinicio del sistema de archivos sea aceptable, haga clic en **Finalize**.

    Nota

    Esta tarea reinicia el sistema de archivos y, por lo general, tarda de 10 a 15 minutos. El sistema no está disponible durante este tiempo.

Resultados

Cuando se completa la tarea de finalización de la migración de tarea, el sistema está usando los gabinetes de destino y se pueden eliminar los gabinetes de origen.

Descripciones de cuadros de diálogo de migración de almacenamiento

Las descripciones de los cuadros de diálogo de DD System Manager proporcionan información adicional sobre la migración de almacenamiento. Esta información también está disponible al hacer clic en el ícono de ayuda de los cuadros de diálogo.

Cuadro de diálogo Select a Task

La configuración en este cuadro de diálogo determina si el sistema se evaluará la preparación para la migración de almacenamiento y se detendrá, o y evaluará la preparación y comenzará con la migración del almacenamiento.

Seleccione **Estimate** para evaluar la preparación del sistema y detenerse.

Seleccione **Migrate** para iniciar la migración después de la evaluación del sistema. Entre la evaluación del sistema y el inicio de la migración, un cuadro de diálogo le solicitará que confirme o cancele la migración de almacenamiento.

Cuadro de diálogo Select Existing Enclosures

La configuración en este cuadro de diálogo selecciona el nivel activo o de retención y los gabinetes de origen para la migración.

Si está instalada la función DD Extended Retention, utilice el cuadro de lista para seleccionar **Active Tier** o **Retention Tier**. El cuadro de lista no aparece cuando no está instalada la función DD Extended Retention.

La lista Existing Enclosures muestra los gabinetes que cumplen con los requisitos para la migración de almacenamiento. Seleccione la casilla de verificación para cada uno de los gabinetes que desea migrar. Cuando esté listo para continuar, haga clic en **Next**.

Cuadro de diálogo Select New Enclosures

La configuración en este cuadro de diálogo selecciona los gabinetes de destino para la migración. Este cuadro de diálogo también muestra el estado de licencia de almacenamiento, además del botón **Add Licenses**.

La lista Available Enclosures muestra los destinos que cumplen con los requisitos para la migración de almacenamiento. Seleccione la casilla de verificación para cada uno de los gabinetes de destino que desee.

La barra de estado de la licencia representa todas las licencias de almacenamiento instaladas en el sistema. La parte verde representa las licencias que están en uso y el y la parte clara representa la capacidad de almacenamiento con licencia disponible para los gabinetes de destino. Si necesita instalar licencias adicionales para admitir los controladores de destino seleccionados, haga clic en **Add Licenses**.

Cuando esté listo para continuar, haga clic en **Next**.

Cuadro de diálogo Review Migration Plan

Este cuadro de diálogo presenta una estimación de la duración de la migración de almacenamiento, organizada en función de las tres etapas de la migración de almacenamiento.

La etapa 1 de migración de almacenamiento ejecuta una serie de pruebas para verificar que el sistema esté listo para la migración. Los resultados de las pruebas aparecerán en el cuadro de diálogo Verify Migration Preconditions.

Durante la etapa 2, los datos se copian de los gabinetes de origen a los gabinetes de destino. Cuando hay una gran cantidad de datos presente, la copia puede tardar días o semanas en completarse debido a que la copia se ejecuta en segundo plano, mientras el sistema continúa proporcionando datos a los clientes de respaldo. Una configuración en el cuadro de diálogo Migration in Progress le permite cambiar la prioridad de migración, que puede acelerar o desacelerar la migración.

La etapa 3, que se inicia manualmente desde el cuadro de diálogo Copy Complete, actualiza la configuración del sistema para usar los gabinetes de destino y elimina la configuración para los controladores de origen. Durante esta etapa, se reinicia el sistema de archivos y el sistema no está disponible para los clientes de respaldo.

Cuadro de diálogo Verify Migration Preconditions

Este cuadro de diálogo muestra los resultados de las pruebas que se ejecutan antes de que comience la migración.

La siguiente lista muestra la secuencia de prueba y proporciona información adicional sobre cada una de las pruebas.

P1. La plataforma de este sistema es compatible.

Los modelos de sistemas DD anteriores no son compatibles con la migración de almacenamiento.

P2. Una licencia de migración de almacenamiento está disponible.

Se requiere una licencia de migración de almacenamiento.

P3. Actualmente, no se está ejecutando ninguna otra migración.

Debe completar una migración de almacenamiento anterior para de poder iniciar otra.

P4. La solicitud de migración actual es igual a la solicitud de migración interrumpida.

Reanude y complete la migración interrumpida.

P5. Verifique el diseño del grupo de discos en los gabinetes de existentes.

La migración de almacenamiento requiere que cada gabinete de origen contenga solamente un grupo de discos, y todos los discos del grupo deben estar en ese gabinete.

P6. Verifique la capacidad final del sistema.

La capacidad total del sistema después de la migración y la eliminación de los gabinetes de origen no debe superar la capacidad que admite el modelo del sistema DD.

P7. Verifique la capacidad de los gabinetes de reemplazo.

La capacidad útil de los gabinetes de destino debe ser mayor que la de los gabinetes de origen.

P8. Los gabinetes de origen se encuentran en la misma unidad de retención o del nivel activo.

El sistema admite la migración de almacenamiento desde el nivel activo ni desde el nivel de retención. No admite la migración de datos desde ambos niveles al mismo tiempo.

P9. Los gabinetes de origen no forman parte de la unidad principal.

A pesar de que el controlador del sistema se muestra como un gabinete en la CLI, la migración de almacenamiento no es compatible con la migración desde discos instalados en el controlador del sistema.

P10. Pueden agregarse gabinetes de reemplazo al almacenamiento.

Todos los discos de cada gabinete de destino deben ser del mismo tipo (por ejemplo, deben ser todos SATA o todos SAS).

P11. No se está realizando ninguna reconstrucción de RAID en los controladores de origen.

La migración de almacenamiento no puede iniciarse mientras está en curso una reconstrucción de RAID.

P12. La bandeja de origen pertenece a un nivel compatible.

El gabinete de discos de origen debe ser parte de un nivel compatible en el destino de migración.

Cuadros de diálogo de progreso de migración

Esta serie de cuadros de diálogo presenta el estado de la migración de almacenamiento y los controles que se aplican en cada etapa.

Migrar: iniciar migración
Durante la primera etapa, el progreso se muestra en la barra de progreso y controles no están disponibles.

Migrar: migración en curso
Durante la segunda etapa, los datos se copian de los gabinetes de origen a los gabinetes de destino y el progreso se muestra en la barra de progreso. Debido a que la copia de datos puede tardar días o semanas en completarse, se proporcionan controles para que se puedan administrar los recursos utilizados durante la migración y suspender la migración cuando se necesitan recursos para otros procesos.

Puede hacer clic en **Pause** para suspender la migración y luego haga clic en **Resume** para continuar la migración.

Los botones **Low**, **Medium** y **High** definen la configuración de regulación para las necesidades de recursos de migración de almacenamiento. Una configuración de regulación baja otorga a la migración de almacenamiento una prioridad más baja de recursos, lo que da como resultado una migración más lenta y requiere menos recursos del sistema. Por el contrario, una configuración de regulación alta otorga a la migración de almacenamiento de una mayor prioridad de recursos, lo que da como resultado una migración más rápida y requiere más recursos del sistema. La configuración media selecciona una prioridad intermedia.

No es necesario dejar este cuadro de diálogo abierto durante la migración. Para comprobar el estado de la migración después de cerrar este cuadro de diálogo, seleccione **Hardware** > **Storage** y consulte el estado de la migración. Para volver a este cuadro de diálogo desde la página Hardware/Storage page, haga clic en **Manage Migration**. El progreso de la migración también puede verse seleccionando **Health** > **Jobs**.

Migrar: copia completa
Cuando se completa la copia, el proceso de migración espera hasta que el usuario haga clic en **Finalize**. Durante esta etapa final, que tarda de 10 a 15 minutos, se reinicia el sistema de archivos y el sistema no está disponible. Es una buena práctica iniciar esta

etapa durante una ventana de mantenimiento o un período de baja actividad del sistema.

Migración de almacenamiento mediante la CLI

Una migración simplemente requiere la transferencia de todos los bloques asignados de los conjuntos de bloques con formato por medio de los DG de origen (p. ej., los conjuntos de bloques de origen) a los conjuntos de bloques con formato por medio de los DG de destino (p. ej., los conjuntos de bloques de destino). Una vez que haya transferido todos los bloques asignados de los conjuntos de bloques de origen, esos conjuntos de bloques se pueden quitar del sistema de archivos, sus discos se pueden quitar de su nivel de almacenamiento y los gabinetes y discos físicos se pueden eliminar desde el módulo DDR.

Nota

La preparación de nuevos gabinetes para la migración de almacenamiento es administrada por el proceso de migración de almacenamiento. No prepare los gabinetes de destino como lo haría para agregar un gabinete. Por ejemplo, el uso del comando `filesys expand` es adecuado para agregar un gabinete, pero este comando impide que los gabinetes se usen como destinos de migración de almacenamiento.

Una bandeja de discos DS60 contiene cuatro paquetes de discos con 15 discos. Cuando una bandeja DS60 es el origen o el destino de la migración, se hace referencia a los paquetes de disco como ***gabinete*:*paquete***. En este ejemplo, el origen es el gabinete 7, paquete 2 (7:2), y el destino es el gabinete 7, paquete 4 (7:4).

Procedimiento

1. Instale los gabinetes de destino con las instrucciones que se proporcionan en las guías de instalación del producto.
2. Comprueba si se instaló la licencia de la función de migración de almacenamiento.

   ```
   # elicense show
   ```
3. Si no está instalada la licencia, actualice la licencia electrónica para agregar la licencia de función de migración de almacenamiento

   ```
   # elicense update
   ```
4. Vea los estados de los discos para los discos de origen y destino.

   ```
   # disk show state
   ```

   Los discos de origen deben estar en estado activo y los discos de destino deben estar en estado desconocido.
5. Ejecute el comando de verificación previa de migración de almacenamiento para determinar si el sistema está listo para la migración.

   ```
   # storage migration precheck source-enclosures 7:2 destination-enclosures 7:4
   ```
6. Revise la configuración de la regulación de migración.

   ```
   storage migration option show throttle
   ```
7. Cuando el sistema esté listo, comience la migración de almacenamiento.

   ```
   # storage migration start source-enclosures 7:2 destination-enclosures 7:4
   ```

8. Si lo desea, vea los estados de los discos para los discos de origen y destino durante la migración.

   ```
   # disk show state
   ```

   Durante la migración, los discos de origen deben estar en estado de migración y los discos de destino deben estar en el estado de destino.

9. Analice el estado de la migración según sea necesario.

   ```
   # storage migration status
   ```

10. Vea los estados de los discos para los discos de origen y destino.

    ```
    # disk show state
    ```

    Durante la migración, los discos de origen deben estar en estado de migración y los discos de destino deben estar en el estado de destino.

11. Cuando finalice la migración, actualice la configuración para utilizar los gabinetes de destino.

    Nota

    Esta tarea reinicia el sistema de archivos y, por lo general, tarda de 10 a 15 minutos. El sistema no está disponible durante este tiempo.

    ```
    storage migration finalize
    ```

12. Si desea eliminar todos los datos de cada uno de los gabinetes de origen, elimine los datos ahora.

    ```
    storage sanitize start enclosure <enclosure-id>[:<pack-id>]
    ```

    Nota

    El comando storage sanitize no produce una eliminación de datos certificada. Data Domain ofrece eliminación certificada de datos como un servicio. Para obtener más información, comuníquese con el representante de Data Domain.

13. Vea los estados de los discos para los discos de origen y destino.

    ```
    # disk show state
    ```

    Después de la migración, los discos de origen deben estar en estado desconocido y los discos de destino deben estar en estado activo.

Resultados

Cuando se completa la tarea de finalización de la migración de tarea, el sistema está usando el almacenamiento de destino y se puede eliminar el almacenamiento de origen.

Ejemplo de migración de almacenamiento de CLI

elicense show

```
# elicense show
Feature licenses:
## Feature     Count Mode            Expiration Date
-- ----------- ----- --------------- ---------------
1  REPLICATION 1     permanent (int) n/a
2  VTL         1     permanent (int) n/a
-- ----------- ----- --------------- ---------------
```

elicense update

```
# elicense update mylicense.lic
New licenses: Storage Migration
Feature licenses:
## Feature           Count   Mode              Expiration Date
-- -----------       -----  ---------------  ---------------
1  REPLICATION       1      permanent (int)  n/a
2  VTL               1      permanent (int)  n/a
3  Storage Migration 1      permanent (int)
-- -----------       -----  ---------------  ---------------
** This will replace all existing Data Domain licenses on the system with the above EMC ELMS
licenses.
Do you want to proceed? (yes|no) [yes]: yes
eLicense(s) updated.
```

disk show state

Figura 10 `disk show state`

```
# disk show state
Enclosure       Disk
  Row(disk-id)   1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
-------------   ----------------------------------------------
1                .  .  .  .
2                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
4                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5                v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
7               |--------|--------|--------|--------|
                 Pack 1   Pack 2   Pack 3   Pack 4
     E(49-60)   |U  U  U |.  .  s |U  U  U |U  U  U |
     D(37-48)   |U  U  U |.  .  . |U  U  U |U  U  U |
     C(25-36)   |U  U  U |.  .  . |U  U  U |U  U  U |
     B(13-24)   |U  U  U |.  .  . |U  U  U |U  U  U |
     A( 1-12)   |U  U  U |.  .  . |U  U  U |U  U  U |
                |--------|--------|--------|--------|
-------------   ----------------------------------------------

Legend   State            Count
------   ---------------  -----
.        In Use Disks     18
s        Spare Disks      1
v        Available Disks  15
U        Unknown Disks    105
------   ---------------  -----
```

storage migration precheck

```
#storage migration precheck  source-enclosures 2  destination-enclosures 11

  Source enclosures:
  Disks      Count   Disk    Disk         Enclosure   Enclosure
                     Group   Size         Model       Serial No.
  --------   -----   -----   ----------   ---------   --------------
  2.1-2.15   15      dg1     1.81 TiB     ES30        APM00111103820
  --------   -----   -----   ----------   ---------   --------------
  Total source disk size: 27.29 TiB

  Destination enclosures:
  Disks        Count   Disk      Disk       Enclosure   Enclosure
                       Group     Size       Model       Serial No.
  ----------   -----   -------   --------   ---------   --------------
  11.1-11.15   15      unknown   931.51 GiB ES30        APM00111103840
  ----------   -----   -------   --------   ---------   --------------
  Total destination disk size: 13.64 TiB

      1 "Verifying platform support.....................................................PASS"
      2 "Verifying valid storage migration license exists...............................PASS"
      3 "Verifying no other migration is running........................................PASS"
      4 "Verifying request matches interrupted migration................................PASS"
      5 "Verifying data layout on the source shelves....................................PASS"
      6 "Verifying final system capacity................................................PASS"
```

```
      7 "Verifying destination capacity.....................................PASS"
      8 "Verifying source shelves belong to same tier.......................PASS"
      9 "Verifying enclosure 1 is not used as source........................PASS"
     10 "Verifying destination shelves are addable to storage..............PASS"
     11 "Verifying no RAID reconstruction is going on in source shelves.....PASS"
Migration pre-check PASSED

Expected time to migrate data: 8 hrs 33 min
```

storage migration show history

Figura 11 `storage migration show history`

```
# storage migration show history
Id   Source      Source Enclosure   Dest        Dest Enclosure    Status     Start Time                 End Time
     Enclosure*  Serial No.         Enclosure*  Serial No.
--   ----------  ----------------   ----------  ---------------   ---------  -------------------------  -------------------------
2    9:0         SHU952400106A23    7:0         SHU9524084G055B   Finalized  Sat Aug  8 11:59:37 2015   Mon Aug 10 11:10:11 2015
1    9:0         SHU952400106A23    7:0         SHU9524084G055B   Finalized  Thu Aug  6 16:39:55 2015   Fri Aug  7 10:28:07 2015
                                    8:0         SHU9524084G04LR
--   ----------  ----------------   ----------  ---------------   ---------  -------------------------  -------------------------
(*) Enclosure ids at migration start time.
```

storage migration start

```
#storage migration start  source-enclosures 2  destination-enclosures 11

  Source enclosures:
  Disks      Count   Disk    Disk         Enclosure   Enclosure
                     Group   Size         Model       Serial No.
  --------   -----   -----   ----------   ---------   --------------
  2.1-2.15   15      dg1     1.81 TiB     ES30        APM00111103820
  --------   -----   -----   ----------   ---------   --------------
  Total source disk size: 27.29 TiB

  Destination enclosures:
  Disks        Count   Disk      Disk       Enclosure   Enclosure
                       Group     Size       Model       Serial No.
  ----------   -----   -------   --------   ---------   --------------
  11.1-11.15   15      unknown   931.51 GiB ES30        APM00111103840
  ----------   -----   -------   --------   ---------   --------------
  Total destination disk size: 13.64 TiB

  Expected time to migrate data: 84 hrs 40 min

**   Storage migration once started cannot be aborted.
     Existing data on the destination shelves will be overwritten.
        Do you want to continue with the migration? (yes|no) [no]: yes

Performing migration pre-check:
      1 Verifying platform support.....................................................PASS
      2 Verifying valid storage migration license exists...............................PASS
      3 Verifying no other migration is running........................................PASS
      4 Verifying request matches interrupted migration................................PASS
      5 Verifying data layout on the source shelves....................................PASS
      6 Verifying final system capacity................................................PASS
      7 Verifying destination capacity.....................................................PASS
      8 Verifying source shelves belong to same tier.....................................PASS
      9 Verifying enclosure 1 is not used as source.....................................PASS
     10 Verifying destination shelves are addable to storage...........................PASS
     11 Verifying no RAID reconstruction is going on in source shelves.....PASS

Migration pre-check PASSED

Storage migration will reserve space in the filesystem to migrate data.
Space reservation may add up to an hour or more based on system resources.

Storage migration process initiated.
Check storage migration status to monitor progress.
```

storage migration status

Figura 12 `storage migration status`

```
# storage migration status
Id   Source          Destination     State       Percent    Estimated Time to Complete   Current Throttle
     Enclosure(s)    Enclosure(s)                Complete                                Setting
--   ------------    ------------    ---------   --------   --------------------------   ----------------
5    7:2             7:4             migrating   45%        30 hrs 18 mins               high
--   ------------    ------------    ---------   --------   --------------------------   ----------------
```

disk show state, migration in progress

Figura 13 `disk show state, migration in progress`

```
# disk show state
Enclosure        Disk
  Row(disk-id)    1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
--------------   -----------------------------------------------
1                .  .  .  .
2                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
4                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5                v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
7               |--------|--------|--------|--------|
                | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
     E(49-60)   |U  U  U |m  m  s |U  U  U |s  d  d |
     D(37-48)   |U  U  U |m  m  m |U  U  U |d  d  d |
     C(25-36)   |U  U  U |m  m  m |U  U  U |d  d  d |
     B(13-24)   |U  U  U |m  m  m |U  U  U |d  d  d |
     A( 1-12)   |U  U  U |m  m  m |U  U  U |d  d  d |
                |--------|--------|--------|--------|
--------------   -----------------------------------------------

Legend   State              Count
------   -----------------  -----
.        In Use Disks       4
s        Spare Disks        2
v        Available Disks    15
U        Unknown Disks      90
m        Migrating Disks    14
d        Destination Disks  14
```

storage migration finalize

Figura 14 `storage migration finalize`

```
# storage migration finalize

Storage migration finalize restarts the filesystem.
This can take several minutes and the filesystem is unavailable until the operation completes.
        Do you want to continue? (yes|no) [no]: yes

Performing migration finalization pre-check:
(P1)    Verifying storage migration is ready for finalization....PASS
(P2)    Verifying there are no foreign disks.....................PASS
(P3)    Verifying data layout on the source shelves..............PASS

Migration finalization pre-check PASSED
Finalizing the storage migration with id 5:

Notifying filesystem to finalize migration...

Done.

Disabling the filesystem
Please wait..........
The filesystem is now disabled.
Removing source enclosures from filesystem...

Done.

Removing source enclosures from storage tier...

Done.

Enabling the filesystem
Please wait.....................
The filesystem is now enabled.
Storage migration with id 5 from enclosure(s) 7.2 to enclosure(s) 7.4 has been finalized.
```

disk show state, migration complete

Figura 15 `disk show state, migration complete`

```
# disk show state
Enclosure          Disk
  Row(disk-id)      1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
--------------    ------------------------------------------------
1                   .  .  .  .
2                   U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3                   U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
4                   U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5                   v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6                   U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
7                  |--------|--------|--------|--------|
                   | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
      E(49-60)     |U  U  U |U  U  U |U  U  U |s  .  . |
      D(37-48)     |U  U  U |U  U  U |U  U  U |.  .  . |
      C(25-36)     |U  U  U |U  U  U |U  U  U |.  .  . |
      B(13-24)     |U  U  U |U  U  U |U  U  U |.  .  . |
      A( 1-12)     |U  U  U |U  U  U |U  U  U |.  .  . |
                   |--------|--------|--------|--------|
--------------    ------------------------------------------------

Legend   State             Count
------   ---------------   -----
.        In Use Disks      18
s        Spare Disks       1
v        Available Disks   15
U        Unknown Disks     105
------   ---------------   -----
```

Nota

Actualmente, solo se admite la migración de almacenamiento en el nodo activo. La migración de almacenamiento no se admite en el nodo en espera del clúster de alta disponibilidad.

CAPÍTULO 12

Metadatos en flash

Este capítulo incluye:

- Descripción general de los metadatos en flash (MDoF) 328
- Licencias y capacidad de MDoF 329
- Nivel de caché de disco SSD 330
- Nivel de caché de disco SSD de MDoF: administración del sistema 330
- Alertas de discos SSD 333

Descripción general de los metadatos en flash (MDoF)

MDoF crea cachés de metadatos del sistema de archivos mediante las tecnologías flash. La caché de disco SSD es una caché de baja latencia y un número elevado de operaciones de entrada/salida por segundo (IOPS) para acelerar el acceso a datos y metadatos.

Nota

La versión de software mínima requerida es DD OS 6.0.

El almacenamiento en caché de los metadatos del sistema de archivos en discos SSD mejora el rendimiento de I/O para cargas de trabajo tradicionales y aleatorias.

Para cargas de trabajo tradicionales, la descarga de acceso aleatoria de metadatos de discos duros a discos SSD permite que los discos duros realicen el streaming de solicitudes de lectura y escritura.

Para cargas de trabajo aleatorias, la caché de discos SSD proporciona operaciones de metadatos de baja latencia, lo cual permite que los discos duros atiendan las solicitudes de datos en lugar de las solicitudes de caché.

La caché de lectura en el disco SSD mejora el rendimiento de lectura aleatoria por medio del almacenamiento en caché de los datos a los que se accede con frecuencia. La escritura de datos a NVRAM combinada con las operaciones de metadatos de baja latencia para vaciar la NVRAM mejora más rápido la latencia de escritura aleatoria. La ausencia de caché no impide el funcionamiento del sistema de archivos; solo afecta el rendimiento del sistema de archivos.

Cuando el nivel de caché se crea por primera vez, un reinicio del sistema de archivo solo es necesario si el nivel de caché se agrega después de que el sistema de archivos está funcionando. Para sistemas nuevos que vienen con discos de nivel de caché, no se requiere ningún reinicio del sistema de archivo si el nivel de caché se crea antes de habilitar el sistema de archivos por primera vez. Se puede agregar caché adicional a un sistema activo sin necesidad de habilitar o deshabilitar el sistema de archivos.

Nota

Los sistemas DD9500 que fueron actualizados de DD OS 5.7 a DD OS 6.0 requieren un reinicio de sistema de archivos de un solo uso después de crear el nivel de caché por primera vez.

Una condición específica con respecto a los discos SSD es que, cuando el número restante de bloques de repuesto se acerca a cero, el disco SSD entra en una condición de solo lectura. Cuando se produce una condición de solo lectura, DD OS trata a la unidad como una caché de solo lectura y envía una alerta.

MDoF se admite en los siguientes sistemas Data Domain:

- DD6300
- DD6800
- DD9300
- DD9500
- DD9800

- Instancias de Data Domain Virtual Edition, incluidos los sistemas de DD3300, en configuraciones de capacidad de 16 TB o superiores (nivel de caché de SSD para Data Domain Virtual Edition)

Licencias y capacidad de MDoF

Es necesaria una licencia activada mediante ELMS para el uso de la función MDoF; una licencia de la caché de discos SSD no se activará de manera predeterminada.

En la siguiente tabla se describen las diferentes licencias de capacidad de discos SSD y las capacidades de discos SSD del sistema específico:

Tabla 121 Licencias de capacidad de discos SSD por sistema

Modelo	Memoria	Cantidad de discos SSD	Capacidad de los discos SSD
DD6300	48 GB (base)	1	800 GB
	96 GB (expandida)	2	1600 GB
DD6800	192 GB (base)	2	1600 GB
	192 GB (expandida)	4	3200 GB
DD9300	192 GB (base)	5	4000 GB
	384 GB (expandida)	8	6400 GB
DD9500	256 GB (base)	8	6400 GB
	512 GB (expandida)	15	12000 GB
DD9800	256 GB (base)	8	6400 GB
	768 GB (expandida)	15	12000 GB

Nivel de caché de SSD para Data Domain Virtual Edition

Las instancias de Data Domain Virtual Edition y los sistemas de DD3300 no requieren una licencia para el nivel de caché de SSD. La capacidad de SSD máxima admitida es del 1 % de la capacidad de nivel activo.

En la siguiente tabla se describen las diferentes licencias de capacidad de discos SSD y las capacidades de discos SSD del sistema específico:

Tabla 122 Capacidad de SSD para Data Domain Virtual Edition y DD3300

Configuración de capacidad	Capacidad máxima de SSD
DD VE (16 TB)	160 GB
DD VE (32 TB)	320 GB
DD VE (48 TB)	480 GB
DD VE (64 TB)	640 GB
DD VE (96 TB)	960 GB
DD3300 (8 TB)	160 GB
DD3300 (16 TB)	160 GB

Tabla 122 Capacidad de SSD para Data Domain Virtual Edition y DD3300 (continuación)

Configuración de capacidad	Capacidad máxima de SSD
DD3300 (32 TB)	320 GB

Nivel de caché de disco SSD

El nivel de caché de disco SSD proporciona el almacenamiento de caché de disco SSD para el sistema de archivos. El sistema de archivos obtiene el almacenamiento requerido del nivel de caché de disco SSD sin la intervención activa del usuario.

Nivel de caché de disco SSD de MDoF: administración del sistema

Tenga en cuenta las siguientes consideraciones para la caché de disco SSD:

- Cuando se implementan discos SSD dentro de un controlador, esos discos SSD se tratan como unidades de raíz interna. Aparecen como gabinete 1 en la salida del comando `storage show all`.
- Administre discos SSD individuales con el comando `disk` de la misma manera que se administran los discos duros.
- Ejecute el comando `storage add` para agregar un disco SSD o un gabinete de disco SSD individual para el nivel de caché de disco SSD.
- No es necesario que se administre el espacio de nivel de caché de disco SSD. El sistema de archivos obtiene el almacenamiento requerido del nivel de caché de disco SSD y lo comparte entre sus clientes.
- El comando `filesys create` crea un volumen de disco SSD, si los discos SSD están disponibles en el sistema.

  Nota

  Si se agregan discos SSD al sistema posteriormente, el sistema debe crear automáticamente el volumen de disco SSD y notificar al sistema de archivos. El administrador de la caché de discos SSD notifica a sus clientes registrados para que puedan crear sus objetos almacenados en caché.

- Si el volumen de disco SSD contiene solo un disco activo, la última unidad que queda offline aparecerá nuevamente en línea si se extrae la unidad activa desde el sistema.

La siguiente sección describe cómo administrar el nivel de caché de disco SSD desde Data Domain System Manager con la CLI de DD OS.

Administración del nivel de caché de disco SSD

Las funciones de configuración de almacenamiento le permiten agregar y quitar almacenamiento del nivel de caché de disco SSD.

Procedimiento

1. Seleccione **Hardware** > **Storage** > **Overview**.
2. Expanda el cuadro de diálogo **Cache Tier**.

3. Haga clic en **Configure**.

   La cantidad máxima de almacenamiento que se puede agregar al nivel activo depende de la controladora DD que se use.

   Nota

   La barra de capacidad con licencia muestra la parte de la capacidad con licencia (utilizada y restante) para los gabinetes instalados.

4. Seleccione la casilla de verificación de la bandeja que desee agregar.
5. Haga clic en el botón **Add to Tier**.
6. Haga clic en **OK** para agregar el almacenamiento.

   Nota

   Para eliminar una bandeja agregada, selecciónela en la lista Tier Configuration, haga clic en **Remove from Configuration** y, a continuación, haga clic en **OK**.

Equivalente de la CLI
Cuando los discos SSD de nivel de caché se instalan en la unidad principal:

a. Agregue los discos SSD al nivel de caché.

```
#  storage add disks 1.13,1.14 tier cache
Checking storage requirements...done
Adding disk 1.13 to the cache tier...done

Updating system information...done

Disk 1.13 successfully added to the cache tier.


Checking storage requirements...
done
Adding disk 1.14 to the cache tier...done

Updating system information...done

Disk 1.14 successfully added to the cache tier.
```

b. Verifique el estado de los discos SSD recién agregados.

```
# disk show state
Enclosure   Disk
             1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
---------   ---------------------------------------------
1            .  .  .  .  s  .  .  s  s  s  s  s  v  v
2            U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3            U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
---------   ---------------------------------------------

Legend   State             Count
------   ---------------   -----
.        In Use Disks      6
s        Spare Disks       6
v        Available Disks   2
U        Unknown Disks     30
------   ---------------   -----
Total 44 disks
```

Cuando los discos SSD de nivel de caché se instalan en una bandeja externa:

a. Verifique que el sistema reconozca la bandeja de disco SSD. En el ejemplo que aparece a continuación, la bandeja de disco SSD es el gabinete 2.

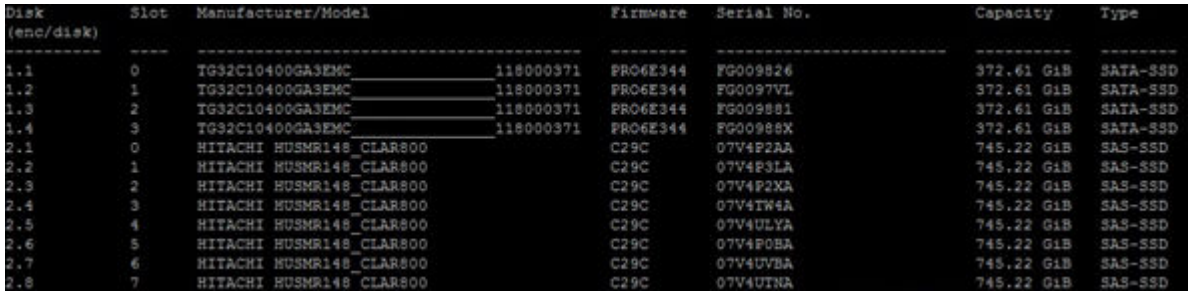
```
# disk show state
Enclosure   Disk
Row(disk-id) 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
---------    ----------------------------------------------
1            .  .  .  .
2            U  U  U  U  U  U  U  U  -  -  -  -  -  -  -
3            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
4            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
5            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
7            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
8            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
9            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
10           |--------|--------|--------|--------|
             | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
   E(49-60)  |v  v  v |v  v  v |v  v  v |v  v  v |
   D(37-48)  |v  v  v |v  v  v |v  v  v |v  v  v |
   C(25-36)  |v  v  v |v  v  v |v  v  v |v  v  v |
   B(13-24)  |v  v  v |v  v  v |v  v  v |v  v  v |
   A( 1-12)  |v  v  v |v  v  v |v  v  v |v  v  v |
             |--------|--------|--------|--------|
11           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
12           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
13           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
---------    ----------------------------------------------

Legend   State               Count
------   ------------------  -----
.        In Use Disks        32
v        Available Disks     182
U        Unknown Disks       8
-        Not Installed Disks 7
------   ------------------ -----
Total 222 disks
```

b. Identifique el ID de bandeja en la bandeja de disco SSD. Los discos SSD se mostrarán como `SAS-SSD` o `SATA-SSD` en la columna `Type`.

```
#  disk show hardware
```

Figura 16



Disk (enc/disk)	Slot	Manufacturer/Model	Firmware	Serial No.	Capacity	Type
1.1	0	TG32C10400GA3EMC_____118000371	PRO6E344	FG009826	372.61 GiB	SATA-SSD
1.2	1	TG32C10400GA3EMC_____118000371	PRO6E344	FG0097VL	372.61 GiB	SATA-SSD
1.3	2	TG32C10400GA3EMC_____118000371	PRO6E344	FG009881	372.61 GiB	SATA-SSD
1.4	3	TG32C10400GA3EMC_____118000371	PRO6E344	FG00988X	372.61 GiB	SATA-SSD
2.1	0	HITACHI HUSMR148_CLAR800	C29C	07V4P2AA	745.22 GiB	SAS-SSD
2.2	1	HITACHI HUSMR148_CLAR800	C29C	07V4P3LA	745.22 GiB	SAS-SSD
2.3	2	HITACHI HUSMR148_CLAR800	C29C	07V4P2XA	745.22 GiB	SAS-SSD
2.4	3	HITACHI HUSMR148_CLAR800	C29C	07V4IW4A	745.22 GiB	SAS-SSD
2.5	4	HITACHI HUSMR148_CLAR800	C29C	07V4ULYA	745.22 GiB	SAS-SSD
2.6	5	HITACHI HUSMR148_CLAR800	C29C	07V4P0BA	745.22 GiB	SAS-SSD
2.7	6	HITACHI HUSMR148_CLAR800	C29C	07V4UVBA	745.22 GiB	SAS-SSD
2.8	7	HITACHI HUSMR148_CLAR800	C29C	07V4UTNA	745.22 GiB	SAS-SSD

c. Agregue la bandeja de discos SSD al nivel de caché.

```
#  storage add enclosure 2 tier cache

Checking storage requirements...done
Adding enclosure 2 to the cache tier...Enclosure 2
successfully added to the cache tier.

Updating system information...done

Successfully added: 2  done
```

d. Verifique el estado de los discos SSD recién agregados.

```
# disk show state
Enclosure   Disk
Row(disk-id) 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
---------    ----------------------------------------------
1            .  .  .  .
```

```
2            .  .  .  .  .  .  .  .  -  -  -  -  -  -  -
3            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
4            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
5            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
7            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
8            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
9            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
10          |--------|--------|--------|--------|
            | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
   E(49-60) |v  v  v |v  v  v |v  v  v |v  v  v |
   D(37-48) |v  v  v |v  v  v |v  v  v |v  v  v |
   C(25-36) |v  v  v |v  v  v |v  v  v |v  v  v |
   B(13-24) |v  v  v |v  v  v |v  v  v |v  v  v |
   A( 1-12) |v  v  v |v  v  v |v  v  v |v  v  v |
            |--------|--------|--------|--------|
11           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
12           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
13           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
---------   -----------------------------------------------

Legend   State               Count
------   ------------------  -----
.        In Use Disks        32
v        Available Disks     182
U        Unknown Disks       8
-        Not Installed Disks 7
------   ------------------ -----
Total 222 disks
```

Para quitar un disco SSD montado en una controladora desde el nivel de caché:

```
# storage remove disk 1.13

Removing disk 1.13...done

Updating system information...done

Disk 1.13 successfully removed.
```

Para eliminar una bandeja de discos SSD del sistema:

```
# storage remove enclosure 2

Removing enclosure 2...Enclosure 2 successfully removed.

Updating system information...done

Successfuly removed: 2 done
```

Alertas de discos SSD

Hay tres alertas específicas para el nivel de caché de disco SSD.

Las alertas de nivel de caché de disco SSD son:

- Licencias
  Si el sistema de archivos está habilitado y hay menos capacidad física de caché configurada de lo que permite la licencia, se genera una alerta con la capacidad de disco SSD actual y la licencia de capacidad. Esta alerta se clasifica como una alerta de advertencia. La ausencia de caché no impide el funcionamiento del sistema de archivos; solo afecta el rendimiento del sistema de archivos. Se puede agregar caché adicional a un sistema activo sin necesidad de habilitar o deshabilitar el sistema de archivos.
- Condición de solo lectura

Cuando el número restante de bloques de repuesto se acerca a cero, el disco SSD entra en una condición de solo lectura. Cuando se produce una condición de solo lectura, DD OS trata a la unidad como una caché de solo lectura.

Una alerta `EVT-ALMACENAMIENTO-00001` se muestra cuando el disco SSD está en un estado de solo lectura y debe reemplazarse.

- Vida útil del disco SSD
  Cuando un disco SSD llega al final de su vida útil, el sistema genera una alerta de falla de hardware para identificar la ubicación del disco SSD dentro de la bandeja de discos SSD. Esta alerta se clasifica como una alerta crítica.

  Una alerta `EVT-STORAGE-00016` se muestra cuando el contador EOL llega a 98. La unidad falla proactivamente cuando el contador EOL llega a 99.

CAPÍTULO 13

Destino SCSI

Este capítulo incluye:

- Descripción general del destino de SCSI 336
- Vista Fibre Channel 337
- Diferencias entre el monitoreo de vínculos de FC entre las versiones de SO de DD 348

Descripción general del destino de SCSI

El destino de SCSI (interfaz estándar de equipos pequeños) es un demonio de administración unificado para todos los servicios y transportes de SCSI. El destino de SCSI admite tanto DD VTL (librería de cintas virtuales) como DD Boost mediante FC (Fibre Channel) y servicios de bloques de vDisk/ProtectPoint, además de cualquier elemento que tenga un LUN (número de unidad lógica) de destino en un sistema DD.

Servicios y transportes de destino de SCSI

El demonio de destino de SCSI comienza cuando los puertos de FC están presentes o DD VTL tiene licencia. Proporciona administración unificada para todos los *servicios* y *transportes* de destino de SCSI.

- Un *servicio* es todo lo que tiene un LUN de destino en un sistema DD que usa comandos de destino de SCSI, como DD VTL (unidades y cambiadores de cintas), DD Boost mediante FC (dispositivos de procesador) o vDisk (dispositivo de disco virtual).
- Un *transporte* permite que los *dispositivos* se vuelvan visibles para los *iniciadores*.
- Un *iniciador* es un cliente de respaldo que se conecta a un sistema para leer y escribir datos usando el protocolo FC. Un iniciador específico puede admitir DD Boost mediante FC, vDisk o DD VTL, pero no mediante los tres.
- Los *dispositivos* son visibles en una SAN (red de almacenamiento) a través de los puertos físicos. Los iniciadores de host se comunican con el sistema DD a través de la SAN.
- Los *grupos de acceso* administran el acceso entre dispositivos e iniciadores.
- Un *terminal* es el destino lógico en un sistema DD al cual se conecta el iniciador. Puede deshabilitar, habilitar o renombrar terminales. Para eliminar terminales, el hardware de transporte asociado ya no debe existir. Los terminales se detectan y crean automáticamente cuando se produce una nueva conexión de transporte. Los terminales tienen los siguientes atributos: topología de puertos, estado FCP2-RETRY, WWPN y WWNN.
- *NPIV* (ID virtualización de puertos N) es una función de Fibre Channel que permite que múltiples terminales compartan un único puerto físico. NPIV alivia los requisitos de hardware y proporciona funcionalidades de conmutación por error.
- En DD OS 6.0, los usuarios pueden especificar la secuencia de direcciones del sistema secundario para la conmutación por error. Por ejemplo, si el sistema especifica 0a, 0b, 1a, 1b, y el usuario especifica 1a, 1b, 0a, 0b, la secuencia determinada por el usuario se utiliza para la conmutación por error. El comando `scsitarget endpoint show detailed` muestra la secuencia determinada por el usuario.

Tenga en cuenta las siguientes excepciones:

- DD Boost puede proporcionar servicio a clientes de FC y de IP simultáneamente; sin embargo, ambos transportes no pueden compartir el mismo iniciador.
- Debe haber solo un iniciador por grupo de acceso. A cada grupo de acceso se le asigna un tipo (DD VTL, servicios de bloque de vDisk/ProtectPoint o DD Boost mediante FC).

Arquitecturas de destino de SCSI: compatibles y no compatibles

El destino de SCSI admite las siguientes arquitecturas:

- **DD VTL más DD Boost mediante FC desde distintos iniciadores:** Dos iniciadores diferentes (en el mismo cliente o en clientes distintos) pueden acceder a un

sistema DD usando DD VTL y DD Boost mediante FC, a través de terminales de destino del sistema DD iguales o diferentes.

- **DD VTL más DD Boost mediante FC de un iniciador a dos sistemas DD diferentes:** Un único iniciador puede acceder a dos sistemas DD diferentes usando cualquier servicio.

El destino de SCSI no admite la siguiente arquitectura:

- **DD VTL más DD Boost mediante FC de un iniciador al mismo sistema DD:** Un único iniciador no puede acceder al mismo sistema DD mediante servicios diferentes.

Protocolo delgado

El protocolo delgado es un demonio ligero para DD VTL y vDisk que responde a los comandos SCSI cuando el protocolo principal no puede. Para los ambientes de Fibre Channel con varios protocolos, el protocolo delgado:

- Evita bloqueos del iniciador
- Evita anulaciones innecesarias del iniciador
- Impide que los dispositivos de iniciador desaparezcan
- Es compatible con el modo en espera
- Es compatible con dispositivos que se pueden descubrir de manera anticipada y rápida
- Mejora el protocolo de comportamiento de alta disponibilidad
- No requiere el acceso rápido al registro

Para obtener más información acerca de DD Boost y el comando scscitarget (CLI)

Para obtener más información acerca de cómo usar DD Boost a través del administrador del sistema de DD, consulte el capítulo relacionado en este libro. Para obtener otro tipo de información acerca de DD Boost, consulte la *Guía de administración de Data Domain Boost para OpenStorage*.

En este capítulo, se describe cómo usar el destino de SCSI mediante el administrador del sistema DD. Una vez que se haya familiarizado con las tareas básicas, el comando `scscitarget` en la *Guía de referencia de comandos de Data Domain Operating System* ofrece tareas de administración más avanzadas.

Cuando haya mucho tráfico de DD VTL, evite ejecutar el comando `scsitarget group use`, que cambia las listas de los terminales en uso por uno o varios dispositivos vDisk o de destino de SCSI en un grupo entre las listas de terminales primarios y secundarios.

Vista Fibre Channel

La vista Fibre Channel muestra el estado actual de si está habilitado Fibre Channel o NPIV. También muestra dos pestañas: Physical Resources y Access Groups. Entre los recursos físicos, se incluyen los iniciadores y los puntos finales. Un grupo de acceso es un conjunto de iniciadores WWPN (nombres de puertos mundiales) o alias, y las unidades y los intercambiadores a los que pueden obtener acceso.

Habilitación de NPIV

NPIV (ID virtualización de puertos N) es una función de Fibre Channel en la que múltiples terminales pueden compartir un único puerto físico. NPIV alivia los requisitos de hardware y proporciona funcionalidades de conmutación por error/conmutación

por recuperación de terminales. NPIV no está configurada de manera predeterminada; debe habilitarla.

Nota

NPIV está habilitada de forma predeterminada en la configuración de alta disponibilidad.

NPIV proporciona consolidación de múltiples sistemas simplificada:

- NPIV es un estándar de ANSI T11 que permite registrar un único puerto físico de HBA con fabric Fibre Channel mediante WWPN múltiples
- Los puertos físicos y virtuales tienen las mismas propiedades de puertos y se comportan exactamente del mismo modo.
- Es posible que haya m:1 relaciones entre los terminales y el puerto, es decir, múltiples terminales pueden compartir el mismo puerto físico.

Específicamente, la habilitación de NPIV activa las siguientes características:

- Se permiten múltiples terminales por puerto físico, cada uno mediante un puerto (NPIV) virtual. La base de puertos es un marcador de posición para el puerto físico y no está asociada a un terminal.
- La conmutación por error/conmutación por recuperación de terminales se habilita automáticamente cuando se usa NPIV.

  Nota

  Después de habilitar NPIV, debe especificarse la dirección secundaria del sistema en cada uno de los terminales. De lo contrario, no se llevará a cabo la conmutación por error del terminal.

- Se pueden consolidar varios sistemas DD en un solo sistema DD; sin embargo, la cantidad de tarjetas HBA sigue siendo la misma en el sistema DD único.
- La conmutación por error del terminal se desencadena cuando FC-SSM detecta que un puerto pasa de estar en línea a estar offline. Si el puerto físico está offline antes de que se habilite scsitarget y el puerto sigue estando offline después de habilitar scsitarget, no es posible realizar una conmutación por error de terminal porque FC-SSM no genera un evento de puerto offline. Si el puerto vuelve a estar en línea y la conmutación por recuperación automática está habilitada, todos los terminales con conmutación por error que usen ese puerto como puerto primario realizarán una conmutación por recuperación al puerto primario.

Las funciones de alta disponibilidad de Data Domain requieren que NPIV transfiera los WWN entre los nodos de un par de alta disponibilidad durante el proceso de conmutación por error.

Nota

Antes de habilitar NPIV, se deben cumplir las siguientes condiciones:

- El sistema DD debe ejecutar DD OS 5.7.
- Todos los puertos deben estar conectados a SLIC y HBA Fibre Channel de 4 Gb, 8 Gb y 16 Gb.
- El ID del sistema DD debe ser válido, es decir, no debe ser 0.

Además, las topologías de puerto y nombres de los puertos se revisarán y pueden impedir la habilitación de NPIV:

- NPIV se permite si la topología para *todos* los puertos es de preferencia de loop.
- NPIV se permite si la topología para *algunos* de los puertos es de preferencia de loop; sin embargo, NPIV debe estar deshabilitada para los puertos que son de solo loop, o se debe volver a configurar la topología de preferencia de loop para la funcionalidad adecuada.
- NPIV *no* se permite si *ninguno* tiene una topología de preferencia de loop de los puertos.
- Si los nombres de los puertos están presentes en grupos de acceso, los nombres de puertos se reemplazan con los nombres de terminales asociados.

Procedimiento

1. Seleccione **Hardware** > **Fibre Channel**.
2. Junto a NPIV: Disabled, seleccione **Enable**.
3. En el cuadro de diálogo Enable NPIV, recibirá una advertencia que indica que todos los puertos Fibre Channel deben deshabilitarse antes de que se pueda habilitar NPIV. Si está seguro de que desea hacerlo, seleccione **Yes**.

   Equivalente de la CLI

   a. Asegúrese de que NPIV (global) esté habilitada.

   ```
   # scsitarget transport option show npiv
   SCSI Target Transport Options
   Option   Value
   ------   --------
   npiv     disabled
   ------   --------
   ```

   b. Si NPIV está deshabilitada, habilítela. Primero debe deshabilitar todos los puertos.

   ```
   # scsitarget port disable all
   All ports successfully disabled.
   # scsitarget transport option set npiv enabled
   Enabling FiberChannel NPIV mode may require SAN zoning to
   be changed to configure both base port and NPIV WWPNs.
   Any FiberChannel port names used in the access groups will
   be converted to their corresponding endpoint names in order
   to prevent ambiguity.
       Do you want to continue? (yes|no) [no]:
   ```

   c. Vuelva a habilitar los puertos deshabilitados.

   ```
   # scsitarget port enable all
   All ports successfully enabled.
   ```

   d. Asegúrese de que los puertos físicos tengan una configuración de NPIV establecida en “auto”.

```
# scsitarget port show detailed 0a
System Address:     0a
Enabled:            Yes
Status:             Online
Transport:          FibreChannel
Operational Status: Normal
FC NPIV:            Enabled (auto)
.
.
.
```

e. Cree un terminal nuevo mediante los puertos primarios y secundarios que haya seleccionado.

```
# scsitarget endpoint add test0a0b system-address 0aprimary-system-address 0a secondary-system-address 0b
```

Tenga en cuenta que el terminal está deshabilitado por defecto, por lo tanto, debe habilitarlo.

```
# scsitarget endpoint enable test0a0b
```

Luego, visualice la información del terminal.

```
# scsitarget endpoint show detailed test0a0b
Endpoint:                 test0a0b
Current System Address:   0b
Primary System Address:   0a
Secondary System Address: 0b
Enabled:                  Yes
Status:                   Online
Transport:                FibreChannel
FC WWNN:                  50:02:18:80:08:a0:00:91
FC WWPN:                  50:02:18:84:08:b6:00:91
```

f. Zonifique un sistema de host al WWPN generado automáticamente del terminal recientemente creado.

g. Cree un dispositivo de DD VTL, vDisk o DD Boost mediante Fibre Channel (DFC) y haga que esté disponible en el sistema host.

h. Asegúrese de que se pueda acceder al dispositivo DD elegido en el host (de lectura o escritura).

i. Pruebe la conmutación por error del terminal mediante la opción “secundaria” para transferir el terminal a la dirección secundaria del sistema (SSA).

```
# scsitarget endpoint use test0a0b secondary
```

j. Asegúrese de que aún se pueda acceder al dispositivo DD elegido en el host (de lectura o escritura). Pruebe la conmutación por recuperación mediante la opción “primaria” para volver a transferir el terminal a la dirección primaria del sistema (PSA).

```
# scsitarget endpoint use test0a0b primary
```

k. Asegúrese de que aún se pueda acceder al dispositivo DD elegido en el host (de lectura o escritura).

Deshabilitación de NPIV

Para poder deshabilitar NPIV, no debe tener ningún puerto con múltiples punto finales.

Nota

NPIV se requiere para la configuración de alta disponibilidad. Se habilita de forma predeterminada y no se puede desactivar.

Procedimiento

1. Seleccione **Hardware** > **Fibre Channel**.
2. Junto a NPIV: Enabled, seleccione **Disable**.
3. En el cuadro de diálogo Disable NPIV, revise los mensajes sobre la corrección de la configuración y, cuando esté listo, seleccione **OK**.

Pestaña Resources

En la pestaña **Hardware** > **Fibre Channel** > **Resources**, se muestra información acerca de los puertos, los terminales y los iniciadores.

Tabla 123 Puertos

Elemento	Descripción
Dirección del sistema	Dirección del sistema para el puerto
WWPN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del puerto Fibre Channel (FC)
WWNN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del nodo FC
Activado	Estado operacional del puerto; ya sea habilitado o deshabilitado
NPIV	Estado de NPIV; ya sea habilitado o deshabilitado.
Link Status	Estado del vínculo, ya sea en línea u offline; es decir, si el puerto está activo y es capaz de administrar el tráfico.
Operation Status	Estado operacional: Normal o Marginal.
# of Endpoints	Cantidad de terminales asociados con este puerto.

Tabla 124 Terminales

Elemento	Descripción
Nombre	Nombre de terminal
WWPN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del puerto Fibre Channel (FC)
WWNN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del nodo FC
Dirección del sistema	Dirección del sistema del terminal.
Activado	Estado operacional del puerto; Activado o Desactivado
Link Status	En línea u Offline; es decir, si el puerto está activo y es capaz de administrar el tráfico

Tabla 125 Initiators

Elemento	Descripción
Nombre	Nombre del iniciador
Servicio	Soporte de servicio por iniciador, que es DD VTL, DD Boost o vDisk
WWPN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del puerto Fibre Channel (FC)
WWNN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del nodo FC
Vendor Name	Modelo de iniciador
Terminales en línea	Terminales vistos por el iniciador Se muestra `none` u `offline` si el iniciador no está disponible.

Configuración de un puerto

Se descubren los puertos y un solo terminal se crea automáticamente para cada puerto en el arranque.

Las propiedades del puerto base dependen de si NPIV está habilitado:

- En el modo de no NPIV, los puertos usan las mismas propiedades que el terminal, es decir, el WWPN del puerto base y del terminal son iguales.
- En el modo NPIV, las propiedades del puerto base derivan de los valores predeterminados, es decir, un WWPN nuevo se genera para el puerto base y se conserva para permitir una alternancia coherente entre los modos NPIV. Además, el modo NPIV proporciona la capacidad de admitir múltiples terminales por puerto.

Procedimiento

1. Seleccione **Hardware** > **Fibre Channel** > **Resources**.
2. En **Ports**, seleccione un puerto y, a continuación, seleccione**Modify** (lápiz).
3. En el cuadro de diálogo Configure Port, seleccione si desea habilitar o deshabilitar NPIV automáticamente para este puerto.
4. Para Topology, seleccione Loop Preferred, Loop Only, Point to Point o Default.
5. Para Speed, seleccione 1, 2, 4, 8, u 16 Gbps, o auto.
6. Seleccione **OK**.

Activación de un puerto

Puertos deben habilitarse antes de que se puedan utilizar.

Procedimiento

1. Seleccione **Hardware** > **Fibre Channel** > **Resources**.
2. Seleccione **More Tasks** > **Ports** > **Enable**. Si todos los puertos ya están habilitados, se muestra un mensaje al respecto.
3. En el cuadro de diálogo Enable Endpoints, seleccione uno o más puertos de la lista y seleccione **Next**.

4. Después de la confirmación, seleccione **Next** para completar la tarea.

Deshabilitación de un puerto

Simplemente puede deshabilitar un puerto (o varios puertos), o bien, puede decidir realizar un failover de todos los puntos finales del puerto (o los puertos) en otro puerto.

Procedimiento

1. Seleccione **Hardware** > **Fibre Channel** > **Resources**.
2. Seleccione **More Tasks** > **Ports** > **Disable**.
3. En el cuadro de diálogo Disable Endpoints, seleccione uno o más puertos de la lista y seleccione **Next**.
4. En el cuadro de diálogo de confirmación, puede simplemente continuar con la deshabilitación del puerto, o bien, puede decidir realizar un failover de todos los puntos finales de los puertos en otro puerto.

Cómo agregar un terminal

Un terminal es un objeto virtual que está mapeado a un puerto virtual subyacente. En el modo de no NPIV (no disponible en la configuración de alta disponibilidad), se permite únicamente un solo terminal por puerto físico y la base de puertos se usa para configurar ese terminal para el fabric. Cuando se habilita NPIV, se permiten múltiples terminales por puerto físico, cada uno de los cuales usa un puerto virtual (NPIV), y se habilita la conmutación por error/conmutación por recuperación de terminales.

Nota

El modo de no NPIV no está disponible en configuraciones de alta disponibilidad. NPIV está habilitado de forma predeterminada y no se puede desactivar.

Nota

En el modo de NPIV, los terminales:

- Tienen una dirección principal de sistema.
- Pueden tener cero o más direcciones secundarias de sistema.
- Son todos aptos para la conmutación por error a una dirección de sistema alternativa en caso de que falle un puerto; sin embargo, no se admite la conmutación por error a un puerto marginal.
- Pueden restablecerse mediante conmutación por error para usar su puerto primario cuando el puerto vuelve a estar en línea.

Nota

Cuando se usa NPIV, se recomienda usar un solo protocolo (es decir, DD VTL Fibre Channel, DD Boost mediante Fibre Channel o vDisk Fibre Channel) por terminal. Para las configuraciones de conmutación por error, también se deben configurar los terminales secundarios para que tengan el mismo protocolo que la instancia primaria.

Procedimiento

1. Seleccione **Hardware** > **Fibre Channel** > **Resources**.
2. En **Endpoints**, seleccione **Add** (signo +).

3. En el cuadro de diálogo Add Endpoint, ingrese un nombre para el terminal (de 1 a 128 caracteres). El campo no puede estar vacío o contener la palabra “all”, y no puede contener los caracteres asterisco (*), signo de interrogación (?), barras frontal o trasera (/, \) o paréntesis derecho o izquierdo [(,)].
4. En Endpoint Status, seleccione Enabled o Disabled.
5. Si está habilitado NPIV, para la dirección del sistema primario, seleccione un valor de la lista desplegable. La dirección primaria del sistema debe ser distinta a cualquier dirección secundaria del sistema.
6. Si está habilitado NPIV, para las operaciones de conmutación por error a las direcciones secundarias del sistema, seleccione la casilla correspondiente junto a la dirección secundaria del sistema.
7. Seleccione **OK**.

Configuración de un terminal

Después de que haya agregado un terminal, puede modificarlo mediante el cuadro de diálogo Configure Endpoint.

Nota

Cuando se usa NPIV, se recomienda usar un solo protocolo (es decir, DD VTL Fibre Channel, DD Boost mediante Fibre Channel o vDisk Fibre Channel) por terminal. Para las configuraciones de conmutación por error, también se deben configurar los terminales secundarios para que tengan el mismo protocolo que la instancia primaria.

Procedimiento

1. Seleccione **Hardware** > **Fibre Channel** > **Resources**.
2. En **Endpoints**, seleccione un terminal y, a continuación, seleccione **Modify** (lápiz).
3. En el cuadro de diálogo Configure Endpoint, ingrese un nombre para el terminal (de 1 a 128 caracteres). El campo no puede estar vacío o contener la palabra “all”, y no puede contener los caracteres asterisco (*), signo de interrogación (?), barras frontal o trasera (/, \) o paréntesis derecho o izquierdo [(,)].
4. En Endpoint Status, seleccione Enabled o Disabled.
5. Para la dirección del sistema primario, seleccione un valor de la lista desplegable. La dirección primaria del sistema debe ser distinta a cualquier dirección secundaria del sistema.
6. Para las operaciones de conmutación por error a las direcciones secundarias del sistema, seleccione la casilla correspondiente junto a la dirección secundaria del sistema.
7. Seleccione **OK**.

Modificación de la dirección del sistema de un extremo

Puede modificar la dirección del sistema activo de un extremo de destino de SCSI con la opción del comando `scsitarget endpoint modify`. Esto resulta útil si el extremo está asociado con una dirección del sistema que ya no existe, por ejemplo, después de una actualización de la controladora o cuando se transfirió una HBA (host bus adapter) de la controladora. Cuando se modifica la dirección del sistema para un extremo, todas las propiedades del extremo, incluidas WWPN y WWNN (nombre de puerto mundial y de nodos, respectivamente), si existen, se preservan y se utilizan con la nueva dirección del sistema.

En el siguiente ejemplo, el extremo ep-1 se asignó a la dirección del sistema 5a, pero esta dirección del sistema ya no es válida. Una nueva HBA de la controladora se

agregó a la dirección del sistema 10a. El subsistema de destino de SCSI creó automáticamente un nuevo extremo, ep-new, para la nueva dirección de sistema. Debido a que solo un único extremo puede asociarse con una dirección del sistema determinada, ep-new debe eliminarse y, luego, ep-1 debe asignarse a la dirección del sistema 10a.

Nota

El extremo modificado puede demorar un poco en conectarse en línea, según el ambiente SAN, ya que el WWPN y el WWNN se han transferido a una dirección del sistema diferente. Es posible que necesite actualizar la zonificación de SAN para que refleje la nueva configuración.

Procedimiento

1. Muestre todos los extremos para verificar los que se deben modificar:

   ```
   # scsitarget endpoint show list
   ```

2. Deshabilite todos los extremos:

   ```
   # scsitarget endpoint disable all
   ```

3. Elimine el extremo nuevo e innecesario, ep-new:

   ```
   # scsitarget endpoint del ep-new
   ```

4. Modifique el extremo que desea usar, ep-1, asignándola a la nueva dirección del sistema, 10a:

   ```
   # scsitarget endpoint modify ep-1 system-address 10a
   ```

5. Habilite todos los extremos:

   ```
   # scsitarget endpoint enable all
   ```

Habilitación de un punto final

La habilitación de un punto final habilita el puerto solo si este actualmente está deshabilitado, es decir, si el sistema opera en modo de no NPIV.

Procedimiento

1. Seleccione **Hardware** > **Fibre Channel** > **Resources**.
2. Seleccione **More Tasks** > **Endpoints** > **Enable**. Si todos los puntos finales ya están activados, se muestra un mensaje al respecto.
3. En el cuadro de diálogo Enable Endpoints, seleccione uno o más terminales de la lista y seleccione **Next**.
4. Después de la confirmación, seleccione **Next** para completar la tarea.

Desactivación de un punto final

La deshabilitación de un punto final no deshabilita el puerto asociado, a menos que se deshabiliten todos los puntos finales que usan el puerto, es decir, el sistema opera en modo de no NPIV.

Procedimiento

1. Seleccione **Hardware** > **Fibre Channel** > **Resources**.
2. Seleccione **More Tasks** > **Endpoints** > **Disable**.

3. En el cuadro de diálogo Disable Endpoints, seleccione uno o más puntos finales de la lista y seleccione **Next**. Si un punto final está en uso, se le advierte que al deshabilitarlo puede interrumpir el sistema.
4. Seleccione **Next** para completar la tarea.

Eliminación de un punto final

Posiblemente quiera eliminar un punto final si el hardware subyacente ya no está disponible. Sin embargo, si aún hay hardware subyacente presente, o si hay hardware subyacente que se pasa a estar disponible, de manera automática se descubre un nuevo punto final para el hardware y se configura según los valores predeterminados.

Procedimiento

1. Seleccione **Hardware** > **Fibre Channel** > **Resources**.
2. Seleccione **More Tasks** > **Endpoints** > **Delete**.
3. En el cuadro de diálogo Delete Endpoints, seleccione uno o más puntos finales de la lista y seleccione **Next**. Si un punto final está en uso, se le advierte acerca de que eliminarlo puede interrumpir el sistema.
4. Seleccione **Next** para completar la tarea.

Cómo agregar un iniciador

Agregue iniciadores para proporcionar clientes de respaldo a fin de conectar el sistema a los datos de lectura y escritura usando el protocolo FC (Fibre Channel). Un iniciador específico puede admitir DD Boost mediante FC o DD VTL, pero no ambos. Se puede configurar un máximo de 1024 iniciadores para un sistema DD.

Procedimiento

1. Seleccione **Hardware** > **Fibre Channel** > **Resources**.
2. En Initiators, seleccione Add (signo +)
3. En el cuadro de diálogo Add Initiator, ingrese el WWPN único del puerto en el formato especificado.
4. Ingrese un nombre para el iniciador.
5. Seleccione el método de dirección: **Auto** se usa para las direcciones estándar y **VSA** (Volume Set Addressing) se usa principalmente para los buses virtuales de direcciones, objetivos y LUN..
6. Seleccione **OK**.

Equivalente de la CLI

```
# scsitarget group add My_Group initiator My_Initiator
```

Modificación o eliminación de un iniciador

Antes de eliminar un iniciador, debe estar offline y no debe estar conectado a ningún grupo. De lo contrario, obtendrá un mensaje de error y el iniciador no se eliminará. Debe eliminar todos los iniciadores en un grupo de acceso antes de eliminar el grupo de acceso. Si un iniciador permanece visible, es posible redescubrirlo automáticamente.

Procedimiento

1. Seleccione **Hardware** > **Fibre Channel** > **Resources**.

2. En Initiators, seleccione uno de los iniciadores. Si desea eliminarlo, seleccione Delete (X). Si desea modificarlo, seleccione Modify (lápiz) para que se muestre el cuadro de diálogo Modify Initiator.
3. Cambie el nombre o el método de dirección del iniciador (**Auto** se usa para las direcciones estándar y **VSA** [Volume Set Addressing] se usa principalmente para los buses virtuales de direcciones, objetivos y LUN).
4. Seleccione **OK**.

Recomendación para configurar los alias de iniciadores: solo CLI
Se recomienda enfáticamente que los alias de iniciadores se configuren para minimizar confusiones y errores humanos durante el proceso de configuración.

```
# vtl initiator set alias NewAliasName wwpn 21:00:00:e0:8b:9d:0b:e8
# vtl initiator show
Initiator  Group    Status   WWNN                     WWPN                     Port
---------  -------  -------  -----------------------  -----------------------  ---
NewVTL     aussie1  Online   20:00:00:e0:8b:9d:0b:e8  21:00:00:e0:8b:9d:0b:e8  6a
                    Offline  20:00:00:e0:8b:9d:0b:e8  21:00:00:e0:8b:9d:0b:e8  6b

Initiator  Symbolic Port Name  Address Method
---------  ------------------  --------------
NewVTL                              auto
---------  ------------------  --------------
```

Configuración de una dirección física (ID de loop)

Algunos software de respaldo requieren que todos los objetivos de loop privados tengan una dirección física (ID de loop) que no entre en conflicto con otro nodo. El rango para un ID de loop es de 0 a 125.

Procedimiento

1. Seleccione **Hardware** > **Fibre Channel** > **Resources**.
2. Seleccione **More Tasks** > **Set Loop ID**.
3. En el cuadro de diálogo Set Loop ID, ingrese el ID de loop (de 0 a 125) y seleccione **OK**.

Configuración de opciones de conmutación por error

Puede configurar opciones de conmutación por error y conmutación por recuperación automáticas cuando NPIV está habilitado.

Este es el comportamiento esperado para la conmutación por error de puertos Fibre Channel, por aplicación:

- Se espera que las operaciones de DD Boost mediante Fibre Channel continúen sin intervención del usuario cuando se realiza una conmutación por error de los terminales Fibre Channel.
- Se espera que las operaciones de DD VTL de Fibre Channel se interrumpan cuando se realiza una conmutación por error de los puntos finales de DD VTL de Fibre Channel. Es posible que deba realizar descubrimiento (es decir, descubrimiento del sistema operativo y la configuración de los dispositivos DD VTL) en los iniciadores mediante el terminal Fibre Channel afectado. Debe prever un reinicio de las operaciones activas de respaldo y restauración.
- Se espera que las operaciones de Fibre Channel de vDisk) continúen sin intervención del usuario cuando se realiza una conmutación por error de los punto finales Fibre Channel.

No se garantiza la conmutación por recuperación automática si todos los puertos se deshabilitan y posteriormente se habilitan (acción que podría ser activada por el administrador), ya que no se especifica el orden en el que se habilitan los puertos.

Procedimiento

1. Seleccione **Hardware** > **Fibre Channel** > **Resources**.
2. Seleccione **More Tasks** > **Set Failover Options**.
3. En el cuadro de diálogo Set Failover Options, ingrese los valores de demora conmutación por error y conmutación por recuperación (en segundos), especifique si se debe habilitar la conmutación por error automática y seleccione **OK**.

Pestaña Access Groups

La pestaña **Hardware** > **Fibre Channel** > **Access Groups** proporciona información sobre grupos de acceso de DD VTL y DD Boost. Si selecciona el vínculo a *View DD Boost Groups* o *View VTL Groups*, el sistema lo dirige a las páginas de DD Boost o DD VTL.

Tabla 126 Grupos de acceso

Elemento	Descripción
Group Name	Nombre del grupo de acceso.
Servicio	Servicio para este grupo de acceso: DD Boost o DD VTL.
Terminales	Terminales asociados con este grupo de acceso.
Initiators	Iniciadores asociados con este grupo de acceso.
Number of Devices.	Cantidad de dispositivos asociados con este grupo de acceso.

Diferencias entre el monitoreo de vínculos de FC entre las versiones de SO de DD

Las diferentes versiones de SO de DD manejan el monitoreo de vínculos de FC (Fibre Channel) de diversas maneras.

SO de DD 5.3 y posterior
El monitoreo de puertos detecta un puerto FC en el reinicio de sistema y emite una alerta si el puerto está habilitado y offline. Para quitar la alerta, deshabilite cualquier puerto que no se use con los comandos `scsitarget port`.

SO de DD 5.1 hasta 5.3
Si un puerto está offline, una alerta le avisa que el vínculo está caído. Esta alerta está administrada, lo que significa que permanece activa hasta que se la quita. Esto ocurre cuando el puerto FC de DD VTL está en línea o deshabilitado. Si el puerto no está en uso, deshabilítelo a menos que deba ser monitoreado.

SO de DD 5.0 hasta 5.1
Si un puerto está offline, una alerta le avisa que el vínculo está caído. La alerta no está administrada, lo que significa que no permanece activa y no aparece en la lista de alertas actual. Cuando el puerto está en línea, una alerta le avisa que el vínculo está activo. Si el puerto no está en uso, deshabilítelo a menos que deba ser monitoreado.

SO de DD 4.9 hasta 5.0

Se debe incluir un puerto FC en un grupo DD VTL para que se monitoree.

CAPÍTULO 14

Trabajo con DD Boost

Este capítulo incluye:

- Acerca de Data Domain Boost 352
- Administración de DD Boost con DD System Manager 353
- Acerca de los grupos de interfaces 369
- Destrucción de DD Boost 377
- Configuración de DD Boost-over-Fibre Channel 377
- Uso de DD Boost en sistemas de alta disponibilidad 382
- Acerca de las pestañas de DD Boost 382

Acerca de Data Domain Boost

Data Domain Boost (DD Boost) ofrece integración avanzada con aplicaciones empresariales y de respaldo para mejorar el rendimiento y facilitar el uso. DD Boost distribuye partes del proceso de deduplicación a un servidor de respaldo o un cliente de aplicación, lo cual permite la deduplicación del lado del cliente para lograr procesos de respaldo y recuperación más rápidos y más eficientes.

DD Boost es un producto opcional que requiere una licencia independiente para operar en el sistema Data Domain. Puede comprar una clave de licencia del software DD Boost para un sistema Data Domain directamente de Data Domain.

Nota

Una licencia especial, BLOCK-SERVICES-PROTECTPOINT, está disponible para permitir a los clientes usar los servicios de bloques de ProtectPoint para tener la funcionalidad de DD Boost sin una licencia de DD Boost. Si está habilitado DD Boost ProtectPoint solo para clientes (es decir, si solo se instaló la licencia de BLOCK-SERVICES-PROTECTPOINT) el estado de la licencia indica que DD Boost esté habilitado para ProtectPoint solamente.

DD Boost cuenta con dos componentes: un componente que se ejecuta en el servidor de respaldo y otro que se ejecuta en el sistema Data Domain.

- En el contexto de la aplicación de respaldo NetWorker, la aplicación de respaldo Avamar y otras aplicaciones de respaldo de partners de DDBoost, el componente que se ejecuta en el servidor de respaldo (bibliotecas de DD Boost) se integra en la aplicación de respaldo específica.
- En el contexto de las aplicaciones de respaldo de Symantec (NetBackup y Backup Exec) y el plug-in Oracle RMAN, debe descargar una versión adecuada del plug-in DD Boost que se instala en cada servidor de medios. El plug-in DD Boost incluye las bibliotecas DD Boost para integrarse con el servidor DD Boost que se ejecuta en el sistema Data Domain.

La aplicación de respaldo (por ejemplo, Avamar, NetWorker, NetBackup o Backup Exec) establece políticas que controlan cuándo ocurren los respaldos y las duplicaciones. Los administradores administran el respaldo, la duplicación y las restauraciones desde una sola consola y pueden usar todas las funciones de DD Boost, incluido el software Replicator con eficiencia de WAN. La aplicación administra todos los archivos (colecciones de datos) en el catálogo, incluso aquellos creados por el sistema Data Domain.

En el sistema Data Domain, las unidades de almacenamiento que usted crea se exponen a aplicaciones de respaldo que usan el protocolo DD Boost. Para las aplicaciones de Symantec, las unidades de almacenamiento se visualizan como pools de discos. Para Networker, las unidades de almacenamiento se visualizan como unidades lógicas de almacenamiento (LSU). Una unidad de almacenamiento es un MTree; por lo tanto, admite configuración de cuotas de MTree. (No cree un MTree en lugar de una unidad de almacenamiento).

Este capítulo no contiene instrucciones de instalación. Consulte la documentación del producto que desee instalar. Por ejemplo, para obtener información sobre la configuración de DD Boost con aplicaciones de respaldo de Symantec (NetBackup y Backup Exec), consulte la *Guía de administración de Data Domain Boost para OpenStorage*. Para obtener información sobre la configuración de DD Boost con cualquier otra aplicación, consulte la documentación específica de la aplicación.

También puede encontrarse información adicional sobre la configuración y la administración de DD Boost en el sistema Data Domain en la *Guía de administración de Data Domain Boost para OpenStorage* (para NetBackup y Backup Exec) y la *Guía de administración de Data Domain Boost para integración de partners* (para otras aplicaciones de respaldo).

Administración de DD Boost con DD System Manager

Acceda a la vista DD Boost en DD System Manager.

Procedimiento

1. Seleccione **Data Management** > **File System**. Verifique que el sistema de archivos esté habilitado y en ejecución; para ello, escriba lo siguiente:
2. Seleccione **Protocols** > **DD Boost**.

   Si accede a la página DD Boost sin una licencia, el estado indica que DD Boost no tiene licencias. Haga clic en **Add License** e ingrese una licencia válida en el cuadro de diálogo Add License Key.

   Nota

   Una licencia especial, BLOCK-SERVICES-PROTECTPOINT, está disponible para permitir a los clientes usar los servicios de bloques de ProtectPoint para tener la funcionalidad de DD Boost sin una licencia de DD Boost. Si está habilitado DD Boost ProtectPoint solo para clientes (es decir, si solo se instaló la licencia de BLOCK-SERVICES-PROTECTPOINT) el estado de la licencia indica que DD Boost esté habilitado para ProtectPoint solamente.

   Use las pestañas de DD Boost (Settings, Active Connections, IP Network, Fibre Channel y Storage Units) para administrar DD Boost.

Especificación de nombres de usuario de DD Boost

Un usuario de DD Boost también es usuario de DD OS. Puede especificar un usuario de DD Boost al seleccionar un nombre de usuario de DD OS existente o al crear uno nuevo y hacer que sea un usuario de DD Boost.

Las aplicaciones de respaldo usan el nombre de usuario y la contraseña de DD Boost para conectarse al sistema Data Domain. Debe configurar esta información de identificación en cada servidor de respaldo que se conecte a este sistema. El sistema Data Domain admite varios usuarios de DD Boost: Para obtener información completa sobre la configuración de DD Boost con Symantec NetBackup y Backup Exec, consulte la *Guía de administración de Data Domain Boost para OpenStorage*. Para obtener información sobre cómo configurar DD Boost con otras aplicaciones, consulte la *Guía de administración de Data Domain Boost para integración de partners* y la documentación específica de la aplicación.

Procedimiento

1. Seleccione **Protocols** > **DD Boost**.
2. Seleccione **Add** (+) arriba de la lista Users with DD Boost Access.

   Aparecerá el cuadro de diálogo Add User.

3. Para seleccionar un usuario existente, seleccione el nombre de usuario en la lista desplegable.

Si es posible, seleccione un nombre de usuario con los privilegios de función de administración establecidos en *none*.

4. Para crear y seleccionar un usuario nuevo, seleccione **Create a new Local User** y realice lo siguiente:
   a. Ingrese el nombre de usuario nuevo en el campo User.

      El usuario debe estar configurado en la aplicación de respaldo para conectarse al sistema Data Domain.

   b. Escriba la contraseña dos veces en los campos adecuados.
5. Haga clic en **Add**.

Cambio de contraseñas de usuario de DD Boost

Puede cambiar una contraseña de usuario de DD Boost.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **Settings**.
2. Seleccione un usuario de la lista Users with DD Boost Access.
3. Haga clic en el botón **Edit** (ícono de lápiz) que aparece arriba de la lista de usuarios de DD Boost.

   Aparecerá el cuadro de diálogo Change Password.

4. Escriba la contraseña dos veces en los cuadros adecuados.
5. Haga clic en **Change**.

Eliminación de un nombre de usuario de DD Boost

Puede eliminar un usuario de la lista de acceso de DD Boost.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **Settings**.
2. Seleccione el usuario que necesite eliminar de la lista Users with DD Boost Access.
3. Haga clic en **Remove** (X) arriba de la lista de usuarios de DD Boost.

   Aparecerá el cuadro de diálogo Remove User.

4. Haga clic en **Remove**.

   Después de la eliminación, el usuario permanece en la lista de acceso de DD OS.

Activación de DD Boost

Puede usar la pestaña DD Boost Settings para habilitar DD Boost y seleccionar o agregar un usuario de DD Boost.

Procedimiento

1. Seleccione **Protocols** > **DD Boost**.
2. En el área DD Boost Status, haga clic en **Enable**.

   Aparecerá el cuadro de diálogo Enable DD Boost.

3. Seleccione un nombre de usuario existente del menú o agregue un usuario nuevo; para ello, proporcione el nombre, la contraseña y la función.

Configuración de Kerberos

Puede configurar Kerberos mediante la pestaña DD Boost Settings.

Procedimiento

1. Seleccione **Protocols > DD Boost > Settings**.
2. Haga clic en **Configure** en el área de estado de Kerberos Mode.

   Aparecerá la pestaña Authentication en **Administration > Access**.

   Nota

   También puede habilitar Kerberos navegando directamente a Authentication en **Administration > Access** en System Manager.

3. En Active Directory/Kerberos Authentication, haga clic en **Configure**.

   Se mostrará el cuadro de diálogo Active Directory/Kerberos Authentication. Elija el tipo de centro de distribución de claves de Kerberos (KDC) que desea usar:

   - **Disabled**

     Nota

     Si selecciona **Disabled**, los clientes de NFS no utilizarán la autenticación de Kerberos. Los clientes CIFS utilizan la autenticación de grupo de trabajo.

   - **Windows/Active Directory**

     Nota

     Complete los campos Realm Name, Under Name y Password para la autenticación de Active Directory.

   - **Unix**

     a. Ingrese el nombre de dominio, los nombres de host/dirección IP de uno a tres servidores KDC.

     b. Cargue el archivo keytab desde uno de los servidores KDC.

Desactivación de DD Boost

Al desactivar DD Boost, se cierran todas las conexiones con el servidor de respaldo. Cuando deshabilita o destruye DD Boost, el servicio FC de DD Boost también se deshabilitva.

Antes de comenzar

Asegúrese de que no haya trabajos en ejecución en la aplicación de respaldo antes de desactivarlo.

Nota

La replicación de archivos iniciada por DD Boost entre dos restauraciones de Data Domain no se cancela.

Procedimiento

1. Seleccione **Protocols** > **DD Boost**.
2. En el área DD Boost Status, haga clic en **Disable**.
3. Haga clic en **OK** en el cuadro de diálogo de confirmación Disable DD Boost.

Visualización de unidades de almacenamiento de DD Boost

Puede acceder a la pestaña Storage Units para ver y administrar unidades de almacenamiento de DD Boost.

La pestaña DD Boost Storage Unit:

- Muestra las unidades de almacenamiento y proporciona la siguiente información de cada unidad de almacenamiento:

Tabla 127 Información de la unidad de almacenamiento

Elemento	Descripción
Storage Unit	El nombre de la unidad de almacenamiento.
User	El usuario de DD Boost es el propietario de la unidad de almacenamiento.
Quota Hard Limit	El porcentaje de límite máximo de cuota utilizado.
Last 24 hr Pre-Comp	La cantidad de datos crudos de la aplicación de respaldo que se ha escrito en las últimas 24 horas.
Last 24 hr Post-Comp	La cantidad de almacenamiento utilizado después de la compresión en las últimas 24 horas.
Last 24 hr Comp Ratio	La proporción de compresión de las últimas 24 horas.
Weekly Avg Post-Comp	La cantidad promedio de almacenamiento comprimido utilizado en las últimas cinco semanas.
Last Week Post-Comp	La cantidad promedio de almacenamiento comprimido utilizado en los últimos siete días.
Weekly Avg Comp Ratio	La proporción de compresión promedio de las últimas cinco semanas.
Last Week Comp Ratio	La proporción de compresión promedio de los últimos siete días.

- Permite crear, modificar y eliminar unidades de almacenamiento.
- Muestra cuatro pestañas relacionadas para una unidad de almacenamiento seleccionada de la lista: Storage Unit, Space Usage, Daily Written y Data Movement.

  Nota

  La pestaña Data Movement está disponible solo si se instaló la licencia opcional de Data Domain Extended Retention (anteriormente DD Archiver) o Data Domain Cloud Tier (DD Cloud Tier).

- Lo lleva a la pestaña **Replication** > **On-Demand** > **File Replication**, donde puede hacer clic en el vínculo **View DD Boost Replications**.

Nota

Se requiere una licencia de DD Replicator para que DD Boost muestre pestañas que no sean la pestaña File Replication.

Creación de una unidad de almacenamiento

Debe crear al menos una unidad de almacenamiento en el sistema Data Domain, y se debe asignar un usuario de DD Boost a esa unidad. Puede usar la pestaña Storage Units para crear una unidad de almacenamiento.

Cada unidad de almacenamiento es un subdirectorio de nivel superior del directorio `/data/col1`; no hay jerarquía entre las unidades de almacenamiento.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **Storage Units**.
2. Haga clic en **Create** (+).

   Aparecerá el cuadro de diálogo Create Storage Unit.

3. Ingrese el nombre de la unidad de almacenamiento en el cuadro Name.

   El nombre de cada unidad de almacenamiento debe ser único. Los nombres de las unidades de almacenamiento pueden contener hasta 50 caracteres. Puede utilizar los siguientes caracteres:

   - caracteres alfabéticos en mayúscula y minúscula: A-Z, a-z
   - números: 0-9
   - espacio insertado

     Nota

     El nombre de la unidad de almacenamiento debe estar entre comillas dobles (") si tiene un espacio insertado.

   - coma (,)
   - punto (.), siempre y cuando no preceda al nombre
   - signo de exclamación (!)
   - signo de número (#)
   - signo de dólar ($)
   - signo de porcentaje (%)
   - signo más (+)
   - arroba (@)
   - signo de igual (=)
   - Y comercial (&)
   - punto y coma (;)
   - paréntesis [(y)]
   - corchetes ([y])
   - llaves ({ y })
   - signo de intercalación (^)

- tilde (~)
- apóstrofe (comilla simple recta)
- comilla simple inclinada (')
- signo menos (-)
- carácter de subrayado (_)

4. Para seleccionar un nombre de usuario existente que tendrá acceso a esta unidad de almacenamiento, seleccione el nombre de usuario de la lista desplegable.

   Si es posible, seleccione un nombre de usuario con los privilegios de función de administración establecidos en *none*.

5. Para crear y seleccionar un nombre de usuario nuevo que tendrá acceso a esta unidad de almacenamiento, seleccione **Create a new Local User** y realice lo siguiente:

   a. Ingrese el nombre de usuario nuevo en el cuadro User.

      El usuario debe estar configurado en la aplicación de respaldo para conectarse al sistema Data Domain.

   b. Escriba la contraseña dos veces en los cuadros adecuados.

6. Para configurar restricciones de espacio de almacenamiento a fin de evitar que una unidad de almacenamiento consuma espacio en exceso: ingrese una configuración de cuota de límite flexible o rígido, o un límite rígido y un límite flexible. Con un límite flexible, se envía una alerta cuando el tamaño de la unidad de almacenamiento supera el límite, pero aún se pueden escribir datos en ella. Los datos no se pueden escribir en la unidad de almacenamiento cuando se alcanza el límite estricto.

   Nota

   Los límites de la cuota son valores previamente comprimidos. Para establecer límites de la cuota, seleccione **Set to Specific Value** y especifique el valor. Seleccione la unidad de medida: MiB, GiB, TiB o PiB.

   Nota

   Cuando establece límites flexibles y estrictos, el límite flexible de una cuota no puede superar el límite estricto.

7. Haga clic en **Create**.
8. Repita los pasos anteriores para cada sistema Data Domain habilitado para Boost.

Visualización de información de unidades de almacenamiento

Desde la pestaña DD Boost Storage Units, puede seleccionar una unidad de almacenamiento y acceder a las pestañas Storage Unit, Space Usage, Daily Written y Data Movement para la unidad de almacenamiento seleccionada.

Pestaña Storage Unit
En la pestaña Storage Unit se muestra información detallada de una unidad de almacenamiento seleccionada en sus paneles Summary y Quota. El panel Snapshot

muestra detalles de la instantánea, le permite crear instantáneas y programaciones nuevas, y proporciona un vínculo a la pestaña **Data Management** > **Snapshots**.

- El panel Summary muestra información resumida de la unidad de almacenamiento seleccionada.

  Tabla 128 Panel Summary

Elemento de Summary	Descripción
Total Files	El número total de imágenes de archivos en la unidad de almacenamiento. Para obtener detalles de compresión que puede descargar en un archivo de registro, haga clic en el vínculo Download Compression Details. La generación puede llevar varios minutos. Una vez que se complete, haga clic en Download.
Full Path	`/data/col1/filename`
Status	R: lectura; W: escritura; Q: cuota definida
Pre-Comp Used	La cantidad de almacenamiento previamente comprimido que ya está en uso.

- El panel Quota muestra información de cuotas de la unidad de almacenamiento seleccionada.

  Tabla 129 Panel Quota

Elemento de Quota	Descripción
Quota Enforcement	Enabled o Disabled. Al hacer clic en Quota, se accede a la pestaña **Data Management** > **Quota**, donde puede configurar cuotas.
Pre-Comp Soft Limit	El valor actual del conjunto de cuotas de advertencia para la unidad de almacenamiento.
Pre-Comp Hard Limit	El valor actual del conjunto de cuotas máximas para la unidad de almacenamiento.
Quota Summary	Porcentaje de límite duro utilizado.

  Para modificar los límites máximo y de advertencia previos a la compresión que se muestran en la pestaña:

  1. Haga clic en el vínculo **Quota** en el panel Quota.
  2. En el cuadro de diálogo Configure Quota, especifique valores para cuotas máximas y de advertencia y seleccione la unidad de medida: MiB, GiB, TiB o PiB. Haga clic en **OK**.

- Instantáneas
  El panel Snapshots muestra información sobre las instantáneas de la unidad de almacenamiento.

  Tabla 130 Panel Snapshots

Elemento	Descripción
Total Snapshots	El número total de instantáneas creados para este MTree. Se puede crear un total de 750 instantáneas para cada MTree.

Tabla 130 Panel Snapshots (continuación)

Elemento	Descripción
Expired	El número de instantáneas en este MTree que se han marcado para su eliminación, pero que todavía no se han quitado con la operación de borrado.
Unexpired	El número de instantáneas en este MTree que están marcados para conservarse.
Oldest Snapshot	La fecha de la instantánea más antigua para este MTree.
Newest Snapshot	La fecha de la instantánea más reciente para este MTree.
Next Scheduled	La fecha de la próxima instantánea programado.
Assigned Snapshot Schedules	El nombre de la programación de instantáneas asignada a este MTree.

Mediante el panel Snapshots, puede realizar las siguientes acciones:

- Asigne una programación de instantáneas a una unidad de almacenamiento seleccionada: Haga clic en **Assign Schedules**. Seleccione la casilla de verificación de la programación y haga clic en **OK** y **Close**.
- Cree una programación nueva: Haga clic en **Assign Snapshot Schedules** > **Create Snapshot Schedule**. Especifique el nombre de la programación nueva.

  Nota

  El nombre de la instantánea puede estar compuesto únicamente por letras, números, _, -, `%d` (día numérico del mes: 01-31), `%a` (nombre abreviado del día de semana), `%m` (mes numérico del año: 01-12), `%b` (nombre abreviado del mes), `%y` (año, dos dígitos), `%Y` (año, cuatro dígitos), `%H` (horas: 00-23) y `%M` (minutos: 00-59), siguiendo el patrón que se muestra en el cuadro de diálogo. Especifique el patrón nuevo y haga clic en **Validate Pattern & Update Sample**. Haga clic en **Next**.

  - Seleccione cuándo se ejecutará la programación: semanalmente, todos los días (o en días seleccionados), mensualmente en días específicos que selecciona al hacer clic en la fecha en la programación, o el último día del mes. Haga clic en **Next**.
  - Especifique las horas del día a las que se debe ejecutar la programación: Seleccione At Specific Times o In Intervals. Si selecciona una hora específica, selecciónela de la lista. Haga clic en Add (**+**) para agregar una hora (formato de 24 horas). Para intervalos, seleccione In Intervals y establezca las horas de inicio y de finalización, y la frecuencia (Every); por ejemplo, cada ocho horas. Haga clic en **Next**.
  - Especifique el período de retención para las instantáneas en días, meses o años. Haga clic en **Next**.
  - Revise el resumen de la configuración. Haga clic en **Back** para editar valores. Haga clic en **Finish** para crear la programación.

- Haga clic en el vínculo Snapshots para ir a la pestaña **Data Management** > **Snapshots**.

Pestaña Space Usage
El gráfico de la pestaña Space Usage muestra una representación visual del uso de datos de la unidad de almacenamiento en el tiempo.

- Haga clic en un punto de una línea del gráfico para visualizar un cuadro con los datos de ese punto.
- Al hacer clic en **Print**(en la parte inferior del gráfico), se abre el cuadro de diálogo Print.
- Al hacer clic en **Show in new window**, se muestra el gráfico en una nueva ventana del navegador.

Se muestran dos tipos de datos del gráfico: Espacio lógico utilizado (antes de la compresión) y la capacidad física utilizada (después de la compresión).

Pestaña Daily Written
La vista Daily Written contiene un gráfico donde se muestra una representación visual de los datos que se escriben diariamente en el sistema a lo largo de un período específico, que puede ser de 7 a 120 días. Se muestra el volumen de datos a través del paso del tiempo, con los volúmenes previos y posteriores a la compresión.

Pestaña Data Movement
Un gráfico en el mismo formato que el gráfico Daily Written que muestra la cantidad de espacio en disco movida al área de almacenamiento de DD Extended Retention (si la licencia de DD Extended Retention está habilitada).

Modificación de una unidad de almacenamiento

Puede usar el cuadro de diálogo Modify Storage Unit cara cambiar el nombre de una unidad de almacenamiento, seleccionar un usuario existente diferente, crear y seleccionar un usuario nuevo, y editar la configuración de cuotas.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **Storage Units**.
2. En la lista Storage Unit, seleccione la unidad de almacenamiento que desee modificar.
3. Haga clic en el ícono de lápiz.

   Aparecerá el cuadro de diálogo Modify Storage Unit.

4. Para cambiar el nombre de la unidad de almacenamiento, edite el texto del campo **Name**.
5. Para seleccionar un usuario existente diferente, seleccione el nombre de usuario en la lista desplegable.

   Si es posible, seleccione un nombre de usuario con los privilegios de función de administración establecidos en *none*.

6. Para crear y seleccionar un usuario nuevo, seleccione **Create a new Local User** y realice lo siguiente:
   a. Ingrese el nombre de usuario nuevo en el cuadro User.

      El usuario debe estar configurado en la aplicación de respaldo para conectarse al sistema Data Domain.

   b. Escriba la contraseña dos veces en los cuadros adecuados.
7. Edite Quota Settings según sea necesario.

Para configurar restricciones de espacio de almacenamiento a fin de evitar que una unidad de almacenamiento consuma espacio en exceso: ingrese una configuración de cuota de límite flexible o rígido, o un límite rígido y un límite flexible. Con un límite flexible, se envía una alerta cuando el tamaño de la unidad de almacenamiento supera el límite, pero aún se pueden escribir datos en ella. Los datos no se pueden escribir en la unidad de almacenamiento cuando se alcanza el límite estricto.

Nota

Los límites de la cuota son valores previamente comprimidos. Para establecer límites de la cuota, seleccione **Set to Specific Value** y especifique el valor. Seleccione la unidad de medida: MiB, GiB, TiB o PiB.

Nota

Cuando establece límites flexibles y estrictos, el límite flexible de una cuota no puede superar el límite estricto.

8. Haga clic en **Modify**.

Cambio de nombre de una unidad de almacenamiento

Puede usar el cuadro de diálogo Modify Storage Unit para cambiar el nombre de una unidad de almacenamiento.

Al cambiar el nombre de una unidad de almacenamiento, se cambia el nombre, pero se conserva lo siguiente:

- Propiedad de nombre de usuario
- Configuración de límite de flujo
- Configuración de cuota de capacidad y tamaño físico informado
- Asociación de AIR en el sistema Data Domain local

Procedimiento

1. Vaya a **Protocols** > **DD Boost** > **Storage Units**.
2. En la lista Storage Unit, seleccione la unidad de almacenamiento a la que desee cambiarle el nombre.
3. Haga clic en el ícono de lápiz.

   Aparecerá el cuadro de diálogo Modify Storage Unit.

4. Edite el texto del campo **Name**.
5. Haga clic en **Modify**.

Eliminación de una unidad de almacenamiento

Puede usar la pestaña Storage Units para eliminar una unidad de almacenamiento del sistema Data Domain. Al eliminar una unidad de almacenamiento, se elimina la unidad y todas las imágenes contenidas allí del sistema Data Domain.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **Storage Units**.

2. Seleccione la unidad de almacenamiento que se eliminará de la lista.
3. Hagaclic en Delete (**X**).
4. Haga clic en **OK**.

Resultados

La unidad de almacenamiento se eliminará del sistema Data Domain. También debe quitar manualmente las entradas del catálogo de la aplicación de respaldo.

Cómo revertir la eliminación de una unidad de almacenamiento

Puede usar la pestaña Storage Units para revertir la eliminación de una unidad de almacenamiento.

Al revertir la eliminación de una unidad de almacenamiento se recupera una unidad eliminada anteriormente, incluido lo siguiente:

- Propiedad de nombre de usuario
- Configuración de límite de flujo
- Configuración de cuota de capacidad y tamaño físico informado
- Asociación de AIR en el sistema Data Domain local

Nota

Las unidades de almacenamiento eliminadas están disponibles hasta que se ejecuta el siguiente comando `filesys clean`.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **Storage Units** > **More Tasks** > **Undelete Storage Unit...**.
2. En el cuadro de diálogo Undelete Storage Units, seleccione las unidades de almacenamiento de las que desee revertir la eliminación.
3. Haga clic en **OK**.

Selección de opciones de DD Boost

Puede usar el cuadro de diálogo Set DD Boost Options para especificar opciones de configuración para el procesamiento distribuido de segmentos, los respaldos sintéticos virtuales, la optimización de bajo ancho de banda para replicación de archivos, el cifrado de replicación de archivos y la preferencia de red de replicación de archivos (IPv4 o IPv6).

Procedimiento

1. Para mostrar la configuración de las opciones de DD Boost, seleccione **Protocols** > **DD Boost** > **Settings** > **Advanced Options**.
2. Para cambiar esta configuración, seleccione **More Tasks** > **Set Options**.

   Aparecerá el cuadro de diálogo Set DD Boost Options.

3. Seleccione las opciones que desee habilitar.
4. Deseleccione de las opciones que desee deshabilitar.

   Para deseleccionar una opción File Replication Network Preference, seleccione otra opción.

5. Configure las opciones de seguridad de DD Boost.
   a. Seleccione una opción de **Authentication Mode**:
      - None
      - Two-way
      - Two-way Password
   b. Seleccione una opción de **Encryption Strength**:
      - None
      - Medium
      - High

   El sistema Data Domain compara el modo de autenticación y el nivel de cifrado globales con el modo de autenticación y el nivel de cifrado por cliente para calcular el modo de autenticación eficaz y el nivel de cifrado de autenticación. El sistema no utiliza el modo de autenticación más alto de una entrada y la configuración de cifrado más alta de otra entrada. El modo de autenticación eficaz y el nivel de cifrado provienen de la entrada única que proporciona el modo de autenticación más alto.
6. Haga clic en **OK**.

Nota

También puede administrar el procesamiento distribuido de segmentos mediante los comandos `ddboost option`, que se describen en la *Guía de referencia de comandos de Data Domain Operating System*.

Procesamiento distribuido de segmentos

El procesamiento distribuido de segmentos aumenta el rendimiento de respaldo prácticamente en todos los casos al eliminar la transmisión de datos duplicados entre el servidor de medios y el sistema Data Domain.

Puede administrar el procesamiento distribuido de segmentos por medio de los comandos `ddboost option`, que se describen en la *Guía de referencia de comandos de Data Domain Operating System*.

Nota

El procesamiento distribuido de segmentos está habilitado de forma predeterminada con las configuraciones de Data Domain Extended Retention (anteriormente Data Domain Archiver) y no se puede deshabilitar.

Respaldos sintéticos virtuales

Un respaldo completo sintético virtual es la combinación del último respaldo completo (sintético o completo) y todos los respaldos incrementales posteriores. Los respaldos sintéticos virtuales están activados de forma predeterminada.

Optimización de ancho de banda bajo

Si usa replicación de archivos en una red con bajo ancho de banda (WAN), puede aumentar la velocidad de replicación mediante el uso de optimización de bajo ancho de banda. Esta función proporciona compresión adicional durante la transferencia de

datos. La compresión con bajo ancho de banda está disponible para sistemas Data Domain con una licencia de Replication instalada.

La optimización de bajo ancho de banda, que está deshabilitada de forma predeterminada, está diseñada para usarse en redes con menos de 6 Mb/s de ancho de banda agregado. No use esta opción si se requiere el máximo rendimiento de escritura del sistema de archivos.

Nota

También puede administrar la optimización de ancho de banda bajo por medio de los comandos `ddboost file-replication` , que se describen en detalle en la *Guía de referencia de comandos de Data Domain Operating System*.

Cifrado de replicación de archivos

Puede cifrar el flujo de replicación de datos al habilitar la opción de cifrado de replicación de archivos de DD Boost.

Nota

Si el cifrado de replicación de archivos de DD Boost se usa en los sistemas sin la opción Data at Rest, se debe activar en los sistemas de origen y de destino.

Configuración de puertos TCP de replicación administrada de archivos
Para la replicación administrada de archivos de DD Boost, use el mismo puerto de escucha global en los sistemas Data Domain de origen y de destino. Para configurar el puerto de escucha, use el comando `replication option` como se describe en la *Guía de referencia de comandos de Data Domain Operating System*.

Preferencia de red de replicación de archivos

Use esta opción para establecer el tipo de red de preferencia para la replicación de archivos de DD Boost en IPv4 o IPv6.

Administración de certificados para DD Boost

Un certificado de host permite que los programas de clientes de DD Boost verifiquen la identidad del sistema cuando se establece una conexión. Los certificados de CA identifican autoridades de certificación que deben ser de confianza para el sistema. En los temas de esta sección se describe cómo administrar certificados de host y de CA para DD Boost.

Cómo agregar un certificado de host para DD Boost

Agregue un certificado de host al sistema. DD OS admite un certificado de host para DD Boost.

Procedimiento

1. Si aún no ha solicitado un certificado de host, solicítelo a una CA de confianza.
2. Cuando haya recibido un certificado de host, cópielo o muévalo a la computadora desde la que ejecuta DD Service Manager.
3. Inicie DD System Manager en el sistema en el que desee agregar un certificado de host.

Nota

DD System Manager admite administración de certificados solo en el sistema de administración (que es el sistema que ejecuta DD System Manager).

4. Seleccione **Protocols** > **DD Boost** > **More Tasks** > **Manage Certificates...**

Nota

Si intenta administrar certificados de forma remota en un sistema administrado, DD System Manager muestra un mensaje de información en la parte superior del cuadro de diálogo de administración de certificados. Para administrar certificados para un sistema, debe iniciar DD System Manager en ese sistema.

5. En el área Host Certificate, haga clic en **Add**.
6. Para agregar un certificado de host adjunto en un archivo .p12, realice lo siguiente:
   a. Seleccione **I want to upload the certificate as a .p12 file**.
   b. Escriba la contraseña en el cuadro **Password**.
   c. Haga clic en **Browse** y seleccione el certificado de host para cargarlo en el sistema.
   d. Haga clic en **Add**.
7. Para agregar un certificado de host adjunto en un archivo .pem, realice lo siguiente:
   a. Seleccione **I want to upload the public key as a .pem file and use a generated private key**.
   b. Haga clic en **Browse** y seleccione el certificado de host para cargarlo en el sistema.
   c. Haga clic en **Add**.

Cómo agregar certificados de CA para DD Boost

Agregue un certificado para una CA de confianza al sistema. DD OS admite varios certificados para CA de confianza.

Procedimiento

1. Obtenga un certificado para la CA de confianza.
2. Copie o mueva el certificado de CA de confianza a la computadora desde la que ejecuta DD Service Manager.
3. Inicie DD System Manager en el sistema en el que desee agregar el certificado de CA.

Nota

DD System Manager admite administración de certificados solo en el sistema de administración (que es el sistema que ejecuta DD System Manager).

4. Seleccione **Protocols** > **DD Boost** > **More Tasks** > **Manage Certificates...**.

Nota

Si intenta administrar certificados de forma remota en un sistema administrado, DD System Manager muestra un mensaje de información en la parte superior del cuadro de diálogo de administración de certificados. Para administrar certificados para un sistema, debe iniciar DD System Manager en ese sistema.

5. En el área CA Certificates, haga clic en **Add**.

   Aparecerá el cuadro de diálogo Add CA Certificate for DD Boost.

6. Para agregar un certificado de CA adjunto en un archivo .pem, realice lo siguiente:
   a. Seleccione **I want to upload the certificate as a .pem file**.
   b. Haga clic en **Browse**, seleccione el archivo de certificado de host que desee cargar al sistema y haga clic en **Open**.
   c. Haga clic en **Add**.
7. Para agregar un certificado de CA con la función de copiar y pegar, realice lo siguiente:
   a. Copie el texto del certificado al portapapeles con los controles del sistema operativo.
   b. Seleccione **I want to copy and paste the certificate text**.
   c. Pegue el texto del certificado en el cuadro que aparece debajo de la selección de copiar y pegar.
   d. Haga clic en **Add**.

Administración de cifrado y acceso de clientes de DD Boost

Puede usar la pestaña DD Boost Settings para configurar qué clientes específicos, o conjuntos de clientes, pueden establecer una conexión de DD Boost con el sistema Data Domain y si el cliente usará cifrado o no. De forma predeterminada, el sistema se configura para permitir que todos los clientes tengan acceso, sin cifrado.

Nota

Si se habilita el cifrado en transferencia, esto tendrá un impacto en el rendimiento del sistema.

Nota

DD Boost ofrece opciones de cifrado y autenticación globales para defender su sistema frente a ataques de intermediario (MITM). Especifique la configuración de autenticación y cifrado utilizando la GUI o comandos de la CLI en el sistema Data Domain. Para obtener más información, consulte la *Guía de administración de Data Domain Boost for OpenStorage 3.4* y Cómo agregar un cliente de DD Boost en la página 367 o la *Guía de referencia de comandos de Datos Domain 6.1*.

Cómo agregar un cliente de DD Boost

Cree un cliente de DD Boost permitido y especifique si este usará cifrado.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **Settings**.
2. En la sección Allowed Clients, haga clic en **Create (+).**

   Aparecerá el cuadro de diálogo Add Allowed Client.

3. Especifique el nombre de host del cliente.

   Puede ser un nombre de dominio calificado (por ej. host1.emc.com) o un nombre de host con un carácter comodín (por ej. *.emc.com).

4. Seleccione una opción de Encryption Strength.

   Las opciones son None (sin cifrado), Medium (AES128-SHA1) o High (AES256-SHA1).

5. Seleccione el modo de autenticación.

   Las opciones son One Way, Two Way, Two Way Password o Anonymous.

6. Haga clic en **OK**.

Modificación de un cliente de DD Boost

Puede cambiar el nombre, la potencia de cifrado y el modo de autenticación de un cliente de DD Boost permitido.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **Settings**.
2. En la lista Allowed Clients, seleccione el cliente que desee modificar.
3. Haga clic en el botón **Edit**, que muestra un ícono de lápiz.

   Aparecerá el cuadro de diálogo Modify Allowed Client.

4. Para cambiar el nombre de un cliente, edite el texto de Client.
5. Para cambiar la opción de Encryption Strength, selecciónela.

   Las opciones son None (sin cifrado), Medium (AES128-SHA1) o High (AES256-SHA1).

6. Para cambiar el modo de autenticación, seleccione la opción.

   Las opciones son One Way, Two Way o Anonymous.

7. Haga clic en **OK**.

Eliminación de un cliente de DD Boost

Puede eliminar un cliente de DD Boost permitido.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **Settings**.
2. Seleccione el cliente en la lista.
3. Hagaclic en Delete (**X**).

   Aparecerá el cuadro de diálogo Delete Allowed Clients.

4. Confirme y seleccione el nombre del cliente. Haga clic en **OK**.

Acerca de los grupos de interfaces

Esta función le permite combinar varios vínculos Ethernet en un grupo y registrar solo una interfaz en el sistema Data Domain con la aplicación de respaldo. DD Boost Library negocia con el sistema Data Domain para obtener la mejor interfaz para enviar datos. El balanceo de carga proporciona un rendimiento físico más alto para el sistema Data Domain.

Al configurar un grupo de interfaces, se crea una red privada dentro del sistema Data Domain, que consta de las direcciones IP designadas como grupo. Los clientes se asignan a un solo grupo y la interfaz del grupo usa balanceo de carga para mejorar el rendimiento de transferencia de datos y aumentar la confiabilidad.

Por ejemplo, en el ambiente Symantec NetBackup, los clientes del servidor de medios usan una sola dirección IP de red pública para acceder al sistema Data Domain. Toda la comunicación con el sistema Data Domain se inicia a través de esta conexión IP administrada, que se configura en el servidor NetBackup.

Si se configura un grupo de interfaces, cuando el sistema Data Domain recibe datos de los clientes del servidor de medios, se realiza un balanceo de carga de la transferencia de datos y esta se distribuye en todas las interfaces del grupo, lo que proporciona un rendimiento de entrada/salida más alto, especialmente para los clientes que usan varias conexiones de 1 GigE.

El balanceo de carga de la transferencia de datos se realiza en función de la cantidad de conexiones pendientes en las interfaces. Solo tienen balanceo de carga las conexiones para trabajos de respaldo y restauración. Compruebe el área de conexiones activas para obtener más información sobre el número de conexiones pendientes en las interfaces de un grupo.

Si una interfaz del grupo falla, todos los trabajos en transferencia a esa interfaz se reanudan automáticamente en los vínculos operativos en buen estado (sin conocimiento de las aplicaciones de respaldo). Todos los trabajos que se inician después de la falla también se envían a una interfaz en buen estado del grupo. Si el grupo está deshabilitado o falla un intento de recuperar en una interfaz alternativa, se usa la dirección IP administrada para la recuperación. Ante una falla en un grupo, no se usarán interfaces de otro grupo.

Tenga en cuenta la siguiente información al administrar grupos de interfaces.

- La dirección IP debe estar configurada en el sistema Data Domain y su interfaz debe estar habilitada. Para comprobar la configuración de la interfaz, seleccione la página **Hardware** > **Ethernet** > **Interfaces** y verifique los puertos libres. Consulte el capítulo `net` de la *Guía de referencia de comandos de Data Domain Operating System* o la *Guía de configuración inicial de Data Domain Operating System* para obtener información sobre cómo configurar una dirección IP para una interfaz.
- Puede usar los comandos `ifgroup` para administrar grupos de interfaces; esos comandos se describen en detalle en la *Guía de referencia de comandos de Data Domain Operating System*.
- Los grupos de interfaces proporcionan compatibilidad completa con direcciones IPv6 estáticas, con las mismas funcionalidades para IPv6 que para IPv4. Se permiten conexiones de cliente IPv4 e IPv6 simultáneas. Un cliente conectado con IPv6 solo ve las interfaces de IFGROUP de IPv6. Un cliente conectado con IPv4 solo ve las interfaces de IFGROUP de IPv4. Los IFGROUP individuales incluyen todas las direcciones IPv4 o todas las direcciones IPv6. Para obtener información detallada, consulte la *Guía de administración de Data Domain Boost para integración de partners* o la *Guía de administración de Data Domain Boost para OpenStorage*.

- Las interfaces configuradas se incluyen en Active Connections, en la parte inferior de la página Activities.

Nota

Consulte Uso de DD Boost en sistemas de alta disponibilidad en la página 382 para obtener información importante acerca del uso de grupos de interfaz con los sistemas de alta disponibilidad.

En los temas siguientes se describe cómo administrar grupos de interfaces.

Interfaces

IFGROUP admite interfaces físicas y virtuales.

Una interfaz de IFGROUP es miembro de un solo IFGROUP *<group-name>* y puede constar de lo siguiente:

- Interfaz física, como `eth0a`
- Interfaz virtual, creada para la conmutación por error de vínculos o la agregación de vínculos, como `veth1`
- Interfaz de alias virtual, como `eth0a:2` o `veth1:2`
- Interfaz VLAN virtual, como `eth0a.1` o `veth1.1`
- Dentro de un IFGROUP *<group-name>*, todas las interfaces deben estar en interfaces únicas (Ethernet, Ethernet virtual) para garantizar la conmutación por error en caso de error de red.

IFGROUP proporciona compatibilidad total con direcciones estáticas IPv6, con las mismas funcionalidades para IPv6 que para IPv4. Se permiten conexiones de cliente IPv4 e IPv6 simultáneas. Un cliente conectado con IPv6 solo ve las interfaces de IFGROUP de IPv6. Un cliente conectado con IPv4 solo ve las interfaces de IFGROUP de IPv4. Los IFGROUP individuales incluyen todas las direcciones IPv4 o todas las direcciones IPv6.

Para obtener más información, consulte la *Guía de administración de Data Domain Boost para integración de partners* o la *Guía de administración de Data Domain Boost para OpenStorage*.

Aplicación de interfaz

IFGROUP le permite aplicar conectividad de red privada, lo que garantiza que un trabajo fallido no se vuelva a conectar en la red pública después de errores de red.

Cuando se activa la aplicación de interfaz, un trabajo fallido solo se puede recuperar en una dirección IP de red privada alternativa. La aplicación de interfaz solo está disponible para clientes que usan interfaces IFGROUP.

La aplicación de interfaz está desactivada (FALSE) de manera predeterminada. Para habilitar la aplicación de interfaz, debe agregar la siguiente configuración en el registro del sistema:

`system.ENFORCE_IFGROUP_RW=TRUE`

Una vez que realizó esta entrada en el registro, debe realizar un `filesys restart` para que la configuración tenga efecto.

Para obtener más información, consulte la *Guía de administración de Data Domain Boost para integración de partners* o la *Guía de administración de Data Domain Boost para OpenStorage*.

Clientes

IFGROUP admite distintos formatos de nombre para los clientes. La selección de clientes se basa en un orden de precedencia especificado.

Un cliente de IFGROUP integra un solo ifgroup *<group-name>* y puede constar de lo siguiente:

- Un nombre de dominio calificado (FQDN), como ddboost.datadomain.com
- Un host parcial, que permite la búsqueda de los primeros caracteres *n* del nombre de host. Por ejemplo, cuando n = 3, `rtp_.*emc.com` y `dur_.*emc.com` son formatos válidos. Se admiten cinco valores diferentes de *n* (1-5).
- Caracteres comodín, como `*.datadomain.com` o "*"
- Un nombre corto para el cliente, como ddboost
- Un rango de IP público del cliente, como 128.5.20.0/24

Antes del procedimiento de lectura o escritura, el cliente solicita una dirección IP de IFGROUP del servidor. Para seleccionar la asociación de IFGROUP de cliente, la información del cliente se evalúa de acuerdo con el siguiente orden de precedencia.

1. Dirección IP del sistema Data Domain conectado. Si ya hay una conexión activa entre el cliente y el sistema Data Domain, y la conexión existe en la interfaz del IFGROUP, las interfaces del IFGROUP se ponen a disposición del cliente.
2. Rango de IP del cliente conectado. Se realiza una comprobación de máscara IP respecto del IP de origen del cliente; si la dirección IP de origen del cliente coincide con la máscara de la lista de clientes de IFGROUP, las interfaces de IFGROUP se ponen a disposición del cliente.
   - Para IPv4, puede seleccionar cinco máscaras de diferente rango, según la red.
   - Para IPv6, las máscaras fijas /64, /112 y /128 están disponibles.

   Esta comprobación de rango de hosts es útil para VLAN separadas con muchos clientes, donde no hay un único nombre de host (dominio) parcial.
3. Nombre del cliente: `abc-11.d1.com`
4. Nombre de dominio del cliente: `*.d1.com`
5. Todos los clientes: `*`

Para obtener más información, consulte la *Guía de administración de Data Domain Boost para integración de partners*.

Creación de grupos de interfaces

Puede usar la pestaña IP Network para crear grupos de interfaces y agregar interfaces y clientes a los grupos.

Los grupos de interfaces múltiples mejoran la eficiencia de DD Boost, dado que le permiten realizar lo siguiente:

- Configurar DD Boost para usar interfaces específicas configuradas en grupos.
- Asignar clientes a uno de esos grupos de interfaces.
- Monitorear qué interfaces están activas con clientes de DD Boost.

Crear grupos de interfaces primero y después agregar clientes (a medida que los servidores de medios nuevos estén disponibles) a un grupo de interfaces.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **IP Network**.
2. En la sección Interface Groups, haga clic en Add (**+**).
3. Escriba el nombre del grupo de interfaces.
4. Seleccione una o más interfaces. Se puede configurar un máximo de 32 interfaces.

   Nota

   En función de la configuración de creación de alias, es posible que algunas interfaces no se puedan seleccionar si comparten una interfaz física con otra interfaz del mismo grupo. Esto se debe a que cada interfaz dentro del grupo debe estar en una interfaz física diferente para garantizar la recuperación de failover.

5. Haga clic en **OK**.
6. En la sección Configured Clients, haga clic en Add (**+**).
7. Escriba un nombre de cliente completo o `*.midominio.com`.

   Nota

   El cliente * inicialmente está disponible para el grupo predeterminado. El cliente * solamente puede pertenecer a un ifgroup.

8. Seleccione un grupo de interfaces previamente configurado y haga clic en **OK**.

Activación y desactivación de grupos de interfaces

Puede usar la pestaña IP Network para activar y desactivar grupos de interfaces.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **IP Network**.
2. En la sección de grupos de interfaces, seleccione el grupo de interfaces en la lista.

   Nota

   Si el grupo de interfaces no tiene clientes ni interfaces asignados, no puede activar el grupo.

3. Haga clic en **Edit** (lápiz).
4. Haga clic en **Enabled** para habilitar al grupo de interfaces; deseleccione la casilla de verificación para deshabilitarlo.
5. Haga clic en **OK**.

Modificación del nombre y de las interfaces de un grupo de interfaces

Puede usar la pestaña IP Network para cambiar el nombre y las interfaces asociadas con un grupo de interfaces.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **IP Network**.
2. En la sección de grupos de interfaces, seleccione el grupo de interfaces en la lista.
3. Haga clic en **Edit** (lápiz).
4. Vuelva a escribir el nombre para modificarlo.

   El nombre del grupo debe tener entre 1 y 24 caracteres, que solo pueden ser letras, números, guiones bajos y guiones. No puede ser igual que otro nombre de grupo y no puede ser “default”, “yes”, “no” ni “all.”

5. Seleccione o deseleccione interfaces de cliente en la lista Interfaces.

   Nota

   Si quita todas las interfaces del grupo, se deshabilitará automáticamente.

6. Haga clic en **Aceptar**.

Eliminación de un grupo de interfaces

Puede usar la pestaña IP Network para eliminar un grupo de interfaces. Al eliminar un grupo de interfaces, se eliminan todas las interfaces y los clientes asociados con el grupo.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **IP Network**.
2. En la sección de grupos de interfaces, seleccione el grupo de interfaces en la lista. El grupo predeterminado no se puede eliminar.
3. Hagaclic en Delete (**X**).
4. Confirme la eliminación.

Cómo agregar un cliente a un grupo de interfaces

Puede usar la pestaña IP Network para agregar clientes a grupos de interfaces.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **IP Network**.
2. En la sección Configured Clients, haga clic en Add (**+**).
3. Introduzca un nombre para el cliente.

   Los nombres de cliente deben ser únicos y pueden constar de:

   - **FQDN**
   - ***.domain**
   - Rango de IP público de cliente:
     - Para IPv4, `xx.xx.xx.0/24` proporciona una máscara de 24 bits en la dirección IP de conexión. El /24 representa los bits que se enmascaran cuando se evalúa el acceso de la dirección IP de origen del cliente a IFGROUP.
     - Para IPv6, `xxxx::0/112` proporciona una máscara de 112 bits respecto de la IP de conexión. El /112 representa los bits que se enmascaran

cuando se evalúa el acceso de la dirección IP de origen del cliente a IFGROUP.

Los nombres de cliente tienen una longitud máxima de 128 caracteres.

4. Seleccione un grupo de interfaces previamente configurado y haga clic en **OK**.

Modificación del nombre o del grupo de interfaces de un cliente

Puede usar la pestaña IP Network para cambiar el nombre o el grupo de interfaces de un cliente.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **IP Network**.
2. En la sección Configured Clients, seleccione al cliente.
3. Haga clic en **Edit** (lápiz).
4. Escriba un nombre de cliente nuevo.

   Los nombres de cliente deben ser únicos y pueden constar de:

   - `FQDN`
   - `*.domain`
   - Rango de IP público de cliente:
     - Para IPv4, `xx.xx.xx.0/24` proporciona una máscara de 24 bits en la dirección IP de conexión. El /24 representa los bits que se enmascaran cuando se evalúa el acceso de la dirección IP de origen del cliente a IFGROUP.
     - Para IPv6, `xxxx::0/112` proporciona una máscara de 112 bits respecto de la IP de conexión. El /112 representa los bits que se enmascaran cuando se evalúa el acceso de la dirección IP de origen del cliente a IFGROUP.

   Los nombres de cliente tienen una longitud máxima de 128 caracteres.
5. Seleccione un grupo de interfaces nuevo del menú.

   Nota

   El grupo de interfaces anterior está deshabilitado si no tiene clientes.
6. Haga clic en **Aceptar**.

Eliminación de un cliente del grupo de interfaces

Puede usar la pestaña IP Network para eliminar un cliente de un grupo de interfaces.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **IP Network**.
2. En la sección Configured Clients, seleccione al cliente.
3. Hagaclic en Delete (**X**).

   Nota

   Si el grupo de interfaces al que pertenece el cliente no tiene otros clientes, se deshabilita el grupo de interfaces.

4. Confirme la eliminación.

Uso de grupos de interfaces para la replicación de archivos administrados (MFR)

Los grupos de interfaz pueden usarse para controlar las interfaces que se usan para DD Boost MFR, dirigir la conexión de replicación mediante una red específica y usar varias interfaces de red con alto ancho de banda y confiabilidad para las condiciones de de conmutación por error. Todos los tipos de IP de Data Domain son compatibles: IPv4 o IPv6, IP de alias de IP/VLAN y LACP/agregación de conmutación por error.

Nota

Los grupos de interfaz que se utilizan para replicación son diferentes de los grupos de interfaz explicados anteriormente y solo se admiten en la replicación de archivos administrada (MFR) de DD Boost. Para obtener información detallada sobre el uso de grupos de interfaces para MFR, consulte la *Guía de administración de Data Domain Boost para integración de partners* o la *Guía de administración de Data Domain Boost para OpenStorage*.

Sin el uso de grupos de interfaces, la configuración para la replicación requiere varios pasos:

1. Agregar una entrada en el archivo `/etc/hosts` en el sistema Data Domain de origen para el sistema Data Domain de destino y codificar de forma rígida una de las interfaces de red LAN privadas como la dirección IP de destino.
2. Agregar una ruta en el sistema Data Domain de origen al sistema Data Domain de destino especificando un puerto físico o virtual en el sistema Data Domain de origen a la dirección IP del destino remoto.
3. Configurar LACP mediante la red en todos los switches entre los sistemas Data Domain para balanceo de carga y conmutación por error.
4. Requerir que las aplicaciones diferentes utilicen nombres diferentes para el sistema Data Domain de destino, a fin de evitar conflictos de asignación de nombres en el archivo `/etc/hosts`.

El uso de grupos de interfaces para la replicación simplifica esta configuración mediante los comandos de DD OS System Manager o la CLI de DD OS. El uso de grupos de interfaces para configurar la ruta de replicación le permite:

- Redirigir una dirección IP resuelta por el nombre de host lejos de la red pública, utilizando otra dirección IP privada del sistema de Data Domain.
- Identificar un grupo de interfaces en función de criterios de selección configurados, lo que proporciona un grupo de interfaces único en el que todas las interfaces están accesibles desde el sistema Data Domain de destino.
- Seleccionar una interfaz de red privada en una lista de interfaces que pertenezcan a un grupo, lo que garantiza que la interfaz esté en estado óptimo.
- Proporcionar balanceo de carga en múltiples interfaces de Data Domain dentro de la misma red privada.
- Proporcionar una interfaz de conmutación por error para recuperación para las interfaces del grupo de interfaces.
- Proporcionar conmutación por error de host si está configurado en el sistema Data Domain de origen.
- Usar traducción de direcciones de red (NAT)

El orden de selección para determinar a una coincidencia de grupo de interfaces para replicación de archivos es:

1. La ruta local de MTree (unidad de almacenamiento) y un nombre de host de Data Domain remoto específico
2. La ruta local de MTree (unidad de almacenamiento) con cualquier nombre de host remoto de Data Domain
3. Cualquier ruta de MTree (unidad de almacenamiento) con un nombre de host de Data Domain específico

El mismo MTree puede aparecer en varios grupos de interfaces solamente si tiene un nombre de host de Data Domain diferente. El mismo nombre de host de Data Domain puede aparecer en varios grupos de interfaces solamente si tiene una ruta de MTree diferente. Se espera que el nombre de host remoto sea un nombre de dominio calificado, por ejemplo, dd890-1.emc.com.

La selección de grupos de interfaces se realiza localmente en el sistema Data Domain de origen y en el sistema de Data Domain de destino, independientes entre sí. Para una red de replicación de WAN, solamente debe configurarse el grupo de interfaces remota, ya que la dirección IP de origen corresponde al gateway para la dirección IP remota.

Cómo agregar una ruta de replicación a un grupo de interfaces

Utilice la pestaña IP Network para agregar rutas a grupos de interfaces.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **IP Network**.
2. En la sección Configured Replication Paths, haga clic en Add (**+**).
3. Introduzca valores para **MTree** o **Remote Host**.
4. Seleccione un grupo de interfaces previamente configurado y haga clic en **OK**.

Modificación de una ruta de replicación para un grupo de interfaces

Puede usar la pestaña IP Network para modificar rutas de replicación de grupos de interfaces.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **IP Network**.
2. En la sección Configured Replication Paths, seleccione la ruta de replicación.
3. Haga clic en **Edit** (lápiz).
4. Modifique cualquiera de los valores de **MTree**, **Remote Host** o **Interface Group**.
5. Haga clic en **OK**.

Eliminación de una ruta de replicación para un grupo de interfaces

Puede usar la pestaña IP Network para eliminar rutas de replicación de grupos de interfaces.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **IP Network**.
2. En la sección Configured Replication Paths, seleccione la ruta de replicación.
3. Hagaclic en Delete (**X**).

4. En el cuadro de diálogo Delete Replication Path(s), haga clic en **OK**.

Destrucción de DD Boost

Puede usar esta opción para eliminar permanentemente todos los datos (imágenes) incluidos en las unidades de almacenamiento. Cuando desactiva o destruye DD Boost, el servicio FC de DD Boost también se desactiva. Únicamente un usuario administrativo puede destruir DD Boost.

Procedimiento

1. Quite manualmente (haga que venzan) las entradas correspondientes del catálogo de la aplicación de respaldo.

   Nota

   Si hay varias aplicaciones de respaldo que usan el mismo sistema Data Domain, quite todas las entradas de cada uno de los catálogos de las aplicaciones.

2. Seleccione **Protocols** > **DD Boost** > **More Tasks** > **Destroy DD Boost...**.
3. Ingrese las credenciales administrativas cuando se le pida.
4. Haga clic en **OK**.

Configuración de DD Boost-over-Fibre Channel

En versiones anteriores de DD OS, todas las comunicaciones entre la biblioteca de DD Boost y el sistema Data Domain se realizaba mediante redes de IP. Ahora, DD OS ofrece Fibre Channel como un mecanismo de transporte alternativo para la comunicación entre DD Boost Library y el sistema Data Domain.

Nota

Se admiten ambientes de clientes Windows, Linux, HP-UX (arquitectura Itanium de 64 bits), AIX y Solaris.

Habilitación de usuarios de DD Boost

Antes de poder configurar el servicio DD Boost-over-FC en un sistema Data Domain, debe agregar uno o más usuarios de DD Boost y habilitar DD Boost.

Antes de comenzar

- Inicie sesión en DD System Manager. Para obtener instrucciones, consulte “Inicio y cierre de sesión de DD System Manager.”
  Equivalente de la CLI

  ```
  login as: sysadmin
  Data Domain OS 5.7.x.x-12345
  Using keyboard-interactive authentication.
  Password:
  ```

- Si utiliza la CLI, asegúrese de que el demonio de destino SCSI esté habilitado:

  ```
  # scsitarget enable
  Please wait ...
  SCSI Target subsystem is enabled.
  ```

Nota

Si utiliza DD System Manager, el demonio de destino SCSI se habilita automáticamente cuando habilita el servicio DD Boost mediante FC (más adelante en este procedimiento).

- Verifique que la licencia de DD Boost esté instalada. En DD System Manager, seleccione **Protocols** > **DD Boost** > **Settings**. Si en Status se indica que DD Boost no tiene licencia, haga clic en **Add License** e ingrese una licencia válida en el cuadro de diálogo Add License Key.
  Equivalentes de la CLI

```
# license show
```

```
# license add código de licencia
```

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **Settings**.
2. En la sección Users with DD Boost Access, especifique uno o más nombres de usuario de DD Boost.

   Un usuario de DD Boost también es usuario de DD OS. Cuando especifica un nombre de usuario de DD Boost, puede seleccionar un nombre de usuario de DD OS existente, o puede crear uno nuevo y hacer que sea un usuario de DD Boost. En esta versión se admiten varios usuarios de DD Boost. Para obtener instrucciones detalladas, consulte “Especificación de nombres de usuario de DD Boost”.

   Equivalentes de la CLI

```
# user add username [password password]
```

```
# ddboost set user-name exampleuser
```

3. Haga clic en **Enable** para habilitar DD Boost.

   Equivalente de la CLI

```
# ddboost enable
Starting DDBOOST, please wait..............
DDBOOST is enabled.
```

Resultados

Ahora está listo para configurar el servicio DD Boost-over-FC en el sistema Data Domain.

Configuración de DD Boost

Una vez que haya agregado usuarios y habilitado DD Boost, debe habilitar la opción Fibre Channel y especificar el nombre del servidor de DD Boost Fibre Channel. En función de su aplicación, es posible que también deba crear una o más unidades de almacenamiento e instalar el plug-in/API de DD Boost en los servidores de medios que tendrán acceso al sistema Data Domain.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **Fibre Channel**.
2. Haga clic en el botón **Enable** para habilitar el transporte de Fibre Channel.

Equivalente de la CLI

```
# ddboost option set fc enabled
Please wait...
DD Boost option "FC" set to enabled.
```

3. Para cambiar el nombre del servidor de DD Boost Fibre Channel predeterminado (nombre de host), haga clic en **Edit**, escriba un nombre de servidor nuevo y haga clic en **OK**.

   Equivalente de la CLI

   ```
   # ddboost fc dfc-server-name set DFC-ddbeta2
   DDBoost dfc-server-name is set to "DFC-ddbeta2" for DDBoost FC.
   Configure clients to use "DFC-DFC-ddbeta2" for DDBoost FC.
   ```

4. Seleccione **Protocols** > **DD Boost** > **Storage Units** para crear una unidad de almacenamiento (si la aplicación todavía no la creó).

   Debe crear al menos una unidad de almacenamiento en el sistema Data Domain, y se debe asignar un usuario de DD Boost a esa unidad. Para obtener instrucciones detalladas, consulte “Creación de una unidad de almacenamiento”.

   Equivalente de la CLI

   ```
   # ddboost storage-unit create storage_unit_name-su
   ```

5. Instale el complemento/API de DD Boost (si es necesario, en función de la aplicación).

   El software de complemento de DD Boost OpenStorage se debe instalar en los servidores de medios de NetBackup que necesiten acceso al sistema Data Domain. Este complemento incluye DD Boost Library, que se integra con el sistema Data Domain. Para obtener instrucciones detalladas de instalación y configuración, consulte la *Guía de administración para integración de partners de Data Domain Boost* o la *Guía de administración de Data Domain Boost para OpenStorage*.

Resultados

Ahora está listo para verificar la conectividad y crear grupos de acceso.

Verificación de conectividad y creación de grupos de acceso

Vaya a **Hardware** > **Fibre Channel** > **Resources** para administrar iniciadores y terminales para los puntos de acceso. Vaya a **Protocols** > **DD Boost** > **Fibre Channel** para crear y administrar grupos de acceso de DD Boost mediante FC.

Nota

Evite realizar cambios en el grupo de acceso en un sistema Data Domain durante trabajos de respaldo o restauración activos. Un cambio puede hacer que un trabajo activo falle. El impacto de los cambios durante trabajos activos depende de una combinación de configuraciones de software de respaldo y host.

Procedimiento

1. Seleccione **Hardware** > **Fibre Channel** > **Resources** > **Initiators** para verificar que haya iniciadores presentes.

Se recomienda que asigne alias a los iniciadores para reducir la confusión durante el proceso de configuración.

Equivalente de la CLI

```
# scsitarget initiator show list
Initiator      System Address                Group   Service
------------   -----------------------   ----------   -------
initiator-1    21:00:00:24:ff:31:b7:16         n/a       n/a
initiator-2    21:00:00:24:ff:31:b8:32         n/a       n/a
initiator-3    25:00:00:21:88:00:73:ee         n/a       n/a
initiator-4    50:06:01:6d:3c:e0:68:14         n/a       n/a
initiator-5    50:06:01:6a:46:e0:55:9a         n/a       n/a
initiator-6    21:00:00:24:ff:31:b7:17         n/a       n/a
initiator-7    21:00:00:24:ff:31:b8:33         n/a       n/a
initiator-8    25:10:00:21:88:00:73:ee         n/a       n/a
initiator-9    50:06:01:6c:3c:e0:68:14         n/a       n/a
initiator-10   50:06:01:6b:46:e0:55:9a         n/a       n/a
tsm6_p23       21:00:00:24:ff:31:ce:f8   SetUp_Test       VTL
------------   -----------------------   ----------   -------
```

2. Para asignar un alias a un iniciador, seleccione uno de los iniciadores y haga clic en el ícono de lápiz (Edit). En el campo Name del cuadro de diálogo Modify Initiator, ingrese el alias y haga clic en **OK**.

   Equivalentes de la CLI

   ```
   # scsitarget initiator rename initiator-1 initiator-renamed
   Initiator 'initiator-1' successfully renamed.
   ```

   ```
   # scsitarget initiator show list
   Initiator           System Address                 Group
   Service
   -----------------   -----------------------   ----------
   -------
   initiator-2         21:00:00:24:ff:31:b8:32          n/a
   n/a
   initiator-renamed   21:00:00:24:ff:31:b7:16          n/a
   n/a
   -----------------   -----------------------   ----------
   -------
   ```

3. En la pestaña Resources, verifique que los terminales estén presentes y habilitados.

   Equivalente de la CLI

   ```
   # scsitarget endpoint show list
   -------------   --------------   ------------   -------   ------
   endpoint-fc-0   5a               FibreChannel   Yes       Online
   endpoint-fc-1   5b               FibreChannel   Yes       Online
   -------------   --------------   ------------   -------   ------
   ```

4. Vaya a **Protocols** > **DD Boost** > **Fibre Channel**.
5. En el área DD Boost Access Groups, haga clic en el ícono **+** para agregar un grupo de acceso.
6. Escriba un nombre único para el grupo de acceso. No se admiten nombres duplicados.

   Equivalente de la CLI

   ```
   # ddboost fc group create test-dfc-group
   DDBoost FC Group "test-dfc-group" successfully created.
   ```

7. Seleccione uno o más iniciadores. De manera opcional, reemplace el nombre del iniciador introduciendo uno nuevo. Haga clic en **Next**.

   Equivalente de la CLI

```
#ddboost fc group add test-dfc-group initiator initiator-5
Initiator(s) "initiator-5" added to group "test-dfc-group".
```

Un iniciador es un puerto en una HBA conectado a un cliente de respaldo que se conecta con el sistema para leer y escribir datos a través del protocolo Fibre Channel. El WWPN es el World-Wide Port Name del puerto de Fibre Channel en el servidor de medios.

8. Especifique el número de dispositivos de DD Boost que usará el grupo. Este número determina qué dispositivos puede detectar el iniciador y, por lo tanto, el número de rutas de I/O al sistema Data Domain. El número predeterminado es 1; el mínimo es 1 y el máximo es 64.

   Equivalente de la CLI

   ```
   # ddboost fc group modify Test device-set count 5
   Added 3 devices.
   ```

   Para conocer el valor recomendado para diferentes clientes, consulte la guía *Data Domain Boost for OpenStorage Administration Guide*.

9. Indique qué terminales se deben incluir en el grupo: todos, ninguno o seleccione elementos específicos de la lista de terminales. Haga clic en **Next**.

   Equivalentes de la CLI

   ```
   # scsitarget group add Test device ddboost-dev8 primary-
   endpoint allsecondary-endpoint all
   Device 'ddboost-dev8' successfully added to group.
   ```

   ```
   # scsitarget group add Test device ddboost-dev8 primary-
   endpointendpoint-fc-1 secondary-endpoint fc-port-0
   Device 'ddboost-dev8' is already in group 'Test'.
   ```

   Al presentar los LUN a través de puertos de FC en HBA, los puertos se pueden designar como primarios, secundarios o ninguno. Un puerto primario para un conjunto de LUN es el puerto que actualmente anuncia esos LUN para un fabric. Un puerto secundario es un puerto que difundirá un conjunto de LUN en caso de falla de la ruta principal (esto requiere la intervención manual). La configuración none se utiliza en caso de que no desee publicar los LUN seleccionados. La presentación de LUN depende de la topología de SAN.

10. Revise el resumen y realice las modificaciones que desee. Haga clic en **Finish** para crear el grupo de acceso, que se muestra en la lista DD Boost Access Groups.

    Equivalente de la CLI

    ```
    # scsitarget group show detailed
    ```

Nota

Para cambiar la configuración de un grupo de acceso existente, selecciónelo de la lista y haga clic en el ícono de lápiz (Modify).

Eliminación de grupos de acceso

Puede usar la pestaña Fibre Channel para eliminar grupos de acceso.

Procedimiento

1. Seleccione **Protocols** > **DD Boost** > **Fibre Channel**.

2. Seleccione el grupo que desee eliminar de la lista DD Boost Access Groups.

   Nota

   No puede eliminar un grupo que tenga iniciadores asignados. Edite el grupo para quitar los iniciadores primero.

3. Hagaclic en Delete (**X**).

Uso de DD Boost en sistemas de alta disponibilidad

La alta disponibilidad proporciona conmutación por error transparente de cualquier aplicación que utilice DD Boost, es decir, cualquier operación de respaldo o restauración continúa sin necesidad de que haya una intervención manual. Todos los demás escenarios de usuario de DD Boost también son compatibles con sistemas de alta disponibilidad, incluidos la replicación administrada de archivos (MFR), el procesamiento distribuido de segmentos (DSP), la copia de archivos y los grupos de interfaces dinámicas (DIG).

Tenga en cuenta estas consideraciones especiales para el uso de DD Boost en sistemas de alta disponibilidad:

- En los sistemas de Data Domain habilitados para alta disponibilidad, los failovers del servidor DD se producen en menos de 10 minutos. Sin embargo, la recuperación de las aplicaciones de DD Boost puede tardar más, ya que la recuperación de aplicaciones de Boost no puede comenzar hasta que no finalice la conmutación por error del servidor DD. Además, la recuperación de aplicaciones de Boost no puede comenzar hasta que la aplicación invoca la biblioteca de Boost.
- DD Boost en sistemas de alta disponibilidad requiere que las aplicaciones de Boost estén utilizando bibliotecas Boost de alta disponibilidad; las aplicaciones que usan bibliotecas Boost sin alta disponibilidad no ven la conmutación por error transparente.
- MFR producirá una conmutación por error transparente cuando los sistemas de origen y destino estén habilitados con alta disponibilidad. MFR también es compatible con configuraciones de alta disponibilidad parciales (es decir, cuando el sistema de origen o destino está habilitado, pero no los dos) cuando la falla se produce en el sistema compatible con alta disponibilidad. Para obtener más información, consulte la *Guía de administración de DD Boost para OpenStorage* o la *Guía de administración de DD Boost para integración de partners*.
- Los grupos de interfaces dinámicas no deben incluir direcciones IP asociadas con la interconexión directa entre los sistemas Data Domain activos y en espera.
- Los clientes de DD Boost deben estar configurados para usar direcciones IP flotantes.

Acerca de las pestañas de DD Boost

Obtenga información sobre el uso de las pestañas de DD Boost en DD System Manager.

Configuración

Puede usar la pestaña Settings para habilitar o deshabilitar DD Boost, seleccionar clientes y usuarios, y especificar opciones avanzadas.

La pestaña Settings muestra el estado de DD Boost (Enabled o Disabled). Use el botón **Status** para alternar entre **Enabled** o **Disabled**.

En **Allowed Clients**, seleccione los clientes que deben tener acceso al sistema. Use los botones **Add**, **Modify** y **Delete** para administrar la lista de clientes.

En **Users with DD Boost Access**, seleccione los usuarios que deben tener acceso a DD Boost. Use los botones **Add**, **Change Password** y **Remove** para administrar la lista de usuarios.

Expanda **Advanced Options** para ver qué opciones avanzadas están habilitadas. Vaya a **More Tasks** > **Set Options** para restablecer estas opciones.

Conexiones activas

Puede usar la pestaña Active Connections para ver información acerca de clientes, interfaces y archivos salientes.

Tabla 131 Información de clientes conectados

Elemento	Descripción
Client	El nombre del cliente conectado.
Idle	Si el cliente está inactivo (Yes) o no (No).
Plug-In Version	La versión de complemento de DD Boost instalada, como 2.2.1.1.
OS Version	La versión de sistema operativo instalada, como Linux 2.6.1 7-1.2142_FC4smp x86_64.
Application Version	La versión de la aplicación de respaldo instalada, como NetBackup 6.5.6.
Encrypted	Si la conexión está cifrada (Yes) o no (No).
DSP	Si la conexión está usando o no procesamiento distribuido de segmentos (DSP).
Transport	El tipo de transporte utilizado, como IPv4, IPv6 o DFC (Fibre Channel).

Tabla 132 Información de conexión de la interfaz configurada

Elemento	Descripción
Interface	La dirección IP de la interfaz.
Interface Group	Una de las siguientes: • El nombre del grupo de interfaces. • Nada, si no es miembro de uno.
Backup	El número de conexiones de respaldo activas.
Restore	El número de conexiones de restauración activas.
Replication	El número de conexiones de replicación activas.
Synthetic	La cantidad de respaldos sintéticos.
Total	La cantidad total de conexiones de la interfaz.

Tabla 133 Información de replicación de archivos salientes

Elemento de archivos salientes	Descripción
File Name	El nombre del archivo de imagen saliente.
Target Host	El nombre del host que recibe el archivo.
Logical Bytes to Transfer	El número de bytes lógicos para transferir.
Logical Bytes Transferred	El número de bytes lógicos que ya se transfirieron.
Low Bandwidth Optimization	El número de bytes de bajo ancho de banda que ya se transfirieron.

Red IP

En la pestaña IP Network se muestran grupos de interfaces configurados. Entre los detalles se incluye si un grupo está habilitado o no, y las interfaces de clientes configuradas. Los administradores pueden usar el menú Interface Group para ver qué clientes están asociados con un grupo de interfaces.

Fibre Channel

La pestaña Fibre Channel enumera los grupos de acceso configurados de DD Boost. Use la pestaña Fibre Channel para crear y eliminar grupos de acceso y también para configurar los iniciadores, los dispositivos y los puntos finales para los grupos de acceso de DD Boost.

Unidades de almacenamiento:

Puede usar la pestaña **Storage Units** para ver, crear, modificar y eliminar unidades de almacenamiento.

Tabla 134 Pestaña Storage Units

Elemento	Descripción
Unidades de almacenamiento:	
View DD Boost Replications	Vea los contextos de replicación de DD Boost.
Storage Unit	El nombre de la unidad de almacenamiento.
User	Nombre de usuario asociado a la unidad de almacenamiento.
Quota Hard Limit	El conjunto de cuotas máximas para la unidad de almacenamiento.
Last 24hr Pre-Comp	La cantidad de datos escritos en la unidad de almacenamiento en las últimas 24 horas, antes de la compresión.
Last 24hr Post-Comp	La cantidad de datos escritos en la unidad de almacenamiento en las últimas 24 horas, después de la compresión.
Last 24hr Comp Ratio	Tasa de compresión de los datos escritos en la unidad de almacenamiento en las últimas 24 horas.

Tabla 134 Pestaña Storage Units (continuación)

Elemento	Descripción
Weekly Avg Post-Comp	Cantidad media de datos escritos en la unidad de almacenamiento cada semana, después de la compresión.
Last Week Post-Comp	Cantidad de datos escritos en la unidad de almacenamiento en la última semana, después de la compresión.
Weekly Avg Comp Ratio	Tasa media de compresión de los datos escritos en la unidad de almacenamiento cada semana.
Last Week Comp Ratio	Tasa de compresión de los datos escritos en la unidad de almacenamiento en la última semana.

Seleccione una unidad de almacenamiento para ver información detallada sobre ella. La información detallada está disponible en tres pestañas:

- Pestaña Storage Unit

  Tabla 135 Detalles de la unidad de almacenamiento: Pestaña Storage Unit

Elemento	Descripción
Total Files	El número total de imágenes de archivos en la unidad de almacenamiento.
Full Path	La ruta de acceso completa de la unidad de almacenamiento.
Status	El estado actual de la unidad de almacenamiento (se admiten combinaciones). El estado puede ser: ■ D: eliminado ■ RO: solo lectura ■ RW: lectura y escritura ■ RD: destino de replicación ■ RLE: DD Retention Lock habilitado ■ RLD: DD Retention Lock deshabilitado
Pre-Comp Used	La cantidad de almacenamiento previamente comprimido que ya está en uso.
Used (Post-Comp)	El tamaño total después de la compresión de los archivos en la unidad de almacenamiento.
Compression	La proporción de compresión lograda en los archivos.
Schedules	La cantidad de programaciones de medición de la capacidad física asignadas a la unidad de almacenamiento.
Submitted Measurements	La cantidad de veces que se ha medido la capacidad física de la unidad de almacenamiento.
Quota Enforcement	Haga clic en Quota para ir a la página Data Management Quota, que muestra los valores/porcentaje de cuota mínimos y máximos utilizados por MTrees.
Pre-Comp Soft Limit	El valor actual del conjunto de cuotas de advertencia para la unidad de almacenamiento.

Tabla 135 Detalles de la unidad de almacenamiento: Pestaña Storage Unit (continuación)

Elemento	Descripción
Pre-Comp Hard Limit	El valor actual del conjunto de cuotas máximas para la unidad de almacenamiento.
Quota Summary	Porcentaje de límite duro utilizado.
Instantáneas totales	Cantidad total de instantáneas de la unidad de almacenamiento.
Expired	Cantidad total de instantáneas vencidas de la unidad de almacenamiento.
Unexpired	Cantidad total de instantáneas válidas de la unidad de almacenamiento.
Oldest Snapshot	La instantánea más antigua de la unidad de almacenamiento.
Newest Snapshot	La instantánea más reciente de la unidad de almacenamiento.
Next Scheduled	La fecha de la próxima instantánea programada de la unidad de almacenamiento.
Assigned Snapshot Schedules	Las programaciones de instantáneas asignadas a la unidad de almacenamiento.

- Pestaña Space Usage: Muestra un gráfico que indica los bytes en uso antes de la compresión, los bytes en uso después de la compresión y el factor de compresión.
- Pestaña Daily Written: Muestra un gráfico que indica los bytes escritos antes de la compresión, los bytes escritos después de la compresión y el factor total de compresión.

CAPÍTULO 15

Librería de cintas virtuales DD

Este capítulo incluye:

- Descripción general de librerías de cintas virtuales de DD 388
- Planificación de una DD VTL 389
- Administración de una DD VTL 396
- Trabajo con librerías 400
- Uso de una librería seleccionada 404
- Visualización de información del convertidor 412
- Trabajo con unidades 413
- Trabajo con una unidad seleccionada 415
- Trabajo con cintas 415
- Trabajo con el vault 417
- Trabajar con vault en la nube 418
- Trabajo con grupos de acceso 425
- Trabajo con un grupo de acceso seleccionado 429
- Trabajo con recursos 432
- Trabajo con pools 436
- Trabajo con un pool seleccionado 439

Descripción general de librerías de cintas virtuales de DD

Una biblioteca de cintas virtuales de Data Domain (DD VTL) es un sistema de respaldo basado en disco que emula el uso de cintas físicas. Permite que las aplicaciones de respaldo se conecten y administren el almacenamiento de sistemas DD a través de funciones prácticamente idénticas a una librería de cintas física.

El software de respaldo tiene acceso a las unidades de cinta virtuales de la misma manera que a las unidades de cinta físicas. Una vez que se crean estas unidades en DD VTL, aparecen para el software de respaldo como unidades de cinta SCSI. DD VTL en sí aparece para el software de respaldo como un dispositivo robótico SCSI al que se tiene acceso por medio de interfaces de driver estándar. Sin embargo, el software de respaldo (no el sistema DD configurado como DD VTL) administra el movimiento del cambiador de medios y las imágenes de respaldo.

Los siguientes términos tienen un significado especial cuando se usan con DD VTL:

- *Librería*: Una librería emula una librería de cintas físicas con unidades, cambiadores, CAP (puertos de acceso a cartuchos) y slots (slots de cartucho).
- *Cinta*: Una cinta se representa como un archivo. Las cintas se pueden importar del vault a una librería. Además, se pueden exportar de una librería al vault. Las cintas se pueden mover dentro de una librería entre las unidades, slots y CAP.
- *Pool*: Un pool es un conjunto de cintas que se asigna a un directorio en el sistema de archivos. Los pools se usan para replicar cintas en un destino. De forma predeterminada, los pools se crean como pools de MTree, a menos que los especifique como pools de directorios al crearlos. Puede convertir pools basados en directorios en pools basados en MTrees para aprovechar las funciones adicionales de los MTrees.
- *Vault*: El vault contiene cintas que no están en uso en ninguna librería. Las cintas residen en una librería o en el vault.

DD VTL se ha probado con software de respaldo y configuraciones de hardware específicos, y es compatible con estos. Para obtener más información, consulte la *Guía de compatibilidad de respaldo* correspondiente en el sitio de soporte en línea.

DD VTL admite el uso simultáneo de interfaces de la librería de cintas y el sistema de archivos (NFS/CIFS/DD Boost).

Cuando se requiere DR (recuperación ante desastres), los pools y las cintas se pueden replicar a un sistema DD remoto a través de DD Replicator.

Para proteger los datos de las cintas contra modificación, las cintas se pueden bloquear con el software DD Retention Lock Governance.

Nota

En este momento, para 16 Gb/s, Data Domain admite topologías de punto a punto y de fabric. Otras topologías presentarán problemas.

El artículo de la base de conocimientos *Data Domain: VTL Best Practices Guide*, disponible en https://support.emc.com/kb/180591, proporciona información adicional sobre las mejores prácticas de DD VTL.

Planificación de una DD VTL

La función DD VTL (librería de cintas virtuales) tiene requisitos muy específicos, como licencias adecuadas, tarjetas de interfaz, permisos de usuario, etc. Los requisitos completos se incluyen aquí, junto con detalles y recomendaciones.

- Una licencia de DD VTL adecuada.
  - DD VTL es una función con licencia y debe usar el protocolo de administración de datos en red (NDMP) sobre IP (protocolo de Internet) o DD VTL directamente sobre FC (Fibre Channel).
  - Se requiere una licencia adicional para sistemas IBM i: la licencia I/OS.
  - Al agregar una licencia de DD VTL a través de DD System Manager, la función de DD VTL se deshabilita y se habilita automáticamente.
- Una tarjeta de interfaz FC o DD VTL configurada para usar NDMP.
  - Si la comunicación de DD VTL entre un servidor de respaldo y un sistema DD es a través de una interfaz FC, el sistema DD debe tener una tarjeta de interfaz FC instalada. Tenga en cuenta que, cuando se quita (o se cambia) una tarjeta de interfaz FC de un sistema DD, se deben actualizar todas las opciones de configuración de DD VTL asociadas con la tarjeta.
  - Si la comunicación de DD VTL entre un servidor de respaldo y un sistema DD es a través de NDMP, no se requiere una tarjeta de interfaz FC. No obstante, es necesario configurar el grupo de acceso TapeServer. Además, cuando se usa NDMP, no se aplican las funciones de iniciador y puerto.
  - El filtro de red debe configurarse para permitir que el cliente NDMP envíe información al sistema DD. Ejecute el comando **`net filter add operation allow clients`** ***`<dirección-IP-del-cliente>`*** para otorgarle acceso al cliente NDMP.
    - Para mayor seguridad, ejecute el comando **`net filter add operation allow clients`** ***`<client-IP-address>`*** **`interfaces`** ***`<dirección IP-de-la-interfaz-DD>`***.
    - Agregue la opción **`seq-id 1`** en el comando para hacer cumplir esta regla antes que cualquier otra regla de filtro de red.
- Un tamaño de registro mínimo (bloque) de software de respaldo.
  - Si es posible, configure el software de respaldo para usar un tamaño de registro mínimo (bloque) de 64 KiB o más. Los tamaños más grandes generalmente ofrecen rendimiento más rápido y mejor compresión de datos.
  - En función de la aplicación de respaldo, si cambia el tamaño después de la configuración inicial, los datos escritos con el tamaño original podrían volverse ilegibles.
- Acceso del usuario adecuado al sistema.
  - Para las operaciones de cinta básicas y el monitoreo, solo se requiere un nombre de inicio de sesión del usuario.
  - Para habilitar y configurar servicios DD VTL y realizar otras tareas de configuración, se requiere un inicio de sesión de sysadmin.

Límites de DD VTL

Antes de configurar o usar DD VTL, revise estos límites de tamaño, slots, etc.

- I/O Size: el tamaño de I/O máximo admitido para cualquier sistema DD que use DD VTL es 1 MB.
- Libraries: DD VTL admite un máximo de 64 bibliotecas por sistema DD (es decir, 64 instancias de DD VTL en cada sistema DD).
- Initiators: DD VTL admite un máximo de 1,024 iniciadores o WWPN (world-wide port names) por sistema DD.
- Tape Drives: la información acerca de las unidades de cinta se presenta en la siguiente sección.
- Data Streams: la información acerca de los flujos de datos se presenta en la tabla siguiente.

Tabla 136 Flujos de datos enviados a un sistema Data Domain

Modelo	RAM/NVRAM	Flujos de escritura de respaldo	Flujos de lectura de respaldo	Flujos de origen de replicación[a]	Flujos de destino[a] de replicación	Mixto
DD140, DD160, DD610	4 GB o 6 GB/0.5 GB	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20
DD620, DD630, DD640	8 GB/0.5 GB o 1 GB	20	16	20	20	w<=20; r<=16; ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; Total<=30
DD640, DD670	16 GB o 20 GB/1 GB	90	30	60	90	w<=90; r<=30; ReplSrc<=60; ReplDest<=90; ReplDest+w<=90; Total<=90
DD670, DD860	36 GB/1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD860	72 GB[b] / 1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD890	96 GB/2 GB	180	50	90	180	w<=180; r<=50; ReplSrc <=90;ReplDest<=180; ReplDest +w<=180; Total<=180
DD990	128 o 256 GB[b] / 4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD2200	8 GB	20	16	16	20	w<=20; r<=16; ReplSrc<=16; ReplDest<=20; ReplDest+w<=20; Total<=20
DD2200	16 GB	60	16	30	60	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest+w<=60; Total<=60
DD2500	32 o 64 GB/2 GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180

Tabla 136 Flujos de datos enviados a un sistema Data Domain (continuación)

Modelo	RAM/NVRAM	Flujos de escritura de respaldo	Flujos de lectura de respaldo	Flujos de origen de replicación[a]	Flujos de destino[a] de replicación	Mixto
DD4200	128 GB[b] / 4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD4500	192 GB[b] / 4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD7200	128 o 256 GB[b] / 4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD9500	256/512 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD9800	256/768 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD6300	De 48 a 96 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD6800	192 GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest +w<=400; Total<=400
DD9300	De 192 a 384 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest +w<=800; Total<=800
DD VE (8 TB)	8 GB / 512 MB	20	16	20	20	w<= 20 ; r<= 16 ReplSrc<=20; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=20;Total<=20
DD VE (16 TB)	16 GB / 512 MB o 24 GB / 1 GB	45	30	45	45	w<= 45 ; r<= 30 ReplSrc<=45; ReplDest<=45; ReplDest+w<=45; w+r+ReplSrc <=45;Total<=45
DD VE (32 TB)	24 GB/1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE (48 TB)	36 GB/1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE (64 TB)	48 GB/1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE (96 TB)	64 GB/2 GB	180	50	90	180	w<= 180 ; r<= 50 ReplSrc<=90; ReplDest<=180; ReplDest

Tabla 136 Flujos de datos enviados a un sistema Data Domain (continuación)

Modelo	RAM/NVRAM	Flujos de escritura de respaldo	Flujos de lectura de respaldo	Flujos de origen de replicación [a]	Flujos de destino[a] de replicación	Mixto
						+w<=180; w+r+ReplSrc <=180;Total<=180
DD3300 (4 TB)	12 GB (memoria virtual) / 512 MB	20	16	30	20	w<= 20 ; r<= 16 ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=30;Total<=30
DD3300 (8 TB)	32 GB (memoria virtual) / 1536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 (16 TB)	32 GB (memoria virtual) / 1536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 (32 TB)	46 GB (memoria virtual) / 1536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=140

a. DirRepl, OptDup, MTreeRepl
b. La opción de software Data Domain Extended Retention está disponible solo para estos dispositivos con memoria extendida (máxima)

- Slots: DD VTL admite un máximo de:
  - 32,000 slots por librería
  - 64,000 slots por sistema DD

  El sistema DD agrega automáticamente slots para mantener el número de slots igual o mayor que el número de unidades.

  Nota

  Algunos controladores de dispositivos (por ejemplo, controladores del dispositivo de cinta IBM AIX) limitan las configuraciones de librerías a límites de unidades/slots específicos, que pueden ser inferiores que los admitidos por el sistema DD. Las aplicaciones de respaldo y las unidades usadas por estas pueden verse afectadas por esta limitación.

- CAP (puertos de acceso a cartuchos): DD VTL admite un máximo de:
  - 100 CAP por librería
  - 1000 CAP por sistema DD

Cantidad de unidades admitidas por una DD VTL

La cantidad máxima de unidades admitidas por una DD VTL depende de la cantidad de cores de CPU y la cantidad de memoria instalada (RAM y NVRAM, si corresponde) en un sistema DD.

Nota

No hay referencias a números de modelos en esta tabla, porque hay muchas combinaciones de cores de CPU y memorias para cada modelo, y la cantidad de unidades admitidas depende *únicamente* de los cores de CPU y las memorias, no del modelo en particular.

Tabla 137 Cantidad de unidades admitidas por una DD VTL

N.º de cores de CPU	RAM (en GB)	NVRAM (en GB)	Número máximo de unidades admitidas
Menos de 32	4 o menos	N/C	64
	Más de 4, hasta 38	N/C	128
	Más de 38, hasta 128	N/C	256
	Más de 128	N/C	540
De 32 a 39	Hasta 128	Menos de 4	270
	Hasta 128	4 o más	540
	Más de 128	N/C	540
De 40 a 59	N/C	N/C	540
60 o más	N/C	N/C	1,080

Códigos de barras de cintas

Cuando crea una cinta, debe asignar un *código de barras* único (nunca códigos de barras duplicados, ya que esto puede causar un comportamiento inesperado). Cada código de barras está compuesto por ocho caracteres: los primeros seis son números o letras en mayúscula (0-9, A-Z) y los últimos dos son el código de cinta del tipo de cinta admitido, como se muestra en la siguiente tabla.

Nota

A pesar de que un código de barras de DD VTL consta de ocho caracteres, seis u ocho caracteres se pueden transmitir a una aplicación de respaldo, según el tipo de cambiador.

Tabla 138 Códigos de cinta por tipo de cinta

Tipo de cinta	Capacidad predeterminada (a menos que se indique)	Código de cinta
LTO-1	100 GiB	L1
LTO-1	50 GiB (no predeterminada)	LA[a]
LTO-1	30 GiB (no predeterminada)	LB

Tabla 138 Códigos de cinta por tipo de cinta (continuación)

Tipo de cinta	Capacidad predeterminada (a menos que se indique)	Código de cinta
LTO-1	10 GiB (no predeterminada)	LC
LTO-2	200 GiB	L2
LTO-3	400 GiB	L3
LTO-4	800 GiB	L4
LTO-5 (predeterminado)	1.5 TiB	L5

a. Para TSM, use el código de cinta L2 si se ignora el código LA.

Para las bibliotecas de cintas múltiples, los códigos de barras se incrementan automáticamente si el sexto carácter (antes de la "L") es un número. Si ocurre un desbordamiento (9 a 0), la numeración se mueve una posición a la izquierda. Si el siguiente carácter para incrementar es una letra, el incremento se interrumpe. Aquí hay algunos códigos de barras de ejemplo y cómo se incrementará cada uno:

- 000000L1 crea cintas con capacidad de 100 GiB y puede aceptar un conteo de hasta 100,000 cintas (de 000000 a 99999).
- AA0000LA crea cintas con capacidad de 50 GiB y puede aceptar un conteo de hasta 10,000 cintas (de 0000 a 9999).
- AAAA00LB crea cintas con capacidad de 30 GiB y puede aceptar un conteo de hasta 100 cintas (de 00 a 99).
- AAAAAALC crea una cinta con capacidad de 10 GiB. Solo se puede crear una cinta con este nombre.
- AAA350L1 crea cintas con capacidad de 100 GiB y puede aceptar un conteo de hasta 650 cintas (de 350 a 999).
- 000AAALA crea una cinta con capacidad de 50 GiB. Solo se puede crear una cinta con este nombre.
- 5M7Q3KLB crea una cinta con capacidad de 30 GiB. Solo se puede crear una cinta con este nombre.

Compatibilidad con unidades de cinta LTO

Puede tener diferentes generaciones de tecnología LTO (Cinta lineal abierta) en la configuración; la compatibilidad entre estas generaciones se presenta en formato tabular.

En esta tabla:

- RW = compatible con lectura y escritura
- R = compatible con solo lectura
- — = no compatible

Tabla 139 Compatibilidad con unidades de cinta LTO

formato de cinta	Unidad LTO-5	Unidad LTO-4	Unidad LTO-3	Unidad LTO-2	Unidad LTO-1
Cinta LTO-5	RW	—	—	—	—
Cinta LTO-4	RW	RW	—	—	—
Cinta LTO-3	R	RW	RW	—	—
Cinta LTO-2	—	R	RW	RW	—
Cinta LTO-1	—	—	R	RW	RW

Configuración de una DD VTL

Para configurar una DD VTL simple, use el asistente de configuración, que se describe en el capítulo *Introducción*.

Hay documentación similar disponible en la *Guía de configuración inicial de Data Domain Operating System*.

Después, continúe con los siguientes temas para habilitar DD VTL, crear bibliotecas y crear e importar cintas.

Nota

Si el ambiente de implementación incluye un sistema AS400 como cliente de DD VTL, consulte Configuración de las opciones predeterminadas de DD VTL en la página 398 para configurar el prefijo del número de serie para los cambiadores y las unidades VTL antes de configurar la relación DD VTL entre el sistema Data Domain y el sistema cliente AS400.

Sistemas de alta disponibilidad y DD VTL

Los sistemas de alta disponibilidad son compatibles con DD VTL. Sin embargo, si un trabajo DD VTL está en curso durante una conmutación por error, el trabajo deberá reiniciarse manualmente después de que finalice la conmutación por error.

La *Guía de compatibilidad de respaldo de Data Domain Operating System* proporciona detalles adicionales sobre los requisitos de HBA, switch, firmware y driver para el uso de DD VTL en un ambiente de alta disponibilidad.

Transferencia de cintas de DD VTL a la nube

DD VTL admite el almacenamiento del vault de VTL en el almacenamiento de DD Cloud Tier. Para utilizar esta funcionalidad, el sistema Data Domain debe ser una configuración de Cloud Tier compatible y tener una licencia de Cloud Tier, además de la licencia de VTL.

Debe obtener la licencia del almacenamiento de DD Cloud Tier y configurarlo antes de configurar DD VTL para utilizar el almacenamiento de nube para el vault. En DD Cloud Tier en la página 509, se proporciona información adicional sobre los requisitos para DD Cloud Tier y sobre cómo configurar DD Cloud Tier.

Los requisitos de interfaz de red y FC para VTL son los mismos tanto para el almacenamiento de vault local como para el basado en la nube. DD VTL no requiere una configuración especial para utilizar el almacenamiento de nube para el vault. Al configurar DD VTL, seleccione el almacenamiento de nube como la ubicación de vault.

Sin embargo, cuando se trabaja con un vault basado en la nube, hay algunas opciones de administración de datos que son únicas del vault basado en la nube. En Trabajar con vault en la nube en la página 418, se brinda más información.

Administración de una DD VTL

Puede administrar una DD VTL mediante Data Domain System Manager (DD System Manager) o mediante la interfaz de la línea de comandos (CLI) de Data Domain Operating System (DD OS). Después de iniciar sesión, puede comprobar el estado de su proceso de DD VTL, comprobar la información de licencia y revisar y configurar opciones.

Inicio de sesión

Para usar una interfaz gráfica del usuario (GUI) para administrar su biblioteca de cintas virtuales DD (DD VTL), inicie sesión en DD System Manager.

Equivalente de la CLI

También puede iniciar sesión en la CLI:

```
login as: sysadmin
Data Domain OS
Using keyboard-interactive authentication.
Password:
```

Habilitación del demonio de destino SCSI (CLI únicamente)

Si inicia sesión desde la CLI, debe habilitar el demonio de destino SCSI (el servicio Fibre Channel). Este demonio se activa durante las selecciones de activación de la DD VTL o de DD Boost-FC en DD System Manager. En la CLI, estos procesos se deben habilitar por separado.

```
# scsitarget enable
Please wait ...
SCSI Target subsystem is enabled.
```

Acceso a la DD VTL

En el menú a la izquierda de **Protocols** > **VTL**.

Status

En el área **Virtual Tape Libraries** > **VTL Service**, puede ver que el estado de su proceso de DD VTL se muestra en la parte superior, por ejemplo, **Enabled: Running**. La primera parte del estado será **Enabled** (activado) o Disabled **Disabled** (desactivado). La segunda parte será uno de los siguientes estados de proceso.

Tabla 140 Estados del proceso de DD VTL

Estado	Descripción
Running	El proceso de DD VTL está habilitado y activo (se muestra en verde).
Starting	El proceso de DD VTL se está iniciando.
Stopping	El proceso de DD VTL se está apagando.
Stopped	El proceso de DD VTL está deshabilitado (se muestra en rojo).
Timing out	El proceso de DD VTL se bloqueó y está intentando un reinicio automático.

Tabla 140 Estados del proceso de DD VTL (continuación)

Estado	Descripción
Stuck	Después de varios reinicios automáticos fallidos, el proceso de DD VTL no puede apagarse normalmente, por lo que se está intentando interrumpirlo.

Licencia de DD VTL
La línea de licencia de VTL indica si la licencia de DD VTL se ha aplicado. Si dice Unlicensed, seleccione **Add License**. Ingrese el número de licencia en el cuadro de diálogo Add License Key. Seleccione **Next** y **OK**.

Nota

Se debe completar toda la información de licencia como parte del proceso de configuración de fábrica; sin embargo, si la opción de DD VTL se adquirió posteriormente, es posible que el número de licencia de DD VTL no esté disponible en ese momento.

Equivalente de la CLI
También puede verificar que la licencia de DD VTL se haya instalado en la CLI:

```
# elicense show
## License Key                  Feature
--    -------------------       -----------
1     DEFA-EFCD-FCDE-CDEF       Replication
2     EFCD-FCDE-CDEF-DEFA       VTL
--    -------------------       -----------
```

Si la licencia no está presente, cada unidad viene con documentación (una tarjeta de instalación rápida) que mostrará las licencias que se han comprado. Ingrese uno de los siguientes comandos para completar la clave de licencia.

```
# license add <license-code>
```

```
# elicense update <license-file>
```

I/OS License (para usuarios de IBM i)
Para los clientes de IBM i, la línea I/OS License le indica si se ha aplicado la licencia de I/OS. Si dice Unlicensed, seleccione **Add License**. Debe ingresar una licencia de I/OS válida en uno de los siguientes formatos: `xxxx-xxxx-xxxx-xxxx` or `xxxx-xxxx-xxxx-xxxx-xxxx`. La licencia de I/OS debe estar instalada antes de crear la biblioteca y las unidades que se usarán en el sistema IBM i. Seleccione **Next** y **OK**.

Habilitación de DD VTL

Al habilitar la DD VTL, se transmite el WWN de la HBA de Data Domain al fabric del cliente y se habilitan todas las bibliotecas y unidades de bibliotecas. Si se requiere un plan de envío en la forma de procesos de control de cambios, este proceso se debe habilitar para facilitar la zonificación.

Procedimiento

1. Asegúrese de contar con una licencia de DD VTL y de que el sistema de archivos esté habilitado.
2. Seleccione **Virtual Tape Libraries** > **VTL Service**.
3. A la derecha del área Status, seleccione **Enable**.
4. En el cuadro de diálogo Enable Service, seleccione **OK**.

5. Después de que se habilite la DD VTL, tenga en cuenta que el estado cambiará a **Enabled: Running** en color verde. Además, tenga en cuenta que las opciones de la DD VTL configurada se muestran en el área Option Defaults.

Equivalente de la CLI

```
# vtl enable Starting VTL, please wait ... VTL is enabled.
```

Deshabilitación de DD VTL

Al deshabilitar DD VTL, se cierran todas las bibliotecas y finaliza el proceso de DD VTL.

Procedimiento

1. Seleccione **Virtual Tape Libraries** > **VTL Service**.
2. A la derecha del área Status, seleccione **Disable**.
3. En el cuadro de diálogo Disable Service, seleccione **OK**.
4. Después de que se haya deshabilitado DD VTL, tenga en cuenta que el área Status cambiará a **Disabled: Stopped** en color rojo.

Equivalente de la CLI

```
# vtl disable
```

Valores predeterminados de opción de DD VTL

El área Option Default de la página VTL Service muestra la configuración actual de las opciones predeterminadas de DD VTL (auto-eject, auto-offline y barcode-length) que se pueden configurar.

En el área **Virtual Tape Libraries** > **VTL Service**, se muestran las opciones predeterminadas actuales para DD VTL. Seleccione **Configure** para cambiar cualquiera de estos valores.

Tabla 141 Valores predeterminados de opciones

Elemento	Descripción
Propiedad	Muestra las opciones configuradas: • auto-eject • auto-offline • barcode-length
Valor	Proporciona el valor de cada opción configurada: • auto-eject: default (deshabilitada), enabled o disabled • auto-offline: default (deshabilitada), enabled o disabled • barcode-length: default (8), 6 u 8

Configuración de las opciones predeterminadas de DD VTL

Puede configurar opciones predeterminadas de DD VTL al agregar una licencia, al crear una biblioteca o en cualquier momento después de eso.

Nota

De manera predeterminada, se asignan opciones globales a las DD VTL, y esas opciones se actualizan cada vez que cambian las opciones globales, a menos que se cambien manualmente mediante este método.

Procedimiento

1. Seleccione **Virtual Tape Libraries** > **VTL Service**.
2. En el área Option Defaults, seleccione **Configure**. En el cuadro de diálogo Configure Default Options, cambie cualquiera de las opciones predeterminadas o todas.

Tabla 142 Opciones predeterminadas de DD VTL

Opción	Valores	Notas
auto-eject	default (deshabilitada), enabled o disabled	Habilitar la expulsión automática causa que cualquier cinta colocada en un CAP (puerto de acceso a cartuchos) se mueva automáticamente al vault virtual, a menos que: • La cinta haya provenido del vault, en cuyo caso permanece en el CAP. • Un comando `ALLOW_MEDIUM_REMOVAL` con un valor 0 (falso) se haya emitido a la biblioteca para impedir la extracción del medio del CAP al exterior.
auto-offline	default (deshabilitada), enabled o disabled	Habilitar la desconexión automática desconecta automáticamente una unidad antes de que se realice una operación de transferencia de cinta.
barcode-length	default (8), 6 u 8 [establecida automáticamente en 6 para los modelos de cambiador L180, RESTORER-L180 y DDVTL]	A pesar de que un código de barras de la DD VTL consta de ocho caracteres, seis u ocho caracteres se pueden transmitir a una aplicación de respaldo, según el tipo de cambiador.

3. Seleccione **OK**.
4. O, para deshabilitar todas estas opciones de servicio, seleccione **Reset to Factory** y los valores se restablecerán inmediatamente a los valores predeterminados de fábrica.

Requistos posteriores

Si el ambiente de DD VTL contiene un AS400 como cliente de DD VTL, configure la opción DD VTL para el prefijo de número de serie manualmente antes de añadir el AS400 al ambiente de DD VTL. Esto es necesario para evitar números de serie duplicados cuando hay varios sistemas Data Domain que utilizan DD VTL. El valor de prefijo de número de serie:

- Debe ser un valor único de seis dígitos de modo que ningún otro DD VTL en cualquier sistema Data Domain en el ambiente tenga el mismo número de prefijo
- No debe terminar en cero

Configure este valor una sola vez durante la implementación del sistema Data Domain y la configuración de DD VTL. Persistirá con cualquier futura actualización de DD OS en el sistema. Establecer este valor no requiere que se reinicie el servicio de DD VTL. Cualquier biblioteca de DD VTL creada después de establecer este valor utilizará el nuevo prefijo para el número de serie.

CLI equivalent

```
# vtl option set serial-number-prefix value
# vtl option show serial-number-prefix
```

Trabajo con librerías

Una librería emula una librería de cintas físicas con unidades, cambiadores, CAP (puertos de acceso a cartuchos) y slots (slots de cartucho). Al seleccionar **Virtual Tape Libraries** > **VTL Service** > **Libraries**, se muestra información detallada de todas las librerías configuradas.

Tabla 143 Información de librerías

Elemento	Descripción
Nombre	El nombre de una librería configurada.
de unidades	El número de unidades configuradas en la librería.
Slots	El número de slots configurados en la librería.
CAPs	El número de CAP (puertos de acceso a cartuchos) configurados en la librería.

Desde el menú More Tasks, puede crear y eliminar librerías, así como buscar cintas.

Creación de librerías

DD VTL admite un máximo de 64 bibliotecas por sistema, es decir, 64 instancias de biblioteca de cintas virtuales activas simultáneamente en cada sistema DD.

Antes de comenzar

Si el ambiente de implementación incluye un sistema AS400 como cliente DD VTL, consulte Configuración de las opciones predeterminadas de DD VTL en la página 398 para configurar el prefijo del número de serie para los cambiadores y las unidades VTL antes de crear la biblioteca DD VTL y configurar la relación DD VTL entre el sistema Data Domain y el sistema cliente AS400.

Procedimiento

1. Seleccione **Virtual Tape Libraries** > **VTL Service** > **Libraries**.

2. Seleccione **More Tasks** > **Library** > **Create**.
3. En el cuadro de diálogo Create Library, ingrese la siguiente información:

Tabla 144 Cuadro de diálogo Create Library

Campo	Entrada del usuario
Library Name	Ingrese el nombre de entre 1 y 32 caracteres alfanuméricos.
Cantidad de unidades	Ingrese la cantidad de unidades, de 1 a 98 (consulte la sección Nota). La cantidad de unidades que se crearán corresponderá al número de flujos de datos que se escribirán en una librería. **Nota** La cantidad máxima de unidades admitidas por una DD VTL depende de la cantidad de cores de CPU y la cantidad de memoria instalada (RAM y NVRAM, si corresponde) en un sistema DD.
Drive Model	Seleccione el modelo deseado de la lista desplegable: • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5 (predeterminado) • HP-LTO-3 • HP-LTO-4 No mezcle tipos de unidades, o tipos de medios, en la misma librería. Esto puede generar resultados inesperados o errores en la operación de respaldo.
Cantidad de slots	Ingrese el número de slots en la librería. Aquí se incluyen algunos puntos que debe tener en cuenta: • El número de slots debe ser igual o mayor que el número de unidades. • Puede tener hasta 32,000 slots por librería individual. • Puede tener hasta 64,000 slots por sistema. • Intente tener suficientes slots para que las cintas permanezcan en la DD VTL y nunca se deban exportar a un vault (para evitar volver a configurar la DD VTL y facilitar la sobrecarga de administración). • Tenga en cuenta las aplicaciones con licencias por el número de slots. Como ejemplo, para un cartucho de 100 GB estándar en un sistema DD580, puede configurar 5000 slots. Esto sería suficiente para admitir hasta 500 TB (suponiendo que los datos se pueden comprimir razonablemente).
Number of CAPs	Ingrese el número de puertos de acceso a cartuchos (CAP) (opcional).

Tabla 144 Cuadro de diálogo Create Library (continuación)

Campo	Entrada del usuario
	• Puede tener hasta 100 CAP por librería. • Puede tener hasta 1000 CAP por sistema. Compruebe la documentación específica para la aplicación de software de respaldo en el sitio del servicio de soporte en línea para recibir orientación.
Changer Model Name	Seleccione el modelo deseado de la lista desplegable: • L180 (predeterminado) • RESTORER-L180 • TS3500 • I2000 • I6000 • DDVTL Compruebe la documentación específica para la aplicación de software de respaldo en el sitio del servicio de soporte en línea para recibir orientación. Consulte también la matriz de soporte de DD VTL para conocer la compatibilidad de las bibliotecas emuladas con el software admitido.
Opciones	
auto-eject	default (deshabilitada), enable o disable
auto-offline	default (deshabilitada), enable o disable
barcode-length	default (8), 6 u 8 [establecida automáticamente en 6 para los modelos de cambiador L180, RESTORER-L180 y DDVTL]

4. Seleccione **OK**.

   Después de que el cuadro de diálogo de estado Create Library muestre **Completed**, seleccione **OK**.

   La librería nueva aparecerá en el ícono Libraries del árbol VTL Service y las opciones configuradas aparecerán como íconos en la librería. Al seleccionar la librería, se mostrarán detalles acerca de esta en el panel de información.

   Tenga en cuenta que el acceso a las VTL y a las unidades se administra a través de Access Groups.

Equivalente de la CLI

```
# vtl add NewVTL model L180 slots 50 caps 5
This adds the VTL library, NewVTL. Use 'vtl show config NewVTL'
to view it.

# vtl drive add NewVTL count 4 model IBM-LTO-3
This adds 4 IBM-LTO-3 drives to the VTL library, NewVTL.
```

Eliminación de librerías

Cuando una cinta está en una unidad dentro de una biblioteca y se elimina esa biblioteca, la cinta se mueve al vault. Sin embargo, el pool de la cinta no cambia.

Procedimiento

1. Seleccione **Virtual Tape Libraries** > **VTL Service** > **Libraries**.
2. Seleccione **More Tasks** > **Library** > **Delete**.
3. En el cuadro de diálogo Delete Libraries, seleccione o confirme la casilla de verificación de los elementos que desea eliminar:
   - El nombre de cada biblioteca,
   - o, Library Names, para eliminar todas las bibliotecas.
4. Seleccione **Next**.
5. Verifique las bibliotecas que se eliminarán y seleccione **Submit** en los cuadros de diálogo de confirmación.
6. Después de que el cuadro de diálogo Delete Libraries Status muestre `Completed`, seleccione **Close**. Las bibliotecas seleccionadas se eliminarán de la DD VTL.

Equivalente de la CLI

```
# vtl del OldVTL
```

Búsqueda de cintas

Puede usar una variedad de criterios (ubicación, pool o código de barras) para buscar una cinta.

Procedimiento

1. Seleccione **Virtual Tape Libraries** o **Pools**.
2. Seleccione el área en la que desea buscar (librería, vault, pool).
3. Seleccione **More Tasks** > **Tapes** > **Search**.
4. En el cuadro de diálogo Search Tapes, especifique información acerca de las cintas que desea buscar.

Tabla 145 Cuadro de diálogo Search Tapes

Campo	Entrada del usuario
Location	Especifique una ubicación o deje el valor predeterminado (All).
Pool	Seleccione el nombre del pool en el que desee buscar la cinta. Si no se han creado pools, use el pool predeterminado.
Barcode	Especifique un código de barras único o deje el (*) predeterminado para devolver un grupo de cintas. El código de barras permite los caracteres comodín ? y *, donde ? coincide con cualquier carácter único y * coincide con 0 o más caracteres.
Count	Especifique el número máximo de cintas que desea que se devuelvan. Si deja este campo en blanco, se utilizará el código de barras predeterminado (*).

5. Seleccione **Search**.

Uso de una librería seleccionada

Al seleccionar **Virtual Tape Libraries** > **VTL Service** > **Libraries** > *library*, se muestra información detallada de una librería seleccionada.

Tabla 146 Dispositivos

Elemento	Descripción
Dispositivo	Los elementos en la librería, como unidades, slots y CAP (puertos de acceso a cartuchos).
Loaded	El número de dispositivos con medios cargados.
Vacío	El número de dispositivos sin medios cargados.
Total	El número total de dispositivos vacíos y cargados.

Tabla 147 Opciones

Propiedad	Valor
auto-eject	enabled o disabled
auto-offline	enabled o disabled
barcode-length	6 u 8

Tabla 148 Cintas.

Elemento	Descripción
Pool	El nombre del pool donde están ubicadas las cintas.
Tape Count	El número de cintas en ese pool.
Capacidad	La capacidad total configurada de las cintas en ese pool, en GiB (Gibibytes, el equivalente de base 2 de GB, Gigabytes).
Utilizado	La cantidad de espacio total utilizado en las cintas virtuales en ese pool.
Average Compression	La cantidad de compresión promedio lograda en los datos de las cintas de ese pool.

En el menú More Tasks, puede eliminar, renombrar o configurar las opciones de una librería; crear, eliminar, importar, exportar o trasladar cintas; y agregar o eliminar slots y CAP.

Creación de cintas

Puede crear cintas en una biblioteca o un pool. Si se inicia desde un pool, el sistema crea las cintas primero y, a continuación, las importa a la biblioteca.

Procedimiento

1. Seleccione **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library* o **Vault** or **Pools** > **Pools >** *pool*.

2. Seleccione **More Tasks** > **Tapes** > **Create**.
3. En el cuadro de diálogo Create Tapes, ingrese la siguiente información acerca de la cinta:

Tabla 149 Cuadro de diálogo Create Tapes

Campo	Entrada del usuario
Library (si se inicia desde una biblioteca)	Si hay un menú desplegable habilitado, seleccione la biblioteca o deje la selección predeterminada.
Nombre de pool	Seleccione el nombre del pool en el que residirá la cinta de la lista desplegable. Si no se han creado pools, use el pool Default.
Cantidad de cintas	Para una biblioteca, seleccione un valor de 1 a 20. Para un pool, seleccione un valor de 1 a 100,000 o deje el valor predeterminado (20). [Aunque el número de cintas admitidas es ilimitado, no puede crear más de 100,000 cintas a la vez].
Starting Barcode	Ingrese el número de código de barras inicial (con el formato A99000LA).
Tape Capacity	Especifique el número de GiB entre 1 y 4000 para cada cinta (esta configuración anula la configuración de capacidad de código de barras) (opcional). Para obtener un uso eficiente del espacio en disco, use 100 GiB o menos.

4. Seleccione **OK** y **Close**.

Equivalente de la CLI

```
 # vtl tape add A00000L1 capacity 100 count 5 pool VTL_Pool ...
added 5 tape(s)...
```

Nota

Debe aumentar automáticamente los nombres de los volúmenes de cinta en formato de base 10.

Eliminación de cintas

Puede eliminar cintas desde una biblioteca o un pool. Si se inicia desde una biblioteca, el sistema primero exporta las cintas y, a continuación, las elimina. Las cintas deben estar en el vault, no en una biblioteca. En un sistema DD de destino de replicación, no se permite eliminar una cinta.

Procedimiento

1. Seleccione **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library* or **Vault** o **Pools** > **Pools >** *pool*.
2. Seleccione **More Tasks** > **Tapes** > **Delete**.
3. En el cuadro de diálogo Delete Tapes, especifique información de búsqueda acerca de las cintas que desea eliminar y seleccione **Search**:

Tabla 150 Cuadro de diálogo Delete Tapes

Campo	Entrada del usuario
Ubicación	Si hay una lista desplegable, seleccione una biblioteca o deje la selección de **Vault** predeterminada.
Pool	Seleccione el nombre del pool en el que desee buscar la cinta. Si no se han creado pools, use el pool Default.
Barcode	Especifique un código de barras único o deje el (*) predeterminado para buscar un grupo de cintas. El código de barras permite los caracteres comodín ? y *, donde ? coincide con cualquier carácter único y * coincide con 0 o más caracteres.
Conteo	Especifique el número máximo de cintas que desea que se devuelvan. Si deja este campo en blanco, se utilizará el código de barras predeterminado (*).
Tapes Per Page	Seleccione el número máximo de cintas para mostrar por página; los valores posibles son 15, 30 y 45.
Select all pages	Seleccione la casilla de verificación **Select All Pages** para seleccionar todas las cintas devueltas por la consulta de búsqueda.
Items Selected	Muestra el número de cintas seleccionadas entre varias páginas, y se actualiza automáticamente con cada selección de cintas.

4. Seleccione la casilla de verificación de la cinta que se debe eliminar o la casilla de verificación de la columna de encabezado para eliminar todas las cintas y, a continuación, seleccione **Next**.
5. Seleccione **Submit** en la ventana de confirmación y seleccione **Close**.

Nota

Después de que se quita una cinta, el espacio en disco físico utilizado para la cinta no se reclama hasta después de una operación de limpieza del sistema de archivos.

Equivalente de la CLI

```
# vtl tape del barcode [count count] [pool pool]
```

Por ejemplo:

```
# vtl tape del A00000L1
```

Nota

Puede actuar en rangos; sin embargo, si falta una cinta en el rango, la acción se interrumpirá.

Importación de cintas

Importar una cinta significa que una cinta existente se moverá del vault a un slot, una unidad o un puerto de acceso a cartuchos (CAP) de una librería.

El número de cintas que puede importar a la vez se limita según el número de slots vacíos en la librería, es decir, no puede importar más cintas que el número de slots actualmente vacíos.

Para ver los slots disponibles para una librería, seleccione la librería del menú de agrupamiento. El panel de información de la librería muestra el conteo en la columna Empty.

- Si una cinta está en una unidad y se conoce que el origen de la cinta es un slot, se reserva un slot.
- Si una cinta está en una unidad y el origen de la cinta es desconocido (slot o CAP), se reserva un slot.
- Si una cinta está en una unidad y se conoce que el origen de la cinta es un CAP, no se reserva un slot. (La cinta vuelve al CAP cuando se quita de la unidad).
- Para mover una cinta a una unidad, consulte la sección sobre cómo mover cintas a continuación.

Procedimiento

1. Puede importar cintas a través del paso a. o del paso b.

   a. Seleccione **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *biblioteca*. A continuación, seleccione **More Tasks** > **Tapes** > **Import**. En el cuadro de diálogo Import Tapes, especifique información de búsqueda acerca de las cintas que desea importar y seleccione **Search**:

   Tabla 151 Cuadro de diálogo Import Tapes

Campo	Entrada del usuario
Location	Si hay una lista desplegable, seleccione la ubicación de la cinta o deje el valor predeterminado de **Vault**.
Pool	Seleccione el nombre del pool en el que desee buscar la cinta. Si no se han creado pools, use el pool Default.
Barcode	Especifique un código de barras único o deje el (*) predeterminado para devolver un grupo de cintas. El código de barras permite los caracteres comodín ? y *, donde ? coincide con cualquier carácter único y * coincide con 0 o más caracteres.
Conteo	Especifique el número máximo de cintas que desea que se devuelvan. Si deja este campo en blanco, se utilizará el código de barras predeterminado (*).
Seleccione Destination > Device	Seleccione el dispositivo de destino donde se importará la cinta. Los valores posibles son Drive, CAP y Slot.
Tapes Per Page	Selecciona el número máximo de cintas para mostrar por página. Los valores posibles son 15, 30 y 45.
Items Selected	Muestra el número de cintas seleccionadas entre varias páginas, y se actualiza automáticamente con cada selección de cintas.

   En función de las condiciones anteriores, se busca un conjunto de cintas predeterminado para seleccionar las cintas que se van a importar. Si cambia el pool, el código de barras o el conteo, seleccione Search para actualizar el conjunto de cintas disponible.

   b. Seleccione **Virtual Tape Libraries** > **VTL Service** > **Libraries**> *library*> **Changer** > **Drives >** *drive* **> Tapes**. Seleccione las cintas para importar al seleccionar la casilla de verificación que aparece junto a:

- Una cinta individual;
- la columna **Barcode** para seleccionar todas las cintas de la página actual;
- o bien, la casilla de verificación **Select all pages** para seleccionar todas las cintas devueltas por la consulta de búsqueda.

Solo se pueden importar las cintas que muestren Vault en la ubicación.

Seleccione **Import from Vault**. Este botón está deshabilitado de forma predeterminada y se habilita únicamente si todas las cintas seleccionadas provienen del vault.

2. En la vista Import Tapes:, verifique la información de resumen y la lista de cintas, y seleccione **OK**.
3. Seleccione **Close** en la ventana de estado.

Equivalente de la CLI

```
# vtl tape show pool VTL_Pool
Processing tapes....
Barcode  Pool     Location State    Size    Used (%)           Comp ModTime
-------- -------- -------- ----- ------- --------------- ---- -------------------
A00000L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00001L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00002L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00003L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00004L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
-------- -------- -------- ----- ------- --------------- ---- -------------------
VTL Tape Summary
----------------
Total number of tapes:     5
Total pools:               1
Total size of tapes:       500 GiB
Total space used by tapes: 0.0 GiB
Average Compression:       0.0x

# vtl import NewVTL barcode A00000L3 count 5 pool VTL_Pool
... imported 5 tape(s)...

# vtl tape show pool VTL_Pool
Processing tapes....

VTL Tape Summary
----------------
Total number of tapes:     5
Total pools:               1
Total size of tapes:       500 GiB
Total space used by tapes: 0.0 GiB
Average Compression:       0.0x
```

Exportación de cintas

La *exportación de cintas quita* las cintas de un slot, una unidad o un puerto de acceso a cartuchos (CAP) y los envía al vault.

Procedimiento

1. Puede exportar cintas a través del paso a. o del paso b.
   a. Seleccione **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *biblioteca*. A continuación, seleccione **More Tasks** > **Tapes** > **Export**. En el cuadro de diálogo Export Tapes, especifique información de búsqueda acerca de las cintas que desea exportar y seleccione **Search**:

Tabla 152 Cuadro de diálogo Export Tapes

Campo	Entrada del usuario
Location	Si hay una lista desplegable, seleccione el nombre de la biblioteca donde está ubicada la cinta o deje la biblioteca seleccionada.
Pool	Seleccione el nombre del pool en el que desee buscar la cinta. Si no se han creado pools, use el pool Default.
Barcode	Especifique un código de barras único o deje el (*) predeterminado para devolver un grupo de cintas. El código de barras permite los caracteres comodín ? y *, donde ? coincide con cualquier carácter único y * coincide con 0 o más caracteres.
Conteo	Especifique el número máximo de cintas que desea que se devuelvan. Si deja este campo en blanco, se utilizará el código de barras predeterminado (*).
Tapes Per Page	Selecciona el número máximo de cintas para mostrar por página. Los valores posibles son 15, 30 y 45.
Select all pages	Seleccione la casilla de verificación **Select All Pages** para seleccionar todas las cintas devueltas por la consulta de búsqueda.
Items Selected	Muestra el número de cintas seleccionadas entre varias páginas, y se actualiza automáticamente con cada selección de cintas.

b. Seleccione **Virtual Tape Libraries** > **VTL Service** > **Libraries**> *library*> **Changer** > **Drives >** *drive* **> Tapes**. Seleccione las cintas para exportar al seleccionar la casilla de verificación que aparece junto a:

- Una cinta individual;
- la columna **Barcode** para seleccionar todas las cintas de la página actual;
- o bien, la casilla de verificación **Select all pages** para seleccionar todas las cintas devueltas por la consulta de búsqueda.

Solo se pueden exportar las cintas con un nombre de biblioteca en la columna Location.

Seleccione **Export from Library**. Este botón se muestra de forma predeterminada y está habilitado únicamente si todas las cintas seleccionadas tienen un nombre de biblioteca en la columna Location.

2. En la vista Export Tapes:, verifique la información de resumen y la lista de cintas, y seleccione **OK**.
3. Seleccione **Close** en la ventana de estado.

Equivalente de la CLI

```
# vtl export NewVTL cap address 1 count 4
... exported 4 tape(s)...
```

Transferencia de cintas entre dispositivos dentro de una librería

Las cintas se pueden transferir entre dispositivos físicos dentro de una librería para imitar los procedimientos del software de respaldo para librerías de cintas físicas (que transfieren una cinta en una librería de un slot a una unidad, un slot a un CAP, un CAP a una unidad, y a la inversa). En una librería de cintas físicas, el software de respaldo

nunca transfiere una cinta fuera de la librería. Por lo tanto, la librería de destino no puede cambiar y se muestra solamente como aclaración.

Procedimiento

1. Seleccione **Virtual Tape Libraries** > **VTL Service** > **Libraries** > ***biblioteca***.

   Tenga en cuenta que cuando se inicia desde una librería, el panel Tapes permite que las cintas se transfieran únicamente entre dispositivos.

2. Seleccione **More Tasks** > **Tapes** > **Move**.

   Tenga en cuenta que cuando se inicia desde una librería, el panel Tapes permite que las cintas se transfieran únicamente entre dispositivos.

3. En el cuadro de diálogo Move Tape, especifique información de búsqueda acerca de las cintas que desea transferir y seleccione **Search**:

   Tabla 153 Cuadro de diálogo Move Tape

Campo	Entrada del usuario
Location	La ubicación no se puede modificar.
Pool	Seleccione un pool
Barcode	Especifique un código de barras único o deje el (*) predeterminado para devolver un grupo de cintas. El código de barras permite los caracteres comodín ? y *, donde ? coincide con cualquier carácter único y * coincide con 0 o más caracteres.
Conteo	Especifique el número máximo de cintas que desea que se devuelvan. Si deja este campo en blanco, se utilizará el código de barras predeterminado (*).
Tapes Per Page	Selecciona el número máximo de cintas para mostrar por página. Los valores posibles son 15, 30 y 45.
Items Selected	Muestra el número de cintas seleccionadas entre varias páginas, y se actualiza automáticamente con cada selección de cintas.

4. En la lista de resultados de la búsqueda, seleccione las cintas que desee mover.
5. Realice una de las siguientes acciones

   a. Seleccione el dispositivo de la lista Device (por ejemplo, un slot, una unidad o un CAP) e ingrese una dirección de inicio con números secuenciales para la segunda cinta y las posteriores. Para cada cinta que se va a transferir, si la dirección especificada está ocupada, se usa la siguiente dirección disponible.

   b. Deje la dirección en blanco si la cinta de una unidad provino originalmente de un slot y volverá a ese slot, o si la cinta se transferirá al siguiente slot disponible.

6. Seleccione **Next**.
7. En el cuadro de diálogo Move Tape, verifique la información de resumen y la lista de cintas, y seleccione **Submit**.
8. Seleccione **Close** en la ventana de estado.

Cómo agregar slots

Puede agregar slots desde una librería configurada para cambiar el número de elementos de almacenamiento.

Nota

Algunas aplicaciones de respaldo no reconocen automáticamente que se han agregado slots a una DD VTL. Consulte la documentación de la aplicación para obtener información sobre cómo configurar la aplicación para que reconozca este tipo de cambio.

Procedimiento

1. Seleccione **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *biblioteca*.
2. Seleccione **More Tasks** > **Slots** > **Add**.
3. En el cuadro de diálogo Add Slots, especifique el número de slots que desee agregar. El número total de slots en una librería o en todas las librerías de un sistema no puede superar 32,000 para una librería y 64,000 para un sistema.
4. Seleccione **OK** y **Close** cuando el estado muestre `Completed`.

Eliminación de slots

Puede eliminar slots desde una biblioteca configurada para cambiar el número de elementos de almacenamiento.

Nota

Algunas aplicaciones de respaldo no reconocen automáticamente que se han eliminado slots de una DD VTL. Consulte la documentación de la aplicación para obtener información sobre cómo configurar la aplicación para que reconozca este tipo de cambio.

Procedimiento

1. Si el slot que desea eliminar contiene cartuchos, muévalos al vault. El sistema eliminará únicamente los slots vacíos no confirmados.
2. Seleccione **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *biblioteca*.
3. Seleccione **More Tasks** > **Slots** > **Delete**.
4. En el cuadro de diálogo Delete Slots, especifique el número de slots que desee eliminar.
5. Seleccione **OK** y **Close** cuando el estado muestre `Completed`.

Cómo agregar CAP

Puede agregar CAP (puertos de acceso a cartuchos) desde una biblioteca configurada para cambiar el número de elementos de almacenamiento.

Nota

Los CAP son utilizados por una cantidad limitada de aplicaciones de respaldo. Consulte la documentación de su aplicación para asegurarse de que se admitan CAP.

Procedimiento

1. Seleccione **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library*.
2. Seleccione **More Tasks** > **CAPs** > **Add**.
3. En el cuadro de diálogo Add CAPs, especifique el número de CAP que desee agregar. Puede agregar entre 1 y 100 CAP por biblioteca y entre 1 y 1000 CAP por sistema.
4. Seleccione **OK** y **Close** cuando el estado muestre `Completed`.

Eliminación de CAP

Puede eliminar CAP (puertos de acceso de cartuchos) desde una biblioteca configurada para cambiar el número de elementos de almacenamiento.

Nota

Algunas aplicaciones de respaldo no reconocen automáticamente que se han eliminado CAP de una DD VTL. Consulte la documentación de la aplicación para obtener información sobre cómo configurar la aplicación para que reconozca este tipo de cambio.

Procedimiento

1. Si el CAP que desea eliminar contiene cartuchos, muévalos al vault; de lo contrario, esto se realizará automáticamente.
2. Seleccione **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *biblioteca*.
3. Seleccione **More Tasks** > **CAPs** > **Delete**.
4. En el cuadro de diálogo Delete CAPs, especifique el número de CAP que desee eliminar. Puede eliminar un máximo de 100 CAP por biblioteca o 1000 CAP por sistema.
5. Seleccione **OK** y **Close** cuando el estado muestre `Completed`.

Visualización de información del convertidor

Solo puede haber un convertidor por DD VTL. El modelo de convertidor que seleccione depende de la configuración específica.

Procedimiento

1. Seleccione **Virtual Tape Libraries** > **VTL Service** > **Libraries**.
2. Seleccione una biblioteca específica.
3. Si no se expande, seleccione el signo más (**+**) a la izquierda para abrir la biblioteca y seleccione un elemento de convertidor para que se muestre el panel de información del convertidor, que incluye la siguiente información.

Tabla 154 Panel de información del convertidor

Elemento	Descripción
Proveedor	El nombre del proveedor que fabricó el convertidor
Producto	El nombre del modelo
Revisión	El nivel de revisión

Tabla 154 Panel de información del convertidor (continuación)

Elemento	Descripción
Serial Number	El número de serie del convertidor

Trabajo con unidades

Al seleccionar **Virtual Tape Libraries** > **VTL Service** > **Libraries** > *biblioteca* >**Drives**, se muestra información detallada de todas las unidades en una biblioteca seleccionada.

Tabla 155 Panel de información de unidades

Columna	Descripción
Drive	La lista de unidades por nombre, donde el nombre es “Unidad #” y # es un número entre 1 y n que representa la dirección o ubicación de la unidad en la lista de unidades.
Vendor	El fabricante o proveedor de la unidad; por ejemplo, IBM.
Product	El nombre de producto de la unidad; por ejemplo, ULTRIUM-TD5.
Revisión	El número de revisión del producto de la unidad.
Serial Number	El número de serie del producto de la unidad.
Status	Si la unidad está vacía, abierta, bloqueada o cargada. Debe haber una cinta presente para que la unidad se bloquee o se cargue.
Cinta	El código de barras de la cinta en la unidad (si existe).
Pool	El pool de la cinta en la unidad (si existe).

Tape and library drivers: para trabajar con unidades, debe usar controladoras de cinta y biblioteca suministrados por su proveedor de software de respaldo que admitan las unidades IBM LTO-1, IBM LTO-2, IBM LTO-3, IBM LTO-4, IBM LTO-5 (predeterminada), HP-LTO-3 o HP-LTO-4 y las bibliotecas StorageTek L180 (predeterminada), RESTORER-L180, IBM TS3500, I2000, I6000 o DDVTL. Para obtener más información, consulte las guías *Application Compatibility Matrices and Integration Guides* de sus proveedores. Al configurar unidades, recuerde también los límites de transferencias de datos de respaldo, que se determinan en la plataforma en uso.

LTO drive capacities: dado que el sistema DD trata las unidades LTO como unidades virtuales, puede establecer una capacidad máxima de 4 TiB (4000 GiB) para cada tipo de unidad. Las capacidades predeterminadas para cada tipo de unidad LTO son las siguientes:

- Unidad LTO-1: 100 GiB
- Unidad LTO-2: 200 GiB
- Unidad LTO-3: 400 GiB
- Unidad LTO-4: 800 GiB
- Unidad LTO-5: 1.5 TiB

Migrating LTO-1 tapes: puede migrar cintas de VTL de tipo LTO-1 existentes a VTL que incluyan otras cintas y unidades de tipo LTO compatibles. Las opciones de migración son diferentes para cada aplicación de respaldo, de modo que debe seguir

las instrucciones de la guía de migración de cintas LTO específica de su aplicación. Para obtener la guía adecuada, visite el sitio del servicio de soporte en línea y, en el cuadro de texto de búsqueda, escriba **LTO Tape Migration for VTLs**.

Tape full: Early warning: recibirá una advertencia cuando el espacio en cinta restante esté casi completamente lleno, es decir, más que el 99.9, pero menos que el 100 por ciento. La aplicación puede seguir escribiendo hasta que se llene la cinta para alcanzar la capacidad del 100 por ciento. Sin embargo, la última escritura no se podrá recuperar.

En el menú More Tasks, puede crear o eliminar una unidad.

Creación de unidades

Consulte la sección *Cantidad de unidades admitidas por una DD VTL* para determinar el número máximo de unidades admitidas por su DD VTL en particular.

Procedimiento

1. Seleccione **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library***>** **Changer** > **Drives**.
2. Seleccione **More Tasks** > **Drives** > **Create**.
3. En el cuadro de diálogo Create Drive, ingrese la siguiente información:

   Tabla 156 Cuadro de diálogo Create Drive

Campo	Entrada del usuario
Ubicación	Seleccione el nombre de una librería o deje el nombre seleccionado.
Cantidad de unidades	Consulte la tabla de la sección *Cantidad de unidades admitidas por una DD VTL*, que aparece antes en este capítulo.
Model Name	Seleccione el modelo de la lista desplegable. Si ya existe otra unidad, esta opción está inactiva y se debe usar el tipo de unidad existente. No puede combinar tipos de unidades en la misma librería. • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5 (predeterminado) • HP-LTO-3 • HP-LTO-4

4. Seleccione **OK** y, cuando el estado muestre `Completed`, seleccione **OK**.

   La unidad agregada aparecerá en la lista Drives.

Eliminación de unidades

Una unidad debe estar vacía antes de que pueda eliminarse.

Procedimiento

1. Si hay una cinta en la unidad que desea eliminar, quite la cinta.
2. Seleccione **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *library* **>** **Changer** > **Drives**.

3. Seleccione **More Tasks** > **Drives** > **Delete**.
4. En el cuadro de diálogo Delete Drives, seleccione las casillas de verificación de las unidades que desee eliminar o seleccione la casilla de verificación **Drive** para eliminar todas las unidades.
5. Seleccione **Next** y, después de verificar que se hayan seleccionado las unidades correctas para eliminar, seleccione **Submit**.
6. Cuando aparezca en el cuadro de diálogo `Completed`, seleccione **Close**.

   La unidad se eliminará de la lista Drives.

Trabajo con una unidad seleccionada

Al seleccionar **Virtual Tape Libraries** > **VTL Service** > **Libraries** > *librería*> **Drives** >*unidad*, se muestra información detallada de una unidad seleccionada.

Tabla 157 Pestaña Drive

Columna	Descripción
Drive	La lista de unidades por nombre, donde el nombre es “Unidad #” y # es un número entre 1 y n que representa la dirección o ubicación de la unidad en la lista de unidades.
Vendor	El fabricante o proveedor de la unidad; por ejemplo, IBM.
Product	El nombre de producto de la unidad; por ejemplo, ULTRIUM-TD5.
Revision	El número de revisión del producto de la unidad.
Serial Number	El número de serie del producto de la unidad.
Status	Si la unidad está vacía, abierta, bloqueada o cargada. Debe haber una cinta presente para que la unidad se bloquee o se cargue.
Tape	El código de barras de la cinta en la unidad (si existe).
Pool	El pool de la cinta en la unidad (si existe).

Tabla 158 Pestaña Statistics

Columna	Descripción
Endpoint	El nombre específico del terminal.
Ops/s	Las operaciones por segundo.
Read KiB/s	La velocidad de lecturas en KiB por segundo.
Write KiB/s	La velocidad de escrituras en KiB por segundo.

Desde el menú More Tasks, puede eliminar la unidad o realizar una actualización.

Trabajo con cintas

Una cinta se representa como un archivo. Las cintas se pueden importar del vault a una librería. Además, se pueden exportar de una librería al vault. Las cintas se pueden

mover dentro de una biblioteca entre las unidades, slots (slots de cartuchos) y CAP (puertos de acceso a cartuchos).

Cuando se crean cintas, se colocan en el vault. Después de que se agregan al vault, se pueden importar, exportar, mover, explorar y quitar.

Al seleccionar **Virtual Tape Libraries** > **VTL Service** > **Libraries***> biblioteca >***Tapes**, se muestra información detallada de todas las cintas de una biblioteca seleccionada.

Tabla 159 Descripción de cintas

Elemento	Descripción
Código de barras	El código de barras único para la cinta.
Pool	El nombre del pool que contiene la cinta. El pool predeterminado contiene todas las cintas no asignadas a un pool creado por el usuario.
Ubicación	La ubicación de la cinta, ya sea en una biblioteca (unidad, CAP o número de slot) o en el vault virtual.
State	El estado de la cinta: • RW: lectura y escritura • RL: bloqueo de retención • RO: solo lectura • WP: protección contra escritura • RD: destino de replicación
Capacidad	La capacidad total de la cinta.
Utilizado	La cantidad de espacio en uso en la cinta.
Compresión	La cantidad de compresión realizada en los datos de una cinta.
Last Modified	La fecha del último cambio en la información de la cinta. Las horas de modificación utilizadas por el sistema para políticas basadas en la antigüedad pueden diferir de la hora de la última modificación que se muestra en las secciones de información de la cinta de DD System Manager.
Locked Until	Si se estableció el vencimiento de DD Retention Lock, se muestra la hora establecida. Si no existe un bloqueo de retención, este valor es `Not specified`.

Desde el panel de información, puede importar una cinta del vault, exportar una cinta a la biblioteca, establecer el estado de una cinta, crear una cinta o eliminar una cinta.

En el menú More Tasks, puede mover una cinta.

Cambio del estado de bloqueo de retención o escritura de una cinta

Antes de cambiar el estado de bloqueo de retención o escritura de una cinta, la cinta se debe haber creado e importado. Las cintas DD VTL siguen la política de bloqueo de retención de Data Domain estándar. Una vez que ha vencido el período de retención de una cinta, no se puede escribir ni modificar (sin embargo, se puede eliminar).

Procedimiento

1. Seleccione **Virtual Tape Libraries** > **VTL Service** > **Libraries** > ***biblioteca*** > **Tapes**.
2. Seleccione la cinta que desee modificar de la lista y seleccione **Set State** (arriba de la lista).
3. En el cuadro de diálogo Set Tape State, seleccione **Read-Writeable**, **Write-Protected** o **Retention-Lock**.
4. Si el estado es Retention-Lock, realice una de las siguientes acciones:
   - Especifique la fecha de vencimiento de la cinta en un número de días, semanas, meses o años especificado;
   - o bien, seleccione el ícono de calendario y seleccione la fecha del calendario. El bloqueo de retención vence al mediodía del día seleccionado.
5. Seleccione **Next** y, a continuación, seleccione **Submit** para cambiar el estado.

Trabajo con el vault

El vault contiene cintas que no están en uso en ninguna librería. Las cintas residen en una librería o en el vault.

Al seleccionar **Virtual Tape Libraries** > **VTL Service** > **Vault**, se muestra información detallada del pool predeterminado y otros pools existentes en el vault.

Los sistemas con DD Cloud Tier y DD VTL ofrecen la opción de almacenar vaults en el almacenamiento de nube.

Tabla 160 Resumen del pool

Elemento	Descripción
Pool Count	La cantidad de pools de VTL.
Tape Count	El número de cintas en los pools.
Size	El volumen total de espacio en los pools.
Logical Used	La cantidad de espacio utilizado en los pools.
Compression	El volumen de compresión promedio en los pools.

El panel **Protection Distribution** muestra la siguiente información.

Nota

Esta tabla solo aparece si DD Cloud Tier está habilitado en el sistema Data Domain.

Tabla 161 Distribución de protección

Elemento	Descripción
Storage type	Vault o nube.
Cloud provider	Para los sistemas con cintas en DD Cloud Tier, hay una columna correspondiente a cada proveedor de nube.
Logical Used	La cantidad de espacio utilizado en los pools.
Pool Count	La cantidad de pools de VTL.

Tabla 161 Distribución de protección (continuación)

Elemento	Descripción
Tape Count	El número de cintas en los pools.

Desde el menú More Tasks, puede crear, eliminar y buscar cintas en el vault.

Trabajar con vault en la nube

DD VTL admite varios parámetros que son exclusivos de las configuraciones en las que la vault se almacena el almacenamiento en niveles de DD Cloud.

Las siguientes operaciones están disponibles para trabajar con el almacenamiento en vaults en la nube.

- Configure la política de movimiento de datos y la información de la unidad en la nube para el pool de VTL especificado. Ejecute el comando **vtl pool modify *<pool-name>* data-movement-policy {user-managed | age-threshold *<days>* | none} to-tier {cloud} cloud-unit *<cloud-unit-name>***.
  Las políticas de movimiento de datos disponibles son las siguientes:
  - Administrado por el usuario: El administrador puede establecer esta política en un pool y seleccionar manualmente las cintas del pool para realizar la migración al nivel de nube. Las cintas se migran al nivel de nube en la primera operación de movimiento de datos luego de que se seleccionen las cintas.
  - Umbral de antigüedad: El administrador puede establecer esta política en un pool para permitir a DD VTL seleccionar automáticamente las cintas del pool para realizar la migración al nivel de nube en función de la antigüedad de la cinta. Las cintas se seleccionan para la migración en las seis horas posteriores al cumplimiento del umbral de antigüedad y se migran en la primera operación de movimiento de datos después de que se seleccionen las cintas.
- Seleccione una cinta especificada para la migración al nivel de nube. Ejecute el comando **vtl tape select-for-move barcode *<barcode>* [count *<count>*] pool *<pool>* to-tier {cloud}.**
- Deseleccione una cinta especificada para la migración al nivel de nube. Ejecute el comando **vtl tape deselect-for-move barcode *<barcode>* [count *<count>*] pool *<pool>* to-tier {cloud}.**
- Recupere una cinta del nivel de nube. Ejecute el comando **vtl tape recall start barcode *<barcode>* [count *<count>*] pool *<pool>***.
  Después de la recuperación, la cinta reside en una vault local de DD VTL y debe importarse a la biblioteca para permitir el acceso.

  Nota

  Ejecute el comando `vtl tape show` en cualquier momento para comprobar la ubicación actual de una cinta. La ubicación de la cinta se actualiza una hora después de que se mueva la cinta hacia o desde el nivel de nube.

Preparación del pool de la VTL para el movimiento de datos

Establezca la política de transferencia de datos en el pool de VTL para administrar la migración de datos de VTL del vault local a DD Cloud Tier.

El movimiento de datos de VTL se produce en el nivel del volumen de la cinta. Los volúmenes de cinta individuales o las colecciones de volúmenes de cinta se pueden

mover al nivel de nube, pero sólo desde la ubicación de vault. No se pueden mover las cintas en otros elementos de una VTL.

Nota

El pool y el vault de VTL predeterminado, los directorios `/data/col1/backup` o las configuraciones existentes de la biblioteca no pueden utilizarse para la cinta fuera de la nube.

Procedimiento

1. Seleccione **Protocols** > **DD VTL**.
2. Expanda la lista de pools y seleccione un pool en el cual desee habilitar la migración a DD Cloud Tier.
3. En el panel **Cloud Data Movement**, haga clic en **Create**, en **Cloud Data Movement Policy**.
4. En la lista desplegable **Policy**, seleccione una política de transferencia de datos:
   - **Age of tapes in days**
   - **Manual selection**
5. Configure los detalles de la política de transferencia de datos.
   - En **Age of tapes in days**, seleccione un umbral de antigüedad después del cual las cintas se migrarán a DD Cloud Tier y especifique una unidad de nube de destino.
   - En **Manual selection**, especifique una unidad de nube de destino.
6. Haga clic en **Create**.

   Nota

   Después de crear la política de transferencia de datos, los botones **Edit** y **Clear** pueden utilizarse para modificar o eliminar la política de transferencia de datos.

Equivalente de la CLI

Procedimiento

1. Establezca la política de movimiento de datos como user-managed o age-threshold

   Nota

   Los nombres de la unidad de pool y nube de VTL distinguen mayúsculas de minúsculas y los comandos fallarán si no respeta.

   - Para establecer la política de movimiento de datos como user-managed, ejecute el siguiente comando:
     `vtl pool modify cloud-vtl-pool data-movement-policy user-managed to-tier cloud cloud-unit ecs-unit1`

```
**   Any tapes that are already selected will be migrated on the next data-movement run.
VTL data-movement policy is set to "user-managed" for VTL pool "cloud-vtl-pool".
```

   - Para establecer la política de movimiento de datos como age-threshold, ejecute el siguiente comando:

Nota

El mínimo es de 14 días y el máximo es 182,250 días.

```
vtl pool modify cloud-vtl-pool data-movement-policy age-
threshold 14 to-tier cloud cloud-unit ecs-unit1
```

```
**   Any tapes that are already selected will be migrated on the next data-movement
run.
VTL data-movement policy "age-threshold" is set to 14 days for the VTL pool "cloud-
vtl-pool".
```

2. Verifique la política de movimiento de datos para el pool de VTL.

   Ejecute el siguiente comando:
   `vtl pool show all`

```
VTL Pools
Pool                    Status   Tapes   Size (GiB)   Used (GiB)   Comp   Cloud Unit
Cloud Policy
---------------------   ------   -----   ----------   ----------   ----   ----------
------------
cloud-vtl-pool          RW          50          250           41    45x   ecs-unit1
user-managed
Default                 RW           0            0            0     0x   -
none
---------------------   ------   -----   ----------   ----------   ----   ----------
------------
8080 tapes in 5 pools

 RO  : Read Only
 RD  : Replication Destination
 BCM : Backwards-Compatibility
```

3. Verificar que la política de MTree del pool de VTL sea `app-managed`.

   Ejecute el siguiente comando:
   `data-movement policy show all`

```
Mtree                       Target(Tier/Unit Name)   Policy        Value
-------------------------   ----------------------   -----------   -------
/data/col1/cloud-vtl-pool   Cloud/ecs-unit1          app-managed   enabled
-------------------------   ----------------------   -----------   -------
```

Quitar cintas del inventario de aplicaciones de respaldo

Use la aplicación de respaldo para verificar que los volúmenes de cinta que se transferirán a la nube estén marcados e inventariados según los requisitos de las aplicaciones de respaldo.

Selección de volúmenes de cintas para la transferencia de datos

Seleccione manualmente cintas para migrar a DD Cloud Tier (de inmediato o en la siguiente migración de datos programada) o elimine manualmente las cintas del programa de migración.

Antes de comenzar

Verifique que la aplicación de respaldo reconozca los cambios de estado de los volúmenes transferidos al almacenamiento de nube. Complete los pasos necesarios para que la aplicación de respaldo actualice su inventario a fin de reflejar el estado más reciente del volumen.

Si la cinta no está en el vault, no puede migrarse a DD Cloud Tier.

Procedimiento

1. Seleccione **Protocols** > **DD VTL**.
2. Expanda la lista de pools y seleccione el pool que está configurado para migrar cintas a DD Cloud Tier.
3. En el panel Pool, haga clic en la pestaña **Tape**.
4. Seleccione las cintas para la migración a DD Cloud Tier.
5. Haga clic en **Select for Cloud Move** para migrar la cinta en la siguiente migración programada o en **Move to Cloud Now** para migrar inmediatamente la cinta.

   Nota

   Si la política de transferencia de datos se basa en la antigüedad de la cintas, la opción **Select for Cloud Move** no estará disponible, ya que el sistema Data Domain selecciona automáticamente las cintas para la migración.

6. En el cuadro de diálogo de confirmación, haga clic en **Yes**.

Anular la selección de volúmenes de cintas para la transferencia de datos

Las cintas seleccionadas para la migración a DD Cloud Tier pueden eliminarse del programa de migración.

Procedimiento

1. Seleccione **Protocols** > **DD VTL**.
2. Expanda la lista de pools y seleccione el pool que está configurado para migrar cintas a DD Cloud Tier.
3. En el panel Pool, haga clic en la pestaña **Tape**.
4. Seleccione las cintas para la migración a DD Cloud Tier.
5. Haga clic en **Unselect Cloud Move** para eliminar la cinta del programa de migración.
6. En el cuadro de diálogo de confirmación, haga clic en **Yes**.

Equivalente de la CLI

Procedimiento

1. Identifique la ubicación de la ranura a la que debe transferirse el volumen de cintas.

   Ejecute el siguiente comando:
   `vtl tape show cloud-vtl`
   .

```
Processing tapes....
Barcode    Pool             Location            State    Size           Used (%)
Comp   Modification Time
--------   --------------   -----------------   -----   -----   ----------------
----   -------------------
T00001L3   cloud-vtl-pool   cloud-vtl slot 1    RW      5 GiB   5.0 GiB (99.07%)
205x   2017/05/05 10:43:43
T00002L3   cloud-vtl-pool   cloud-vtl slot 2    RW      5 GiB   5.0 GiB (99.07%)
36x   2017/05/05 10:45:10
T00003L3   cloud-vtl-pool   cloud-vtl slot 3    RW      5 GiB   5.0 GiB (99.07%)
73x   2017/05/05 10:45:26
```

2. Especifique el valor numérico de la ranura para exportar las cintas desde DD VTL.

   Ejecute el siguiente comando:
   ```
   vtl export cloud-vtl-pool slot 1 count 1
   ```
   .

3. Verifique que las cintas estén en el vault.

   Ejecute el siguiente comando:
   ```
   vtl tape show vault
   ```
   .

4. Seleccione las cintas para la transferencia de datos.

   Ejecute el siguiente comando:
   ```
   vtl tape select-for-move barcode T00001L3 count 1 pool
   cloud-vtl-pool to-tier cloud
   ```
   .

   Nota

   Si la política de transferencia de datos es de umbral de antigüedad, la transferencia de datos se realiza automáticamente después de 15-20 minutos.

5. Consulte la lista de las cintas programadas para transferirse al almacenamiento de nube durante la siguiente operación de transferencia de datos. Las cintas seleccionadas para la transferencia muestran una `(S)` en la columna de ubicación.

   Ejecute el siguiente comando:
   ```
   vtl tape show vault
   ```
   .

```
Processing tapes.....
Barcode    Pool                Location    State      Size           Used (%)   Comp
Modification Time
--------   -----------------   ---------   ------   ------   ----------------   ----
-------------------
T00003L3   cloud-vtl-pool      vault (S)   RW        5 GiB   5.0 GiB (99.07%)    63x
2017/05/05 10:43:43
T00006L3   cloud-vtl-pool      ecs-unit1   n/a       5 GiB   5.0 GiB (99.07%)    62x
2017/05/05 10:45:49
--------   -----------------   ---------   ------   ------   ----------------   ----
-------------------
* RD : Replication Destination
(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next
data-movement run.
(R) Recall operation is in progress for the tape.

VTL Tape Summary
----------------
Total number of tapes:     4024
Total pools:               3
Total size of tapes:       40175 GiB
Total space used by tapes: 39.6 GiB
Average Compression:       9.7x
```

6. Si la política de transferencia de datos es administrada por el usuario, inicie la operación de transferencia de datos.

   Ejecute el siguiente comando:
   ```
   data-movement start
   ```
   .

7. Observe el estado de la operación de transferencia de datos.

   Ejecute el siguiente comando:
   ```
   data-movement watch
   ```
   .

8. Verifique que los volúmenes de cintas se transfieran correctamente al almacenamiento de nube.

   Ejecute el siguiente comando:
   ```
   vtl tape show all cloud-unit ecs-unit1
   ```
   .

```
Processing tapes.....
Barcode  Pool           Location  State  Size         Used (%) Comp Modification Time
-------- -------------- --------- ----- ----- ---------------- ---- -------------------
T00001L3 cloud-vtl-pool ecs-unit1 n/a   5 GiB 5.0 GiB (99.07%)  89x 2017/05/05 10:41:41
T00006L3 cloud-vtl-pool ecs-unit1 n/a   5 GiB 5.0 GiB (99.07%)  62x 2017/05/05 10:45:49
-------- -------------- --------- ----- ----- ---------------- ---- -------------------
(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next
data-movement run.
(R) Recall operation is in progress for the tape.

VTL Tape Summary
----------------
Total number of tapes:     4
Total pools:               2
Total size of tapes:       16 GiB
Total space used by tapes: 14.9 GiB
Average Compression:       59.5x
```

Restaurar datos que se encuentran en la nube

Cuando un cliente solicita datos para realizar una restauración desde el servidor de aplicaciones de respaldo, la aplicación de respaldo debe generar una alerta o un mensaje que solicite los volúmenes requeridos de la unidad de nube.

El volumen debe recuperarse de la nube e ingresarse en la biblioteca VTL de Data Domain antes de que se deba notificar a la aplicación de respaldo de la presencia de los volúmenes.

Nota

Verifique que la aplicación de respaldo reconozca los cambios de estado de los volúmenes transferidos al almacenamiento en la nube. Complete los pasos necesarios para que la aplicación de respaldo actualice su inventario a fin de reflejar el estado más reciente del volumen.

Recuperación manual de un volumen de cinta del almacenamiento de nube

Recupere una cinta de DD Cloud Tier al vault de VTL local.

Procedimiento

1. Seleccione **Protocols** > **DD VTL**.
2. Expanda la lista de pools y seleccione el pool que está configurado para migrar cintas a DD Cloud Tier.
3. En el panel Pool, haga clic en la pestaña **Tape**.
4. Seleccione una o más cintas que estén ubicadas en una unidad de nube.
5. Haga clic en **Recall Cloud Tapes** para recuperar cintas de DD Cloud Tier.

Resultados

Después de la siguiente migración de datos programada, las cintas se recuperan desde la unidad de nube en el vault. Las cintas se pueden restituir a una librería desde el vault.

Equivalente de la CLI

Procedimiento

1. Identifique el volumen necesario para restaurar los datos.
2. Recupere el volumen de la cinta de la vault.

   Ejecute el siguiente comando:
   ```
   vtl tape recall start barcode T00001L3 count 1 pool cloud-vtl-pool
   ```
3. Verificar la operación de recuperación iniciada.

   Ejecute el siguiente comando:
   ```
   data-movement status
   ```
4. Verifique que la operación de recuperación se haya realizado correctamente.

   Ejecute el siguiente comando:
   ```
   vtl tape show all barcode T00001L3
   ```

```
Processing tapes....
Barcode    Pool             Location           State    Size           Used (%)
Comp   Modification Time
--------   --------------   ----------------   -----   -----   ----------------
----   -------------------
T00001L3   cloud-vtl-pool   cloud-vtl slot 1   RW      5 GiB   5.0 GiB (99.07%)
239x   2017/05/05 10:41:41
--------   --------------   ----------------   -----   -----   ----------------
----   -------------------
(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next
data-movement run.
(R) Recall operation is in progress for the tape.

VTL Tape Summary
----------------
Total number of tapes:     1
Total pools:               1
Total size of tapes:       5 GiB
Total space used by tapes: 5.0 GiB
Average Compression:       239.1x
```

5. Valide la ubicación del archivo.

   Ejecute el siguiente comando:
   ```
   filesys report generate file-location path /data/col1/cloud-vtl-pool
   ```

```
filesys report generate file-location path /data/col1/cloud-vtl-pool
--------------------------------      --------------------------
File Name                             Location(Unit Name)
--------------------------------      --------------------------
/data/col1/cloud-vtl-pool/.vtl_pool     Active
/data/col1/cloud-vtl-pool/.vtc/T00001L3 Active
-----------------------------------------------------------------
```

6. Importe la cinta recuperada a DD VTL.

   Ejecute el siguiente comando:
   ```
   vtl import cloud-vtl barcode T00001L3 count 1 pool cloud-vtl-pool element slot
   ```

```
imported 1 tape(s)...sysadmin@ddbeta70# vtl tape show cloud-vtlProcessing tapes.....
```

7. Compruebe el volumen en el inventario de la aplicación de respaldo.
8. Restaurar los datos con la aplicación de respaldo.
9. Cuando se complete la restauración, compruebe el volumen de la cinta en el inventario de la aplicación de respaldo.
10. Exporte el volumen de cinta de Data Domain VTL al vault de Data Domain.
11. Vuelva a mover la cinta hacia la unidad de nube.

Trabajo con grupos de acceso

Los *grupos de acceso* tienen una colección de WWPN (nombres de puertos mundiales) de iniciadores o alias, y las unidades y los cambiadores que requieren para acceder. Un grupo predeterminado de DD VTL denominado *TapeServer* le permite agregar dispositivos que serán compatibles con las aplicaciones de respaldo basadas en el protocolo NDMP (Network Data Management Protocol).

La configuración de grupos de acceso permite que los iniciadores (por lo general, aplicaciones de respaldo) lean y escriban datos en dispositivos del mismo grupo de acceso.

Los grupos de acceso permiten que los clientes obtengan acceso solo a LUN seleccionados (cambiadores de medios o unidades de cinta virtuales) en un sistema. Una configuración de cliente para un grupo de acceso solo puede acceder a los dispositivos en su grupo.

Evite realizar cambios en el grupo de acceso en un sistema DD durante trabajos de respaldo o restauración activos. Un cambio puede hacer que un trabajo activo falle. El impacto de los cambios durante trabajos activos depende de una combinación de configuraciones de software de respaldo y host.

Al seleccionar **Access Groups** > **Groups**, se muestra la siguiente información para todos los grupos de acceso.

Tabla 162 Información del grupo de acceso

Elemento	Descripción
Group Name	Nombre del grupo
Initiators	Cantidad de iniciadores en el grupo
Dispositivos	Cantidad de dispositivos en el grupo

Si selecciona **View All Access Groups**, se lo dirige a la vista Fibre Channel.

Desde el menú More Tasks, puede crear o eliminar un grupo.

Creación de un grupo de acceso

Los grupos de acceso administran el acceso entre dispositivos e iniciadores. No utilice el grupo de acceso predeterminado TapeServer a menos que esté utilizando NDMP.

Procedimiento

1. Seleccione **Access Groups** > **Groups**.
2. Seleccione **More Tasks** > **Group** > **Create**
3. En el cuadro de diálogo Create Access Group, ingrese un nombre de 1 a 128 caracteres y seleccione **Next.**
4. Agregue dispositivos y seleccione **Next.**

5. Revise el resumen y seleccione **Finish** o **Back**, según corresponda.

   Equivalente de la CLI

   ```
   # vtl group create My_Group
   ```

Agregar un dispositivo de grupo de acceso

La configuración de grupos de acceso permite que los iniciadores (por lo general, aplicaciones de respaldo) lean y escriban datos en dispositivos del mismo grupo de acceso.

Procedimiento

1. Seleccione **Access Groups** > **Groups**. Puede seleccionar un *grupo* específico.
2. Seleccione **More Tasks** > **Group** > **Create** o **Group** > **Configure**.
3. En el cuadro de diálogo Create or Modify Access Group, ingrese o modifique el campo **Group Name** si lo desea. (Este campo es obligatorio).
4. Para configurar los iniciadores de un grupo de acceso, seleccione la casilla junto al iniciador. Puede agregar iniciadores a un grupo en otro momento.
5. Seleccione **Next**.
6. Si se muestra Devices, seleccione Add (**+**) para que se muestre el cuadro de diálogo Add Devices.
   a. Verifique que la biblioteca correcta se seleccione de la lista desplegable Library Name o seleccione otra.
   b. En el área Device, seleccione las casillas de verificación de los dispositivos (cambiador y unidades) que se deben incluir en el grupo.
   c. De manera opcional, especifique el LUN de inicio en el cuadro de texto LUN Start Address.

      Este es el LUN que el sistema DD devuelve al iniciador. Cada dispositivo se identifica exclusivamente por la biblioteca y el nombre de dispositivo. (Por ejemplo, es posible tener la unidad 1 en la biblioteca 1 y la unidad 1 en la biblioteca 2). Por lo tanto, un LUN se asocia con un dispositivo, que se identifica con su biblioteca y nombre de dispositivo.

      Al presentar los LUN por medio de puertos de FC en HBA/tarjeta SLIC, los puertos se pueden designar como primarios, secundarios o ninguno. Un puerto principal para un conjunto de LUN es el puerto que actualmente publica esos LUN en un fabric. Un puerto secundario es un puerto que difundirá un conjunto de LUN en caso de falla de la ruta principal (esto requiere la intervención manual). La configuración none se utiliza en caso de que no desee publicar los LUN seleccionados. La presentación de LUN depende de la topología de SAN en cuestión.

      Los iniciadores en el grupo de acceso interactúan con los dispositivos LUN que se agregan al grupo.

      El LUN máximo aceptado al crear un grupo de acceso es 16383.

      Un LUN se puede usar solo una vez para un grupo individual. El mismo LUN se puede usar con diversos grupos.

      Algunos iniciadores (clientes) tienen reglas específicas para la numeración de LUN de destino, por ejemplo, requisito de LUN 0 o requisito de LUN contiguos. Si estas reglas no se cumplen, es posible que un iniciador no pueda acceder a algunos LUN asignados a un puerto de destino de DD VTL o a ninguno de ellos.

Consulte las reglas especiales en la documentación de iniciadores y, si es necesario, cambie los LUN del dispositivo en el puerto objetivo de DD VTL para cumplir con las reglas. Por ejemplo, si el iniciador requiere que un LUN 0 se asigne al puerto objetivo de DD VTL, verifique los LUN para dispositivos asignados a los puertos y, si no se asignó ningún dispositivo a un LUN 0, cambie el LUN de un dispositivo de modo que se asigne a un LUN 0.

d. En el área Primary and Secondary Endpoints, seleccione una opción para determinar desde qué puertos se ve el dispositivo seleccionado. Las siguientes condiciones se aplican a los puertos designados:

- all: El dispositivo seleccionado se ve desde todos los puertos.
- none: El dispositivo seleccionado no se ve desde ningún puerto.
- select: El dispositivo seleccionado se ve desde determinados puertos. Seleccione las casillas de verificación de los puertos correspondientes. Si solo se seleccionan puertos principales, el dispositivo seleccionado podrá verse solo desde puertos principales.

  Si solo se seleccionan puertos secundarios, el dispositivo seleccionado podrá verse solo desde puertos secundarios. Los puertos secundarios se pueden usar si los puertos primarios no están disponibles.

El cambio a un puerto secundario no es una operación automática. Debe cambiar manualmente el dispositivo DD VTL a los puertos secundarios si los puertos principales no están disponibles.

La lista de puertos es una lista de números de puertos físicos. Un número de puerto define el slot de PCI, y la letra define el puerto en una tarjeta PCI. Los ejemplos son 1a, 1b o 2a, 2b.

Una unidad aparece con el mismo LUN en todos los puertos que haya configurado.

e. Seleccione **OK**.

Se lo dirige nuevamente al cuadro de diálogo Devices donde se muestra el nuevo grupo. Para agregar más dispositivos, repita estos cinco pasos secundarios.

7. Seleccione **Next**.
8. Seleccione **Close** cuando se muestre el mensaje de estado `Completed`.

Equivalente de la CLI

```
# vtl group add VTL_Group vtl NewVTL changer lun 0 primary-port all secondary-port all# vtl group add VTL_Group vtl NewVTL drive 1 lun 1 primary-port all secondary-port all# vtl group add SetUp_Test vtl SetUp_Test drive 3 lun 3 primary-port endpoint-fc-0 secondary-port endpoint-fc-1

# vtl group show Setup_Test
Group: SetUp_Test

Initiators:
Initiator Alias   Initiator WWPN
---------------   ----------------------
tsm6_p23          21:00:00:24:ff:31:ce:f8
---------------   ----------------------

Devices:
Device Name          LUN   Primary Ports   Secondary Ports    In-use Ports
------------------   ---   -------------   ---------------   -------------
SetUp_Test changer     0             all               all             all
SetUp_Test drive 1     1             all               all             all
```

```
SetUp_Test drive 2     2              5a                5b              5a
SetUp_Test drive 3     3   endpoint-fc-0     endpoint-fc-1   endpoint-fc-0
------------------   ---   -------------   ---------------   -------------
```

Modificación o eliminación a un dispositivo de grupo de acceso

Es posible que necesite modificar o eliminar un dispositivo de un grupo de acceso.

Procedimiento

1. Seleccione **Protocols** > **VTL** > **Access Groups** > **Groups***> grupo*.
2. Seleccione **More Tasks** > **Group** > **Configure**.
3. En el cuadro de diálogo Modify Access Group, ingrese o modifique el campo **Group Name**. (Este campo es obligatorio).
4. Para configurar los iniciadores de un grupo de acceso, seleccione la casilla junto al iniciador. Puede agregar iniciadores a un grupo en otro momento.
5. Seleccione **Next**.
6. Seleccione un dispositivo, y seleccione el ícono de edición (lápiz) para que se muestre el cuadro de diálogo Modify Initiator. Luego, siga los pasos A a E. Si simplemente desea eliminar el dispositivo, seleccione el ícono de eliminación (X) y pase al paso E.
   a. Verifique que la biblioteca correcta se seleccione de la lista desplegable Library o seleccione otra.
   b. En el área Devices to Modify, seleccione las casillas de verificación de los dispositivos que se deben modificar (cambiador y unidades).
   c. Opcionalmente, modifique el LUN de inicio (número de unidad lógica) en la casilla LUN Start Address.

      Este es el LUN que el sistema DD devuelve al iniciador. Cada dispositivo se identifica exclusivamente por la biblioteca y el nombre de dispositivo. (Por ejemplo, es posible tener la unidad 1 en la biblioteca 1 y la unidad 1 en la biblioteca 2). Por lo tanto, un LUN se asocia con un dispositivo, que se identifica con su biblioteca y nombre de dispositivo.

      Los iniciadores en el grupo de acceso interactúan con los dispositivos LUN que se agregan al grupo.

      El LUN máximo aceptado al crear un grupo de acceso es 16383.

      Un LUN se puede usar solo una vez para un grupo individual. El mismo LUN se puede usar con diversos grupos.

      Algunos iniciadores (clientes) tienen reglas específicas para la numeración de LUN de destino, por ejemplo, requisito de LUN 0 o requisito de LUN contiguos. Si estas reglas no se cumplen, es posible que un iniciador no pueda acceder a algunos LUN asignados a un puerto de destino de DD VTL o a ninguno de ellos.

      Consulte las reglas especiales en la documentación de iniciadores y, si es necesario, cambie los LUN del dispositivo en el puerto objetivo de DD VTL para cumplir con las reglas. Por ejemplo, si el iniciador requiere que un LUN 0 se asigne al puerto objetivo de DD VTL, verifique los LUN para dispositivos asignados a los puertos y, si no se asignó ningún dispositivo a un LUN 0, cambie el LUN de un dispositivo de modo que se asigne a un LUN 0.

   d. En el área Primary and Secondary Ports, cambie la opción que determina los puertos desde los cuales se ve el dispositivo seleccionado. Las siguientes condiciones se aplican a los puertos designados:

- all: El dispositivo seleccionado se ve desde todos los puertos.
- none: El dispositivo seleccionado no se ve desde ningún puerto.
- select: El dispositivo seleccionado se ve desde determinados puertos. Seleccione las casillas de verificación de los puertos desde los cuales se verá.
  Si solo se seleccionan puertos principales, el dispositivo seleccionado podrá verse solo desde puertos principales.

  Si solo se seleccionan puertos secundarios, el dispositivo seleccionado podrá verse solo desde puertos secundarios. Los puertos secundarios se pueden usar si los puertos primarios no están disponibles.

El cambio a un puerto secundario no es una operación automática. Debe cambiar manualmente el dispositivo DD VTL a los puertos secundarios si los puertos principales no están disponibles.

La lista de puertos es una lista de números de puertos físicos. Un número de puerto define el slot de PCI, y la letra define el puerto en una tarjeta PCI. Los ejemplos son 1a, 1b o 2a, 2b.

Una unidad aparece con el mismo LUN en todos los puertos que haya configurado.

e. Seleccione **OK**.

Eliminación del grupo de acceso

Antes de poder eliminar un grupo de acceso, debe quitar todos sus iniciadores y LUN.

Procedimiento

1. Quite todos los iniciadores y LUN del grupo.
2. Seleccione **Access Groups** > **Groups**.
3. Seleccione **More Tasks** > **Group** > **Delete**.
4. En el cuadro de diálogo Delete Group, seleccione la casilla de verificación del grupo que se debe eliminar y seleccione **Next**.
5. En el cuadro de diálogo Groups confirmation, verifique la eliminación y seleccione **Submit**.
6. Seleccione **Close** cuando el estado Delete Groups se muestre como `Completed`.

Equivalente de la CLI

```
# scsitarget group destroy My_Group
```

Trabajo con un grupo de acceso seleccionado

Al seleccionar **Access Groups** > **Groups** > *grupo*, se muestra la siguiente información para un grupo de acceso seleccionado.

Tabla 163 Pestaña LUN

Elemento	Descripción
LUN	Dirección del dispositivo: el número máximo es 16383. Un LUN se puede usar solo una vez dentro de un grupo, pero se puede volver a usar dentro de otro. Los dispositivos DD VTL agregados a un grupo deben ser LUN contiguos.
Library	Nombre de la biblioteca asociada con el LUN
Dispositivo	Cargadores y unidades
Terminales en uso	Conjunto de terminales que actualmente están en uso: primario o secundario.
Terminales principales	Puntos final inicial (o predeterminado) utilizado por la aplicación de respaldo En caso de falla en este terminal, se pueden usar los terminales secundarios, si están disponibles.
Punto finales secundarios	Conjunto de punto finales de conmutación por error para usar si falla el terminal primario

Tabla 164 Pestaña Iniciators

Elemento	Descripción
Nombre	Nombre del iniciador, que es el WWPN o el alias asignado al iniciador
WWPN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del puerto Fibre Channel

Desde el menú More Tasks, con un grupo seleccionado, puede configurar ese grupo o establecer los terminales en uso.

Selección de extremos para un dispositivo

Debido a que los extremos conectan un dispositivo a un iniciador, use este proceso para configurar los extremos antes de conectar el dispositivo.

Procedimiento

1. Seleccione **Access Groups** > **Groups**> *group*.
2. Seleccione **More Tasks** > **Endpoints** > **Set In-Use**.
3. En el cuadro de diálogo para establecer extremos en uso, seleccione solo dispositivos específicos o seleccione **Devices** para seleccionar todos los dispositivos en la lista.
4. Indique si los extremos son principales o secundarios.
5. Seleccione **OK**.

Configuración del grupo TapeServer en dispositivos con NDMP

El grupo TapeServer de DD VTL consta de unidades de cintas que comparten interfaz con aplicaciones de respaldo basadas en el protocolo NDMP (Network Data Management Protocol) y que envían información de control y flujos de datos por

medio de IP (Internet Protocol) en vez de Fibre Channel (FC). Un dispositivo usado por NDMP TapeServer debe estar en TapeServer del grupo DD VTL, disponible *solo* para NDMP TapeServer.

Procedimiento

1. Agregue unidades de cintas a una biblioteca nueva o existente (en este ejemplo, denominada “dd990-16”).
2. Cree slots y CAP para la biblioteca.
3. Agregue los dispositivos creados en una biblioteca (en este ejemplo, “dd990-16”) al grupo de acceso TapeServer.
4. Habilite el demonio NDMP ingresando en la línea de comandos:

```
# ndmpd enable
Starting NDMP daemon, please wait.............
NDMP daemon is enabled.
```

5. Asegúrese de que el demonio de NDMP vea los dispositivos en el grupo TapeServer:

```
# ndmpd show devicenames
NDMP Device          Virtual Name       Vendor   Product       Serial Number
-----------------    ----------------   ------   -----------   -------------
/dev/dd_ch_c0t0l0    dd990-16 changer   STK      L180          6290820000
/dev/dd_st_c0t1l0    dd990-16 drive 1   IBM      ULTRIUM-TD3   6290820001
/dev/dd_st_c0t2l0    dd990-16 drive 2   IBM      ULTRIUM-TD3   6290820002
/dev/dd_st_c0t3l0    dd990-16 drive 3   IBM      ULTRIUM-TD3   6290820003
/dev/dd_st_c0t4l0    dd990-16 drive 4   IBM      ULTRIUM-TD3   6290820004
-----------------    ----------------   ------   -----------   -------------
```

6. Agregue un usuario de NDMP (ndmp en este ejemplo) con el siguiente comando:

```
# ndmpd user add ndmp
Enter password:
Verify password:
```

7. Verifique que el usuario ndmp se agregue correctamente:

```
# ndmpd user show
ndmp
```

8. Mostrar la configuración de NDMP:

```
# ndmpd option show all
Name              Value
--------------    --------
authentication    text
debug             disabled
port              10000
preferred-ip
--------------    --------
```

9. Cambie la autenticación de contraseñas de usuario predeterminada para usar el cifrado MD5 para la seguridad mejorada y verifique el cambio (vea si el valor de autenticación cambió de texto a md5):

```
# ndmpd option set authentication md5# ndmpd option show all
Name              Value
--------------    --------
authentication    md5
debug             disabled
port              10000
preferred-ip
--------------    --------
```

Resultados

NDMP ahora está configurado, y el grupo de acceso TapeServer muestra la configuración del dispositivo. Consulte el capítulo `ndmpd` de la *Guía de referencia de*

comandos de Data Domain Operating System para acceder al conjunto completo de comandos y opciones.

Trabajo con recursos

Al seleccionar **Resources** > **Resources**, se muestra información acerca de los iniciadores y los terminales. Un*iniciador* es un cliente de respaldo que se conecta a un sistema para leer y escribir datos usando el protocolo Fibre Channel (FC). Un iniciador específico puede admitir DD Boost mediante FC o DD VTL, pero no ambos. Un *terminal* es el destino lógico en un sistema DD al cual se conecta el iniciador.

Tabla 165 Pestaña Iniciators

Elemento	Descripción
Nombre	Nombre del iniciador, que es el WWPN o el alias asignado al iniciador
WWPN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del puerto Fibre Channel (FC)
WWNN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del nodo FC
Terminales en línea	Nombre del grupo en el que los puertos se ven según el iniciador Se muestra `None` o `Offline` si el iniciador no está disponible.

Tabla 166 Pestaña Endpoints

Elemento	Descripción
Nombre	Nombre específico del terminal
WWPN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del puerto Fibre Channel (FC)
WWNN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del nodo FC
Dirección del sistema	Dirección del sistema para el terminal.
Activado	Estado operacional del puerto HBA, que es `Yes` (habilitado) o `No` (deshabilitado).
Status	Estado del vínculo de DD VTL, que es `Online` (capaz de controlar el tráfico) u `Offline`.

Configuración de recursos

Al seleccionar **Configure Resources**, el sistema lo dirige al área Fibre Channel, donde puede configurar los terminales y los iniciadores.

Trabajo con iniciadores

Al seleccionar **Resources** > **Resources** > **Initiators**, se muestra información acerca de los iniciadores. Un *iniciador* es el WWPN (nombre de puerto mundial) del HBA (adaptador de bus del host) de FC (Fibre Channel) del sistema del cliente con el cual el sistema DD comparte interfaces. Un*nombre de iniciador* es un alias para el WWPN del cliente, para facilitar el uso.

Mientras que un cliente se asigna como un iniciador, pero antes de que un grupo de acceso se haya agregado, el cliente no puede acceder a ningún dato en un sistema DD.

Después de agregar un grupo de acceso para el iniciador o cliente, el cliente puede acceder solo a los dispositivos en ese grupo de acceso. Un cliente puede tener grupos de acceso para diversos dispositivos.

Un grupo de acceso puede contener múltiples iniciadores, pero un iniciador puede existir solo en un grupo de acceso.

Nota

Se puede configurar un máximo de 1024 iniciadores para un sistema DD.

Tabla 167 Información del iniciador

Elemento	Descripción
Nombre	Nombre del iniciador
Group	Grupo asociado con el iniciador
Terminales en línea	Terminales vistos por el iniciador Se muestra `none` o `offline` si el iniciador no está disponible.
WWPN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del puerto Fibre Channel (FC)
WWNN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del nodo FC
Vendor Name	Nombre del proveedor por iniciador

Al seleccionar **Configure Initiators**, el sistema lo dirige al área Fibre Channel, donde puede configurar los terminales y los iniciadores.

Equivalente de la CLI

```
# vtl initiator show
Initiator  Group      Status  WWNN                    WWPN                    Port
---------  ---------  ------  ----------------------  ----------------------  ----
tsm6_p1    tsm3500_a  Online  20:00:00:24:ff:31:ce:f8  21:00:00:24:ff:31:ce:f8 10b
---------  ---------  ------  ----------------------  ----------------------  ----

Initiator  Symbolic Port Name                          Address Method
---------  ------------------------------------------  --------------
tsm6_p1    QLE2562 FW:v5.06.03 DVR:v8.03.07.15.05.09-k  auto
---------  ------------------------------------------  --------------
```

Trabajo con terminales

Al seleccionar **Resources** > **Resources** > **Endpoints**, se proporciona información acerca del hardware y la conectividad de los terminales.

Tabla 168 Pestaña Hardware

Elemento	Descripción
System Address	Dirección del sistema del terminal.
WWPN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del puerto Fibre Channel (FC)
WWNN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del nodo FC
Enabled	Estado operacional del puerto HBA, que es `Yes` (habilitado) o `No` (deshabilitado).
NPIV	Estado de NPIV de este terminal: Enabled o Disabled.
Link Status	Estado del vínculo de este terminal: Online u Offline.
Operation Status	Estado operacional de este terminal: Normal o Marginal.
# of Endpoints	Cantidad de terminales asociados con este terminal.

Tabla 169 Pestaña Endpoints

Elemento	Descripción
Name	Nombre específico del terminal
WWPN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del puerto Fibre Channel (FC)
WWNN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del nodo FC
System Address	Dirección del sistema del terminal.
Enabled	Estado operacional del puerto HBA, que es `Yes` (habilitado) o `No` (deshabilitado).
Link Status	Estado del vínculo de este terminal: Online u Offline.

Configuración de terminales

Si selecciona **Configure Endpoints**, el sistema lo dirige al área Fibre Channel, donde puede cambiar cualquiera de los datos anteriores para el terminal.

Equivalente de la CLI

```
# scsitarget endpoint show list
Endpoint       System Address  Transport     Enabled  Status
```

```
--------       --------------  ---------     -------  ------
endpoint-fc-0  5a              FibreChannel  Yes      Online
endpoint-fc-1  5b              FibreChannel  Yes      Online
```

Trabajo con un punto final seleccionado

Al seleccionar **Resources** > **Resources** > **Endpoints** > *endpoint*, se proporciona información acerca del hardware, la conectividad y las estadísticas del punto final.

Tabla 170 Pestaña Hardware

Elemento	Descripción
Dirección del sistema	Dirección del sistema del punto final.
WWPN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del puerto Fibre Channel
WWNN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del nodo FC
Activado	Estado operacional del puerto HBA, que es `Yes` (habilitado) o `No` (deshabilitado).
NPIV	Estado de NPIV de este punto final: Enabled o Disabled.
Link Status	Estado del vínculo de este punto final: Online u Offline.
Operation Status	Estado operacional de este punto final: Normal o Marginal.
# of Endpoints	Cantidad de puntos finales asociados con este punto final.

Tabla 171 Pestaña Summary

Elemento	Descripción
Nombre	Nombre específico del punto final
WWPN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del puerto Fibre Channel
WWNN	Nombre de puerto mundial único, que es un identificador de 64 bits (un valor de 60 bits precedido por un identificador *Network Address Authority* de 4 bits) del nodo FC
Dirección del sistema	Dirección del sistema del punto final.
Activado	Estado operacional del puerto HBA, que es `Yes` (habilitado) o `No` (deshabilitado).
Link Status	Estado del vínculo de este punto final: Online u Offline.

Tabla 172 Pestaña Statistics

Elemento	Descripción
Punto final	Nombre específico del punto final
Library	Nombre de la biblioteca que contiene el punto final
Dispositivo	Cantidad de dispositivos
Operaciones/s	Operaciones por segundo
KiB/s de lectura	Velocidad de lecturas en KiB por segundo
KiB/s de escritura	Velocidad de escrituras en KiB por segundo

Tabla 173 Pestaña Detailed Statistics

Elemento	Descripción
Punto final	Nombre específico del punto final
N.º de comandos de control	Número de comandos de control
N.º de comandos de lectura	Número de comandos de lectura
N.º de comandos de escritura	Número de comandos de escritura
Entrada (MiB)	Número de MiB escritos (el equivalente binario de MB)
Salida (MiB)	Número de MiB leídos
N.º de protocolo de error	Número de protocolos de error
N.º de falla de vinculación	Número de fallas de vinculación
N.º de Crc no válido	Número de CRC (comprobaciones de redundancia cíclica)
N.º de TxWord no válido	Número de palabras de tx (transmisión) no validas
N.º de LIP	Número de LIP (primitivas de inicialización de loop)
N:º de señal perdida	Número de señales o conexiones que se han perdido
N.º de sincronizaciones perdidas	Número de señales o conexiones que han perdido sincronización

Trabajo con pools

Al seleccionar **Pools** > **Pools**, se muestra información detallada del pool predeterminado y otros pools existentes. Un *pool* es un conjunto de cintas que se asigna a un directorio en el sistema de archivos. Los pools se usan para replicar cintas en un destino. Puede convertir pools basados en directorios en pools basados en MTrees para aprovechar las funciones adicionales de los MTrees.

Tenga en cuenta lo siguiente acerca de los pools:

- Los pools pueden ser de dos tipos: MTree (recomendado) o de directorio, que es compatible con versiones anteriores.
- Un pool se puede replicar sin importar dónde están ubicadas las cintas individuales. Las cintas pueden estar en el vault o en una biblioteca (slot, cap o unidad).
- Puede copiar y mover cintas de un pool a otro.

- El software de respaldo no puede acceder a los pools.
- No se requieren licencias ni configuración de DD VTL en un destino de replicación cuando se replican pools.
- Debe crear cintas con códigos de barra únicos. Los códigos de barra duplicados pueden causar comportamiento impredecible en aplicaciones de respaldo y pueden ser confusos para los usuarios.
- Dos cintas en dos pools diferentes de un sistema DD pueden tener el mismo nombre y, en este caso, ninguna cinta se puede mover al pool de la otra. De igual manera, un pool enviado a un destino de replicación debe tener un nombre que sea único en el destino.

Tabla 174 Pestaña Pools

Elemento	Descripción
Name	El nombre del pool.
Type	Si es un pool de MTree o de directorio.
Status	El estado del pool.
Tape Count	El número de cintas en el pool.
Size	La capacidad total configurada de cintas en el pool, en GiB (Gibibytes base-2 equivalente de GB, Gigabytes).
Physical Used	La cantidad de espacio total utilizada en cintas virtuales en el pool.
Compression	La cantidad de compresión promedio lograda para los datos en las cintas del pool.
Cloud Unit	El nombre de la unidad de nube donde el pool de DD VTL migra los datos.
Cloud Data Movement Policy	La política de movimiento de datos que rige la migración de datos de DD VTL al almacenamiento de DD Cloud Tier.

Tabla 175 Pestaña Replication

Elemento	Descripción
Name	El nombre del pool.
Configured	Si la replicación está configurada para este pool: yes o no.
Remote Source	Contiene una entrada solo si el pool está replicado desde otro sistema DD.
Remote Destination	Contiene una entrada solo si el pool se replica a otro sistema DD.

Desde el menú More Tasks, puede crear y eliminar pools, así como buscar cintas.

Creación de pools

Puede crear pools compatibles con versiones anteriores, si es necesario para la configuración, por ejemplo, para replicación con un sistema anterior al SO DD 5.2.

Procedimiento

1. Seleccione **Pools** > **Pools**.
2. Seleccione **More Tasks** > **Pool** > **Create**.
3. En el cuadro de diálogo Create Pool, especifique un nombre para el pool, teniendo en cuenta lo siguiente:
   - no puede ser “all,”“vault” ni “summary”;
   - no puede tener un espacio o un punto al principio ni al final;
   - distingue entre mayúsculas y minúsculas.
4. Si desea crear un pool de directorio (que sea compatible con la versión anterior de DD System Manager), seleccione la opción “Create a directory backwards compatibility mode pool. ” No obstante, tenga en cuenta que las ventajas de usar un pool MTree incluyen capacidades para hacer lo siguiente:
   - realizar snapshots individuales y snapshots de calendario;
   - aplicar bloqueos de retención;
   - configurar una política de retención individual;
   - obtener información de compresión;
   - obtener políticas de migración de datos al nivel de la retención;
   - establecer una política de uso de espacio de almacenamiento (soporte de cuotas) al configurar límites estrictos y límites flexibles.
5. Seleccione **OK** para mostrar el cuadro de diálogo Create Pool Status.
6. Cuando aparezca `Completed` en el cuadro de diálogo Create Pool Status, seleccione **Close**. El pool se agregará al subárbol Pools y ahora podrá agregar cintas virtuales en este.

Equivalente de la CLI

```
# vtl pool add VTL_Pool
A VTL pool named VTL_Pool is added.
```

Eliminación de pools

Antes de que se pueda eliminar un pool, debe haber eliminado todas las cintas contenidas en este. Si la replicación está configurada para el pool, también se debe eliminar el par de replicación. La eliminación de un pool se corresponde con el cambio de nombre del MTree y su posterior eliminación, lo que ocurre en el siguiente proceso de limpieza.

Procedimiento

1. Seleccione **Pools** > **Pools** > ***pool***.
2. Seleccione **More Tasks** > **Pool** > **Delete**.
3. En el cuadro de diálogo Delete Pools, seleccione la casilla de verificación de los elementos que desea eliminar:
   - El nombre de cada pool,
   - o bien, **Pool Names**, para eliminar todos los pools.
4. Seleccione **Submit** en los cuadros de diálogo de confirmación.

5. Cuando `Completed` aparezca en el cuadro de diálogo Delete Pool Status, seleccione **Close**.

   El pool se eliminará del subárbol Pools.

Trabajo con un pool seleccionado

Virtual Tape Libraries > **VTL Service** > **Vault** > *pool* y **Pools** > **Pools** > *pool* muestran información detallada de un pool. Tenga en cuenta que el pool "Default" siempre existe.

Pestaña Pool

Tabla 176 Resumen

Elemento	Descripción
Convert to MTree Pool	Seleccione este botón para convertir un pool de directorio en un pool de MTree.
Type	Si es un pool de MTree o de directorio.
Tape Count	El número de cintas en el pool.
Capacity	La capacidad total configurada de cintas en el pool, en GiB (Gibibytes, equivalente de base 2 de GB, Gigabytes).
Logical Used	La cantidad de espacio total utilizada en cintas virtuales en el pool.
Compression	La cantidad de compresión promedio lograda para los datos en las cintas del pool.

Tabla 177 Pestaña Pool: Transferencia de datos de nube: distribución de protección

Elemento	Descripción
Pool type (%)	Nube y pool de VTL (si corresponde), con el porcentaje actual de los datos entre paréntesis.
Name	Nombre del pool de VTL local o el proveedor de nube.
Logical Used	La cantidad de espacio total utilizada en cintas virtuales en el pool.
Tape Count	El número de cintas en el pool.

Tabla 178 Pestaña Pool: Transferencia de datos de nube: política de transferencia de datos de nube

Elemento	Descripción
Policy	Antigüedad de las cintas en días o selección manual.
Older Than	Umbral de antigüedad para una política de transferencia de datos basados en la antigüedad.
Cloud Unit	Unidad de nube de destino.

Pestaña Tape

Tabla 179 Controles de cintas

Elemento	Descripción
Create	Cree una nueva cinta.
Delete	Elimine las cintas seleccionadas.
Copy	Haga una copia de una cinta.
Move between Pool	Transfiera las cintas seleccionadas a un pool diferente.
Select for Cloud Move[a]	Programe las cintas seleccionadas para la migración a DD Cloud Tier.
Unselect from Cloud Move[a]	Elimine las cintas seleccionadas del programa para la migración a DD Cloud Tier.
Recall Cloud Tapes	Recupere las cintas seleccionadas desde DD Cloud Tier.
Move to Cloud Now	Migre las cintas seleccionadas a DD Cloud Tier sin tener que esperar a la siguiente migración programada.

a. Esta opción solo está disponible si la política de movimiento de datos está configurada para la selección manual.

Tabla 180 Información de cintas

Elemento	Descripción
Barcode	Código de barras de cintas.
Size	Tamaño máximo de la cinta.
Physical Used	Capacidad de almacenamiento físico utilizada por la cinta.
Compression	Tasa de compresión en la cinta.
Location	Ubicación de la cinta.
Modification Time	Momento en que se modificó la cinta por última vez.
Recall Time	Última vez que se recuperó la cinta.

Pestaña Replication

Tabla 181 Replicación

Elemento	Descripción
Name	El nombre del pool.
Configured	Si la replicación está configurada para este pool: yes o no.
Remote Source	Contiene una entrada solo si el pool está replicado desde otro sistema DD.
Remote Destination	Contiene una entrada solo si el pool se replica a otro sistema DD.

You can also select the **Replication Detail** button, at the top right, to go directly to the Replication information panel for the selected pool.

En el área Virtual Tape Libraries o Pools, en el menú More Tasks, puede crear, eliminar, mover, copiar o buscar una cinta en el pool.

En el área Pools, en el menú More Tasks, puede eliminar un pool o cambiarle el nombre.

Conversión de un pool de directorio en un pool MTree

Los pools MTree tienen muchas ventajas con respecto a los pools de directorio. Para obtener más información, consulte la sección *Creación de pools*.

Procedimiento

1. Asegúrese de que se hayan cumplido los siguientes requisitos previos:
   - Los pools de origen y de destino deben estar sincronizados, de modo que el número de cintas y los datos de cada lado permanezcan intactos.
   - El pool de directorio no debe ser un origen o destino de replicación.
   - El sistema de archivos no debe estar lleno.
   - El sistema de archivos no debe haber alcanzado el número máximo de MTrees permitidos (100).
   - No debe haber un MTree existente con el mismo nombre.
   - Si el pool de directorio se está replicando en varios sistemas, esos sistemas de replicación deben ser conocidos para el sistema de administración.
   - Si el pool de directorio se está replicando en un sistema operativo DD anterior (por ejemplo, de DD OS 5.5 a DD OS 5.4), no se puede convertir. Solución alternativa:
     - Replique el pool de directorio en un segundo sistema DD.
     - Replique el pool de directorio del segundo sistema DD en un tercer sistema DD.
     - Elimine los sistemas DD segundo y tercero de la red de Data Domain del sistema DD de administración.
     - En cualquiera de los sistemas que ejecutan DD OS 5.5, en el submenú Pools, seleccione **Pools** y un pool de directorio. En la pestaña Pools, seleccione **Convert to MTree Pool**.
2. Con el pool de directorio que desea convertir resaltado, elija **Convert to MTree Pool**.
3. Seleccione **OK** en el cuadro de diálogo Convert to MTree Pool.
4. Tenga en cuenta que la conversión afecta la replicación de las siguientes formas:
   - DD VTL se deshabilita temporalmente en los sistemas replicados durante la conversión.
   - Los datos de destino se copian en un pool nuevo en el sistema de destino para conservar los datos hasta que se inicie y sincronice la nueva replicación. Después, puede eliminar de forma segura el pool copiado temporalmente; este se denomina **CONVERTED-***pool*, donde *pool* es el nombre del pool que se actualizó (o los primeros 18 caracteres para nombres de pool extensos). [Esto corresponde únicamente a DD OS 5.4.1.0 y versiones posteriores].
   - El directorio de replicación de destino se convertirá a formato MTree. [Esto corresponde únicamente a DD OS 5.2 y versiones posteriores].

- Los pares de replicación se dividen antes de la conversión del pool y se vuelven a establecer después si no se producen errores.
- DD Retention Lock no se puede habilitar en sistemas involucrados en la conversión de pools MTree.

Transferencia de cintas entre pools

Si residen en la vault, las cintas se pueden mover entre los pools para admitir actividades de replicación. Por ejemplo, los pools son necesarios si todas las cintas se crearon en el pool predeterminado, pero después necesita grupos independientes para replicar grupos de cintas. Puede crear pools con nombre y reorganizar los grupos de cintas en pools nuevos.

Nota

No puede mover las cintas de un pool de cintas que sea un origen de replicación de directorios. Como solución alternativa, puede hacer lo siguiente:

- Copie la cinta en un pool nuevo y, a continuación, elimine la cinta del pool antiguo.
- Use un pool de MTree, que le permite mover cintas de un pool de cintas que sea un origen de replicación de directorios.

Procedimiento

1. Con un pool resaltado, seleccione **More Tasks** > **Tapes** > **Move**.

   Tenga en cuenta que cuando se inicia desde el pool, el panel Tapes permite que las cintas se transfieran únicamente entre pools.

2. En el cuadro de diálogo Move Tapes, especifique la información para buscar las cintas que desea mover y seleccione **Search**:

   Tabla 182 Cuadro de diálogo Move Tapes

Campo	Entrada del usuario
Ubicación	La ubicación no se puede modificar.
Pool	Seleccione el nombre del pool donde residen las cintas. Si no se han creado pools, use el pool Default.
Barcode	Especifique un código de barras único o deje el (*) predeterminado para importar un grupo de cintas. El código de barras permite los caracteres comodín ? y *, donde ? coincide con cualquier carácter único y * coincide con 0 o más caracteres.
Conteo	Especifique el número máximo de cintas que desea que se devuelvan. Si deja este campo en blanco, se utilizará el código de barras predeterminado (*).
Tapes Per Page	Selecciona el número máximo de cintas para mostrar por página. Los valores posibles son 15, 30 y 45.
Items Selected	Muestra el número de cintas seleccionadas entre varias páginas, y se actualiza automáticamente con cada selección de cintas.

3. En la lista de resultados de la búsqueda, seleccione las cintas que desee mover.

4. En Select Destination: En la lista Location, seleccione la ubicación del pool al que se moverán las cintas. Esta opción está disponible únicamente cuando se inicia desde la vista Pool (mencionada).
5. Seleccione **Next**.
6. En la visita Move Tapes, verifique la información de resumen y la lista de cintas, y seleccione **Submit**.
7. Seleccione **Close** en la ventana de estado.

Copiado de cintas entre pools

Las cintas se pueden copiar entre los pools, o del vault a un pool, para admitir actividades de replicación. Esta opción está disponible únicamente cuando se inicia desde la vista Pool (mencionada).

Procedimiento

1. Con un pool resaltado, seleccione **More Tasks** > **Tapes** > **Copy**.
2. En el cuadro de diálogo Copy Tapes Between Pools, seleccione las casillas de verificación de las cintas que desea copiar o ingrese información para buscar las cintas que desea copiar y seleccione **Search**:

Tabla 183 Cuadro de diálogo Copy Tapes Between Pools

Campo	Entrada del usuario
Ubicación	Seleccione una biblioteca o el **Vault** para ubicar la cinta. Aunque las cintas siempre se muestran en un pool (en el menú Pools), técnicamente están en una biblioteca o en el vault, pero no en ambos, y nunca están en dos bibliotecas al mismo tiempo. Use las opciones de importación y exportación para mover las cintas entre el vault y una biblioteca.
Pool	Para copiar cintas entre los pools, seleccione el nombre del pool donde residen actualmente las cintas. Si no se han creado pools, use el pool **Default**.
Barcode	Especifique un código de barras único o deje el (*) predeterminado para importar un grupo de cintas. El código de barras permite los caracteres comodín ? y *, donde ? coincide con cualquier carácter único y * coincide con 0 o más caracteres.
Conteo	Especifique el número máximo de cintas que desea que se importen. Si deja este campo en blanco, se utilizará el código de barras predeterminado (*).
Tapes Per Page	Selecciona el número máximo de cintas para mostrar por página. Los valores posibles son 15, 30 y 45.
Items Selected	Muestra el número de cintas seleccionadas entre varias páginas, y se actualiza automáticamente con cada selección de cintas.

3. En la lista de resultados de la búsqueda, seleccione las cintas que desee copiar.
4. En Select Destination: Pool list, seleccione el pool donde se copiarán las cintas. Si hay una cinta con un código de barras que coincida en el pool de destino, se mostrará un error y se anulará la copia.
5. Seleccione **Next**.
6. En el cuadro de diálogo Copy Tapes Between Pools, verifique la información de resumen y la lista de cintas, y seleccione **Submit**.
7. Seleccione **Close** en la ventana Copy Tapes Between Pools Status.

Cambio de nombres de pools

El nombre de un pool se puede cambiar solo si ninguna de sus cintas está en una biblioteca.

Procedimiento

1. Seleccione **Pools** > **Pools** > ***pool***.
2. Seleccione **More Tasks** > **Pool** > **Rename**.
3. En el cuadro de diálogo Rename Pool, especifique el nombre nuevo del pool, con la advertencia de que este nombre:
   - no puede ser “all,”“vault” ni “summary”;
   - no puede tener un espacio o un punto al principio ni al final;
   - distingue entre mayúsculas y minúsculas.
4. Seleccione **OK** para mostrar el cuadro de diálogo de estado Rename Pool.
5. Después de que el cuadro de diálogo de estado Rename Pool muestre `Completed`, seleccione **OK**.

   Se cambiará el nombre del pool en el subárbol Pools en las áreas Pools y Virtual Tape Libraries.

CAPÍTULO 16

DD Replicator

Este capítulo incluye:

- Descripción general de VNX Replicator 446
- Requisitos previos para la configuración de replicaciones 447
- Compatibilidad de versiones de replicación 450
- Tipos de replicación 454
- Uso de DD Encryption con DD Replicator 460
- Topologías de replicación 461
- Administración de la replicación 466
- Monitoreo de la replicación 482
- Replicación con HA 484
- Replicación de un sistema con cuotas a uno sin ellas 484
- Replication Scaling Context 485
- Migración de replicación de directorio a MTree 485
- Uso de la replicación de recopilaciones para la recuperación ante desastres con SMT 490

Descripción general de VNX Replicator

Data Domain Replicator (DD Replicator) ofrece replicación cifrada automatizada, basada en políticas y eficiente en la red para DR (recuperación ante desastres) y consolidación de respaldo y archivo de múltiples sitios. DD Replicator replica de manera asíncrona únicamente los datos comprimidos y duplicados a través de una WAN (red de área amplia).

DD Replicator realiza dos niveles de deduplicación para reducir de forma significativa los requisitos de ancho de banda: deduplicación *local* y *entre sitios*. La deduplicación local determina los segmentos únicos que se replicarán a través de una WAN. La deduplicación entre sitios reduce aún más los requisitos de ancho de banda cuando se replican varios sitios a un mismo sistema de destino. Con la deduplicación entre sitios, no se vuelve a replicar ningún segmento redundante que haya sido transferido anteriormente por cualquier otro sitio o como resultado de un respaldo o archivo local. Esto mejora la eficiencia de la red entre todos los sitios y reduce los requisitos diarios de ancho de banda de red hasta en un 99 %, lo que hace que la replicación basada en la red sea rápida, confiable y rentable.

Para satisfacer una amplia variedad de requisitos de recuperación ante desastres, DD Replicator ofrece topologías de replicación flexibles, como espejeado de sistemas completos, bidireccional, de muchos a uno, de uno a muchos y en cascada. Además, puede elegir replicar todos los datos o un subconjunto de los datos en el sistema DD. Para lograr el máximo nivel de seguridad, DD Replicator puede cifrar los datos que se replican entre sistemas DD mediante el protocolo estándar de capa de conexión segura (SSL).

DD Replicator escala el rendimiento y los índices de consolidación compatibles para admitir grandes ambientes empresariales.

Antes de comenzar con DD Replicator, tenga en cuenta los siguientes requisitos generales:

- DD Replicator es un producto con licencia. Consulte a su representante de ventas de Data Domain para comprar licencias.
- Por lo general, puede replicar datos solamente entre las máquinas que tienen una separación de dos versiones entre sí, por ejemplo, de 5.6 a 6.0. Sin embargo, es posible que haya excepciones a esta regla (debido a una numeración atípica de las versiones), por lo tanto, revise las tablas de la sección *Compatibilidad de versiones de replicación* o consulte con su representante de Data Domain.
- Si no puede administrar y monitorear DD Replicator desde la versión actual de DD System Manager, use los comandos `replication` que se describen en la *Guía de referencia de comandos de Data Domain Operating System*.

Requisitos previos para la configuración de replicaciones

Antes de configurar una replicación, revise los siguientes requisitos previos para minimizar el tiempo de transferencia de datos inicial, evitar la sobrescritura de datos, etc.

- **Contexts**: determine el número máximo de contextos para sus sistemas DD revisando los números de flujos de replicación en la siguiente tabla.

  Tabla 184 Flujos de datos enviados a un sistema Data Domain

Modelo	RAM/NVRAM	Flujos de escritura de respaldo	Flujos de lectura de respaldo	Flujos de origen de replicación[a]	Flujos de destino[a] de replicación	Mixto
DD140, DD160, DD610	4 GB o 6 GB/0.5 GB	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20
DD620, DD630, DD640	8 GB/0.5 GB o 1 GB	20	16	20	20	w<=20; r<=16; ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; Total<=30
DD640, DD670	16 GB o 20 GB/1 GB	90	30	60	90	w<=90; r<=30; ReplSrc<=60; ReplDest<=90; ReplDest+w<=90; Total<=90
DD670, DD860	36 GB/1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD860	72 GB[b] / 1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD890	96 GB/2 GB	180	50	90	180	w<=180; r<=50; ReplSrc <=90;ReplDest<=180; ReplDest +w<=180; Total<=180
DD990	128 o 256 GB[b] / 4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD2200	8 GB	20	16	16	20	w<=20; r<=16; ReplSrc<=16; ReplDest<=20; ReplDest+w<=20; Total<=20
DD2200	16 GB	60	16	30	60	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest+w<=60; Total<=60
DD2500	32 o 64 GB/2 GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD4200	128 GB[b] / 4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270

Tabla 184 Flujos de datos enviados a un sistema Data Domain (continuación)

Modelo	RAM/NVRAM	Flujos de escritura de respaldo	Flujos de lectura de respaldo	Flujos de origen de replicación [a]	Flujos de destino[a] de replicación	Mixto
DD4500	192 GB[b] / 4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD7200	128 o 256 GB[b] / 4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD9500	256/512 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD9800	256/768 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD6300	De 48 a 96 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD6800	192 GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest +w<=400; Total<=400
DD9300	De 192 a 384 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest +w<=800; Total<=800
DD VE (8 TB)	8 GB / 512 MB	20	16	20	20	w<= 20 ; r<= 16 ReplSrc<=20; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=20;Total<=20
DD VE (16 TB)	16 GB / 512 MB o 24 GB / 1 GB	45	30	45	45	w<= 45 ; r<= 30 ReplSrc<=45; ReplDest<=45; ReplDest+w<=45; w+r+ReplSrc <=45;Total<=45
DD VE (32 TB)	24 GB/1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE (48 TB)	36 GB/1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE (64 TB)	48 GB/1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE (96 TB)	64 GB/2 GB	180	50	90	180	w<= 180 ; r<= 50 ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; w+r+ReplSrc <=180;Total<=180

Tabla 184 Flujos de datos enviados a un sistema Data Domain (continuación)

Modelo	RAM/NVRAM	Flujos de escritura de respaldo	Flujos de lectura de respaldo	Flujos de origen de replicación [a]	Flujos de destino[a] de replicación	Mixto
DD3300 (4 TB)	12 GB (memoria virtual) / 512 MB	20	16	30	20	w<= 20 ; r<= 16 ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=30;Total<=30
DD3300 (8 TB)	32 GB (memoria virtual) / 1536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 (16 TB)	32 GB (memoria virtual) / 1536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 (32 TB)	46 GB (memoria virtual) / 1536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=140

a. DirRepl, OptDup, MTreeRepl
b. La opción de software Data Domain Extended Retention está disponible solo para estos dispositivos con memoria extendida (máxima)

- **Compatibility**: si está usando sistemas DD que ejecutan diferentes versiones de DD OS, revise la siguiente sección sobre compatibilidad de versiones de replicación.
- **Initial Replication**: si el origen tiene muchos datos, la operación de replicación inicial puede llevar muchas horas. Considere la posibilidad de colocar los dos sistemas DD en la misma ubicación con un vínculo de alta velocidad y baja latencia. Después de la primera replicación, puede mover los sistemas a sus ubicaciones deseadas, porque solo se enviarán los datos nuevos.
- **Bandwidth Delay Settings**: tanto el origen como el destino deben tener la misma configuración de retraso de ancho de banda. Este ajuste controla el rendimiento de la replicación de beneficio en vínculos de latencia más alta al controlar el tamaño de búfer de TCP (protocolo de control de transmisión). A continuación, el sistema de origen puede enviar suficientes datos al destino mientras espera el reconocimiento.
- **Only One Context for Directories/Subdirectories**: un directorio (y sus subdirectorios) puede estar en un solo contexto a la vez, por lo que debe asegurarse de que un subdirectorio de un directorio de origen no se use en otro contexto de replicación de directorios.
- **Adequate Storage**: como mínimo, el destino debe tener *la misma cantidad de espacio* que el origen.
- **Destination Empty for Directory Replication**: el directorio de destino debe estar vacío para la replicación de directorios; de lo contrario, su contenido ya no será necesario, porque se sobrescribirá.
- **Security**: DD OS requiere que el puerto 3009 esté abierto a fin de configurar la replicación segura mediante una conexión Ethernet.

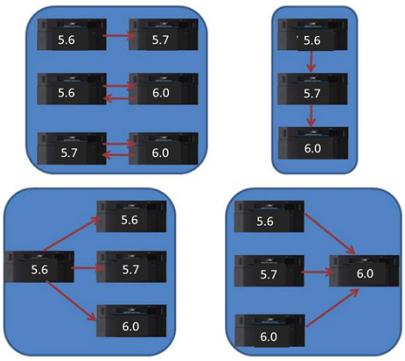
Compatibilidad de versiones de replicación

Para usar sistemas DD que ejecutan diferentes versiones de DD OS para un origen o destino, las siguientes tablas proporcionan información de compatibilidad para replicación de un solo nodo, de DD Extended Retention, de DD Retention Lock, de MTrees, de directorios, de recopilaciones, delta (optimización del ancho de banda bajo) y en cascada.

En general:

- Para DD Boost u OST, consulte "Compatibilidad de versiones de duplicación optimizadas" en la *Guía de administración de Data Domain Boost para integración de partners* o en la *Guía de administración de Data Domain Boost para OpenStorage* para conocer las configuraciones compatibles.
- La replicación de MTree y de directorios no se pueden usar simultáneamente para replicar los mismos datos.
- El procedimiento de recuperación es válido para todas las configuraciones de replicación compatibles.
- La migración de archivos se admite cuando se admite la replicación de recopilaciones.
- No se admite la replicación de MTrees entre un sistema DD de origen que ejecuta DD OS 5.2.x y un sistema DD de destino que ejecuta DD OS 5.4.x o 5.5.x cuando DD Retention Lock Governance está habilitado en el MTree de origen.
- Para la replicación de MTrees de un sistema DD de origen que ejecuta DD OS 6.0 a un sistema DD de destino que ejecuta una versión anterior de DD OS, el proceso de replicación se comporta de acuerdo con la versión anterior de DD OS en el sistema DD de destino. Si se realiza una replicación en cascada o de la operación de restauración desde el sistema DD de destino, no se aplican respaldos sintéticos virtuales.
- Para las configuraciones en cascada, el número máximo de saltos es dos, es decir, tres sistemas DD.
  La migración de directorio a MTree admite la compatibilidad con versiones anteriores de hasta dos versiones anteriores. Consulte Migración de replicación de directorio a MTree en la página 485 para obtener más información acerca de la migración de directorio a Mtree.
- La replicación de uno a muchos, de muchos a uno y en cascada admite hasta tres familias de versiones de DD OS consecutivas, como se indica en estas figuras.

Figura 17 Configuraciones de replicación válidas



En estas tablas:

- Cada versión de DD OS incluye todas las versiones de esa familia, por ejemplo, DD OS 5.7 incluye 5.7.1, 5.7.x, 6.0, etc.
- c = replicación de recopilaciones
- dir = replicación de directorios
- m = replicación de MTree
- del = replicación delta (optimización del ancho de banda bajo)
- dest = destino
- src = origen
- N/C = no corresponde

Tabla 185 Configuración: de un solo nodo a un solo nodo

origen / destino	5.0 (dest)	5.1 (dest)	5.2 (dest)	5.3 (dest)	5.4 (dest)	5.5 (dest)	5.6 (dest)	5.7 (dest)	6.0 (dest)	6.1 (dest)	6.2 (dest)
5.0 (src)	c, dir, del	dir, del	dir, del	N/C	N/C	N/C	N/C	N/C	N/C	N/C	N/C
5.1 (src)	dir, del	c, dir, del, m[a]	dir, del, m[a]	dir, del, m[a]	dir, del, m[a]	N/C	N/C	N/C	N/C	N/C	N/C
5.2 (src)	dir, del	dir, del, m[a]	c, dir, del, m[b]	dir, del, m	dir, del, m	dir, del, m	N/C	N/C	N/C	N/C	N/C
5.3 (src)	N/C	dir, del, m[a]	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m	N/C	N/C	N/C	N/C	N/C
5.4 (src)	N/C	dir, del, m[a]	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m	N/C	N/C	N/C	N/C
5.5 (src)	N/C	N/C	dir, del, m	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m	N/C	N/C	N/C
5.6 (src)	N/C	N/C	N/C	N/C	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m	N/C	N/C
5.7 (src)	N/C	N/C	N/C	N/C	N/C	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m	N/C
6.0 (src)	N/C	N/C	N/C	N/C	N/C	N/C	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m
6.1 (src)	N/C	N/C	N/C	N/C	N/C	N/C	N/C	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m
6.2 (src)	N/C	N/C	N/C	N/C	N/C	N/C	N/C	N/C	dir, del, m	dir, del, m	c, dir, del, m

a. La replicación de MTrees no se admite para DD VTL.
b. La replicación de recopilaciones se admite solo para datos de cumplimiento

Tabla 186 Configuración: DD Extended Retention a DD Extended Retention

origen / destino	5.0 (dest)	5.1 (dest)	5.2 (dest)	5.3 (dest)	5.4 (dest)	5.5 (dest)	5.6 (dest)	5.7 (dest)	6.0 (dest)	6.1 (dest)	6.2 (dest)
5.0 (src)	c	N/C	N/C	N/C	N/C	N/C	N/C	N/C	N/C	N/C	N/C
5.1 (src)	N/C	c	m[a]	m[b]	m[b]	N/C	N/C	N/C	N/C	N/C	N/C
5.2 (src)	N/C	m[a]	c, m[a]	m[a]	m[a]	m[a]	N/C	N/C	N/C	N/C	N/C
5.3 (src)	N/C	m[c]	m[c]	c, m	m	m	N/C	N/C	N/C		N/C

Tabla 186 Configuración: DD Extended Retention a DD Extended Retention (continuación)

origen / destino	5.0 (dest)	5.1 (dest)	5.2 (dest)	5.3 (dest)	5.4 (dest)	5.5 (dest)	5.6 (dest)	5.7 (dest)	6.0 (dest)	6.1 (dest)	6.2 (dest)
5.4 (src)	N/C	m[c]	m[c]	m	c, m	m	m	N/C	N/C	N/C	N/C
5.5 (src)	N/C	N/C	m[c]	m	m	c, m	m	m	N/C	N/C	N/C
5.6 (src)	N/C	N/C	N/C	N/C	m	m	c, m	m	m		N/C
5.7 (src)	N/C	N/C	N/C	N/C	N/C	m	m	c, m	m	m	N/C
6.0 (src)	N/C	N/C	N/C	N/C	N/C	N/C	m	m	c, m	m	m
6.1 (src)	N/C	N/C	N/C	N/C	N/C	N/C	N/C	m	m	c, m	m
6.2 (src)	N/C	N/C	N/C	N/C	N/C	N/C	N/C	N/C	m	m	c, m

a. La migración de archivos no se admite con replicación de MTree en el origen o en el destino en esta configuración.
b. La migración de archivos no se admite con replicación de MTree en el origen en esta configuración.
c. La migración de archivos no se admite con replicación de MTree en el destino en esta configuración.

Tabla 187 Configuración: de un solo nodo a DD Extended Retention

origen / destino	5.0 (dest)	5.1 (dest)	5.2 (dest)	5.3 (dest)	5.4 (dest)	5.5 (dest)	5.6 (dest)	5.7 (dest)	6.0 (dest)	6.1 (dest)	6.2 (dest)
5.0 (src)	dir	dir	N/C	N/C	N/C	N/C	N/C	N/C	N/C	N/C	N/C
5.1 (src)	dir	dir, m[a]	dir, m[a]	dir, m	dir, m	N/C	N/C	N/C	N/C	N/C	N/C
5.2 (src)	dir	dir, m[a]	dir, m[a]	dir, m	dir, m	dir, m	N/C	N/C	N/C	N/C	N/C
5.3 (src)	N/C	dir, m[a]	dir, m[a]	dir, m	dir, m	dir, m	N/C	N/C	N/C	N/C	N/C
5.4 (src)	N/C	dir, m[a]	dir, m[a]	dir, m	dir, m	dir, m	dir, m	N/C	N/C	N/C	N/C
5.5 (src)	N/C	N/C	dir, m[a]	dir, m	dir, m	dir, m	dir, m	dir, m	N/C	N/C	N/C
5.6 (src)	N/C	N/C	N/C	N/C	dir, m	dir, m	dir, m	dir, m	dir, m	N/C	N/C
5.7 (src)	N/C	N/C	N/C	N/C	N/C	dir, m	dir, m	dir, m	dir, m	dir, m	N/C
6.0 (src)	N/C	N/C	N/C	N/C	N/C	N/C	dir, m	dir, m	dir, m	dir, m	dir, m
6.1 (src)	N/C	N/C	N/C	N/C	N/C	N/C	N/C	dir, m	dir, m	dir, m	dir, m
6.2 (src)	N/C	N/C	N/C	N/C	N/C	N/C	N/C	N/C	dir, m	dir, m	dir, m

a. La migración de archivos no se admite para esta configuración.

Tipos de replicación

La replicación consta comúnmente de un sistema DD de *origen* (que recibe datos desde un sistema de respaldo) y uno o más sistemas DD de *destino*. Cada sistema DD puede ser el origen o el destino de contextos de replicación. Durante la replicación, cada sistema DD puede ejecutar operaciones normales de respaldo y restauración.

Cada tipo de replicación establece un *contexto* asociado con un directorio o MTree existente en el origen. El contexto replicado se crea en el destino cuando se establece un contexto. El contexto establece un par de replicación, que siempre está activo, y todos los datos que llegan al origen se copian en el destino cuanto antes. Las rutas configuradas en contextos de replicación son referencias absolutas y no cambian en función del sistema en el que están configuradas.

Un sistema Data Domain se puede configurar para replicación de recopilaciones, MTrees o directorios.

- La *replicación de directorios* proporciona replicación en el nivel de directorios individuales.

- La *replicación de recopilaciones* duplica toda el área de almacenamiento de datos en el origen y la transfiere al destino, y el volumen replicado es de solo lectura.
- La *replicación de MTrees* replica todos los MTrees (es decir, una estructura de archivos virtuales que permite administración avanzada). Los pools de medios también se pueden replicar y, de forma predeterminada (a partir del SO DD 5.3), se crea un MTree que se replicará. (También se puede crear un pool de medios en modo de compatibilidad con versiones anteriores que, cuando se replique, sea un contexto de replicación de directorios).

Para todos los tipos de replicación, tenga en cuenta los siguientes requisitos:

- Un sistema Data Domain de destino debe tener capacidad de almacenamiento disponible de, al menos, el tamaño del tamaño máximo previsto del directorio de origen. Asegúrese de que el sistema Data Domain de destino tenga suficiente ancho de banda de red y espacio en disco para manejar todo el tráfico de orígenes de replicación.
- El sistema de archivos debe estar habilitado o, según el tipo de replicación, se habilitará como parte de la inicialización de la replicación.
- El origen debe existir.
- El destino no debe existir.
- El destino se creará cuando se genere e inicialice un contexto.
- Una vez inicializada la replicación, la propiedad y los permisos del destino son siempre idénticos a los del origen.
- En las opciones del comando de replicación, el destino siempre identifica un par de replicación específico.
- Ambos sistemas deben tener una ruta activa visible a través de la red IP para que cada sistema pueda resolver el nombre de host de su partner.

La selección del tipo de replicación depende de sus necesidades específicas. En las siguientes secciones se proporcionan descripciones y funciones de estos tres tipos, además de una breve introducción a la replicación administrada de archivos que usa DD Boost.

Replicación administrada de archivos

La *replicación administrada de archivos* que usa DD Boost es un tipo de replicación que se administra y controla con software de respaldo.

Con la replicación administrada de archivos, las imágenes de respaldo se transfieren directamente de un sistema DD a otro, de a una por vez, ante la solicitud del software de respaldo.

El software de respaldo rastrea todas las copias, lo que permite un monitoreo sencillo del estado de replicación y la recuperación de varias copias.

La replicación de archivos administrada ofrece topologías de replicación flexibles que incluyen el espejeado del sistema completo, bidireccional, muchos a uno, uno a muchos y en cascada, lo que permite la deduplicación eficiente entre sitios.

Aquí se incluyen algunos puntos adicionales para tener en cuenta acerca de la replicación de archivos administrada:

- No necesitan configurarse contextos de replicación.
- Las políticas de ciclo de vida controlan la replicación de información sin intervención del usuario.
- DD Boost generará y eliminará contextos según sea necesario sobre la marcha.

Para obtener más información, consulte los comandos `ddboost file-replication` en la *Guía de referencia de comandos de Data Domain Operating System*.

Replicación de directorios

La *replicación de directorios* transfiere datos deduplicados dentro de un directorio del sistema de archivos DD configurado como un origen de replicación a un directorio configurado como un destino de replicación en otro sistema.

Con la replicación de directorios, un sistema DD puede ser, simultáneamente, el origen de algunos contextos de replicación y el destino de otros. El sistema DD también puede recibir datos de las aplicaciones de respaldo y archivo mientras está replicando datos.

La replicación de directorios tiene los mismos efectos de deduplicación entre sitios y topologías de implementación de red flexibles que la replicación administrada de archivos (el tipo que usa DD Boost).

Aquí se incluyen algunos puntos adicionales para tener en cuenta cuando se usa la replicación de directorios:

- No combine datos de CIFS y NFS dentro del mismo directorio. Un solo sistema DD de destino puede recibir respaldos de clientes CIFS y clientes NFS, mientras se usen directorios por separado para cada uno.
- Un directorio puede estar solo en un contexto a la vez. Un directorio principal no se puede usar en un contexto de replicación si un directorio secundario de este ya se está replicando.
- El cambio de nombre (la transferencia) de archivos o cintas *dentro o fuera* de un directorio de origen de replicación de directorios *no* está permitido. El cambio de nombres de archivos o cintas *dentro* de un directorio de origen de replicación de directorios *sí* está permitido.
- Un sistema DD de destino debe tener capacidad de almacenamiento disponible de, al menos, el tamaño posterior a la compresión del tamaño máximo previsto posterior a la compresión del directorio de origen.
- Cuando se inicia la replicación, se crea automáticamente un directorio de destino.
- Una vez inicializada la replicación, la propiedad y los permisos del directorio de destino son siempre idénticos a los del directorio de origen. Siempre que exista el contexto, el directorio de destino se conserva en estado de solo lectura y puede recibir datos solamente del directorio de origen.
- En cualquier momento, debido a diferencias en la compresión global, el tamaño del directorio de origen y de destino puede diferir.

Recomendaciones sobre la creación de carpetas

La replicación de directorios replica datos al nivel de los subdirectorios individuales en `/data/col1/backup`.

Para proporcionar una separación granular de los datos, debe crear, desde un sistema de host, otros directorios (DirA, DirB, etc.) dentro del Mtree /backup. Cada directorio debe basarse en su ambiente y el deseo de replicar esos directorios en otra ubicación. No replicará todo el MTree /backup, sino que configurará los contextos de replicación en cada subdirectorio en /data/col1/backup/ (p. ej. /data/col1/backup/DirC). El objetivo de estas tres razones:

- Permite el control de las ubicaciones de destino, ya que DirA iría a un sitio y DirB iría a otro.

- Este nivel de granularidad permite la administración, el monitoreo y el aislamiento de fallas. Cada contexto de replicación se puede pausar, detener, destruir o informar.
- El rendimiento se limita a un solo contexto. La creación de varios contextos puede mejorar el rendimiento de replicación adicional.
- Como recomendación general, se pueden requerir aproximadamente 5 a 10 contextos para distribuir la replicación entre varios flujos de replicación. Esto se debe validar con el diseño del sitio y el volumen y la composición de los datos en la ubicación.

Nota

La recomendación de un número de contextos es un tema que depende del diseño y, en algunos casos, hay implicancias significativas relacionadas con las selecciones realizadas acerca de segregar los datos con el fin de optimizar la replicación. Los datos generalmente se optimizan de la manera en la que quedarán inactivos, no de la manera en la que se replicarán. Tenga esto en cuenta al alterar un ambiente de respaldo.

Replicación de MTree

La *replicación de MTree* se usa para replicar MTrees entre sistemas DD. Se crean instantáneas periódicos en el origen y las diferencias entre ellos se transfieren al destino aprovechando el mismo mecanismo de deduplicación entre sites que se usa para la replicación de directorios. Esto garantiza que los datos del destino siempre sean una copia en un punto en el tiempo del origen, con coherencia de archivos. Esto también reduce la replicación de renovaciones en los datos, lo que genera un uso más eficiente de la WAN.

Aunque la replicación de directorios debe replicar cada cambio en el contenido del directorio de origen en orden, el uso de instantáneas en la replicación de MTree permite omitir algunos cambios intermedios en el origen. Omitir estos cambios reduce aún más la cantidad de datos que se envían a través de la red y, por lo tanto, reduce el retardo de la replicación.

Con la replicación de MTree, un sistema DD puede ser, simultáneamente, el origen de algunos contextos de replicación y el destino de otros. El sistema DD también puede recibir datos de las aplicaciones de respaldo y archivo mientras está replicando datos.

La replicación de MTree tiene los mismos efectos de deduplicación entre sites y topologías de implementación de red flexibles que la replicación administrada de archivos (el tipo que usa DD Boost).

Aquí se incluyen algunos puntos adicionales para tener en cuenta cuando se usa la replicación de MTree:

- Cuando se inicia la replicación, se crea automáticamente un MTree de destino de solo lectura.
- Los datos se pueden segregar de forma lógica en varios MTrees para promover un mejor rendimiento de la replicación.
- Se deben crear instantáneas en los contextos de origen.
- No se pueden crear instantáneas en un destino de replicación.
- Las instantáneas se replican con una retención fija de un año; sin embargo, la retención se puede y se debe ajustar en el destino.
- Los contextos de replicación se deben configurar tanto en el origen como en el destino.

- Replicar cartuchos de cintas (o pools) DD VTL significa simplemente replicar MTrees o directorios que contienen cartuchos de cintas DD VTL. Los pools de medios se replican en la replicación de MTree de forma predeterminada. Se puede crear un pool de medios en modo de compatibilidad con versiones anteriores y, a continuación, se puede replicar a través de la replicación basada en directorios. No puede usar la sintaxis pool:// para crear contextos de replicación a través de la línea de comandos. Al especificar la replicación basada en pools en DD System Manager, se creará la replicación de directorios o MTrees en función del tipo de pool de medios.
- No se permite replicar directorios en un MTree.
- Un sistema DD de destino debe tener capacidad de almacenamiento disponible de, al menos, el tamaño posterior a la compresión del tamaño máximo previsto posterior a la compresión del MTree de origen.
- Una vez inicializada la replicación, la propiedad y los permisos del MTree de destino son siempre idénticos a los del MTree de origen. Si el contexto está configurado, el MTree de destino se conserva en estado de solo lectura y puede recibir datos solamente del MTree de origen.
- En cualquier momento, debido a diferencias en la compresión global, el tamaño del MTree de origen y de destino puede diferir.
- Se admite replicación de MTree de sistemas DD Extended Retention a sistemas que no sean DD Extended Retention si ambos están ejecutando DD OS 5.5 o versiones posteriores.
- De forma predeterminada, se admite DD Retention Lock Compliance con la replicación de MTree. Si hay licencias de DD Retention Lock en un origen, el destino también debe tener una licencia de DD Retention Lock; de lo contrario, la replicación fallará. (Para que eso no ocurra, debe deshabilitar DD Retention Lock). Si DD Retention Lock está habilitado en un contexto de replicación, un contexto de destino replicado siempre contendrá datos con bloqueo de retención.

Detalles de replicación de MTree

La replicación de MTree implica los siguientes pasos:

1. Se crea una instantánea en el contexto de replicación de origen.
2. Esta instantánea se compara con la instantánea anterior más reciente.
3. Las diferencias entre las dos instantáneas se envían al contexto de replicación de destino.
4. En el destino, el MTree se actualiza, pero no se expone ningún archivo al usuario hasta que todos los cambios se reciben en el sistema de destino.

Estos pasos se repiten cada vez que se crea una instantánea en el MTree de origen. En las siguientes situaciones, se desencadena la creación de una instantánea en el sistema de origen:

- Instantánea periódica generada por el sistema (cuando el retardo de la replicación es superior a 15 minutos y no se replican instantáneas actualmente).
- Instantánea creada por el usuario (en un momento que especifica el usuario, como después de la finalización de un trabajo de respaldo).

Para ver ejemplos que muestran la interacción de diferentes tipos de instantáneas, consulte el artículo de la base de conocimientos *How MTree Replication Works*, disponible en https://support.emc.com/kb/180832.

Después de replicar la instantánea, se cierra la conexión con el destino. Cuando se replica la siguiente instantánea, se establece una nueva conexión entre el origen y el destino.

Automatic Multi-Streaming (AMS)
Automatic Multi-Streaming (AMS) mejora el rendimiento de replicación de MTree. Utiliza múltiples flujos para replicar un archivo grande único (32 GB o más) a fin de mejorar el uso de ancho de banda de red durante la replicación. Al aumentar la velocidad de replicación para archivos individuales, AMS también mejora la eficiencia de la canalización de la línea de espera de replicación y proporciona un rendimiento de replicación mejorado y un menor retraso de replicación.

AMS selecciona automáticamente la mejor opción para la carga de trabajo cuando esta presenta varias opciones de optimización. Por ejemplo, si la carga de trabajo es un archivo grande con atributos de copia rápida, la operación de replicación usa la optimización de copia rápida para evitar la sobrecarga de escanear el archivo para identificar segmentos únicos entre el par de replicación. Si la carga de trabajo utiliza respaldos sintéticos, la replicación utiliza la replicación sintética sobre AMS para aprovechar las operaciones locales en el sistema de destino para cada flujo de replicación a fin de generar el archivo.

AMS siempre está activado y no se puede desactivar.

Replicación de recopilaciones

La *replicación de recopilaciones* ejecuta el espejeado de todo el sistema en una topología de uno a uno y transfiere continuamente los cambios en la recopilación subyacente, incluidos todos los archivos y directorios lógicos del sistema de archivos de DD.

La replicación de recopilaciones no tiene la flexibilidad de los otros tipos, pero puede proporcionar un rendimiento más alto y admitir más objetos con menos sobrecarga, lo que puede funcionar mejor para casos empresariales de alta escala.

La replicación de recopilaciones replica toda el área `/data/col1` de un sistema DD de origen a un sistema DD de destino.

Nota

La replicación de recopilaciones no se admite en sistemas compatibles con nivel de nube.

Aquí se incluyen algunos puntos adicionales para tener en cuenta cuando se usa la replicación de recopilaciones:

- No es posible el control granular de replicaciones. Todos los datos se copian del origen al destino, lo que produce una copia de solo lectura.
- La replicación de recopilaciones requiere que la capacidad de almacenamiento del sistema de destino sea igual a la capacidad del almacenamiento de origen, o superior a ella. Si la capacidad del destino es inferior a la del origen, la capacidad disponible en el origen se reduce a la del destino.
- El sistema DD que se usará como destino de la replicación de recopilaciones debe estar vacío antes de la configuración de la replicación. Una vez que se configura la replicación, este sistema se dedica a recibir datos del sistema de origen.
- Con la replicación de recopilaciones, todas las cuentas y contraseñas de los usuarios se replican del origen al destino. Sin embargo, a partir del SO DD 5.5.1.0, otros elementos de configuración y opciones de configuración del usuario del sistema DD no se replican en el destino; debe reconfigurarlos explícitamente después de la recuperación.
- La replicación de recopilaciones es compatible con DD Secure Multitenancy (SMT). La información principal de SMT, que se encuentra en el espacio de

nombres del registro, incluidas las definiciones de grupo de usuarios y unidad de grupo de usuarios con UUID coincidentes, se transfiere automáticamente durante la operación de replicación. Sin embargo, la siguiente información de SMT no se incluye de manera automática para la replicación y debe configurarse manualmente en el sistema de destino:

- Listas de notificación de alerta para cada unidad de grupos de usuarios
- Todos los usuarios asignados al protocolo DD Boost que pueden utilizar los grupos de usuarios de SMT, si DD Boost está configurado en el sistema
- La unidad de grupo de usuarios predeterminada asociada con cada usuario de DD Boost, si corresponde, si DD Boost está configurado en el sistema

Uso de la replicación de recopilaciones para la recuperación ante desastres con SMT en la página 490 describe cómo configurar manualmente estos elementos en el destino de replicación.

- DD Retention Lock Compliance admite replicación de recopilaciones.
- La replicación de recopilaciones no se admite en sistemas compatibles con nivel de nube.
- Con la replicación de recopilaciones, no se pueden procesar datos que no se hayan replicado para la limpieza del sistema de archivos en un contexto de replicación en el sistema de origen. Si la limpieza del sistema de archivos no puede completarse debido a que los sistemas de origen y destino no están sincronizados, el sistema informa el estado de la operación de limpieza como `partial` y solo las estadísticas limitadas del sistema están disponibles para la operación de limpieza. Si la replicación de la recopilación está deshabilitada, la cantidad de datos que no se pueden procesar para la limpieza del sistema de archivos aumenta porque la fuente de replicación y los sistemas de destino permanecen sin sincronización. El artículo de la base de conocimientos *Data Domain: An overview of Data Domain File System (DDFS) clean/garbage collection (GC) phases*, disponible en el sitio de soporte en línea en https://support.emc.com, proporciona más información.
- Para mejorar el rendimiento en un ambiente de gran ancho de banda, ejecute el comando **`replication modify <destino> crepl-gc-gw-optim`** para desactivar la optimización de ancho de banda de replicación de recopilaciones.

Uso de DD Encryption con DD Replicator

DD Replicator se puede usar con la función *DD Encryption* opcional, que permite que los datos cifrados se repliquen con replicación de recopilaciones, MTrees o directorios.

Los contextos de replicación siempre se autentican con una *seña secreta compartida*. Esa seña secreta compartida se usa para establecer una clave de sesión con un protocolo de intercambio de claves Diffie-Hellman, y esa clave de sesión se usa para cifrar y descifrar la clave de cifrado del sistema Data Domain cuando corresponde.

Cada tipo de replicación funciona de manera exclusiva con cifrado y ofrece el mismo nivel de seguridad.

- La *replicación de recopilaciones* requiere que el origen y el destino tengan la misma configuración de cifrado, porque se espera que los datos de destino sean una réplica exacta de los datos de origen. En particular, la función de cifrado debe estar activada o desactivada tanto en el origen como en el destino y, si la función está activada, el algoritmo de cifrado y las contraseñas del sistema deben coincidir. Los parámetros se comprueban durante la fase de asociación de replicación. Durante la replicación de recopilaciones, el origen transmite los datos en forma cifrada y las claves de cifrado al destino. Los datos pueden recuperarse en el

destino porque el destino tiene la misma frase de contraseña y la misma clave de cifrado del sistema.

Nota

La replicación de recopilaciones no se admite en sistemas compatibles con nivel de nube.

- *La replicación de MTrees o directorios* no requiere que la configuración de cifrado sea la misma en el origen y en el destino. En lugar de esto, el origen y el destino intercambian de manera segura la clave de cifrado del destino durante la fase de asociación de replicación y los datos se vuelven a cifrar en el origen con la clave de cifrado del destino antes de la transmisión al destino.
  Si el destino tiene una configuración de cifrado diferente, los datos transmitidos se preparan según corresponda. Por ejemplo, si la función está desactivada en el destino, el origen descifra los datos y estos se envían al destino sin cifrar.
- En una topología de *replicación en cascada*, la réplica está encadenada entre tres o más sistemas Data Domain. El último sistema de la cadena puede configurarse para la replicación de recopilaciones, MTrees o directorios. Si el último sistema es un destino de replicación de recopilaciones, usa las mismas claves de cifrado y datos cifrados que el origen. Si el último sistema es un destino de replicación de MTrees o directorios, usa su propia clave y los datos se cifran en el origen. Se usa la clave de cifrado del destino en cada vínculo para el cifrado. El cifrado de los sistemas de la cadena funciona igual que en un par de replicación.

Topologías de replicación

DD Replicator admite cinco topologías de replicación (uno a uno, uno a muchos, muchos a uno, bidireccional y en cascada). Las tablas de esta sección muestran (1) cómo funcionan estas topologías con tres tipos de replicación (MTree, directorio y recopilación) y dos tipos de sistemas DD (un solo nodo [SN] y DD Extended Retention) y (2) cómo se admiten topologías combinadas con la replicación en cascada.

En general:

- Los sistemas de un solo nodo (SN) admiten todas las topologías de replicación.
- Se puede usar un solo nodo a un solo nodo (SN -> SN) para todos los tipos de replicación.
- Los sistemas DD Extended Retention no pueden ser el origen de una replicación de directorios.
- La replicación de recopilaciones no se puede configurar de un sistema de un solo nodo (SN) a un sistema habilitado para DD Extended Retention ni de un sistema habilitado para DD Extended Retention a un sistema SN.
- No se puede configurar la replicación de recopilaciones desde un sistema SN a un sistema DD con alta disponibilidad habilitada ni desde un sistema DD con alta disponibilidad habilitada a un sistema SN.
- Para la replicación de directorios y MTtrees, los sistemas DD de alta disponibilidad se tratan como sistemas SN.
- No se puede configurar la replicación de recopilaciones si alguno de los sistemas o ambos tienen habilitado Cloud Tier.

En esta tabla:

- SN = sistema DD de un solo nodo (sin DD Extended Retention)

- ER = sistema DD Extended Retention

Tabla 188 Compatibilidad de topología por tipo de replicación y tipo de sistema DD

Topologías	Replicación de MTree	Replicación de directorios	Replicación de recopilaciones
uno a uno	{SN | ER} -> {SN | ER} ER->SN [compatible a partir de la versión 5.5; antes de 5.5, es de recuperación únicamente]	SN -> SN SN -> ER	SN -> SN ER -> ER
uno a uno bidireccional	{SN | ER} -> {SN | ER}	SN -> SN	sin soporte
uno a muchos	{SN | ER} -> {SN | ER}	SN -> SN SN -> ER	sin soporte
muchos a uno	{SN | ER} -> {SN | ER}	SN -> SN SN -> ER	sin soporte
en cascada	{SN | ER } -> {SN | ER} -> {SN | ER}	SN -> SN -> SN SN -> SN -> ER	ER -> ER -> ER SN -> SN -> SN

La replicación en cascada admite topologías combinadas donde la segunda sección de una conexión en cascada es diferente del primer tipo en una conexión (por ejemplo, A -> B es replicación de directorios y B -> C es replicación de recopilaciones).

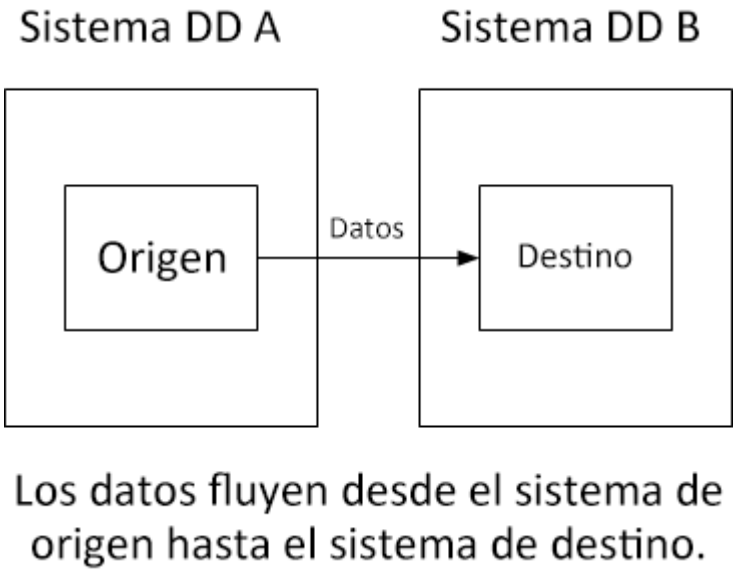
Tabla 189 Topologías combinadas compatibles con replicación en cascada

Topologías combinadas	
SN – Dir Repl -> ER – MTree Repl -> ER – MTree Repl	SN – Dir Repl -> ER – Col Repl -> ER – Col Repl
SN – MTree Repl -> SN – Col Repl -> SN – Col Repl	SN – MTree Repl -> ER – Col Repl -> ER – Col Repl

Replicación de uno a uno

El tipo de replicación más simple es de un sistema de origen DD a un sistema de destino DD, también conocido como un par de replicación *uno a uno*. Esta topología de replicación se puede configurar con tipos de replicación de directorios, MTree o recopilaciones.

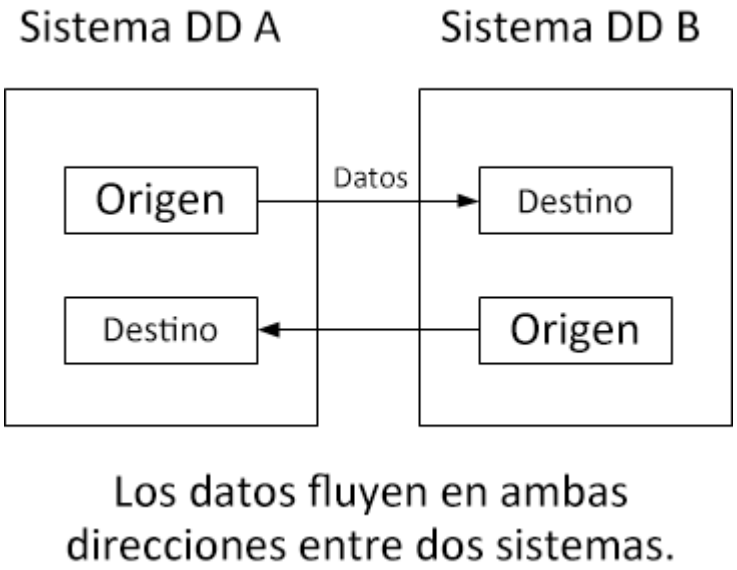
Figura 18 Par de replicación de uno a uno



Replicación bidireccional

En un par de replicación bidireccional, los datos de un directorio o MTree en el sistema DD A se replican en un sistema DD B y de otro directorio o MTree en el sistema DD B al sistema DD A.

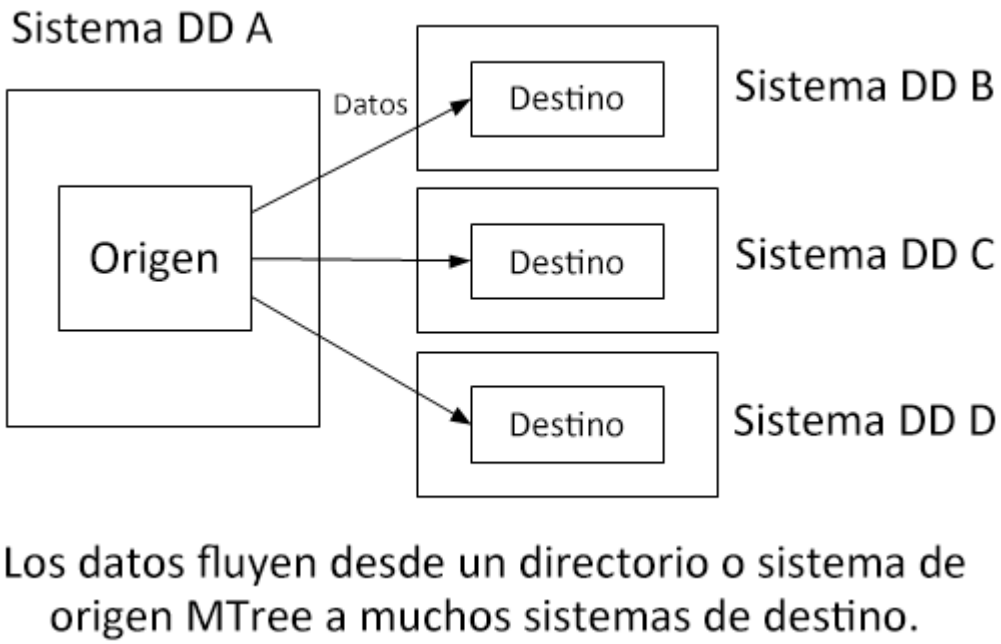
Figura 19 Replicación bidireccional



Replicación de uno a muchos

En la replicación de uno a muchos, los datos fluyen desde un directorio o MTree de origen en un sistema DD hacia varios sistemas DD de destino. Es posible usar este tipo de replicación para crear más de dos copias y contar con una mayor protección de datos o para distribuir datos para el uso en múltiples sitios.

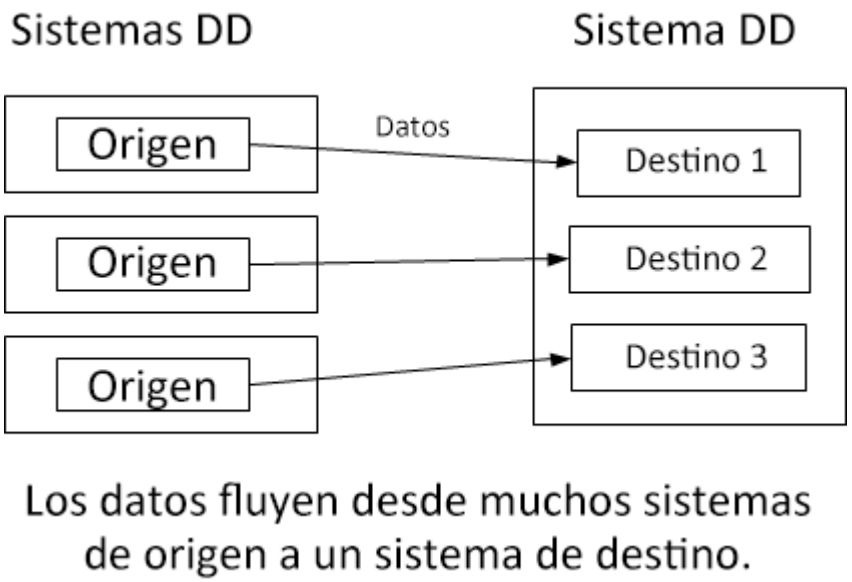
Figura 20 Replicación de uno a muchos



Replicación de muchos a uno

En la replicación de muchos a uno, ya sea con MTree o directorios, los datos de replicación fluyen de varios sistemas DD de origen a un solo sistema DD de destino. Este tipo de replicación puede usarse para ofrecer protección de recuperación de datos para varias sucursales en un sistema de TI de la sede central.

Figura 21 Replicación de muchos a uno

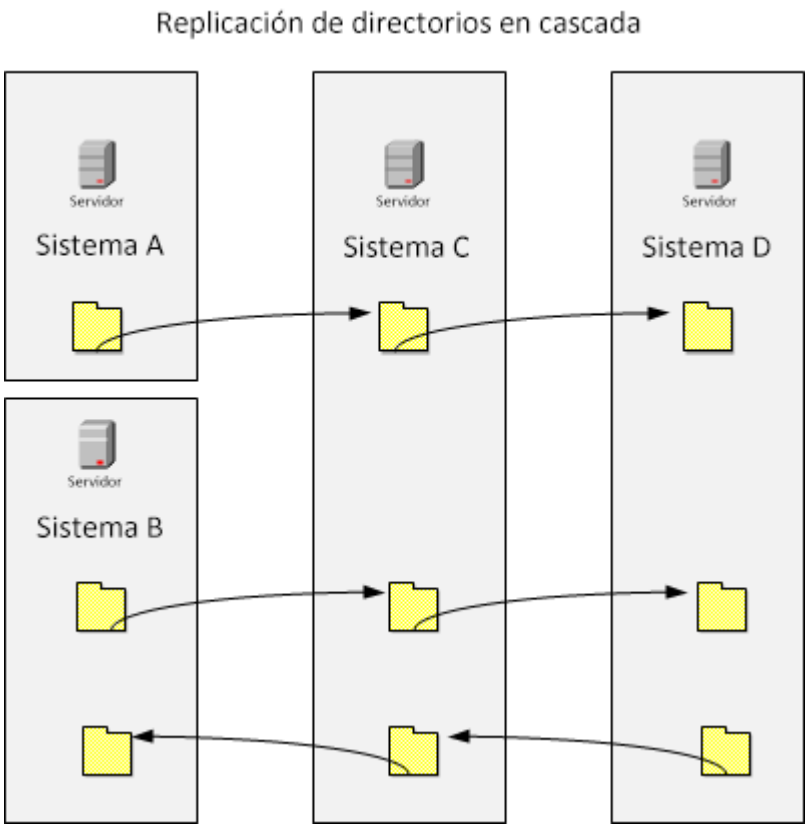


Replicación en cascada

En la topología de replicación en cascada, un directorio o MTree de origen se encadena entre tres sistemas DD. El último salto de la cadena puede configurarse para la replicación de recopilaciones, MTrees o directorios, en función de si el origen es directorio o MTree.

Por ejemplo, el sistema DD A replica uno o más MTrees en el sistema DD B, que después replica esos MTrees en el sistema DD C. Los MTrees del sistema DD B son tanto un destino (del sistema DD A) como un origen (del sistema DD C).

Figura 22 Replicación de directorios en cascada



La recuperación de datos se puede ejecutar desde el contexto del par de replicación no degradado. Por ejemplo:

- En el caso de que el sistema DD A requiera una recuperación, los datos se pueden recuperar del sistema DD B.
- En el caso de que el sistema DD B requiera una recuperación, el método más simple es realizar una resincronización de replicación del sistema DD A en el sistema DD B (el reemplazo). En este caso, el contexto de replicación del sistema DD B en el sistema DD C se debe dividir primero. Después de que el contexto de replicación del sistema DD A en el sistema DD B finaliza la resincronización, se debe configurar y volver a sincronizar un nuevo contexto del sistema DD B al sistema DD C.

Administración de la replicación

Puede administrar la replicación mediante Data Domain System Manager (DD System Manager) o mediante la interfaz de la línea de comandos (CLI) de Data Domain Operating System (DD OS).

Para usar una interfaz gráfica del usuario (GUI) para administrar la replicación, inicie sesión en DD System Manager.

Procedimiento

1. En el menú a la izquierda de DD System Manager, seleccione **Replication**. Si aún no se agregó la licencia, seleccione **Add License**.
2. Seleccione **Automatic** u **On-Demand** (debe tener una licencia de DD Boost para según demanda).

   Equivalente de la CLI

   También puede iniciar sesión en la CLI:

   ```
   login as: sysadmin
   Data Domain OS 6.0.x.x-12345
   Using keyboard-interactive authentication.
   Password:
   ```

Estado de replicación

El *estado de replicación* muestra el conteo de todo el sistema de contextos de replicación que exhiben un estado de advertencia (texto en amarillo) o de error (texto en rojo), o si las condiciones son normales.

Vista Summary

La vista Summary muestra los contextos de replicación configurados para un sistema DD e incluye información adicional acerca del sistema DD seleccionado, es decir, información de resumen acerca de los pares de replicación entrantes y salientes. El enfoque está en el sistema DD en sí y sus entradas y salidas.

La tabla Summary se puede filtrar al especificar un nombre de origen o de destino, o al seleccionar un estado (Error, Warning o Normal).

Tabla 190 Vista Replication Summary

Elemento	Descripción
Source	El nombre de la ruta y el sistema del contexto de origen, con formato *sistema.ruta*. Por ejemplo, para el directorio `dir1` en `system dd120-22`, verá `dd120-22.chaos.local/data/col1/dir1`.
Destination	El nombre de la ruta y el sistema del contexto de destino, con formato *sistema.ruta*. Por ejemplo, para MTree `MTree1` en `system dd120-44`, verá `dd120-44.chaos.local/data/col1/MTree1`.
Type	Tipo de contexto: MTree, directorio (Dir) o Pool.
State	Entre los estados posibles del par de replicación se incluyen:

Tabla 190 Vista Replication Summary (continuación)

Elemento	Descripción
	• Normal: si la réplica se está iniciando, replicando, recuperando, resincronizando o migrando. • Idle: para la replicación de MTree, este estado puede mostrar si el proceso de replicación no está activo actualmente o si hay errores de red (como si el sistema de destino no está disponible). • Warning: si hay una demora inusual de los primeros cinco estados, o del estado Uninitialized. • Error: todos los estados de error posibles, como Disconnected.
Sincronizado a partir de una hora	La hora de registro de la última operación de sincronización de replicación automática realizada por el origen. Para la replicación de MTree, este valor se actualiza cuando se expone una instantánea en el destino. Para la replicación de directorios, se actualiza cuando se aplica un punto de sincronización insertado por el origen. Durante la inicialización de la replicación se muestra un valor de unknown.
Pre-Comp Remaining:	Cantidad de datos previamente comprimidos que quedan para replicar.
Completion Time (Est.)	El valor es `Completed` o la cantidad estimada de tiempo necesario para completar la transferencia de datos de replicación en función de la velocidad de transferencia de las últimas 24 horas.

Información detallada de un contexto de replicación

Al seleccionar un contexto de replicación de la vista Summary, se completa la información de ese contexto en Detailed Information, Performance Graph, Completion Stats y Completion Predictor.

Tabla 191 Información detallada

Elemento	Descripción
State Description	Mensaje acerca del estado de la réplica.
Source	El nombre de ruta y el sistema del contexto de origen, con formato `system.path`. Por ejemplo, para el directorio `dir1` en el sistema `dd120-22`, verá `dd120-22.chaos.local/data/col1/dir1`.
Destination	El nombre de ruta y el sistema del contexto de destino, con formato `system.path`. Por ejemplo, para el MTree `MTree1` en el sistema `dd120-44`, verá `dd120-44.chaos.local/data/col1/MTree1`.
Connection Port	El nombre del sistema y el puerto de escucha usados para la conexión de replicación.

Tabla 192 Gráfico de rendimiento

Elemento	Descripción
Pre-Comp Remaining:	Datos previamente comprimidos que quedan para replicar.
Pre-Comp Written	Datos previamente comprimidos escritos en el origen.
Post-Comp Replicated	Datos posteriores a la compresión que se han replicado.

Tabla 193 Completion Stats

Elemento	Descripción
Synced As Of Time	La hora de registro de la última operación de sincronización de replicación automática realizada por el origen. Para la replicación de MTree, este valor se actualiza cuando se expone una instantánea en el destino. Para la replicación de directorios, se actualiza cuando se aplica un punto de sincronización insertado por el origen. Durante la inicialización de la replicación se muestra un valor de unknown.
Completion Time (Est.)	El valor es `Completed` o la cantidad estimada de tiempo necesario para completar la transferencia de datos de replicación en función de la tasa de transferencia de las últimas 24 horas.
Pre-Comp Remaining:	Cantidad de datos que quedan para replicar.
Files Remaining	Cantidad de archivos que todavía no se han replicado (replicación de directorios únicamente).
Status	Para los terminales de origen y destino, muestra el estado (Enabled, Disabled, Not Licensed, etc.) de los principales componentes del sistema, como: • Replicación • Sistema de archivos • DD Retention Lock • DD Encryption en reposo • DD Encryption por cable • Espacio disponible • Optimización del ancho de banda bajo • Tasa de compresión • Relación de optimización del ancho de banda bajo

Completion Predictor
Completion Predictor es un widget para rastrear el progreso de un trabajo de respaldo y para predecir cuándo se completará una replicación para un contexto seleccionado.

Creación de un par de replicación

Antes de crear un par de replicación, asegúrese de que el destino no *exista*; de lo contrario, recibirá un error.

Procedimiento

1. Seleccione **Replication** > **Automatic** > **Summary tab** > **Create Pair** .
2. En el cuadro de diálogo Create Pair, agregue información para crear un par de replicación de pool, un directorio, un conjunto o un MTree de entrada o de salida, como se describe en las siguientes secciones.

Cómo agregar un sistema DD para replicación

Es posible que deba agregar un sistema DD como host o como destino para poder crear un par de replicación.

Nota

Asegúrese de que el sistema que se va a agregar ejecute una versión compatible de DD OS.

Procedimiento

1. En el cuadro de diálogo Create Pair, seleccione Add System.
2. Para el sistema, ingrese el nombre de host o la dirección IP del sistema que desea agregar.
3. Para el nombre de usuario y la contraseña, ingrese el nombre de usuario y la contraseña de sysadmin.
4. Opcionalmente, haga clic en **More Options** para ingresar una dirección IP (o un nombre de sistema) proxy de un sistema que no se pueda conectar directamente. Si está configurado, ingrese un puerto personalizado en lugar del puerto 3009 predeterminado.

   Nota

   Se admiten direcciones IPv6 únicamente cuando se agrega un sistema con DD OS 5.5 o versiones posteriores a un sistema administrado con DD OS 5.5 o versiones posteriores.

   ---

5. Seleccione **OK**.

   Nota

   Si el sistema no está disponible después de agregarlo a DD System Manager, asegúrese de que haya una ruta desde el sistema administrado hasta el sistema que se va a agregar. Si se ingresa un nombre de host (nombre de dominio calificado [FQDN] o no FQDN), asegúrese de que se pueda resolver en el sistema administrado. Configure un nombre de dominio para el sistema administrado, asegúrese de que exista una entrada DNS para el sistema o asegúrese de que se haya definido una dirección IP para el mapeo del nombre de host.

   ---

6. Si el certificado del sistema no está verificado, el cuadro de diálogo Verify Certificate mostrará detalles acerca del certificado. Verifique las credenciales del sistema. Haga clic en **OK** si confía en el certificado; de lo contrario, haga clic en **Cancel**.

Creación de un par de replicación de recopilaciones

Consulte la sección *Replicación de recopilaciones* para obtener información general acerca de este tipo de recopilación.

Antes de crear un par de replicación de recopilaciones, asegúrese de lo siguiente:

- La capacidad de almacenamiento del sistema de destino debe ser igual a la capacidad del almacenamiento de origen o superior a ella. (Si la capacidad del destino es inferior a la del origen, la capacidad disponible en el origen se reduce a la del destino).
- El destino se destruye y, posteriormente, se vuelve a crear, pero no se habilita.
- Cada destino y cada origen están únicamente en un contexto a la vez.
- El sistema de archivos está deshabilitado en la réplica mientras se configura y habilita el cifrado en el origen.
- El sistema de archivos está deshabilitado en el origen mientras se configura y habilita el cifrado en la réplica.

Procedimiento

1. En el cuadro de diálogo Create Pair, seleccione **Collection** del menú **Replication Type**.
2. Seleccione el nombre de host del sistema de origen en el menú **Source System**.
3. Seleccione el nombre de host del sistema de destino en el menú **Destination System**. La lista incluye únicamente los hosts de la lista DD-Network.
4. Si desea cambiar opciones de configuración de la conexión de host, seleccione la pestaña **Advanced**.
5. Seleccione **OK**. Comenzará la replicación del origen al destino.

Resultados

Los resultados de prueba de Data Domain devuelven las siguientes reglas de rendimiento para la inicialización de la replicación. Estas son *solo* reglas; el rendimiento real visualizado en ambientes de producción puede variar.

- En una LAN de gibibit: Con un conteo de bandejas lo suficientemente alto para generar entradas/salidas máximas y condiciones ideales, la replicación de recopilaciones puede saturar un vínculo de 1 GigE (sobrecarga del protocolo del 10 % del módulo), así como 400 a 900 MB/s en 10 gigE, en función de la plataforma.
- En una WAN, el rendimiento se rige por la velocidad de línea del vínculo de la WAN, el ancho de banda, la latencia y la tasa de pérdida de paquetes.

Creación de un par de replicación de MTree, directorios o pools

Consulte las secciones*Replicación de MTree* y *Replicación de directorios* para obtener información general acerca de estos tipos de replicación.

Al crear un par de replicación de MTree, directorios o pools:

- Asegúrese de que la replicación esté en tránsito\salida en la interfaz correcta. Al definir un contexto de replicación, los nombres de host del origen y el destino deben resolverse con búsquedas directas e inversas. Para hacer que los datos transiten las interfaces alternativas del sistema en lugar de la interfaz de resolución predeterminada, se debe modificar el contexto de replicación después de la creación. Puede ser necesario configurar archivos de host para garantizar que los contextos se definan en interfaces que no sean de resolución (cruzadas).

- Puede “invertir” el contexto de una replicación de MTree, es decir, puede alternar el origen y el destino.
- Los subdirectorios con un MTree no se pueden replicar, porque se replica el MTree completo.
- Se admite replicación de MTree de sistemas habilitados para DD Extended Retention a sistemas no habilitados para DD Extended Retention si ambos ejecutan DD OS 5.5 o versiones posteriores.
- El sistema DD de destino debe tener capacidad de almacenamiento disponible de, al menos, el tamaño posterior a la compresión del tamaño máximo previsto del directorio o MTree de origen.
- Cuando se inicia la replicación, se crea automáticamente un directorio de destino.
- Un sistema DD puede ser, simultáneamente, el origen de un contexto y el destino de otro.

Procedimiento

1. En el cuadro de diálogo Create Pair, seleccione **Directory**, **MTree** (predeterminado) o **Pool** del menú **Replication Type**.
2. Seleccione el nombre de host del sistema de origen en el menú **Source System**.
3. Seleccione el nombre de host del sistema de destino en el menú **Destination System**.
4. Ingrese la ruta de origen en el cuadro de texto **Source Path** (tenga en cuenta que la primera parte de la ruta es una constante que cambia en función del tipo de replicación elegido).
5. Ingrese la ruta de destino en el cuadro de texto **Destination Path** (tenga en cuenta que la primera parte de la ruta es una constante que cambia en función del tipo de replicación elegido).
6. Si desea cambiar opciones de configuración de la conexión de host, seleccione la pestaña **Advanced**.
7. Seleccione **OK**.

   Comenzará la replicación del origen al destino.

   Los resultados de pruebas de Data Domain revolvieron las siguientes reglas para estimar el tiempo necesario para el inicio de la replicación.

   Estas son *solo* reglas y pueden no ser precisas en ambientes de producción específicos.

   - Cuando se usa una WAN de conexión T3 de 100 ms, el rendimiento es de alrededor de 40 MiB/s de datos previamente comprimidos, lo que genera la transferencia de datos de:
     40 MiB/s = 25 segundos/GiB = 3.456 TiB/día
   - Cuando se usa el equivalente de base 2 de LAN gigabit, el rendimiento es de alrededor de 80 MiB/s de datos previamente comprimidos, lo que genera la transferencia de datos de alrededor del doble de la velocidad para una WAN T3.

Ejemplo 2 Equivalente de la CLI

Aquí se incluye un ejemplo de cómo crear pares de replicación de MTree y directorios en la CLI. En este ejemplo, el sistema Data Domain de origen es `dd640` y el sistema Data Domain de destino es `dlh5`. Para obtener más detalles sobre el uso en otros

Ejemplo 2 Equivalente de la CLI (continuación)

escenarios, consulte la *Guía de referencia de comandos de Data Domain Operating System*.

1. Cree un MTree en el sistema Data Domain de origen:

```
sysadmin@dd640# mtree create /data/col1/Oracle2
MTree "/data/col1/Oracle2" created successfully.
```

2. Cree el contexto de replicación en el sistema Data Domain de destino utilizando el nombre de host completo.

```
sysadmin@dlh5# replication add source mtree://dd640.chaos.local/data/col1/Oracle2
destination mtree://dlh5.chaos.local/data/col1/Oracle2
```

3. Cree el contexto de replicación en el sistema Data Domain de origen utilizando el nombre de host completo.

```
sysadmin@dd640# replication add source mtree://dd640.chaos.local/data/col1/Oracle2
destination mtree://dlh5.chaos.local/data/col1/Oracle2
```

4. Para verificar que se haya creado el contexto de replicación de MTree, utilice el comando `replication show config`.
   La salida se trunca horizontalmente en este ejemplo.

```
sysadmin@dlh5# replication show config
CTX  Source                                      Destination
---  ------------------------------------------
----------------------------------------
1    dir://dd640.chaos.local/backup/Oracle2      dir://dlh5.chaos.local/backup/
Oracle2
2    mtree://dd640.chaos.local/data/col1/Oracle2 mtree://dlh5.chaos.local/data/col1/
Oracle2
---  ------------------------------------------
----------------------------------------
 * Used for recovery only.
```

5. Para iniciar la replicación entre un origen y un destino, use el comando `replication initialize` en el origen. Este comando comprueba que la configuración y las conexiones sean correctas y devuelve mensajes de error si se producen problemas.

```
sysadmin@dd640# replication initialize mtree://dlh5.chaos.local/data/col1/Oracle2
 (00:08) Waiting for initialize to start...
 (00:10) Intialize started.
 Use 'replication watch mtree://dlh5.chaos.local/data/col1/Oracle2' to monitor progress.
```

Configuración de replicación bidireccional
Para crear un par de replicación bidireccional, use el procedimiento de pares de replicación de directorios o MTree (por ejemplo, con mtree2) del host A al host B. Use el mismo procedimiento para crear un par de replicación (por ejemplo, con mtree1) del host B al host A. Para esta configuración, los nombres de ruta no pueden ser iguales.

Configuración de replicación de uno a muchos
Para crear un par de replicación de uno a muchos, use el procedimiento del par de replicación de directorio o MTree (por ejemplo, con mtree1) en el host A para: (1) mtree1 en el host B, (2) mtree1 en el host C y (3) mtree1 en el host D. No se puede realizar una recuperación de replicaciones en un contexto de origen cuya ruta sea la ruta de origen para otros contextos; los otros contextos se deben quitar y volver a sincronizar después de la recuperación.

Configuración de replicación de muchos a uno
Para crear un par de replicación de muchos a uno, use el procedimiento del par de replicación de directorio o MTree [por ejemplo, (1) mtree1 del host A a mtree1 en el host C y (2) mtree2 en el host B a mtree2 en el host C].

Configuración de la replicación en cascada
Para crear un par de replicación en cascada, use el procedimiento para pares de replicación de directorios o MTree: (1) mtree1 en el host A al mtree1 en el host B, y (2) en el host B, cree un par para mtree1 a mtree1 en el host C. El contexto de destino final (en el host C en este ejemplo, pero se admiten más de tres saltos) puede ser una réplica de recopilaciones o una réplica de directorios o MTree.

Activación y desactivación de un par de replicación

Al desactivar un par de replicación, se pausa temporalmente la replicación de datos activa entre un origen y un destino. El origen deja de enviar datos al destino y el destino deja de funcionar como conexión activa para el origen.

Procedimiento

1. Seleccione uno o más pares de replicación de la tabla Summary y seleccione **Disable Pair**.
2. En el cuadro de diálogo Disable Pair, seleccione **Next** y, a continuación, **OK**.
3. Para reanudar la operación de un par de replicación desactivado, seleccione uno o más pares de replicación de la tabla Summary y seleccione **Enable Pair** para que se muestre el cuadro de diálogo Enable Pair.
4. Seleccione **Next** y, a continuación, **OK**. Se reanudará la replicación de datos.

Equivalente de la CLI

```
# replication disable {destination | all}

# replication enable {destination | all}
```

Eliminación de un par de replicación

Cuando se elimina un par de replicación de MTree o un directorio, el directorio o el MTree de destino, respectivamente, pasan a tener capacidad de escritura. Cuando se elimina un par de replicación de recopilaciones, el sistema DD de destino se vuelve un sistema de lectura/escritura independiente y el sistema de archivos se deshabilita.

Procedimiento

1. Seleccione uno o más pares de replicación de la tabla Summary y seleccione **Delete Pair**.
2. En el cuadro de diálogo Delete Pair, seleccione **Next** y, a continuación, **OK**. Se eliminarán los pares de replicación.

Equivalente de la CLI
Antes de ejecutar este comando, siempre ejecute el comando `filesys disable`. Luego, ejecute el comando `filesys enable`.

```
# replication break {destination | all}
```

Pueden surgir ciertas situaciones en las que se deba resincronizar la replicación para resolver un problema. Para obtener información sobre la interrupción y la resincronización de la replicación, consulte el artículo de la base de conocimiento *Break and Resync Directory Replication*, disponible en https://support.emc.com/kb/180668.

Cambio de configuración de conexión de hosts

Para dirigir el tráfico fuera de un puerto específico, puede modificar un contexto actual al alterar el parámetro de host de conexión con un nombre de host previamente

definido en el archivo de hosts locales para abordar el sistema alternativo. Ese nombre de host corresponderá al destino. La entrada del host indicará una dirección de destino alternativa para ese host. Esta puede requerirse en los sistemas de origen y de destino.

Procedimiento

1. Seleccione el par de replicación en la tabla Summary y seleccione **Modify Settings**. También puede cambiar esta configuración cuando lleva a cabo las acciones Create Pair, Start Resync o Start Recover al seleccionar la pestaña **Advanced**.
2. En el cuadro de diálogo Modify Connection Settings, modifique las siguientes opciones de configuración según lo desee:
   a. **Use Low Bandwidth Optimization**: en empresas con conjuntos de datos pequeños y redes con ancho de banda de 6 Mbps o menos, DD Replicator puede reducir aún más la cantidad de datos que se deben enviar mediante *el modo de optimización del ancho de banda bajo*. Esto permite que los sitios remotos con ancho de banda limitado usen menos ancho de banda o repliquen y protejan más datos por medio de las redes existentes. Esta optimización se debe habilitar en los sistemas DD de origen y de destino. Si el origen y el destino tienen configuraciones de optimización de bajo ancho de banda incompatibles, la optimización de bajo ancho de banda estará inactiva para ese contexto. Después de habilitar la optimización del ancho de banda bajo en el origen y en el destino, ambos sistemas deben someterse a un ciclo de limpieza completo para preparar los datos existentes; por lo tanto, ejecute `filesys clean start` en ambos sistemas. La duración del ciclo de limpieza depende de la cantidad de datos del sistema DD, pero lleva más tiempo que una limpieza normal. Para obtener más información acerca de los comandos `filesys`, consulte la *Guía de referencia de comandos de Data Domain Operating System*.

      Importante: La optimización del ancho de banda bajo no se admite si la opción de software DD Extended Retention está habilitada en un sistema DD. Tampoco es compatible para replicación de recopilaciones.

   b. **Enable Encryption Over Wire**: DD Replicator admite el cifrado de datos en transferencia mediante el uso del protocolo SSL (capa de conexión segura) estándar versión 1.0.1, que usa las suites de cifrado ADH-AES256-GCM-SHA384 y DHE-RSA-AES256-GCM-SHA384 para establecer conexiones de replicación seguras. Ambos lados de la conexión deben habilitar esta función para que continúe el cifrado.
   c. **Network Preference**: Puede elegir IPv4 o IPv6. Un servicio de replicación habilitado para IPv6 igualmente puede aceptar conexiones desde un cliente de la replicación IPv4 si el servicio está accesible por medio de IPv4. Un servicio de replicación habilitado para IPv6 igualmente puede comunicarse con un servicio de replicación IPv4 si el servicio está accesible por medio de IPv4.
   d. **Use Non-default Connection Host**: el sistema de origen transmite datos a un puerto de escucha del sistema de destino. Dado que en un sistema de origen la replicación puede estar configurada para muchos sistemas de destino (donde cada uno puede tener un puerto de escucha distinto), cada contexto en el origen puede configurar el puerto de conexión al puerto de escucha correspondiente del destino.
3. Seleccione **Next** y, a continuación, **Close**.

   Se actualizará la configuración del par de replicación y se reanudará la replicación.

Equivalente de la CLI

```
#replication modify <destino> connection-host <nuevo-nombre-de-host> [port <puerto>]
```

Administración de sistemas de replicación

Puede agregar o eliminar los sistemas Data Domain que se utilizarán para la replicación mediante el cuadro de diálogo Manage Systems.

Procedimiento

1. Seleccione **Manage Systems**.
2. En el cuadro de diálogo Manage Systems, agregue o elimine sistemas Data Domain, según sea necesario.
3. Seleccione **Close**.

Recuperación de datos de un par de replicación

Si los datos de replicación de origen se vuelven inaccesibles, se pueden *recuperar* del destino del par de replicación. El origen debe estar vacío antes de que se pueda continuar con la recuperación. La recuperación se puede realizar para todas las topologías de replicación, excepto para la replicación de MTree.

En las próximas secciones se describe la recuperación de datos desde un pool de directorio, así como de pares de replicación de recopilaciones y de directorio.

Recuperación de datos de pools de directorio

Puede recuperar datos desde un pool de directorio, pero no desde un pool basado en MTree.

Procedimiento

1. Seleccione **More** > **Start Recover**.
2. En el cuadro de diálogo Start Recover, seleccione **Pool** en el menú **Replication Type**.
3. Seleccione el nombre de host del sistema de origen en el menú **System to recover to**.
4. Seleccione el nombre de host del sistema de destino en el menú **System to recover from**.
5. Seleccione el contexto en el destino del que se recuperarán los datos.
6. Si desea cambiar opciones de configuración de la conexión de host, seleccione la pestaña **Advanced**.
7. Seleccione **OK** para comenzar la recuperación.

Recuperación de datos de pares de replicación de recopilaciones

Para recuperar correctamente los datos de pares de replicación de recopilaciones, el sistema de archivos de origen debe estar en estado intacto y el contexto de destino debe estar totalmente inicializado.

Procedimiento

1. Seleccione **More** > **Start Recover** para que se muestre el cuadro de diálogo Start Recover.
2. Seleccione **Collection** en el menú **Replication Type**.

3. Seleccione el nombre de host del sistema de origen en el menú **System to recover to**.
4. Seleccione el nombre de host del sistema de destino en el menú **System to recover from**.
5. Seleccione el contexto en el destino del que se recuperarán los datos. Solo existirá una recopilación en el destino.
6. Para cambiar opciones de configuración de la conexión de host, seleccione la pestaña **Advanced**.
7. Seleccione **OK** para comenzar la recuperación.

Recuperación de datos de par de replicación de directorios

Para recuperar correctamente datos de par de replicación de directorios, se debe crear el mismo directorio que se usa en el contexto original (pero se debe dejar vacío).

Procedimiento

1. Seleccione **More** > **Start Recover** para que se muestre el cuadro de diálogo Start Recover.
2. Seleccione **Directory** en el menú **Replication Type**.
3. Seleccione el nombre de host del *sistema en el que se deben restaurar los datos* del menú **System to recover to**.
4. Seleccione el nombre de host del *sistema que será el origen de datos* del menú **System to recover from**.
5. Seleccione el contexto para restaurar de la lista de contextos.
6. Para cambiar opciones de configuración de la conexión de host, seleccione la pestaña **Advanced**.
7. Seleccione **OK** para comenzar la recuperación.

Anulación de la recuperación de un par de replicación

Si la recuperación de un par de replicación falla o se debe finalizar, puede detener la recuperación de replicaciones.

Procedimiento

1. Seleccione el menú More y seleccione **Abort Recover** para que se muestre el cuadro de diálogo Abort Recover, que muestra los contextos que actualmente están realizando una recuperación.
2. Seleccione la casilla de verificación de uno o más contextos para anular de la lista.
3. Seleccione **OK**.

Requistos posteriores

Deberá reiniciar la recuperación en cuanto pueda.

Resincronización de un par de replicación de MTree, directorios o pools

La *resincronización* es el proceso de recuperar (o volver a sincronizar) los datos entre un par de replicación de origen y de destino después de una interrupción manual. El par de replicación se resincroniza de modo que ambos puntos finales contengan los mismos datos. La resincronización está disponible para replicación de MTree, directorios y pools, pero no para replicación de recopilaciones.

Una resincronización de replicación también se puede usar en los siguientes casos:

- Para crear un contexto que se ha eliminado.
- Cuando un destino se queda sin espacio, pero el origen todavía contiene datos para replicar.
- Para convertir un par de replicación de directorio en un par de replicación de MTree.

Procedimiento

1. Elimine el contexto en los sistemas de destino y de origen de la replicación.
2. En el sistema de origen o de destino de la replicación, seleccione **More** > **Start Resync** para que se muestre el cuadro de diálogo Start Resync.
3. Seleccione el tipo de replicación que desee resincronizar: **Directory**, **MTree** o **Pool**.
4. Seleccione el nombre de host del sistema de origen de la replicación del menú **Source System**.
5. Seleccione el nombre de host del sistema de destino de la replicación del menú **Destination System**.
6. Ingrese la ruta de origen de la replicación en el cuadro de texto **Source Path**.
7. Ingrese la ruta de destino de la replicación en el cuadro de texto **Destination Path**.
8. Para cambiar opciones de configuración de la conexión de host, seleccione la pestaña **Advanced**.
9. Seleccione **OK**.

Equivalente de la CLI

```
# replication resync destination
```

Anulación de la resincronización de un par de replicación

Si la resincronización de un par de replicación falla o se debe finalizar, puede detener la resincronización.

Procedimiento

1. Desde el sistema de origen o de destino de la replicación, seleccione **More** > **Abort Resync** para que se muestre el cuadro de diálogo Abort Resync, que muestra todos los contextos que actualmente están realizando una resincronización.
2. Seleccione las casillas de verificación de uno o más contextos para anular su resincronización.
3. Seleccione **OK**.

Vista de DD Boost

La vista DD Boost proporciona información de configuración y solución de problemas para los administradores de NetBackup que han configurado sistemas DD para usar DD Boost AIR (replicación automática de imágenes) o cualquier aplicación de DD Boost que use replicación de archivos administrada.

Para obtener instrucciones de configuración de DD Boost AIR, consulte la *Guía de administración de Data Domain Boost para OpenStorage*.

La pestaña **File Replication** muestra:

- Currently Active File Replication:
  - La dirección (saliente y entrante) y el número de archivos en cada una.
  - Los datos restantes para replicarse (valor previamente comprimido en GiB) y la cantidad de datos ya replicados (valor previamente comprimido en GiB).
  - Total size: la cantidad de datos para replicar y los datos ya replicados (valor previamente comprimido en GiB).
- Most Recent Status: el total de replicaciones de archivos y si se completaron o fallaron
  - durante la última hora
  - durante las últimas 24 horas
- Remote Systems:
  - Seleccione una replicación de la lista.
  - Seleccione el período de tiempo para abarcar del menú.
  - Seleccione **Show Details** para obtener más información acerca de estos archivos del sistema remoto.

La pestaña **Storage Unit Associations** muestra la siguiente información, que puede usar con fines de auditoría o para comprobar el estado de eventos de DD Boost AIR usados para replicaciones de imágenes de la unidad de almacenamiento:

- Una lista de todas las **Associations** de unidad de almacenamiento conocidas para el sistema. El origen se encuentra a la izquierda y el destino a la derecha. Esta información muestra la configuración de AIR en el sistema Data Domain.
- **Event Queue** es la lista de eventos pendientes. Muestra la unidad de almacenamiento local, el ID de evento y el estado del evento.

Se realiza un intento para hacer coincidir ambos extremos de una ruta de DD Boost para formar un par y presentarlo como un par/log. Si la coincidencia no es posible, por varios motivos, la ruta remota se mostrará como *pendiente*.

Archivos del sistema remoto

En el botón Show Details se proporciona información del sistema remoto de replicación de archivos seleccionado. File Replications muestra la información de inicio y finalización, además del tamaño y la cantidad de datos del sistema remoto de replicación de archivos seleccionado. El gráfico de rendimiento muestra el rendimiento en el tiempo del sistema remoto de replicación de archivos seleccionado.

Tabla 194 Replicación de archivos

Elemento	Descripción
Start	Punto de inicio del período de tiempo.
End	Punto de finalización del período de tiempo.
File Name	Nombre del archivo de replicación específico.
Status	Estado más reciente (Success, Failure).
Pre-Comp Size (MiB)	Cantidad de datos entrantes y salientes previamente comprimidos, en comparación con el rendimiento de red o los datos posteriores a la compresión (en MiB).
Network Bytes (MiB)	Cantidad de datos de rendimiento de red (en MiB).

Tabla 195 Gráfico de rendimiento

Elemento	Descripción
Duración	Duración de la replicación (1d, 7d o 30d).
Interval	Intervalo de replicación (Daily o Weekly).
Pre-Comp Replicated	Cantidad de datos entrantes y salientes previamente comprimidos (en GiB).
Post-Comp Replicated	Cantidad de datos posteriores a la compresión (en GiB).
Network Bytes	Cantidad de datos de rendimiento de red (en GiB).
Files Succeeded	Cantidad de datos que se replicaron correctamente.
Files Failed	Cantidad de archivos que no se pudieron replicar.
Show in new window	Abre una ventana separada.
Print	Imprime el gráfico.

Vista Performance

La vista Performance muestra un gráfico que representa la fluctuación de datos durante la replicación. Estas son estadísticas agregadas de cada par de replicación para este sistema DD.

- **Duration** (eje X) es 30 días de forma predeterminada.
- **Replication Performance** (eje Y) está en GibiBytes o MebiBytes (los equivalentes binarios de GigaBytes y MegaBytes).
- **Network In** son los bytes de red de replicación total que ingresan al sistema (todos los contextos).
- **Network Out** son los bytes de red de replicación total que salen del sistema (todos los contextos).
- Para una lectura de un punto específico en el tiempo, desplace el cursor sobre un lugar del gráfico.
- Durante los momentos de inactividad (cuando no se están transfiriendo datos), la forma del gráfico puede mostrar una línea gradualmente descendente en lugar de la línea bruscamente descendente esperada.

Vista Advanced Settings

La vista Advanced Settings le permite administrar opciones de regulación y de red.

Opciones de regulación

- **Throttle Override**: muestra la tasa de regulación si está configurada o 0, que significa que todo el tráfico de replicación está detenido.
- **Permanent Schedule**: muestra el horario y los días de la semana en que se aplica la regulación calendarizada.

Configuración de red

- **Bandwidth**: muestra la velocidad del flujo de datos establecida si se configuró el ancho de banda o Unlimited (predeterminado) si no. El flujo de datos promedio al destino de replicación es de al menos 98,304 bits por segundo (12 KiB).

- **Delay**: muestra la configuración de retraso de red establecida (en milisegundos) si se configuró o None (predeterminado) si no.
- **Listen Port**: muestra el valor del puerto de escucha establecido si se configuró o 2051 (predeterminado) si no.

Cómo agregar opciones de regulación

Para modificar la cantidad de ancho de banda utilizado por una red para replicación, puede configurar una *regulación de replicación* para el tráfico de replicación.

Hay tres tipos de opciones de regulación de replicación:

- **Scheduled throttle**: la tasa de regulación se establece como un período o tiempo predeterminado.
- **Current throttle**: la tasa de regulación se establece hasta el próximo cambio programado o hasta un reinicio del sistema.
- **Override throttle**: se omiten los dos tipos anteriores de regulación. Esto persiste, aunque se reinicie el sistema, hasta que seleccione **Clear Throttle Override** o emita el comando `replication throttle reset override .`

También puede establecer una regulación predeterminada o una regulación para destinos específicos, como se indica a continuación:

- **Default throttle**: cuando se configura, todos los contextos de replicación se limitan a esta regulación, excepto aquellos destinos especificados por las regulaciones de destino (consulte el siguiente punto).
- **Destination throttle**: esta regulación se usa cuando solamente se deben regular pocos destinos o cuando un destino requiere una configuración de regulación diferente de la regulación predeterminada. Cuando existe una regulación predeterminada, esta regulación tiene prioridad para el destino especificado. Por ejemplo, puede configurar la regulación de replicación predeterminada en *10 kbps*, pero, al usar una regulación de destino, puede configurar un solo contexto de replicación de recopilaciones como *ilimitado*.

Nota

Actualmente, puede establecer y modificar una regulación de destino únicamente usando la interfaz de la línea de comandos (CLI); esta funcionalidad no está disponible en DD System Manager. Para obtener documentación sobre esta función, consulte el comando `replication throttle` en la *Guía de referencia de comandos de Data Domain Operating System*. Si DD System Manager detecta que se ha configurado una o más regulaciones de destino, recibirá una advertencia y deberá usar la CLI para continuar.

Notas adicionales sobre la regulación de replicación:

- Las regulaciones se configuran solo en el origen. La única regulación que se aplica al destino es la opción **0 Bps (Disabled)**, que deshabilita todo el tráfico de replicación.
- El valor mínimo de una regulación de replicación es 98,304 bits por segundo.

Procedimiento

1. Seleccione **Replication** > **Advanced Settings** > **Add Throttle Setting** para que se muestre el cuadro de diálogo Add Throttle Setting.
2. Configure los días de la semana en los que la regulación debe estar activa; para ello, seleccione **Every Day** o seleccione las casillas de verificación junto a los días individuales.

3. Configure la hora a la que debe comenzar la regulación con los selectores desplegables **Start Time** para hora:minuto y AM/PM.
4. Para **Throttle Rate**:
   - Seleccione **Unlimited** para no configurar límites.
   - Escriba un número en el cuadro de texto (por ejemplo, 20000) y seleccione la tasa del menú (bps, Kbps, Bps o KBps).
   - Seleccione la opción **0 Bps (disabled)** para deshabilitar todo el tráfico de replicación.
5. Seleccione **OK** para configurar el calendario. El nuevo calendario se muestra en **Permanent Schedule**.

Resultados

La replicación se ejecuta a la tasa establecida hasta el próximo cambio programado o hasta que una nueva configuración de regulación fuerza un cambio.

Eliminación de opciones de regulación

Puede eliminar una sola opción de regulación o todas las opciones de regulación a la vez.

Procedimiento

1. Seleccione **Replication** > **Advanced Settings** > **Delete Throttle Setting** para que se muestre el cuadro de diálogo Delete Throttle Setting.
2. Seleccione la casilla de verificación de la opción de regulación que desee eliminar o seleccione la casilla de verificación del encabezado para eliminar todas las opciones. Esta lista puede incluir opciones del estado “deshabilitado”.
3. Seleccione **OK** para eliminar las opciones.
4. En el cuadro de diálogo Delete Throttle Setting Status, seleccione **Close**.

Reemplazo temporal de una configuración de regulación

Un reemplazo de regulación cambia temporalmente la configuración de una regulación. La configuración actual se muestra en la parte superior de la ventana.

Procedimiento

1. Seleccione **Replication** > **Advanced Settings** > **Set Throttle Override** para mostrar el cuadro de diálogo Throttle Override.
2. Configure un nuevo reemplazo de regulación o borre un reemplazo anterior.
   a. Para configurar un nuevo reemplazo de regulación, realice una de las siguientes acciones:
      - Seleccione **Unlimited** para revertir a la tasa de regulación establecida por el sistema (no se realiza regulación).
      - Establezca la tasa y los bits de regulación en el cuadro de texto (por ejemplo, 20000) y (bps, Kbps, Bps o KBps).
      - Seleccione **0 Bps (Disabled)** para establecer la tasa de regulación en 0, para que se detenga de manera eficaz todo el tráfico de red de replicación.
      - Para aplicar el cambio temporalmente, seleccione **Clear at next scheduled throttle event**.

b. Para borrar un reemplazo establecido anteriormente, seleccione **Clear Throttle Override**.

3. Seleccione **OK**.

Cambio de la configuración de red

Al usar las opciones de configuración de ancho de banda y de retraso de red juntas, la replicación calcula el tamaño adecuado del búfer de TCP (protocolo de control de transmisión) para el uso de replicación. Estas opciones de configuración de red son globales para el sistema DD y se deben establecer una sola vez por sistema.

Tenga en cuenta lo siguiente:

- Puede determinar el ancho de banda real y los valores de retraso real de la red para cada servidor a través del comando `ping`.
- Los parámetros de red predeterminados en una restauración funcionan bien para la replicación en configuraciones de latencia baja, como una red Ethernet local de 100 Mbps o 1000 Mbps, donde el ciclo de ida y vuelta de latencia (conforme a la medición del comando `ping`) generalmente es menor de 1 milisegundo. Los valores predeterminados también funcionan bien para la replicación en WAN con ancho de banda bajo a moderado, donde la latencia puede ser tan alta como 50 a 100 milisegundos. Sin embargo, para las redes con alta latencia y alto ancho de banda, es necesario realizar algunos ajustes de los parámetros de red.
  El número clave para ajustar es el número de retraso del ancho de banda que se obtiene al multiplicar el ancho de banda y el ciclo de ida y vuelta de latencia de la red. Este número es una medición de cuántos datos se pueden transmitir en la red antes de que puedan volver reconocimientos del otro extremo. Si el número de retraso del ancho de banda de una red de replicación es mayor de 100,000, el rendimiento de la replicación se beneficia de la configuración de los parámetros de red en ambas restauraciones.

Procedimiento

1. Seleccione **Replication** > **Advanced Settings** > **Change Network Settings** para que se muestre el cuadro de diálogo Network Settings.
2. En el área Network Settings, seleccione **Custom Values**.
3. Ingrese los valores de **Delay** y **Bandwidth** en los cuadros de texto. La configuración de retraso de red está en milisegundos, y el ancho de banda está en bytes por segundo.
4. En el área Listen Port, ingrese un valor nuevo en el cuadro de texto. El puerto de escucha de IP predeterminado para un destino de replicación que recibe flujos de datos del origen de replicación es 2051. Esta es una configuración global del sistema DD.
5. Seleccione **OK**. La configuración nueva aparecerá en la tabla Network Settings.

Monitoreo de la replicación

DD System Manager ofrece muchas maneras de rastrear el estado de las replicaciones, desde comprobar el estado del par de replicación hasta rastrear trabajos de respaldo, comprobar el rendimiento y rastrear un proceso de replicación.

Visualización del tiempo de finalización estimado para trabajos de respaldo

Puede usar la función Completion Predictor para ver el tiempo estimado de finalización de un trabajo de replicación de respaldo.

Procedimiento

1. Seleccione **Replication** > **Summary**.
2. Seleccione un contexto de replicación del que desee que se muestre información detallada.
3. En el área Completion Predictor, seleccione opciones de la lista desplegable **Source Time** para el tiempo de finalización de una replicación y seleccione **Track**.

   En el área Completion Time, se mostrará el tiempo estimado de cuándo un trabajo de respaldo en particular finalizará la replicación en el destino. Si la replicación ha finalizado, en el área se muestra `Completed`.

Comprobación del rendimiento de contextos de replicación

Para comprobar el rendimiento de un contexto de replicación en el tiempo, seleccione un contexto de replicación en la vista Summary y, a continuación, seleccione **Performance Graph** en el área Detailed Information.

Rastreo del estado de un proceso de replicación

Para mostrar el progreso de una inicialización de replicación, resincronización u operación de recuperación, use la vista **Replication** > **Summary** para consultar el estado actual.

Equivalente de la CLI

```
# replication show config all
CTX  Source                                    Destination
Connection Host and Port     Enabled
---  ------------------------        ------------------------        -------------------------
-------
1       dir://host2/backup/dir2     dir://host3/backup/dir3
host3.company.com               Yes
2       dir://host3/backup/dir3     dir://host2/backup/dir2
host3.company.com               Yes
```

Al especificar una versión de IP, use el siguiente comando para comprobar su configuración:

```
# replication show config rctx://2

CTX:                        2
Source:                     mtree://ddbeta1.dallasrdc.com/data/col1/EDM1
Destination:                mtree://ddbeta2.dallasrdc.com/data/col1/EDM_ipv6
Connection Host:            ddbeta2-ipv6.dallasrdc.com
Connection Port:            (default)
Ipversion:                  ipv6
Low-bw-optim:               disabled
Encryption:                 disabled
Enabled:                    yes
Propagate-retention-lock:   enabled
```

Retraso de replicación

La cantidad de tiempo entre dos copias de datos se conoce como retraso de replicación.

Puede medir el retraso de replicación entre dos contextos con el comando de estado de replicación. Para obtener información acerca de cómo determinar la causa del retraso de replicación y mitigar su impacto, consulte el artículo de la base de

conocimientos *Troubleshooting Replication Lag*, disponible en https://support.emc.com/kb/180482.

Replicación con HA

Las direcciones flotantes permiten a los sistemas de alta disponibilidad especificar una sola dirección IP para la configuración de replicación que funcionará independientemente de qué nodo del par de alta disponibilidad sea el nodo activo.

Mediante redes IP, los sistemas de alta disponibilidad usan una dirección IP flotante para proporcionar acceso a los datos al par de alta disponibilidad de Data Domain, independientemente de qué nodo físico sea el nodo activo. El comando net config proporciona la opción `[type {fixed | floating}]` para configurar una dirección IP flotante. La *Guía de referencia de comandos de Data Domain Operating System* proporciona más información.

Si se requiere un nombre de dominio para acceder a la dirección IP flotante, especifique el nombre del sistema de alta disponibilidad como el nombre de dominio. Ejecute el comando `ha status` para buscar el nombre del sistema de alta disponibilidad.

Nota

Ejecute el comando `net show hostname type ha-system` para mostrar el nombre del sistema de alta disponibilidad y, si es necesario, ejecute el comando `net set hostname ha-system command` para cambiar el nombre del sistema de alta disponibilidad.

Todos los accesos al sistema de archivos deben ser por medio de una IP flotante. Al configurar las operaciones de respaldo y replicación en un par de alta disponibilidad, siempre especifique la dirección IP flotante como la dirección IP para el sistema Data Domain. Las funciones de Data Domain como DD Boost y replicación aceptarán la dirección IP flotante para el par de alta disponibilidad de la misma manera que aceptan la dirección IP del sistema para un sistema sin alta disponibilidad.

Replicación entre sistemas con alta disponibilidad y sin alta disponibilidad
Si desea configurar una replicación entre un sistema de alta disponibilidad (HA) y un sistema que ejecuta DD OS 5.7.0.3 o versiones anteriores, debe crear y administrar la replicación en el sistema de alta disponibilidad en el caso de que desee usar la interfaz gráfica del usuario (GUI) de DD System Manager.

Sin embargo, puede realizar replicaciones de un sistema sin alta disponibilidad a un sistema de alta disponibilidad mediante la CLI, así como desde el sistema de alta disponibilidad hacia el sistema sin alta disponibilidad.

No se admite la replicación de recopilaciones entre los sistemas de alta disponibilidad y sin alta disponibilidad. La replicación de directorios o MTrees se requiere para replicar datos entre sistemas de alta disponibilidad y sin alta disponibilidad.

Replicación de un sistema con cuotas a uno sin ellas

Replique un sistema Data Domain con DD OS que admite cuotas, a un sistema con un DD OS que no las tenga.

- Una resincronización inversa, que envía los datos del sistema sin cuotas y lo ubica nuevamente en un MTree en el sistema habilitado para cuotas (y que continúa habilitado para tener cuotas).

- Una inicialización inversa desde el sistema sin cuotas, que toma sus datos y crea un nuevo MTree en el sistema que admite las cuotas, pero que sin embargo no tiene cuotas habilitadas ya que fue creado a partir de datos en un sistema sin cuotas.

Nota

Las cuotas se implementaron a partir del DD OS 5.2.

Replication Scaling Context

La función Replication Scaling Context proporciona más flexibilidad cuando se configuran contextos de replicación.

En ambientes con más de 299 contextos de replicación que incluyen contextos de replicación de directorios y de MTree, esta función le permite configurar los contextos en cualquier orden. Anteriormente, era necesario configurar los contextos de replicación de directorio primero y los contextos de replicación de MTree después.

La cantidad total de contextos de replicación no puede exceder 540.

Nota

Esta función solo aparece en los sistemas Data Domain que ejecutan DD OS versión 6.0.

Migración de replicación de directorio a MTree

La función de optimización de la replicación de directorio a MTree (D2M) le permite migrar contextos de replicación de directorio existentes a nuevos contextos de replicación basados en MTrees, que son particiones lógicas del sistema de archivos. Esta función también le permite monitorear el proceso a medida que se desarrolla y verificar que se haya completado correctamente.

La función D2M es compatible con las versiones 5.6, 5.7 y 6.0 de Data Domain Operating System.

El sistema Data Domain de origen debe ejecutar DD OS 6.0 para usar esta función, pero el sistema de destino puede ejecutar 5.6, 5.7 o 6.0. Sin embargo, los beneficios de la optimización de rendimiento solo se ven cuando los sistemas de origen y de destino ejecutan 6.0.

Nota

Aunque puede utilizar la interfaz gráfica del usuario (GUI) para esta operación, se recomienda usar la interfaz de la línea de comandos (CLI) para un rendimiento óptimo.

Ejecución de migración de la replicación de directorio a la replicación de MTree

No apague ni reinicie el sistema durante la migración de directorio a MTree (D2M).

Procedimiento

1. Detenga todas las operaciones de recopilación en el directorio de origen de replicación.
2. Crear un MTree en el sistema DD de origen: `mtree create /data/col1/nombre-del-mtree`

Nota

No cree el MTree en el sistema DD de destino.

3. (Opcional) Habilite DD Retention Lock en el MTree.

Nota

Si el sistema de origen contiene archivos retention-locked, es posible que desee conservar DD Retention Lock en el nuevo MTree.

Consulte Activación de DD Retention Lock Compliance en un MTree.

4. Cree el contexto de replicación de MTree en los sistemas DD de origen y destino: **`replication add source mtree://`*`nombre-del-sistema-de-origen/mtree-de-origen`*` replication add destination mtree://`*`nombre-del-sistema-de-destino/mtree-de-destino`*
5. Inicie la migración de D2M: **`replication dir-to-mtree start from`** ***`rctx://1`*** **`to`** ***`rctx://2`***

   En el ejemplo anterior,
   `rctx://1`
   se refiere al contexto de replicación de directorio, que replica el directorio `backup backup/dir1` en el sistema de origen;
   `rctx://2`
   se refiere al contexto de replicación de MTree, que replica el MTree `/data/col1/mtree1` en el sistema de origen.

Nota

Este comando puede tardar más de lo esperado en completarse. No presione Ctrl-C durante este proceso; si lo hace, se cancelará la migración de D2M.

```
Phase 1 of 4 (precheck):
    Marking source directory /backup/dir1 as read-only...Done.

Phase 2 of 4 (sync):
    Syncing directory replication context...0 files flushed.
current=45 sync_target=47 head=47
current=45 sync_target=47 head=47
Done. (00:09)

Phase 3 of 4 (fastcopy):
    Starting fastcopy from /backup/dir1 to /data/col1/
mtree1...
    Waiting for fastcopy to complete...(00:00)
    Fastcopy status: fastcopy /backup/dir1 to /data/col1/
mtree1: copied 24
files, 1 directory in 0.13 seconds
    Creating snapshot 'REPL-D2M-
mtree1-2015-12-07-14-54-02'...Done

Phase 4 of 4 (initialize):
    Initializing MTree replication context...
(00:08) Waiting for initialize to start...
(00:11) Initialize started.
```

```
Use 'replication dir-to-mtree watch rctx://2' to monitor
progress.
```

Visualización del progreso de la migración de directorio a MTree

Puede ver qué etapa de la migración está en curso en la replicación de directorio a MTree (D2M).

Procedimiento

1. Escriba **`replication dir-to-mtree watch rctx://2`** para ver el progreso.

   `rctx://2`
   especifica el contexto de replicación.

   Debería ver la siguiente salida:

```
Use Control-C to stop monitoring.
Phase 4 of 4 (initialize).
(00:00) Replication initialize started...
(00:02) initializing:
(00:14)     100% complete, pre-comp: 0 KB/s, network: 0 KB/
s
(00:14) Replication initialize completed.
Migration for ctx 2 successfully completed.
```

Comprobación del estado de la migración de replicación de directorio a MTree

Puede usar el comando `replication dir-to-mtree status` para comprobar si la migración de directorio a MTree (D2M) se completó satisfactoriamente.

Procedimiento

1. Escriba el siguiente comando; aquí,
   `rctx://2`
   representa el contexto de replicación de MTree en el sistema de origen:
   `replication dir-to-mtree status rctx://2`

   La salida debe ser similar a lo siguiente:

```
Directory Replication CTX:          1
MTree Replication CTX:              2
Directory Replication Source:       dir://127.0.0.2/backup/dir1
MTree Replication Source:           mtree://127.0.0.2/data/
col1/mtree1
MTree Replication Destination:      mtree://127.0.0.3/data/
col1/mtree1
Migration Status:                   completed
```

   Si no hay ninguna migración en curso, debería ver lo siguiente:

```
# replication dir-to-mtree status rctx://2
No migration status for context 2.
```

2. Comience a recopilar datos para el MTree en el sistema DD de origen una vez finalizado el proceso de migración.
3. (Opcional) Divida el contexto de replicación de directorio en los sistemas de origen y destino.

Consulte la *Guía de referencia de comandos de Data Domain Operating System versión 6.0* para obtener más información acerca del comando `replication break`.

Anulación de la replicación de D2M

Si es necesario, puede anular el procedimiento de migración de directorio a MTree (D2M).

El comando `replication dir-to-mtree abort` anula el proceso de migración en curso y revierte el directorio del estado de solo lectura al de lectura y escritura.

Procedimiento

1. En la interfaz de la línea de comandos (CLI), escriba el siguiente comando; aquí, `rctx://2`
   es el contexto de replicación de MTree: **`replication dir-to-mtree abort rctx://2`**

   Debería ver la siguiente salida:

   ```
   Canceling directory to MTree migration for context dir-name.
   Marking source directory dir-name as read-write...Done.
   The migration is now aborted.
   Remove the MTree replication context and MTree on both source
   and destination
   host by running 'replication break' and 'mtree delete'
   commands.
   ```

2. Divida el contexto de replicación de MTree: **`replication break rctx://2`**
3. Elimine el MTree en el sistema de origen: **`mtree delete ruta-de-mtree`**

Solución de problemas de D2M

Si se produce un error al configurar una replicación de directorio a MTree (D2M), hay una operación que puede realizar para resolver diversos problemas.

El procedimiento `dir-to-mtree abort` puede ayudar a anular correctamente el proceso de D2M. Debe ejecutar este procedimiento en los siguientes casos:

- El estado de la migración de D2M aparece como migración anulada.
- El sistema Data Domain se reinició durante la migración de D2M.
- Se produjo un error al ejecutar un comando `replication dir-to-mtree start`.
- La recopilación no se detuvo antes de iniciar la migración.
- El contexto de replicación de MTree se inicializó antes de que se introdujera el comando `replication dir-to-mtree start`.

Nota

No ejecute **`replication break`** en el contexto de replicación de MTree antes de que finalice el proceso de D2M.
Ejecute siempre **`replication dir-to-mtree abort`** antes de ejecutar el comando **`replication break`** en ctx mrepl.

La ejecución del comando **`replication break`** de manera prematura hará que el directorio de origen drepl sea de solo lectura permanentemente.

Si esto ocurre, comuníquese con el servicio de soporte.

Procedimiento

1. Escriba **`replication dir-to-mtree abort`** para anular el proceso.
2. Divida el contexto de replicación de MTree recién creado en el origen y el destino de los sistemas Data Domain.

   En el siguiente ejemplo, el contexto de replicación de MTree es `rctx://2`
   .

   ```
   replication break rctx://2
   ```

3. Elimine los MTrees correspondientes de los sistemas de origen y destino.

   ```
   mtree delete mtree-path
   ```

   Nota

   Los MTrees marcados para eliminación permanecen en el sistema de archivos hasta que se ejecuta el comando `filesys clean`.

   Consulte la *Guía de referencia de comandos de Data Domain Operating System, versión 6.0* para obtener más información.

4. Tanto en los sistemas de origen como en los de destino, ejecute el comando `filesys clean start`.

   Para obtener más información sobre los comandos `filesys clean`, consulte la *Guía de referencia de comandos de Data Domain Operating System, versión 6.0*.

5. Reinicie el proceso.

   Consulte Ejecución de migración de la replicación de directorio a la replicación de MTree.

Solución de problemas de D2M adicionales

Hay soluciones disponibles si olvidó habilitar DD Retention Lock para el nuevo MTree o si se produce un error después de que se ha inicializado la migración de directorio a MTree.

DD Retention Lock no se habilitó.
Si olvidó habilitar DD Retention Lock para el nuevo MTree y el directorio de origen contiene archivos o directorios retention-locked, tiene las siguientes opciones:

- Permitir que la migración de D2M continúe. Sin embargo, no tendrá la información de DD Retention Lock en el MTree después de la migración.
- Anular el proceso actual de D2M como se describe en Anulación de la replicación de D2M en la página 488 y reiniciar el proceso con DD Retention Lock habilitado en el MTree de origen.

Se produce un error después de la inicialización

Si el proceso `replication dir-to-mtree start` finaliza sin errores, pero se detecta un error durante la inicialización de la replicación de MTree (fase 4 del proceso de migración de D2M), puede realizar los siguientes pasos:

1. Asegurarse de que no haya ningún problema de red.
2. Inicializar el contexto de replicación.

Uso de la replicación de recopilaciones para la recuperación ante desastres con SMT

Para utilizar el sistema de destino de un par de replicación de recopilaciones configurado con SMT como un sistema de reemplazo para la recuperación de desastres, deben realizarse pasos de configuración de SMT adicionales además de otros pasos de configuración necesarios para poner un sistema de reemplazo en línea.

Antes de comenzar

Utilizar el sistema de destino de replicación de recopilaciones de esta manera requiere que se configuren y se guarden informes de soporte automático. El artículo de la base de conocimientos *Réplica de recopilaciones con smt activado*, disponible en https://support.emc.com, proporciona información adicional.

El sistema de reemplazo no tendrá los siguientes detalles de SMT:

- Listas de notificación de alerta para cada unidad de grupos de usuarios
- Todos los usuarios asignados al protocolo DD Boost que pueden utilizar los grupos de usuarios de SMT, si DD Boost está configurado en el sistema
- La unidad de grupo de usuarios predeterminada asociada con cada usuario de DD Boost, si corresponde, si DD Boost está configurado en el sistema

Complete los siguientes pasos para configurar SMT en el sistema de reemplazo.

Procedimiento

1. En el informe de soporte automático, ubique la salida del comando `smt tenant-unit show detailed`.

```
Tenant-unit: "tu1"
Summary:
Name   Self-Service   Number of Mtrees   Types          Pre-Comp(GiB)
----   ------------   ----------------   --------       -------------
tu1    Enabled        2                  DD Boost       2.0
----   ------------   ----------------   --------       -------------

Management-User:
User     Role
------   ------------
tu1_ta   tenant-admin
tu1_tu   tenant-user
tum_ta   tenant-admin
------   ------------

Management-Group:
Group    Role
------   ------------
```

```
qatest   tenant-admin
------   ------------

DDBoost:
Name   Pre-Comp (GiB)   Status   User    Tenant-Unit
----   --------------   ------   -----   -----------
su1               2.0   RW/Q     ddbu1   tu1
----   --------------   ------   -----   -----------
Q    : Quota Defined
RO   : Read Only
RW   : Read Write

Getting users with default-tenant-unit tu1
DD Boost user   Default tenant-unit
-------------   -------------------
ddbu1           tu1
-------------   -------------------

Mtrees:
Name             Pre-Comp (GiB)   Status   Tenant-Unit
--------------   --------------   ------   -----------
/data/col1/m1               0.0   RW/Q     tu1
/data/col1/su1              2.0   RW/Q     tu1
--------------   --------------   ------   -----------
D    : Deleted
Q    : Quota Defined
RO   : Read Only
RW   : Read Write
RD   : Replication Destination
RLGE : Retention-Lock Governance Enabled
RLGD : Retention-Lock Governance Disabled
RLCE : Retention-Lock Compliance Enabled

Quota:
Tenant-unit: tu1
Mtree            Pre-Comp (MiB)   Soft-Limit (MiB)   Hard-Limit(MiB)
--------------   --------------   ----------------   ----------------
/data/col1/m1                 0              71680             81920
/data/col1/su1             2048              30720             51200
--------------   --------------   ----------------   ----------------

Alerts:
Tenant-unit: "tu1"
Notification list "tu1_grp"
Members
------------------
tom.tenant@abc.com
------------------

No such active alerts.
```

2. En el sistema de reemplazo, habilite SMT si todavía no está habilitado.
3. En el sistema de reemplazo, obtenga la licencia y habilite DD Boost si es necesario y todavía no está habilitado.
4. Si DD Boost está configurado, asigne cada usuario enumerado en la sección `DD Boost` de la salida "smt tenant-unit show detailed" como un usuario de DD Boost.

   ```
   # ddboost user assign ddbu1
   ```

5. Si DD Boost está configurado, asigne cada usuario enumerado en la sección `DD Boost` de la salida `smt tenant-unit show detailed` a la unidad de grupos de usuarios predeterminada que se muestra, si corresponde, en la salida.

   ```
   # ddboost user option set ddbu1 default-tenant-unit tu1
   ```

6. Cree un nuevo grupo de notificaciones de alerta con el mismo nombre que el grupo de notificaciones de alerta en la sección `Alerts` de la salida `smt tenant-unit show detailed`.

```
# alert notify-list create tu1_grp tenant-unit tu1
```

7. Asigne cada dirección de correo electrónico en el grupo de notificación de alerta en la sección `Alerts` de la salida `smt tenant-unit show detailed` al nuevo grupo de notificación de alerta.

```
# alert notify-list add tu1_grp emails tom.tenant@abc.com
```

CAPÍTULO 17

Multiusuario seguro de DD

Este capítulo incluye:

- Descripción general de multiusuario seguro de Data Domain 494
- Aprovisionamiento de una unidad de grupos de usuario 498
- Activación del modo Tenant Self-Service 502
- Acceso a datos por protocolo 502
- Operaciones de administración de datos 504

Descripción general de multiusuario seguro de Data Domain

Multiusuario seguro (SMT) de Data Domain se refiere al alojamiento de una infraestructura de TI por parte de un departamento de TI interno o un proveedor de servicios externo para más de un consumidor o una carga de trabajo (unidad de negocios, departamento o grupo de usuarios) simultáneamente.

SMT proporciona la capacidad de aislar de forma segura varios usuarios y cargas de trabajo en una infraestructura compartida, de manera que las actividades de un grupo de usuarios no son evidentes ni estén visibles para los otros grupos de usuarios.

Un *grupo de usuarios* es un consumidor (unidad de negocios, departamento o cliente) que mantiene una presencia persistente en un ambiente alojado.

Dentro de una empresa, un grupo de usuarios puede constar de uno o más departamentos o unidades de negocios en un sistema Data Domain configurado y administrado por el personal de TI.

- Para un caso de uso de una unidad de negocios (BU), los departamentos de Finanzas y Recursos Humanos de una empresa podrían compartir el mismo sistema Data Domain sin que uno advirtiera la presencia del otro.
- Para un caso de uso de un proveedor de servicios (SP), el SP podría implementar uno o varios sistemas Data Domain para admitir diversos servicios de almacenamiento de protección para varios clientes finales.

Ambos casos de uso enfatizan la segregación de datos de distintos clientes en el mismo sistema Data Domain físico.

Aspectos básicos de la arquitectura de SMT

La función de multiusuario seguro (SMT) proporciona un enfoque simple para la configuración de grupos de usuarios y unidades de grupo de usuarios, mediante MTrees. La configuración SMT se realiza mediante la interfaz de línea de comandos de DD OS o DD Management Center. Esta guía de administración proporciona la teoría de SMT y algunos instrucciones generales de la línea de comandos.

La arquitectura básica de SMT es la siguiente.

- Se crea un grupo de usuarios en el sistema DD o DD Management Center.
- Se crea una unidad de grupo de usuarios en un sistema DD para el grupo de usuarios.
- Se crean uno o varios MTrees para satisfacer los requisitos de almacenamiento de los diferentes tipos de respaldo del grupo de usuarios.
- Los MTrees creados recientemente se agregan a la unidad de grupo de usuarios.
- Las aplicaciones de respaldo se configuran para enviar cada respaldo a su MTree de unidad de grupo de usuarios configurado.

Nota

Para obtener más información sobre DD Management Center, consulte *DD Management Center User Guide*. Para obtener más información acerca de la interfaz de línea de comandos de DD OS, consulte *DD OS Command Reference*.

Terminología utilizada en multiusuario seguro (SMT)

Comprender la terminología utilizada en SMT le permitirá comprender mejor este ambiente único.

MTrees
Los *MTrees* son particiones lógicas del sistema de archivos que ofrecen el grado más alto de granularidad de administración, lo que significa que los usuarios pueden ejecutar operaciones en un MTree específico sin afectar a todo el sistema de archivos. Los MTrees se asignan a las unidades de grupo de usuarios y contienen las configuraciones individualizadas de esa unidad de grupo de usuarios para administrar y monitorear SMT.

Multiusuario
Multiusuario se refiere al alojamiento de una infraestructura de TI por parte de un departamento de TI interno o un proveedor de servicios externo para más de un consumidor o carga de trabajo (unidad de negocios, departamento, grupo de usuarios). Data Domain SMT habilita la *protección de datos como servicio*.

RBAC (Control de acceso basado en funciones)
El *RBAC* ofrece diversas funciones con distintos niveles de privilegio, que se combinan para proporcionar el aislamiento administrativo en un sistema Data Domain multiusuario. (En la siguiente sección, se definen estas funciones).

Storage Unit
Una *unidad de almacenamiento* es un MTree configurado para el protocolo DD Boost. El aislamiento de datos se logra creando una unidad de almacenamiento y asignándola a un usuario de DD Boost. El protocolo DD Boost solo permite el acceso a las unidades de almacenamiento asignadas a los usuarios de DD Boost conectados al sistema Data Domain.

Grupo de usuarios
Un *grupo de usuarios* es un consumidor (unidad de negocios, departamento o cliente) que mantiene una presencia persistente en un ambiente alojado.

Autoservicio de grupo de usuarios
El *autoservicio de grupo de usuarios* es un método que permite que un grupo de usuarios inicie sesión en un sistema Data Domain para realizar algunos servicios básicos (agregar, editar o eliminar usuarios locales; grupos de NIS; o grupos de AD). Esto reduce el cuello de botella de siempre tener que depender de un administrador para estas tareas básicas. El grupo de usuarios puede acceder solamente a sus unidades de grupos de usuarios asignadas. Desde luego, los usuarios de grupos de usuarios y los administradores de grupos de usuarios tendrá privilegios diferentes.

Unidad de grupo de usuarios
Una *unidad de grupo de usuarios* es la partición de un sistema Data Domain que funciona como la unidad de aislamiento administrativo entre grupos de usuarios. Las unidades de grupo de usuarios que se asignan a un grupo de usuarios en el mismo sistema Data Domain o en sistemas Data Domain diferentes están protegidas y lógicamente aisladas una de otra, lo cual garantiza la seguridad y el aislamiento de la ruta de control al ejecutar diversos grupos de usuarios simultáneamente en la infraestructura compartida. Las unidades de grupo de usuarios contienen uno o varios *MTrees*, que contienen todos los elementos de configuración necesarios en una configuración multiusuario. Los usuarios, los grupos de administración, los grupos de notificaciones y otros elementos de configuración son parte de una unidad de grupo de usuarios.

Aislamiento de red y ruta de control

El *aislamiento de rutas de control* se logra proporcionando las funciones de usuario de *administrador de grupo de usuarios* y *usuario de grupo de usuarios* para una unidad de grupo de usuarios. El *aislamiento de red* de datos y acceso administrativo se logra mediante la asociación de un conjunto fijo de *direcciones IP de acceso a datos* y *direcciones IP de administración* con una unidad de grupo de usuarios.

Las funciones de *administrador de grupo de usuarios* y *usuario de grupo de usuarios* se limitan en alcance y capacidad a unidades de grupo de usuarios específicas y a un conjunto limitado de operaciones que pueden ejecutar en estas unidades. Para garantizar una ruta de datos lógicamente segura y aislada, un administrador del sistema debe configurar uno o varios MTrees de unidades de grupo de usuarios para cada protocolo en un ambiente SMT. Los protocolos compatibles incluyen DD Boost, NFS, CIFS y DD VTL. El acceso está estrictamente regulado por los mecanismos de control de acceso nativos de cada protocolo.

Las *sesiones de grupos de usuarios de autoservicio* (por medio de ssh) pueden restringirse a un conjunto fijo de *direcciones IP de administración* en un sistema DD. Las sesiones de acceso administrativo (por medio de ssh/http/https) también pueden restringirse a un conjunto fijo de direcciones IP de administración en sistemas DD. Sin embargo, de forma predeterminada, no hay direcciones IP de administración asociadas con una unidad de grupo de usuarios, por lo que es la restricción de solo estándar es mediante las funciones de *administrador de grupo de usuarios* y *usuario de grupo de usuarios*. Debe utilizar `smt tenant-unit management-ip` para agregar y mantener direcciones IP de administración para las unidades de grupo de usuarios.

De manera similar, el acceso a los datos y el flujo de datos (desde y hacia las unidades de grupo de usuarios) pueden restringirse a un conjunto fijo de *direcciones IP de acceso a datos* locales o remotas. El uso de direcciones IP de acceso a datos asignadas mejora la seguridad de los protocolos de DD Boost y NFS mediante la adición de las verificaciones de seguridad relacionadas con SMT. Por ejemplo, la lista de unidades de almacenamiento arrojadas por RPC de DD Boost puede limitarse a aquellas que pertenecen a la unidad de grupo de usuarios con la dirección IP de acceso a datos local asignada. Para NFS, el acceso y la visibilidad de las exportaciones se pueden filtrar en función de las direcciones IP de acceso a datos locales configuradas. Por ejemplo, el uso de `showmount -e` de la dirección IP de acceso a datos local de una unidad de grupo de usuarios solo mostrará las exportaciones NFS que pertenecen a esa unidad de grupo de usuarios.

El *sysadmin* debe usar `smt tenant-unit data-ip` para agregar y mantener direcciones IP de acceso a datos para unidades de grupo de usuarios.

Nota

Si intenta montar un MTree en un SMT usando una dirección IP que no es de SMT, la operación fallará.

Si varias unidades de grupo de usuarios pertenecen al mismo grupo de usuarios, pueden compartir un gateway predeterminado. Sin embargo, varias unidades de grupo de usuarios que pertenecen a diferentes grupos de usuarios no pueden utilizar el mismo gateway predeterminado.

Varias unidades de grupo de usuarios que pertenecen al mismo grupo de usuarios pueden compartir un gateway predeterminado. Las unidades de grupo de usuarios que pertenecen a diferentes grupos de usuarios no pueden usar el mismo gateway predeterminado.

Comprensión de RBAC en SMT

En SMT (multiusuario seguro), el permiso para ejecutar una tarea depende de la función asignada a un usuario. DD Management Center usa RBAC (control de acceso basado en funciones) para controlar estos permisos.

Todos los usuarios de DD Management Center pueden hacer lo siguiente:

- Ver todos los grupos de usuarios
- Crear, leer, actualizar o eliminar unidades de grupo de usuarios que corresponden a cualquier grupo de usuarios si el usuario es un administrador en el sistema Data Domain que aloja la unidad
- Asignar o cancelar la asignación de unidades de grupo de usuarios hacia o desde un grupo de usuarios si el usuario es un administrador del sistema Data Domain que aloja la unidad
- Ver las unidades de grupo de usuarios que pertenecen a cualquier grupo de usuarios si el usuario tiene una función asignada en el sistema Data Domain que aloja la unidad

Ejecutar tareas más avanzadas según la función del usuario, de la siguiente manera:

Función admin
Un usuario con una función *admin* puede ejecutar todas las operaciones administrativas en un sistema Data Domain. Un *admin* también puede ejecutar todas las operaciones administrativas de SMT en un sistema Data Domain, incluida la configuración de SMT, la asignación de funciones de usuarios de SMT, la habilitación del modo de autoservicio de grupos de usuarios, la creación de un grupo de usuarios, etc. En un contexto de SMT, suele referirse al *admin* como el *propietario*. En DD OS, la función se conoce como *sysadmin*.

Para tener permiso para editar o eliminar un grupo de usuarios, debe ser un *admin* de DD Management Center y un *sysadmin* de un DD OS en todos los sistemas Data Domain que están asociados con las unidades de grupo de usuarios de ese grupo. Si el grupo de usuarios no tiene ninguna unidad de grupo de usuarios, solo debe ser un *admin* de DD Management Center para editar o eliminar ese grupo de usuarios.

Función limited-admin
Un usuario con una función *limited-admin* puede ejecutar las mismas operaciones administrativas en un sistema Data Domain que un usuario con la función *admin*. Sin embargo, los usuarios con la función *limited-admin* no pueden eliminar ni destruir MTrees. En DD OS, existe una función equivalente a *limited-admin*.

Función tenant-admin
Un usuario con una función *tenant-admin* puede ejecutar ciertas tareas solo cuando el modo *Tenant Self-Service* está habilitado para una unidad de grupo de usuarios. Entre las responsabilidades, se incluyen la programación y la ejecución de una aplicación de respaldo para el grupo de usuarios y el monitoreo de recursos y estadísticas dentro de la unidad de grupo de usuarios asignada. El *tenant-admin* puede ver registros de auditoría, pero RBAC asegura que solo los registros de auditoría de las unidades de grupo de usuarios que pertenecen al *tenant-admin* sean accesibles. Además, los *administradores de grupos de usuarios* garantizan la separación administrativa cuando el modo Tenant Self-Service está habilitado. En el contexto de SMT, es normal referirse al *tenant-admin* como el *backup admin*.

Función tenant-user
Los usuarios con la función *tenant-user* pueden monitorear el rendimiento y el uso de componentes de SMT solo en las unidades de grupo de usuarios asignadas a estos y solo cuando el modo de autoservicio de grupos de usuarios está habilitado, pero un

usuario con esa función no puede visualizar registros de auditoría para las unidades de grupos de usuarios asignadas. Además, los *usuarios de grupos de usuarios* pueden ejecutar los comandos `show` y `list` .

Sin función

Un usuario con la función *none* no puede ejecutar ninguna operación en un sistema Data Domain, excepto cambiar su contraseña y acceder a datos mediante DD Boost. Sin embargo, una vez que SMT se habilita, el *admin* puede seleccionar un usuario con la función *none* del sistema Data Domain y asignarle una función específica de SMT como *tenant-admin* o *tenant-user*. Luego, ese usuario puede ejecutar operaciones en objetos de administración de SMT.

Grupos de administración

Los BSP (proveedores de servicio de respaldo) pueden usar *grupos de administración* definidos en un único AD (Active Directory) o NIS (servicio de información de red) para simplificar la administración de funciones de usuario en las unidades de grupo de usuarios. Cada grupo de usuarios de BSP puede ser una empresa externa y separada y puede usar un servicio como AD o NIS.

Con los grupos de administración de SMT, los servidores de AD y NIS son instalados y configurados por el *admin* de la misma forma que los usuarios locales de SMT. El *admin* puede solicitar a su administrador de AD o NIS que cree y complete el grupo. El *admin* luego asigna una función de SMT a todo el grupo. Cualquier usuario dentro del grupo que inicia sesión en el sistema Data Domain se registra con la función asignada al grupo.

Cuando los usuarios abandonan una empresa de grupo de usuarios o se unen a esta, pueden ser quitados o agregados al grupo por el administrador de AD o NIS. No es necesario modificar la configuración de RBAC en un sistema Data Domain cuando se agregan o se quitan los usuarios que son parte del grupo.

Aprovisionamiento de una unidad de grupos de usuario

Al iniciar el asistente de configuración, comience el procedimiento de aprovisionamiento inicial para la seguridad de multiusuario (SMT). Durante el procedimiento, el asistente crea y provisiona una nueva unidad de grupos de usuario según los requisitos de configuración del grupo de usuarios. El administrador introduce la información a medida que se le indica. Después de completar el procedimiento, el administrador procede con el siguiente conjunto de tareas, comenzando con la habilitación del modo de autoservicio de grupo de usuarios. Después de la configuración inicial, los procedimientos manuales y las modificaciones de configuración pueden realizarse según sea necesario.

Procedimiento

1. Inicie SMT.

   ```
   # smt enable SMT enabled.
   ```

2. Compruebe que SMT esté activado.

   ```
   # smt status SMT is enabled.
   ```

3. Inicie el asistente de configuración de SMT.

   ```
   # smt tenant-unit setup No tenant-units.
   ```

4. Siga los indicadores de configuración.

```
SMT TENANT-UNIT Configuration

  Configure SMT TENANT-UNIT at this time (yes|no) [no]: yes

  Do you want to create new tenant-unit (yes/no)? : yes
```

```
Tenant-unit Name
  Enter tenant-unit name to be created
  : SMT_5.7_tenant_unit
Invalid tenant-unit name.
  Enter tenant-unit name to be created
  : SMT_57_tenant_unit

Pending Tenant-unit Settings
Create Tenant-unit   SMT_57_tenant_unit

Do you want to save these settings (Save|Cancel|Retry): save
SMT Tenant-unit Name Configurations saved.

SMT TENANT-UNIT MANAGEMENT-IP Configuration

  Configure SMT TENANT-UNIT MANAGEMENT-IP at this time (yes|no) [no]: yes

  Do you want to add a local management ip to this tenant-unit? (yes|no) [no]: yes

port  enabled  state  DHCP        IP address              netmask     type additional
                                                       /prefix length        setting
----- ------- ------- ---- -------------------------- -------------- ---- ----------
ethMa   yes   running  no  192.168.10.57              255.255.255.0   n/a
                           fe80::260:16ff:fe49:f4b0** /64
eth3a   yes   running ipv4 192.168.10.236*            255.255.255.0*  n/a
                           fe80::260:48ff:fe1c:60fc** /64
eth3b   yes   running  no  192.168.50.57              255.255.255.0   n/a
                           fe80::260:48ff:fe1c:60fd** /64
eth4b   yes   running  no  192.168.60.57              255.255.255.0   n/a
                           fe80::260:48ff:fe1f:5183** /64
----- ------- ------- ---- -------------------------- -------------- ---- ----------
* Value from DHCP
** auto_generated IPv6 address

Choose an ip from above table or enter a new ip address. New ip addresses will need
to be created manually.

Ip Address
  Enter the local management ip address to be added to this tenant-unit
  : 192.168.10.57

  Do you want to add a remote management ip to this tenant-unit? (yes|no) [no]:

Pending Management-ip Settings

Add Local Management-ip    192.168.10.57
  Do you want to save these settings (Save|Cancel|Retry): yes
  unrecognized input, expecting one of Save|Cancel|Retry

  Do you want to save these settings (Save|Cancel|Retry): save
  Local management access ip "192.168.10.57" added to tenant-unit "SMT_57_tenant_unit".

SMT Tenant-unit Management-IP Configurations saved.

SMT TENANT-UNIT MANAGEMENT-IP Configuration

  Do you want to add another local management ip to this tenant-unit? (yes|no) [no]:

  Do you want to add another remote management ip to this tenant-unit? (yes|no) [no]:

SMT TENANT-UNIT DDBOOST Configuration
  Configure SMT TENANT-UNIT DDBOOST at this time (yes|no) [no]:

SMT TENANT-UNIT MTREE Configuration
  Configure SMT TENANT-UNIT MTREE at this time (yes|no) [no]: yes

Name                       Pre-Comp (GiB)   Status   Tenant-Unit
-------------------------  --------------   ------   -----------
/data/col1/laptop_backup          4846.2   RO/RD     -
```

```
/data/col1/random                 23469.9   RO/RD     -
/data/col1/software2               2003.7   RO/RD     -
/data/col1/tsm6                  763704.9   RO/RD     -
------------------------   --------------   ------   -----------
D    : Deleted
Q    : Quota Defined
RO   : Read Only
RW   : Read Write
RD   : Replication Destination
RLGE : Retention-Lock Governance Enabled
RLGD : Retention-Lock Governance Disabled
RLCE : Retention-Lock Compliance Enabled

  Do you want to assign an existing MTree to this tenant-unit? (yes|no) [no]:

  Do you want to create a mtree for this tenant-unit now? (yes|no) [no]: yes

MTree Name
  Enter MTree name
  :  SMT_57_tenant_unit
Invalid mtree path name.
  Enter MTree name
  :
SMT_57_tenant_unit


Invalid mtree path name.
  Enter MTree name
  : /data/col1/SMT_57_tenant_unit

MTree Soft-Quota
  Enter the quota soft-limit to be set on this MTree (<n> {MiB|GiB|TiB|PiB}|none)
  :

MTree Hard-Quota
  Enter the quota hard-limit to be set on this MTree (<n> {MiB|GiB|TiB|PiB}|none)
  :

Pending MTree Settings
Create MTree        /data/col1/SMT_57_tenant_unit
MTree Soft Limit    none
MTree Hard Limit    none

  Do you want to save these settings (Save|Cancel|Retry): save
  MTree "/data/col1/SMT_57_tenant_unit" created successfully.
  MTree "/data/col1/SMT_57_tenant_unit" assigned to tenant-unit  "SMT_57_tenant_unit".

SMT Tenant-unit MTree Configurations saved.

SMT TENANT-UNIT MTREE Configuration

Name                       Pre-Comp (GiB)   Status   Tenant-Unit
------------------------   --------------   ------   -----------
/data/col1/laptop_backup          4846.2   RO/RD     -
/data/col1/random                23469.9   RO/RD     -
/data/col1/software2              2003.7   RO/RD     -
/data/col1/tsm6                 763704.9   RO/RD     -
------------------------   --------------   ------   -----------
D    : Deleted
Q    : Quota Defined
RO   : Read Only
RW   : Read Write
RD   : Replication Destination
RLGE : Retention-Lock Governance Enabled
RLGD : Retention-Lock Governance Disabled
RLCE : Retention-Lock Compliance Enabled

  Do you want to assign another MTree to this tenant-unit? (yes|no) [no]: yes

  Do you want to assign an existing MTree to this tenant-unit? (yes|no) [no]:
```

```
  Do you want to create another mtree for this tenant-unit? (yes|no) [no]:

SMT TENANT-UNIT SELF-SERVICE Configuration

  Configure SMT TENANT-UNIT SELF-SERVICE at this time (yes|no) [no]: yes
  Self-service of this tenant-unit is disabled

  Do you want to enable self-service of this tenant-unit? (yes|no) [no]: yes

  Do you want to configure a management user for this tenant-unit? (yes|no) [no]:

  Do you want to configure a management group for this tenant-unit (yes|no) [no]: yes

Management-Group Name
  Enter the group name to be assigned to this tenant-unit
  : SMT_57_tenant_unit_group

What role do you want to assign to this group  (tenant-user|tenant-admin) [tenant-user]:
tenant-admin

Management-Group Type
  What type do you want to assign to this group (nis|active-directory)?
  : nis

Pending Self-Service Settings
Enable Self-Service       SMT_57_tenant_unit
Assign Management-group   SMT_57_tenant_unit_group
Management-group role     tenant-admin
Management-group type     nis

  Do you want to save these settings (Save|Cancel|Retry): save
  Tenant self-service enabled for tenant-unit "SMT_57_tenant_unit"
  Management group "SMT_57_tenant_unit_group" with type "nis" is assigned to tenant-unit
  "SMT_57_tenant_unit" as "tenant-admin".

SMT Tenant-unit Self-Service Configurations saved.

SMT TENANT-UNIT SELF-SERVICE Configuration

  Do you want to configure another management user for this tenant-unit? (yes|no) [no]:

  Do you want to configure another management group for this tenant-unit? (yes|no)
[no]:

SMT TENANT-UNIT ALERT Configuration

  Configure SMT TENANT-UNIT ALERT at this time (yes|no) [no]: yes
  No notification lists.

Alert Configuration

Alert Group Name
  Specify alert notify-list group name to be created
  : SMT_57_tenant_unit_notify

Alert email addresses
  Enter email address to receive alert for this tenant-unit
  : dd_proserv@emc.com

  Do you want to add more emails (yes/no)?
  : no

Pending Alert Settings
Create Notify-list group   SMT_57_tenant_unit_notify
Add emails                 dd_proserv@emc.com

  Do you want to save these settings (Save|Cancel|Retry): save
  Created notification list "SMT_57_tenant_unit_notify" for tenant "SMT_57_tenant_unit".
  Added emails to notification list "SMT_57_tenant_unit_notify".
```

```
SMT Tenant-unit Alert Configurations saved.

Configuration complete.
```

Activación del modo Tenant Self-Service

Para la separación administrativa de responsabilidades y la delegación de tareas administrativas para implementar el autoservicio de grupo de usuarios, que se requiere para el aislamiento de rutas de control, el administrador del sistema puede habilitar este modo en una unidad de grupos de usuario y luego asignar los usuarios para administrar la unidad en las funciones de administrador de grupo de usuarios y grupo de usuarios-usuario. Con estas funciones, los usuarios que no son administradores pueden ejecutar tareas específicas en la unidad de grupo de usuarios que se les asignó. Además de la separación administrativa, el modo Tenant Self-Service ayuda a reducir la carga administrativa del personal del proveedor de servicios y de TI interno.

Procedimiento

1. Vea el estado del modo Tenant Self-Service para una o todas las unidades de grupo de usuarios.

   ```
   # smt tenant-unit option show { tenant-unit | all }
   ```

2. Active el modo Tenant Self-Service en una unidad de grupo de usuarios seleccionada.

   ```
   # smt tenant-unit option set tenant-unit self-service { enabled
   | disabled }
   ```

Acceso a datos por protocolo

Las rutas de datos seguras, con controles de acceso específicos del protocolo, habilitan la seguridad y el aislamiento para las unidades de grupo de usuarios. En un ambiente Secure Multitenancy (SMT), los comandos de administración de protocolos de acceso a datos también se optimizan con el parámetro de unidad de grupo de usuarios para permitir la creación de informes consolidada.

Los sistemas de DD admiten diversos protocolos de acceso a datos simultáneamente, incluidos DD Boost, NFS, CIFS y DD VTL. Un sistema DD se puede presentar como una interfaz específica de la aplicación, como un servidor de archivos que ofrece acceso a NFS o CIFS a través de Ethernet, un dispositivo DD VTL o un dispositivo DD Boost.

Los mecanismos de control de acceso nativo de cada protocolo admitido garantizan que las rutas de datos para cada grupo de usuarios permanezcan separadas y aisladas. Estos mecanismos incluyen listas de control de acceso (ACL) para CIFS, exportaciones para NFS, credenciales de DD Boost y control de acceso orientado a las credenciales multiusuario de Boost.

DD Boost para varios usuarios y unidades de almacenamiento en SMT

Al usar DD Boost de múltiples usuarios con SMT (multiusuario seguro), los permisos de usuario se establecen según la propiedad de la unidad de almacenamiento.

DD Boost para varios usuarios se refiere al uso de diversas credenciales de usuario de DD Boost para el control de acceso a DD Boost, en el cual cada usuario tiene un nombre y una contraseña individuales.

Una *unidad de almacenamiento* es un MTree configurado para el protocolo DD Boost. Un usuario se puede asociar con una o más unidades de almacenamiento, o ser "propietario" de estas. Las unidades de almacenamiento que son propiedad de un

usuario no pueden pertenecer a otro. Por lo tanto, solo el usuario que es propietario de la unidad de almacenamiento puede acceder a esta para cualquier tipo de acceso a datos, como respaldo/restauración. La cantidad de nombres de usuarios de DD Boost no puede exceder la cantidad máxima de MTrees. (Consulte en el capítulo “MTrees” de este libro la cantidad máxima actual de MTrees para cada modelo de DD). Las unidades de almacenamiento que están asociadas con SMT deben tener asignadas la función *none*.

Cada aplicación de respaldo debe autenticarse con su nombre de usuario y contraseña de DD Boost. Después de la autenticación, DD Boost verifica las credenciales autenticadas para confirmar la propiedad de la unidad de almacenamiento. La aplicación de respaldo recibe acceso a la unidad de almacenamiento solo si la información de identificación del usuario presentada por la aplicación coinciden con los nombres de usuario asociados con la unidad de almacenamiento. Si la información de identificación y los nombres de usuario no coinciden, el trabajo falla con un error de permiso.

Configuración del acceso para CIFS

Common Internet File System (CIFS) es un protocolo de uso compartido de archivos para el acceso remoto a archivos. En una configuración Secure Multitenancy (SMT), los respaldos y las restauraciones requieren acceso de cliente a los recursos compartidos de CIFS que residen en el MTree de la unidad de grupo de usuarios asociada. El aislamiento de datos se logra usando los recursos compartidos de CIFS y las ACL de CIFS.

Procedimiento

1. Cree un MTree para CIFS y asigne el MTree a la unidad de grupo de usuarios.

   ```
   # mtree create ruta-de-mtree tenant-unit unidad-de-grupo-de-usuarios
   ```

2. Establezca cuotas de límite de advertencia y de límite máximo para el MTree.

   ```
   # mtree create ruta-de-mtree tenant-unit unidad-de-grupo-de-usuarios] [quota-soft-limit n{MiB|GiB|TiB|PiB} ] [quota-hard-limit n {MiB|GiB|TiB|PiB}
   ```

3. Cree un recurso compartido de CIFS para *pathname* del MTree.

   ```
   # cifs share create uso compartido path nombre de ruta clients clientes
   ```

Configuración del acceso a NFS

NFS es un protocolo de uso compartido de archivos basado en UNIX para el acceso remoto a archivos. En un ambiente Secure Multitenancy (SMT), los respaldos y las restauraciones requieren el acceso de cliente a exportaciones de NFS que residen en el MTree de la unidad de grupo de usuarios asociada. El aislamiento de datos se logra usando las exportaciones de NFS y el aislamiento de la red. NFS determina si un MTree está asociado con una unidad de grupo de usuarios aislada por la red. De ser así, NFS verifica las propiedades de conexión asociadas con la unidad de grupo de usuarios. Entre las propiedades de conexión, se incluyen la dirección IP de destino y la interfaz o el nombre del host del cliente.

Procedimiento

1. Cree un MTree para NFS y asigne el MTree a la unidad de grupo de usuarios.

   ```
   # mtree create ruta-de-mtree tenant-unit unidad-de-grupo-de-usuarios
   ```

2. Establezca cuotas de límite de advertencia y de límite máximo para el MTree.

```
# mtree create ruta-de-mtree tenant-unit unidad-de-grupo-de-usuarios] [quota-soft-limit n{MiB|GiB|TiB|PiB} ] [quota-hard-limit n {MiB|GiB|TiB|PiB}
```

3. Cree una exportación de NFS agregando uno o más clientes al MTree.

```
# nfs add ruta de-la-lista-de-clientes
```

Configuración de acceso para DD VTL

El aislamiento de datos de grupos de usuarios de DD VTL se logra usando los grupos de acceso de DD VTL que crean una ruta de acceso virtual entre el sistema de host y DD VTL. (La conexión física de Fibre Channel entre el sistema de host y DD VTL ya debe existir).

Al colocar las cintas en DD VTL, se permite que la aplicación de respaldo las escriba y las lea en el sistema de host. Las cintas DD VTL se crean en un pool de DD VTL, que es un MTree. Debido a que los pools de DD VTL son MTrees, los pools pueden asignarse a las unidades de grupo de usuarios Esta asociación habilita el monitoreo y la creación de informes de SMT.

Por ejemplo, si a un administrador de grupo de usuarios se le asigna una unidad de grupo de usuarios que contiene un pool de DD VTL, puede ejecutar comandos MTree para que se muestre la información de solo lectura. Los comandos solo se pueden ejecutar en el pool de DD VTL asignado a la unidad de grupo de usuarios.

Estos pueden incluir los siguientes:

- `mtree list` para ver una lista de MTrees en la unidad de grupo de usuarios.
- `mtree show compression` para ver estadísticas acerca de la compresión de MTrees.
- `mtree show performance` para ver estadísticas acerca del rendimiento.

La salida de la mayoría de los comandos `list` y `show` incluye estadísticas que permiten que los proveedores de servicios midan el uso de espacio y calculen las tarifas de cobro retroactivo.

Las operaciones de DD VTL no se ven afectadas y continúan funcionando normalmente.

Uso de NDMP TapeServer de DD VTL

El aislamiento de datos de grupo de usuarios de DD VTL también se logra usando NDMP. El SO de DD implementa un servidor de cintas NDMP (Protocolo de administración de datos de red) que permite a los sistemas con capacidad de NDMP enviar datos de respaldo al sistema DD mediante un respaldo de tipo NDMP triple.

Los datos de respaldo son escritos en cintas virtuales (que se encuentran en un pool) por una DD VTL asignada a un *TapeServer* especial de grupo de DD VTL.

Debido a que los datos de respaldo se escriben en cintas en un pool, la información del tema DD VTL acerca de MTrees también se aplica a NDMP TapeServer de Data Domain.

Operaciones de administración de datos

Las operaciones de administración Secure Multitenancy (SMT) incluyen el monitoreo de unidades de grupos de usuarios y otros objetos, como las unidades de almacenamiento y las estructuras de datos MTrees. Para algunos objetos de SMT, es posible que se requieran configuraciones o modificaciones adicionales.

Obtención de estadísticas de rendimiento

Cada MTree puede medirse de acuerdo con las estadísticas de rendimiento o "uso" y otra información en tiempo real. Las tasas de consumo históricas están disponibles para las unidades de almacenamiento de DD Boost. El resultado del comando permite al administrador de grupo de usuarios obtener las estadísticas de uso y las relaciones de compresión para un MTree asociado con una unidad de grupos de usuario, o para todos los MTrees y las unidades de grupos de usuario asociadas. Los resultados pueden filtrarse para que se muestre el uso en intervalos de minutos a meses. Los resultados se pasan al administrador, que usa las estadísticas como métrica retroactiva. Se usa un método similar para recopilar estadísticas de uso y relaciones de compresión para unidades de almacenamiento.

Procedimiento

1. Obtenga estadísticas de rendimiento en tiempo real de MTree.

   ```
   # mtree show stats
   ```

2. Obtenga estadísticas de rendimiento para MTrees asociados con una unidad de grupo de usuarios.

   ```
   # mtree show performance
   ```

3. Obtenga estadísticas de compresión para MTrees asociados con una unidad de grupo de usuarios.

   ```
   # mtree show compression
   ```

Modificación de cuotas

Para cumplir con los criterios de QoS, un administrador de sistemas usa las "perillas" del SO de DD para ajustar los parámetros requeridos por la configuración del grupo de usuarios. Por ejemplo, el administrador puede definir los límites de cuotas "de advertencia" y "máximas" en las unidades de almacenamiento de DD Boost. Los límites de cuotas "de advertencia" y "máximas" de flujos de datos pueden asignarse solo a unidades de almacenamiento asignadas a unidades de grupo de usuarios. Una vez que el administrador define las cuotas, el administrador de grupo de usuarios puede supervisar una unidad de grupos de usuario o todas para garantizar que ningún objeto supere sus cuotas asignadas y prive a otros de los recursos del sistema.

Las cuotas se definen inicialmente cuando lo indica el asistente de configuración, pero se pueden ajustar o modificar más adelante. En el siguiente ejemplo, se muestra cómo modificar cuotas para DD Boost. (También puede usar `quota capacity` y `quota streams` para manejar las cuotas y los límites de capacidad y flujo de datos).

Procedimiento

1. Para modificar los límites de cuotas de advertencia y máximas en la unidad de almacenamiento de DD Boost "su33":

   ```
   ddboost storage-unit modify su33 quota-soft-limit 10 Gib quota-hard-limit 20 Gib
   ```

2. Para modificar los límites de flujo de datos de advertencia y máximos en la unidad de almacenamiento de DD Boost "su33":

   ```
   ddboost storage-unit modify su33 write-stream-soft-limit 20 read-stream-soft-limit 6 repl -stream-soft-limit 20 combined-stream-soft-limit 20
   ```

3. Para informar el tamaño físico para la unidad de almacenamiento de DD Boost "su33":

```
ddboost storage-unit modify su33 report-physical-size 8 GiB
```

SMT y replicación

En caso de desastre, las funciones de usuario indican cómo un usuario puede asistir en las operaciones de recuperación. Diversos tipos de replicación están disponibles en una configuración de SMT. (Consulte el capítulo *DD Replicator* para obtener más detalles acerca de cómo ejecutar una replicación).

Estos son algunos puntos que se deben considerar acerca de las funciones de los usuarios:

- El administrador puede recuperar MTrees desde una copia replicada.
- El administrador de grupos de usuarios puede replicar MTrees desde un sistema a otro, usando la replicación de archivos administrada de DD Boost.
- El administrador de grupos de usuarios puede recuperar MTrees desde una copia replicada también usando la replicación de archivos administrada de DD Boost.

Replicación de recopilaciones
La replicación de recopilaciones replica información de configuraciones de unidades de grupo de usuarios principales.

Replicación segura por medio de Internet pública
Para protegerse contra ataques de intermediario (MITM) cuando se replican a través de una conexión a Internet pública, la autenticación incluye validar la información relacionada con el certificado SSL en el origen y el destino de replicación.

Replicación de MTree (NFS/CIFS) con replicación de archivos administrada de DD Boost
La replicación de MTree es compatible con MTrees asignados a unidades de grupo de usuarios, con replicación de archivos administrada de DD Boost. Durante la replicación de MTree, un MTree asignado a una unidad de grupo de usuarios en un sistema puede replicarse a un MTree asignado a una unidad de grupo de usuarios en otro sistema. No se permite la replicación de MTree entre dos grupos de usuarios diferentes en los dos sistemas DD. Cuando se configura el modo de seguridad como *estricto*, se permite la replicación de MTree solo cuando los MTrees pertenecen a los mismos grupos de usuarios.

Para la compatibilidad con versiones anteriores, se admite la replicación de MTree desde un MTree asignado a una unidad de grupo de usuarios hasta un MTree no asignado, pero debe configurarse manualmente. La configuración manual garantiza que el MTree de destino tenga la configuración correcta para la unidad de grupo de usuarios. En cambio, también se admite la replicación de MTree desde un MTree no asignado a un MTree asignado a una unidad de grupo de usuarios.

Al configurar la replicación de MTree orientada a SMT, el *modo de seguridad* define el grado de comprobación que se realiza en el grupo de usuarios. El modo *predeterminado* comprueba que el origen y destino no pertenezcan a diferentes grupos de usuarios. El modo *estricto* garantiza que el origen y el destino pertenecen al mismo grupo de usuarios. Por lo tanto, cuando se utiliza el modo estricto, se debe crear un grupo de usuarios en la máquina de destino con el mismo UUID que el UUID del grupo de usuarios en la máquina de origen que está asociada con el MTree que se va a replicar.

Replicación de archivos administrada de DD Boost (también con DD Boost AIR)
La replicación de archivos administrada de DD Boost se admite entre unidades de almacenamiento, independientemente de si una unidad de almacenamiento, o ambas, están asignadas a unidades de grupo de usuarios.

Durante la replicación de archivos administrada de DD Boost, las unidades de almacenamiento no se replican por completo. En lugar de esto, determinados archivos dentro de una unidad de almacenamiento son seleccionados por la aplicación de respaldo para la replicación. Los archivos seleccionados en una unidad de almacenamiento a una unidad de grupo de usuarios en un sistema pueden replicarse a una unidad de almacenamiento asignada a una unidad de grupo de usuarios en otro sistema.

Para la compatibilidad con versiones anteriores, los archivos seleccionados en una unidad de almacenamiento asignada a una unidad de grupo de usuarios pueden replicarse a una unidad de almacenamiento no asignada. En cambio, los archivos seleccionados en una unidad de almacenamiento no asignada pueden replicarse en una unidad de almacenamiento asignada a una unidad de grupo de usuarios.

La replicación de archivos administrada de DD Boost también se puede usar en implementaciones de DD Boost AIR.

Control de replicación para QoS
Se puede especificar un límite superior en el rendimiento de replicación (`repl-in`) para un MTree. Dado que los MTrees para cada grupo de usuarios se asignan a una unidad de grupo de usuarios, el uso de recursos de replicación de cada grupo de usuarios puede limitarse mediante la aplicación de esos límites. La relación de esta función con SMT es que la replicación de MTree está sujeta a ese límite de rendimiento.

Alertas de grupos de usuarios de SMT

Un sistema DD genera *eventos* cuando encuentra problemas potenciales con software o hardware. Cuando se genera un evento, una notificación de *alerta* se envía inmediatamente por correo electrónico a los miembros designados en la lista de notificaciones y al administrador de Data Domain.

Las alertas de SMT son específicas para cada unidad de grupo de usuarios y difieren de las alertas del sistema DD. Cuando el modo Tenant Self-Service está habilitado, el administrador de grupo de usuarios puede elegir recibir alertas acerca de diversos objetos del sistema con los que está asociado y acerca de eventos importantes, como un apagado inesperado del sistema. Un administrador de grupo de usuarios solo puede ver o modificar las listas de notificaciones con las que está asociado.

El siguiente ejemplo muestra una alerta de muestra. Tenga en cuenta que los dos mensajes de eventos en la parte inferior de la notificación son específicos del ambiente multiusuario (indicados con la palabra “Grupo de usuarios”). Para ver toda la lista de alertas de SMT y de DD OS, consulte la *Guía de referencia rápida de la MID de Data Domain* o la MIB de SNMP.

```
EVT-ENVIRONMENT-00021. Descripción: El sistema se apagó mediante un
método anormal; por ejemplo, no mediante uno de los siguientes
métodos: 1) Mediante el comando de control de chasis de IPMI 2)
Mediante el botón de encendido 3) Mediante el apagado del sistema
operativo

Acción: Esta alerta se espera después de un evento de pérdida de AC
(alimentación principal). Si este apagado no se espera y persiste,
comuníquese con su proveedor de soporte contratado o visítenos en
línea en https://my.datadomain.com.

Descripción del grupo de usuarios: El sistema ha experimentado una
pérdida de alimentación inesperada y se ha reiniciado.

Acción del grupo de usuarios: Esta alerta se genera cuando el sistema
se reinicia después de una pérdida de alimentación. Si se repite esta
alerta, póngase en contacto con el administrador del sistema.
```

Administración de snapshots

Un *snapshot* es una copia de solo lectura de un MTree capturado en un punto específico en el tiempo. Un snapshot puede utilizarse para varias cosas, por ejemplo, como un punto de restauración en caso de error de funcionamiento del sistema. La función requerida para usar `snapshot` es administrador o administrador de grupo de usuarios.

Para ver la información del snapshot para un MTree o una unidad de grupo de usuarios:

```
# snapshot list mtree mtree-path | tenant-unit tenant-unit
```

Para ver un calendario de snapshots para un MTree o una unidad de grupo de usuarios:

```
# snapshot schedule show [name | mtrees mtree-listmtree-list | tenant-unit tenant-unit]
```

Creación de una copia rápida del sistema de archivos

Una operación de copia rápida copia archivos y árboles de directorios de un directorio de origen a uno de destino en un sistema DD. Hay circunstancias especiales en lo que se refiere a la copia rápida con Secure Multitenancy (SMT).

Hay ciertas consideraciones que se deben tener en cuenta al realizar una copia rápida del sistema de archivos con el modo Tenant Self-Service activado:

- Un administrador de grupo de usuarios puede realizar una copia rápida de archivos de una unidad de grupo de usuarios a otra cuando este es el administrador de ambas unidades y las dos unidades corresponden al mismo grupo de usuarios.
- Un administrador de grupo de usuarios puede realizar una copia rápida de archivos dentro de la misma unidad de grupo de usuarios.
- Un administrador de grupo de usuarios puede realizar una copia rápida de archivos dentro de las unidades de grupo de usuarios en el origen y en el destino.

Para ejecutar una copia rápida del sistema de archivos:

```
# filesys fastcopy source <src> destination <dest>
```

CAPÍTULO 18

DD Cloud Tier

Este capítulo incluye:

- Descripción general de DD Cloud Tier 510
- Configuración de Cloud Tier 514
- Configuración de unidades de nube 516
- Transferencia de datos 530
- Uso de la interfaz de la línea de comandos (CLI) para configurar DD Cloud Tier 535
- Configuración del cifrado de unidades de nube DD 539
- Información necesaria en caso de pérdida del sistema 540
- Uso de DD Replicator con Cloud Tier 540
- Uso de la biblioteca de cintas virtuales (VTL) de DD con Cloud Tier 541
- Visualización de gráficos de consumo de capacidad para DD Cloud Tier 541
- Registros de DD Cloud Tier 542
- Uso de la interfaz de la línea de comandos (CLI) para eliminar DD Cloud Tier .. 542

Descripción general de DD Cloud Tier

DD Cloud Tier es una función nativa de DD OS 6.0 (o posterior) para transferir datos del nivel activo al almacenamiento de objetos de bajo costo y alta capacidad en la nube pública, privada o híbrida para retención a largo plazo. DD Cloud Tier es lo más adecuado para el almacenamiento a largo plazo de datos de acceso poco frecuente que se mantiene por motivos normativos, de cumplimiento de normas y de gobierno corporativo. Los datos ideales para DD Cloud Tier son aquellos que están más allá de su ventana de recuperación normal.

DD Cloud Tier se administra mediante un solo espacio de nombres de Data Domain. No se requiere ningún gateway de nube independiente o dispositivo virtual. La transferencia de datos es compatible con el marco de trabajo de administración de políticas de Data Domain nativo. Conceptualmente, el almacenamiento de nube se trata como un nivel de almacenamiento adicional (DD Cloud Tier) conectado al sistema Data Domain, y se transfieren datos entre niveles según sea necesario. Los metadatos del sistema de archivos asociados con los datos almacenados en la nube se conservan en el almacenamiento local y también se reflejan en la nube. Los metadatos que residen en el almacenamiento local facilitan operaciones como la deduplicación, la limpieza, la copia rápida y la replicación. Este almacenamiento local se divide en depósitos autónomos, llamados unidades de nube, para favorecer la capacidad de administración.

Plataformas compatibles

Cloud Tier es compatible con plataformas físicas que tengan la memoria, la CPU y la conectividad del almacenamiento necesarias para dar cabida a otro nivel de almacenamiento.

DD Cloud Tier es compatible con los siguientes sistemas:

Tabla 196 Configuraciones compatibles de DD Cloud Tier

Modelo	Memoria	Capacidad de la nube	Número requerido de módulos de I/O de SAS	Tipos de bandejas de discos compatibles para almacenamiento de metadatos	Número de bandejas ES30 o paquetes de discos DS60 requeridos	Capacidad requerida para el almacenamiento de metadatos
DD990	256 GB	1140 TB	4	ES30	4	60 discos duros de 3 TB = 180 TB
DD3300 (4 TB)	16 GB	8 TB	N/D	N/D	N/D	1 disco virtual de 1 TB = 1 TB
DD3300 (8 TB)	48 GB	16 TB	N/D	N/D	N/D	2 discos virtuales de 1 TB = 2 TB
DD3300 (16 TB)	48 GB	32 TB	N/D	N/D	N/D	2 discos virtuales de 1 TB = 2 TB

Tabla 196 Configuraciones compatibles de DD Cloud Tier (continuación)

Modelo	Memoria	Capacidad de la nube	Número requerido de módulos de I/O de SAS	Tipos de bandejas de discos compatibles para almacenamiento de metadatos	Número de bandejas ES30 o paquetes de discos DS60 requeridos	Capacidad requerida para el almacenamiento de metadatos
DD3300 (32 TB)	64 GB	64 TB	N/D	N/D	N/D	4 discos virtuales de 1 TB = 4 TB
DD4200	128 GB	378 TB	3	DS60 o ES30	2	30 discos duros de 3 TB = 90 TB
DD4500	192 GB	570 TB	3	DS60 o ES30	2	30 discos duros de 4 TB = 120 TB
DD6800	192 GB	576 TB	2	DS60 o ES30	2	30 discos duros de 4 TB = 120 TB
DD7200	256 GB	856 TB	4	DS60 o ES30	4	60 discos duros de 4 TB = 240 TB
DD9300	384 GB	1400 TB	2	DS60 o ES30	4	60 discos duros de 4 TB = 240 TB
DD9500	512 GB	1,728 TB	4	DS60 o ES30	5	75 discos duros de 4 TB = 300 TB
DD9800	768 GB	2016 TB	4	DS60 o ES30	5	75 discos duros de 4 TB = 300 TB
DD VE (16 TB)	32 GB	32 TB	N/D	N/D	N/D	1 disco virtual de 500 GB = 500 GB[a]
DD VE (64 TB)	60 GB	128 TB	N/D	N/D	N/D	1 disco virtual de 500 GB = 500 GB[a]
DD VE (96 TB)	80 GB	192 TB	N/D	N/D	N/D	1 disco virtual de 500 GB = 500 GB[a]

a. El tamaño mínimo de metadatos es un límite rígido. Data Domain recomienda que los usuarios comiencen con 1 TB para almacenamiento de metadatos y que realicen una expansión en incrementos de 1 TB. La *Guía de instalación y administración de Data Domain Virtual Edition* proporciona más detalles sobre el uso de DD Cloud Tier con DD VE.

Nota

DD Cloud Tier es compatible con la alta disponibilidad (HA) de Data Domain. Ambos nodos deben ejecutar DD OS 6.0 (o posterior) y deben ser compatibles con alta disponibilidad.

Nota

DD Cloud Tier no es compatible con los sistemas que no están detallados ni con los sistemas que tienen la función Extended Retention habilitada o configurada con replicación de recopilaciones.

Nota

La función Cloud Tier puede consumir todo el ancho de banda disponible en un vínculo WAN compartido, en especial en una configuración de ancho de banda bajo (1 GB/s), y esto puede afectar otras aplicaciones que comparten el vínculo WAN. Si hay aplicaciones compartidas en la WAN, se recomienda el uso de QoS u otra limitación de la red para evitar la congestión y garantizar un rendimiento coherente en el transcurso del tiempo.
Si el ancho de banda está restringido, la tasa de transferencia de datos será lenta y no se podrá transferir la misma cantidad de datos a la nube. Es mejor usar un vínculo dedicado para los datos que se transfieren al nivel de nube.

Nota

No envíe tráfico sobre controladoras de interfaz de red de administración incorporados (interfaces ethMx).

Rendimiento de DD Cloud Tier

El sistema Data Domain usa las optimizaciones internas para maximizar el rendimiento de DD Cloud Tier.

Propagación en la nube
El motor de migración actual a la nube se basa en archivos, y se utiliza un motor optimizado de deduplicación eficiente para identificar y migrar solo segmentos únicos a la nube. La eficiencia de este motor de migración basada en archivos es elevada cuando se migran datos de mayor generación al nivel de la nube, que ya tiene algunos datos para deduplicar. Sin embargo, cuando el nivel de la nube está vacío o casi vacío, no hay datos para deduplicar. Se produce una sobrecarga de ciclos de procesamiento que se invierten en la deduplicación. Con la migración basada en la propagación, el filtrado de deduplicación se mantiene en el nivel activo propio y solo se migran datos únicos de forma masiva al nivel de la nube. En la propagación a la nube, el motor migra el contenido del almacenamiento local al almacenamiento de nube sin procesarlo para la deduplicación. Cuando la propagación de la nube está activa, los archivos marcados para la migración al almacenamiento de nube no se limpian (es decir, el espacio no se libera) como parte de la limpieza del sistema de archivos de nivel activo hasta que se completa la migración de todos los archivos identificados por propagación. Se debe dimensionar el almacenamiento en niveles activo para tenerlo en cuenta en ambientes en los que se migrarán grandes cantidades de datos al almacenamiento de nube. Si se completa menos del 5 % de la capacidad del almacenamiento de DD Cloud Tier y se usan 30 TiB (o más) de datos después de la compresión, el sistema Data Domain usa

automáticamente la propagación a la nube cuando migra datos al almacenamiento de nube.

Después de consumir el 5 % de la capacidad de DD Cloud Tier, la propagación en la nube se desactiva automáticamente y los datos se procesan para deduplicación antes de la migración al almacenamiento de nube.

Estos son puntos adicionales para tener en cuenta cuando se utiliza la migración de propagación:

- La migración se admite en el modo de propagación solo cuando:
  - El tamaño utilizado después de la compresión del nivel activo es 30 TiB o más, según lo que se informa en la salida del comando que muestra el espacio de filesys.
  - El nivel activo se encuentra completo en un valor inferior al 70 % cuando la migración comienza como se informa en la salida del comando que muestra el espacio de filesys.

  Nota

  Si el uso del nivel activo durante el ciclo de migración en curso en el modo de propagación supera el 90 %, la migración se anula y luego se reinicia en el modo de FileCopy normal.
- La migración en modo de propagación se suspende automáticamente mediante la limpieza en el nivel activo durante toda la duración de la limpieza en el nivel activo. Cuando se completa la limpieza, la propagación se reanuda automáticamente y reinicia la migración a la nube.
- La migración en modo de propagación se suspende automáticamente si se recibe el evento UNAVAIL de la nube en la unidad de nube (la unidad de nube se informa como “disconnected”) a la que se realiza la migración y solo se reanuda una vez que la unidad de nube está disponible y se informa como activa.
- La limpieza no se puede iniciar en una unidad de nube que es el destino de una operación de migración en curso en modo de propagación.

  Nota

  En dos sistemas de unidades de nube, para forzar el inicio de la limpieza en una segunda unidad de nube, en la que no se realiza la propagación, suspenda la migración en modo de propagación utilizando la CLI de suspensión de movimiento de datos y, a continuación, ejecute la CLI de inicio de limpieza de la nube en la segunda unidad de nube.
- La verificación de archivos basada en probabilidades en la nube, incluso si se programa según la política predeterminada, se omite y no se produce en una unidad de nube en la que la migración está en curso en modo de propagación.
- Si la limpieza ya está en curso en el nivel de nube o en el nivel activo y se inicia el movimiento de datos programado en modo de propagación, el movimiento de datos se suspende automáticamente durante la actividad de limpieza.
- La migración en modo de propagación omite la migración de archivos, desde MTrees, que son destinos de replicación, aunque los archivos sean elegibles para la migración. Los archivos de estos MTrees, que son MTrees de destino de replicación (RO/RD), se migran utilizando el motor de FileCopy una vez que se completa la migración en modo de propagación de todos los MTrees elegibles.
- Si la función de creación de informes sobre la capacidad física se habilita y se programa, la migración en modo de propagación suspende la función de creación de informes sobre capacidad durante la migración basada en propagación.

- La migración en modo de propagación solo se admite en todos los sistemas y configuraciones de Data Domain habilitados para la nube con más de 80 GB de RAM. La migración basada en la propagación se encuentra deshabilitada de forma predeterminada para DD VE.

Tamaño de objetos grandes
DD Cloud Tier utiliza tamaños de objetos de 1 MB o 4 MB (según el proveedor de almacenamiento de nube) para reducir la sobrecarga de metadatos y disminuir la cantidad de objetos que se migrarán al almacenamiento de nube.

Configuración de Cloud Tier

Para configurar Cloud Tier, agregue la licencia y los gabinetes, establezca una frase de contraseña del sistema y cree un sistema de archivos que admita la transferencia de datos hacia la nube.

- Para Cloud Tier, se requiere la licencia de capacidad de nube.
- Para licenciar Cloud Tier, consulte las *Notas de la versión de Data Domain Operating System* correspondientes para obtener información más actualizada sobre las características del producto, las actualizaciones de software y las guías de compatibilidad de software, además de detalles acerca de productos, licencias y servicios de Data Domain.
- Para establecer una frase de contraseña del sistema, utilice la pestaña **Administration** > **Access** > **Administrator Access**.
  Si la frase de contraseña del sistema no está configurada, aparecerá el botón **Set Passphrase** en el área Passphrase. Si hay una frase de contraseña del sistema configurada, aparecerá el botón **Change Passphrase** y la única opción que tendrá será cambiar la frase.
- Para configurar el almacenamiento, utilice la pestaña **Hardware** > **Storage**.
- Para crear un sistema de archivos, utilice el asistente File System Create.

Configuración del almacenamiento para DD Cloud Tier

El almacenamiento de nivel de nube en el sistema DD se requiere para las unidades de nube. Allí se contienen los metadatos para los archivos, mientras que los datos residen en la nube.

Procedimiento

1. Seleccione **Hardware** > **Storage**.
2. En la pestaña Overview, expanda **Cloud Tier**.
3. Haga clic en **Configure**.

   Se mostrará el cuadro de diálogo Configure Cloud Tier.
4. Seleccione la casilla de verificación de la bandeja que se agregará desde la sección Addable Storage.

   ⚠ PRECAUCIÓN

   Los sistemas DD3300 requieren el uso de dispositivos de almacenamiento de 1 TB para almacenamiento de metadatos de DD Cloud Tier.
5. Haga clic en el botón **Add to Tier**.
6. Haga clic en **Save** para agregar el almacenamiento.

7. Seleccione **Data Management** > **File System** y habilite la función Cloud Tier.
8. Haga clic en **Disable** (en la parte inferior de la pantalla) para deshabilitar el sistema de archivos.
9. Haga clic en **OK**.
10. Después de que el sistema de archivos esté deshabilitado, seleccione **Enable Cloud Tier**.

    Para habilitar el nivel de nube, debe cumplir con el requisito de almacenamiento para la capacidad con licencia. Configure el nivel de nube del sistema de archivos. Haga clic en **Next.**
    Un sistema de archivos de nube requiere un área de almacenamiento local para una copia local de los metadatos de la nube.

11. Seleccione **Enable file system**.

    El nivel de nube se habilita con el almacenamiento designado.

12. Haga clic en **OK**.

    Debe crear unidades de nube por separado, después de que se crea el sistema de archivos.

Estimación de espacio que se puede limpiar

La herramienta de estimación del espacio que se puede limpiar evalúa la cantidad de espacio que se puede liberar en un nivel activo si `data-movement` mueve los archivos elegibles a la nube y GC limpia el sistema de archivos.

Esta herramienta funciona con o sin una licencia de nube/archiving presente.

Si no hay ninguna licencia de nube/activa, proporcione el umbral de antigüedad que debe utilizarse para evaluar el espacio total que se puede limpiar en el nivel activo. Si hay un umbral de antigüedad junto con una política establecida en MTrees, la preferencia se le da al umbral de antigüedad que proporciona el usuario.

Existen tres flujos de trabajo:

- Un sistema con políticas de migración en la nube establecidas: Los archivos se identifican como “elegibles” en función de la política establecida en los respectivos MTrees y se calcula el espacio que se puede limpiar.
- Un sistema con políticas de migración en la nube establecidas, pero con un umbral de antigüedad proporcionado por el usuario: Los archivos se identifican en función del umbral de antigüedad proporcionado por el usuario, lo que anula las políticas del sistema.
- Un sistema sin nube: Es un requisito obligatorio que el usuario proporcione un umbral de antigüedad que se utilizará para determinar el espacio total que se puede limpiar.

Algunos puntos adicionales para considerar:

- El movimiento de datos no se puede ejecutar en paralelo con la comprobación de elegibilidad para el movimiento de datos, y viceversa.
- La limpieza en el nivel activo no se puede iniciar si la comprobación de elegibilidad se está ejecutando, y viceversa.
- La limpieza en el nivel de nube no se puede iniciar si la comprobación de elegibilidad se está ejecutando, y viceversa.
- Si se recibe el evento UNAVAIL, no debe tener ningún impacto en la operación de comprobación de elegibilidad.

- Si el sistema de archivos se detiene o falla, la comprobación de elegibilidad se detiene y no se reanuda automáticamente cuando el sistema de archivos vuelve a iniciarse.

Nota

No se permite iniciar la comprobación de elegibilidad desde la GUI de Data Domain System Manager.

Configuración de unidades de nube

El nivel de nube consta de un máximo de dos unidades de nube, y cada una se asigna a un proveedor de nube, lo que permite varios proveedores de nube por sistema Data Domain. El sistema Data Domain debe estar conectado a la nube y tener una cuenta con un proveedor de nube compatible.

La configuración de unidades de nube incluye estos pasos:

- Configuración de la red, incluida la configuración de firewall y proxy
- Importación de certificados de CA
- Adición de unidades de nube

Configuración de firewall y proxy

Puertos de firewall de red

- El puerto 443 (HTTPS) o el puerto 80 (HTTP) deben estar abiertos a las redes de proveedor de nube para la dirección IP de terminal y la dirección IP de autenticación de proveedor para el tráfico bidireccional.
  Por ejemplo, para Amazon S3, s3-ap-southeast-1.amazonaws.com y s3.amazonaws.com deben tener el puerto 80 o el puerto 443 desbloqueados y configurados para permitir el tráfico IP bidireccional.

  Nota

  Varios proveedores de nube pública utilizan rangos de IP para sus direcciones de terminal y autenticación. En esta situación, los rangos de IP utilizados por el proveedor deban desbloquearse para adaptarse a los posibles cambios de IP.

- Los rangos de las direcciones IP de destino de proveedor de nube remoto y autenticación deben poder pasar por el firewall.
- Para la nube privada de ECS, los rangos de direcciones IP de acceso de almacenamiento web (S3) y autenticación local de ECS y los puertos 9020 (HTTP) y 9021 (HTTPS) deben poder pasar a través de firewalls locales.

  Nota

  Las reglas de puerto y acceso a las direcciones IP de balanceo de carga de la nube privada ECS también deben configurarse.

Ajustes del proxy

Si hay alguna configuración del proxy existente que haga que los datos por encima de un determinado tamaño se rechacen, se debe cambiar esa configuración para permitir objetos con un tamaño de hasta 4.5 MB.

Si el tráfico del cliente se enruta a través de un proxy, se debe importar un certificado del proxy con autofirma o firmado por CA. Consulte “Importación de certificados de CA” para obtener más información.

Suites de cifrado de OpenSSL

- Cifrados: ECDHE-RSA-AES256-SHA384, AES256-GCM-SHA384
- Versión de TLS: 1.2

Nota

La comunicación predeterminada con todos los proveedores de nube se inicia con cifrado seguro.

Protocolos compatibles

- HTTP
- HTTPS

Nota

La comunicación predeterminada con todos los proveedores de nube pública se produce en HTTP seguro (HTTPS), pero se puede sobrescribir la configuración predeterminada para usar HTTP.

Importación de certificados de CA

Antes de agregar unidades de nube a Elastic Cloud Storage (ECS), Virtustream Storage Cloud, Alibaba Cloud, Amazon Web Services S3 (AWS) y la nube de Azure, debe importar los certificados de CA.

Antes de comenzar

Para los proveedores de nube pública AWS, Azure y Virtustream, los certificados de CA raíz se pueden descargar desde https://www.digicert.com/digicert-root-certificates.htm.

- Para un proveedor de nube AWS, descargue el certificado raíz de Baltimore CyberTrust.
- Para un proveedor de nube Virtustream, descargue el certificado de CA raíz de DigiCert High Assurance EV.
- Para ECS, la autoridad de certificación raíz varía por cliente.
  La implementación de almacenamiento de nube en ECS requiere un balanceo de carga. Si se utiliza un terminal de HTTPS como terminal en la configuración, asegúrese de importar el certificado de CA raíz. Para obtener más información, póngase en contacto con su proveedor de balanceo de carga.
- Para un proveedor de nube Azure, descargue el certificado raíz de Baltimore CyberTrust.
- Para un proveedor de S3 Flexible, importe el certificado de CA raíz. Para obtener más información, comuníquese con su proveedor de S3 Flexible.

Si su certificado descargado tiene una extensión .crt, es probable que deba convertirse en un certificado con codificación PEM. Si es así, utilice OpenSSL para convertir el archivo de formato .crt a .pem (por ejemplo, `openssl x509 -inform der -in BaltimoreCyberTrustRoot.crt -out BaltimoreCyberTrustRoot.pem`).

Para Alibaba:

1. Descargue el certificado raíz de GlobalSign R1 en https://support.globalsign.com/customer/portal/articles/1426602-globalsign-root-certificates.

2. Convierta el certificado descargado en un formato codificado en PEM. El comando OpenSSL para esta conversión es `openssl x509 -inform der -in <root_cert.crt> -out <root_cert.pem>`.
3. Importe el certificado al sistema Data Domain.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Cloud Units**.
2. En la barra de herramientas, haga clic en **Manage Certificates**.

   Aparece el cuadro de diálogo Manage Certificates for Cloud.
3. Haga clic en **Add**.
4. Seleccione una de estas opciones:
   - **I want to upload the certificate as a .pem file.**
     Navegue y seleccione el archivo de certificado.
   - **I want to copy and paste the certificate text.**
     - Copie el contenido del archivo .pem en el búfer de copia.
     - Pegue el búfer en el cuadro de diálogo.
5. Haga clic en **Add**.

Adición de una unidad de nube a Elastic Cloud Storage (ECS)

Un sistema Data Domain o una instancia de DD VE requiere una sincronización de hora de cierre con el sistema ECS para configurar una unidad de nube de Data Domain. Configurar NTP en el sistema Data Domain o la instancia de DD VE y el sistema ECS resuelve este problema.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Cloud Units**.
2. Haga clic en **Add**.

   Se muestra el cuadro de diálogo Add Cloud Unit.
3. Escriba un nombre para esta unidad de nube. Solo se permiten caracteres alfanuméricos.

   Los campos restantes en el cuadro de diálogo Add Cloud Unit pertenecen a la cuenta del proveedor de nube.
4. Para **Cloud provider**, seleccione **EMC Elastic Cloud Storage (ECS)** en la lista desplegable.
5. Ingrese la **clave de acceso** del proveedor como texto de la contraseña.
6. Ingrese la **clave secreta** del proveedor como texto de la contraseña.
7. Ingrese el **terminal** del proveedor en este formato:`http://<nombre de host/IP>:<puerto>`. Si está utilizando un terminal seguro, utilice `https` en su lugar.

   Nota

   La implementación de almacenamiento de nube en ECS requiere un balanceo de carga.

   De forma predeterminada, ECS ejecuta el protocolo de S3 en el puerto 9020 para HTTP y 9021 para HTTPS. Cuando se utiliza un balanceo de carga, esos puertos, a veces, se vuelven a asignar en 80 para HTTP y 443 para HTTPS,

respectivamente. Consulte con su administrador de red para conocer los puertos adecuados.

8. Si se requiere un servidor proxy HTTP para eludir un firewall para este proveedor, haga clic en **Configure** para **HTTP Proxy Server**.

   Ingrese el nombre de host del servidor proxy, el puerto, el nombre de usuario y la contraseña.

   Nota

   Existe un paso opcional para ejecutar la herramienta de verificación de proveedor de nube antes de agregar la unidad de nube. Esta herramienta realiza pruebas previas a la comprobación para garantizar que se cumplan todos los requisitos antes de agregar la unidad de nube real.

9. Haga clic en **Add**.

   Ahora, en la ventana principal del sistema de archivos se muestra información de resumen de la nueva unidad de nube, además de un control para la habilitación y deshabilitación de la unidad de nube.

Adición de una unidad de nube para Virtustream

Virtustream ofrece una variedad de clases de almacenamiento. *Cloud Providers Compatibility Matrix*, disponible en http://compatibilityguide.emc.com:8080/CompGuideApp/, proporciona la información más actualizada acerca de las clases de almacenamiento compatibles.

Los siguientes terminales son utilizados por el proveedor de nube Virtustream, según la clase de almacenamiento y la región. Asegúrese de que DNS pueda resolver estos nombres de host antes de configurar las unidades de nube.

- s-us.objectstorage.io
- s-eu.objectstorage.io
- s-eu-west-1.objectstorage.io
- s-eu-west-2.objectstorage.io
- s-us-central-1.objectstorage.io

Procedimiento

1. Seleccione **Data Management** > **File System** > **Cloud Units**.
2. Haga clic en **Add**.

   Se muestra el cuadro de diálogo Add Cloud Unit.

3. Escriba un nombre para esta unidad de nube. Solo se permiten caracteres alfanuméricos.

   Los campos restantes en el cuadro de diálogo Add Cloud Unit pertenecen a la cuenta del proveedor de nube.

4. Para **Cloud provider**, seleccione **Virtustream Storage Cloud** en la lista desplegable.
5. Seleccione la clase de almacenamiento en la lista desplegable.
6. Seleccione la región adecuada correspondiente al tipo de cuenta de la lista desplegable.

7. Ingrese la **clave de acceso** del proveedor como texto de la contraseña.
8. Ingrese la **clave secreta** del proveedor como texto de la contraseña.
9. Si se requiere un servidor proxy HTTP para eludir un firewall para este proveedor, haga clic en **Configure** para **HTTP Proxy Server**.

   Ingrese el nombre de host del servidor proxy, el puerto, el nombre de usuario y la contraseña.

   Nota

   Existe un paso opcional para ejecutar la herramienta de verificación de proveedor de nube antes de agregar la unidad de nube. Esta herramienta realiza pruebas previas a la comprobación para garantizar que se cumplan todos los requisitos antes de agregar la unidad de nube real.

10. Haga clic en **Save**.

    Ahora, en la ventana principal del sistema de archivos se muestra información de resumen de la nueva unidad de nube, además de un control para la habilitación y deshabilitación de la unidad de nube.

Agregar una unidad de nube para Alibaba

Las regiones se configuran en el nivel del depósito en lugar de en el nivel de objetos. Por lo tanto, todos los objetos en el depósito se almacenan en la misma región. Se especifica una región cuando se crea un depósito, y no se puede cambiar una vez que se crea.

Tabla 197 Regiones de Alibaba

Regiones	Ubicación	Nombre de la región
Regiones de China continental	Este de China 1 (Hangzhou)	oss-cn-hangzhou
	Este de China 2 (Shanghái)	oss-cn-shanghai
	Norte de China 1 (Qingdao)	oss-cn-qingdao
	Norte de China 2 (Pekín)	oss-cn-beijing
	Norte de China 3 (Zhangjiakou)	oss-cn-zhangjiakou
	Norte de China 5 (Huhehaote)	oss-cn-huhehaote
	Sur de China 1 (Shenzhen)	oss-cn-shenzhen
Regiones internacionales	Hong Kong	oss-cn-hongkong
	Oeste de EE. UU. 1 (Silicon Valley)	oss-us-west-1
	Este de EE. UU. 1 (Virginia)	oss-us-east-1
	Sudeste del Pacífico Asiático 1 (Singapur)	oss-ap-southeast-1
	Sudeste del Pacífico Asiático 2 (Sídney)	oss-ap-southeast-2

Tabla 197 Regiones de Alibaba (continuación)

Regiones	Ubicación	Nombre de la región
	Sudeste del Pacífico Asiático 3 (Kuala Lumpur)	oss-ap-southeast-3
	Sudeste del Pacífico Asiático 5 (Yakarta)	oss-ap-southeast-5
	Noreste del Pacífico Asiático 1 (Tokio)	oss-ap-northeast-1
	Suroeste del Pacífico Asiático 1 (Bombay)	oss-ap-south-1
	Región central de la UE 1 (Fráncfort)	oss-eu-central-1
	Oriente Medio 1 (Dubái)	oss-me-east-1

La información de identificación de Alibaba Cloud debe contar con permisos para crear y eliminar depósitos, y para agregar, modificar y eliminar archivos dentro de los depósitos que se crean. Se recomienda AliyunOSSFullAccess, pero estos son los requisitos mínimos:

- ListBuckets
- GetBucket
- PutBucket
- DeleteBucket
- GetObject
- PutObject
- DeleteObject

Procedimiento

1. Seleccione **Data Management** > **File System** > **Cloud Units**.
2. Haga clic en **Add**.

   Se muestra el cuadro de diálogo Add Cloud Unit.
3. Escriba un nombre para esta unidad de nube. Solo se permiten caracteres alfanuméricos.

   Los campos restantes en el cuadro de diálogo **Add Cloud Unit** pertenecen a la cuenta del proveedor de nube.
4. En **Cloud provider**, seleccione **Alibaba Cloud** en la lista desplegable.
5. Seleccione **Standard** o **IA** en la lista desplegable **Storage class**.
6. En la lista desplegable, seleccione la región en **Storage region**.
7. Ingrese la **clave de acceso** del proveedor como texto de la contraseña.
8. Ingrese la **clave secreta** del proveedor como texto de la contraseña.
9. Asegúrese de que el puerto 443 (HTTPS) no esté bloqueado en los firewalls. La comunicación con el proveedor de nube de Alibaba se produce en el puerto 443.
10. Si se requiere un servidor proxy HTTP para eludir un firewall para este proveedor, haga clic en **Configure** para **HTTP Proxy Server**.

Ingrese el nombre de host del servidor proxy, el puerto, el nombre de usuario y la contraseña.

Nota

Existe un paso opcional para ejecutar la herramienta de verificación de proveedor de nube antes de agregar la unidad de nube. Esta herramienta realiza pruebas previas a la comprobación para garantizar que se cumplan todos los requisitos antes de agregar la unidad de nube real.

11. Haga clic en **Add**.

    Ahora, en la ventana principal del sistema de archivos se muestra información de resumen de la nueva unidad de nube, además de un control para la habilitación y deshabilitación de la unidad de nube.

Adición de una unidad de nube para Amazon Web Services S3

AWS ofrece una variedad de clases de almacenamiento. *Cloud Providers Compatibility Matrix*, disponible en http://compatibilityguide.emc.com:8080/CompGuideApp/, proporciona la información más actualizada acerca de las clases de almacenamiento compatibles.

Para mejorar la seguridad, la función de nivel de nube utiliza Signature Version 4 para todas las solicitudes de AWS. El protocolo de firma Signature Version 4 está habilitado de forma predeterminada.

Los siguientes terminales son utilizados por el proveedor de nube AWS, según la clase de almacenamiento y la región. Asegúrese de que DNS pueda resolver estos nombres de host antes de configurar las unidades de nube.

- s3.amazonaws.com
- s3-us-west-1.amazonaws.com
- s3-us-west-2.amazonaws.com
- s3-eu-west-1.amazonaws.com
- s3-ap-northeast-1.amazonaws.com
- s3-ap-southeast-1.amazonaws.com
- s3-ap-southeast-2.amazonaws.com
- s3-sa-east-1.amazonaws.com
- ap-south-1
- ap-northeast-2
- eu-central-1

Nota

No se admite la región de China.

Nota

La información de identificación de AWS debe contar con permisos para crear y eliminar depósitos, y para agregar, modificar y eliminar archivos dentro de los depósitos que crean. Se recomienda S3FullAccess, pero estos son los requisitos mínimos:

- CreateBucket
- ListBucket
- DeleteBucket
- ListAllMyBuckets
- GetObject
- PutObject
- DeleteObject

Procedimiento

1. Seleccione **Data Management** > **File System** > **Cloud Units**.
2. Haga clic en **Add**.

   Se muestra el cuadro de diálogo Add Cloud Unit.
3. Escriba un nombre para esta unidad de nube. Solo se permiten caracteres alfanuméricos.

   Los campos restantes en el cuadro de diálogo Add Cloud Unit pertenecen a la cuenta del proveedor de nube.
4. Para **Cloud provider**, seleccione **Amazon Web Services S3** en la lista desplegable.
5. Seleccione la clase de almacenamiento en la lista desplegable.
6. En la lista desplegable, seleccione el tipo de **región de almacenamiento** que corresponda.
7. Ingrese la **clave de acceso** del proveedor como texto de la contraseña.
8. Ingrese la **clave secreta** del proveedor como texto de la contraseña.
9. Asegúrese de que el puerto 443 (HTTPS) no esté bloqueado en los firewalls. La comunicación con el proveedor de nube de AWS se produce en el puerto 443.
10. Si se requiere un servidor proxy HTTP para eludir un firewall para este proveedor, haga clic en **Configure** para **HTTP Proxy Server**.

    Ingrese el nombre de host del servidor proxy, el puerto, el nombre de usuario y la contraseña.

    Nota

    Existe un paso opcional para ejecutar la herramienta de verificación de proveedor de nube antes de agregar la unidad de nube. Esta herramienta realiza pruebas previas a la comprobación para garantizar que se cumplan todos los requisitos antes de agregar la unidad de nube real.
11. Haga clic en **Add**.

Ahora, en la ventana principal del sistema de archivos se muestra información de resumen de la nueva unidad de nube, además de un control para la habilitación y deshabilitación de la unidad de nube.

Adición de una unidad de nube para Azure

Microsoft Azure ofrece una variedad de tipos de cuentas de almacenamiento. *Cloud Providers Compatibility Matrix*, disponible en http://compatibilityguide.emc.com:8080/CompGuideApp/, proporciona la información más actualizada acerca de las clases de almacenamiento compatibles.

Los siguientes terminales son utilizados por el proveedor de nube Azure, según la clase de almacenamiento y la región. Asegúrese de que DNS pueda resolver estos nombres de host antes de configurar las unidades de nube.

- *Nombre de cuenta*.blob.core.windows.net

El nombre de cuenta se obtiene desde la consola de proveedor de nube de Azure.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Cloud Units**.
2. Haga clic en **Add**.

   Se muestra el cuadro de diálogo Add Cloud Unit.
3. Escriba un nombre para esta unidad de nube. Solo se permiten caracteres alfanuméricos.

   Los campos restantes en el cuadro de diálogo Add Cloud Unit pertenecen a la cuenta del proveedor de nube.
4. Para **Cloud provider**, seleccione **Microsoft Azure Storage** en la lista desplegable.
5. Para **Account type**, seleccione **Government** o **Public**.
6. Seleccione la clase de almacenamiento en la lista desplegable.
7. Ingrese el **nombre de cuenta** del proveedor.
8. Ingrese la **clave principal** del proveedor como texto de la contraseña.
9. Ingrese la **clave secundaria** del proveedor como texto de la contraseña.
10. Asegúrese de que el puerto 443 (HTTPS) no esté bloqueado en los firewalls. La comunicación con el proveedor de nube de Azure se produce en el puerto 443.
11. Si se requiere un servidor proxy HTTP para eludir un firewall para este proveedor, haga clic en **Configure** para **HTTP Proxy Server**.

    Ingrese el nombre de host del servidor proxy, el puerto, el nombre de usuario y la contraseña.

    Nota

    Existe un paso opcional para ejecutar la herramienta de verificación de proveedor de nube antes de agregar la unidad de nube. Esta herramienta realiza pruebas previas a la comprobación para garantizar que se cumplan todos los requisitos antes de agregar la unidad de nube real.
12. Haga clic en **Add**.

Ahora, en la ventana principal del sistema de archivos se muestra información de resumen de la nueva unidad de nube, además de un control para la habilitación y deshabilitación de la unidad de nube.

Agregar una unidad de nube para el proveedor de Google Cloud

Las siguientes tablas enumeran las ubicaciones de almacenamiento de nube disponibles para almacenar datos.

Tabla 198 Ubicaciones con varias regiones

Nombre de varias regiones	Descripción de varias regiones
Asia	Centros de datos en Asia
EE UU	Centros de datos en los Estados Unidos
UE	Centros de datos en la Unión Europea

Tabla 199 Ubicaciones regionales

Ubicaciones regionales	Ubicación	Nombre de la región
Norteamérica	northamerica-northeast1	Montreal
	us-central1	Iowa
	us-east1	Carolina del Sur
	us-east4	Virginia del Norte
	us-west1	Oregón
	us-west2	Los Ángeles
América del Sur	southamerica-east1	São Paulo
Europa	europe-north1	Finlandia
	europe-west1	Bélgica
	europe-west2	Londres
	europe-west3	Fráncfort
	europe-west4	Países Bajos
Asia	asia-east1	Taiwán
	asia-northeast1	Tokio
	asia-south1	Bombay
	asia-southeast1	Singapur
Australia	australia-southeast1	Sydney

La información de identificación del proveedor de Google Cloud debe contar con permisos para crear y eliminar depósitos, y para agregar, modificar y eliminar archivos dentro de los depósitos que se crean. Estos son los requisitos mínimos:

- ListBucket
- PutBucket
- GetBucket

- DeleteBucket
- GetObject
- PutObject
- DeleteObject

Nota

DD Cloud Tier solo es compatible con Nearline y se selecciona automáticamente durante la configuración.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Cloud Units**.
2. Haga clic en **Add**.

   Se muestra el cuadro de diálogo Add Cloud Unit.
3. Escriba un nombre para esta unidad de nube. Solo se permiten caracteres alfanuméricos.

   Los campos restantes en el cuadro de diálogo **Add Cloud Unit** pertenecen a la cuenta del proveedor de nube.
4. En **Cloud provider**, seleccione **Google Cloud Storage** en la lista desplegable.
5. Ingrese la **clave de acceso** del proveedor como texto de la contraseña.
6. Ingrese la **clave secreta** del proveedor como texto de la contraseña.
7. **Storage class** se establece como **Nearline** de forma predeterminada.

   Si se selecciona una ubicación de varias regiones (Asia, UE o EE. UU.), la clase de almacenamiento y la restricción de ubicación son Nearline Multi-regional. En todas las demás ubicaciones regionales, la clase de almacenamiento se establece en Nearline Regional.
8. Seleccione **Region**.
9. Asegúrese de que el puerto 443 (HTTPS) no esté bloqueado en los firewalls. La comunicación con el proveedor de Google Cloud se produce en el puerto 443.
10. Si se requiere un servidor proxy HTTP para eludir un firewall para este proveedor, haga clic en **Configure** para **HTTP Proxy Server**.

    Ingrese el nombre de host del servidor proxy, el puerto, el nombre de usuario y la contraseña.

    Nota

    Existe un paso opcional para ejecutar la herramienta de verificación de proveedor de nube antes de agregar la unidad de nube. Esta herramienta realiza pruebas previas a la comprobación para garantizar que se cumplan todos los requisitos antes de agregar la unidad de nube real.
11. Haga clic en **Add**.

    Ahora, en la ventana principal del sistema de archivos se muestra información de resumen de la nueva unidad de nube, además de un control para la habilitación y deshabilitación de la unidad de nube.

Adición de una unidad de nube de un proveedor de S3 Flexible

La función Cloud Tier admite proveedores de nube S3 calificados adicionales con una opción de configuración de proveedores de S3 Flexible.

La opción de proveedor de S3 Flexible es compatible con las clases de almacenamiento estándar y estándar de acceso poco frecuente. Los siguientes terminales variarán según el proveedor de nube, la clase de almacenamiento y la región. Asegúrese de que DNS pueda resolver estos nombres de host antes de configurar las unidades de nube.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Cloud Units**.
2. Haga clic en **Add**.

   Se muestra el cuadro de diálogo Add Cloud Unit.
3. Escriba un nombre para esta unidad de nube. Solo se permiten caracteres alfanuméricos.

   Los campos restantes en el cuadro de diálogo Add Cloud Unit pertenecen a la cuenta del proveedor de nube.
4. Para **Cloud provider**, seleccione **Flexible Cloud Tier Provider Framework for S3** en la lista desplegable.
5. Ingrese la **clave de acceso** del proveedor como texto de la contraseña.
6. Ingrese la **clave secreta** del proveedor como texto de la contraseña.
7. Especifique la opción que corresponda en **Storage region**.
8. Ingrese el **terminal** del proveedor en este formato:`http://<nombre de host/IP>:<puerto>`. Si está utilizando un terminal seguro, utilice `https` en su lugar.
9. En **Storage class**, seleccione la clase de almacenamiento adecuada de la lista desplegable.
10. Asegúrese de que el puerto 443 (HTTPS) no esté bloqueado en los firewalls. La comunicación con el proveedor de nube de S3 se produce en el puerto 443.
11. Si se requiere un servidor proxy HTTP para eludir un firewall para este proveedor, haga clic en **Configure** para **HTTP Proxy Server**.

    Ingrese el nombre de host del servidor proxy, el puerto, el nombre de usuario y la contraseña.

    Nota

    Existe un paso opcional para ejecutar la herramienta de verificación de proveedor de nube antes de agregar la unidad de nube. Esta herramienta realiza pruebas previas a la comprobación para garantizar que se cumplan todos los requisitos antes de agregar la unidad de nube real.
12. Haga clic en **Add**.

    Ahora, en la ventana principal del sistema de archivos se muestra información de resumen de la nueva unidad de nube, además de un control para la habilitación y deshabilitación de la unidad de nube.

Modificación de una unidad de nube o un perfil en la nube

Modifique las credenciales de la unidad de nube, el nombre de un proveedor de S3 Flexible o los detalles de un perfil de nube.

Modificación de credenciales de la unidad de nube

Procedimiento

1. Seleccione **Data Management** > **File System** > **Cloud Units**.
2. Haga clic en el ícono del lápiz de la unidad de nube cuyas credenciales desea modificar.

   Se mostrará el cuadro de diálogo Modify Cloud Unit.
3. En **Account name**, escriba el nuevo nombre de cuenta.
4. Para **Access key**, escriba la nueva clave de acceso de proveedor como texto de la contraseña.

   Nota

   No se admite la modificación de la clave de acceso para los ambientes de ECS.
5. Para **Secret key**, escriba la nueva clave secreta del proveedor como texto de la contraseña.
6. Para **Primary key**, escriba la nueva clave principal del proveedor como texto de la contraseña.

   Nota

   Solo se admite la modificación de la clave principal para ambientes de Azure.
7. Si se requiere un servidor proxy HTTP para eludir un firewall para este proveedor, haga clic en **Configure** para **HTTP Proxy Server**.
8. Haga clic en **OK**.

Modificación del nombre de un proveedor de S3 Flexible

Procedimiento

1. Seleccione **Data Management** > **File System** > **Cloud Units**.
2. Haga clic en el ícono del lápiz de la unidad de nube de S3 Flexible cuyas credenciales desea modificar.

   Se mostrará el cuadro de diálogo Modify Cloud Unit.
3. En **S3 Provider Name**, escriba el nuevo nombre del proveedor.
4. Haga clic en **OK**.

Uso de la CLI para modificar un perfil de nube

Procedimiento

1. Ejecute el comando `cloud profile modify` para modificar los detalles de un perfil de nube. El sistema le solicita modificar detalles individuales del perfil de nube.

Para perfiles Virtustream, AWS S3 o Azure, ejecute este comando para agregar una clase de almacenamiento a un perfil de nube existente.

Los detalles del perfil que se pueden modificar dependen del proveedor de nube:

- Alibaba Cloud admite la modificación de la clave de acceso y la clave secreta.
- AWS S3 admite la modificación de la clave de acceso y la clave secreta.
- Azure admite la modificación de la clave de acceso, la clave secreta y la clave principal.
- ECS admite la modificación de la clave secreta.
- Virtustream admite la modificación de la clave de acceso y la clave secreta.
- S3 Flexible admite la modificación de la clave de acceso, la clave secreta y el nombre del proveedor.

Eliminación de una unidad de nube

Esta operación resulta en la pérdida de todos los datos en la unidad de nube seleccionada para su eliminación. Asegúrese de eliminar todos los archivos antes de eliminar las unidades de nube.

Antes de comenzar

- Compruebe si la transferencia de datos a la nube se está realizando (comando de la CLI: data-movement status). Si es así, detenga la transferencia de datos con el comando de la CLI “data-movement stop”.
- Compruebe si se está ejecutando la limpieza de nube para esta unidad de nube (comando de la CLI: cloud clean status). Si es así, detenga la limpieza de nube mediante el comando de la CLI de “cloud clean”.
- Compruebe si una política de transferencia de datos está configurada para esta unidad de nube (comando de la CLI: data-movement policy show). Si es así, elimine esta política mediante el comando de la CLI “data-movement policy reset”.

Procedimiento

1. Utilice el siguiente comando de la CLI para identificar los archivos en la unidad de nube.
   ```
   # filesys report generate file-location
   ```
2. Elimine los archivos que se encuentran en la unidad de nube que se eliminará.
3. Utilice el siguiente comando de la CLI para ejecutar la limpieza de nube.
   ```
   # cloud clean start nombre-de-unidad
   ```
   Espere a que se complete la limpieza. La limpieza puede tardar mucho tiempo según la cantidad de datos que está presente en la unidad de nube.
4. Deshabilite el sistema de archivos.
5. Utilice el siguiente comando de la CLI para eliminar la unidad de nube.
   ```
   # cloud unit del nombre-de-unidad
   ```
   Internamente, esto marca la unidad de nube como DELETE_PENDING.
6. Use el siguiente comando de la CLI para validar que la unidad de nube está en el estado DELETE_PENDING.
   ```
   # cloud unit list
   ```

7. Active el sistema de archivos.

   El sistema de archivos inicia el procedimiento en segundo plano para eliminar todos los objetos restantes de los depósitos en la nube de esta unidad de nube y, a continuación, elimina los depósitos. Este proceso puede tardar mucho tiempo, según el número de objetos restantes en estos depósitos. Hasta que finaliza la limpieza de depósitos, esta unidad de nube sigue consumiendo una ranura en el sistema Data Domain, lo cual puede impedir la creación de una nueva unidad de nube si ambas ranuras están ocupados.

8. Compruebe periódicamente el estado mediante el siguiente comando de la CLI:

   ```
   # cloud unit list
   ```

   El estado permanece en DELETE_PENDING mientras se ejecuta la limpieza en segundo plano.

9. Verifique desde el portal de S3 del proveedor de nube que se hayan eliminado todos los depósitos correspondientes y el espacio asociado se haya liberado.

10. Si es necesario, vuelva a configurar las políticas de transferencia de datos para los MTrees afectados y reinicie la transferencia de datos.

Resultados

Si tiene dificultades para completar este procedimiento, póngase en contacto con el soporte técnico.

Transferencia de datos

Los datos se transfieren del nivel activo al nivel de nube según lo especificado por la política de transferencia de datos individuales. La política está configurada en función de cada MTree. La transferencia de datos se puede iniciar manualmente o automáticamente mediante un programa.

Adición de políticas de transferencia de datos a MTrees

Un archivo se transfiere del nivel activo al nivel de nube según la fecha en que se modificó por última vez. Para conservar la integridad de los datos, se transfiere todo el archivo en este momento. La *política de transferencia de datos* establece el umbral de antigüedad de archivos, el rango de antigüedad y el destino.

Nota

No se puede configurar una política de transferencia de datos para el MTree /backup.

Procedimiento

1. Seleccione **Data Management** > **MTree**.
2. En el panel superior, seleccione el MTree al que desea agregar una política de transferencia de datos.
3. Haga clic en la pestaña **Resumen**.
4. En **Data Movement Policy**, haga clic en **Add**.
5. Para **File Age in Days**, establezca el umbral de antigüedad de archivos (**Older than**) y, de manera opcional, la antigüedad de rango (**Younger than**).

Nota

La cantidad mínima de días para **Older than** es 14. En el caso de las aplicaciones de respaldo no integradas, no se puede acceder directamente a los archivos que se transfieren al nivel de nube; es necesario recuperarlos al nivel activo para poder acceder a ellos. Por lo tanto, elija el valor de umbral de antigüedad según corresponda para minimizar o evitar la necesidad de acceder a un archivo que se transfirió al nivel de nube.

6. Para **Destination**, especifique el destino de la unidad de nube.
7. Haga clic en **Add**.

Transferencia manual de datos

Puede iniciar y detener la transferencia de datos de forma manual. Se transfieren todos los archivos de todos los MTrees que tengan una política de transferencia de datos válida.

Procedimiento

1. Seleccione **Data Management** > **File System**.
2. En la parte inferior de la página, haga clic en **Show Status of File System Services**.

   Se muestran los siguientes elementos de estado:

   - Sistema de archivos
   - Medición de la capacidad física
   - Transferencia de datos
   - Limpieza de nivel activo

3. Para **Data Movement**, haga clic en **Start**.

Transferencia automática de datos

Puede transferir datos automáticamente mediante una programación y una regulación. Las programaciones pueden ser diarias, semanales o mensuales.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Settings**.
2. Haga clic en la pestaña **Data Movement**.
3. Establezca la programación y la regulación.

Nota

La regulación sirve para adaptar recursos para procesos internos de Data Domain; no afecta el ancho de banda de red.

Nota

Si una unidad de nube no está accesible cuando se ejecuta la transferencia de datos de nivel de nube, se omite la unidad de nube en esa ejecución. La transferencia de datos en esa unidad de nube se produce en la siguiente ejecución si la unidad de nube está disponible. La programación de transferencia de datos determina la duración entre dos ejecuciones. Si la unidad de nube está disponible y usted no puede esperar a la siguiente ejecución programada, puede iniciar manualmente la transferencia de datos.

Recuperación de un archivo desde el nivel de nube

En el caso de las aplicaciones de respaldo no integradas, debe recuperar los datos al nivel activo antes de poder restaurar los datos. Los administradores de respaldo deben activar una recuperación o las aplicaciones de respaldo deben realizar una recuperación antes de que se puedan restaurar los respaldos basados en la nube. Cuando se recupera un archivo, la antigüedad se restablece y se inicia nuevamente desde 0, y el archivo es elegible según la política de antigüedad. Los archivos solo se pueden recuperar en el mismo MTree. Las aplicaciones integradas pueden restaurar un archivo directamente.

Nota

En un contexto de replicación de MTree, el archivo es de solo lectura en el MTree de destino.

Nota

Si un archivo reside solo en una instantánea, no se puede recuperar directamente. Para recuperar un archivo en una instantánea, use FastCopy para copiar el archivo desde la instantánea al MTree activo; a continuación, recupere el archivo de la nube. Un archivo se puede recuperar únicamente de la nube a un MTree activo.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Summary**.
2. Realice una de las siguientes acciones
   - En la sección Cloud Tier del panel Space Usage, haga clic en **Recall**.
   - Expanda el panel de estado File System en la parte inferior de la pantalla y haga clic en **Recall**.

     Nota

     El vínculo **Recall** está disponible únicamente si una unidad de nube está creada y tiene datos.
3. En el cuadro de diálogo Recall File from Cloud, ingrese el nombre exacto del archivo (sin comodines) y la ruta de acceso completa del archivo que se debe recuperar, por ejemplo: `/data/col1/mt11/file1.txt`. Haga clic en **Recall**.
4. Para comprobar el estado de la recuperación, realice una de las siguientes acciones:
   - En la sección Cloud Tier del panel Space Usage, haga clic en **Details**.
   - Expanda el panel de estado File System en la parte inferior de la pantalla y haga clic en **Details**.

Aparece el cuadro de diálogo Cloud File Recall Details con la ruta del archivo, el proveedor de nube, el progreso de la recuperación y la cantidad de datos transferidos. Si se producen errores irrecuperables durante la recuperación, se muestra un mensaje de error. Desplace el cursor sobre el mensaje de error para que aparezca un mensaje de globo con más detalles y posibles acciones correctivas.

Resultados

Una vez que el archivo se ha recuperado al nivel activo, puede restaurar los datos.

Nota

En el caso de las aplicaciones no integradas, una vez que un archivo se ha recuperado del nivel de nube al nivel activo, deben transcurrir al menos 14 días antes de que el archivo sea elegible para la transferencia de datos. Después de 14 días, se producirá el procesamiento de la transferencia de datos normal para el archivo. El archivo tiene que esperar que el umbral de antigüedad o rango de antigüedad vuelva a la nube, ya que esta vez se examinará ptime en lugar de mtime. Esta restricción no se aplica a las aplicaciones integradas.

Nota

Para transferencia de datos, las aplicaciones no integradas configuran una política de transferencia de datos basada en antigüedad en el sistema Data Domain para especificar qué archivos se deben migrar al nivel de nube, y esta política se aplica de manera uniforme a todos los archivos en un MTree. Las aplicaciones integradas utilizan una política de transferencia de datos administrada por aplicaciones, lo cual le permite identificar los archivos específicos que se deben migrar al nivel de nube.

Uso de la CLI para recuperar un archivo desde el nivel de nube

En el caso de las aplicaciones de respaldo no integradas, debe recuperar los datos al nivel activo antes de poder restaurar los datos. Los administradores de respaldo deben activar una recuperación o las aplicaciones de respaldo deben realizar una recuperación antes de que se puedan restaurar los respaldos basados en la nube. Una vez recuperado un archivo, su antigüedad se restablece y se inicia nuevamente desde 0, y el archivo cumplirá con los requisitos según la política de antigüedad. Los archivos solo se pueden recuperar en el MTree de origen. Las aplicaciones integradas pueden recuperar un archivo directamente.

Nota

Si un archivo reside solo en una instantánea, no se puede recuperar directamente. Para recuperar un archivo en una instantánea, use FastCopy para copiar el archivo desde la instantánea al MTree activo; a continuación, recupere el archivo de la nube. Un archivo se puede recuperar únicamente de la nube a un MTree activo.

Procedimiento

1. Compruebe la ubicación del archivo mediante `filesys report generate file-location [path {<nombre-de-ruta> | all}] [output-file <nombre-de-archivo>]`

   El nombre de ruta puede ser un archivo o directorio; si es un directorio, se enumeran todos los archivos en el directorio.

```
Filename                    Location
--------                    --------
/data/col1/mt11/file1.txt   Cloud Unit 1
```

2. Recupere el archivo mediante
   `data-movement recall path <nombre-de-ruta>`

   Este comando es asíncrono e inicia la recuperación.

```
data-movement recall path /data/col1/mt11/file1.txt
Recall started for "/data/col1/mt11/file1.txt".
```

3. Monitoree el estado de la recuperación mediante
   `data-movement status [path {pathname | all | [queued] [running] [completed] [failed]} | to-tier cloud | all]`

```
data-movement status path /data/col1/mt11/file1.txt
Data-movement recall:
---------------------
Data-movement for "/data/col1/mt11/file1.txt": phase 2 of 3
(Verifying)
80% complete; time: phase  XX:XX:XX total  XX:XX:XX
Copied (post-comp): XX XX, (pre-comp) XX XX
```

   Si el estado muestra que no se está ejecutando la recuperación para una ruta determinada, es posible que la recuperación haya terminado o haya fallado.

4. Verifique la ubicación del archivo mediante
   `ifilesys report generate file-location [path {<nombre-de-ruta> | all}] [output-file <nombre-de-archivo>]`

```
Filename                    Location
--------                    --------
/data/col1/mt11/file1.txt   Active
```

Resultados

Una vez que el archivo se ha recuperado al nivel activo, puede restaurar los datos.

Nota

En el caso de las aplicaciones no integradas, una vez que un archivo se ha recuperado del nivel de nube al nivel activo, deben transcurrir al menos 14 días antes de que el archivo sea elegible para la transferencia de datos. Después de 14 días, se producirá el procesamiento de la transferencia de datos normal para el archivo. Esta restricción no se aplica a las aplicaciones integradas.

Nota

Para transferencia de datos, las aplicaciones no integradas configuran una política de transferencia de datos basada en antigüedad en el sistema Data Domain para especificar qué archivos se deben migrar al nivel de nube, y esta política se aplica de manera uniforme a todos los archivos en un MTree. Las aplicaciones integradas utilizan una política de transferencia de datos administrada por aplicaciones, lo cual le permite identificar los archivos específicos que se deben migrar al nivel de nube.

Restauración directa desde el nivel de nube

La restauración directa permite que las aplicaciones no integradas lean archivos directamente desde el nivel de nube sin pasar por el nivel activo.

Entre las consideraciones clave en la elección de utilizar restauración directa, se incluyen las siguientes:

- La restauración directa no requiere una aplicación integrada y es transparente para las aplicaciones no integradas.
- La lectura desde el nivel de nube no requiere que primero se realice una copia en el nivel activo.
- Hay histogramas y estadísticas disponibles para el seguimiento de lecturas directas del nivel de nube.
- La restauración directa es compatible solo con los proveedores de nube ECS.
- Las aplicaciones experimentan latencia de nivel de nube.
- La lectura directa desde el nivel de nube no está optimizada para ancho de banda.
- La restauración directa es compatible con un número reducido de trabajos.

La restauración directa es útil con aplicaciones no integradas que no necesitan conocer el nivel de nube y no tienen que restaurar archivos de nube con frecuencia.

Uso de la interfaz de la línea de comandos (CLI) para configurar DD Cloud Tier

Puede usar la interfaz de la línea de comandos de Data Domain para configurar DD Cloud Tier.

Procedimiento

1. Configure almacenamiento para los niveles activo y de nube. Como requisito previo, las licencias de capacidad adecuadas para los niveles activo y de nube deben estar instaladas.

   a. Asegúrese de que estén instaladas las licencias para las funciones CLOUDTIER-CAPACITY y CAPACITY-ACTIVE. Para verificar la licencia de ELMS:

   ```
   # elicense show
   ```

   Si no está instalada la licencia, utilice el comando `elicense update` para instalarla. Escriba el comando y pegue el contenido del archivo de licencia después de este indicador. Después de pegar, asegúrese de que haya un retorno de carro y luego presione **Control-D** para guardar. Se le solicitará reemplazar licencias y, después de contestar de manera afirmativa, se aplican y se muestran las licencias.

   ```
   # elicense update
   Enter the content of license file and then press Control-D,
   or press Control-C to cancel.
   ```

   b. Visualice el almacenamiento disponible:

   ```
   # storage show all# disk show state
   ```

   c. Agregue almacenamiento al nivel activo:

   ```
   # storage add enclosures <número de gabinete> tier active
   ```

   d. Agregue almacenamiento al nivel de nube.

   ```
   # storage add enclosures <número de gabinete> tier cloud
   ```

2. Instale certificados.

   Antes de poder crear un perfil de nube, debe instalar los certificados asociados. Consulte Importación de certificados en la página 625 para obtener más información.

   Para los proveedores de nube pública AWS, Azure y Virtustream, los certificados de CA raíz se pueden descargar desde https://www.digicert.com/digicert-root-certificates.htm.

   - Para un proveedor de nube de AWS o Azure, descargue el certificado raíz de Baltimore CyberTrust.
   - Para Alibaba, descargue el certificado raíz de GlobalSign R1 en https://support.globalsign.com/customer/portal/articles/1426602-globalsign-rootcertificates.
   - Para un proveedor de nube Virtustream, descargue el certificado de CA raíz de DigiCert High Assurance EV.
   - Para ECS, la autoridad de certificación raíz varía por cliente. Para obtener más información, póngase en contacto con su proveedor de balanceo de carga.

   Los archivos de certificados descargados tienen una extensión .crt. Utilice openssl en cualquier sistema Linux o Unix donde esté instalado para convertir el archivo de formato .crt a .pem.

   ```
   $openssl x509 -inform der -in DigiCertHighAssuranceEVRootCA.crt
   -out DigiCertHighAssuranceEVRootCA.pem
   ```

   ```
   $openssl x509 -inform der -in BaltimoreCyberTrustRoot.crt -out
   BaltimoreCyberTrustRoot.pem
   ```

   ```
   # adminaccess certificate import ca application cloud
   Enter the certificate and then press Control-D, or press
   Control-C to cancel.
   ```

3. Para configurar el sistema Data Domain para transferencia de datos a la nube, primero debe habilitar la función “cloud” y establecer la frase de contraseña del sistema si no lo hizo todavía.

   ```
   # cloud enable
   Cloud feature requires that passphrase be set on the system.
   Enter new passphrase:
   Re-enter new passphrase:
   Passphrases matched.
   The passphrase is set.
   Encryption is recommended on the cloud tier.
       Do you want to enable encryption? (yes|no) [yes]:
   Encryption feature is enabled on the cloud tier.
   Cloud feature is enabled.
   ```

4. Configure el perfil de nube con las credenciales del proveedor de nube. Las variables y los indicadores varían según el proveedor.

   ```
   # cloud profile add <nombredeperfil>
   ```

   Nota

   Por motivos de seguridad, este comando no muestra las claves de acceso ni la seña secreta que usted especifica.

   Seleccione el proveedor:

   ```
   Enter provider name (alibabacloud|aws|azure|ecs|google|
   s3_flexible|virtustream)
   ```

- Alibaba Cloud requiere la clave de acceso, la clave secreta, la clase de almacenamiento y la región.
- AWS S3 requiere la clave de acceso, la clave secreta, la clase de almacenamiento y la región.
- Azure requiere el nombre de cuenta, independientemente de que sea una cuenta Azure Government o no, la clave primaria, la clave secundaria y la clase de almacenamiento.
- ECS requiere la entrada de la clave de acceso, la seña secreta y el terminal.
- Google Cloud Platform requiere la clave de acceso, la clave secreta y la región. (La clase de almacenamiento es Nearline).
- Los proveedores de S3 Flexible requieren el nombre del proveedor, la clave de acceso, la clave secreta, la región, el terminal y la clase de almacenamiento.
- Virtustream requiere la clave de acceso, la seña secreta, la clase de almacenamiento y la región.

Al final de cada adición de perfil, se le preguntará si desea configurar un proxy. Si lo hace, se requieren estos valores: *nombre de host de proxy*, *puerto de proxy*, *nombre de usuario de proxy* y *contraseña de proxy*.

5. Verifique la configuración de perfil de nube:

```
# cloud profile show
```

6. Si no se ha creado, cree el sistema de archivos de nivel activo:

```
# filesys create
```

7. Active el sistema de archivos:

```
# filesys enable
```

8. Configure la unidad de nube:

```
# cloud unit add nombredeunidad profile nombredeperfil
```

Use el comando `cloud unit list` para enumerar las unidades de nube.

9. De manera opcional, configure el cifrado para la unidad de nube.
   a. Verifique que la licencia ENCRYPTION esté instalada.

```
# elicense show
```

   b. Active el cifrado para la unidad de nube:

```
# filesys encryption enable cloud-unit nombredeunidad
```

   c. Verifique el estado de cifrado:

```
# filesys encryption status
```

10. Cree uno o más MTrees.

```
# mtree create /data/col1/mt11
```

11. Verifique la configuración de DD Cloud Tier:

```
# cloud provider verify
This operation will perform test data movement after creating a temporary profile and
bucket.
```

```
Do you want to continue? (yes|no) [yes]:
Enter provider name (aws|azure|virtustream|ecs|s3_generic): aws
Enter the access key:
Enter the secret key:
Enter the region (us-east-1|us-west-1|us-west-2|eu-west-1|apnortheast-1|ap-southeast-1|
ap-southeast-2|
sa-east-1|ap-south-1|ap-northeast-2|eu-central-1):

Verifying cloud provider …
This process may take a few minutes.
Cloud Enablement Check:
 Checking Cloud feature enabled: PASSED
 Checking Cloud volume: PASSED

Connectivity Check:
 Checking firewall access: PASSED
 Validating certificate PASSED

Account Validation:
 Creating temporary profile: PASSED
 Creating temporary bucket: PASSED

S3 API Validation:
 Validating Put Bucket: PASSED
 Validating List Bucket: PASSED
 Validating Put Object: PASSED
 Validating Get Object: PASSED
 Validating List Object: PASSED
 Validating Delete Object: PASSED
 Validating Bulk Delete: PASSED

Cleaning Up:
 Deleting temporary bucket: PASSED
 Deleting temporary profile: PASSED

Provider verification passed.
```

12. Configure la política de migración de archivos para este MTree. Puede especificar varios MTrees en este comando. La política se puede basar en el umbral o el intervalo de antigüedad.

    a. Para configurar el umbral de antigüedad (migración de archivos anteriores a la antigüedad especificada a la nube):

    ```
    # data-movement policy set age-threshold antigüedad_en_días
    to-tier cloud cloud-unit nombredeunidad mtrees nombredemtree
    ```

    b. Para configurar el rango de antigüedad (migración solo de esos archivos que se encuentran en el rango de antigüedad especificado):

    ```
    # data-movement policy set age-range min-age
    antigüedad_en_días max-age antigüedad_en_días to-tier cloud
    cloud-unit nombredeunidad mtrees nombredemtree
    ```

13. Exporte el sistema de archivos y, desde el cliente, monte el sistema de archivos y recopile datos en el nivel activo. Cambie la fecha de modificación de los archivos recopilados a fin de que cumplan los requisitos para la migración de datos. (Configure la fecha en anteriores al valor de umbral de antigüedad especificado al configurar la política de transferencia de datos).
14. Inicie la migración de los archivos antiguos. Una vez más, puede especificar varios MTrees con este comando.

    ```
    # data-movement start mtrees nombredemtree
    ```

    Para comprobar el estado de la transferencia de datos:

    ```
    # data-movement status
    ```

También puede ver el progreso de la transferencia de datos:

```
# data-movement watch
```

15. Verifique que la migración de archivos haya funcionado y que los archivos ahora estén en el nivel de nube:

```
# filesys report generate file-location path all
```

16. Una vez que ha migrado un archivo al nivel de nube, no puede leer directamente del archivo (si intenta hacerlo, se produce un error). El archivo solo se puede recuperar al nivel activo. Para recuperar un archivo al nivel activo:

```
# data-movement recall path nombrederuta
```

Configuración del cifrado de unidades de nube DD

El cifrado se puede habilitar en tres niveles: sistema Data Domain, nivel activo y unidad de nube. El cifrado de nivel activo solo es aplicable si el cifrado está habilitado para el sistema Data Domain. Las unidades de nube tienen controles independientes para habilitar el cifrado.

Procedimiento

1. Seleccione **Data Management** > **File System** > **DD Encryption**.

   Nota

   Si ninguna licencia de cifrado está presente en el sistema, se muestra la página Add Licenses.

2. En el panel DD Encryption, realice una de las siguientes acciones.
   - Para habilitar el cifrado de **Cloud Unit *x***, haga clic en **Enable**.
   - Para deshabilitar el cifrado de **Cloud Unit *x***, haga clic en **Disable**.

   Nota

   Se le solicitará que ingrese las credenciales del director de seguridad para habilitar el cifrado.

3. Escriba el **nombre de usuario** y la **contraseña** del director de seguridad. Como opción, seleccione **Restart file system now**.
4. Haga clic en **Enable** o **Disable** según corresponda.
5. En el panel File System Lock, bloquee o desbloquee el sistema de archivos.
6. En el panel Key Management, haga clic en **Configure**.
7. En el cuadro de diálogo Change Key Manager, configure las credenciales del director de seguridad y el administrador de claves.

   Nota

   Se permite el cifrado de nube solo a través de Data Domain Embedded Key Manager. No se admiten administradores de claves externos.

8. Haga clic en **OK**.

9. Utilice el panel DD Encryption Keys para configurar las claves de cifrado.

Información necesaria en caso de pérdida del sistema

Una vez que el nivel de nube está configurado en el sistema Data Domain, registre la siguiente información sobre el sistema y almacénela en una ubicación segura fuera del sistema Data Domain. Esta información será necesaria para recuperar los datos del nivel de nube en caso de que el sistema Data Domain se pierda.

Nota

Este proceso está diseñado para situaciones de emergencia únicamente e implica mucho tiempo y esfuerzo del personal de Ingeniería de Data Domain.

- Número de serie del sistema Data Domain original
- Frase de contraseña del sistema Data Domain original
- Número de versión de DD OS del sistema Data Domain original
- Información de perfil y de configuración del nivel de nube

Uso de DD Replicator con Cloud Tier

La replicación de recopilaciones no es compatible con los sistemas Data Domain habilitados para Cloud Tier.

La replicación de directorios solo funciona en el MTree /backup, y este MTree no se puede asignar a Cloud Tier. Por lo tanto, la replicación de directorios no se ve afectada por Cloud Tier.

La replicación administrada de archivos y la replicación de MTree son compatibles en los sistemas Data Domain habilitados para Cloud Tier. Uno o ambos sistemas pueden tener habilitado Cloud Tier. Si el sistema de origen está habilitado para Cloud Tier, es posible que los datos deban leerse desde la nube si el archivo ya se migró a Cloud Tier. Un archivo replicado siempre se coloca primero en el nivel activo del sistema de destino incluso cuando Cloud Tier está habilitado. Un archivo puede devolverse de Cloud Tier al nivel activo en el MTree de origen solamente. La recuperación de un archivo en el MTree de destino no está permitida.

Nota

Si el sistema de origen ejecuta DD OS 5.6 o 5.7 y replica en un sistema habilitado para Cloud Tier utilizando la replicación de MTree, el sistema de origen debe actualizarse a una versión que pueda replicar datos a un sistema habilitado para Cloud Tier. Consulte los requisitos del sistema de las *Notas de la versión de DD OS*.

Nota

Los archivos en Cloud Tier no pueden utilizarse como archivos de base para las operaciones de respaldo virtual sintético. Los respaldos completos eternos o sintéticos incrementales deben garantizar que los archivos permanezcan en el nivel activo si se van a utilizar en la síntesis virtual de respaldos nuevos.

Uso de la biblioteca de cintas virtuales (VTL) de DD con Cloud Tier

En sistemas configurados con Cloud Tier y DD VTL, se admite el uso del almacenamiento de nube como vault de VTL. Para utilizar las cintas de DD VTL fuera de la nube, primero obtenga la licencia del almacenamiento de nube y configúrelo, y luego selecciónelo como la ubicación de vault de VTL.

En Transferencia de cintas de DD VTL a la nube en la página 395, se proporciona información adicional acerca de cómo utilizar VTL con Cloud Tier.

Visualización de gráficos de consumo de capacidad para DD Cloud Tier

Hay tres gráficos disponibles para ver las estadísticas de consumo de Cloud Tier: Space Usage, Consumption y Daily Written.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Charts**.
2. Para **Chart**, seleccione una de las siguientes opciones:
   - Space Usage
   - Consumption
   - Daily Written
3. Para **Scope**, seleccione **Cloud Tier**.
   - La pestaña Space Usage muestra el uso del espacio con el tiempo, en MiB. Puede seleccionar una duración (una semana, un mes, tres meses, un año o todas). Los datos se presentan (codificados por color) como usados antes de la compresión (azul), usados después de la compresión (rojo) y el factor de compresión (verde).
   - La pestaña Consumption muestra la cantidad de almacenamiento después de la compresión utilizada y la tasa de compresión con el tiempo, lo cual le permite analizar las tendencias de consumo. Puede seleccionar una duración (una semana, un mes, tres meses, un año o todas). Los datos se presentan (codificados por color) como capacidad (azul), utilizados después de la compresión (rojo), factor de compresión (verde), limpieza (naranja) y transferencia de datos (violeta).
   - La pestaña Daily Written muestra la cantidad de datos escritos por día. Puede seleccionar una duración (una semana, un mes, tres meses, un año o todas). Los datos se presentan (codificados por color) como escritos antes de la compresión (azul), utilizados después de la compresión (rojo) y el factor de compresión (verde).

Registros de DD Cloud Tier

Si DD Cloud Tier sufre una falla de cualquier tipo, en la configuración o la operación, el sistema crea automáticamente una carpeta con un registro de fecha y hora asociado al momento de la falla.

Monte el directorio `/ddvar/log/debug` para acceder a los registros.

Nota

La salida del comando `log list view` no enumera todos los archivos de registro detallados creados para la falla de DD Cloud Tier.

Uso de la interfaz de la línea de comandos (CLI) para eliminar DD Cloud Tier

Puede usar la interfaz de la línea de comandos de Data Domain para eliminar la configuración de DD Cloud Tier.

Antes de comenzar

Elimine todos los archivos en las unidades de nube antes de eliminar la configuración de DD Cloud Tier del sistema. Ejecute el comando `filesys report generate file-location path all output-file file_loc` para identificar los archivos en las unidades de nube y elimínelos de los puntos de montaje NFS de los MTrees.

Nota

El comando mencionado anteriormente crea el informe `file_loc` en el directorio `/ddr/var/`.

Procedimiento

1. Deshabilite el sistema de archivos.

```
# filesys disable

This action will disable the file system.
Applications may experience interruptions
while the file system is disabled.
    Are you sure? (yes|no) [no]: yes

ok, proceeding.

Please wait.............
The filesystem is now disabled.
```

2. Enumere las unidades de nube en el sistema.

```
# cloud unit list
Name           Profile        Status
------------   ------------   ------
cloud_unit-1   cloudProfile   Active
cloud_unit-2   cloudProfile2  Active
------------   ------------   ------
```

3. Elimine las unidades de nube de forma individual.

```
# cloud unit del cloud_unit-1
```

```
This command irrevocably destroys all data
 in the cloud unit "cloud_unit-1".
    Are you sure? (yes|no) [no]: yes

ok, proceeding.

Enter sysadmin password to confirm:

Destroying cloud unit "cloud_unit-1"
Cloud unit 'cloud_unit-1' deleted. The data in the cloud will be deleted asynchronously
on the filesystem startup.

# cloud unit del cloud_unit-2

This command irrevocably destroys all data
 in the cloud unit "cloud_unit-2".
    Are you sure? (yes|no) [no]: yes

ok, proceeding.

Enter sysadmin password to confirm:

Destroying cloud unit "cloud_unit-2"
Cloud unit 'cloud_unit-2' deleted. The data in the cloud will be deleted asynchronously
on the filesystem startup.
```

4. Verifique que las operaciones de eliminación estén en curso.

```
# cloud unit list
Name           Profile        Status
------------   ------------   ------
cloud_unit-1   cloudProfile   Delete-Pending
cloud_unit-2   cloudProfile2  Delete-Pending
------------   ------------   ------
```

5. Reinicie el sistema de archivos.

```
# filesys enable
Please wait.....................................
The filesystem is now enabled.
```

6. Ejecute el comando `cloud unit list` para verificar que no aparezca ninguna unidad de nube.

   Póngase en contacto con el servicio de soporte si una o ambas unidades de nube se siguen mostrando con el estado `Delete-Pending`.

7. Identifique los gabinetes de discos que están asignados a DD Cloud Tier.

```
# storage show tier cloud

Cloud tier details:
Disk   Disks               Count   Disk     Additional
Group                              Size     Information
------ ------------------- ------  -------- ------------
dgX    2.1-2.15, 3.1-3.15  30      3.6 TiB
------ ------------------- ------  -------- ------------
Current cloud tier size: 0.0 TiB
Cloud tier maximum capacity: 108.0 TiB
```

8. Elimine los gabinetes de discos de DD Cloud Tier.

```
# storage remove enclosures 2, 3

Removing enclosure 2...Enclosure 2 successfully removed.

Updating system information...done

Successfuly removed: 2 done
```

```
Removing enclosure 3...Enclosure 3 successfully removed.
Updating system information...done
Successfuly removed: 3 done
```

CAPÍTULO 19

DD Extended Retention

Este capítulo incluye:

- Descripción general de DD Extended Retention 546
- Protocolos compatibles con DD Extended Retention 548
- Alta disponibilidad y Extended Retention 548
- Uso de DD Replicator con DD Extended Retention 548
- Hardware y licencias para DD Extended Retention 550
- Administración de DD Extended Retention 555
- Actualizaciones y recuperación con DD Extended Retention 566
- Migrar datos de nivel de archiving a DD Cloud Tier 568

Descripción general de DD Extended Retention

Data Domain Extended Retention (DD Extended Retention) ofrece un enfoque de organización en niveles interno que permite la retención rentable de datos de respaldo a largo plazo en un sistema DD. Con DD Extended Retention, puede aprovechar los sistemas DD para retención de respaldos a largo plazo y minimizar el uso de cintas.

Nota

DD Extended Retention se conocía anteriormente como *Data Domain Archiver.*

Sistema de archivos en dos niveles

El sistema interno de archivos en dos niveles de un sistema DD habilitado para DD Extended Retention consiste en un *nivel activo* y un *nivel de retención*. Sin embargo, el sistema de archivos aparece como una entidad única. Los datos entrantes se colocan primero en el nivel activo del sistema de archivos. Luego, los datos (en forma de archivos completos) se transfieren al nivel de retención del sistema de archivos, como lo especifica su *Política de transferencia de datos* individual. Por ejemplo, el nivel activo puede conservar los respaldos incrementales diarios y semanales completos por 90 días, mientras que el nivel de retención puede conservar los completos mensuales por siete años.

El nivel de retención consta de una o más unidades de retención, cada una de las cuales puede extraer el almacenamiento de una o más bandejas.

Nota

A partir de la versión 5.5.1 de DD OS, solo se permite una unidad de retención por nivel de retención. Sin embargo, los sistemas instalados antes de la versión 5.5.1 de DD OS pueden continuar teniendo más de una unidad de retención, pero no se les podrá agregar ninguna otra unidad de retención.

Transparencia de las operaciones

Los sistemas DD habilitados para DD Extended Retention son compatibles con las aplicaciones de respaldo existentes que utilizan métodos de acceso a datos simultáneos por medio de protocolos de servicios de archivos NFS y CIFS mediante Ethernet, mediante DD VTL para sistemas abiertos e IBMi, o como objetivo basado en disco con interfaces específicas de aplicaciones, como DD Boost (para usar con Avamar®, NetWorker®, GreenPlum, Symantec OpenStorage y Oracle RMAN).

DD Extended Retention extiende la arquitectura de DD con la transferencia automática y transparente de datos del nivel activo al nivel de retención. Se puede acceder a todos los datos en los dos niveles, aunque puede haber una pequeña demora en el acceso inicial a los datos en el nivel de retención. El espacio de nombres del sistema es global y no resulta afectado por la transferencia de datos. No se requiere el particionamiento del sistema para aprovechar el sistema de archivos en dos niveles.

Política de transferencia de datos

La *Política de transferencia de datos*, que usted puede personalizar, es la política por la cual los archivos se transfieren del nivel activo al nivel de retención. Se basa en la hora en que el archivo se modificó por última vez. Puede definir otra política para cada subconjunto de datos diferente, ya que la política se puede establecer individualmente para cada MTree. Los archivos que se pueden actualizar requieren una política diferente a la de los que nunca se modifican.

Deduplicación dentro de la unidad de retención
Con fines de aislamiento de fallas, la deduplicación se produce por completo dentro de la unidad de retención para los sistemas DD habilitados para DD Extended Retention. No hay deduplicación cruzada entre los niveles activo y de retención, o entre las diferentes unidades de retención (si corresponde).

Almacenamiento extraído de cada nivel
El concepto de organización en niveles se extiende al nivel de almacenamiento para un sistema DD habilitado para DD Extended Retention. El nivel activo del sistema de archivos extrae el almacenamiento del nivel activo de almacenamiento. El nivel de retención del sistema de archivos extrae el almacenamiento del nivel de retención del almacenamiento.

Nota

Para los niveles activo y de retención, DD OS 5.2 y las versiones posteriores son compatibles con las bandejas ES20 y ES30, y DD OS 5.7 y las versiones posteriores son compatibles con las bandejas DS60 en algunos modelos. No se pueden combinar distintos tipos de bandejas Data Domain en el mismo conjunto de bandejas, y los conjuntos de bandejas deben balancearse de acuerdo con las reglas de configuración especificadas en la *Guía de hardware de bandeja de expansión ES30* o en la *Guía de hardware de bandeja de expansión DS60*. Con DD Extended Retention, puede incorporar mucho más almacenamiento a la misma controladora. Por ejemplo, puede conectar hasta un máximo de 56 bandejas ES30 en un DD990 con DD Extended Retention. El nivel activo debe incluir almacenamiento que tenga al menos una bandeja. Para la configuración mínima y máxima de bandejas para los modelos de controladora de Data Domain, consulte las guías de hardware de bandejas de expansión de ES30 y DS60.

Protección de datos
En un sistema DD habilitado para DD Extended Retention, los datos se protegen con funciones de aislamiento de fallas incorporadas, funcionalidades de recuperación ante desastres y DIA (Arquitectura de invulnerabilidad de datos). La DIA comprueba los archivos cuando se transfieren del nivel activo al nivel de retención. Una vez que los datos se copian en el nivel de retención, las estructuras del sistema de archivos y del contenedor se vuelven a leer y se verifican. La ubicación del archivo se actualiza y el espacio en el nivel activo se recupera después de se verifica que el archivo se ha escrito correctamente en el nivel de retención.

Cuando se completa una unidad de retención, la información del espacio de nombres y los archivos del sistema se copian en esta de modo que sea posible recuperar los datos de la unidad de retención incluso si se pierden otras partes del sistema.

Nota

El saneamiento y otras formas de replicación no son compatibles con los sistemas DD habilitados para DD Extended Retention.

Recuperación de espacio
Para recuperar espacio que se ha liberado al transferir datos al nivel de retención, puede usar *Space Reclamation* (a partir del SO 5.3 de DD), que funciona en segundo plano como una actividad de baja prioridad. Se suspende cuando hay actividades con más prioridad, como la transferencia y la limpieza de datos.

Cifrado de datos inactivos
A partir de la versión 5.5.1 de DD OS, puede usar la función *Encryption of Data at Rest* en sistemas DD habilitados para DD Extended Retention, si tiene una licencia de cifrado. El cifrado no está activado de forma predeterminada.

Es una extensión de la capacidad de cifrado ya disponible, anterior a la versión 5.5.1 de DD OS, para sistemas que no usan DD Extended Retention.

Consulte el capítulo *Administración del cifrado de datos inactivos* en esta guía para obtener instrucciones completas acerca de la configuración y del uso de la función de cifrado.

Protocolos compatibles con DD Extended Retention

Los sistemas habilitados para DD Extended Retention son compatibles con los protocolos NFS, CIFS y DD Boost. Se agregó la compatibilidad con DD VTL en DD OS 5.2 y la compatibilidad con NDMP se agregó en DD OS 5.3.

Nota

Para ver una lista de las aplicaciones compatibles con DD Boost, consulte la *lista de compatibilidad con DD Boost* en el sitio del servicio de soporte en línea.

Cuando usa DD Extended Retention, los datos primero se almacenan en el nivel activo. Los archivos se transfieren en su totalidad al nivel de retención, como lo especifica la política de transferencia de datos. Todos los archivos figuran en el mismo espacio de nombre. No se requiere la partición de datos, y puede continuar expandiendo el sistema de archivos como lo desee.

Todos los datos son visibles para todos los usuarios, y todos los metadatos del sistema de archivos se encuentran en el nivel activo.

La desventaja de transferir datos del nivel activo al nivel de retención es una mayor capacidad frente a un tiempo de acceso levemente más lento si la unidad a la que se debe acceder no está preparada para esto.

Alta disponibilidad y Extended Retention

Los sistemas Data Domain con alta disponibilidad (HA) habilitada no son compatibles con DD Extended Retention. DD OS actualmente no admite Extended Retention con alta disponibilidad.

Uso de DD Replicator con DD Extended Retention

Algunas formas de replicación son compatibles con los sistemas DD habilitados para DD Extended Retention.

Los tipos de replicación compatibles dependen de los datos que se deben proteger:

- Para proteger datos en un sistema como *origen*, un sistema DD habilitado para DD Extended Retention admite la replicación de recopilación, la replicación de MTrees y una replicación de archivos administrada de DD Boost.
- Para proteger datos de otros sistemas como un *destino*, un sistema DD habilitado para DD Extended Retention también admite la replicación de directorios, además de la replicación de recopilación, la replicación de MTrees y la replicación de archivos administrada de DD Boost.

Nota

La replicación delta (optimización de ancho de banda bajo) no es compatible con DD Extended Retention. Debe deshabilitar la replicación delta en todos los contextos antes de habilitar DD Extended Retention en un sistema DD.

Replicación de recopilación con DD Extended Retention

La replicación de recopilación se lleva a cabo entre el nivel activo y la unidad de retención correspondientes de los dos sistemas DD con DD Extended Retention habilitado. Si fallan el nivel activo o la unidad de retención en el origen, los datos se pueden copiar de la unidad correspondiente en el sitio remoto a una nueva unidad, que se le envía como unidad de reemplazo.

Entre los requisitos previos para la configuración de la replicación de recopilación, se incluyen los siguientes:

- Los sistemas de origen y de destino deben estar configurados como sistemas DD con DD Extended Retention habilitado.
- El sistema de archivos no se debe habilitar en el destino hasta que se haya agregado en él la unidad de retención y se haya configurado la replicación.

Replicación de directorio con DD Extended Retention

Para la replicación de directorio, un sistema DD habilitado para Extended Retention funciona como destino de replicación y admite topologías personalizadas y muchos a uno desde un sistema DD compatible. Sin embargo, los sistemas DD habilitados para DD Extended Retention no son compatibles con la replicación de dirección bidireccional y no pueden ser *orígenes* de replicación de directorio.

Nota

Para copiar datos usando la replicación de directorio en un sistema DD habilitado para DD Extended Retention, el origen debe ejecutar el SO DD 5.0 o una versión posterior. Por lo tanto, en los sistemas que ejecutan el SO DD 5.0 o una versión anterior, debe importar primero los datos a un sistema intermedio que ejecute el SO DD 5.0 o una versión posterior. Por ejemplo, la replicación de un sistema habilitado para Extended Retention con un SO DD 4.9 podría hacerse a otro sistema con un SO DD 5.2. Entonces, la replicación podría realizarse desde el sistema SO DD 5.2 al sistema SO DD 4.9.

Replicación de MTree con DD Extended Retention

Puede configurar la replicación de MTree entre dos sistemas DD habilitados para DD Extended Retention. Los datos replicados se colocan primero en el nivel activo en el sistema de destino. La política de transferencia de datos en el sistema de destino determina cuándo los datos replicados se transfieren al nivel de retención.

Tenga en cuenta que las restricciones y políticas de la replicación de MTree varían según la versión de SO DD, de la siguiente manera:

- A partir del SO DD 5.1, los datos pueden replicarse desde un sistema habilitado para Extended Retention que no sea DD a un sistema habilitado para DD Extended Retention con replicación de MTree.

- A partir del SO DD 5.2, los datos pueden protegerse dentro de un nivel activo replicándolo al nivel activo de un sistema habilitado para DD Extended Retention.
- A partir del SO DD 5.5, la replicación de MTree se admite desde un sistema habilitado para DD Extended Retention a un sistema habilitado para DD Extended Retention que no sea DD si ambos están ejecutando el SO DD 5.5 o una versión posterior.
- Para el SO DD 5.3 y 5.4, si planea habilitar DD Extended Retention, no configure la replicación para el MTree de respaldo en la máquina de origen. (El SO DD 5.5 y las versiones posteriores no tienen esta restricción).

Replicación de archivos administrada con DD Extended Retention

Para los sistemas DD habilitados para DD Extended Retention, las topologías compatibles para la replicación de archivos administrada por DD Boost son personalizadas, bidireccional, de uno a muchos, de muchos a uno y en cascada.

Nota

Para DD Boost 2.3 o versiones posteriores, puede especificar cómo varias copias se realizan y administran dentro de la aplicación de respaldo.

Hardware y licencias para DD Extended Retention

Se necesitan determinadas configuraciones de hardware para sistemas DD habilitados para DD Extended Retention. Las licencias, especialmente las licencias de bandejas separadas, también son específicas para esta función.

Hardware compatible para DD Extended Retention

Los requisitos de hardware para sistemas DD habilitados para DD Extended Retention incluyen requisitos de memoria, bandejas, tarjetas NIC/FC, etc. Para obtener detalles sobre las configuraciones de hardware requeridas para DD Extended Retention, consulte a la guía de instalación y configuración de su sistema DD y las guías de hardware de bandejas de expansión de sus bandejas de expansión.

Los siguientes sistemas DD admiten DD Extended Retention:

DD860

- 72 GB de RAM
- 1 módulo de I/O NVRAM (1 GB)
- 3 módulos de I/O SAS de cuatro puertos
- 2 puertos de 1 GbE en la tarjeta madre
- 0 a 2 tarjetas de I/O NIC de 1/10 GbE para conectividad externa
- 0 a 2 tarjetas de I/O HBA FC de dos puertos para conectividad externa
- 0 a 2 tarjetas NIC y FC combinadas
- 1 a 24 bandejas ES20 o ES30 (discos de 1 TB o 2 TB), que no deben superar la capacidad útil máxima del sistema de 142 TB

Si DD Extended Retention está habilitado en un sistema DD860, la capacidad útil de almacenamiento máxima de un nivel activo es de 142 TB. El nivel de retención puede tener una capacidad útil máxima de 142 TB. Los niveles activo y de retención tienen una capacidad útil de almacenamiento total de 284 TB.

DD990

- 256 GB de RAM
- 1 módulo de I/O NVRAM (2 GB)
- 4 módulos de I/O SAS de cuatro puertos
- 2 puertos de 1 GbE en la tarjeta madre
- 0 a 4 tarjetas de I/O NIC de 1 GbE para conectividad externa
- 0 a 3 tarjetas NIC de 10 GbE para conectividad externa
- 0 a 3 tarjetas HBA FC de dos puertos para conectividad externa
- 0 a 3 tarjetas NIC y FC combinadas, que no deben superar tres de ningún módulo de I/O específico
- 1 a 56 bandejas ES20 o ES30 (discos de 1, 2 o 3 TB), que no deben superar la capacidad útil máxima del sistema de 570 TB

Si DD Extended Retention está habilitado en un sistema DD990, la capacidad útil de almacenamiento máxima del nivel activo es de 570 TB. El nivel de retención puede tener una capacidad útil máxima de 570 TB. Los niveles activo y de retención tienen una capacidad útil de almacenamiento total de 1140 TB.

DD4200

- 128 GB de RAM
- 1 módulo de I/O NVRAM (4 GB)
- 4 módulos de I/O SAS de cuatro puertos
- 1 puerto de 1 GbE en la tarjeta madre
- 0 a 6 tarjetas NIC de 1/10 GbE para conectividad externa
- 0 a 6 tarjetas HBA FC de dos puertos para conectividad externa
- 0 a 6 tarjetas NIC y FC combinadas, que no deben superar cuatro de ningún módulo de I/O específico
- 1 a 16 bandejas ES30 (discos de 2 o 3 TB), que no deben superar la capacidad útil máxima del sistema de 192 TB Se admiten bandejas SATA ES30 (discos de 1, 2 o 3 TB) para actualizaciones de controladoras del sistema.

Si DD Extended Retention está habilitado en un sistema DD4200, la capacidad útil de almacenamiento máxima del nivel activo es de 192 TB. El nivel de retención puede tener una capacidad útil máxima de 192 TB. Los niveles activo y de retención tienen una capacidad útil de almacenamiento total de 384 TB. Se admite conectividad externa para configuraciones de DD Extended Retention de hasta 16 bandejas.

DD4500

- 192 GB de RAM
- 1 módulo de I/O NVRAM (4 GB)
- 4 módulos de I/O SAS de cuatro puertos
- 1 puerto de 1 GbE en la tarjeta madre
- 0 a 6 tarjetas de I/O NIC de 1/10 GbE para conectividad externa
- 0 a 6 tarjetas HBA FC de dos puertos para conectividad externa
- 0 a 5 tarjetas NIC y FC combinadas, que no deben superar cuatro de ningún módulo de I/O específico

- 1 a 20 bandejas ES30 (discos de 2 o 3 TB), que no deben superar la capacidad útil máxima del sistema de 285 TB Se admiten bandejas SATA ES30 (1, 2 o 3 TB) para actualizaciones de controladoras del sistema.

Si DD Extended Retention está habilitado en un sistema DD4500, la capacidad útil de almacenamiento máxima del nivel activo es de 285 TB. El nivel de retención puede tener una capacidad útil máxima de 285 TB. Los niveles activo y de retención tienen una capacidad útil de almacenamiento total de 570 TB. Se admite conectividad externa para configuraciones de DD Extended Retention de hasta 24 bandejas.

DD6800

- 192 GB de RAM
- 1 módulo de I/O NVRAM (8 GB)
- 3 módulos de I/O SAS de cuatro puertos
- 1 puerto de 1 GbE en la tarjeta madre
- 0 a 4 tarjetas NIC de 1/10 GbE para conectividad externa
- 0 a 4 tarjetas HBA FC de dos puertos para conectividad externa
- 0 a 4 tarjetas NIC y FC combinadas
- Las combinaciones de bandejas se documentan en la guía de instalación y configuración de su sistema DD y en las guías de hardware de bandejas de expansión de sus bandejas de expansión.

Si DD Extended Retention está habilitado en un sistema DD6800, la capacidad útil de almacenamiento máxima del nivel activo es de 288 TB. El nivel de retención puede tener una capacidad útil máxima de 288 TB. Los niveles activos y de retención tienen una capacidad útil de almacenamiento total de 0.6 PB. Se admite conectividad externa para configuraciones de DD Extended Retention de hasta 28 bandejas.

DD7200

- 256 GB de RAM
- 1 módulo de I/O NVRAM (4 GB)
- 4 módulos de I/O SAS de cuatro puertos
- 1 puerto de 1 GbE en la tarjeta madre
- 0 a 6 tarjetas NIC de 1/10 GbE para conectividad externa
- 0 a 6 tarjetas HBA FC de dos puertos para conectividad externa
- 0 a 5 tarjetas NIC y FC combinadas, que no deben superar cuatro de ningún módulo de I/O específico
- 1 a 20 bandejas ES30 (discos de 2 o 3 TB), que no deben superar la capacidad útil máxima del sistema de 432 TB Se admiten bandejas SATA ES30 (1, 2 o 3 TB) para actualizaciones de controladoras del sistema.

Si DD Extended Retention está habilitado en un sistema DD7200, la capacidad útil de almacenamiento máxima del nivel activo es de 432 TB. El nivel de retención puede tener una capacidad útil máxima de 432 TB. Los niveles activo y de retención tienen una capacidad útil de almacenamiento total de 864 TB. Se admite conectividad externa para configuraciones de DD Extended Retention de hasta 32 bandejas.

DD9300

- 384 GB de RAM
- 1 módulo de I/O NVRAM (8 GB)

- 3 módulos de I/O SAS de cuatro puertos
- 1 puerto de 1 GbE en la tarjeta madre
- 0 a 4 tarjetas NIC de 1/10 GbE para conectividad externa
- 0 a 4 tarjetas HBA FC de dos puertos para conectividad externa
- 0 a 4 tarjetas NIC y FC combinadas
- Las combinaciones de bandejas se documentan en la guía de instalación y configuración de su sistema DD y en las guías de hardware de bandejas de expansión de sus bandejas de expansión.

Si DD Extended Retention está habilitado en un sistema DD9300, la capacidad útil de almacenamiento máxima del nivel activo es de 720 TB. El nivel de retención puede tener una capacidad útil máxima de 720 TB. Los niveles activos y de retención tienen una capacidad útil de almacenamiento total de 1.4 PB. Se admite conectividad externa para configuraciones de DD Extended Retention de hasta 28 bandejas.

DD9500

- 512 GB de RAM
- 1 módulo de I/O NVRAM (8 GB)
- 4 módulos de I/O SAS de cuatro puertos
- 1 puerto de 1 GbE cuádruple en la tarjeta madre
- 0 a 4 tarjetas NIC de 10 GbE para conectividad externa
- 0 a 4 tarjetas HBA FC de 16 GbE de dos puertos para conectividad externa
- Las combinaciones de bandejas se documentan en la guía de instalación y configuración de su sistema DD y en las guías de hardware de bandejas de expansión de sus bandejas de expansión.

Si DD Extended Retention está habilitado en un sistema DD9500, la capacidad útil de almacenamiento máxima del nivel activo es de 864 TB. El nivel de retención puede tener una capacidad útil máxima de 864 TB. Los niveles activo y de retención tienen una capacidad útil de almacenamiento total de 1.7 PB. Se admite conectividad externa para configuraciones de DD Extended Retention de hasta 56 bandejas.

DD9800

- 768 GB de RAM
- 1 módulo de I/O NVRAM (8 GB)
- 4 módulos de I/O SAS de cuatro puertos
- 1 puerto de 1 GbE cuádruple en la tarjeta madre
- 0 a 4 tarjetas NIC de 10 GbE para conectividad externa
- 0 a 4 tarjetas HBA FC de 16 GbE de dos puertos para conectividad externa
- Las combinaciones de bandejas se documentan en la guía de instalación y configuración de su sistema DD y en las guías de hardware de bandejas de expansión de sus bandejas de expansión.

Si DD Extended Retention está habilitado en un sistema DD9800, la capacidad útil de almacenamiento máxima del nivel activo es de 1,008 TB. El nivel de retención puede tener una capacidad útil máxima de 1,008 TB. Los niveles activos y de retención tienen una capacidad útil de almacenamiento total de 2.0 PB. Se admite conectividad externa para configuraciones de DD Extended Retention de hasta 56 bandejas.

Licencias para DD Extended Retention

DD Extended Retention es una opción de software con licencia instalada en un sistema DD compatible.

Se requiere una licencia de capacidad separada para cada bandeja de almacenamiento, para las bandejas instaladas en los niveles activo y de retención. Las licencias de capacidad de bandeja son específicas para una bandeja de nivel activo o de retención.

Se requiere una licencia de almacenamiento expandido para ampliar la capacidad de almacenamiento en el nivel activo a un grado superior a la capacidad de entrada, que varía según el modelo de Data Domain. No puede usar el almacenamiento adicional sin aplicar primero las licencias correspondientes.

Agregar licencias de capacidad de bandejas para DD Extended Retention

Cada bandeja en un sistema DD habilitado para DD Extended Retention debe tener una licencia separada.

Procedimiento

1. Seleccione **Administration** > **Licenses**.
2. Haga clic en **Add Licenses**.
3. Introduzca una o varias licencias, una por línea, presionando la tecla Enter después de cada una. Cuando haya terminado, haga clic en **Add**. Si hay errores, se muestra un resumen de las licencias agregadas y de las que no se agregaron debido a un error. Seleccione el número de licencia errónea para repararlo.

Resultados

Las licencias para el sistema DD se muestran en dos grupos:

- Licencias de opciones de software, necesarias para opciones como DD Extended Retention y DD Boost.
- Licencias de capacidad de bandeja, donde se muestra la capacidad de la bandeja (en TiB), el modelo de bandeja (como ES30) y el nivel de almacenamiento de la bandeja (activo o de retención).

Para eliminar una licencia, selecciónela de la lista Licenses y haga clic en **Delete Selected Licenses**. Si se le solicita confirmación, lea la advertencia y haga clic en **OK** para continuar.

Configuración del almacenamiento para DD Extended Retention

El almacenamiento adicional para DD Extended Retention exige las licencias adecuadas y suficiente memoria instalada en el sistema DD para brindar soporte. Los mensajes de error muestran si se necesitan más licencias o memoria.

Procedimiento

1. Seleccione la pestaña **Hardware** > **Storage**.
2. En la pestaña Overview, seleccione **Configure Storage**.
3. En la pestaña Configure Storage, seleccione el almacenamiento que se debe agregar de la lista Addable Storage.
4. Seleccione la configuración adecuada para Tier Configuration (o **Active** o **Retention**) del menú. El nivel activo es análogo a un sistema DD estándar y debe dimensionarse de forma similar. La cantidad máxima de almacenamiento que se puede agregar al nivel activo depende del controlador DD que se use.

5. Seleccione la casilla de verificación de la bandeja que desee agregar.
6. Haga clic en el botón **Add to Tier**.
7. Haga clic en **OK** para agregar el almacenamiento.
8. Para eliminar una bandeja agregada, selecciónela en la lista Tier Configuration, haga clic en **Remove from Tier** y, a continuación, seleccione **OK**.

Infraestructura proporcionada por el cliente para DD Extended Retention

Antes de habilitar DD Extended Retention, su ambiente y configuración deben cumplir con ciertos requisitos.

- **Especificaciones, requisitos del sitio, espacio de rack y cableado de interconexión**: Consulte la *Guía de instalación y configuración de Data Domain* para conocer su modelo de sistema DD.
- **Racks y cableado**: Se recomienda que el rack de su sistema pueda expandirse en el futuro: Todas las bandejas están conectadas a un único sistema DD.

  Nota

  - Consulte la *Guía de hardware de bandeja de expansión de Data Domain* para obtener información sobre su modelo de bandeja (ES20, ES30 o DS60).

Administración de DD Extended Retention

Para configurar y usar DD Extended Retention en el sistema DD, puede usar DD System Manager o DD CLI.

- DD System Manager, anteriormente conocido como Enterprise Manager, es una interfaz gráfica del usuario (GUI), que se describe en esta guía.
- Los comandos `archive`, ingresados en la interfaz de la línea de comandos (CLI) de DD, se describen en la *Guía de referencia de comandos de Data Domain Operating System*.

El único comando que no está disponible cuando se usa DD System Manager es `archive report`.

Activación de sistemas DD para DD Extended Retention

Antes de usar un sistema DD system para DD Extended Retention, debe tener la licencia correcta y la configuración correcta del sistema de archivos.

Procedimiento

1. Asegúrese de que se haya aplicado la licencia correcta. Seleccione **Administration** > **Licenses**, y compruebe la lista de las licencias de funciones para Extended Retention.
2. Seleccione **Data Management** > **File System** > **More Tasks** > **Enable DD Extended Retention**.

   Esta opción está disponible únicamente si su sistema Data Domain es compatible con DD Extended Retention y el sistema de archivos todavía no se ha configurado para DD Extended Retention. Tenga en cuenta que después de que se habilita DD Extended Retention, no se puede deshabilitar sin destruir el sistema de archivos.

a. Si el sistema de archivos ya está habilitado (como un sistema que no es DD Extended Retention), se le pedirá que lo deshabilite. Para hacerlo, haga clic en **Disable**.

b. Si se le pide que confirme si desea convertir el sistema de archivos para que DD lo use Extended Retention, haga clic en **OK**.

Después de que un sistema de archivos se convierte en un sistema de archivos DD Extended Retention, la página del sistema de archivos se actualiza para incluir información acerca de ambos niveles, y hay una nueva pestaña denominada **Retention Units**.

Equivalente de la CLI

También puede verificar que la licencia de Extended Retention se haya instalado en la CLI.

Para utilizar el método de licencias existente:

```
# license show
## License Key                    Feature
--    -------------------        -----------
1     AAAA-BBBB-CCCC-DDDD        Replication
2     EEEE-FFFF-GGGG-HHHH        VTL
--    -------------------        -----------
```

Si la licencia no está presente, cada unidad incluye documentación (una tarjeta de instalación rápida) que muestra las licencias que se han comprado. Ingrese el siguiente comando para completar el número de licencia.

```
# license add license-code
```

A continuación, habilite Extended Retention:

```
# archive enable
```

Para utilizar las licencias electrónicas:

```
# elicense show
Feature licenses:
## Feature     Count Mode            Expiration Date
-- ----------- ----- --------------- ---------------
1  REPLICATION 1     permanent (int) n/a
2  VTL         1     permanent (int) n/a
-- ----------- ----- --------------- ---------------
```

Si la licencia no está presente, actualice el archivo de licencia con la licencia de la nueva función.

```
# elicense update mylicense.lic
New licenses: Storage Migration
Feature licenses:
## Feature            Count   Mode             Expiration Date
-- -----------------  -----  ---------------  ---------------
1  REPLICATION        1      permanent (int)  n/a
2  VTL                1      permanent (int)  n/a
3  EXTENDED RETENTION 1      permanent (int)  n/a
-- ------------------ -----  ---------------  ---------------
** This will replace all existing Data Domain licenses on the system with the above
EMC ELMS licenses.
Do you want to proceed? (yes|no) [yes]: yes
eLicense(s) updated.
```

A continuación, habilite Extended Retention:

```
# archive enable
```

Creación de un sistema de archivos en dos niveles para DD Extended Retention

DD Extended Retention tiene un sistema de archivos en dos niveles para los niveles activo y de retención. El sistema DD debe haberse habilitado para DD Extended Retention antes de habilitar este sistema de archivos especial.

Procedimiento

1. Seleccione **Data Management** > **File System**.
2. Si existe un sistema de archivos, destrúyalo.
3. Seleccione **More Tasks** > **Create file system**.
4. Seleccione un sistema de archivos con capacidad de retención y haga clic en **Next**.
5. Seleccione **Configure** en el cuadro de diálogo File System Create.

   Debe configurar el almacenamiento antes de que se pueda crear un sistema de archivos.
6. Utilice el cuadro de diálogo Configure Storage para agregar y eliminar almacenamiento disponible de los niveles activo y de retención, y haga clic en **OK** cuando haya terminado.

   El almacenamiento en el nivel activo se usa para crear el nivel activo del sistema de archivos, y el almacenamiento en el nivel de retención se utiliza para crear una unidad de retención.

   Nota

   A partir de la versión 5.5.1 de DD OS, solo se permite una unidad de retención por nivel de retención. Sin embargo, los sistemas instalados antes de la versión 5.5.1 de DD OS pueden continuar teniendo más de una unidad de retención, pero no se puede agregar ninguna otra unidad de retención

   ---
7. Use el cuadro de diálogo File System Create para:
   a. Seleccionar el tamaño de la unidad de retención desde la lista desplegable.
   b. Seleccione la opción **Enable file system after creation** option.
   c. Haga clic en **Next**.

   En una página de resumen, se muestra el tamaño de los niveles activo y de retención en el nuevo sistema de archivos.
8. Haga clic en **Finish** para crear el nuevo sistema de archivos.

   Se muestra el progreso de cada paso de creación, y una barra de progreso supervisa el estado general.
9. Después de que finalice la ejecución del sistema de archivos, haga clic en **OK**.

   Equivalente de la CLI
   Para agregar bandejas adicionales, use este comando una vez para cada gabinete.

   ```
   # storage add tier archive enclosure 5
   ```

   Cree una unidad de archivo y agréguela al sistema de archivos. Se le pedirá que especifique la cantidad de gabinetes en la unidad de archiving:

```
# filesys archive unit add
```

Verifique que se haya creado la unidad de archivo y se haya agregado al sistema de archivos:

```
# filesys archive unit list all
```

Verifique el sistema de archivos, como se ve en el sistema:

```
# filesys show space
```

Panel del sistema de archivos para DD Extended Retention

Después de habilitar un sistema DD para DD Extended Retention, el panel **Data Management** > **File System** tendrá un aspecto levemente diferente (desde un sistema habilitado para Extended Retention que no sea DD).

- En **State**, se muestra si el sistema de archivos está habilitado o deshabilitado. Puede cambiar el estado con el botón Disable/Enable inmediatamente a la derecha.
- En **Clean Status**, se muestra la hora en que finalizó la última operación de limpieza o el estado de limpieza actual si la operación se está ejecutando en el momento. Si se puede ejecutar la limpieza, aparece un botón **Start Cleaning**. Cuando se realiza la limpieza, el botón **Start Cleaning** cambia a un botón **Stop Cleaning** .
- En **Data Movement Status**, se muestra la hora en la que finalizó la última transferencia de datos. Si se puede realizar la transferencia de datos, aparece un botón **Start**. Cuando se está realizando la transferencia de datos, el botón **Start** cambia al botón **Stop**.
- En **Space Reclamation Status**, se muestra la cantidad de espacio recuperado después de eliminar datos en el nivel de retención. Si se puede ejecutar la recuperación de espacio, aparece un botón **Start**. Si ya se está ejecutando, aparecen los botones **Stop** y **Suspend**. Si se estaba ejecutando antes y se suspendió, se muestran los botones **Stop** y **Resume**. También hay un botón **More Information** que mostrará información detallada acerca de las horas de inicio y finalización, el porcentaje completo, las unidades recuperadas, el espacio liberado y otros datos.
- Si selecciona **More Tasks** > **Destroy**, puede eliminar todos los datos en el sistema de archivos, incluidas las cintas virtuales. A esto solo lo puede realizar el administrador del sistema.
- Al seleccionar **More Tasks** > **Fast Copy**, puede clonar archivos y MTrees de un directorio de origen a un directorio de destino. Tenga en cuenta que, para los sistemas habilitados para DD Extended Retention, la copia rápida no transferirá datos entre niveles activos y de retención.
- Al seleccionar **More Tasks** > **Expand Capacity**, puede expandir el nivel activo o de retención.

Expansión del nivel activo o de retención

Cuando se habilita el sistema de archivos, puede expandir el nivel activo o de retención.

Para expandir el nivel **Active** :

Procedimiento

1. Seleccione **Data Management > File System > More Tasks > Expand Capacity**.

2. En el cuadro de diálogo Expand File System Capacity, seleccione **Active Tier** y, a continuación, haga clic en **Next**.
3. Haga clic en **Configure**.
4. En el cuadro de diálogo Configure Storage, asegúrese de que el valor Active Tier se muestre como la selección de configuración y haga clic en **OK**.
5. Una vez que se completa la configuración, se lo dirige nuevamente al cuadro de diálogo Expand File System Capacity. Seleccione **Finish** para completar la expansión del nivel activo.

Para expandir el nivel de **retención**:

Procedimiento

1. Seleccione **Data Management > File System > More Tasks > Expand Capacity**.
2. En el cuadro de diálogo Expand File System Capacity, seleccione **Retention Tier** y luego **Next**.
3. Si la unidad de retención está disponible, verá el cuadro de diálogo **Select Retention Unit**. Seleccione la unidad de retención que desea expandir y, luego, **Next**. Si la unidad de retención no está disponible, verá el cuadro de diálogo **Create Retention Unit** y deberá crear una antes de continuar.

   Nota

   Para garantizar el rendimiento óptimo de un sistema DD con DD Extended Retention habilitado, siempre debe expandir el nivel de retención en incrementos de al menos dos bandejas. Tampoco debe esperar a que la unidad de retención esté casi completa antes de expandirla.

4. Seleccione el tamaño al que desea expandir la unidad de retención y, luego, haga clic en **Configure**.
5. Una vez que se completa la configuración, se lo dirige nuevamente al cuadro de diálogo Expand File System Capacity. Seleccione **Finish** para completar la expansión del nivel de retención.

Recuperación de espacio en el nivel de retención

Puede recuperar espacio de los datos eliminados en el nivel de retención ejecutando la función de recuperación de espacio (presentada en DD OS 5.3). La recuperación de espacio también se produce durante la limpieza del sistema.

Procedimiento

1. Seleccione **Data Management** > **File System**. Justo sobre las pestañas, en **Space Reclamation Status**, se muestra la cantidad de espacio recuperado después de eliminar datos en el nivel de retención.
2. Si se puede ejecutar la recuperación de espacio, aparece un botón **Start**. Si ya se está ejecutando, aparecen los botones **Stop** y **Suspend**. Si se estaba ejecutando antes y se suspendió, se muestran los botones **Stop** y **Resume**.
3. Seleccione **More Information** para obtener detalles acerca del nombre del ciclo, las horas de inicio y finalización, el tiempo de ejecución efectivo, el porcentaje completado (si está en curso), las unidades recuperadas, el espacio liberado n la unidad de destino y el espacio liberado total.

Nota

Cuando se usa el comando `archive space-reclamation`, el sistema ejecuta la recuperación de espacio en segundo plano hasta que se detiene manualmente a menos que utilice la opción de realizar un ciclo de uno. También puede usar el comando `archive space-reclamation schedule set` para establecer la hora de inicio para la recuperación de espacio.

Equivalente de la CLI
Para habilitar la recuperación de espacio:

```
# archive space-reclamation start
```

Para deshabilitar la recuperación de espacio:

```
# archive space-reclamation stop
```

Para que se muestre el estado de la recuperación de espacio:

```
# archive space-reclamation status-detailed
Space-reclamation will start when 'archive data-movement'
completes.

Previous Cycle:
---------------
Start time                 : Feb 21 2014 14:17
End time                   : Feb 21 2014 14:49
Effective run time         : 0   days, 00:32.
Percent completed          : 00 % (was stopped by user)
Units reclaimed            : None
Space freed on target unit : None
Total space freed          : None
```

Pestañas del sistema de archivos para DD Extended Retention

Después de habilitar un sistema DD para DD Extended Retention, las pestañas **Data Management** > **File System** también se verán levemente diferentes (desde un sistema habilitado para Extended Retention que no sea DD), y habrá una pestaña adicional: **Unidades de retención**

Pestaña Summary
En la pestaña Summary, se muestra información acerca de la compresión y el uso del espacio en disco para los niveles activo y de retención.

Space Usage: Se muestran el tamaño total, la cantidad de espacio usado, la cantidad de espacio disponible y los totales combinados para los niveles activo y de retención. La cantidad de espacio limpiable se muestra para el nivel activo.

Active Tier and Retention Tier: Se muestran los valores anteriores y posteriores a la compresión usados actualmente y aquellos escritos en las últimas 24 horas. También se muestran los factores globales, locales y de compresión total (porcentaje de reducción).

Pestaña Retention Units
En la pestaña Retention Units, se muestran las unidades de retención. A partir de la versión 5.5.1.4 de DD OS, solo se permite una unidad de retención por nivel de retención. Sin embargo, los sistemas instalados antes de la versión 5.5.1.4 de DD OS pueden continuar teniendo más de una unidad de retención, pero no se les podrá agregar ninguna otra unidad de retención

Se muestra la siguiente información: la condición de la unidad (New, Empty, Sealed, Target o Cleaning), su estado (Disabled, Ready o Stand-by), su fecha de inicio

(cuándo se transfirió al nivel de retención) y el tamaño de la unidad. La unidad estará en la condición de limpieza (Cleaning) si se está ejecutando la recuperación de espacio. Si la unidad se ha sellado, lo que significa que no se pueden agregar más datos, se proporciona la fecha de sellado. Al seleccionar la casilla de verificación de la unidad de retención, se muestra información adicional (Tamaño, Utilizada, Disponible y Limpiable) en el panel Detailed Information.

Existen dos botones: **Delete** (para eliminar la unidad) y **Expand** (para agregar almacenamiento a una unidad). La unidad debe estar en un estado nuevo u de destino para expandirse.

Pestaña Configuration

Con la pestaña Configuration, puede configurar el sistema.

Al seleccionar el botón **Edit** en Options, se muestra el cuadro de diálogo para modificar la configuración, donde puede cambiar los parámetros Local Compresión Type (las opciones son none, lz [predeterminada], gz y gzfast) y Retention Tier Local Comp(ression) (las opciones son none, lz, gz [predeterminada] y gzfast), además de habilitar la función Report Replica Writable.

Si selecciona el botón **Edit** en Clean Schedule, se muestra el cuadro de diálogo para modificar el calendario, donde puede encontrar el calendario de limpieza, además del porcentaje de aceleración.

Si selecciona **Edit** en Data Movement Policy, se muestra el cuadro de diálogo de la política de transferencia de datos, donde puede configurar diversos parámetros. File Age Threshold es un valor predeterminado de todo el sistema que se aplica a todos los MTrees para los cuales no ha definido un valor predeterminado. El valor mínimo es de 14 días. Con Data Movement Schedule, puede establecer con qué frecuencia se realizará la transferencia de datos; el calendario recomendado es cada dos semanas. Con File System Cleaning, puede elegir que no se realice la limpieza del sistema después de la transferencia de datos; sin embargo, se recomienda enfáticamente que deje esta opción seleccionada.

Umbral de antigüedad de archivos por MTree Link

Si selecciona el vínculo **File Age Threshold per MTree**, se lo dirigirá de File System al área de MTree (a la que también se puede acceder seleccionado **Data Management** > **MTree**), donde puede definir un umbral de antigüedad de archivos personalizado para cada MTree.

Seleccione el MTree y luego seleccione **Edit** junto a Data Movement Policy. En el cuadro de diálogo para modificar el umbral de antigüedad, introduzca un nuevo valor para el umbral de antigüedad y seleccione **OK**. A partir de DD OS 5.5.1, el valor mínimo es de 14 días.

Pestaña Encryption

La pestaña Encryption le permite habilitar o deshabilitar el cifrado de datos inactivos, que es compatible solo con sistemas con una única unidad de retención. A partir de la versión 5.5.1, DD Extended Retention admite solo una única unidad de retención, de modo que la configuración de sistemas en versiones 5.5.1 o posteriores cumplirá con esta restricción. Sin embargo, los sistemas instalados antes de la versión 5.5.1 pueden tener más de una unidad de retención, pero no funcionarán con el cifrado de datos inactivos hasta que todas las unidades de retención menos una se hayan quitado, o hasta que los datos se hayan transferido o migrado a una unidad de retención.

Pestaña Space Usage

Con la pestaña Space Usage, puede seleccionar uno de los tres tipos de gráficos ([completo] Sistema de archivos; Activo [nivel]; Archivo [nivel]) para ver el uso de espacio en el tiempo en MiB. También puede seleccionar un valor de duración (7, 30, 60 o 120 días) en el extremo superior derecho. Los datos se presentan (codificados

por color) como escritos antes de la compresión (azul), utilizados después de la compresión (rojo), y el factor de compresión (negro).

Pestaña Consumption
Con la pestaña Consumption, puede seleccionar uno de los tres tipos de gráfico ([completo] Sistema de archivos; Activo [nivel]; Archivo [nivel]) para ver la cantidad de almacenamiento posterior a la compresión utilizado y el valor de compresión en el tiempo, lo cual le permite ver las tendencias de consumo. También puede seleccionar un valor de duración (7, 30, 60 o 120 días) en el extremo superior derecho. Con la casilla de verificación Capacity, puede elegir si desea que se muestre el almacenamiento posterior a la compresión frente a la capacidad total del sistema.

Pestaña Daily Written
Con la pestaña Daily Written, puede seleccionar una duración (7, 30, 60 o 120 días) para ver la cantidad de datos escritos por día. Los datos se presentan (codificados por color) en formato de gráfico y de tabla como escritos antes de la compresión (azul), utilizados después de compresión (rojo), y el factor de compresión (negro).

Expansión de una unidad de retención

Para garantizar el rendimiento óptimo, no espere a que una unidad de retención esté casi llena para expandirla ni la expanda en incrementos de a una bandeja. El almacenamiento no se puede mover del nivel activo al nivel de retención una vez que se creó el sistema de archivos. Solo pueden agregarse gabinetes no utilizados al nivel de retención.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Retention Units**.
2. Seleccione la unidad de retención.

   Tenga en cuenta que si hay una limpieza en ejecución, no se puede expandir una unidad de retención.
3. Haga clic en **Expand**.

   El sistema muestra el tamaño actual de nivel de retención, un tamaño aproximado de expansión y una capacidad expandida total. Si hay almacenamiento adicional disponible, puede hacer clic en el vínculo Configure.
4. Haga clic en **Next**.

   El sistema muestra una advertencia que le indica que no se puede revertir el sistema de archivos a su tamaño original después de esta operación.
5. Haga clic en **Expand** para expandir el sistema de archivos.

Eliminación de una unidad de retención

Si ya no se requieren todos los archivos en una unidad de retención, eliminarlos hace que la unidad vuelva a estar disponible para el uso. Puede generar un informe de ubicación de archivos para asegurarse de que la unidad de retención esté realmente vacía, eliminar la unidad de retención y luego agregarla como una nueva unidad de retención.

Procedimiento

1. Seleccione **Data Management** > **File System** and click **Disable** para deshabilitar el sistema de archivos si está en ejecución.
2. Seleccione **Data Management** > **File System** > **Retention Units**.
3. Seleccione la unidad de retención.

4. Haga clic en **Delete**.

Modificar la compresión local del nivel de retención

Puede modificar el algoritmo de compresión local para la transferencia de datos subsiguiente hacia el nivel de retención.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Configuration**.
2. Seleccione **Edit** a la derecha de **Options**.
3. Seleccione una de las opciones de compresión desde el menú Retention Tier Local Compression Type y haga clic en **OK**.

   El valor predeterminado es gz, que es una compresión con técnicas de descompresión que usa la menor cantidad de espacio para el almacenamiento de datos (de 10 % a 20 % menos que lz en promedio; sin embargo, algunos conjuntos de datos obtienen compresión más alta).

Información acerca de la política de transferencia de datos

Un archivo se transfiere del nivel activo al nivel de retención según la fecha en que se modificó por última vez. Para conservar la integridad de los datos, se transfiere todo el archivo en este momento. La *política de transferencia de datos* establece dos cosas: un *umbral de antigüedad de archivos* y un *calendario de transferencia de datos*. Si los datos no se han modificado durante los días establecidos por el umbral de antigüedad de archivos, se transfieren del nivel activo al nivel de retención en la fecha definida por el calendario de transferencia de datos.

Nota

A partir del SO DD 5.5.1, el umbral de antigüedad de archivos debe ser un mínimo de 14 días.

Puede especificar diferentes umbrales de antigüedad de archivos para cada MTree definido. Un MTree es un subárbol dentro del espacio de nombres que es un conjunto lógico de datos para fines administrativos. Por ejemplo, puede colocar datos financieros, correos electrónicos y datos de ingeniería en MTrees separados.

Para aprovechar la función de *recuperación de espacio*, incluida en la versión del SO DD 5.3, se recomienda que programe la transferencia de datos y la limpieza del sistema de archivos cada dos semanas (14 días). De forma predeterminada, la limpieza se ejecuta siempre después de que se completa la transferencia de datos. Se recomienda enfáticamente no cambiar este valor predeterminado.

Evite estos errores comunes de dimensionamiento:

- Establecer una política de transferencia de datos que sea demasiado agresiva; los datos se transferirán demasiado pronto.
- Establecer una política de transferencia de datos demasiado conservadora: después de que el nivel activo se completa, no podrá escribir datos en el sistema.
- Tener un nivel activo subdimensionado y luego establecer una política de transferencia de datos demasiado agresiva para compensar.

Tenga en cuenta las siguientes advertencias relacionadas con snapshots y la limpieza del sistema de archivos:

- Los archivos en los snapshots no se limpian, aun después de que se han transferido al nivel de retención. El espacio no se puede recuperar hasta que los snapshots se hayan eliminado.

- Se recomienda definir el umbral de antigüedad de archivos para snapshots como un mínimo de 14 días.

Estos son dos ejemplos de cómo establecer la política de transferencia de datos.

- Podría segregar los datos con diferentes niveles de cambio en dos MTrees diferentes y configurar el umbral de antigüedad de archivos para que se transfieran los datos inmediatamente después de que estos se estabilicen. Cree un MTree A para respaldos incrementales diarios y un MTree B para respaldos completos semanales. Configure el umbral de antigüedad de archivos para el MTree A de modo que sus datos no se transfieran *nunca*, pero configure el umbral de antigüedad de archivos para el MTree B en 14 días (el umbral mínimo).
- Para los datos que no pueden separarse en diferentes MTrees, puede hacer lo siguiente: Suponga que el período de retención de respaldos incrementales diarios es de ocho semanas, y el período de retención de respaldos completos semanales es de tres días. En este caso, lo mejor sería definir el umbral de antigüedad de archivos en nueve semanas. Si se configurara uno menor, podrían transferirse datos incrementales diarios que pronto se eliminarían.

Modificación de la política de transferencia de datos

Puede establecer distintas políticas de transferencia de datos para cada MTree.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Configuration**.
2. Haga clic en **Edit** a la derecha de **Data Movement Policy**.
3. En el cuadro de diálogo de la Política de transferencia de datos, especifique el valor predeterminado de umbral de antigüedad de archivo para todo el sistema en cantidad de días. A partir de la versión 5.5.1 de DD OS, este valor debe ser mayor o igual a 14 días. Este valor se aplica a los MTrees nuevos y a los MTrees a los que no se ha asignado un valor de umbral de antigüedad individual usando el vínculo **File Age Threshold per MTree** (consulte el paso 7). Cuando comienza la transferencia de datos, todos los archivos que no se han modificado para la cantidad de días del umbral especificado se transferirán del nivel activo al nivel de retención.
4. Especifique un calendario de transferencia de datos, es decir, cuándo se debe realizar; por ejemplo, diariamente, semanalmente, cada dos semanas (cada 14 días), mensualmente o el último día del mes. También puede elegir uno o varios días específicos y un horario en horas y minutos. Se recomienda enfáticamente que programe la transferencia de datos y la limpieza del sistema de archivos cada dos semanas (cada 14 días) para aprovechar la función de recuperación de espacio (introducida en la versión 5.3 de DD OS).
5. Especifique un valor para Data Movement Throttle, es decir, el porcentaje de los recursos disponibles que el sistema usa para transferencia de datos. Un valor del 100 % indica que no se regulará la transferencia de datos.
6. De forma predeterminada, la limpieza del sistema de archivos se ejecuta siempre después de que se completa la transferencia de datos. Se recomienda enfáticamente que deje la opción **Start file system clean after Data Movement** seleccionada.
7. Seleccione OK.
8. Nuevamente en la pestaña Configuration, puede especificar los valores de umbral de antigüedad para los MTrees individuales usando el vínculo **File Age Threshold per MTree** en el extremo inferior derecho.

Equivalente de la CLI

Para configurar el umbral de antigüedad:

```
# archive data-movement policy set age-threshold {days|none}
mtrees mtree-list
```

Si es necesario, para configurar el umbral de antigüedad *predeterminado*:

```
# archive data-movement policy set default-age-threshold days
```

Para verificar la configuración de umbral de antigüedad:

```
# archive data-movement policy show [mtree mtree-list]
```

Para especificar el calendario de migración:

```
# archive data-movement schedule set days days time time [no-
clean]
```

Los valores de calendario aceptables incluyen los siguientes:

- días dom. hora 00:00
- días lun. mar. hora 00:00
- días 2 hora 10:00
- días 2,15 hora 10:00
- días última hora 10:00 - último día del mes

Para verificar el calendario de migración:

```
# archive data-movement schedule show
```

Para deshabilitar el calendario de limpieza de archivos:

Nota

El motivo para deshabilitar el calendario de limpieza es eliminar un conflicto de calendarización entre la limpieza y la transferencia de datos. Cuando finaliza la transferencia de datos, comienza automáticamente la limpieza. Si deshabilita la transferencia de datos, debe volver a habilitar la limpieza del sistema de archivos.

```
# filesys clean set schedule never
```

Iniciar o detener la transferencia de datos según demanda

Aún si tiene una política de transferencia de datos regular, puede iniciar o detener la transferencia de datos *según demanda*.

Procedimiento

1. Seleccione **Data Management** > **File System**.
2. Haga clic en **Start** a la derecha de **Data Movement Status**.
3. El cuadro de diálogo Start Data Movement le advierte que los datos se transferirán del nivel activo al nivel de retención, como se define en la política de transferencia de datos, seguido de una limpieza del sistema de archivos. Seleccione **Start** para comenzar la transferencia de datos.

   Si una limpieza del sistema de archivos ya está en curso, la transferencia de datos se llevará a cabo después de que finalice la limpieza. Sin embargo, otra limpieza también se iniciará automáticamente después de que se complete la transferencia de datos según demanda.
4. El botón **Start** se reemplazará por el botón **Stop**.

5. En cualquier momento, si desea detener la transferencia de datos, haga clic en **Stop** y en **OK** en el cuadro de diálogo Stop Data Movement para confirmar.

Uso del paquete de transferencia de datos

Los datos se compactan en la partición objetivo después de cada migración de archivo (a partir del SO DD 5.2). De forma predeterminada, se habilita esta función, que se denomina *paquete de transferencia de datos*.

Cuando esta función está habilitada, mejora la compresión general del nivel de retención, pero hay un pequeño incremento en el tiempo de migración.

Para determinar si esta función está habilitada, seleccione **Data Management** > **File System** > **Configuration**.

El valor actual para **Packing data during Retention Tier data movement** puede ser Enabled o Disabled. Consulte a un ingeniero del sistema si desea cambiar esta configuración.

Actualizaciones y recuperación con DD Extended Retention

En las siguientes secciones, se describe cómo ejecutar actualizaciones de software y hardware y cómo recuperar datos para sistemas DD habilitados para DD Extended Retention.

Actualización al DD OS 5.7 con DD Extended Retention

La política de actualización para un sistema DD habilitado para DD Extended Retention es la misma que para un sistema DD estándar.

Se admite la actualización de hasta dos versiones anteriores principales. Para obtener instrucciones sobre cómo actualizar DD OS, consulte la sección de instrucciones de actualización de las *Notas de la versión* de la versión de DD OS de destino.

Al actualizar un sistema DD habilitado para DD Extended Retention a DD OS 5.7, asegúrese de actualizar los calendarios de transferencia de datos existentes a quincenales (14 días) para aprovechar la función de recuperación de espacio.

Los sistemas DD habilitados para DD Extended Retention ejecutan automáticamente una limpieza después de que se completa la transferencia de datos; por lo tanto, no debe calendarizar una limpieza por separado con DD System Manager o la CLI (interfaz de la línea de comandos).

Si el nivel activo está disponible, el proceso actualiza el nivel activo y la unidad de retención, y pone al sistema en un estado que la actualización anterior no ha verificado si está completo. El sistema de archivos borra este estado después de que se habilita y verifica que se ha actualizado el nivel de retención. No se permite una actualización posterior hasta que se borre este estado.

Si el nivel activo no está disponible, el proceso de actualización actualiza el chasis del sistema y lo pone en un estado donde está listo para crear o aceptar un sistema de archivos.

Si la unidad de retención está disponible después de que el proceso de actualización ha finalizado, la unidad se actualiza automáticamente cuando se conecta al sistema o en el siguiente inicio del sistema.

Actualización de hardware con DD Extended Retention

Puede actualizar un sistema DD habilitado para DD Extended Retention a un sistema de mayor rendimiento o de una versión posterior. Por ejemplo, podría reemplazar un

sistema DD860 habilitado para DD Extended Retention con un sistema DD990 habilitado para DD Extended Retention.

Nota

Comuníquese con su proveedor de servicios contratado y consulte acerca de las instrucciones en la *Guía de actualización del controlador del sistema*.

Este tipo de actualización afecta a DD Extended Retention de la siguiente manera:

- Si un nuevo sistema tiene una versión más reciente de SO DD que los niveles activo y de retención, estos se actualizan a la nueva versión del sistema. De lo contrario, el nuevo sistema se actualiza a la versión de los niveles activo y de retención.
- Los niveles activo y de retención que están conectados a un nuevo sistema pasan a ser propiedad del nuevo sistema.
- Si hay un nivel activo, el registro en el nivel activo se instala en el nuevo sistema. De lo contrario, el registro en el nivel de retención con el registro actualizado más recientemente se instala en el nuevo sistema.

Recuperación de un sistema habilitado para DD Extended Retention

Si se pierden el nivel activo y un subconjunto de unidades de retención en un sistema DD habilitado para DD Extended Retention, y no hay réplica disponible, el servicio de soporte puede reconstituir cualquier unidad de retención sellada restante en un sistema DD.

Un sistema DD habilitado para DD Extended Retention está diseñado para permanecer disponible para brindar servicios a las solicitudes de lectura y escritura cuando se pierden una o varias unidades de retención. Es posible que el sistema de archivos no detecte que una unidad de retención se perdió hasta que el sistema de archivos se reinicia o intenta acceder a datos almacenados en la unidad de retención. Esta última circunstancia puede provocar un reinicio del sistema de archivos. Después de que el sistema de archivos ha detectado que se ha perdido una unidad de retención, arroja un error en respuesta a las solicitudes de datos almacenados en esa unidad.

Si los datos perdidos no se pueden recuperar a partir de una réplica, el servicio de soporte podría limpiar el sistema eliminando la unidad de retención perdida y cualquier archivo que resida total o parcialmente en esta.

Uso de la recuperación de replicación

El procedimiento de recuperación de replicación para un sistema DD habilitado para DD Extended Retention depende del tipo de replicación.

- Replicación de recopilación: el nuevo origen debe configurarse como un sistema DD habilitado para DD Extended Retention con la misma cantidad de unidades de retención (o más) que el destino. El sistema de archivos no se debe habilitar en el nuevo origen hasta que se hayan agregado las unidades de retención y se haya iniciado la recuperación de replicación.

  Nota

  Si necesita recuperar solo una porción de un sistema, como una unidad de retención, desde una réplica de recolecciones, póngase en contacto con el servicio de soporte.

- Replicación de MTrees: Consulte la sección *Replicación de MTrees* en el capítulo *Trabajo con DD Replicator*.
- Replicación de archivos administrados por DD Boost: Consulte la *Guía de administración de Data Domain Boost para OpenStorage*.

Recuperación de fallas del sistema

Un sistema DD habilitado para DD Extended Retention está equipado con herramientas para abordar las fallas en las diferentes partes del sistema.

Procedimiento

1. Restaure la conexión entre la controladora del sistema y el almacenamiento. Si se pierde la controladora del sistema, reemplácelo con uno nuevo.
2. Si hay pérdida de datos y una réplica está disponible, intente recuperar los datos de la réplica. Si una réplica no está disponible, limite la pérdida de datos aprovechando las funciones de aislamiento de fallas de DD Extended Retention a través del soporte.

Migrar datos de nivel de archiving a DD Cloud Tier

Este procedimiento utiliza la replicación de MTree para migrar datos desde el nivel de archiving en un sistema Data Domain con retención extendida a un sistema Data Domain de nodo único o una instancia DD VE con DD Cloud Tier.

Antes de comenzar

- Se requieren licencias de replicación y DD Cloud Tier.
- El sistema de destino debe ejecutar la versión 6.0 (o una posterior) de Data Domain Operating System para admitir DD Cloud Tier.
- El sistema de destino debe tener suficiente capacidad de nivel activo para contener los datos del nivel activo y del nivel de archiving en el sistema de origen, ya que los datos no se moverán al almacenamiento de DD Cloud Tier en el sistema de destino durante al menos 14 días.
- Data Domain recomienda que cualquier planificación de capacidad incluya suficiente capacidad de nivel activo para un mínimo de 14 días de datos replicados.
- Todos los trabajos de respaldo y otras actividades de escritura en el sistema de origen deben redirigirse al sistema de destino.
- El sistema de destino debe cumplir los mismos requisitos de cumplimiento de normas que ha cumplido el sistema de origen.
- El cliente debe proporcionar todas las cuentas y credenciales apropiadas para los sistemas Data Domain de destino y de origen.

Consideraciones adicionales:

- Póngase en contacto con el soporte de Dell EMC si se requiere una migración de datos inmediata al almacenamiento de DD Cloud Tier.
- Las aplicaciones de respaldo del cliente no pueden rastrear esta migración de datos.
- Este procedimiento no abarca la replicación de archivos administrados (MFR).
- Con respecto al otorgamiento de licencias, los sistemas Data Domain pueden utilizar las siguientes:
  - Licencias heredadas (utilice el comando `license show`)

- Licencias de ELMS (utilice el comando `elicense show`)

Los sistemas Data Domain que utilizan licencias heredadas pueden agregar licencias de forma incremental. Tenga en cuenta que no todas las funciones más recientes son compatibles con licencias heredadas.

Los sistemas Data Domain instalados con DD OS 6.0 o posterior, convertidos o actualizados con funciones que requieren licencias de ELMS utilizan los comandos `elicense` cuando aplican y muestran licencias. Cuando se aplica un nuevo archivo de clave de licencia, el nuevo conjunto de claves reemplaza a todas las claves anteriores por completo.

⚠ PRECAUCIÓN

Cuando se actualice una licencia de ELMS, asegúrese de no quitar la capacidad ni las funciones existentes.

Este procedimiento abarca los siguientes usos:

- El cliente desea mover los datos del almacenamiento de nivel de archiving al almacenamiento DD Cloud Tier en el sistema de destino.
- El cliente desea mover los datos del almacenamiento de nivel activo y de archiving en el sistema de origen al almacenamiento DD de nivel activo en el sistema de destino.
- El cliente desea mover los datos del almacenamiento de nivel de archiving en varios sistemas de origen al almacenamiento activo o de DD Cloud Tier en el sistema de destino.
- El cliente desea reutilizar el sistema de origen o sus gabinetes de disco después de finalizar la operación de migración.

Planificación de la capacidad

Antes de comenzar

El sistema de destino debe tener suficiente capacidad en el nivel activo para almacenar los niveles activos y de archiving combinados del sistema de origen.

Además, el nivel activo del sistema de origen debe tener suficiente espacio para conservar todos los datos de los respaldos programados desde el momento en que se detiene el movimiento de datos hacia el nivel de archiving hasta que se completa la migración del sistema de origen al sistema de destino.

Este procedimiento se desarrolló y se probó utilizando dos sistemas DD9800 y una conexión LAN de 10 GbE.

Procedimiento

1. Con las credenciales de inicio de sesión de la cuenta sysadmin proporcionadas por el cliente, inicie sesión en el sistema Data Domain de origen e identifique la cantidad de datos que se recopilaron en el nivel activo del sistema de origen en los últimos siete días.

   Nota

   Esta información también puede extraerse del soporte automático más reciente que generó el dispositivo. Si utiliza un soporte automático para obtener esta información, asegúrese de que sea el más reciente.

```
# filesys show compression
From: 2018-08-29 17:00 To: 2018-09-05 17:00
```

```
Active Tier:
                Pre-Comp   Post-Comp   Global-Comp   Local-Comp      Total-Comp
                   (GiB)       (GiB)        Factor       Factor          Factor
                                                                  (Reduction %)
-------------   --------   ---------   -----------   ----------   -------------
Written:
  Last 7 days    80730.2     37440.7          1.0x         2.2x     2.2x
(53.6)
  Last 24 hrs    80730.2     37440.7          1.0x         2.2x     2.2x
(53.6)
-------------   --------   ---------   -----------   ----------   -------------

Archive Tier:
                Pre-Comp   Post-Comp   Global-Comp   Local-Comp      Total-Comp
                   (GiB)       (GiB)        Factor       Factor          Factor
…
…
Currently Used:*
               Pre-Comp   Post-Comp   Global-Comp   Local-Comp      Total-Comp
                  (GiB)       (GiB)        Factor       Factor          Factor

…
…
       Reduction % = ((Pre-Comp - Post-Comp) / Pre-Comp) * 100
```

En este ejemplo, la recopilación semanal es de aproximadamente 37 TB por semana, lo que equivale a 5,28 TB por día.

2. En el sistema de origen, ejecute el comando `filesys show space` para determinar la cantidad de espacio libre en el nivel activo.

```
# filesys show space
Active Tier:
Resource           Size GiB   Used GiB   Avail GiB   Use%   Cleanable GiB*
----------------   --------   --------   ---------   ----   --------------
/data: pre-comp           -    69480.4           -      -                -
/data: post-comp    30352.2       35.5     30316.7     0%              0.0
/ddvar                 47.2        9.2        35.6    21%                -
/ddvar/core           984.3        2.0       932.3     0%                -
----------------   --------   --------   ---------   ----   --------------

Cloud Tier
Resource           Size GiB   Used GiB   Avail GiB   Use%   Cleanable GiB
----------------   --------   --------   ---------   ----   -------------
/data: pre-comp           -        0.0           -      -               -
/data: post-comp        0.0        0.0         0.0     0%             0.0
----------------   --------   --------   ---------   ----   -------------

Total:
Resource           Size GiB   Used GiB   Avail GiB   Use%   Cleanable GiB
----------------   --------   --------   ---------   ----   -------------
/data: pre-comp           -    69480.4           -      -               -
/data: post-comp    30352.2       35.5     30316.7     0%             0.0
/ddvar                 47.2        9.2        35.6    21%               -
/ddvar/core           984.3        2.0       932.3     0%               -
----------------   --------   --------   ---------   ----   -------------
 * Estimated based on last cleaning of 2018/09/04 06:03:57.
```

3. Calcule la cantidad de espacio consumido en el mes anterior y cuánto espacio adicional será necesario hasta que se complete la migración al sistema de destino.
4. Si el espacio disponible en el nivel activo del sistema de origen es menor que el necesario, agregue almacenamiento adicional al nivel activo antes de continuar con la migración.

⚠ PRECAUCIÓN

Esto requiere detener este procedimiento y reanudarlo después de agregar almacenamiento.

5. Continúe con el resto de los pasos de migración después de que haya suficiente capacidad disponible en el nivel activo del sistema de origen.

Detener el movimiento de datos en el nivel de archiving

Procedimiento

1. Vea las programaciones de archiving establecidas en el sistema de origen.

```
# archive data-movement schedule show
Archive data movement is scheduled to run on day(s) "tue" at
"06:00" hrs
```

2. Establezca la programación de archiving de modo que nunca se detenga el movimiento de datos.

```
# archive data-movement schedule set never
The archive data-movement schedule will be deleted.
        Are you sure? (yes|no|?) [no]: yes
Ok, proceeding.
The archive data-movement is not scheduled.
```

3. Verifique que la programación de movimiento de datos esté establecida en Never.

```
# archive data-movement schedule show
There is no archive data movement schedule.
```

4. Determine si se ha configurado una programación de recuperación de espacio de nivel de archiving en el sistema de origen.

```
# archive space-reclamation schedule show
Archive space-reclamation is scheduled to run on day(s) "mon"
at "10:10" hrs
```

5. Establezca la programación de recuperación de espacio de modo que nunca se detenga el movimiento de datos.

```
# archive space-reclamation schedule set never
The archive space-reclamation schedule will be reset to "never".
        Are you sure? (yes|no|?) [no]: yes
 ok, proceeding.
 The archive space-reclamation schedule is reset to "never".
```

6. Verifique que la programación de recuperación de espacio esté establecida en Never.

```
# archive space-reclamation schedule show
Archive space-reclamation does not have any schedule.
```

7. Verifique que no haya ningún movimiento de datos en curso en el sistema de origen.

```
# archive data-movement status
Data-movement was started on Jun 12 2018 06:00 and completed on
Jun 12 2018 06:01
```

8. Verifique que no haya ninguna recuperación de espacio en curso en el sistema de origen.

```
# archive space-reclamation status
Space-reclamation has never been started.
```

9. Si las operaciones de movimiento de datos o de recuperación de espacio están en curso, espere a que terminen antes de continuar.

Comprobar ubicaciones de archivos

Opcionalmente, vea los MTrees del sistema de origen para determinar si los archivos de cada MTree se encuentran en el nivel activo o en el nivel de archiving. Esta tarea tiene fines informativos y no es necesaria para completar la transferencia de datos desde el sistema de origen hasta el sistema de destino.

Procedimiento

1. Vea los MTrees en el sistema de origen con una política de movimiento de datos. Registre esta información para utilizarla al configurar la replicación en el sistema de destino.

```
# archive data-movement policy show
The default age-threshold value is "none".
Mtree-name                    Age-threshold
----------------------------  --------------
/data/col1/backup             none (default)
/data/col1/large_files_100gb  1
----------------------------  --------------
```

2. Vea las ubicaciones de los archivos en un MTree específico.

```
# archive report generate file-location path /data/col1/large_files_100gb
-------------------------------                 ---------------------------
File Name                                       Location(Tier/Archive Unit)
-------------------------------                 ---------------------------
/data/col1/large_files_100gb/File_50g.0002.0000  Active
/data/col1/large_files_100gb/File_50g.0001.0000  Active
/data/col1/large_files_100gb/File_50g.0003.0000  archive-unit-2
/data/col1/large_files_100gb/File_50g.0006.0000  archive-unit-2
```

3. Opcionalmente, ejecute el comando `archive report generate file-location path all` para ver una lista de todos los archivos presentes en el sistema.

Nota

En función del número de archivos almacenados en el sistema de origen, este comando requerirá bastante tiempo para completarse.

Aplicar la licencia de replicación de Data Domain

Procedimiento

1. Vea las licencias en un sistema de origen con las licencias heredadas.

```
# license show
Feature licenses:
##   License Key           Feature
--   -------------------   ------------------
1    SSRF-VRVZ-ZHYB-WDRF   EXTENDED-RETENTION
2    WTXV-TSWX-HWDR-RHDX   DDBOOST
--   -------------------   ------------------
```

2. Añada la licencia de replicación.

```
# license add <license-key>
```

3. Verifique que la licencia de replicación se haya agregado al sistema de origen.

```
# license show
Feature licenses:
```

```
##   License Key           Feature
--   -------------------   ------------------
1    SSRF-VRVZ-ZHYB-WDRF   EXTENDED-RETENTION
2    WTXV-TSWX-HWDR-RHDX   DDBOOST
3    EZXW-SZZF-BGCS-VRZX   REPLICATION
--   -------------------   ------------------
```

4. Vea las licencias en el sistema de destino con licencias ELMS.

```
# elicense show
System locking-id: APM00000000001

Licensing scheme: EMC Electronic License Management System (ELMS) node-locked mode

Capacity licenses:
##   Feature              Shelf Model   Capacity     Mode        Expiration Date
--   ------------------   -----------   ----------   ---------   ---------------
1    CAPACITY-ACTIVE      ES30          32.74 TiB    permanent   n/a
2    SSD-CAPACITY         n/a           1.45 TiB     permanent   n/a
3    CLOUDTIER-CAPACITY   n/a           218.27 TiB   permanent   n/a
--   ------------------   -----------   ----------   ---------   ---------------
Licensed Active Tier capacity: 32.74 TiB*
* Depending on the hardware platform, usable filesystem capacities may vary.

Feature licenses:
##   Feature                        Count   Mode              Expiration Date
--   ----------------------------   -----   ---------------   ---------------
1    DDBOOST                            1   permanent         n/a
--   ----------------------------   -----   ---------------   ---------------
License file last modified at : 2018/06/28 06:29:03.
```

5. Añada la licencia de replicación actualizando la clave de licencia obtenida del portal de licencias. Abra el archivo de licencia en un editor de texto y, a continuación, cópielo y péguelo en el mensaje de actualización seguido de **Ctrl + D**.

```
# elicense update
Enter the content of license file and then press Control-D, or
press Control-C to cancel.
```

6. Verifique que la licencia de replicación se haya agregado al sistema de origen.

```
# elicense show
System locking-id: APM00000000001

Licensing scheme: EMC Electronic License Management System (ELMS) node-locked mode

Capacity licenses:
##   Feature              Shelf Model   Capacity     Mode        Expiration Date
--   ------------------   -----------   ----------   ---------   ---------------
1    CAPACITY-ACTIVE      ES30          32.74 TiB    permanent   n/a
2    SSD-CAPACITY         n/a           1.45 TiB     permanent   n/a
3    CLOUDTIER-CAPACITY   n/a           218.27 TiB   permanent   n/a
--   ------------------   -----------   ----------   ---------   ---------------
Licensed Active Tier capacity: 32.74 TiB*
* Depending on the hardware platform, usable filesystem capacities may vary.

Feature licenses:
##   Feature                        Count   Mode              Expiration Date
--   ----------------------------   -----   ---------------   ---------------
1    REPLICATION                        1   permanent         n/a
2    DDBOOST                            1   permanent         n/a
--   ----------------------------   -----   ---------------   ---------------
License file last modified at : 2018/06/28 06:29:03.
```

Iniciar la replicación desde el sistema de origen al sistema de destino

Tome nota del número máximo óptimo de MTrees y contextos de replicación que puede tener un sistema Data Domain. Si el sistema de origen tiene varios MTrees que superan el contexto de replicación máximo permitido a la vez, es posible que se

requieran varios contextos de replicación en serie para transferir los datos al sistema de destino. Por ejemplo, el DD860 admite 90 contextos de replicación de MTree y el DD990 admite un máximo de 270 contextos de replicación de MTree.

Procedimiento

1. Determine el nombre de host del sistema de origen.

```
# hostname
The Hostname is: Source.ER.FQDN
```

2. Determine el nombre de host del sistema de destino.

```
# hostname
The Hostname is: Target.DD.FQDN
```

3. En el sistema de origen, establezca el contexto de replicación de MTree en el sistema de destino.

```
# replication add source mtree://Source.ER.FQDN/data/col1/large_files_100gb destination
mtree://Target.DD.FQDN/data/col1/large_files_100gb encryption enabled
Encryption enabled for replication context mtree://Target.DD.FQDN/data/col1/
large_files_100gb
Please verify that replication encryption is also enabled for this context on the
remote host.
```

4. En el sistema de destino, establezca el contexto de replicación de MTree en el sistema de origen.

```
# replication add source mtree://Source.ER.FQDN/data/col1/large_files_100gb destination
mtree://Target.DD.FQDN/data/col1/large_files_100gb encryption enabled
Encryption enabled for replication context mtree://Target.DD.FQDN/data/col1/
large_files_100gb
Please verify that replication encryption is also enabled for this context on the
remote host.
```

5. En el sistema de origen, inicie la operación de replicación. No es necesario ejecutar este comando en el sistema de destino.

Nota

El tiempo necesario para que el contexto de replicación se inicialice depende de la cantidad de datos presentes en el MTree de origen que se replica por primera vez.

```
# replication initialize mtree://Target.ER.FQDN/data/col1/
large_files_100gb
(00:08) Waiting for initialize to start...
(00:10) Initialize started.
Use 'replication watch mtree://Target.DDR.FQDN/data/col1/one'
to monitor progress.
```

6. En el sistema de origen, verifique que no haya errores en la configuración de replicación.

Nota

El tiempo necesario para que el contexto de replicación se inicialice depende de la cantidad de datos presentes en el MTree de origen que se replica por primera vez.

```
#  replication status mtree://target.ER.FQDN/data/col1/
large_files_100gb
CTX:                                    1
Mode:                                   source
Destination:                            mtree://Target.DD.FQDN/
data/col1/one
Enabled:                                yes
```

```
Low bandwidth optimization:             disabled
Replication encryption:                 enabled
Replication propagate-retention-lock:   enabled
Local filesystem status:                enabled
Connection:                             connected since Tue Jun
12 17:46:14
State:                                  initializing 3/3 0%
Error:                                  no error
Sync'ed-as-of time:                     -
Current throttle:                       unlimited
```

7. En el sistema de origen, verifique que la replicación esté en curso.

```
#  replication watch mtree://Source.ER.FQDN/data/col1/large_files_100gb
Use Control-C to stop monitoring.

(00:00) Replication initialize started...
(00:02) initializing:
(00:18)       0% complete, pre-comp: 213183 KB/s, network: 120855 KB/s
(00:22)       0% complete, pre-comp: 246130 KB/s, network: 120719 KB/s
```

Monitorear el progreso de la replicación

Procedimiento

1. Vea los detalles de configuración de todos los contextos de replicación de MTree en el sistema de origen.

```
# replication show config
```

2. Vea el progreso general en todas las operaciones de replicación en curso.

```
# replication show detailed-stats
```

3. Vea el progreso de una operación de replicación específica.

```
# replication show detailed-stats mtree://Target.ER.FQDN/data/col1/large_files_100gb
```

4. Vea el rendimiento de todos los contextos de replicación.

```
# replication show performance all
06/12 17:58:14
       rctx://1               rctx://2               rctx://3
 Pre-comp    Network     Pre-comp    Network     Pre-comp    Network
  (KB/s)     (KB/s)       (KB/s)     (KB/s)       (KB/s)     (KB/s)
 ---------  ---------    ---------  ---------    ---------  ---------
     29459      37607        36374      38071     13089559      39043
    113832      45061        38138      37327     13012122      38812
     29298      42153        33231      36388     12869385      38387
```

Confirme que la inicialización de la replicación esté completa o sincronizada

Procedimiento

1. En el sistema de origen, vea las estadísticas de replicación.

```
# replication show detailed-stats
```

Cuando se completa una operación de replicación, la salida muestra un valor de cero en la columna `Post-comp Bytes Remaining`. El valor de la columna `Sync'ed-as-of` muestra la hora más reciente en la que los sistemas de origen y de destino estuvieron sincronizados.

2. Si la replicación sigue en curso, espere a que se completen las operaciones.
3. Verifique los tamaños de MTree en la coincidencia de los sistemas de origen y de destino. Ejecute el siguiente comando en ambos sistemas:

```
# mtree list
Name                          Pre-Comp (GiB)   Status
----------------------------  --------------   ------
```

```
/data/col1/large_files_100gb           2500.0   RW
----------------------------   --------------   ------
```

Interrumpir el contexto de replicación

Antes de comenzar

Verifique que el MTree en el sistema de origen ya no recopile datos.

Procedimiento

1. Interrumpa el contexto de replicación en el sistema de origen.

   ```
   # replication break mtree://Target.DD.FQDN /data/col1/
   large_files_100gb
   ```

2. Interrumpa el contexto de replicación en el sistema de destino.

   ```
   # replication break mtree://Target.DD.FQDN /data/col1/
   large_files_100gb
   ```

3. Verifique que el contexto de replicación se haya interrumpido en el sistema de origen.

   ```
   # replication show config
   ```

4. Verifique que el contexto de replicación se haya interrumpido en el sistema de destino.

   ```
   # replication show config
   ```

5. Verifique que el MTree en el sistema de destino esté establecido en lectura/escritura

   ```
   # mtree list
   Name                           Pre-Comp (GiB)   Status
   ----------------------------   --------------   ------
   /data/col1/large_files_100gb   2500.0           RW
   ----------------------------   --------------   ------
   ```

Replanificar el sistema de origen

Antes de comenzar

⚠ PRECAUCIÓN

Los siguientes elementos deben completarse antes de replanificar el sistema de origen. No continúe con esta tarea hasta que se completen todos los requisitos:

- **Todos los datos del sistema de origen se replican en el sistema de destino.**
- **Todos los trabajos de respaldo ahora apuntan al sistema de destino.**
- **El sistema de destino realiza todas las lecturas y restauraciones de los respaldos antiguos.**
- **El sistema de destino cumple todos los requisitos de cumplimiento de normas.**

Procedimiento

1. Destruya el sistema de archivos en el sistema de origen y establézcalo en cero.

   ```
   # filesys destroy and-zero
   ```

Nota

El nivel de archiving no se puede deshabilitar. La única manera de quitarlo es destruir el sistema de archivos.

2. Identifique los gabinetes de disco que se adjuntan al nivel de archiving.

```
# storage show tier archive
Archive tier details:
Disk      Disks      Count   Disk       Additional
Group                       Size       Information
-------   --------   -----   --------   -----------
dg2       4.1-4.15   15      1.8 TiB
dg3       3.1-3.15   15      1.8 TiB
```

3. Quite los gabinetes de nivel de archiving del sistema.

```
# storage remove enclosures 3
Removing enclosure 3...Enclosure 3 successfully removed.

Updating system information...done

Successfully removed: 3  done

# storage remove enclosures 4
Removing enclosure 4...Enclosure 4 successfully removed.

Updating system information...done

Successfully removed: 4  done
```

4. Verifique que los gabinetes de nivel de archiving se quiten del sistema

```
# storage show all
Active tier details:
Disk      Disks      Count   Disk       Additional
Group                       Size       Information
-------   --------   -----   --------   -----------
dg1       2.1-2.14   14      1.8 TiB
(spare)   2.15       1       1.8 TiB
-------   --------   -----   --------   -----------
Current active tier size: 21.8 TiB
Active tier maximum capacity: 43.7 TiB
Storage addable disks:
Disk        Disks      Count   Disk       Enclosure   Shelf
Capacity   Additional
Type                           Size       Model       License
Needed   Information
---------   --------   -----   --------   ---------
--------------   ---------
(unknown)   3.1-3.15   15      1.8 TiB    ES30        21.8 TiB
(unknown)   4.1-4.15   15      1.8 TiB    ES30        21.8 TiB
---------   --------   -----   --------   ---------
--------------   ---------
```

5. Quite los gabinetes de nivel de archiving del rack.

Configurar DD Cloud Tier en el sistema de destino

DD Cloud Tier requiere DD OS 6.0.X o posterior, y solamente se admite en ciertos modelos de sistema Data Domain. Plataformas compatibles en la página 510 proporciona la lista de modelos compatibles con DD Cloud Tier. DD Cloud Tier y el almacenamiento de nivel de archiving no se pueden configurar simultáneamente en el mismo sistema Data Domain.

Procedimiento

1. Configure almacenamiento para los niveles activo y de nube. Como requisito previo, las licencias de capacidad adecuadas para los niveles activo y de nube deben estar instaladas.

   a. Asegúrese de que estén instaladas las licencias para las funciones CLOUDTIER-CAPACITY y CAPACITY-ACTIVE. Para verificar la licencia de ELMS:

   ```
   # elicense show
   ```

   Si no está instalada la licencia, utilice el comando `elicense update` para instalarla. Escriba el comando y pegue el contenido del archivo de licencia después de este indicador. Después de pegar, asegúrese de que haya un retorno de carro y luego presione `Control-D` para guardar. Se le solicitará reemplazar licencias y, después de contestar de manera afirmativa, se aplican y se muestran las licencias.

   ```
   # elicense update
   Enter the content of license file and then press Control-D,
   or press Control-C to cancel.
   ```

   b. Visualice el almacenamiento disponible:

   ```
   # storage show all# disk show state
   ```

   c. Agregue almacenamiento al nivel activo:

   ```
   # storage add enclosures <número de gabinete> tier active
   ```

   d. Agregue almacenamiento al nivel de nube.

   ```
   # storage add enclosures <número de gabinete> tier cloud
   ```

2. Instale certificados.

   Antes de poder crear un perfil de nube, debe instalar los certificados asociados. Consulte Importación de certificados en la página 625 para obtener más información.

   Para los proveedores de nube pública AWS, Azure y Virtustream, los certificados de CA raíz se pueden descargar desde https://www.digicert.com/digicert-root-certificates.htm.

   - Para un proveedor de nube de AWS o Azure, descargue el certificado raíz de Baltimore CyberTrust.
   - Para Alibaba, descargue el certificado raíz de GlobalSign R1 en https://support.globalsign.com/customer/portal/articles/1426602-globalsign-rootcertificates.
   - Para un proveedor de nube Virtustream, descargue el certificado de CA raíz de DigiCert High Assurance EV.
   - Para ECS, la autoridad de certificación raíz varía por cliente. Para obtener más información, póngase en contacto con su proveedor de balanceo de carga.

   Los archivos de certificados descargados tienen una extensión .crt. Utilice openssl en cualquier sistema Linux o Unix donde esté instalado para convertir el archivo de formato .crt a .pem.

   ```
   $openssl x509 -inform der -in DigiCertHighAssuranceEVRootCA.crt
   -out DigiCertHighAssuranceEVRootCA.pem
   ```

```
$openssl x509 -inform der -in BaltimoreCyberTrustRoot.crt -out
BaltimoreCyberTrustRoot.pem
```

```
# adminaccess certificate import ca application cloud
Enter the certificate and then press Control-D, or press
Control-C to cancel.
```

3. Para configurar el sistema Data Domain para transferencia de datos a la nube, primero debe habilitar la función “cloud” y establecer la frase de contraseña del sistema si no lo hizo todavía.

```
# cloud enable
Cloud feature requires that passphrase be set on the system.
Enter new passphrase:
Re-enter new passphrase:
Passphrases matched.
The passphrase is set.
Encryption is recommended on the cloud tier.
    Do you want to enable encryption? (yes|no) [yes]:
Encryption feature is enabled on the cloud tier.
Cloud feature is enabled.
```

4. Configure el perfil de nube con las credenciales del proveedor de nube. Las variables y los indicadores varían según el proveedor.

```
# cloud profile add <nombredeperfil>
```

Nota

Por motivos de seguridad, este comando no muestra las claves de acceso ni la seña secreta que usted especifica.

Seleccione el proveedor:

```
Enter provider name (alibabacloud|aws|azure|ecs|google|
s3_flexible|virtustream)
```

- Alibaba Cloud requiere la clave de acceso, la clave secreta, la clase de almacenamiento y la región.
- AWS S3 requiere la clave de acceso, la clave secreta, la clase de almacenamiento y la región.
- Azure requiere el nombre de cuenta, independientemente de que sea una cuenta Azure Government o no, la clave primaria, la clave secundaria y la clase de almacenamiento.
- ECS requiere la entrada de la clave de acceso, la seña secreta y el terminal.
- Google Cloud Platform requiere la clave de acceso, la clave secreta y la región. (La clase de almacenamiento es Nearline).
- Los proveedores de S3 Flexible requieren el nombre del proveedor, la clave de acceso, la clave secreta, la región, el terminal y la clase de almacenamiento.
- Virtustream requiere la clave de acceso, la seña secreta, la clase de almacenamiento y la región.

Al final de cada adición de perfil, se le preguntará si desea configurar un proxy. Si lo hace, se requieren estos valores: *nombre de host de proxy*, *puerto de proxy*, *nombre de usuario de proxy* y *contraseña de proxy*.

5. Verifique la configuración de perfil de nube:

```
# cloud profile show
```

6. Si no se ha creado, cree el sistema de archivos de nivel activo:

   ```
   # filesys create
   ```

7. Active el sistema de archivos:

   ```
   # filesys enable
   ```

8. Configure la unidad de nube:

   ```
   # cloud unit add nombredeunidad profile nombredeperfil
   ```

   Use el comando `cloud unit list` para enumerar las unidades de nube.

9. De manera opcional, configure el cifrado para la unidad de nube.

   a. Verifique que la licencia ENCRYPTION esté instalada.

      ```
      # elicense show
      ```

   b. Active el cifrado para la unidad de nube:

      ```
      # filesys encryption enable cloud-unit nombredeunidad
      ```

   c. Verifique el estado de cifrado:

      ```
      # filesys encryption status
      ```

10. Cree uno o más MTrees.

    ```
    # mtree create /data/col1/mt11
    ```

11. Verifique la configuración de DD Cloud Tier:

```
# cloud provider verify
This operation will perform test data movement after creating a temporary profile and
bucket.
Do you want to continue? (yes|no) [yes]:
Enter provider name (aws|azure|virtustream|ecs|s3_generic): aws
Enter the access key:
Enter the secret key:
Enter the region (us-east-1|us-west-1|us-west-2|eu-west-1|apnortheast-1|ap-southeast-1|
ap-southeast-2|
sa-east-1|ap-south-1|ap-northeast-2|eu-central-1):

Verifying cloud provider …
This process may take a few minutes.
Cloud Enablement Check:
 Checking Cloud feature enabled: PASSED
 Checking Cloud volume: PASSED

Connectivity Check:
 Checking firewall access: PASSED
 Validating certificate PASSED

Account Validation:
 Creating temporary profile: PASSED
 Creating temporary bucket: PASSED

S3 API Validation:
 Validating Put Bucket: PASSED
 Validating List Bucket: PASSED
 Validating Put Object: PASSED
 Validating Get Object: PASSED
 Validating List Object: PASSED
 Validating Delete Object: PASSED
 Validating Bulk Delete: PASSED

Cleaning Up:
```

```
 Deleting temporary bucket: PASSED
 Deleting temporary profile: PASSED

Provider verification passed.
```

12. Configure la política de migración de archivos para este MTree. Puede especificar varios MTrees en este comando. La política se puede basar en el umbral o el intervalo de antigüedad.

    a. Para configurar el umbral de antigüedad (migración de archivos anteriores a la antigüedad especificada a la nube):

    ```
    # data-movement policy set age-threshold antigüedad_en_días
    to-tier cloud cloud-unit nombredeunidad mtrees nombredemtree
    ```

    b. Para configurar el rango de antigüedad (migración solo de esos archivos que se encuentran en el rango de antigüedad especificado):

    ```
    # data-movement policy set age-range min-age
    antigüedad_en_días max-age antigüedad_en_días to-tier cloud
    cloud-unit nombredeunidad mtrees nombredemtree
    ```

13. Exporte el sistema de archivos y, desde el cliente, monte el sistema de archivos y recopile datos en el nivel activo. Cambie la fecha de modificación de los archivos recopilados a fin de que cumplan los requisitos para la migración de datos. (Configure la fecha en anteriores al valor de umbral de antigüedad especificado al configurar la política de transferencia de datos).
14. Inicie la migración de los archivos antiguos. Una vez más, puede especificar varios MTrees con este comando.

    ```
    # data-movement start mtrees nombredemtree
    ```

    Para comprobar el estado de la transferencia de datos:

    ```
    # data-movement status
    ```

    También puede ver el progreso de la transferencia de datos:

    ```
    # data-movement watch
    ```

15. Verifique que la migración de archivos haya funcionado y que los archivos ahora estén en el nivel de nube:

    ```
    # filesys report generate file-location path all
    ```

16. Una vez que ha migrado un archivo al nivel de nube, no puede leer directamente del archivo (si intenta hacerlo, se produce un error). El archivo solo se puede recuperar al nivel activo. Para recuperar un archivo al nivel activo:

    ```
    # data-movement recall path nombrederuta
    ```

CAPÍTULO 20

DD Retention Lock

Este capítulo incluye:

- Descripción general del DD Retention Lock 584
- Protocolos de acceso a datos admitidos 586
- Activación de DD Retention Lock en un MTree 587
- Control de archivo Retention Lock del lado del cliente 590
- Comportamiento del sistema con DD Retention Lock 596

Descripción general del DD Retention Lock

Cuando los datos se bloquean en un MTree activado con DD Retention Lock, este ayuda a asegurar el mantenimiento de la integridad de datos. Ningún dato bloqueado puede ser sobrescrito, modificado o eliminado por un período de retención definido por el usuario de hasta 70 años.

Hay dos ediciones del DD Retention Lock:

- *Data Domain Retention Lock Governance Edition* conserva la funcionalidad de Data Domain Retention Lock previa a DD OS 5.2. Puede utilizar Domain Retention Lock Governance para definir las políticas de retención de datos que se mantendrán por un período específico para cumplir con las políticas internas de gobierno corporativo de TI, implementadas por el administrador del sistema.
- *Data Domain Retention Lock Compliance Edition* le permite cumplir con los requisitos de mantenimiento de datos más estrictos de las normas reglamentarias, como las de la SEC 17a-4(f). La lista completa de las normas reguladoras incluye lo siguiente:
  - Norma 1.31b de CFTC
  - FDA 21 CFR Parte 11
  - Ley Sarbanes-Oxley
  - IRS 98025 y 97-22
  - Norma ISO 15489-1:
  - MoREQ2010

  Para obtener más información en cuanto a certificaciones, consulte las *Evaluaciones de Cumplimiento - Resumen y conclusiones - EMC Data Domain Retention Lock Compliance Edition* en:

  https://www.emc.com/collateral/analyst-reports/cohasset-dd-retention-lock-assoc-comp-assess-summ-ar.pdf

  (Se requiere inicio de sesión.)

  El cumplimiento de estas normas garantiza que los archivos bloqueados en un sistema Data Domain que utiliza el software Data Domain Retention Lock Compliance Edition no puedan ser modificados o destruidos antes de que expire el período de retención. El Data Domain Retention Lock Compliance Edition requiere de un oficial de seguridad para la implementación de las políticas. Un archivo de registro de auditoría es accesible por el administrador u oficial de seguridad.

Cada edición requiere una licencia complementaria por separado, y ya sea una o ambas pueden utilizarse en un único sistema Data Domain.

El protocolo de retención de bloqueo es el mismo tanto para las versión DD Retention Lock Governance como para la Compliance Editions. Las diferencias en el uso se basan en el comportamiento del sistema con el DD Retention Lock Compliance Edition, ya que impone restricciones estrictas para cumplir con los requisitos de cumplimiento. Para una descripción general, consulte el *EMC Data Domain Retention Lock Software – A Detailed Review* (un informe técnico) disponible en:

https://www.emc.com/collateral/hardware/white-papers/h10666-data-domain-retention-lock-wp.pdf

(Se requiere inicio de sesión.)

El DD Retention Lock Governance Edition no requiere de un oficial de seguridad y proporciona un mayor grado de flexibilidad para la retención de datos de archivos en los sistemas Data Domain.

Con respecto a los requisitos de cumplimientos con el almacenamiento de archivos, las normas de la SEC requieren que se almacene una copia por separado de los datos retention-locked con los mismos requisitos de retención que el original. Los archivos retention-locked pueden replicarse a otro sistema Data Domain utilizando DD Replicator. Si se replica un archivo retention-locked, bloqueará la retención en el sistema de destino, con el mismo nivel de protección del archivo de origen.

DD Retention Lock Governance Edition es compatible con las instancias de Data Domain Virtual Edition en las instalaciones, basadas en la nube y DD3300. DD Retention Lock Compliance Edition no es compatible con las instancias Data Domain Virtual Edition en las instalaciones, basadas en la nube o DD3300.

Los temas incluidos a continuación proporcionan información adicional sobre DD Retention Lock.

Protocolo de DD Retention Lock

Solo los archivos que fueron explícitamente confirmados para ser archivos retention-locked tienen un bloqueo de retención en el sistema Data Domain. Los archivos confirmados para ser archivos retention-locked mediante la emisión de comandos de archivo auxiliar del cliente mientras DD Retention Lock Governance o Compliance se encuentran habilitados en el MTree que contiene los archivos.

Nota

Compatible con ambientes de cliente Linux, Unix y Windows.

Los archivos que se escriben en recursos compartidos o las exportaciones que no se confirmaron para ser conservadas (incluso si DD Retention Lock Governance o Compliance está habilitadas en el MTree que contenga los archivos) pueden ser modificados o eliminados en cualquier momento.

El bloqueo de retención impide que cualquier modificación o eliminación de archivos bajo retención se produzcan directamente desde exportaciones de recursos compartidos CIFS o NFS durante el período de retención especificado por un comando de actualización *atime* del lado del cliente. Algunas aplicaciones de archivado y aplicaciones de respaldo pueden emitir este comando cuando se configure de forma adecuada. Las aplicaciones o utilidades que no emiten este comando no pueden bloquear los archivos utilizando DD Retention Lock.

Los archivos retention-locked están siempre protegidos ante modificación o eliminación prematura, incluso aunque el bloqueo de retención se deshabilite posteriormente o que la licencia de retención de bloqueo deje de ser válida .

No se puede cambiar el nombre o eliminar carpetas o directorios que no estén vacíos en un MTree que tenga el bloqueo de retención habilitado. Sin embargo, puede cambiar el nombre o eliminar las carpetas o directorios vacíos y crear otros nuevos.

El periodo de retención de un archivo con bloqueo de retención se puede ampliar (pero no reducir) al actualizar el *atime* del archivo.

Una vez que vence el período de retención de un archivo el archivo puede ser eliminado mediante un comando, script o aplicación del lado del cliente, tanto en el DD Retention Lock Governance como el Compliance. De todas formas, el archivo no puede ser modificado incluso después de vencer el período de retención del archivo. El sistema Data Domain nunca elimina un archivo en forma automática una vez que vencido su período de retención.

Flujo de DD Retention Lock

El flujo general de actividades con DD Retention Lock.

1. Habilite MTrees para el bloqueo de retención de DD Retention Lock Governance o Compliance usando DD System Manager o los comandos del SO de DD emitidos desde la consola del sistema.
2. Bloquee la retención de archivos en el sistema Data Domain mediante comandos en el cliente emitidos por una aplicación de archiving o respaldo con la configuración correspondiente, de forma manual o mediante scripts.

   Nota

   Es posible que los clientes de Windows necesiten descargar programas de utilidades para la compatibilidad del SO de DD.
3. De manera opcional, extienda los tiempos de retención de archivos usando los comandos en el cliente.
4. También de manera opcional, elimine los archivos cuyo período de retención haya vencido mediante los comandos en el cliente.

Protocolos de acceso a datos admitidos

DD Retention Lock es compatible con protocolos Write Once, Read Many (WORM) basados en NAS estándares del sector, y la integración cumple los requisitos de las aplicaciones de archiving, como Symantec Enterprise Vault, SourceOne, Cloud Tiering Appliance o DiskXtender. Los clientes que usan aplicaciones de respaldo, como CommVault, también pueden desarrollar scripts personalizados para usar Data Domain Retention Lock.

La compatibilidad del protocolo de DD Retention Lock es la siguiente:

- NFS es compatible con DD Retention Lock Governance y Compliance.
- CIFS es compatible con DD Retention Lock Governance y Compliance.
- DD VTL es compatible con DD Retention Lock Governance, pero no con DD Retention Lock Compliance.
  Las cintas virtuales, que aquí se denominan *cintas*, se representan como archivos en el sistema de archivos.
  - Cuando crea un pool de almacenamiento, un conjunto de cintas que se asignan a un directorio del sistema de archivos, está creando un MTree, a menos que seleccione específicamente que desea crear el pool de directorio con el estilo anterior (para compatibilidad con versiones anteriores). También puede convertir pools de almacenamiento creados antes del SO DD 5.3 a MTrees. Estos MTrees pueden tener bloqueo de retención y replicación.
  - Puede establecer el bloqueo de retención en una o más cintas por medio del comando `vtl tape modify`, que se describe en la *Guía de referencia de comandos de Data Domain Operating System*.
    El comando *path* `mtree retention-lock revert` se puede usar para revertir el estado de bloqueo de retención de las cintas bloqueadas con el comando `vtl tape modify`. Después de que la cinta se desbloquea, se pueden realizar actualizaciones en ella. El estado desbloqueado no estará visible a través de DD System Manager o la CLI hasta que el servicio de DD VTL se

deshabilite y se vuelva a habilitar. Sin embargo, las actualizaciones se aplicarán a la cinta desbloqueada. Esta funcionalidad es únicamente para DD Retention Lock Governance Edition.

- El tiempo de retención de las cintas se puede mostrar a través del comando `vtl tape show` con el argumento `time-display retention`.
- Puede establecer el bloqueo de retención en una cinta individual a través de DD System Manager.

- DD Boost es compatible con DD Retention Lock Governance y Compliance.
  Si se usan scripts en el cliente para establecer el bloqueo de retención en archivos de respaldo o imágenes de respaldo, y si también se usa una aplicación de respaldo (Veritas NetBackup, por ejemplo) en el sistema por medio de DD Boost, tenga en cuenta que la aplicación de respaldo puede no compartir el contexto de los scripts del cliente. Por lo tanto, cuando una aplicación de respaldo intenta expirar o eliminar archivos que tenían bloqueo de retención por medio de los scripts del cliente, no se libera espacio en el sistema Data Domain.

  Data Domain recomienda que los administradores cambien la política de períodos de retención para que se alinee con el tiempo de bloqueo de retención. Esto se aplica a muchas de las aplicaciones de respaldo integradas con DD Boost, como NetWorker, Veritas NetBackup y Veritas Backup Exec.

  No se permite establecer el bloqueo de retención durante la recopilación de datos en un archivo de DD BOOST en modo DSP, y el cliente que establece el bloqueo de retención recibe un error. El bloqueo de retención se debe establecer después de que finaliza la recopilación de datos.

  No se permite establecer el bloqueo de retención durante la recopilación de datos en un archivo de DD BOOST en modo OST ni en un archivo NFS, y el cliente que escribe los datos recibe un error en cuanto se establece el bloqueo de retención. El archivo parcial escrito antes del bloqueo de retención se confirma en el disco como un archivo WORM.

Activación de DD Retention Lock en un MTree

Solo los archivos dentro de DD Retention Lock Governance o Compliance activan MTrees que puedan ser retention-locked.

Los MTrees activados para DD Retention Lock Compliance no pueden ser convertidos a MTrees de Retention Lock Governance y viceversa.

Los siguientes procedimientos indican cómo habilitar MTrees ya sea para DD Retention Lock Governance o DD Retention Lock Compliance.

Habilitación de DD Retention Lock Governance en un MTree

Agregue una licencia de DD Retention Lock Governance a un sistema y, luego, habilite DD Retention Lock Governance en uno o más MTrees.

Procedimiento

1. Agregue la licencia de DD Retention Lock Governance si no aparece en Feature Licenses.
   a. Seleccione **Administration** > **Licenses**.
   b. En el área Licenses, haga clic en**Add Licenses**.
   c. En el cuadro de texto License Key, escriba la clave de licencia.

Nota

Las claves de licencia no distinguen mayúsculas de minúsculas. Incluya los guiones al escribir las claves.

d. Haga clic en **Add**.

2. Seleccione un MTree para el bloqueo de retención.
   a. Seleccione **Data Management** > **MTree**.
   b. Seleccione el MTree que desea usar para el bloqueo de retención. También puede crear un MTree vacío y agregarle archivos más adelante.
3. Haga clic en la pestaña MTree Summary para mostrar la información del MTree seleccionado.
4. Desplácese hasta Retention Lock y haga clic en **Edit** a la derecha de Retention Lock.
5. Habilite DD Retention Lock Governance en el MTree y, de ser necesario, modifique los períodos mínimos y máximos predeterminados del bloqueo de retención para el MTree.

   Ejecute las siguientes acciones en el cuadro de diálogo Modify Retention Lock:

   a. Seleccione **Enable** para habilitar el DD Retention Lock Governance en el MTree.
   b. Para cambiar los períodos de retención mínimo o máximo para el MTree, modifique el período mínimo o máximo:

      Escriba un número para el intervalo en el cuadro de texto (por ejemplo, `5` or `14`).

      En la lista desplegable, seleccione un intervalo (minutos, horas, días, años).

      Nota

      Si especifica un período de retención mínimo menor a 12 horas, o un período de retención máximo mayor a 70 años, dará como resultado un error.

   c. Haga clic en **Aceptar** para guardar la configuración.

      Después de cerrar el cuadro de diálogo Modify Retention Lock, se mostrará la información actualizada del MTree en el área Retention Lock Summary.
6. Verifique la información de bloqueo de retención para el MTree.

   Tenga en cuenta los siguientes campos del bloqueo de retención:

   - Parte superior:
     - El campo Status indica el acceso de lectura/escritura para el MTree, el tipo de bloqueo de retención en el MTree y si el bloqueo de retención se encuentra habilitado o deshabilitado.
   - Parte inferior:
     - El campo Status indica si el bloqueo de retención se encuentra habilitado para el MTree.
     - El campo Retention Period indica los períodos de retención mínimos y máximos para el MTree. El período de retención que se especifique para

un archivo en el MTree debe ser igual o mayor qu el período de retención mínimo, e igual o menor que el período máximo de retención.

- El campo UUID es un número único de identificación que se genera para el MTree.

Nota

Para verificar los ajustes de configuración del bloqueo de retención para cualquier MTree, seleccione el MTree en el panel de navegación, y luego haga clic en la pestaña Summary.

Requistos posteriores

Archivos retention-lock en un MTree con bloqueo de retención habilitado.

Activación de DD Retention Lock Compliance en un MTree

Agregue una licencia de DD Retention Lock Compliance a un sistema, configure un administrador de sistemas y uno o más agentes de seguridad, configure y habilite el sistema para el uso del software DD Retention Lock Compliance y, luego, active DD Retention Lock Compliance en uno o más MTree.

Procedimiento

1. Agregue la licencia de DD Retention Lock Compliance al sistema, si no está presente.
   a. Primero, compruebe si la licencia ya está instalada.
      ```
      license show
      ```
   b. Si no se muestra la función RETENTION-LOCK-COMPLIANCE, instale la licencia.
      ```
      license add número de licencia
      ```

      Nota

      Las claves de licencia no distinguen mayúsculas de minúsculas. Incluya los guiones al escribir las claves.

2. Configure una o más cuentas de usuario de agentes de seguridad según las reglas de control de acceso basado en funciones (RBAC).
   a. En la función sysadmin, agregue una cuenta de agente de seguridad.
      ```
      user add usuario role security
      ```
   b. Habilite la autorización del agente de seguridad.
      ```
      authorization policy set security-officer enabled
      ```
3. Configure y active el sistema para utilizar DD Retention Lock Compliance.

Nota

Al habilitar DD Retention Lock Compliance, se cumplen varias restricciones en el acceso de bajo nivel a las funciones del sistema utilizadas durante la solución de problemas. Una vez habilitado, la única manera de deshabilitar DD Retention Lock Compliance es iniciar y volver a cargar el sistema, lo que destruirá todos los datos en el este.

a. Configure el sistema para usar DD Retention Lock Compliance.

```
system retention-lock compliance configure
```

El sistema se reinicia automáticamente.

b. Una vez que finalice el proceso de reinicio del sistema, active DD Retention Lock Compliance en el sistema.

```
system retention-lock compliance enable
```

4. Habilite el proceso de cumplimiento en un MTree que contendrá archivos retention-locked.

```
mtree retention-lock enable mode compliance mtree ruta de mtree
```

Nota

El cumplimiento no se puede habilitar en respaldos ni en pools de MTrees.

5. Para cambiar los períodos bloqueo de retención mínimo y máximo predeterminados de un MTree habilitado para el cumplimiento, ingrese los siguientes comandos con la autorización del agente de seguridad.

```
mtree retention-lock set min-retention-
period período mtree ruta de mtree
mtree retention-lock set max-retention-
period período mtree ruta de mtree
```

Nota

El *período* de retención se especifica en el formato [número] [unidad]. Por ejemplo: 1 minuto, 1 hora, 1 día, 1 mes o 1 año. Si especifica un período de retención mínimo menor a 12 horas, o un período de retención máximo superior a 70 años, dará como resultado un error.

Repita los pasos 4 y 5 para habilitar más MTrees.

Requistos posteriores

Los archivos de bloqueo de retención residen en un MTree habilitado para el bloqueo de retención.

Control de archivo Retention Lock del lado del cliente

En esta sección se describe la interfaz de comandos del cliente de DD Retention Lock para bloquear los archivos almacenados en los sistemas Data Domain. Los comandos de los clientes son los mismos tanto para el DD Retention Lock Governance como para el Compliance. Los ambientes de clientes de Linux, Unix y Windows son compatibles;

Sin embargo, los clientes de Windows pueden llegar a tener que descargar programas de utilidades con comandos para bloquear archivos.

Nota

Si la aplicación ya es compatible con WORM de estándar del sector, al escribir un archivo WORM a un MTree habilitado en un sistema DD Retention Lock Governance o Compliance se bloqueará el archivo en el sistema Data Domain. El tiempo de retención en la aplicación debe estar conforme a la configuración del DD Retention Lock. No debería ser necesario que utilice los comandos que se describen en esta sección. Para comprobar si una aplicación está aprobada y certificada para DD Retention Lock, consulte la *Guía de compatibilidad de aplicaciones de archivado de Data Domain*.

Nota

Algunas máquinas cliente que usan NFS, pero que ejecutan un SO heredado, no pueden establecer el tiempo de retención en un valor superior a 2038. El protocolo NFS no impone el límite de 2038 y permite a la especificación de valores de tiempo hasta 2106. Además, DD OS no impone el límite de 2038.

Los comandos del lado del cliente se utilizan para administrar el bloqueo de retención de archivos individuales. Estos comandos se aplican a todos los sistemas Data Domain capaces de realizar bloqueos de retención y deben ser emitidos junto con la instalación y la configuración de DD Retention Lock en el sistema Data Domain.

Herramientas obligatorias para clientes Windows

Necesita el comando `touch.exe` para ejecutar el bloqueo de retención de un cliente basado en Windows.

Para obtener este comando, descargue e instale las utilidades de las aplicaciones basadas en Unix/Linux según su versión de Windows. Estas utilidades son las más recomendadas por Data Domain y deben utilizarse para cada ambiente de cliente.

- Para Windows 8, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003 y Windows XP: http://sourceforge.net/projects/unxutils/files/latest
- Para Windows Server 2008, Windows Vista Enterprise, Windows Vista Enterprise 64-bit edition, Windows Vista SP1, Windows Vista Ultimate y Windows Vista Ultimate 64-bit edition: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=23754
- Para Windows Server 2003 SP1 y Windows Server 2003 R2: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=20983

Nota

El comando `touch` para Windows puede tener un formato diferente a los ejemplos de Linux que se muestran este capítulo.

Siga las instrucciones de instalación y defina la ruta de búsqueda según sea necesario en la máquina cliente.

Acceso de clientes a archivos del sistema Data Domain

Después de habilitar un MTree para DD Retention Lock Governance o Compliance, puede:

- Crear un recurso compartido CIFS basado en el MTree. Este recurso compartido CIFS puede utilizarse en una máquina cliente.

- Crear un montaje del NFS para el MTree y acceder a sus archivos desde el punto de montaje NFS en una máquina cliente.

Nota

Los comandos que aparecen en esta sección deben utilizarse solo en el cliente. No pueden ser emitidos a través del DD System Manager o CLI. La sintaxis del comando puede variar ligeramente según la utilidad que se encuentre utilizando.

Los siguientes temas describen cómo administrar el control de archivos de bloqueo de retención del lado del cliente.

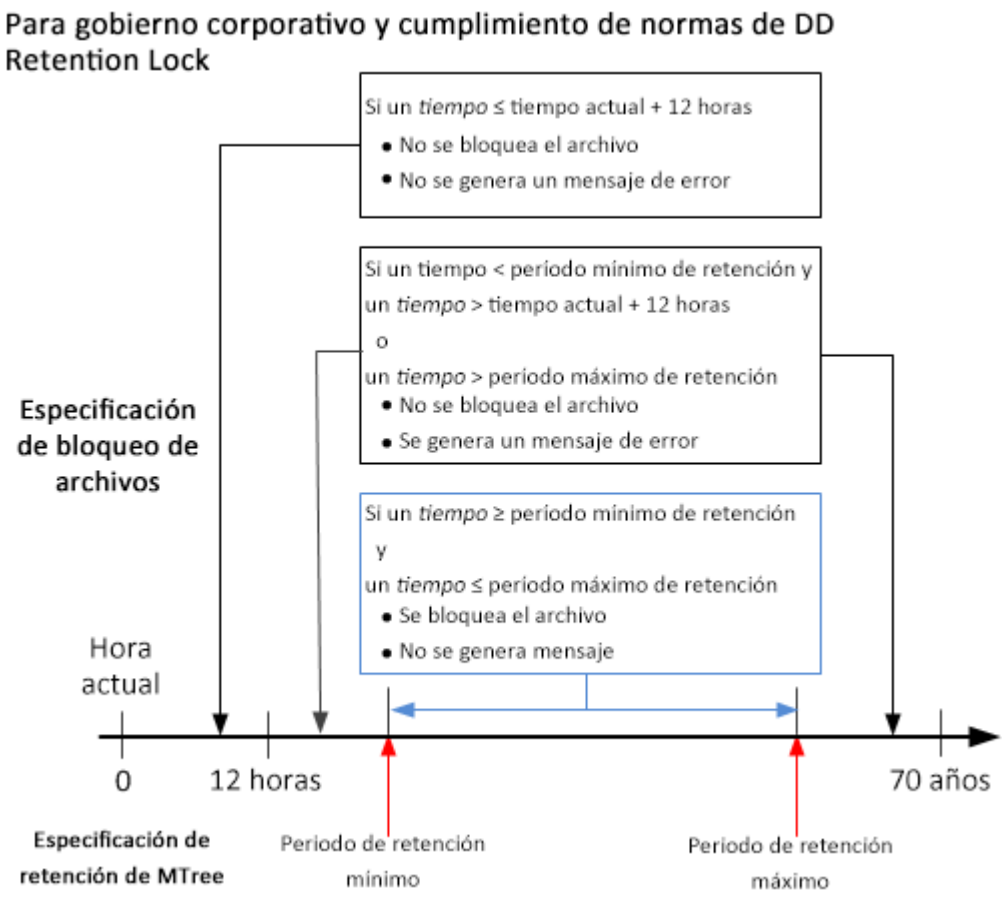
Configuración de bloqueo de retención sobre un archivo

Para ejecutar el bloqueo de retención en un archivo, debe modificar la hora de último acceso (*atime*) del archivo a la hora de retención deseada para el archivo, es decir, la hora en que el archivo puede eliminarse.

Esta acción, por lo general, se ejecuta utilizando la aplicación de archiving, y todas las aplicaciones de archiving que están actualmente calificadas para utilizarse en sistemas Data Domain (según la *Guía de compatibilidad de aplicaciones de archiving de Data Domain*) siguen el protocolo de bloqueo básico que aparece aquí.

El futuro *atime* que especifique debe respetar los períodos mínimos y máximos de retención del MTree del archivo (como compensaciones de la hora actual), tal como se muestra en la siguiente imagen.

Figura 23 Los *atimes* válidos y no válidos para archivos de bloqueo de retención



Nota

Algunas máquinas cliente que usan NFS, pero que ejecutan un SO heredado, no pueden establecer el tiempo de retención en un valor superior a 2038. El protocolo NFS no impone el límite de 2038 y permite a la especificación de valores de tiempo hasta 2106. Además, DD OS no impone el límite de 2038.

Los errores son de permiso denegado (denominados EACCESS, un error del estándar POSIX). Los mismos son devueltos al script o la aplicación de archivo al establecer el *atime*.

Nota

Un archivo debe estar escrito en su totalidad en el sistema Data Domain antes de establecerse como archivo retention-locked

El comando a continuación puede utilizarse en los clientes para establecer el *atime*:

```
touch -a -t [atime] [filename]
```

El formato del *atime* es:

```
[[YY]YY] MMDDhhmm[.ss]
```

Por ejemplo, supongamos que la fecha y la hora actual es 13:00 del 18 de enero de 2012 (sería, por lo tanto, 201201181300), y el período mínimo de retención es de 12 horas. Agregar el período de retención mínimo de 12 horas a los que fecha y hora genera un valor de 201201190100. Por lo tanto, si el valor de *atime* para un archivo se configura en un valor mayor que 201201190100, se aplica un bloqueo de retención a ese archivo.

El siguiente comando:

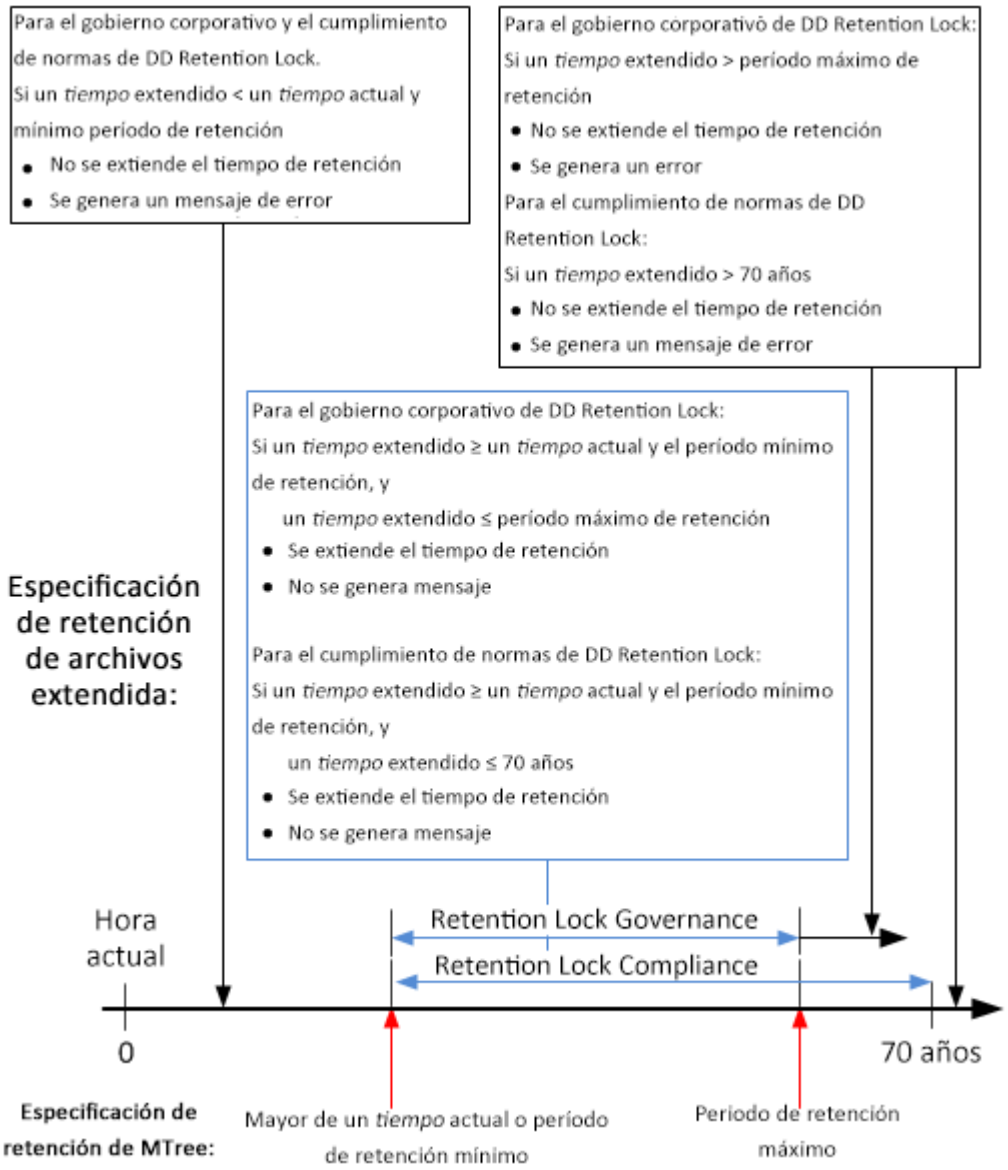
```
ClientOS# touch -a -t 201412312230 SavedData.dat
```

bloqueará el archivo `SavedData.dat` hasta las 22:30 del 31 de diciembre de 2014.

Extensión del bloqueo de retención en un archivo

Para extender el tiempo de retención de un archivo retention-locked, defina el valor del archivo *atime* en un valor mayor que el actual del archivo *atime*, pero menor que el período de retención máximo del MTree del archivo (como una compensación del tiempo actual), como se muestra en la siguiente figura.

Figura 24 Valores válidos y no válidos de *atimes* para la extensión del bloqueo de retención en archivos



Por ejemplo, al cambiar el valor *atime* de `201412312230` a `202012121230` usando el siguiente comando:

```
ClientOS# touch -a -t 202012121230 SavedData.dat
```

el archivo se bloqueará hasta las 12:30 h del 12 de diciembre de 2020.

Nota

Algunas máquinas cliente que utilizan NFS, pero que ejecutan un SO muy antiguo, no pueden establecer el tiempo de retención en un valor superior a 2038. El protocolo NFS no impone el límite de 2038 y permite a la especificación de valores de tiempo hasta 2106. Además, DD OS no impone el límite de 2038.

Los errores son de permiso denegado (denominados EACCESS, un error del estándar POSIX). Estos se devuelven al script a o la aplicación de archiving que establece el valor *atime*.

Identificación de un archivo Retention-Locked

El valor de *atime* de un archivo retention-locked es el de su tiempo de retención. Para determinar si un archivo cuenta con bloqueo de retención, intente establecer el *atime* del archivo a un valor previo que el de *atime*. Esta acción fallará con un error de permiso denegado únicamente si el archivo es un archivo retention-locked.

En primer lugar, agregue el valor de *atime* actual a la lista, y luego ejecute el comando `touch` con un *atime* previo, utilizando estos comandos:

```
ls -l --time=atime [filename]
touch -a -t [atime] [filename]
```

El ejemplo siguiente muestra la secuencia de comandos:

```
ClientOS# ls -l --time=atime SavedData.dat
202012121230
ClientOS# touch -a -t 202012111230 SavedData.dat
```

Si el *atime* de `SavedData.dat` es 202012121230 (12:30 p.m. 12 de diciembre, 2020) y el comando `touch` especifica un *atime* previo, 202012111230 (12:30 p.m. 11 de diciembre, 2020), el comando `touch` dará error, lo que indica que `SavedData.dat` es retention-locked.

Nota

La opción `--time=atime` no es compatible con todas las versiones de Unix.

Especificación de un directorio e intervenir solo en esos archivos

Utilice la línea de comandos para crear un directorio raíz que contenga los archivos a los que se les cambiarán la hora de acceso.

En esta rutina, *root directory to start from* contiene los archivos en los que desea cambiar la hora de acceso mediante este comando del sistema cliente:

```
find [root directory to start from] -exec touch -a -t
[expiration time] {} \;
```

Por ejemplo:

```
ClientOS# find [/backup/data1/] -exec touch -a -t 202012121230 {} \;
```

Leer de una lista de archivos y tocar solo aquellos archivos

En esta rutina, *name of file list* es el nombre de un archivo de texto que contiene los nombres de los archivos en los que desea modificar los tiempos de acceso. Cada línea contiene el nombre de un archivo.

Esta es la sintaxis de los comandos del sistema del cliente:

```
touch -a -t [expiration time] 'cat [name of file list]'
```

Por ejemplo:

```
ClientOS# touch -a -t 202012121230 ‘cat /backup/data1/filelist.txt‘
```

Eliminar o marcar un archivo como expirado

Elimine o marque un archivo como expirado con un bloqueo de retención vencido usando una aplicación de cliente, o elimine un archivo usando el comando standard-file-delete.

Marcar un archivo como expirado usando una aplicación hace que sea inaccesible para esta. Es posible que el archivo se elimine o no del sistema Data Domain mediante la operación de vencimiento. Si no se elimina, la aplicación suele proporcionar una operación de eliminación separada. Debe tener los derechos de acceso apropiados para eliminar el archivo, independientes de DD Retention Lock.

Nota

Si el período de retención del archivo retention-locked no ha vencido, la operación de eliminación resulta en un error de denegación de permiso.

Eliminación con privilegios

Para DD Retention Lock Governance (solamente), puede eliminar los archivos con bloqueos de retención siguiendo este proceso de dos pasos.

Procedimiento

1. Use el comando `mtree retention-lock revert`*path* para revertir los archivos con bloqueos de retención.
2. Elimine el archivo en el sistema del cliente mediante el comando `rm`*filename*.

Utilización de ctime o mtime en archivos Retention-Locked.

ctime es el horario de última modificación de metadatos de un archivo.

ctime
ctime queda establecido con el horario en que ocurra cualquiera de los siguientes eventos:

- Un archivo que no es retention-locked tiene un bloqueo de retención.
- El tiempo de retención de un archivo retention-locked es extenso.
- Se revierte un archivo retention-locked.

Nota

Los permisos de acceso de usuario para un archivo con bloqueo de retención se actualizan mediante la herramienta de línea de comandos de Linux `chmod`.

mtime
mtime es el horario de última modificación de un archivo. Cambia solo cuando el contenido del archivo es modificado. Por lo tanto, el mtime de un archivo retention-locked no puede modificarse.

Comportamiento del sistema con DD Retention Lock

Los temas de comportamiento del sistema serán tratados por separado para DD Retention Lock Governance y DD Retention Lock Compliance en las secciones a continuación.

DD Retention Lock Governance

Algunos comandos del DD OS tienen diferentes comportamientos cuando utilizan DD Retention Lock Governance. Las siguientes secciones describen las diferencias en cada uno.

Replicación

La replicación de colección, la replicación de MTree y la replicación de directorios replican el estado de bloqueo o desbloqueo de los archivos.

Los archivos que tienen bloqueo de retención por gobierno corporativo en su origen también lo serán en su destino y poseen el mismo nivel de protección. Para la replicación, el sistema de origen debe tener una licencia de DD Retention Lock Governance instalada. No se requiere una licencia en el sistema de destino.

La replicación es compatible entre sistemas que:

- Utilicen de la misma versión principal de DD OS (por ejemplo, ambos sistemas están utilizan DD OS 5.5.*x.x*).
- Utilicen versiones DD OS que se encuentran dentro de las dos versiones principales consecutivas, ya sea la más reciente o antigua (por ejemplo, 5.3.*x.x* a 5.5.*x.x* o 5.5.*x.x* a 5.3.*x.x*). La replicación entre versiones solo es compatible en la replicación de directorios y MTree.

Nota

La replicación de MTree no es compatible con DD OS 5.0 y las versiones previas.

NOTA:

- La replicación de colección y la replicación de MTree le replican al sistema de destino los periodos mínimos y máximos de retención configurados en los MTrees.
- La replicación del directorio no le replica al sistema de destino los periodos mínimos y máximos de retención.

El procedimiento para configurar y utilizar la replicación de colección, de MTree y de directorios es el mismo que para los sistemas Data Domain que no cuentan con una licencia de DD Retention Lock Governance.

Resincronización de replicación

El comando `replication resync`*destination* intenta sincronizar el destino con el origen cuando el contexto de replicación del MTree o del directorio se divide entre los sistemas de origen y destino. Este comando no puede utilizarse con la replicación de colección. Tenga presente que:

- Si los archivos se migran a nivel de nube antes de que se divida el contexto, la resincronización de replicación de MTree sobrescribe todos los datos en el destino, por lo que será necesario migrar los archivos al nivel de nube nuevamente.
- Si el directorio de destino tiene DD Retention Lock habilitado, pero el directorio de origen no lo tiene habilitado, la resincronización de la replicación de directorios fallará.
- Con la replicación de Mtree, la resincronización fallará si el MTree de origen no tiene el bloqueo de retención habilitado y el MTree de destino lo tiene habilitado.
- Con la replicación de Mtree, la resincronización fallará si los MTrees de origen y de destino tienen el bloqueo de retención habilitado, pero la opción de propagación del bloqueo de retención está establecida en FALSE.

Copia rápida

Cuando se ejecuta el comando `filesys fastcopy [retention-lock] source`*src*`destination`*dest* en un sistema con un MTree habilitado para DD

Retention Lock Governance, el comando preserva el atributo de bloqueo durante la operación de copia rápida.

Nota

Si el MTree de destino no está habilitado para Retention Lock, el atributo de archivo de Retention Lock no se preserva.

Filesys destroy

Efectos del comando `filesys destroy` cuando se ejecuta en un sistema con un MTree habilitado para DD Retention Lock Governance.

- Todos los datos se destruyen, incluidos los datos retention-locked.
- Todas las opciones `filesys` vuelven a sus valores predeterminados. Esto implica que el bloqueo de retención está deshabilitado y que los períodos de retención mínimo y máximo vuelven a sus valores predeterminados en el nuevo sistema de archivos creado.

Nota

Este comando no está permitido si DD Retention Lock Compliance está habilitado en el sistema.

Eliminación de MTree

Cuando el comando `mtree delete` *mtree-path* intenta eliminar un MTree habilitado para DD Retention Lock Governance (o anteriormente habilitado) que actualmente contiene datos, arroja un error.

Nota

El comportamiento de `mtree delete` es similar al comando para eliminar un directorio; un MTree con Retention Lock habilitado (o anteriormente habilitado) puede eliminarse si el MTree está vacío.

DD Retention Lock Compliance

Algunos comandos del DD OS tienen diferentes comportamientos cuando utilizan DD Retention Lock Compliance. Las siguientes secciones describen las diferencias en cada uno.

Replicación

Un MTree habilitado con DD Retention Lock Compliance puede replicarse solamente mediante un MTree y la replicación de recopilaciones. No es compatible con la replicación de directorios.

La replicación de MTree y colección replica el estado de los archivos de bloqueados o desbloqueados. Los archivos en cumplimiento con el bloqueo de retención en el origen también lo son en el destino y cuentan con el mismo nivel de protección. Los períodos mínimos y máximos de retención configurados en MTrees se replican en el sistema de destino.

Para ejecutar la replicación de colección, the same security officer user debe estar presente tanto en los sistemas de origen como en el de destino antes de iniciar la replicación al sistema de destino y luego para la vida útil del par de origen/réplica.

Resincronización de replicación

El comando `replication resync`*destination* puede utilizarse con una replicación de un MTree, pero no con la replicación de una colección.

- Si el MTree de destino contiene archivos retention-locked que no existen en el de origen, la resincronización fallará.
- Los MTrees de origen y de destino deben estar habilitados para DD Retention Lock Compliance, o la resincronización fallará.

Procedimientos de replicación

En los temas de esta sección, se describen los procedimientos de replicación de recopilaciones y MTrees compatibles con DD Retention Lock Compliance.

Nota

Para obtener una descripción completa de los comandos a los que se hace referencia en los siguientes temas, consulte la *Guía de referencia de comandos de Data Domain Operating System.*

Replicar un MTree: Topología personalizada

Replique un MTree habilitado para DD Retention Lock Compliance de un sistema de origen a un sistema de destino.

Antes de comenzar

Active el DD Retention Lock en un MTree y configure el control del archivo de bloqueo de retención del lado del cliente antes de la replicación.

Procedimiento

1. Hasta que se le indique lo contrario, debe ejecutar los siguientes pasos solo en el sistema de destino.
2. Agregue la licencia de DD Retention Lock Compliance al sistema, si no está presente.
   a. Primero, compruebe si la licencia ya está instalada.
      ```
      license show
      ```
   b. Si no se muestra la función RETENTION-LOCK-COMPLIANCE, instale la licencia.
      `license add`*número de licencia*

      Nota

      Las claves de licencia no distinguen mayúsculas de minúsculas. Incluya los guiones al escribir las claves.
3. Configure una o más cuentas de usuario de agentes de seguridad según las reglas de control de acceso basado en funciones (RBAC).
   a. En la función sysadmin, agregue una cuenta de agente de seguridad.
      `user add`*usuario*`role security`
   b. Habilite la autorización del agente de seguridad.
      ```
      authorization policy set security-officer enabled
      ```

4. Configure y active el sistema para utilizar DD Retention Lock Compliance.

   Nota

   Al habilitar DD Retention Lock Compliance, se cumplen varias restricciones en el acceso de bajo nivel a las funciones del sistema utilizadas durante la solución de problemas. Una vez habilitado, la única manera de deshabilitar DD Retention Lock Compliance es iniciar y volver a cargar el sistema, lo que destruirá todos los datos en el este.

   a. Configure el sistema para usar DD Retention Lock Compliance.

      ```
      system retention-lock compliance configure
      ```

      El sistema se reinicia automáticamente.

   b. Una vez que finalice el proceso de reinicio del sistema, active DD Retention Lock Compliance en el sistema.

      ```
      system retention-lock compliance enable
      ```

5. Cree un contexto de replicación.

   ```
   replication add source mtree://source-system-name/data/
   col1/mtree-namedestination mtree://destination-system-
   name/data/col1/mtree-name
   ```

6. Ejecute los siguientes pasos solo en el sistema de origen.
7. Cree un contexto de replicación.

   ```
   replication add source mtree://source-system-name/data/
   col1/mtree-namedestination mtree://destination-system-
   name/data/col1/mtree-name
   ```

8. Inicialice el contexto de replicación.

   ```
   replication initialize mtree://destination-system-name/
   data/col1/mtree-name
   ```

9. Confirme que la replicación se haya completado.

   ```
   replication status mtree://destination-system-name/data/
   col1/mtree-namedetailed
   ```

   Este comando informa que restarán 0 bits precomprimidos al finalizar la replicación.

Replicar un MTree: Topología uno a muchos

Replique un MTree habilitado para DD Retention Lock Compliance de un sistema de origen a múltiples sistemas de destino.

Antes de comenzar

Habilite el DD Retention Lock Compliance en un MTree y configure el control del archivo de bloqueo de retención del lado del cliente antes de la replicación.

Procedimiento

1. Hasta que se le indique lo contrario, debe ejecutar los siguientes pasos solo en el sistema de destino.
2. Agregue la licencia de DD Retention Lock Compliance al sistema, si no está presente.

   a. Primero, compruebe si la licencia ya está instalada.

```
license show
```

b. Si no se muestra la función RETENTION-LOCK-COMPLIANCE, instale la licencia.

```
license add número de licencia
```

Nota

Las claves de licencia no distinguen mayúsculas de minúsculas. Incluya los guiones al escribir las claves.

3. Configure una o más cuentas de usuario de agentes de seguridad según las reglas de control de acceso basado en funciones (RBAC).

a. En la función sysadmin, agregue una cuenta de agente de seguridad.

```
user add usuario role security
```

b. Habilite la autorización del agente de seguridad.

```
authorization policy set security-officer enabled
```

4. Configure y active el sistema para utilizar DD Retention Lock Compliance.

Nota

Al habilitar DD Retention Lock Compliance, se cumplen varias restricciones en el acceso de bajo nivel a las funciones del sistema utilizadas durante la solución de problemas. Una vez habilitado, la única manera de deshabilitar DD Retention Lock Compliance es iniciar y volver a cargar el sistema, lo que destruirá todos los datos en el este.

a. Configure el sistema para usar DD Retention Lock Compliance.

```
system retention-lock compliance configure
```

El sistema se reinicia automáticamente.

b. Una vez que finalice el proceso de reinicio del sistema, active DD Retention Lock Compliance en el sistema.

```
system retention-lock compliance enable
```

5. Cree un contexto de replicación.

```
replication add source mtree://source-system-name/data/col1/mtree-name destination mtree://destination-system-name/data/col1/mtree-name
```

6. Ejecute los siguientes pasos solo en el sistema de origen.
7. Cree un contexto de replicación para cada sistema de destino.

```
replication add source mtree://source-system-name/data/col1/mtree-name destination mtree://destination-system-name/data/col1/mtree-name
```

8. Inicialice el contexto de replicación para cada MTree del sistema de destino.

```
replication initialize mtree://destination-system-name/data/col1/mtree-name
```

9. Confirme que la replicación se haya completado para cada sistema de destino.

`replication status mtree://destination-system-name/data/col1/mtree-name`detailed
Este comando informa que restarán 0 bits precomprimidos al finalizar la replicación.

Adición de la protección de DD Retention Lock Compliance a un par de replicación de MTree existente

Agregue la protección DD Retention Lock Compliance a una pareja de replicación de MTree existente que no se encuentre activada para el bloqueo de retención.

Procedimiento

1. Hasta que se le indique lo contrario, debe ejecutar los siguientes pasos tanto en el sistema de origen como en el de destino.
2. Inicie sesión en el DD System Manager.

   Aparecerá la ventana del DD System Manager con **DD Network** en el panel de navegación.
3. Seleccione un sistema Data Domain

   En el panel de navegación, expanda **DD Network** y seleccione un sistema.
4. Agregue la licencia de DD Retention Lock Governance si no aparece en Feature Licenses.
   a. Seleccione **Administration** > **Licenses**.
   b. En el área Licenses, haga clic en**Add Licenses**.
   c. En el cuadro de texto License Key, escriba la clave de licencia.

   Nota

   Las claves de licencia no distinguen mayúsculas de minúsculas. Incluya los guiones al escribir las claves.

   d. Haga clic en **Add**.
5. Divida el contexto MTree actual en el par de replicación.

   `replication break mtree://destination-system-name/data/col1/mtree-name`
6. Cree el contexto de replicación nuevo.

   `replication add source mtree://source-system-name/data/col1/mtree-name`destination `mtree://destination-system-name/data/col1/mtree-name`
7. Ejecute los siguientes pasos solo en el sistema de origen.
8. Seleccione un MTree para el bloqueo de retención.

   Haga clic en la pestaña **Data Management** > **MTree** y luego en la casilla de verificación del MTree que desea usar para el bloqueo de retención. (También puede crear un MTree vacía y agregarle archivos más adelante.)
9. Haga clic en la pestaña MTree Summary para mostrar la información del MTree seleccionado.
10. Bloquee los archivos en el MTree que sea compliance-enable.
11. Asegúrese de que los MTress tanto el origen y el destino (réplicas) sean los mismos.

```
replication resync mtree://destination-system-name/data/
col1/mtree-name
```

12. Verifique el progreso de la resincronización.

    ```
    replication watch mtree://destination-system-name/data/
    col1/mtree-name
    ```

13. Confirme que la replicación se haya completado.

    ```
    replication status mtree://destination-system-name/data/
    col1/mtree-namedetailed
    ```

    Este comando informa que restarán 0 bits precomprimidos al finalizar la replicación.

Conversión de un par de replicación de recopilaciones en pares de replicación de MTree

Un procedimiento para los clientes que utilizaban la replicación de recopilaciones con DD Retention Lock Compliance en DD OS 5.2 y desean convertir MTrees habilitados para el cumplimiento en el par de replicación de recopilaciones para pares de replicación de MTree.

Procedimiento

1. En el sistema de origen únicamente:
   a. Cree una instantánea para cada MTree habilitado para DD Retention Lock Compliance.

      ```
      snapshot createsnapshot-name /data/col1/mtree-name
      ```

   b. Sincronice el par de replicación de recopilaciones.

      ```
      replication sync col://destination-system-name
      ```

   c. Confirme que la replicación se haya completado.

      ```
      replication status col://destination-system-namedetailed
      ```

      Este comando informa que restarán 0 bits precomprimidos al finalizar la replicación.

   d. Visualice la información de instantánea para cada MTree habilitado para DD Retention Lock Compliance.

      ```
      snapshot list mtree /data/col1/mtree-name
      ```

      Anote los nombres de instantáneas para su uso posterior.

2. Solamente en el sistema de destino:
   a. Confirme que la replicación se haya completado.

      ```
      replication status mtree://destination-system-name/data/
      col1/mtree-namedetailed
      ```

      Este comando informa que restarán 0 bits precomprimidos al finalizar la replicación.

   b. Visualice cada instantánea de MTree replicada en el sistema de destino.

      ```
      snapshot list mtree /data/col1/mtree-name
      ```

   c. Asegúrese de que todas las instantáneas de MTree de DD Retention Lock Compliance se hayan replicado mediante la comparación de los nombres de instantánea generados con los que fueron generados en el sistema de origen.

      ```
      snapshot list mtree /data/col1/mtree-name
      ```

3. En ambos, tanto los sistemas de origen como los de destino:
   a. Deshabilite el sistema de archivos.
      ```
      filesys disable
      ```
   b. Divida el contexto de replicación de recopilaciones.
      ```
      replication break col://destination-system-name
      ```
   c. Active el sistema de archivos. (Puede requerirse la autorización del oficial de seguridad.)
      ```
      filesys enable
      ```
   d. Agregue un contexto de replicación para cada MTree habilitado con DD Retention Lock Compliance.
      ```
      replication add source mtree://source-system-name/data/
      col1/mtree-namedestination mtree://destination-system-
      name/data/col1/mtree-name
      ```

      Nota

      Los nombres de origen y destino del MTree deben ser los mismos.

4. En el sistema de origen únicamente:
   a. Asegúrese de que los MTrees tanto el origen y el destino sean los mismos.
      ```
      replication resync mtree://destination-system-name
      ```
   b. Verifique el progreso de la resincronización.
      ```
      replication watchdestination
      ```
   c. Confirme que la replicación se haya completado.
      ```
      replication status mtree://destination-system-name/data/
      col1/mtree-namedetailed
      ```
      Este comando informa que restarán 0 bits precomprimidos al finalizar la replicación.

Ejecución de la replicación de colección

Replique /data/col1 desde un sistema de origen compliance-enabled a un sistema de destino compliance-enabled.

Nota

Para la replicación de colección debe utilizar la misma cuenta del oficial de seguridad tanto en los sistemas de origen como de destino.

Procedimiento

1. Hasta que se le indique lo contrario, debe ejecutar los siguientes pasos solo en el sistema de origen.
2. Inicie sesión en el DD System Manager.

   Aparecerá la ventana del DD System Manager con **DD Network** en el panel de navegación.
3. Seleccione un sistema Data Domain

   En el panel de navegación, expanda **DD Network** y seleccione un sistema.

4. Agregue la licencia de DD Retention Lock Governance si no aparece en Feature Licenses.
   a. Seleccione **Administration** > **Licenses**.
   b. En el área Licenses, haga clic en**Add Licenses**.
   c. En el cuadro de texto License Key, escriba la clave de licencia.

   > **Nota**
   >
   > Las claves de licencia no distinguen mayúsculas de minúsculas. Incluya los guiones al escribir las claves.

   d. Haga clic en **Add**.
5. Cree el contexto de replicación.

   ```
   replication add source col://source-system-name
   destination col://destination-system-name
   ```
6. Hasta que se le indique lo contrario, debe ejecutar los siguientes pasos solo en el sistema de destino.
7. Destruir el archivo del sistema

   ```
   filesys destroy
   ```
8. Inicie sesión en el DD System Manager.

   Aparecerá la ventana del DD System Manager con **DD Network** en el panel de navegación.
9. Seleccione un sistema Data Domain

   En el panel de navegación, expanda **DD Network** y seleccione un sistema.
10. Cree un sistema de archivos, pero no lo active.

    ```
    filesys create
    ```
11. Cree el contexto de replicación.

    ```
    replication add source col://source-system-name
    destination col://destination-system-name
    ```
12. Configure y active el sistema para utilizar DD Retention Lock Compliance.

    ```
    system retention-lock compliance configure
    ```

    (El sistema se reiniciará automáticamente y ejecutará el comando `system retention-lock compliance enable`).
13. Ejecute los siguientes pasos solo en el sistema de origen.
14. Inicialice el contexto de replicación.

    ```
    replication initialize source col://source-system-
    namedestination col://destination-system-name
    ```
15. Confirme que la replicación se haya completado.

    ```
    replication status col://destination-system-namedetailed
    ```
    Este comando informa que restarán 0 bits precomprimidos al finalizar la replicación.

Adición de la protección de DD Retention Lock Compliance a un par de replicación de recopilaciones existentes

Agregue la protección de DD Retention Lock Compliance a un par de replicación de recopilaciones que fue creado sin DD Retention Lock Compliance habilitado en los sistemas de origen y de destino.

Procedimiento

1. Hasta que se le indique lo contrario, debe ejecutar los siguientes pasos tanto en el sistema de origen como en el de destino.
2. Desactive la replicación.

   `replication disable col://`*`destination-system-name`*
3. Inicie sesión en el DD System Manager.

   Aparecerá la ventana del DD System Manager con **DD Network** en el panel de navegación.
4. Seleccione un sistema Data Domain

   En el panel de navegación, expanda **DD Network** y seleccione un sistema.
5. Hasta que se indique lo contrario, ejecute los siguientes pasos en el sistema de origen.
6. Configure y active el sistema para utilizar DD Retention Lock Compliance.

   `system retention-lock compliance configure`

   (El sistema se reinicia automáticamente ejecutando el comando `system retention-lock compliance enable`).
7. Active el contexto de replicación.

   `replication enable col://`*`destination-system-name`*
8. Hasta que se indique lo contrario, ejecute los siguientes pasos en el sistema de destino.
9. Configure y active el sistema para utilizar DD Retention Lock Compliance.

   `system retention-lock compliance configure`

   (El sistema se reinicia automáticamente ejecutando el comando `system retention-lock compliance enable`).
10. Active el contexto de replicación.

    `replication enable col://`*`destination-system-name`*

Copia rápida

Cuando se ejecuta el comando `filesys fastcopy [retention-lock] source`*`origen`*`destination`*`destino`* en un sistema con un MTree habilitado para DD Retention Lock Compliance, el comando preserva el atributo de Retention Lock durante la operación de copia rápida.

Nota

Si el MTree de destino no está habilitado para Retention Lock, el atributo de archivo de Retention Lock no se preserva.

Uso de la CLI

Consideraciones para un sistema Data Domain con DD Retention Lock Compliance.

- Los comandos que no sean compatibles con el cumplimiento de las normas no pueden ejecutarse. Los siguientes comandos no están permitidos:
  - `filesys archive unit del`*`archive-unit`*
  - `filesys destroy`
  - `mtree delete`*`mtree-path`*
  - `mtree retention-lock reset {min-retention-period`*`period`* `| max-retention-period`*`period`*`} mtree`*`mtree-path`*
  - `mtree retention-lock disable mtree`*`mtree-path`*
  - `mtree retention-lock revert`
  - `user reset`
- El siguiente comando requiere autorización de un oficial de seguridad en caso de que la licencia a ser eliminada sea para DD Retention Lock Compliance:
  - `license del license-feature [`*`license-feature`* `...] | license-code [`*`license-code`* `...]`
- El siguiente comando requiere autorización de un oficial de seguridad en caso de que el DD Retention Lock Compliance se encuentre habilitado en un MTree especificada en el comando:
  - `mtree retention-lock set {min-retention-period`*`period`* `| max-retention-period`*`period`*`} mtree`*`mtree-path`*
  - `mtree rename`*`mtree-path new-mtree-path`*
- El siguiente comando requiere autorización de un oficial de seguridad en caso de que DD Retention Lock Compliance se encuentre habilitado en el sistema:

  Nota

  Estos comandos deben ejecutarse en modo interactivo.

  - `alerts notify-list reset`
  - `config set timezone`*`zonename`*
  - `config reset timezone`
  - `cifs set authentication active-directory realm { [`*`dc1`* `[`*`dc2`* `...]]`
  - `license reset`
  - `ntp add timeserver`*`time server list`*
  - `ntp del timeserver`*`time server list`*
  - `ntp disable`
  - `ntp enable`
  - `ntp reset`
  - `ntp reset timeservers`
  - `replication break {`*`destination`* `| all}`

- `replication disable {`*`destination`* `| all}`
- `system set date`*`MMDDhhmm`*`[[`*`CC`*`]`*`YY`*`]`

Reloj de sistema

DD Retention Lock Compliance implementa un reloj de seguridad interno para evitar la adulteración maliciosa del reloj del sistema.

El reloj de seguridad monitorea y registra de cerca el reloj del sistema. Si después de un año hay un acumulado de dos semanas de desviación entre el reloj de seguridad y el reloj del sistema, el sistema de archivos se deshabilitará, y únicamente un oficial de seguridad podrá reanudarlo.

Búsqueda de desviación del reloj

Puede ejecutar el comando `system retention-lock compliance status` del DD OS (para la que se requiere autorización de un jefe de seguridad) para obtener la información del reloj del sistema y el de seguridad, incluyendo el último valor registrado del reloj de seguridad y la variación acumulada del reloj del sistema. Este valor se actualiza cada 10 minutos.

Eliminar la desviación del reloj

La desviación del reloj se actualiza cada vez que el reloj de seguridad registre un nuevo valor para el reloj del sistema Luego de un año, se restablece a 0.

En cualquier momento, puede ejecutar el comando del DD OS `system set date`*`MMDDhhmm`*`[[`*`CC`*`]`*`AA`*] para establecer la hora del reloj del sistema (será necesaria la autorización del oficial de seguridad). Si la desviación del reloj aumenta a un valor mayor al preestablecido (2 semanas), el sistema de archivos estará desactivado. Siga estos pasos para reiniciar el sistema de archivos y eliminar el sesgo entre los relojes de seguridad y del sistema.

Procedimiento

1. En la consola del sistema, active el sistema de archivos.

   ```
   filesys enable
   ```

2. Cuando se le solicite, confirme que desea salir del comando `filesys enable` y verifique si la fecha del sistema es correcta.
3. Aparecerá la fecha del sistema.

   ```
   # system show all
   ```

4. Si la fecha del sistema no es correcta, establezca la fecha correcta (será necesaria la autorización del oficial de seguridad) y confírmela.

   ```
   system set date MMDDhhmm[[CC]AA]
   system show date
   ```

5. Activar el sistema de archivos de nuevo

   ```
   filesys enable
   ```

6. Cuando se le solicite, continúe con el procedimiento de habilitación..
7. Aparecerá una solicitud para un oficial de seguridad. Complete la autorización del oficial de seguridad para iniciar el sistema de archivos. El reloj de seguridad se actualizará automáticamente a la fecha actual del sistema.

CAPÍTULO 21

DD Encryption

Este capítulo incluye:

- Descripción general del cifrado de DD 610
- Configuración del cifrado 611
- Acerca de la administración de claves 612
- Configuración del administrador de claves 624
- Cambio de administradores de claves después de la configuración 629
- Comprobación de la configuración del cifrado de datos inactivos 631
- Activación y desactivación del cifrado de datos inactivos 631
- Bloqueo y desbloqueo del sistema de archivos 632

Descripción general del cifrado de DD

El cifrado de datos protege los datos del usuario en caso de robo del sistema Data Domain o pérdida de los medios de almacenamiento físicos durante el tránsito. Además, elimina la exposición accidental de una unidad fallida en caso de que se reemplace.

Cuando los datos ingresan en el sistema Data Domain usando cualquiera de los protocolos admitidos (NFS, CIFS, DD VTL, DD Boost y NDMP Tape Server), el flujo se segmenta, toma huellas digitales y se deduplica (compresión global). Luego, se agrupa en regiones de compresión de varios segmentos, se comprime localmente y se cifra antes de almacenarse en el disco.

Cuando se activa, la función de cifrado de datos inactivos cifra todos los datos que ingresan al sistema Data Domain. No puede habilitar el cifrado en un nivel más granular.

⚠ PRECAUCIÓN

Los datos que se almacenaron antes de que se activara la función DD Encryption no se cifran automáticamente. Para proteger todos los datos en el sistema, asegúrese de habilitar la opción de cifrado de datos existente cuando configure el cifrado.

Notas adicionales:
A partir del SO de DD 5.5.1.0, el cifrado de datos inactivos es compatible con los sistemas habilitados para DD Extended Retention con una única unidad de retención. A partir de la versión 5.5.1.0, DD Extended Retention admite solo una única unidad de retención, de modo que la configuración de sistemas en 5.5.1.0 o versiones posteriores cumplirá con esta restricción. Sin embargo, los sistemas instalados antes de la versión 5.5.1.0 pueden tener más de una unidad de retención, pero no funcionarán con el cifrado de datos inactivos hasta que todas las unidades de retención menos una se hayan quitado, o hasta que los datos se hayan movido o migrado a una unidad de retención.

El comando `filesys encryption apply-changes` aplica los cambios de configuración de cifrado a todos los datos presentes en el sistema de archivos durante el siguiente ciclo de limpieza. Para obtener más información acerca de este comando, consulte la *Guía de referencia de comandos de Data Domain Operating System*.

El cifrado de datos en reposo admite todas las aplicaciones de respaldo actualmente compatibles que se describen en las guías de compatibilidad de respaldo disponibles en el soporte en línea en http://support.emc.com.

Data Domain Replicator se puede usar con cifrado a fin de permitir que los datos cifrados se repliquen mediante la replicación de archivos administrada específica de aplicaciones, MTrees, directorios o recopilaciones o con las diversas topologías. Cada forma de replicación funciona exclusivamente con el cifrado y ofrece el mismo nivel de seguridad. Para obtener más información, consulte la sección acerca de cómo usar el cifrado de datos inactivos con replicación.

Los archivos bloqueados con Data Domain Retention Lock se pueden almacenar, cifrar y replicar.

La función de autosoporte incluye información acerca del estado del cifrado en el sistema Data Domain:

- Si está activado el cifrado o no
- El administrador de claves y qué claves se usan
- El algoritmo de cifrado que está configurado
- El estado del sistema de archivos

Configuración del cifrado

Este procedimiento incluye la configuración del administrador de claves.

Si el estado de cifrado en la pestaña **Data Management** > **File System** > **Encryption** aparece como Not Configured, haga clic en **Configure** para configurar el cifrado en el sistema Data Domain.

Nota

La frase de contraseña del sistema debe establecerse para habilitar el cifrado.

Proporcione la siguiente información:

- Algoritmo
  - Seleccione un algoritmo de cifrado de la lista desplegable o acepte el algoritmo AES de 256 bits (CBC) predeterminado.
    AES de 256 bits en modo Galois/Counter (GCM) es el algoritmo más seguro, pero es bastante más lento que el modo de encadenamiento de bloques de cifrado (CBC).
  - Determine qué datos deben cifrarse: existentes y nuevos, o solo nuevos. Los datos actuales se cifrarán durante el primer ciclo de limpieza después de que se reinicie el sistema de archivos. El cifrado de datos actuales puede demorar más que la operación de limpieza del sistema de archivos estándar.
- Administrador de claves (seleccione uno de los tres)
  - Administrador de claves integrado
    De forma predeterminada, el administrador de claves incorporado de Data Domain entra en vigencia después de reiniciar el sistema de archivos, salvo que configure RSA DPM Key Manager.

    Puede habilitar o deshabilitar la rotación de claves. Si la habilita, escriba un intervalo de rotación de entre 1 y 12 meses.
  - Administrador de claves de RSA DPM
  - Administrador de claves de SafeNet KeySecure

  Nota

  Consulte la sección acerca de la administración de claves para obtener una explicación acerca de cómo funcionan el administrador de claves integrado, el administrador de claves de RSA DPM y el administrador de claves de SafeNet KeySecure.

En el resumen, se muestran los valores de configuración seleccionados. Analícelos para corregirlos. Si quiere cambiar un valor, haga clic en **Back** para navegar hacia la página en la que se ingresó y modificarlo.

Se debe reiniciar el sistema para habilitar el cifrado. Para aplicar la nueva configuración, seleccione la opción para reiniciar el sistema de archivos.

Nota

Pueden interrumpirse las aplicaciones mientras que el sistema de archivos se reinicia.

Acerca de la administración de claves

Las claves de cifrado determinan el rendimiento del algoritmo criptográfico. Están protegidas por una frase de contraseña, que se usa para cifrar la clave de cifrado antes de almacenarla en disco en varias ubicaciones. La frase de contraseña es generada por el usuario y, para modificarla, se necesita un administrador y un director de seguridad.

El administrador de claves controla la generación, la distribución y la administración del ciclo de vida de diversas claves de cifrado. Un sistema Data Domain puede usar el administrador de claves integrado, el administrador RSA Data Protection Manager (DPM) o el administrador de claves de SafeNet KeySecure. La compatibilidad con el protocolo de interoperabilidad de administración de claves (KMIP) se incorporó con DD OS 6.1.

Solo se puede usar uno por vez. Cuando el cifrado se habilita en un sistema Data Domain, el administrador de claves incorporado entra en vigencia de forma predeterminada. Si configura el administrador de claves RSA DPM o el de SafeNet KeySecure, estos reemplazan al administrador de claves integrado y permanecen vigentes hasta que se deshabiliten. Se debe reiniciar el sistema de archivos para que funcione un administrador de claves nuevo.

El administrador de claves integrado y el administrador de claves DPM proporcionan múltiples claves, aunque el sistema use solo una clave a la vez para cifrar datos que ingresan en un sistema Data Domain. Si se configura y se habilita el administrador de claves externo, los sistemas Data Domain usan las claves proporcionadas por el servidor de RSA DPM Key Manager. Si la misma instancia de DPM Key Manager administra varios sistemas Data Domain, todos tendrán la misma clave activa (si están usando la misma clase de claves) siempre que se sincronicen y se reinicie el sistema de archivos. El administrador de claves incorporado genera sus claves internamente.

Ambos administradores de claves rotan las claves y admiten un máximo de 254 claves. El administrador de claves incorporado le permite especificar por cuántos meses está vigente una clave antes de ser reemplazada (después de que se reinicia el sistema). El administrador de claves RSA DPM rota las claves de forma regular, según la clase de clave. La rotación de claves del administrador de claves incorporado se administra en el sistema Data Domain. La rotación de claves del administrador de claves se administra en el servidor del administrador de claves externo.

KeySecure
Se admite KeySecure 8.5 y 8.9, que es un producto de administración de claves compatible con KMIP de Safenet Inc/Gemalto Keysecure. Para poder utilizar el administrador de claves KMIP, los usuarios tienen que configurar el administrador de claves y el sistema Data Domain/DD VE para que se tengan confianza. Los usuarios tienen que crear previamente las claves en el administrador de claves. Un sistema Data Domain recupera estas claves y sus estados de KeySecure después de establecer una conexión segura de TLS. Consulte la *Guía de integración de Gemalto KeySecure y Data Domain Operating System* para obtener más información sobre cómo crear claves y utilizarlas en un sistema Data Domain.

Rectificación de claves perdidas o dañadas

Cree un archivo que contenga todas las claves de cifrado actuales del sistema. Su proveedor de soporte puede usar este archivo para importar las claves nuevamente al

sistema en caso de que se pierdan o dañen. Se recomienda que cree un archivo de exportación de forma regular.

Se le solicitan las credenciales del agente de seguridad para exportar las claves. Para una protección adicional de archivos de clave, puede usar una frase de contraseña distinta de la que se usa en el sistema Data Domain. Después de la exportación, se recomienda que guarde el archivo de clave en un servidor de archivos seguro al que solo puedan acceder usuarios autorizados. Debe recordar la frase de contraseña usada para el archivo de clave. Si se pierde u olvida la frase de contraseña, el sistema Data Domain no puede importar y restaurar las claves. Escriba:

```
# filesys encryption keys export
```

Compatibilidad con el administrador de claves

Todos los administradores de claves son compatibles con todos los protocolos de sistemas de archivos de DD OS.

Replicación
Al configurar sistemas Data Domain para la replicación de MTrees de directorios, configure cada sistema Data Domain por separado. Los dos sistemas pueden usar la misma clase de claves o una diferente, y los mismos administradores de claves o diferentes.

Para la configuración de replicación de recopilaciones, el sistema Data Domain se debe configurar en el origen. Después de una interrupción en la replicación, el sistema de réplica original Data Domain debe configurarse para el administrador de claves. De lo contrario, el sistema Data Domain continua usando la última clave conocida.

Trabajo con RSA DPM Key Manager

Si se configura y se activa RSA DPM Key Manager, el sistema Data Domain usa las claves proporcionadas por RSA DPM Key Manager Server. Si la misma instancia de DPM Key Manager administra varios sistemas Data Domain, todos tendrán la misma clave activa (si están usando la misma clase de claves) siempre que se sincronicen y se reinicie el sistema de archivos. La rotación de claves se administra en el servidor de RSA DPM Key Manager.

Si se configura y se activa RSA DPM Key Manager, el sistema Data Domain usa las claves proporcionadas por RSA DPM Key Manager Server. Si la misma instancia de DPM Key Manager administra varios sistemas Data Domain, todos tendrán la misma clave activa (si están usando la misma clase de claves) siempre que se sincronicen y se reinicie el sistema de archivos. La rotación de claves se administra en el servidor de RSA DPM Key Manager.

Estados de claves de cifrado
Una clave Activated-RW siempre está vigente. Si una clave activa pierde su carácter confidencial, RSA DPM Key Manager proporciona una clave nueva. Cuando el sistema Data Domain detecta la nueva clave, emite una alerta para que el administrador reinicie el sistema de archivos.

Las claves vencidas se vuelven de solo lectura para los datos existentes en el sistema Data Domain, y la nueva clave activa se aplica a todos los datos nuevos que se recopilan. Cuando una clave pierde su carácter confidencial, los datos existentes se vuelven a cifrar con la nueva clave de cifrado después de que se ejecuta una limpieza del sistema de archivos. Si se alcanza el número máximo de claves, las claves no utilizadas se deben eliminar para dejar lugar para las nuevas claves.

Para ver información acerca de las claves de cifrado del sistema Data Domain, abra DD System Manager y vaya a la pestaña **Data Management** > **File System** > **Encryption**.

Las claves se enumeran por número de ID en la sección **Encryption Keys** de la pestaña Encryption. Se muestra la siguiente información para cada clave: cuándo se creó una clave, por cuánto tiempo estuvo vigente, su tipo (RSA DPM o Data Domain), su estado (consulte Estados de claves de cifrado de DPM compatibles con Data Domain) y su tamaño después de la compresión. Si el sistema tiene licencia para Extended Retention, se muestran también los siguientes campos:

Tamaño activo (después de la compresión)
La cantidad de espacio físico en el nivel activo cifrado con la clave.

Tamaño de retención (después de la compresión)
La cantidad de espacio físico en el nivel de retención cifrado con la clave.

Haga clic en el MUID de la clave, y el sistema mostrará la siguiente información para la clave en el cuadro de diálogo Key Details: Nivel/unidad (ejemplo: Active, Retention-unit-2), fecha de creación, fecha de fin de vigencia, estado (consulte Estados de claves de cifrado de DPM compatibles con Data Domain) y el tamaño después de la compresión. Haga clic en Close para cerrar el cuadro de diálogo.

Tabla 200 Estados de claves de cifrado de DPM compatibles con Data Domain

Condición	Definición
Pending-Activated	La clave se ha creado. Después de reiniciar un sistema de archivos, la clave se vuelve Activated-RW.
Activated-RW y Activated-RO	Tanto Activated-RW como Activated-RO leen los datos cifrados con sus claves, respectivamente. Activated-RW es la última clave activada.
De-Activated	Una clave se desactiva cuando la hora actual excede el período de validez. La clave se usa para la lectura.
Compromised	La clave solo puede descifrar. Una vez que todos los datos cifrados con la clave compuesta se vuelven a cifrar, el estado cambia a Destroyed Compromised. Las claves vuelven a cifrarse cuando se ejecuta una limpieza del sistema de archivos. Puede eliminar una clave Destroyed Compromised, si es necesario.
Marked-For-Destroy	Usted ha marcado la clave como destruida para que los datos vuelvan a cifrarse.
Destroyed	Después de volver a cifrar todos los datos cifrados con esta clave, DD OS los cambia de Marked-For-Destroy a Destroyed. Además, cuando la clave que se destruye pierde su carácter confidencial, se vuelve Compromised-Destroyed. Puede eliminar claves Destroyed y Compromised-Destroyed.

Tabla 200 Estados de claves de cifrado de DPM compatibles con Data Domain (continuación)

Condición	Definición
	Nota Una clave no se destruye en el sistema Data Domain hasta que se ejecuta y completa una operación de limpieza.

Cómo mantener las claves sincronizadas con RSA DPM Key Manager

Se realiza una sincronización de claves automática todos los días a la medianoche. Se requiere una sincronización de claves manual solo si no puede esperar para la sincronización calendarizada. Cuando las nuevas claves se sincronizan en el sistema Data Domain, se genera una alerta. Esta alerta se borra después de que se reinicia el sistema de archivos.

Después de que RSA DPM Key Manager Server genera nuevas claves, haga clic en el botón **Sync** para que se muestren en la lista Encryption Key en la pestaña Encryption de Data Domain System Manager'.

Nota

Se requiere un reinicio del sistema de archivos si las claves han cambiado desde la última sincronización.

Procedimiento

1. Con DD System Manager, seleccione el sistema Data Domain con el que está trabajando en el panel de navegación.

   Nota

   Ejecute siempre las funciones de DD System Manager en el sistema que seleccionó en el panel de navegación.

2. Seleccione **Data Management** > **File System** > **Encryption**.
3. En la sección Encryption Keys, seleccione la clave **RSA DPM** y haga clic en **Sync**.

Destrucción de una clave (RSA DPM Key Manager)

Destruya una clave si no desea que ningún dato se cifre con esta. Este procedimiento requiere credenciales de agente de seguridad.

Nota

Para obtener información acerca del agente de seguridad, consulte las secciones acerca de cómo crear usuarios locales y cómo activar la autorización de seguridad.

Para cambiar una clave de DPM de RSA a un estado en que puede destruirse:

Procedimiento

1. Desactive la clave de DPM Server de RSA.
2. Reinicie el sistema de archivos para la clave que se debe desactivar en el sistema Data Domain.

3. Con DD System Manager, seleccione **Data Management** > **File System** > **Encryption**.
4. En la sección Encryption Keys, seleccione la clave en la lista que se debe destruir.
5. Haga clic en **Destroy...**

   El sistema muestra el cuadro de diálogo Destroy que incluye el nivel y el estado de la clave.
6. Escriba el nombre de usuario y la contraseña del agente de seguridad.
7. Confirme que desea destruir la clave haciendo clic en **Destroy**.

Nota

Después de que se haya ejecutado una limpieza del sistema, el estado de la clave cambiará a Destroyed.

Eliminación de una clave

Puede eliminar claves del administrador de claves que están en estado Destroyed o Compromised-Destroyed. Sin embargo, solo debe eliminar una clave cuando la cantidad de claves ha alcanzado el límite máximo de 254. Este procedimiento requiere credenciales de agente de seguridad.

Nota

Para llegar al estado Destroyed, es necesario llevar a cabo el procedimiento de destrucción de claves (de Embedded Key Manager o RSA DPM Key Manager) en una clave y una limpieza del sistema.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Encryption**.
2. En la sección Encryption Keys, seleccione la clave o las claves en la lista que se deben eliminar.
3. Haga clic en **Delete...**.

   El sistema muestra la clave que se debe eliminar, y el nivel y el estado de esta.
4. Escriba el nombre de usuario y la contraseña del agente de seguridad.
5. Confirme que desea eliminar la clave o las claves haciendo clic en **Delete**.

Trabajo con Embedded Key Manager

Cuando se selecciona Embedded Key Manager, el sistema Data Domain crea sus propias claves.

Después de que se configura la política de rotación, se crea automáticamente una nueva clave en la próxima rotación. Con una alerta, se le informa acerca de la creación de una nueva clave. Debe reiniciar del sistema de archivos para activar la nueva clave y desactivar la anterior. Puede deshabilitar la política de rotación de claves haciendo clic en el botón Disable asociado con el estado de rotación de claves de Embedded Key Manager.

Creación de una clave (Embedded Key Manager)

Cree una clave de cifrado para Embedded Key Manager.

Procedimiento

1. Seleccione **Data Management** > **File System** > **DD Encryption**.
2. En la sección Encryption Keys, haga clic en **Create...** .
3. Escriba el nombre de usuario y la contraseña del agente de seguridad.
4. Seleccione **Restart the filesystem now** si desea reiniciar el sistema.

   Se creará una nueva clave para Data Domain, Después de que se reinicie el sistema, la clave anterior se desactivará y se activará la nueva clave.
5. Haga clic en **Create**.

Destrucción de una clave (Embedded Key Manager)

Destruya una clave de cifrado para Embedded Key Manager.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Encryption**.
2. En la sección Encryption Keys, seleccione la clave en la lista que se debe destruir.
3. Haga clic en **Destroy...**.

   El sistema muestra el cuadro de diálogo Destroy que incluye el nivel y el estado de la clave.
4. Escriba el nombre de usuario y la contraseña del agente de seguridad.
5. Confirme que desea destruir la clave haciendo clic en **Destroy**.

Nota

Después de que se haya ejecutado una limpieza del sistema de archivos, el estado de la clave cambiará a Destroyed.

Trabajar con el administrador de claves de KeySecure

El administrador de claves de KeySecure es compatible con administradores de claves externos si se implementa el protocolo de interoperabilidad de administración de claves (KMIP) y administra en forma centralizada las claves de cifrado en una plataforma única y centralizada.

- Las claves se crearán previamente en el administrador de claves.
- El administrador de claves del KMIP no se puede habilitar en sistemas con cifrado habilitado en una o más unidades de nube.

Uso de DD System Manager para configurar y administrar el administrador de claves KeySecure

Esta sección describe cómo usar Data Domain System Manager (DD SM) para administrar el administrador de claves KeySecure.

Creación de una clave para el administrador de claves de KeySecure

Cree una clave de cifrado para el administrador de claves de KeySecure (KMIP).

Procedimiento

1. Desplácese hacia abajo para ver la tabla **Key Manager Encryption Keys**.

2. Haga clic en **Add** para crear una nueva clave de cifrado del administrador de claves.
   a. Escriba el nombre de usuario y la contraseña del director de seguridad.
   b. Haga clic en **Restart the file system now**.
   c. Haga clic en **Create**.
3. Haga clic en **Restart the file system now** para que los cambios surtan efecto.

   Se crea una nueva clave KIMP. Después de que se reinicia el sistema de archivos, la clave anterior se desactiva y se activa la nueva clave.

Modificación del estado de una clave existente en el Administrador de claves de KeySecure

Use DD SM para modificar el estado de una clave de cifrado KIMP existente.

Antes de comenzar

Revise las condiciones para cambiar el estado de una clave:

- Cuando ya existe una clave (está activa) y se crea una clave nueva, esta última cambiará al estado `Pending-Activated` hasta que el usuario reinicie el sistema de archivos.
- Los usuarios pueden desactivar una clave en un estado `Activated-RW` solo si hay una clave `Pending-Activated` en su lugar.
- Una clave en un estado `Pending-Activated` se puede desactivar solo si hay una clave `Pending-Activated` en su lugar.
- Una clave en un estado `Activated-RO` no requiere ninguna condición. Se puede desactivar en cualquier momento.

Procedimiento

1. Seleccione **Data Management** > **File System** > **DD Encryption**.
2. Desplácese hacia abajo para ver la tabla **Key Manager Encryption Keys**.
3. Seleccione la clave correspondiente desde la tabla **Key Manager Encryption Keys**.
4. Para desactivar una clave:
   a. Haga clic en cualquier clave que muestre un estado `Activated`.
   b. Escriba el nombre de usuario y la contraseña del director de seguridad.
   c. Haga clic en **DEACTIVATE**.

Figura 25 Cambio de la clave KMIP a un estado desactivado

5. Haga clic en **Restart the filesystem now**.

Resultados

Se cambia el estado de una clave existente.

Configuración del administrador de claves KeySecure

Use DD SM para configurar la política de rotación de claves desde el sistema Data Domain.

Antes de comenzar

Confirme el período de rotación de clave deseado (semanas o meses), la fecha de inicio de la rotación de claves y la fecha de la próxima rotación de claves.

Procedimiento

1. Seleccione **Data Management** > **File System** > **DD Encryption**.
2. En la sección **Key Management**, haga clic en **Configure**. Se abrirá el cuadro de diálogo **Change Key Manager**.
3. Escriba el nombre de usuario y la contraseña del agente de seguridad.
4. Seleccione **KeySecure Key Manager** del menú desplegable **Key Manager Type**. Aparecerá la información de Change Key Manager.
5. Configure la política de rotación de claves:

   Nota

   La política de rotación se especifica en semanas y meses. El incremento mínimo de la política de rotación de claves es de una semana y el incremento máximo es de 52 semanas (o 12 meses).

   a. Active la política de rotación de claves. Configure el botón **Enable Key rotation policy** como activado.
   b. Especifique las fechas adecuadas en el campo Key rotation schedule.
   c. Seleccione la cantidad adecuada de semanas o meses en el menú desplegable **Weeks** o **Months**.
   d. Haga clic en **OK**.
   e. Haga clic en **Restart the filesystem now** si desea reiniciar el sistema de archivos para que los cambios se realicen inmediatamente de acuerdo con la Fig. 3.

Resultados

Se configuró o cambió la política de rotación de claves.

Uso de la CLI de Data Domain para administrar el administrador de claves KeySecure

En esta sección se describe cómo usar la CLI para administrar el administrador de claves KeySecure

Creación de una nueva clave activa en el administrador de claves KeySecure

Utilice la CLI de Data Domain para crear una nueva clave activa.

Antes de comenzar

Asegúrese de tener la información del usuario correspondiente. Para ejecutar estos comandos se requiere la función de seguridad.

Procedimiento

1. Inicie sesión en el sistema de Data Domain mediante la función de seguridad:

   Nombre de usuario: `<security office user>`

   Contraseña: `<security officer password>`

2. Cree una nueva clave activa:

```
# filesys encryption key-manager keys create
```

3. Aparece una salida similar a la siguiente:

```
New encryption key was successfully created.
The filesystem must be restarted to activate the new key.
```

Resultados

Se crea una nueva clave activa.

Modificación del estado de una clave existente en el Administrador de claves de KeySecure

Utilice la CLI de Data Domain para modificar el estado de una clave existente a un estado desactivado.

Antes de comenzar

Asegúrese de tener la información del usuario correspondiente. Para ejecutar estos comandos se requiere la función de seguridad.

Procedimiento

1. Inicie sesión en el sistema de Data Domain mediante la función de seguridad:

   Nombre de usuario: `<security officer user>`

   Contraseña: `<security officer password>`

2. Modifique el estado de una clave existente:

   ```
   # filesys encryption key-manager keys modify{<key-id> | muid
   <key-muid>}state deactivated
   ```

   Por ejemplo:

   ```
   # filesys encryption key-manager keys modify muid
   740D711374A8C964A62817B4AD193C8DC44374A6ED534C85642782014F2E9D
   41 state deactivated
   ```

3. Aparece una salida similar a la siguiente:

   ```
   Key state modified.
   ```

Resultados

Se modifica el estado de una clave existente.

Configuración o restablecimiento de una política de rotación de claves en el administrador de claves de KeySecure

Utilice la CLI de Data Domain para configurar la política de rotación de claves en el sistema de Data Domain para rotar las claves de forma periódica. Tenga en cuenta que la política de rotación se especifica en semanas y meses. El incremento mínimo de la política de rotación de claves es de una semana y el incremento máximo es de 52 semanas (o 12 meses).

Antes de comenzar

Asegúrese de tener la información del usuario correspondiente. Para ejecutar estos comandos se requiere la función de seguridad.

Procedimiento

1. Inicie sesión en el sistema de Data Domain mediante la función de seguridad:

   Nombre de usuario: `sec`

   Contraseña: `<security officer password>`

2. Configure una política de rotación de claves por primera vez. En nuestro ejemplo, configuramos la política de rotación en **tres semanas**:

```
# filesys encryption key-manager set key-rotation-policy
                  {every <n> {weeks | months} | none}
```

Por ejemplo:

```
# filesys encryption key-manager set key-rotation-policy
every 3 weeks
```

Output that is similar to the following appears:

```
Key-rotation-policy is set. Encryption key will be rotated
every 3 weeks.
```

3. Posteriormente, ejecute este comando si decide cambiar la política de rotación de claves existente. En nuestro ejemplo, configuramos la política de rotación de **tres semanas** a **cuatro meses**:

Nota

Inicie sesión en el sistema de Data Domain mediante la función de seguridad (donde el nombre de usuario es `sec` y la contraseña es <`security officer password`>).

```
# filesys encryption key-manager reset [key-rotation-policy]
```

Por ejemplo:

```
filesys encryption key-manager set key-rotation-policy every
4 months
```

Output that is similar to the following appears:

```
Key-rotation-policy is set. Encryption key will be rotated
every 4 months.
```

4. Visualice la política de rotación de claves actual o verifique que la política esté configurada correctamente:

```
# filesys encryption key-manager show
```

Output that is similar to the following appears:

```
The current key-manager configuration is:
Key Manager:                                Enabled
Server Type:                                KeySecure
Server:                                     <IP address of
KMIP server>
Port:                                       5696
Fips-mode:                                  enabled
Status:                                     Online
Key-class:                                  <key-class>
KMIP-user:                                  <KMIP username>
Key rotation period:                        2 months
Last key rotation date:                     03:14:17 03/19
2018
Next key rotation date:                     01:01:00 05/17
2018
```

Resultados

Se configuró o cambió la política de rotación de claves.

Cómo funcionan las operaciones de limpieza

El cifrado afecta el rendimiento de las operaciones de limpieza cuando, con la clave Activated-RW, se vuelven a generar claves para los datos cifrados con las claves Compromised o Marked-For-Destroyed.

Al final de la operación de limpieza, no habrá datos cifrados con las claves Compromised o Marked-For-Destroyed. Además, cualquier dato escrito con la operación de limpieza se cifra con la clave Activated-RW.

Configuración del administrador de claves

Siga las instrucciones para el tipo de administrador de claves que está usando.

Para obtener más información acerca de la configuración de administradores de claves de SafeNet KeySecure, consulte la *Guía de integración de Gemalto KeySecure y Data Domain Operating System*.

Configuración de cifrado de RSA DPM Key Manager

RSA DPM Key Manager debe configurarse en el servidor DPM de RSA y en el sistema Data Domain.

Cómo realizar esta configuración en un servidor DPM de RSA

Los pasos principales para la configuración del servidor DMP de RSA (utilizando la interfaz gráfica del usuario)

Nota

Consulte la versión más reciente de la *Guía de administración del servidor Data Protection Manager de RSA* para obtener más información acerca de cada paso de este procedimiento.

Las configuraciones de modos de cifrado y algoritmos establecidas en el servidor de RSA DPM Key Manager son ignoradas por el sistema Data Domain. Configure estos parámetros en el sistema Data Domain.

Procedimiento

1. Cree una identidad para el sistema Data Domain utilizando el certificado X509. Un canal seguro se crea de acuerdo con este certificado.
2. Cree una clase de claves con los atributos adecuados:
   - Longitud de la clave: 256 bits
   - Duración: Por ejemplo, seis meses o lo que corresponda según su política.
   - Generación automática de claves: Seleccione esta opción para que las claves se generen automáticamente.

   Nota

   Varios sistemas Data Domain pueden compartir la misma clase de claves. Para obtener más información acerca de las clases de claves, consulte la sección acerca de las clases de claves para DPM de RSA.
3. Cree una identidad usando el certificado de host del sistema Data Domain como certificado de identidad. La identidad y la clase de clave deben estar en el mismo grupo de identidades.
4. Importe los certificados. Consulte la sección acerca de cómo importar los certificados para obtener más información.

Acerca de las clases de claves de RSA DPM

El sistema Data Domain recupera una clave de RSA DPM Key Manager por clase de clave. Una clase de clave es un tipo especializado de clase de seguridad utilizado por RSA DPM Key Manager que agrupa claves criptográficas con características similares.

RSA DPM Key Manager Server permite que una clase de clave se configure para regresar a la clave actual o para generar una nueva clave en cada oportunidad. El sistema Data Domain admite solo las clases de clave configuradas para regresar a la clave actual. No use una clase de clave que esté configurada para generar una nueva clave en cada oportunidad.

Nota

Si la longitud de la clave no es de 256 bits, fallará la configuración de DPM.

Importación de certificados

Después de obtener los certificados, impórtelos al sistema Data Domain.

Antes de comenzar

- El certificado de host debe estar en formato PKCS12.
- El certificado CA debe estar en formato PEM.

- Debe obtener certificados de host y CA que sean compatibles con RSA DPM Key Manager. Puede solicitar estos certificados de autoridades de certificados de otros fabricantes o crearlos usando las herramientas apropiadas de la utilidad SSL.
- Si no se establece la frase de contraseña del sistema, no podrá importar el certificado de host. La frase de contraseña se establece cuando habilita el cifrado. Para cambiarla, consulte la sección acerca de cómo cambiar la frase de contraseña del sistema en el capítulo Administración de sistemas Data Domain.

El SO de DD admite certificados sin extensión y certificados con extensiones de servidores y clientes para el uso con DD Manager y RSA DPM Key Manager. Los certificados con extensiones de clientes son compatibles solo con RSA DPM Key Manager, y los certificados con extensiones de servidores son compatibles solo con DD System Manager.

El SO de DD no es compatible con la funcionalidad de certificados de registro automático del servidor de RSA DPM Key Manager, que carga un certificado registrado automáticamente de forma directa o importa diversos certificados. Esto significa que debe importar los certificados de host y CA para un sistema Data Domain.

La siguiente información describe cómo responder a un par de alertas que pueden aparecer durante la administración de certificados.

- Si HTTPS no logra reiniciarse debido a certificados importados dañados, se utilizan los certificados autofirmados. Si esto ocurre, se emite la alerta administrada UnusableHostCertificate. Para borrar la alerta, elimine los certificados dañados y vuelva a importar los nuevos certificados.
- Si se quitan los certificados importados, por ejemplo, durante un cambio de cabezal del sistema, y los certificados importados no logran copiarse, se emite una alerta administrada MissingHostCertificate. Vuelva a importar los certificados para borrar la alerta.

Después de obtener los certificados, impórtelos al sistema Data Domain de la siguiente manera:

Procedimiento

1. Configure RSA DPM Key Manager Server para usar los certificados de host y CA. Para obtener instrucciones, consulte la *Guía de administración de RSA DPM Key Manager Server*.
2. Para importar los certificados, redirija los archivos de certificados usando la sintaxis de comandos `ssh`. Consulte la *Guía de referencia de comandos de Data Domain Operating System* para obtener detalles.

   ssh sysadmin@<*Data-Domain-system*> adminaccess certificate import {host password *password* |ca } < *path_to_the_certificate*
   Por ejemplo, para importar el certificado de host host.p12 desde el escritorio de su computadora personal hacia el sistema Data Domain DD1 usando `ssh`, ingrese lo siguiente:

   # ssh sysadmin@DD1 adminaccess certificate import host password abc123 < C:\host.p12

3. Importe el certificado CA, por ejemplo, ca.pem, desde su escritorio a DD1 a través de SSH ingresando lo siguiente:

   # `ssh sysadmin@DD1`**adminaccess certificate import ca < C:\ca.pem**

Ejecutar esta configuración en el sistema Data Domain

Configure el cifrado en Data Domain System Manager con DPM Key Manager.

Procedimiento

1. Complete la configuración de DPM Key Manager en RSA DPM Server.
2. El sistema Data Domain debe poder resolver su propia dirección IP usando su nombre de host. Si esta asignación no se ha agregado al servidor DNS, use esta línea de comandos para agregar la entrada al archivo `/etc/hosts`:

   # `net hosts add`*ipaddrhost-list*
   donde *ipaddr* es la dirección IP del sistema Data Domain y *host-list* es el nombre de host del sistema Data Domain.

   Si está trabajando en un ambiente de pila doble, y el sistema muestra el siguiente mensaje de error: "RKM no está configurado correctamente", use el comando `net hosts add`*ipaddrhost-list* para agregar la dirección IPv4 del sistema Data Domain al archivo /etc/hosts.

   Nota

   Un servidor DPM no se puede habilitar en un ambiente que utiliza direcciones IPv6.

   Nota

   De forma predeterminada, se habilita el modo fips. Si la credencial del cliente PKCS #12 no se cifra con el algoritmo aprobado FIPS 140-2, como RC2, debe deshabilitar el modo fips. Consulte la *Guía de referencia de comandos del sistema operativo Data Domain* para obtener información acerca de cómo deshabilitar el modo fips.

3. Inicie sesión en DD System Manager y seleccione el sistema Data Domain con el que está trabajando en el panel de navegación.

   Nota

   Ejecute siempre las funciones de DD System Manager en el sistema que seleccionó en el panel de navegación.

4. Haga clic en la pestaña **Data Management** > **File System** > **Encryption**.
5. Siga las instrucciones en la sección sobre la configuración del cifrado y seleccione **DPM Key Manager**. Si el cifrado ya se ha configurado, siga las instrucciones en la sección sobre cómo cambiar administradores de claves después de la configuración.

Configuración del administrador de claves del KMIP

Con el soporte del KMIP, un dispositivo Data Domain puede recuperar objetos de clave simétricos que se utilizan para el cifrado de datos en reposo de los administradores de claves del KMIP.

Procedimiento

1. Configure una instancia de KeySecure con la dirección IP <IP1>.
2. Cree e instale un certificado de servidor SSL en KeySecure.
3. Habilite el KMIP navegando a **Device** > **Key Server**.

   Asegúrese de que <IP1> sea la dirección que se utiliza, que el puerto sea <Port1> y que se utilice el certificado de servidor del paso 2.

4. Cree una solicitud de firma de certificado (RSE) para el sistema en el sistema Data Domain/DD VE o computadora con Linux.

   a. Inicie sesión en Data Domain.

   b. Emita el comando `adminaccess certificate cert-signing-request generate`.

   Si el comando es correcto, genera el archivo `CertificateSigningRequest.csr`, que se encuentra en `/ddvar/certificates/`.

   De manera predeterminada, las exportaciones NFS no cuentan con permiso para acceder a la carpeta de certificados, incluso para un usuario raíz.

```
# mount 16tbddve:/ddvar /mnt/DDVE
# cd /mnt/DDVE/certificates/
bash: cd: /mnt/DDVE/certificates/: Permission denied
# ls -al /mnt/DDVE/
total 800292
drwxr-xr-x 25 root staff      4096 Apr 10 08:32 .
drwxr-xr-x 26 root root       4096 Oct 24 12:11 ..
-rwxr-xr-x  1 root staff       180 Apr 10 08:36 .bashrc
drwxrwsr-x  2 root staff      4096 Aug 18  2016 benchmark
drwxr-sr-x  3 root staff      4096 Apr  4 15:49 cacerts
drwxrwsr-x  2 root staff      4096 Apr  4 12:50 cdes
drwxrws---  2 root staff      4096 Apr 11  2017 certificates
drwxrwsr-x  3 root staff      4096 Jul  1  2016 core
```

5. Asegúrese de que la CA en KeySecure emita/firme la CSR.

   Si el comando es correcto, genera el archivo `CertificateSigningRequest.csr`, que se encuentra en `/ddvar/certificates/`.

6. Descargue el certificado firmado (x.509 pem file] en el sistema Data Domain y utilice la clave privada de la CSR para crear un archivo pkcs #12.

   Cambie el nombre de `csr` a `pem` en el nombre del archivo.

7. Descargar el certificado raíz de la CA de la CA de KeySecure (**Security** > **Local CAs**).
8. En el sistema Data Domain/DD VE, utilice la CLI `adminaccess` para instalar el certificado de cliente pkcs #12 y el certificado de la CA. Utilice **keysecure** como tipo de aplicación.
9. En KeySecure, cree una clave simétrica con AES-256 como el algoritmo y la longitud de la clave.

   a. Establezca el propietario del usuario que utilizará el KMIP en el sistema Data Domain/DD VE.

   b. Seleccione la opción `Exportable`.

   c. En **Security** > **Keys** > **Attributes** de la clave, asegúrese de establecer **DD_DARE_KEYS** como **Application Namespace**. Asegúrese de establecer key-class como **Application Data** que planea utilizar en el sistema Data Domain/DD VE.

10. Utilice el comando `filesys encryption key-manager set` para configurar TODOS los parámetros para acceder al administrador de claves de KeySecure.
11. Habilite el administrador de claves externo con el comando `filesys encryption key-manager enable`.

12. Habilite el cifrado usando los comandos `filesys encryption enable` y `filesys restart`.

    Esta acción reinicia el sistema de archivos.

13. Las llaves se recuperan automáticamente en el administrador de claves de KeySecure y se visualizan en la tabla claves locales.

    Ejemplo de salida de la tabla de claves locales para `filesys encryption keys show`:

```
Active Tier:

Key   Key                                                              State          Size
Id    MUID                                                                          post-comp

---   ---------------------------------------------------------------  ------------   ---------

0.1   e56                                                              Deactivated       0
0.2   953C694E2128F977FC8B18D7F8A51E44F8847A8D171D0BBDC8C01576FF5DE1D5 Activated-RW      0
---   ---------------------------------------------------------------  ------------  ---------

   * Post-comp size is based on last cleaning of Tue Feb 14 10:02:02 2017.
```

    La clave activa actual se utiliza para cifrar los datos que se recopilan.

14. Sincronice el estado de las claves.

    a. En la interfaz web de KeySecure, cree una nueva clave activa como se describió anteriormente.

    b. En la interfaz web de KeySecure, desactive la clave anterior haciendo clic en la clave y dirigiéndose a la parte inferior de la pestaña **Life Cycle**. Haga clic en **Edit State**. Establezca el **Cryptographic State** como **Deactivated**. Haga clic en **Guardar.**

15. En el sistema Data Domain, sincronice la tabla de claves locales ejecutando el comando `filesys encryption keys sync`.

    Ejemplo de salida de la tabla de claves locales para `filesys encryption keys show`:

```
Active Tier:

Key   Key                                                              State          Size
Id    MUID                                                                          post-comp

---   ---------------------------------------------------------------  ------------   ---------

0.1   e56                                                              Deactivated       0
0.2   953C694E2128F977FC8B18D7F8A51E44F8847A8D171D0BBDC8C01576FF5DE1D5 Deactivated       0
0.3   851631E574D6F02886CAEF2795896D4C401EBC57A0997EFE04A146E584E9A99A Activated-RW      0
---   ---------------------------------------------------------------  ------------  ---------

   * Post-comp size is based on last cleaning of Tue Feb 14 10:12:05 2017.
```

Nota

Las claves se pueden marcar como claves con varias versiones. Cuando se generan versiones 2 y 3 de una clave específica, las consultas del KMIP, actualmente, no recogen estas llaves y es posible que se produzca un problema si esa clave se utiliza en un sistema Data Domain o DD VE.

Cambio de administradores de claves después de la configuración

Seleccione entre Embedded Key Manager o RSA DPM Key Manager.

Antes de comenzar

Para administrar certificados para un sistema, debe iniciar DD System Manager en ese sistema.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Encryption**.
2. En Key Management, haga clic en **Configure**.
3. Escriba el nombre de usuario y la contraseña del agente de seguridad.
4. Seleccione un administrador de claves para utilizar.
   - Embedded Key Manager: Seleccione la opción de activar o desactivar la rotación de claves. Si la activa, ingrese un intervalo de rotación de entre 1 y 12 meses. Seleccione **Restart the file system now** y haga clic en **OK**.
   - RSA DPM Key Manager: Ingrese el nombre del servidor, la clase de clave, el puerto (el predeterminado es 443) y si el certificado de host importado cumple con FIPS. En modo predeterminado se encuentra activado. Seleccione **Restart the file system now** y haga clic en **OK**.
5. Haga clic en **Manage Certificates** para agregar certificados.

Administración de certificados para RSA Key Manager

Debe usar certificados de host y CA con RSA Key Manager.

Nota

Los certificados también son necesarios para RSA Key Manager. Key Manager incorporado no utiliza certificados.

Agregar certificados de CA para RSA Key Manager

Cargue o copie y pegue certificados de CA.

Procedimiento

1. Seleccione una de las siguientes opciones:
   - Seleccione la opción para cargar un certificado de CA como un archivo .pem y haga clic en **Browse** para buscar el archivo.
   - Seleccione la opción para copiar y pegar el contenido del certificado de CA en el campo proporcionado.
2. Haga clic en **Add** para agregar el certificado.

Agregar un certificado de host para RSA Key Manager

Cargue el certificado como un archivo .p12 o cargue una clave pública como un archivo .pem y utilice una clave privada generada.

Para comenzar, seleccione el primero o el segundo de los siguientes pasos:

Procedimiento

1. Seleccione la opción para cargar el certificado como un archivo .p12.
   a. Introduzca una contraseña.
   b. Haga clic en **Browse** para buscar el archivo .p12-
2. Seleccione la opción para cargar la clave pública como un archivo .pem y use la clave privada generada.

a. Haga clic en **Browse** para buscar el archivo .pem.

3. Haga clic en **Add**.

Eliminación de certificados

Seleccione un certificado con la huella digital correcta.

Procedimiento

1. Seleccione los certificados que se deben eliminar.
2. Haga clic en **Delete**.

   El sistema muestra un cuadro de diálogo Delete Certificate con la huella digital del certificado que se debe eliminar.
3. Haga clic en **OK**.

Comprobación de la configuración del cifrado de datos inactivos

Compruebe la configuración de la función DD Encryption.

Haga clic en las fichas **Data Management** > **File System** > **Encryption**. El administrador de claves que se usa actualmente se muestra como Enabled. Para obtener una descripción de la configuración de cifrado, consulte la sección acerca de la vista DD Encryption.

Activación y desactivación del cifrado de datos inactivos

Después de configurar la opción DD Encryption, el estado se habilita y el botón Disabled se activa. Cuando DD Encryption está deshabilitado, el botón Enabled se activa.

Activación del cifrado de datos inactivos

Use DD System Manager para habilitar la función DD Encryption.

Procedimiento

1. Con DD System Manager, seleccione el sistema Data Domain con el que está trabajando en el panel de navegación.
2. En la vista Encryption, haga clic en el botón **Enable**.
3. Las siguientes dos opciones están disponibles:
   - Seleccione **Apply to existing data** y haga clic en **OK**. El cifrado de datos existentes se producirá durante el primer ciclo de limpieza una vez que se reinicia el sistema.
   - Seleccione **Restart the file system now** y haga clic en **OK**. DD Encryption se habilitará después de que se reinicie el sistema de archivos.

Requistos posteriores

Nota

Pueden interrumpirse las aplicaciones mientras que el sistema de archivos se reinicia.

Cómo desactivar el cifrado de datos inactivos

Use DD System Manager para desactivar la función DD Encryption.

Procedimiento

1. Con DD System Manager, seleccione el sistema Data Domain con el que está trabajando en el panel de navegación.
2. En la vista Encryption, haga clic en el botón **Disable**.

   Se mostrará el cuadro de diálogo Disable Encryption.

3. En el área Security Officer Credentials, ingrese el nombre de usuario y la contraseña del agente de seguridad.
4. Seleccione una de las siguientes opciones:
   - Seleccione **Apply to existing data** y haga clic en **OK**. El cifrado de datos existentes se producirá durante el primer ciclo de limpieza después de reiniciar el sistema de archivos.
   - Seleccione **Restart the file system now** y haga clic en **OK**. DD Encryption se deshabilitará después de que se reinicie el sistema de archivos.

Requistos posteriores

Nota

Pueden interrumpirse las aplicaciones mientras que el sistema de archivos se reinicia.

Bloqueo y desbloqueo del sistema de archivos

Use este procedimiento cuando se esté transportando un sistema Data Domain habilitado para DD Encryption (y sus dispositivos de almacenamiento externo) o si desea bloquear un disco que se esté reemplazando. El procedimiento requiere dos cuentas: funciones de agente de seguridad y administración del sistema.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Encryption**.

   En el área File System Lock. el campo Status muestra si el estado del sistema de archivos es Locked o Unlocked.

2. Deshabilite el sistema de archivos haciendo clic en **Disabled** desde el área de estado del sistema de archivos.
3. Use el procedimiento para bloquear y desbloquear el sistema de archivos.

Bloqueo del sistema de archivos.

Para bloquear el sistema de archivos, la opción DD Encryption debe estar habilitada y el sistema de archivos debe estar deshabilitado.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Encryption** y haga clic en **Lock File System**.
2. En los campos de texto del cuadro de diálogo Lock File System, proporcione lo siguiente:

- El nombre de usuario y la contraseña de una cuenta de director de seguridad (un usuario autorizado en el grupo Security User de ese sistema Data Domain).
- La frase de contraseña actual y una nueva

3. Haga clic en **Aceptar**.

   El procedimiento vuelve a cifrar las claves de cifrado con la nueva frase de contraseña. Este proceso destruye la copia en caché de la frase de contraseña actual (en la memoria y en el disco).

Nota

Cambiar la frase de contraseña requiere la autenticación de dos usuarios para prevenir que un empleado con acceso no autorizado destruya los datos.

⚠ PRECAUCIÓN

Asegúrese de cuidar la frase de contraseña. Si la pierde, nunca podrá desbloquear el sistema de archivos ni obtener acceso a los datos. Los datos se perderán irrevocablemente.

4. Apague el sistema:

⚠ PRECAUCIÓN

No use el switch de alimentación del chasis para apagar el sistema. En lugar de ello, escriba el siguiente comando en la línea de comandos:

```
# system poweroff The 'system poweroff' command shuts down
the system and turns off the power. Continue? (yes|no|?)
[no]:
```

5. Transporte el sistema y quite el disco que se debe reemplazar.
6. Encienda el sistema y use el procedimiento para desbloquear el sistema de archivos.

Desbloqueo del sistema de archivos

Este procedimiento prepara un sistema de archivos cifrado para el uso una vez que ha llegado a su destino.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Encryption** y haga clic en **Unlock File System**.
2. En los campos de texto, proporcione la frase de contraseña que se usó para bloquear el sistema de archivos.
3. Haga clic en **Aceptar**.
4. Haga clic en **Close** para salir.

   Si la frase de contraseña es incorrecta, el sistema de archivos no se inicia y el sistema informa un error. Vuelva a ingresar la frase de contraseña correcta, como se indica en el paso anterior.

Cambio del algoritmo de cifrado

Restablezca el algoritmo de cifrado si es necesario o seleccione opciones para cifrar datos nuevos y existentes o solo datos nuevos.

Procedimiento

1. Seleccione **Data Management** > **File System** > **Encryption**
2. Para cambiar el algoritmo de cifrado utilizado para cifrar el sistema Data Domain, haga clic en **Change Algorithm**.

   Se mostrará el cuadro de diálogo Change Algorithm. Los algoritmos de cifrado compatibles son los siguientes:

   - AES-128 CBC
   - AES-256 CBC
   - AES-128 GCM
   - AES-256 GCM

3. Seleccione un algoritmo de cifrado de la lista desplegable o acepte el algoritmo AES de 256 bits (CBC) predeterminado.

   AES de 256 bits en modo Galois/Counter (GCM) es el algoritmo más seguro, pero es bastante más lento que el modo de encadenamiento de bloques de cifrado (CBC).

   Nota

   Para restablecer el algoritmo al AES de 256 bits (CBC) predeterminado, haga clic en Reset to default.

4. Determine qué datos se cifrarán:

   - Para cifrar datos nuevos y existentes, seleccione Apply to Existing data, Restart file system now **Apply to Existing data, Restart file system now** y haga clic en **OK**.
     Los datos actuales se cifrarán durante el primer ciclo de limpieza después de que se reinicie el sistema de archivos.

     Nota

     El cifrado de datos existentes puede demorar más que la operación de limpieza del sistema de archivos estándar.

   - Para cifrar solo nuevos datos, seleccione **Restart file system now** y haga clic en **OK**.

5. Se muestra el estado. Haga clic en **Close** una vez completado el proceso.

   Nota

   Pueden interrumpirse las aplicaciones mientras que el sistema de archivos se reinicia.