Sun StorEdge™ 5310 NAS: Guía de administración del dispositivo y el sistema de puerta de enlace

Sun Microsystems, Inc.
www.sun.com

Referencia 819-5231-10
Febrero de 2005, revisión A

Envíe comentarios sobre este documento a través de: http://www.sun.com/hwdocs/feedback

Para
reciclar

Adobe PostScript

Índice

Prefacio xxi

1. Introducción 1

Desplazamiento por Web Administrator 1

Uso de la interfaz gráfica de usuario 2

Ejecución del asistente de configuración 6

Variaciones en el asistente de configuración 7

▼ Para iniciar el asistente 7

Qué debe hacer a continuación 8

2. Configuración inicial de red 9

Configuración del nombre del servidor 10

▼ Para configurar el nombre del servidor 10

Configuración de las rutas LUN 10

Configuración de las rutas LUN 14

Habilitación de recuperación tras error 15

Habilitar la recuperación de unidad tras error 16

Iniciación de la recuperación 17

▼ Para iniciar la recuperación 17

Configuración de los puertos de red 18

Ubicaciones de los puertos en el dispositivo Sun StorEdge 5310 NAS 18

▼ Para configurar los adaptadores de red 19

Definición de la dirección de puerta de enlace predeterminada 20

▼ Para especificar la dirección de puerta de enlace predeterminada 21

Servicios de nombres 21

Configuración de la Seguridad de Windows 21

Configuración de WINS 23

Configuración de DNS 24

Configuración de NIS 26

Configuración de NIS+ 27

Configuración de servicios de nombres 28

Configuración de la notificación por correo electrónico 30

▼ Para configurar SMTP y enviar mensajes de correo electrónico a los destinatarios 30

Configuración del inicio de sesión 31

▼ Para configurar el inicio de sesión remoto y local 31

Asignación del idioma 32

▼ Para asignar el idioma 32

Copia de seguridad de la información de configuración 33

Qué debe hacer a continuación 33

3. Configuración y gestión del sistema de archivos 35

Conceptos del sistema de archivos 35

RAID 35

LUN 38

Partición 38

Volumen de archivo 39

Segmento 39

Creación del sistema de archivos 40

Creación de LUN y conjuntos de RAID 40

Designación como unidad de reserva de otra unidad 44

Creación de un volumen de archivo o un segmento 45

- Para crear un volumen de archivo o un segmento con el panel Create File Volume (Crear volumen de archivo) 45
- Para crear un volumen de archivo o un segmento con System Manager (Gestor de sistema) 46

Adición de segmentos a un volumen de archivo principal 47

Reconstrucción de un LUN 49

Gestión de segmentos y de volúmenes de archivo 49

Edición de las propiedades de los volúmenes de archivo 50

Eliminación de volúmenes de archivo 52

Visualización de particiones de volúmenes 52

Configuración de iSCSI 53

Configuración de un destino iSCSI 54

Configuración de acceso del iniciador iSCSI 54

- Para crear una lista de acceso de iSCSI 55
- Para crear un LUN iSCSI 56

Métodos de detección del destino SCSI 59

Configuración de un servidor iSNS 59

- Para especificar el servidor iSNS 59

Qué debe hacer a continuación 60

4. Gestión del sistema 61

Definición de la contraseña del administrador 61

- Para definir la contraseña del administrador 61

Control de la hora y la fecha 62

Sincronización de la hora 62

Configuración de la sincronización de la hora 63

Configuración de la fecha y la hora manualmente 64

Uso de software antivirus 65

▼ Para habilitar la protección antivirus 66

Exploración antivirus 68

5. Gestión de los puertos de sistema 69

Ubicaciones de los puertos 69

Acerca de las direcciones IP alias 70

Puertos enlazados 71

Enlaces de adición de puertos 71

Enlaces de alta disponibilidad 72

Puertos enlazados en un sistema de un servidor 72

Puertos enlazados en el sistema de clúster Sun StorEdge 5310 73

Ejemplo de enlaces de puertos en sistemas de dos servidores 75

6. Servicio Active Directory y autenticación 77

Servicios de nombres admitidos 77

Servicio Active Directory 78

▼ Para habilitar el servicio Active Directory 79

▼ Para comprobar el orden de búsqueda de los servicios de nombres 80

▼ Para comprobar la configuración DNS 81

▼ Para publicar recursos compartidos en ADS 81

▼ Para actualizar los contenedores de recursos compartidos de ADS 82

▼ Para eliminar recursos compartidos de ADS 83

Configuración de LDAP 83

▼ Para habilitar el servicio LDAP 83

Cambio del orden de búsqueda de los servicios de nombres 84

▼ Para establecer el orden de búsqueda del usuario, el grupo, el grupo de red y el host 84

7. Seguridad de los grupos, los hosts y los directorios de archivos 85

Grupos locales 85

Configuración de privilegios para los grupos locales 86

Configuración de hosts 89

Adición y edición de hosts 89

Asignación de las credenciales de usuario y grupo 91

Usuarios y grupos de UNIX 91

Usuarios y grupos de Windows 92

Asignación de credenciales 93

Asignación de usuarios 94

Asignación de grupos 95

Asignación de credenciales integrada 96

- Para definir una política de asignaciones 97
- Para asignar grupos y usuarios de Windows a grupos y usuarios de UNIX 98

Definición de la seguridad de los directorios de archivos 98

Definición de la seguridad de directorios de archivos en el modo de grupo de trabajo 99

Definición de la seguridad de los directorios de archivos en el modo de dominio 99

8. Recursos compartidos, cuotas y exportaciones 101

Recursos compartidos 101

Recursos compartidos estáticos 102

Configuración de recursos compartidos estáticos 102

Configuración de clientes SMB/CIFS 107

Recursos compartidos autohome 108

Gestión de cuotas 109

Configuración de las cuotas de grupos y usuarios 110

Configuración de cuotas de árbol de directorios 113

Configuración de exportaciones NFS 116

▼ Para crear las exportaciones 116

▼ Para editar exportaciones 117

Eliminación de exportaciones 118

9. Opciones del sistema 119

Activación de opciones del sistema 119

▼ Para activar una opción 120

Sun StorEdge File Replicator 121

Duplicación del dispositivo Sun StorEdge 5310 NAS 121

Pasos preliminares de la duplicación 121

Requisitos y limitaciones de File Replicator con una configuración de clúster 122

Configuración de sistemas activos y de duplicación 122

Configuración de volúmenes de archivo duplicados 123

▼ Para corregir una duplicación con daños 126

Definición de los umbrales de advertencia 127

Interrupción de la conexión entre servidores de duplicación 128

Promoción de un volumen de archivo duplicado 129

Restablecimiento de la conexión de duplicación 130

Cambio de las funciones de los volúmenes 132

Compliance Archiving Software 133

Activación de Compliance Archiving 133

Auditoría de la compatibilidad 135

Funcionales adicionales de Compliance Archiving 137

10. Supervisión del sistema 139

Supervisión del protocolo simple de administración de red (SNMP) 140

▼ Para configurar SNMP 140

Visualización del estado del sistema 141

▼ Para visualizar el estado del sistema 142

Registro del sistema 142

▼ Para ver el registro del sistema 144

Eventos de sistema 144

Auditoría del sistema 145

Configuración de auditoría 145

▼ Para configurar la auditoría del sistema 145

Archivos de registro de auditoría 146

Eventos auditados 146

Lectura de registros de auditoría 147

Estado del entorno 147

▼ Para ver el estado del ventilador 147

▼ Para ver el estado de la temperatura 148

▼ Para ver el estado de suministro eléctrico 149

▼ Para ver el estado del voltaje 150

Información de uso 151

▼ Para ver el uso de un volumen de archivo 151

▼ Para ver la actividad de red 152

▼ Para ver la actividad del sistema 152

▼ Para ver las estadísticas de red (puertos) 153

Visualización de las rutas de red 154

Acerca de las rutas 154

▼ Para ver las rutas 155

Supervisión de los componentes de sistema 155

Supervisión de UPS 156

Visualización de la información del controlador 157

Visualización del estado de duplicación 157

Visualización del estado de trabajos de copia de seguridad 159

- Para ver el registro de copia de seguridad 159
- Para ver el estado del trabajo de copia de seguridad 160
- Para ver el estado de la cinta 160

11. Mantenimiento del sistema 161

Ajuste de las opciones de acceso remoto 161

- Para definir la seguridad de acceso remoto 162

Configuración del acceso a FTP 162

- Para configurar los usuarios de FTP 163

Apagado del servidor 163

- Para apagar, detener o reiniciar el servidor 163

Puntos de control de archivo 164

Creación de puntos de control de archivo 165

Programación de puntos de control de archivo 166

Cómo compartir puntos de control de archivo 168

Acceso a los puntos de control de archivo 169

Copia de seguridad y restauración 170

Configuración de NDMP 170

Traducción de caracteres CATIA V4/V5 171

- Para habilitar CATIA desde la interfaz de línea de comandos 172
- Para habilitar CATIA automáticamente tras un reinicio 172

Limpieza de los cabezales 172

- Para ejecutar la limpieza de cabezales 172

Actualización del software del dispositivo Sun StorEdge 5310 NAS 173

▼ Para actualizar el software 173

Actualización de niveles de revisión del firmware para matriz y unidad de disco 174

Cómo determinar si se necesita la actualización del firmware 174

Actualización del firmware para matriz y unidad de disco (exige el reinicio) 175

Actualización del firmware para matriz (no exige el reinicio) 177

Actualización del firmware para unidades de disco (exige el reinicio) 181

Captura de la salida del comando `raidctl` 183

A. Administración de consola 195

Acceso al administrador de consola 196

▼ Para acceder a Telnet de Windows 196

▼ Para acceder a la interfaz de línea de comandos 196

Elementos básicos del menú de la consola 197

Directrices básicas 197

Descripciones de las teclas 197

Visualización del menú principal 198

▼ Para utilizar el menú 198

Copia de seguridad de la configuración 198

▼ Para realizar una copia de la información de configuración 199

Gestión del sistema 199

▼ Para configurar TCP/IP 199

▼ Para modificar la contraseña del administrador 200

Control de la hora y la fecha 200

Configuración de la protección antivirus 203

Selección de idioma 204

Rutas de gestión 205

▼ Para gestionar rutas estáticas en la red local 205

Servicios de nombres 205

Configuración de DNS, `syslogd` e inicio de sesión local 206

Configuración de NIS y NIS+ 208

Configuración del orden de búsqueda de los servicios de nombres 209

Gestión del sistema de archivos del servidor 210

Configurar las letras de las unidades 210

- Para crear un nuevo volumen de disco 211
- Para cambiar el nombre de una partición 212
- Para agregar un segmento de extensión 212
- Para borrar un volumen de disco 213

Gestión de recursos compartidos y cuotas 213

Configuración de los recursos compartidos SMB/CIFS 214

Configuración de los recursos compartidos autohome SMB/CIFS 214

- Para definir un recurso compartido 216
- Para editar un recurso compartido 216
- Para borrar un recurso compartido 217

Configuración del servicio Active Directory 217

Habilitación y deshabilitación de cuotas 218

Seguridad 218

Configuración de grupos de usuarios 218

Privilegios de grupo 220

Asignaciones del usuario y de grupo 220

Asignación y objetos seguros 222

Configuración de la lista de hosts 223

Gestión de hosts de confianza 224

Gestión de acceso a volúmenes 225

Bloqueo y desbloqueo de la consola 226

Duplicación de volúmenes de archivo 226
Configuración de servidores activos y de duplicación 226
Configuración de volúmenes de archivo 228
Definición de los umbrales de advertencia 230
Promoción de un volumen de archivo duplicado 230
Restablecimiento de una duplicación 231
Supervisión 234
Configuración SNMP 234
Configuración de la notificación por correo electrónico 234
Visualización de información del sistema 235
Mantenimiento del sistema 238
Configuración del acceso a FTP 239
Gestión de los controladores RAID 240
Montaje de sistemas de archivos 242
Apagado del sistema 242
Gestión de recuperación tras error 243
Configuración de rutas LUN 244
Programación de puntos de control de archivo 247
Configuración de copias de seguridad 248
Configuración de Compliance Archiving Software 248
Configuración de la auditoría del sistema 249

B. Mensajes de error del dispositivo Sun StorEdge 5310 NAS 251

Acerca de la notificación de error `SysMon` 251
Mensajes de error del dispositivo Sun StorEdge 5310 NAS 252
Errores del subsistema UPS 252
Errores del sistema de archivos 255
Errores del subsistema RAID 256
Eventos IPMI 257

C. API de Compliance Archiving Software 259

Características de cumplimiento de normativas 260

Archivos WORM 260

Periodos de retención por archivo 260

Bloqueo administrativo 261

Acceso a la función de compatibilidad 261

Volúmenes compatibles 261

Archivos WORM 261

Periodos de retención de archivos 264

Determinación del estado de un archivo 265

Comportamiento de las llamadas de sistema de UNIX 266

`access(2)` 266

`chmod(2)`, `fchmod(2)` 266

`chown(2)`, `fchown(2)` 267

`link(2)` 267

`read(2)`, `readv(2)` 267

`rename(2)` 267

`stat(2)`, `fstat(2)` 268

`unlink(2)` 268

`utime(2)`, `utimes(2)` 268

`write(2)`, `writev(2)` 268

Comportamiento de los clientes de Windows 269

Creación de archivos WORM 269

Restricciones de metadatos en archivos WORM 269

Establecimiento de periodos de retención 269

Advertencias para los clientes de Windows 270

Otras API 270

D. Componentes del dispositivo Sun StorEdge 5310 NAS 271

Suministros eléctricos del servidor 271

Botones del panel frontal del servidor 272

Indicadores LED de estado 273

Panel trasero del servidor 274

Biblioteca de cintas directamente conectada 274

Componentes del armario de controladores RAID Sun StorEdge 5300 EU y el armario de expansión Sun StorEdge 5300 EU 275

Unidades de expansión FC y SATA mixtas 276

Carcasas de disco 277

Suministros eléctricos 279

E. Envío de un correo electrónico de diagnóstico 281

Índice alfabético 283

Figuras

FIGURA 1-1 Ventana principal 2

FIGURA 1-2 Barra de herramientas 2

FIGURA 1-3 Panel de navegación 3

FIGURA 2-1 Rutas LUN mostradas en el panel Set LUN Path (Configurar ruta LUN) 11

FIGURA 2-2 Configuración de sistema de un solo servidor 12

FIGURA 2-3 Configuración de sistema de dos servidores 13

FIGURA 5-1 Enlaces de puertos en sistemas de dos servidores 75

FIGURA D-1 Suministro eléctrico 272

FIGURA D-2 Panel trasero con una tarjeta HBA 274

FIGURA D-3 Carcasa de la unidad de canal de fibra 277

FIGURA D-4 Módulos de fuente de alimentación 279

Tablas

TABLA 1-1 Iconos de la barra de herramientas 3

TABLA 1-2 Símbolos de carpeta 4

TABLA 1-3 Otros botones 5

TABLA 2-1 Columnas del panel Set LUN Path (Configurar ruta LUN) 11

TABLA 2-2 Rutas LUN en sistemas con un solo servidor 12

TABLA 2-3 Rutas LUN en sistemas con dos servidores 13

TABLA 3-1 Indicadores de estado de las unidades del cuadro de diálogo Add LUN (Agregar LUN) 43

TABLA 3-2 Imágenes de estado de las unidades en Add Hot Spare (Agregar unidad de reserva) 44

TABLA 5-1 Ejemplo de enlaces de puertos en sistemas de dos servidores 76

TABLA 7-1 Privilegios admitidos 87

TABLA 7-2 Privilegios de grupo predeterminados 87

TABLA 7-3 Campos en el SID 92

TABLA 8-1 Ejemplos de rutas de recursos compartidos 102

TABLA 8-2 Ejemplos de permisos con umask 105

TABLA 9-1 Formato del registro de auditoría 136

TABLA 10-1 Pantalla de estado del sistema 142

TABLA 10-2 Iconos de los eventos de sistema 144

TABLA 10-3 Rangos de voltaje aceptables 150

TABLA 10-4 Dispositivos de red y del sistema 152

TABLA 11-1 Tabla de traducción de caracteres CATIA 171

TABLA 11-2 Directorios y archivos de firmware de los componentes 176
TABLA 11-3 Tiempo de actualización del firmware 177
TABLA 11-4 Directorios y archivos de firmware de los componentes 178
TABLA A-1 Teclas de pantalla activa 197
TABLA B-1 Mensajes de error de UPS 252
TABLA B-2 Errores del sistema de archivos 255
TABLA B-3 Mensajes de error de RAID 256
TABLA B-4 Mensajes de error de IPMI 257
TABLA C-1 Metadatos del archivo WORM que se pueden o no se pueden modificar 263
TABLA D-1 Indicadores LED de estado 273

Prefacio

La publicación *Sun StorEdge 5310 NAS: Guía de administración del dispositivo y el sistema de puerta de enlace* es una guía combinada para el administrador y el usuario del dispositivo Sun StorEdge™ 5310 NAS, el clúster Sun StorEdge™ 5310 y el sistema de puerta de enlace Sun StorEdge™ 5310 NAS. En esta guía se describe cómo utilizar el software Web Administrator para configurar y supervisar el sistema. También contiene instrucciones sobre el empleo de la interfaz de línea de comandos (CLI) y otros detalles sobre el hardware del sistema que no se incluyen en el documento *Sun StorEdge 5310 NAS: Guía básica del dispositivo y el sistema de puerta de enlace*.

Antes de leer esta guía

Antes de leer esta guía, el sistema debe estar instalado y configurado como se describe en *Sun StorEdge 5310 NAS: Guía básica del dispositivo y el sistema de puerta de enlace*.

Organización de esta guía

Esta guía contiene las instrucciones para administrar y utilizar el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310.

En el Capítulo 1 se proporciona una descripción general de las características del software Web Administrator.

En el Capítulo 2 se explica la configuración básica de la red y el sistema de archivos.

En el Capítulo 3 se describe la configuración del sistema de conjuntos redundantes de discos independientes (RAID).

En el Capítulo 4 se explican las funciones de gestión.

En el Capítulo 5 se describe la configuración de puertos.

En el Capítulo 6 se explican las convenciones de nomenclatura.

En el Capítulo 7 se describe cómo configurar las funciones de seguridad.

En el Capítulo 8 se explican los recursos compartidos, cuotas y exportaciones.

En el Capítulo 9 se explican las opciones del software sujeto a licencia.

En el Capítulo 10 se describen las funciones de supervisión.

En el Capítulo 11 se describen las funciones de mantenimiento.

En el Apéndice A se incluyen instrucciones sobre el uso de la consola para realizar operaciones del sistema.

En el Apéndice B se describen los mensajes de error que pueden aparecer.

En el Apéndice C se proporciona información sobre el API de Compliance Archiving Software.

En el Apéndice D se incluyen los detalles sobre el hardware del sistema.

En el Apéndice E se describe el envío de correos electrónicos de diagnóstico.

Convenciones tipográficas

Tipo de letra*	Significado	Ejemplos
`AaBbCc123`	Corresponde a nombres de comandos, archivos y directorios; se muestran en la-pantalla del equipo	Edite su archivo `.login`. Utilice `ls -a` para tener una lista de todos los archivos. `% You have mail.`
`AaBbCc123`	Lo que escribe el usuario, a diferencia de lo que aparece en pantalla	`% su` `Password:`
AaBbCc123	Corresponde a títulos de libros, nuevas palabras o términos y palabras que es necesario resaltar. Cambie las variables de línea de comandos por nombres reales o valores.	Consulte el capítulo 6 del *Manual del usuario*. Se conocen como opciones de *clase*. Para efectuar esta operación, *debe* estar conectado como superusuario. Para eliminar un archivo, escriba `rm` *nombre de archivo*.

* Los valores de configuración del explorador pueden no coincidir con este formato.

Documentación relacionada

Los documentos en línea se encuentran disponibles en:

http://www.sun.com/hwdocs/Network_Storage_Solutions/nas

Aplicación	Título	Número de publicación	Formato	Lugar
Instalación	*Notas de la versión del dispositivo y sistema de puerta de enlace Sun StorEdge 5210 y 5310 NAS*	819-3094-*nn*	PDF	En línea
Instalación	*dispositivo Sun StorEdge 5310 NAS Guía básica del dispositivo y el sistema de puerta de enlace*	819-5226-*nn*	PDF HTML	En línea En línea
Instalación del dispositivo NAS (no puerta de enlace)	*Instalación de Sun StorEdge 5310 NAS*	819-1168-*nn*	Impreso PDF	Paquete de envío En línea
Puerta de enlace	*Folleto del sistema de puerta de enlace Sun StorEdge 5310 NAS*	819-5258-*nn*	Impreso PDF	Paquete de envío En línea

Documentación, soporte, cursos de formación

URL	Descripción
http://www.sun.com/documentation/	Descargue los documentos PDF y HTML, o solicite publicaciones impresas.
http://www.sun.com/support/	Obtenga asistencia técnica y descargue parches.
http://www.sun.com/training/	Aprenda sobre los cursos de Sun.

Sitios Web de terceros

Sun no se hace responsable de la disponibilidad de los sitios Web de terceros que se mencionan en este documento. Sun no aprueba ni se hace responsable del contenido, publicidad, productos u otros materiales disponibles en dichos sitios o recursos, o a través de ellos. Sun no será responsable de daños o pérdidas, supuestos o reales, provocados por o a través del uso o confianza del contenido, bienes o servicios disponibles en dichos sitios o recursos, o a través de ellos.

Sun agradece sus comentarios

Deseamos mejorar nuestra documentación y agradecemos sus comentarios y sugerencias. Para enviar comentarios, visite la dirección:

http://www.sun.com/hwdocs/feedback

Los comentarios deben incluir el título y el número de referencia del documento:

Sun StorEdge 5310 NAS: Guía de administración del dispositivo y el sistema de puerta de enlace, número de referencia 819-5231-10.

CAPÍTULO 1

Introducción

La interfaz gráfica de usuario (GUI) de Web Administrator para el dispositivo Sun StorEdge 5310 NAS facilita las configuraciones de seguridad y de red, así como las tareas administrativas en los innovadores sistemas de dispositivo Sun StorEdge 5310 NAS de Sun Microsystems.

Nota – Las funciones y características del software que se describen en este manual se aplican a todas las configuraciones del dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310, para cuyo caso se ha empleado, en general, el término “sistema”. Cuando alguna característica o función está limitada sólo a una de las configuraciones, se especifica el nombre de dicha configuración.

Desplazamiento por Web Administrator

La interfaz gráfica de usuario (GUI) de Web Administrator le permite ajustar los parámetros del sistema mediante una serie de menús, paneles o pantallas con fichas, que se describen en los próximos capítulos.

Uso de la interfaz gráfica de usuario

La ventana principal de Web Administrator le permite desplazarse por los servicios y eventos del sistema, así como verlos y configurarlos. El aspecto de esta ventana varía en función de la configuración del hardware.

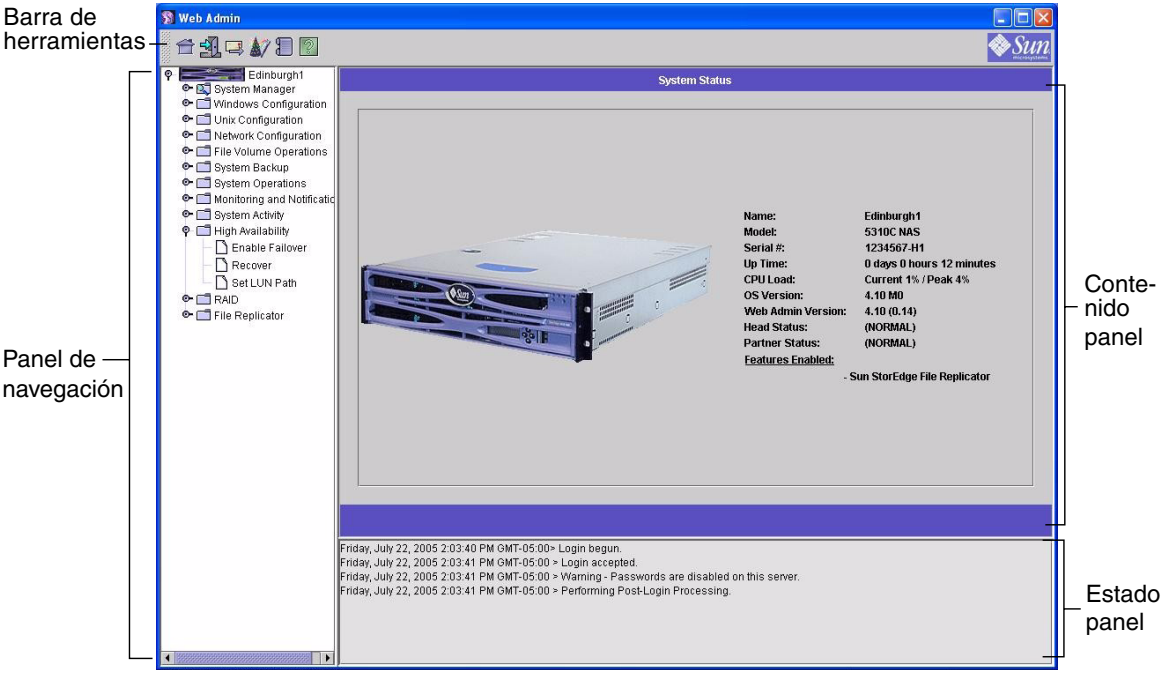


FIGURA 1-1 Ventana principal

Barra de herramientas

La barra de herramientas está situada en la parte superior de la ventana de Web Administrator y permite acceder a la pantalla de estado de inicio, cerrar la sesión, enviar correos electrónicos de diagnóstico, ejecutar el asistente de configuración y acceder a las páginas de ayuda.

FIGURA 1-2 Barra de herramientas

Los iconos de la barra de herramientas se muestran en la TABLA 1-1.

TABLA 1-1 Iconos de la barra de herramientas

Botón	Nombre	Acción
	Inicio	Ver la pantalla de estado de inicio del sistema
	Cerrar sesión	Cerrar la sesión
	Correo electrónico	Enviar de un correo electrónico de diagnóstico
	Asistente	Ejecutar el asistente de configuración
	Registro del sistema	Acceder al registro del sistema
	Ayuda	Acceder a la ayuda

Panel de navegación

Utilice este panel para desplazarse por Web Administrator. Desde aquí puede acceder a todas las funciones administrativas, a los ajustes y a las configuraciones.

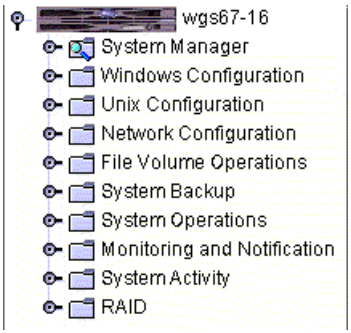
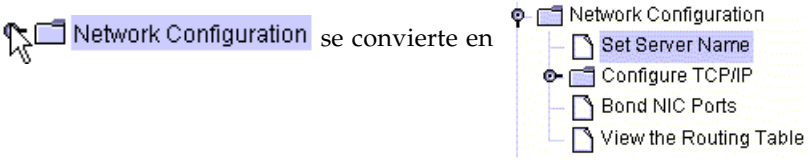


FIGURA 1-3 Panel de navegación

Para abrir una carpeta, haga clic en el símbolo que está junto a la carpeta, o doble clic en la carpeta. Este símbolo cambiará a . Por ejemplo:



Para cerrar la carpeta, haga clic en para que vuelva a la posición .

Símbolos de carpeta

Las carpetas en Web Administrator están representadas con símbolos.

Los símbolos de carpetas se muestran en la TABLA 1-2.

TABLA 1-2 Símbolos de carpeta

Símbolo	Representación
	Volumen de archivo
	Volumen de archivo compatible (con ficha de carpeta roja)
	Volumen de archivo compartido
	Volumen de archivo exportado
	Volumen de archivo compartido y exportado
	Volumen de archivo duplicado
	Duplicación compatible
	Segmento

Otros botones

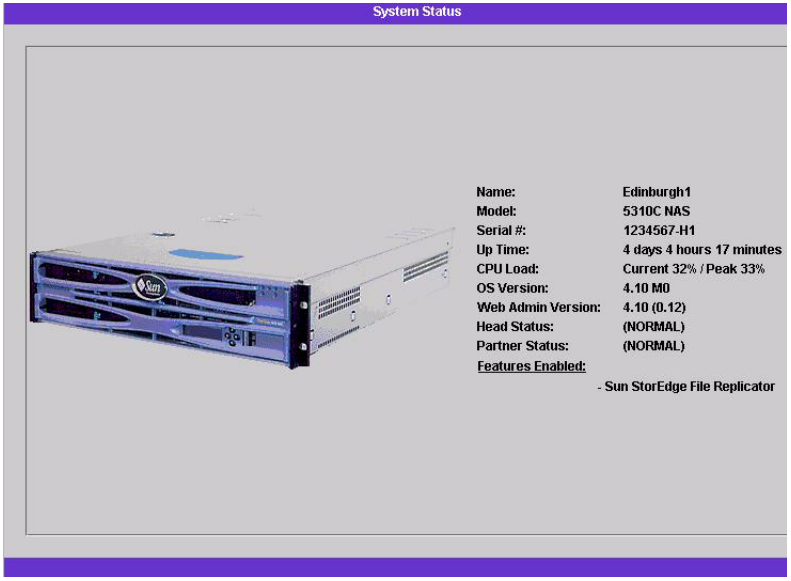
Determinadas pantallas de Web Administrator contienen otros botones. Estos botones adicionales se muestran en la TABLA 1-3.

TABLA 1-3 Otros botones

Botón	Nombre	Acción
	Adición	Añadir elementos
	Arriba	Mover hacia arriba el elemento seleccionado
	Abajo	Mover hacia abajo el elemento seleccionado
	Papelera	Eliminar el elemento seleccionado
	Edición	Editar el elemento seleccionado

Panel de contenido

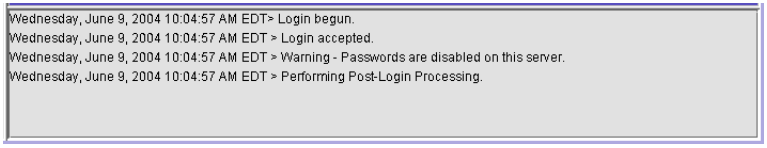
Este panel contiene la información general del sistema.



Para obtener más información acerca del estado del sistema, consulte "Visualización del estado del sistema" en la página 141.

Panel de estado

En la parte inferior de la ventana de Web Administrator, el panel de estado muestra todos los eventos que se han producido desde el último inicio de sesión. Utilice este panel para comprobar que se han guardado los cambios o que los comandos de sistema se han ejecutado correctamente. Los errores y las advertencias se muestran también en este panel.



Nota – El panel de estado muestra la fecha y hora del equipo cliente en que se ejecuta el software Web Administrator, pero no la fecha y hora del sistema.

Uso de la ayuda

Hay pantallas de ayuda disponibles en todas las fichas de Web Administrator para proporcionarle información detallada acerca de los términos, los campos, las casillas de verificación, los botones de opción (botones de radio) y los botones de acción de la pantalla en cuestión.

Para acceder a la pantalla de ayuda de cualquier tema de Web Administrator, deberá hacer clic en el botón Help (Ayuda) situado en la barra de herramientas. La ventana de ayuda correspondiente al panel de contenido que se esté mostrando actualmente aparecerá junto a la pantalla de Web Administrator.

Ejecución del asistente de configuración

El asistente de configuración se ejecuta automáticamente la primera vez que inicia la sesión. El asistente está diseñado para orientarle durante la configuración inicial del sistema. Le ayuda a llevar a cabo los pasos necesarios para establecer una comunicación entre el sistema y la red. Cuando finalice el asistente, tendrá que configurar el sistema de archivos y el acceso de los usuarios.

Variaciones en el asistente de configuración

El asistente de configuración ofrece varias opciones. Algunas de ellas están determinadas automáticamente por el propio sistema. Otras, sin embargo, las determina el usuario, según el entorno de red de que disponga. Esta guía no puede abarcar todas las configuraciones posibles en el espacio disponible. Esta sección proporciona una descripción general del asistente de configuración y describe las rutas posibles que puede tomar en el asistente.

Otras funciones también dependen de las características del sistema. Dichas variaciones se tratan en las secciones correspondientes de esta guía.

Hay tres rutas principales que se pueden tomar con el asistente. Las tres rutas dependen del entorno de red que se use y deberá elegir la opción que proceda. Las tres rutas son:

- **Sólo para UNIX**. Esta ruta le ayuda a configurar el sistema para que funcione en una red que sea totalmente de UNIX®. Omite todas las funciones propias de los entornos Windows.
- **Sólo para Windows**. Esta ruta le ayuda a configurar el sistema para que funcione en una red que sea totalmente de Windows. Omite todas las funciones propias de los entornos UNIX.
- **Para UNIX y Windows**. Esta ruta combina funciones que ayudan a configurar el sistema en entornos de red mixtos que cuentan con funciones propias de Windows y de UNIX.

Seleccione la ruta adecuada según su entorno de red.

▼ Para iniciar el asistente

1. **Para ejecutar el asistente de configuración, haga clic en el botón Wizard (Asistente) de la barra de herramientas.**

   El asistente muestra una página de introducción.

2. **Haga clic en Next (Siguiente) para continuar.**

   El asistente le guiará por los siguientes pasos, que se describen detalladamente en el Capítulo 2, *Configuración inicial de red*:

   1. Definición del nombre del servidor y de la información de contacto
   2. Configuración de los adaptadores de red
   3. Definición de la puerta de enlace predeterminada
   4. Configuración de dominios y grupos de trabajo (en entornos de Windows y entornos mixtos) y habilitación y configuración de ADS (Servicio Active Directory) (en entornos de Windows y entornos mixtos)
   5. Configuración WINS (en entornos de Windows y entornos mixtos)

6. Configuración de DNS

Nota – Si el sistema se inició utilizando DHCP, confirme que la dirección del servidor DNS sea correcta. En caso contrario, desactive la casilla de verificación Configure DNS (Configurar DNS) para evitar retrasos en los reinicios y recuperaciones tras errores.

---

7. Definición de los ajustes de los servicios de información de red (NIS, del inglés Network Information Service) (en entornos UNIX y entornos mixtos)
8. Definición de los ajustes del servicio de información de red Plus (NIS+, del inglés Network Information Service Plus) (en entornos UNIX y entornos mixtos)
9. Configuración de servicios de nombres (en entornos de UNIX y entornos mixtos)
10. Configuración de la notificación por correo electrónico
11. Definición del inicio de sesión remoto y local
12. Asignación del idioma

3. **Confirmación de las preferencias**

   El asistente guarda entonces las preferencias indicadas y comunica si se produce algún fallo en los cambios de configuración.

   Si no desea ejecutar el asistente, en Capítulo 2, *Configuración inicial de red* se describe el acceso a las mismas funciones en la misma secuencia pero desde el panel de navegación.

Qué debe hacer a continuación

En este momento, el sistema debe estar en ejecución y es necesario que el usuario tenga unas nociones básicas sobre el uso de Web Administrator. Ahora, debe establecer el sistema de archivos y configurar el acceso de los usuarios.

La configuración del sistema de archivos incluye la creación de los siguientes elementos (si procede): LUN, particiones, volúmenes de archivo y segmentos. Consulte "Conceptos del sistema de archivos" en la página 35 para obtener más información acerca de estos conceptos.

Cuando el sistema de archivos esté finalizado, deberá definir derechos de acceso para los usuarios y otras funciones de gestión de sistemas. En el Capítulo 4, *Gestión del sistema*, se describen las funciones de gestión básicas. Consulte en el índice las funciones específicas, entre las que se incluyen las descripciones de las funciones, la forma en que operan, cuándo y cómo se aplican y las reglas específicas para configurarlas.

CAPÍTULO 2

Configuración inicial de red

Este capítulo describe cómo se configura el sistema para que pueda conectarse a la red. Después de configurar servicios y comunicaciones de red, deberá configurar el sistema de archivos, definir los derechos de acceso de los usuarios y otras opciones, así como cualquier otra función que haya adquirido.

Este capítulo sigue la misma secuencia que el asistente de configuración. Es posible que no se traten aquí todas las funciones que necesite configurar. Si desea configurar una función específica que no se trate en este capítulo, consulte el índice para buscar instrucciones.

Se incluyen las secciones:

- "Configuración del nombre del servidor" en la página 10
- "Configuración de las rutas LUN" en la página 10
- "Habilitación de recuperación tras error" en la página 15
- "Iniciación de la recuperación" en la página 17
- "Configuración de los puertos de red" en la página 18
- "Definición de la dirección de puerta de enlace predeterminada" en la página 20
- "Servicios de nombres" en la página 21
- "Configuración de la notificación por correo electrónico" en la página 30
- "Configuración del inicio de sesión" en la página 31
- "Asignación del idioma" en la página 32
- "Copia de seguridad de la información de configuración" en la página 33
- "Qué debe hacer a continuación" en la página 33

Configuración del nombre del servidor

Es necesario que configure un nombre de servidor para identificar el servidor de la red.

▼ Para configurar el nombre del servidor

1. **En el panel de navegación, seleccione Network Configuration (Configuración de red) > Set Server Name (Definir nombre del servidor).**
2. **Escriba el nombre de servidor en el cuadro Server Name (Nombre del servidor).**

   Este nombre identifica el sistema, o esta unidad de servidor, en el caso de sistemas con dos servidores de alta disponibilidad (HA) en la red. Dicho nombre sólo puede incluir letras y números (a-z, A-Z, 0-9), "-" (guiones), "_" (guiones bajos) y "." (puntos).

   Nota – El nombre del servidor debe comenzar por una letra (a–z o A–Z), no por un número ni un símbolo. Por ejemplo, "Astro2" y "Saturno_05" son nombres de servidor aceptables, mientras que "5Saturno" y "_Astro2" no lo son.

   ---

3. **Especifique la información de contacto de su empresa, incluidos el nombre de la empresa y los datos de contacto del administrador del dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 o el sistema de puerta de enlace Sun StorEdge 5310.**

   El sistema incluye esta información en los mensajes de correo electrónico de diagnóstico que se envíen. Para obtener más información acerca de los mensajes de correo electrónico de diagnóstico, consulte Apéndice E.
4. **Para guardar las preferencias, haga clic en Apply (Aplicar).**

Configuración de las rutas LUN

Una ruta de número de unidad lógica (LUN) es una designación que describe los servidores y controladores que acceden a un volumen de archivo en un LUN. En cada volumen de archivo existen dos rutas LUN: la ruta principal y una ruta alternativa. Si una ruta falla, el sistema utiliza automáticamente la otra ruta LUN disponible para acceder al volumen de archivo correspondiente. El número de rutas LUN y sus implementaciones dependen del modelo y configuración del sistema.

En un sistema de clúster Sun StorEdge 5310, un servidor (unidad) produce una recuperación tras error de la unidad (consulte “Habilitar la recuperación de unidad tras error” en la página 16) cuando las rutas principal y alternativa fallan.

Las rutas LUN se pueden ver y editar (consulte “Configuración de las rutas LUN” en la página 14) en el panel Set LUN Path (Configurar ruta LUN).

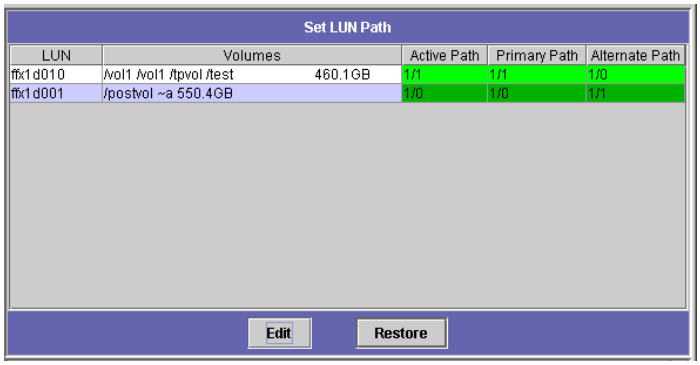


FIGURA 2-1 Rutas LUN mostradas en el panel Set LUN Path (Configurar ruta LUN)

Las columnas están explicadas en la siguiente tabla.

TABLA 2-1 Columnas del panel Set LUN Path (Configurar ruta LUN)

Columna	Contenido
LUN	Los LUN que están disponibles en el sistema.
Volumes (Volúmenes)	Nombres de los volúmenes de archivo: puede haber más de un volumen de archivo en un LUN.
Active Path (Ruta activa)	La ruta LUN activa. “1/1” designa el controlador 1 y su estado activo. Otras designaciones son las siguientes: El primer número designa el número HBA (empezando por 1) El segundo número designa el número de destino del controlador SCSI Por ejemplo, 1/1 designa HBA 1 y destino de controlador SCSI 1.
Primary Path (Ruta principal)	Las rutas LUN principales, las rutas que el sistema selecciona al iniciarse. También son las rutas en las que una ruta LUN se puede “restaurar”. Si la ruta principal no se especifica, el sistema utilizará la primera ruta disponible.
Alternate Path (Ruta alternativa)	Las rutas que se utilizan cuando fallan las rutas principales.

Rutas LUN en sistemas con un solo servidor

A continuación se ilustra una configuración de hardware típica del sistema de un servidor.

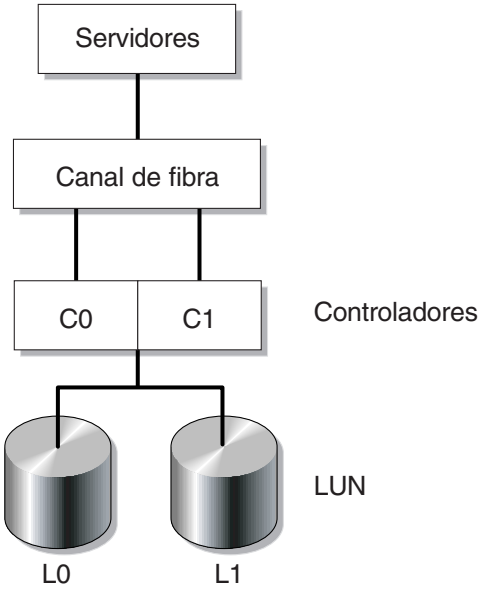


FIGURA 2-2 Configuración de sistema de un solo servidor

La ruta LUN principal a un volumen de archivo en LUN0 es C0-L0; la ruta alternativa es C1-L0. La ruta principal LUN a un volumen de archivo en LUN1 es C1-L1 y la ruta alternativa es C0-L1. Como se muestra, el sistema debe tener las siguientes rutas LUN.

TABLA 2-2 Rutas LUN en sistemas con un solo servidor

Rutas	LUN0	LUN1
Principal	C0-L0	C1-L1
Alternativa	C1-L0	C0-L1

Se puede acceder a cada LUN mediante el controlador 0 (C0) o el controlador 1 (C1).

Rutas LUN en sistemas con dos servidores

A continuación se muestra una configuración de hardware típica en un sistema de clúster Sun StorEdge 5310:

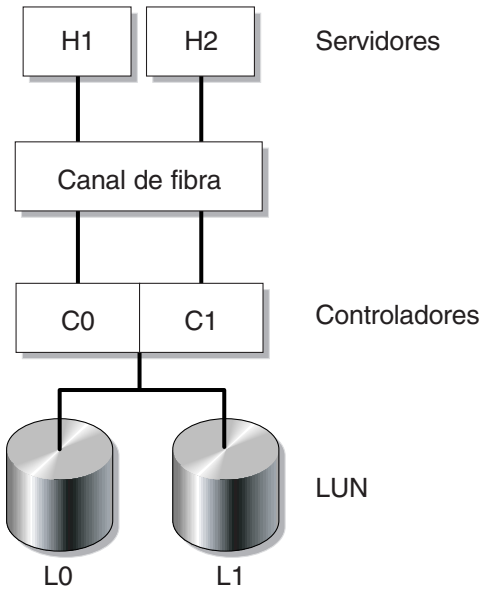


FIGURA 2-3 Configuración de sistema de dos servidores

La ruta LUN principal de la unidad 1 es C0-L0; la ruta alternativa es C0-L1. La ruta LUN principal de la unidad 2 es C1-L0 y la ruta alternativa es C1-L1. Como se muestra, el sistema debe tener las siguientes rutas LUN:

TABLA 2-3 Rutas LUN en sistemas con dos servidores

Unidad 1	**LUN**	**LUN0**	**LUN1**
	Rutas	C0-L0	C0-L1
Unidad 2	**LUN**	**LUN0**	**LUN1**
	Rutas	C1-L0	C1-L1

El acceso a los volúmenes de archivo se realiza habitualmente a través de la ruta LUN principal designada para el LUN al que pertenecen los volúmenes de archivo. En una configuración de clúster, una unidad produce una recuperación tras error en caso de que las rutas principal y alternativa fallen (consulte "Habilitar la recuperación de unidad tras error" en la página 16).

Configuración de las rutas LUN

Con la configuración de una ruta LUN, se designa la ruta LUN actualmente activa. La ruta LUN actualmente activa puede ser la ruta principal o alternativa. Para obtener un rendimiento óptimo, configure la ruta activa como ruta principal. Sólo se puede reasignar un LUN si no dispone de sistemas de archivos. En un sistema de clúster Sun StorEdge 5310, sólo el servidor "propietario" de un LUN podrá reasignarlo a otro servidor.

Nota – En un sistema de clúster Sun StorEdge 5310, cuando arranca el sistema por primera vez, todos los LUN se asignan a un servidor (H1). Utilice el servidor H1 para reasignar algunos LUN al servidor H2 y obtener una distribución homogénea.

Utilice el panel de configuración de la ruta LUN para configurar las rutas activas. En un sistema de clúster Sun StorEdge 5310, puede configurar una ruta no asignada desde cualquier servidor.

▼ Para configurar una ruta LUN

1. **En el panel de navegación, seleccione High Availability (Alta disponibilidad) > Set LUN Path (Configurar ruta LUN).**

   Nota – Los LUN que no tienen una ruta LUN asignada aparecerán inicialmente varias veces en el panel Set LUN Path ya que su presencia se señala mediante varios controladores en varias rutas. Cuando un LUN tiene una ruta asignada, se muestra una vez, en la ruta actual.

   ---

2. **Seleccione un LUN y haga clic en Edit (Editar).**
3. **Seleccione el controlador que desee en el menú desplegable Primary Path (Ruta principal).**

   Ejemplo: La opción desplegable "1/0" asigna el LUN seleccionado al controlador 0 (C0). El valor de la opción es "X/Y": el valor "X" puede ser 0 ó 1. El valor 1 indica que el controlador está activo; 0, que está inactivo.

   Divida homogéneamente los LUN entre las dos rutas disponibles. Por ejemplo, el primer y tercer LUN en 1/0 y el segundo y cuarto LUN en 1/1.

4. **Haga clic en Apply (Aplicar).**

▼ Para restaurar una ruta LUN

Una ruta activa de LUN puede ser distinta a la ruta principal. La opción “Restore” (Restaurar) en el panel Set LUN (Configurar LUN) permite restaurar una ruta activa de LUN a su ruta principal.

Nota – El restablecimiento de una ruta LUN no recupera ningún dato, no es una función de recuperación tras desastre.

---

1. **En el panel de navegación, seleccione High Availability (Alta disponibilidad) > Set LUN Path (Configurar ruta LUN).**
2. **Seleccione un LUN y haga clic en Restore (Restaurar).**

Habilitación de recuperación tras error

Nota – La habilitación de recuperación tras error sólo es aplicable a los sistemas de clúster Sun StorEdge 5310.

Un sistema de clúster Sun StorEdge 5310 consta de un par de servidores activo-activo, denominados “unidades,” que comparten el acceso a los controladores RAID y a varias redes distintas. Los controladores RAID están conectados a cada servidor mediante controladores de fibra. Un cable de conexión privada conecta el primer NIC de los dos servidores y permite que supervisen mutuamente su estado.

En situaciones normales, cada servidor funciona de manera independientemente con responsabilidad sobre un subconjunto de LUN. Si en un servidor ocurre un fallo de hardware que hace que una ruta de datos no esté disponible, el servidor que esté funcionando se convierte en propietario de las direcciones IP y los LUN que gestionaba anteriormente el servidor con fallo. Todas las operaciones del servidor que ha fallado, incluyendo la asignación de direcciones de la interfaz de red y la propiedad de volumen RAID, se transfieren al servidor en funcionamiento. Esto se conoce como “recuperación tras error de la unidad”.

Tras una recuperación tras error de clúster, las operaciones de clientes que utilicen NFS/UDP se transfieren inmediatamente, mientras que NFS/TCP requiere que se vuelva a realizar la conexión, de forma transparente en el contexto de un reintento NFS. CIFS también requiere que se vuelva a realizar la conexión, aunque es posible que distintas aplicaciones lo hagan de forma transparente, lo notifiquen al usuario o requieran su confirmación antes de proceder.

El proceso de recuperación, conocido como “recuperación tras fallo”, se puede iniciar una vez que se haya reparado la unidad defectuosa y esté de nuevo conectada. Con el panel Recover (Recuperar), accesible desde High Availability (Alta disponibilidad) > Recover, determine los LUN gestionados por cada unidad.

Habilitar la recuperación de unidad tras error

En el caso de un fallo de unidad, la recuperación tras error produce que la unidad que esté funcionando se encargue temporalmente de las direcciones IP y los LUN que gestionaba la unidad averiada.

Nota – Cuando habilita la recuperación tras error de unidad, DHCP se deshabilita automáticamente.

▼ Para habilitar la recuperación de unidad tras error

1. **En el panel de navegación, seleccione High Availability (Alta disponibilidad) > Enable Failover (Habilitar recuperación tras error).**
2. **Haga clic en la casilla de verificación Automatic Failover (Recuperación automática tras error).**
3. **Seleccione la casilla Enable Link Failover (Habilitar recuperación tras error de enlace).**

   Al habilitar la recuperación de enlaces tras error se asegura la recuperación de unidad tras error cuando falla una interfaz de red que tiene asignada la función "principal". Este tipo de fallo se suele nombrar como un estado de "enlace inactivo". Si el enlace de red del socio está inactivo, la unidad que desea realizar la recuperación tras error deberá esperar el tiempo especificado después de que la unidad asociada restablezca su enlace de red.

4. **Escriba lo siguiente:**
   - Down Timeout (Tiempo de espera de inactividad): es el número de segundos de espera cuando el enlace de red en una unidad no es fiable y en su unidad asociada está en correcto estado, antes de proceder a una recuperación de unidad tras error.
   - Restore Timeout (Tiempo de espera de restablecimiento): es el número de segundos que debe estar activo el enlace principal de la unidad asociada para que se efectúe la recuperación tras error. Este tiempo se utiliza cuando se inicia una recuperación tras error debido a un enlace inactivo que se cancela debido a que el enlace principal de la unidad asociada estaba inactivo.
5. **Para guardar las preferencias, haga clic en Apply (Aplicar).**
6. **Reiniciar las dos unidades.**

Iniciación de la recuperación

La recuperación del controlador tras error se produce automáticamente cuando un controlador RAID tiene un fallo. El controlador que esté funcionando administrará temporalmente los LUN que gestionaba el controlador averiado.

Nota – La recuperación de controlador tras error está habilitada de forma predeterminada y no se puede desactivar.

Una vez que la unidad o el controlador RAID defectuoso se vuelve a conectar, es necesario iniciar manualmente la recuperación tras fallo del dispositivo Sun StorEdge 5310 NAS o el sistema de clúster Sun StorEdge 5310 después de terminar la recuperación de la unidad o el controlador.

Un servidor que haya fallado y provocado la recuperación tras error, puede "recuperar" la propiedad de los volúmenes de archivo originales una vez que esté totalmente operativo.

Por ejemplo, se asignó el volumen A al servidor H1 que falló, de modo que el servidor H2 se hizo propietario del volumen A durante la recuperación tras error. Ahora que el servidor H1 está operativo, puede recuperar su propiedad del volumen A del servidor H2.

Precaución – Asegúrese de que el servidor que falló se encuentra totalmente operativo antes de intentar la recuperación.

▼ Para iniciar la recuperación

1. **En el panel de navegación, seleccione High Availability (Alta disponibilidad) > Recover (Recuperar) para acceder al panel Recover.**
2. **Para la recuperación de unidades, seleccione el equipo RAID que esté recuperando en la lista RAID.**
   - La lista Head 1 identifica la asignación de LUN del servidor H1.
   - La lista Head 2 (unidad asociada) identifica la asignación de LUN del servidor asociado H2.
3. **Para la recuperación de controladores, en la lista RAID seleccione el equipo RAID que esté recuperando.**
   - La lista Controller 0 identifica la asignación de LUN del controlador 0.
   - La lista Controller 1 (asociado) identifica la asignación de LUN del controlador 1.

4. **Haga clic en Recover (Recuperar).**

   El servidor redistribuye la asignación de LUN para reflejar la configuración que se muestra en pantalla.

Configuración de los puertos de red

Puede optar por habilitar DHCP o por especificar la dirección IP, la máscara de red, la difusión y la función de los puertos de tarjeta de interfaz de red (NIC, del inglés Network Interface Card) para cada puerto de red mediante el panel Configure Network Adapters (Configurar adaptadores de red). También puede agregar direcciones IP alias para cada puerto NIC.

Nota – Cada puerto NIC del clúster Sun StorEdge 5310 debe tener una función asignada.

Puede enlazar dos o más puertos para crear un puerto enlazado. Un puerto de este tipo tiene un ancho de banda superior al de los puertos que lo componen. En "Puertos enlazados" en la página 71 encontrará más información y más instrucciones acerca de los puertos de red enlazados.

Ubicaciones de los puertos en el dispositivo Sun StorEdge 5310 NAS

El dispositivo Sun StorEdge 5310 NAS identifica los puertos siguiendo un orden predefinido que se basa en el tipo de puerto y en su ubicación física y lógica en el servidor. Consulte la *Guía básica del dispositivo Sun StorEdge 5310 NAS y el sistema de puerta de enlace* para identificar donde se ubican los puertos de red de su configuración. Tenga en cuenta que las configuraciones de sistema pueden ser distintas y aquí sólo se muestran ejemplos.

La relación existente entre las tarjetas de interfaz de red (NIC) y los puertos se ilustra en la *Guía básica del dispositivo Sun StorEdge 5310 NAS y el sistema de puerta de enlace*.

▼ Para configurar los adaptadores de red

1. **En el panel de navegación, seleccione Network Configuration (Configuración de red) > Configure TCP/IP (Configurar TCP/IP) > Configure Network Adapters (Configurar adaptadores de red).**

2. **Si la red utiliza un servidor DHCP para asignar direcciones IP y desea habilitarlo, seleccione la casilla de verificación Enable DHCP (Habilitar DHCP).**

   Al habilitar DHCP, el sistema puede obtener dinámicamente una dirección IP procedente del servidor DHCP. Desactive esta casilla de verificación para introducir manualmente una dirección IP y una máscara de red. Si no habilita DHCP y el puerto forma parte de un puerto agregado, la máscara de red seguirá deshabilitada. Consulte "Puertos enlazados" en la página 71 para obtener información acerca de la creación y configuración de puertos agregados.

   Nota – En los sistemas de clúster Sun StorEdge 5310, no puede habilitar un servidor DHCP salvo que se produzca un fallo de unidad desactivada. En su lugar, deberá asignar direcciones IP estáticas a los puertos, de forma que permanezcan coherentes en caso de una recuperación tras error.

   ---

3. **En la lista Adapter (Adaptador), seleccione el puerto que desee configurar.**

   Si ya ha creado un puerto enlazado y desea agregarle direcciones IP alias, deberá seleccionar el puerto enlazado en esta lista. (Consulte "Puertos enlazados" en la página 71 para obtener más información acerca de la creación de puertos enlazados.) Los puertos independientes tienen la etiqueta PORT*x* y los puertos enlazados, BOND*x*.

   Una vez que se crea un puerto enlazado, no se pueden agregar direcciones IP alias a los puertos individuales: sólo se podrán agregar al puerto enlazado.

4. **Especifique la dirección IP para el puerto individual seleccionado o para el puerto enlazado.**

5. **Especifique la máscara de red para el puerto individual seleccionado o para el puerto enlazado.**

   La máscara de red indica qué parte de una dirección IP identifica la dirección de red y qué parte identifica la dirección de host.

   El campo de sólo lectura **Broadcast** (Difusión) se cumplimenta automáticamente al especificar la dirección IP y la máscara de red. La dirección de difusión es la dirección IP que se usa para enviar mensajes de difusión a la subred.

6. **Seleccione una de las siguientes funciones para cada puerto.**

Funciones	Descripción
Principal	La función de puerto Primary (Principal) identifica el puerto de red activo.
Independiente	La función de puerto Independent (Independiente) identifica un puerto de red activo que se utiliza para otros propósitos distintos que proporcionar datos; por ejemplo, para copias de seguridad.
Duplicación	La función de puerto Mirror (Duplicar) muestra que el puerto conecta este servidor con otro servidor para duplicar los volúmenes de archivo.
Privado (clúster Sun StorEdge 5310 sólo)	El puerto Private (Privado) se reserva para la conexión privada, un enlace de red dedicado que supervisa constantemente el estado de la otra unidad. Cada unidad cuenta con un único puerto privado.

Nota – Como mínimo, uno de los puertos debe estar configurado como principal.

Para obtener más información acerca de las funciones de puertos, consulte "Gestión de los puertos de sistema" en la página 69.

7. **Para agregar una dirección IP alias a un puerto seleccionado, especifíquela en el campo IP-Aliases (Alias de IP). Después, haga clic en el botón Add (Agregar) para añadirla a la lista IP-Aliases (Alias de IP).**

   Puede tener hasta nueve alias por cada interfaz en los sistemas con una sola unidad y hasta cuatro alias en los sistemas con dos unidades. Para eliminar un alias de la lista, selecciónelo y haga clic en el botón Trash (Papelera). Los cambios no se guardarán hasta que haga clic en **Apply** (Aplicar).

8. **Repita estos pasos para todos los puertos de la lista Adapter (Adaptador).**

9. **Para guardar los cambios, haga clic en Apply (Aplicar).**

Definición de la dirección de puerta de enlace predeterminada

La dirección de puerta de enlace predeterminada es la dirección IP de la puerta de enlace o del router en la subred local que se usa de forma predeterminada para conectarse a otras subredes. Una puerta de enlace o un router es un dispositivo que envía datos a destinos remotos. Es necesario especificar la dirección de puerta de enlace predeterminada del sistema.

▼ Para especificar la dirección de puerta de enlace predeterminada

1. **En el panel de navegación, seleccione Network Configuration (Configuración de red) > Configure TCP/IP (Configurar TCP/IP) > Set Gateway Address (Definir dirección de puerta de enlace).**
2. **Escriba la dirección de puerta de enlace en el cuadro de texto Gateway (Puerta de enlace).**
3. **Para guardar las preferencias, haga clic en Apply (Aplicar).**

Servicios de nombres

En esta sección se describe la forma de configurar la seguridad de Windows, WINS, DNS, NIS, NIS+ y los servicios de nombres.

Para obtener más información acerca de los servicios de nombres, consulte el Capítulo 6, “Servicio Active Directory y autenticación” en la página 77.

Configuración de la Seguridad de Windows

La configuración del dominio, el grupo de trabajo o el servicio Active Directory (ADS) es una función de Windows. Si está ejecutando una red que sea totalmente UNIX, no tendrá que configurar dominios de Windows ni grupos de trabajo.

El panel **Configure Domains and Workgroups** (Configurar dominios y grupos de trabajo) permite habilitar grupos de trabajo de Windows, seguridad para dominios de NT y ADS. De forma predeterminada, el sistema está configurado en modo de grupo de trabajo de Windows, con el grupo de nombre “workgroup”.

▼ Para configurar la Seguridad de Windows

1. **En el panel de navegación, seleccione Windows Configuration (Configuración de Windows) > Configure Domains and Workgroups (Configurar dominios y grupos de trabajo).**
2. **Para habilitar la seguridad para dominios de Windows, seleccione la opción Domain (Dominio).**

   Esta opción crea una cuenta en el dominio para este servidor. Debe especificar una cuenta de usuario con derechos para agregar servidores al dominio especificado.

a. **Escriba el nombre del dominio en el campo Domain (Dominio).**

   Este nombre debe ajustarse a la restricción de 15 caracteres de NetBIOS.

b. **Escriba el nombre y la contraseña del usuario del dominio administrativo en los campos User Name (Nombre de usuario) y Password (Contraseña).**

   El nombre de usuario puede tener 16 caracteres como máximo.

3. **Para habilitar la seguridad de grupos de trabajo de Windows, seleccione la opción Workgroup (Grupo de trabajo) y, a continuación, escriba el nombre del grupo de trabajo en el campo Name (Nombre).**

   El nombre del grupo de trabajo debe ajustarse a la restricción de 15 caracteres de NetBIOS.

4. **En el campo Comments (Comentarios), escriba una descripción del sistema del dispositivo Sun StorEdge 5310 NAS (optativo).**

5. **Para habilitar ADS, haga clic en la casilla de verificación Enable ADS (Habilitar ADS).**

   Para obtener más información acerca de ADS, consulte "Servicio Active Directory" en la página 78.

Nota – Antes de habilitar ADS, debe verificar que la hora del sistema esté en un margen de 5 minutos con respecto a todos los controladores de dominio de Windows de ADS. Para comprobar la hora, seleccione **System Operations (Operaciones de sistema) > Set Time and Date (Ajustar fecha y hora)** en el panel de navegación.

---

a. **En el campo Domain (Dominio), indique el dominio de Windows en que se está ejecutando ADS.**

   El sistema debe pertenecer a este dominio.

b. **En el campo User Name (Nombre de usuario), escriba el nombre de una cuenta de usuario de Windows que tenga derechos administrativos.**

   Esta persona debe ser el administrador de dominio o un usuario que sea miembro del grupo de administradores de dominio. El cliente ADS comprueba las actualizaciones ADS seguras con este usuario.

Nota – Si especifica aquí el nombre del administrador del dominio y falla la actualización de ADS, deberá cambiar la contraseña de dicho administrador (en el controlador de dominio). El usuario administrador es el único que debe hacer esto y puede reutilizar la misma contraseña. Para obtener más información, consulte el sitio Web de asistencia técnica de Microsoft (artículo Q248808).

---

c. **En el campo Password (Contraseña), escriba la contraseña del usuario administrativo de Windows.**

d. **En el campo Container (Contenedor), escriba la ubicación de la ruta ADS del usuario administrativo de Windows en notación de nombre distinguido (DN, del inglés Distinguished Name) de protocolo ligero de acceso a directorios (LDAP, del inglés Lightweight Directory Access Protocol).**

   Para obtener más información, consulte "Servicio Active Directory" en la página 78.

Nota – No incluya el nombre del dominio en la ruta.

---

e. **Si el dominio de ADS utiliza sitios, escriba el nombre del sitio en el campo Site (Sitio). En caso contrario, deje este campo en blanco. Si lo especifica, el sitio se incluirá cuando se seleccione un controlador del dominio.**

f. **En la sección Kerberos Realm Info (Información del dominio Kerberos), escriba el nombre de dominio que se usa para identificar ADS.**

   Normalmente, se trata del dominio ADS o del dominio DNS. Al hacer clic en Apply (Aplicar), esta entrada se convierte en caracteres en mayúscula.

g. **En el campo Server (Servidor), escriba el nombre de host del servidor del centro de distribución de claves (KDC, del inglés Key Distribution Center) de Kerberos.**

   Normalmente, se trata del nombre de host del controlador de dominios principal del dominio ADS. Puede dejar este campo en blanco si el sistema puede localizar el servidor de KDC mediante DNS.

6. **Para guardar las preferencias, haga clic en Apply (Aplicar).**

   Si cambia el modo de seguridad de grupo de trabajo a dominio NT, o viceversa, el servidor se reiniciará automáticamente cuando haga clic en Apply (Aplicar).

Configuración de WINS

El servicio de nombres de Internet para Windows (WINS) es una función de Windows. Si está ejecutando una red sólo de UNIX, no necesitará configurar WINS.

▼ Para configurar WINS

1. **En el panel de navegación, seleccione Windows Configuration (Configuración de Windows) > Set Up WINS (Configurar WINS).**

2. **Para habilitar WINS, haga clic en la casilla de verificación Enable WINS (Habilitar WINS).**

   Al marcar esta casilla, el sistema se convierte en un cliente WINS.

3. **Escriba la dirección IP del servidor WINS principal en Primary WINS server (Servidor WINS principal).**

   El servidor WINS principal es el servidor al que se acude en primer lugar para la resolución de nombres de NetBIOS.

4. **Escriba los datos necesarios en Secondary WINS server (Servidor WINS secundario).**

   Si el servidor WINS principal no responde, el sistema consulta el servidor WINS secundario.

5. **Especifique el identificador de ámbito de NetBIOS (optativo) en el campo Scope (Ámbito).**

   La definición de un ámbito evitará que un equipo se comunique con sistemas que tengan el mismo ámbito configurado. Por tanto, esta configuración deberá utilizarse con cuidado. El ámbito es útil si desea dividir un grupo de trabajo grande de Windows en grupos más pequeños. Si utiliza un ámbito, el ID del ámbito debe seguir las convenciones de nomenclatura de NetBIOS o las de nomenclatura de dominios y se deben usar 16 caracteres como máximo.

6. **Para guardar las preferencias, haga clic en Apply (Aplicar).**

Configuración de DNS

El sistema de nombres de dominio (DNS) traduce los nombres de host en direcciones IP para el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 o el sistema de puerta de enlace Sun StorEdge 5310.

Nota – Si está utilizando DNS sin DNS dinámico, agregue el nombre de host y dirección IP del servidor a su base de datos de DNS. Si está usando DNS dinámico, no tendrá que actualizar manualmente la base de datos DNS. Consulte la documentación de DNS para obtener más información.

▼ Para configurar DNS

1. **En el panel de navegación, seleccione Network Configuration (Configuración de red) > Configure TCP/IP (Configurar TCP/IP) > Set Up DNS (Configurar DNS).**

2. **Marque la casilla Enable DNS (Habilitar DNS).**

3. **Escriba el nombre de dominio del servidor DNS en el campo Domain Name (Nombre de dominio)**

4. **Escriba la dirección IP del servidor DNS que desea que esté disponible en la red y, a continuación, haga clic en el botón Add (Agregar) para añadir el servidor a la lista Server List (Lista de servidores).**

   Repita este paso para cada servidor DNS que desee añadir. Puede agregar dos servidores DNS como máximo a esta lista.

   A la hora de resolver un nombre de dominio el sistema consultará, en primer lugar, el primer servidor DNS de la lista de servidores. Si este servidor no puede resolver la solicitud, la consulta pasará al siguiente servidor de la lista.

5. **Para reorganizar el orden de la búsqueda en los servidores DNS de la lista, haga clic en el servidor que desea mover y en los botones Arriba o Abajo.**

   Para eliminar un servidor de la lista, seleccione la dirección IP del servidor y haga clic en el botón Papelera.

6. **Seleccione la casilla de verificación Enable Dynamic DNS (Habilitar DNS dinámico) para permitir que un cliente DNS dinámico agregue el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 o el sistema de puerta de enlace Sun StorEdge 5310 al espacio de nombre DNS.**

   No habilite esta opción si el servidor DNS no admite actualizaciones dinámicas. También debe configurar el dominio Kerberos y el servidor KDC siguiendo las instrucciones que figuran en "Configuración de la Seguridad de Windows" en la página 21. Si habilita DNS dinámico seleccionando esta casilla de verificación, las actualizaciones dinámicas que no sean seguras se llevarán a cabo si lo permite el servidor DNS.

7. **Para habilitar las actualizaciones de DNS dinámico, aporte la siguiente información. Esta información no se requiere en las actualizaciones que no sean seguras.**

   a. **En el campo DynDNS User Name (Nombre de usuario de DNS dinámico), escriba el nombre de un usuario de Windows 2000 con autorización para realizar actualizaciones DNS dinámicas.**

      Este usuario debe residir en los dominios ADS y Kerberos especificados en el panel Configure Domains and Workgroups (Configurar dominios y grupos de trabajo) que se describe en "Configuración de la Seguridad de Windows" en la página 21.

Nota – Si especifica aquí el nombre del administrador del dominio y falla la actualización de ADS, el administrador deberá cambiar su contraseña en el controlador de dominio. El usuario administrador es el único que debe hacer esto y puede reutilizar la misma contraseña. Para obtener más información, consulte el sitio Web de asistencia técnica de Microsoft (artículo Q248808).

---

   b. **En el campo DynDNS Password (Contraseña de DynDNS), escriba la contraseña del usuario de DynDNS.**

      Si actualiza este campo, elimine la contraseña entera antes de escribir una nueva.

8. **Para guardar las preferencias, haga clic en Apply (Aplicar).**

Configuración de NIS

El servicio de información de red (NIS) es una función de UNIX. Si está ejecutando una red sólo de Windows, no necesitará configurar NIS.

El panel **Set Up NIS** (Configurar NIS) se utiliza para habilitar NIS y especificar el nombre de dominio y la dirección IP del servidor.

▼ Para configurar NIS

1. **En el panel de navegación, seleccione UNIX Configuration (Configuración de UNIX) > Set Up NIS (Configurar NIS).**
2. **Marque la casilla Enable NIS (Habilitar NIS).**

   De esta forma, NIS configura el sistema para importar la base de datos NIS donde se recoge información sobre el host, el usuario y el grupo.
3. **Escriba el nombre del dominio que desea utilizar para los servicios NIS en el campo Domain Name (Nombre de dominio).**

   Utilice la convención de nomenclatura DNS, por ejemplo, dominio.com.
4. **Escriba la dirección IP o el nombre del servidor NIS en el campo Server (Servidor).**

   La tarea de importación de la base de datos se realiza desde este servidor.

   Si no conoce la dirección IP del servidor, deje en blanco el campo **Server** (Servidor). Recuerde que si deja en blanco el campo **Server** (Servidor), deberá marcar la casilla **Use Broadcast** (Utilizar difusión). Esta opción obtiene automáticamente la dirección IP adecuada del servidor NIS.
5. **Introduzca la frecuencia, en minutos, con que desea que se actualice la información de NIS. El valor predeterminado es 5 minutos.**
6. **Seleccione la casilla Use Broadcast (Utilizar difusión) para obtener de forma automática la dirección IP del servidor NIS.**
7. **Active la casilla Update Hosts (Actualizar hosts) para descargar información de host desde el servidor NIS al servidor del sistema.**
8. **Marque la casilla Update Users (Actualizar usuarios) para descargar información de usuarios desde el servidor NIS al servidor del sistema.**
9. **Active la casilla Update Groups (Actualizar grupos) para descargar información de grupos desde el servidor NIS al servidor del sistema.**
10. **Seleccione la casilla Update Netgroups (Actualizar grupos de red) para descargar información de grupos de red desde el servidor NIS al servidor del sistema.**
11. **Para guardar los cambios, haga clic en Apply (Aplicar).**

Configuración de NIS+

El servicio de información de red Network Information Services Plus (NIS+) es una función de UNIX. Si está ejecutando una red sólo de Windows, no necesitará configurar NIS+.

Nota – No existe relación alguna entre NIS+ y NIS. Los comandos y la estructura general de NIS+ son diferentes a los de NIS.

▼ Para configurar NIS+

1. **Para que el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 o el sistema de puerta de enlace Sun StorEdge 5310 funcione correctamente en un entorno NIS+, debe agregar el sistema al archivo de credenciales del host en el servidor NIS+. Realice los siguientes pasos en el servidor NIS+:**

   a. **Inicie sesión como root.**

   b. **Escriba el siguiente comando:**

      `nisaddcred -p unix.SERVER@DOMAIN -P SERVER.DOMAIN. des`

      donde *SERVIDOR* es el nombre del sistema del dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 o el sistema de puerta de enlace Sun StorEdge 5310, y *DOMINIO* es el nombre del dominio NIS+ al que accede el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 o el sistema de puerta de enlace Sun StorEdge 5310.

Nota – Justo después del argumento **`-P`** deberá escribir un punto (".") al final del nombre del dominio.

      Por ejemplo, si el dispositivo Sun StorEdge 5310 NAS se denomina **SS1** y el dominio NIS+ es sun.com, deberá escribir el siguiente comando:

      `nisaddcred -p unix.ss1@sun.com -P ss1.sun.com. des`

   c. **Se le pedirá una contraseña en el indicador.**

      Esta contraseña le servirá más adelante para configurar el sistema para que utilice NIS+. Escriba la contraseña.

2. **Desde un cliente remoto, abra una ventana del explorador web en el sistema e inicie sesión en Web Administrator.**

3. **En el panel de navegación, seleccione UNIX Configuration (Configuración de UNIX) > Set Up NIS+ (Configurar NIS+).**

4. **Marque la casilla Enable NIS+ (Habilitar NIS+).**

5. **En el campo Home Domain Server (Servidor de dominio principal), escriba la dirección IP del servidor de dominio principal de NIS+.**

   Si no conoce la dirección IP de este servidor, deje el campo en blanco y marque la casilla **Use Broadcast** (Utilizar difusión). Cuando se selecciona esta opción, el sistema obtiene automáticamente la dirección IP adecuada del servidor de dominio principal.

6. **En el campo NIS+ Domain (Dominio de NIS+), escriba el dominio principal de NIS+.**

   Nota – Los nombres de los dominios de NIS+ deben acabar en punto (“.”).

   ---

7. **Escriba la contraseña para RPC seguro del servidor NIS+.**

   Es la misma contraseña que definió en el paso 1c. en la página 27.

8. **Escriba la ruta de búsqueda en forma de lista de dominios separados por dos puntos (“:”).**

   La ruta de búsqueda define los dominios en los que busca NIS+ al intentar obtener información. Si desea buscar solamente el dominio principal y los que tiene relacionados, deje este espacio en blanco.

   Por ejemplo, si el dominio NIS+ es **`eng.sun.com.`** y la ruta de búsqueda se deja en blanco, el sistema busca en primer lugar en **`eng.sun.com.`** y después en **`sun.com.`** para resolver los nombres. Por el contrario, si especifica una ruta de búsqueda como **`sun.com.`**, el sistema buscará sólo en el dominio **`sun.com`** para resolver los nombres.

9. **Si no conoce la dirección IP del servidor del dominio principal, marque la casilla Use Broadcast (Utilizar difusión). Consulte el paso 5.**

10. **Para guardar las preferencias, haga clic en Apply (Aplicar).**

Configuración de servicios de nombres

El orden de búsqueda de los servicios de nombres (NS, Name Service) controla la secuencia que se sigue a la hora de buscar los servicios de nombres para resolver una consulta. Entre estos servicios de nombres se encuentran LDAP, NIS, NIS+, DNS y Local. Para utilizarlos en la resolución de nombres deberá habilitar los servicios seleccionados.

▼ Para establecer el orden de búsqueda del usuario, el grupo, el grupo de red y el host

1. **En el panel de navegación, seleccione UNIX Configuration (Configuración de UNIX) > Configure Name Services (Configurar servicios de nombres).**
2. **En la ficha Users Order (Orden de usuarios), seleccione el orden para buscar los usuarios:**
   a. **En el cuadro Services Not Selected (Servicios no seleccionados), seleccione el servicio que se va a utilizar en la búsqueda de usuarios.**
   b. **Para pasarlo al cuadro Services Selected (Servicios seleccionados), utilice el botón >.**
   c. **Repita este proceso para cada servicio que se vaya a utilizar en la búsqueda de usuarios.**
   d. **Para eliminar un servicio de la búsqueda de usuarios, márquelo y haga clic en el botón <.**
   e. **Establezca el orden de los servicios de búsqueda del cuadro Services Selected (Servicios seleccionados). Para ello deberá seleccionar cada servicio.**
   f. **Para desplazarlos hacia arriba o hacia abajo, utilice los botones Arriba y Abajo. El servicio que se sitúe al comienzo de la lista será el primero que se utilice en la búsqueda de usuario.**
3. **Seleccione los servicios que desee utilizar para las búsquedas de grupos en la ficha Groups Order (Orden de grupos). Para ello siga los pasos descritos en el punto 2.**
4. **Seleccione los servicios que se van a utilizar para las búsquedas de grupos de red en la ficha Netgroup Order (Orden de grupos de red). Para ello siga los pasos descritos en el punto 2.**
5. **Seleccione los servicios que se van a utilizar para las búsquedas de host en la ficha Hosts Order (Orden de hosts). Para ello, siga los pasos que se describen en el punto 2.**
6. **Para guardar los cambios, haga clic en Apply (Aplicar).**

Configuración de la notificación por correo electrónico

Defina el nombre del servidor del protocolo simple de transferencia de correo (SMTP, del inglés Simple Mail Transfer Protocol) y los destinatarios de la notificación por correo electrónico en esta pantalla. Cuando el sistema detecta un error, envía un mensaje de correo electrónico de notificación.

Para garantizar la resolución de nombres, debe tener configurado el nombre de host del servidor SMTP en el panel **Configure Hosts** (Configurar hosts) (consulte "Configuración de hosts" en la página 89) o bien DNS (consulte "Configuración de DNS" en la página 24).

▼ Para configurar SMTP y enviar mensajes de correo electrónico a los destinatarios

1. **En el panel de navegación, seleccione Monitoring and Notification (Supervisión y notificación) > Set Up Email Notification (Configurar notificación por correo electrónico).**
2. **Escriba el nombre del servidor SMTP que desea utilizar para enviar la notificación.**
3. **En el cuadro Email Address (Dirección de correo electrónico), escriba la dirección de correo electrónico de la persona a la que desee enviar automáticamente la notificación de errores del sistema.**
4. **Determine los tipos de correo electrónico del destinatario. Elija Notification (Notificación), Diagnostic (Diagnóstico) o ambos.**
5. **Haga clic en el botón Add (Agregar) para añadir el nuevo destinatario a List (Lista). Repita del paso 1 al paso 4 para todos los destinatarios. Puede especificar un máximo de cuatro direcciones de correo electrónico.**

   Para eliminar un destinatario de la lista, seleccione la dirección y haga clic en el botón Trash (Papelera).
6. **Indique un valor en Notification Level (Nivel de notificación).**
   - Marque la casilla **Errors and Warnings** (Errores y advertencias) para informar a los destinatarios de todos los errores y advertencias que se produzcan.
   - Haga clic en **Errors Only** (Errores sólo) para informar a los destinatarios de correo de los errores (pero no de las advertencias).
   - Haga clic en **None** (Ninguno) para deshabilitar la notificación.
7. **Para guardar las preferencias, haga clic en Apply (Aplicar).**

Configuración del inicio de sesión

La habilitación del inicio de sesión remoto hace posible que el sistema envíe su registro a un servidor designado y que lo guarde en un archivo local. El servidor especificado debe ser un servidor UNIX que ejecute `syslogd`. Si va a hacer referencia al host de inicio de sesión mediante el nombre de dominio, debe configurar las preferencias DNS en el sistema antes de habilitar el inicio de sesión remoto.

Precaución – Debe habilitar el registro remoto o bien crear un archivo de registro en el disco local para evitar que el registro desaparezca cuando se cierre el sistema. De lo contrario, el sistema creará un archivo de registro temporal en la memoria volátil durante el encendido. Esto es suficiente para retener los errores que puedan suceder durante el encendido con el fin de verlos más tarde, pero no se conservarán después de un fallo del suministro eléctrico o un reinicio del sistema.

▼ Para configurar el inicio de sesión remoto y local

1. **En el panel de navegación, seleccione Monitoring and Notification (Supervisión y notificación) > View System Events (Ver eventos de sistema) > Set Up Remote Logging (Configurar inicio de sesión remoto).**
2. **Seleccione el cuadro Enable Remote Syslogd (Habilitar Syslogd remoto).**
3. **En el campo Server (Servidor), escriba el nombre de host DNS si ha configurado las preferencias DNS. De lo contrario, escriba la dirección IP. Hace referencia al lugar al que se enviará el registro de sistema.**
4. **Seleccione el valor que proceda en Facility (Utilidad).**

   La utilidad hace referencia a la aplicación o al componente de sistema que genera los mensajes. *Todos los mensajes enviados al servidor syslogd tendrán este valor de utilidad.* Los valores de utilidad que se pueden seleccionar en el panel Set Up Remote Logging (Configurar inicio de sesión remoto) son:

Utilidad	Descripción
Kern	Los mensajes son generados por el núcleo. Estos mensajes no los puede generar ningún proceso de usuario.
User	Los mensajes son generados por procesos de usuarios aleatorios. Es el valor predeterminado si no se especifica ninguno.
Mail	El sistema de correo.

Utilidad	Descripción
Daemon	Daemons de sistema o de red.
Auth	Sistemas de autorización como, por ejemplo, el inicio de sesión.
Syslog	Mensajes generados internamente por syslogd.
Local0–Local7	Reservado para uso local.

5. **Seleccione los eventos del sistema que se deben registrar activando los tipos de evento que proceda (consulte "Eventos de sistema" en la página 144).**
6. **Seleccione la opción Enable Local Log (Habilitar registro local) para activar un registro de archivo local.**
7. **Introduzca la ruta del archivo de registro (el directorio en el sistema donde desea almacenarlo) y el nombre de archivo en el campo Log File (Archivo de registro).**
8. **Indique el número máximo de archivos de almacenamiento en el campo Archives (Archivos de almacenamiento).**

   Puede indicar un valor entre 1 y 9.
9. **Especifique el tamaño máximo de archivo en kilobytes para cada archivo de almacenamiento en el campo Size (Tamaño).**

   Puede indicar un valor entre 1000 y 999.999 kilobytes.
10. **Para guardar las preferencias, haga clic en Apply (Aplicar).**

Asignación del idioma

El sistema operativo es compatible con Unicode, por lo que puede definir el idioma local para NFS y CIFS. Normalmente, el idioma se suele especificar cuando se ejecuta el asistente durante la configuración inicial. Sin embargo, si necesita restablecer el idioma posteriormente, podrá hacerlo de forma manual.

▼ Para asignar el idioma

1. **En el panel de navegación, seleccione System Operations (Operaciones de sistema) > Assign Language (Asignar idioma).**
2. **Seleccione el idioma local de entre los que se muestran en el menú desplegable.**
3. **Para guardar los cambios, haga clic en Apply (Aplicar).**

Copia de seguridad de la información de configuración

Después de completar la configuración del sistema, realice una copia de seguridad de la información de configuración en caso de que se produzca un fallo en el sistema. Consulte "Copia de seguridad de la configuración" en la página 198 para obtener más datos acerca de cómo realizar copias de seguridad de la información de configuración.

Qué debe hacer a continuación

En este momento, el sistema está ya completamente conectado a la red. Sin embargo, antes de que los usuarios puedan comenzar a almacenar datos, debe configurar el sistema de archivos y establecer los derechos de acceso de los usuarios. El capítulo siguiente, "Configuración y gestión del sistema de archivos" en la página 35, describe las tareas de configuración de un sistema de archivos.

Para configurar cuotas, recursos compartidos, exportaciones y otros controles de acceso, consulte "Recursos compartidos, cuotas y exportaciones" en la página 101 para obtener información detallada.

Si hay una función específica que desee configurar, consulte el índice para obtener las instrucciones necesarias.

CAPÍTULO 3

Configuración y gestión del sistema de archivos

Este capítulo trata los conceptos, la configuración y la gestión del sistema de archivos para el dispositivo Sun StorEdge 5310 NAS y el clúster Sun StorEdge 5310.

Está dividido en las siguientes secciones:

- "Conceptos del sistema de archivos" en la página 35
- "Creación del sistema de archivos" en la página 40
- "Creación de un volumen de archivo o un segmento" en la página 45
- "Reconstrucción de un LUN" en la página 49
- "Gestión de segmentos y de volúmenes de archivo" en la página 49
- "Configuración de iSCSI" en la página 53
- "Qué debe hacer a continuación" en la página 60

Conceptos del sistema de archivos

En las secciones a continuación se proporcionan definiciones de algunos de los conceptos básicos del sistema de archivos y de los atributos que se utilizan en el almacenamiento NAS.

RAID

Los sistemas RAID (con matriz redundante de discos independientes) permiten distribuir los datos por numerosas unidades mediante un controlador de matriz para obtener un mayor rendimiento, seguridad de datos y posibilidades de recuperación. El concepto básico de RAID es la combinación de un grupo de unidades físicas más

pequeñas en lo que se muestra ante la red como una única unidad muy grande. Desde la perspectiva del usuario del equipo, un sistema RAID es exactamente igual que una sola unidad. Desde el punto de vista del administrador del sistema, el componente físico de un sistema RAID es un grupo de dispositivos, aunque en realidad se puede administrar como si fuera una sola unidad.

Existen muchos tipos de configuraciones de RAID. El dispositivo Sun StorEdge 5310 NAS y el clúster Sun StorEdge 5310 son compatibles con RAID 5 exclusivamente. El sistema de puerta de enlace Sun StorEdge 5310 es compatible con RAID 1, RAID 0+1 y RAID 5.

RAID 0 (no compatible)

RAID de nivel 0 no incluye la redundancia para la que se ha desarrollado RAID. Sin embargo, proporciona un aumento significativo del rendimiento. RAID 0 hace uso del concepto de *organización en secciones*. Organizar los datos en secciones significa que son divididos en bandas, o secciones: la primera de ellas se escribe en la primera unidad; la segunda, en la segunda unidad, etc. La principal ventaja de distribuir así los datos es la posibilidad que tienen todas las unidades de la matriz de procesar simultáneamente las fases de lectura y escritura. De esta manera, se agiliza enormemente tanto la lectura de datos como la escritura.

Sin embargo, como el RAID 0 no tiene redundancia disponible, si alguna unidad falla, se pueden perder los datos de toda la matriz. RAID 0 se puede utilizar en las situaciones en que el rendimiento tenga mayor importancia que la pérdida de datos.

RAID 1 (sólo sistema de puerta de enlace Sun StorEdge 5310)

La *duplicación* de unidades es el principal concepto utilizado por la matriz RAID 1, al duplicar el número de unidades que se requieren para la misma capacidad de almacenamiento y, a la vez, proporcionar una copia de seguridad actualizada de la unidad. La unidad duplicada siempre está conectada y se accede a ella con gran rapidez si ocurre un fallo en la unidad principal. Cada unidad principal se encuentra duplicada en una segunda unidad del mismo tamaño. Todas las operaciones de escritura se duplican en ambos miembros de la matriz RAID 1 a la vez. RAID 1 proporciona una excelente alta disponibilidad. Una matriz RAID 1 es de gran utilidad cuando la seguridad e integridad de datos es esencial pero el rendimiento no tiene tanta importancia.

RAID 0+1 (sólo sistema de puerta de enlace Sun StorEdge 5310)

RAID 0+1 combina los dos conceptos anteriores de RAID mejorando tanto el rendimiento como la alta disponibilidad: organización en secciones y duplicación. Los pares de unidades duplicadas se encuentran integrados en una matriz RAID 0.

Todas las operaciones de escritura se duplican y realizan a la vez en ambas unidades duplicadas. La organización en secciones (bandas) de RAID 0 aumenta el rendimiento de la matriz en su conjunto, mientras que la duplicación de unidades de RAID 1 proporciona una excelente alta disponibilidad a cada unidad por separado. RAID 0+1 es una opción adecuada para los entornos en que el rendimiento tenga menos importancia que seguridad pero continúe siendo un requisito esencial.

RAID 5

La matriz RAID 5 aúna las ventajas derivadas de las mejoras en el rendimiento propias de la organización en secciones y la redundancia de la duplicación, y todo ello sin tener que duplicar el número de unidades de la matriz.

RAID 5 emplea la organización en secciones de los datos y la información de *paridad*. La información de paridad consiste en datos creados combinando los bits de la información que se va a almacenar y creando una pequeña cantidad de datos a partir de los cuales se puede extraer el resto de la información. Es decir, la información de paridad repite los datos originales de tal forma que, si se pierde parte del original, la combinación del resto del original y de los datos de paridad dará como resultado el original completo. La información de paridad no se almacena en ninguna unidad en particular. Para la protección de paridad en cada una de las regiones del equipo RAID 5, se hace uso de unidades distintas en la organización de secciones.

La matriz RAID 5 incluye la información de paridad en una sección del conjunto de secciones. Si falla una unidad de la matriz, la información de paridad y el resto de los datos originales de las unidades que quedan en buen estado se utilizan para reconstruir la información que se ha perdido en la unidad que ha fallado. De esta manera, la matriz RAID 5 combina la alta disponibilidad de la duplicación con el rendimiento que proporciona la organización en secciones, lo que permite obtener el mejor tipo de RAID posible. También tiene la ventaja de que requiere muy poco espacio adicional para la información de paridad, lo que contribuye a que sea la solución más económica.

El primer armario con unidades en cada matriz (la unidad de expansión 5300 RAID para matrices de Fibre Channel, o la primera unidad de expansión S conectada a una unidad de expansión 5300 RAID vacía para matrices SATA), contiene dos grupos RAID 5 de seis unidades (5+1) más dos unidades de reserva globales. Todos los siguientes armarios de unidades de expansión F o S contienen uno o dos grupos RAID 5 de siete unidades (6+1) para un total de siete o catorce unidades.

Precaución – No actualice el software del sistema ni el firmware de RAID cuando el subsistema RAID esté en estado crítico, creando un volumen nuevo o reconstruyendo uno existente.

LUN

El número de unidad lógica (LUN) hace referencia a la representación lógica de un dispositivo físico o virtual. En el dispositivo Sun StorEdge 5310 NAS y el clúster Sun StorEdge 5310, hay una correspondencia uno a uno entre los conjuntos de RAID y los LUN. Sin embargo, el sistema considera los LUN como entidades independientes y los trata como un solo volumen de almacenamiento.

Al concebir de este modo los LUN, el dispositivo Sun StorEdge 5310 NAS y el clúster Sun StorEdge 5310 simplifican considerablemente el proceso para establecer un sistema de archivos. A los conjuntos de RAID se accede con independencia de las restricciones de la unidad física mediante el LUN.

La gestión de los recursos de almacenamiento se realiza mediante el LUN con una pequeña gestión directa de los propios equipos RAID. Consulte "Creación de LUN y conjuntos de RAID" en la página 40 para obtener más información acerca de cómo se configuran los LUN y los conjuntos de RAID.

Partición

Las particiones son secciones de un LUN y constituyen una forma de subdividir el espacio total disponible de un LUN. El sistema operativo del dispositivo Sun StorEdge 5310 NAS y el clúster Sun StorEdge 5310 admite 31 particiones como máximo por cada LUN.

Cuando se crea un LUN por primera vez, todo el espacio disponible se ubica en la primera partición y las demás se quedan vacías. Para usar el espacio de una partición, debe crear un volumen de archivo. Cada partición puede contener sólo un volumen de archivo, aunque el mismo volumen puede abarcar distintas particiones. Cuando se crea un volumen de archivo, el tamaño de la partición se ajusta automáticamente para que coincida con el tamaño del volumen. Cualquier espacio adicional del LUN se asigna automáticamente a la partición siguiente. Una vez que haya creado todos los volúmenes de archivo que admita el sistema operativo, no se podrá acceder al espacio adicional del LUN en cuestión.

El tamaño de un volumen de archivo se puede aumentar adjuntando un segmento (consulte "Segmento" en la página 39). Básicamente, el segmento es otro volumen de archivo con unas características especiales. Si agrega un segmento a un volumen existente, los dos se convierten en inseparables y lo único que puede apreciar el usuario es que hay más espacio en el volumen. La flexibilidad de este sistema le permite crear un volumen de archivo y, a continuación, ampliarlo según sus necesidades sin interferir en el trabajo de los usuarios y sin obligarles a distribuir sus datos por los diferentes volúmenes.

Puede que el administrador del sistema esté agregando unidades y LUN, pero lo único que verán los usuarios es que hay más espacio en el volumen.

Volumen de archivo

Un volumen de archivo es el espacio que está disponible para almacenar información y se crea a partir de las particiones que tienen espacio disponible. Si el volumen no utiliza todo el espacio disponible en la partición, el espacio restante se asigna automáticamente a la partición siguiente. El tamaño máximo de los volúmenes de archivo nuevos es de 255 gigabytes. Para crear un volumen de mayor tamaño, es posible crear y adjuntar hasta 63 segmentos (consulte "Segmento" en la página 39) al volumen de archivo original.

Desde el punto de vista del usuario, el volumen de archivo y cualquier estructura de archivos que posea ese volumen son lo más importante. Si el volumen de archivo comienza a llenarse, el administrador puede adjuntar otro segmento y aumentar el espacio disponible de dicho volumen. En términos físicos, esto puede implicar la adición de más unidades e incluso más unidades de expansión. Sin embargo, el usuario no verá el aspecto físico: lo único que apreciará es que hay más espacio de almacenamiento en el volumen.

Segmento

Los segmentos son "volúmenes" de espacio de almacenamiento que se crean de manera similar a los volúmenes de archivo. Pueden adjuntarse a un volumen de archivo existente en cualquier momento. Al adjuntar un segmento, se aumenta la capacidad total del volumen de archivo. Cada segmento se debe crear de forma independiente y, a continuación, se debe agregar al volumen de archivo. Una vez agregado, el volumen y el segmento no se pueden separar.

En líneas generales, los segmentos se crean conforme se necesitan y se adjuntan a medida que los volúmenes se van llenando de datos. La principal ventaja de ampliar el espacio adjuntando segmentos es que cada segmento se puede crear en una nueva unidad, e incluso, en una nueva matriz. Una vez que el segmento se ha adjuntado al volumen de archivo original, el usuario no ve las distintas ubicaciones de almacenamiento físicas. En consecuencia, se puede agregar espacio cuando se necesite sin que la red se quede inactiva para reestructurar el almacenamiento de los datos y crear un volumen de archivo más grande.

Creación del sistema de archivos

Si va a configurar el sistema de puerta de enlace Sun StorEdge 5310, utilice las herramientas de configuración del sistema de almacenamiento para crear las unidades de reserva y los LUN. Consulte la documentación incluida con el sistema de almacenamiento conectado a su puerta de enlace.

Si va a configurar el dispositivo Sun StorEdge 5310 NAS o el sistema de clúster, consulte "Creación de LUN y conjuntos de RAID" en la página 40 y "Designación como unidad de reserva de otra unidad" en la página 44.

Creación de LUN y conjuntos de RAID

El dispositivo Sun StorEdge 5310 NAS y el clúster Sun StorEdge 5310 combinan la creación y la definición del conjunto de RAID en la definición del LUN. Consulte "Conceptos del sistema de archivos" en la página 35 para obtener más información. En realidad, ambos objetos se crean simultáneamente. El dispositivo Sun StorEdge 5310 NAS y los sistemas de clúster permiten elegir la estructura básica del conjunto de RAID y definen el LUN. De esta manera, se automatizan muchas tareas que normalmente están asociadas a la definición del equipo RAID.

Precaución – Sólo para usuarios del clúster Sun StorEdge 5310: Cada servidor gestiona sus propios LUN. Antes de agregar un LUN, asegúrese de que la recuperación tras error está configurada y habilitada. Consulte "Habilitación de recuperación tras error" en la página 15 para obtener más información.

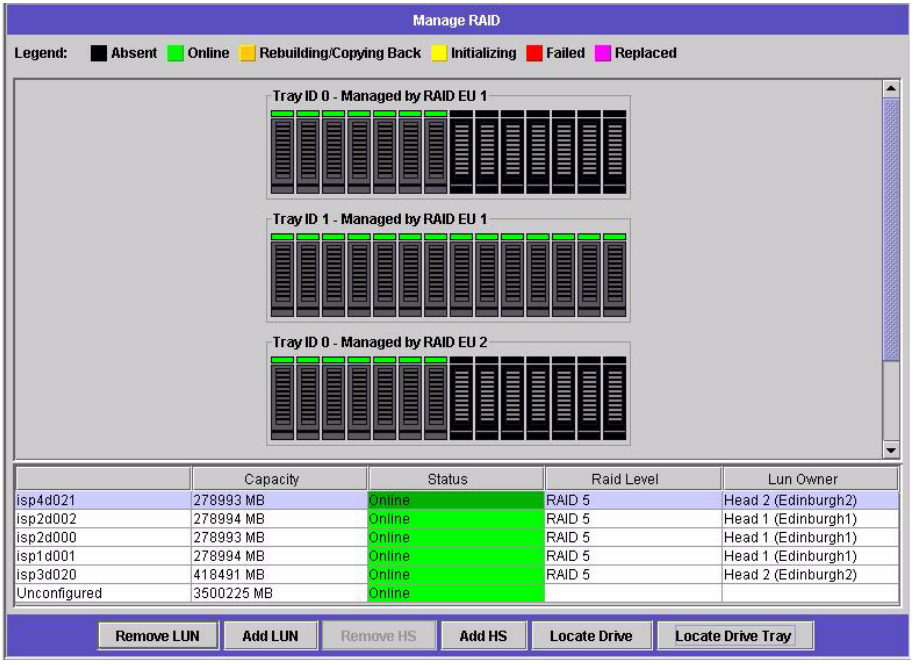
El dispositivo Sun StorEdge 5310 NAS y los sistemas de clúster también automatizan la definición de las particiones. Las particiones se definen automáticamente al crear un LUN. Inicialmente, el dispositivo Sun StorEdge 5310 NAS y los sistemas de clúster tienen dos unidades de reserva asignadas y, como mínimo, dos LUN predeterminados.

Los conjuntos de RAID y los LUN se crean simultáneamente en el dispositivo Sun StorEdge 5310 NAS y los sistemas de clúster, lo que simplifica el proceso de establecer ambas entidades.

Al agregar un LUN, debe asegurarse de que no ha asignado a los discos del LUN ninguna otra función (como, por ejemplo, unidad de reserva) antes de crear ese LUN. Las unidades que se hayan asignado a otro LUN o que actúen como unidades de reserva no estarán disponibles para incluirlas en un LUN nuevo.

▼ Para agregar un nuevo LUN

1. **En el panel de navegación, seleccione RAID > Manage RAID (Gestionar RAID).**
   El panel Manage RAID (Gestionar RAID) se muestra en pantalla.

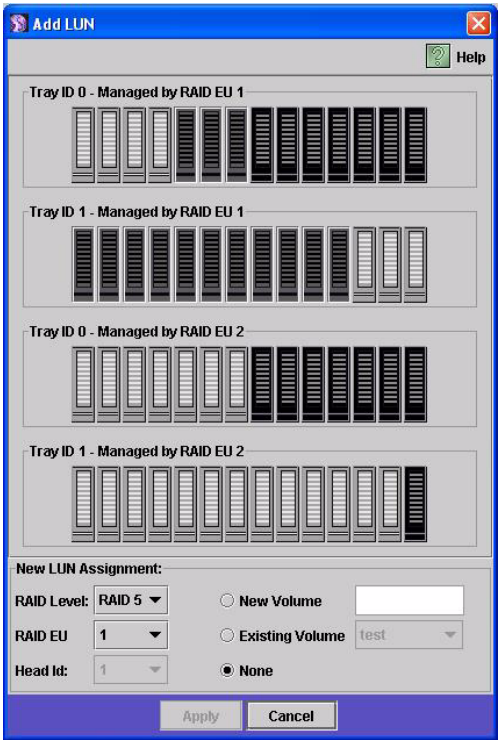


Nota – Para localizar una bandeja de unidades o una sola unidad, puede hacer clic en el botón Locate Drive (Localizar unidad) o Locate Drive Tray (Localizar bandeja de unidades), lo que causará que destelle el indicador del LCD de esa bandeja o esa unidad.

---

2. **Haga clic en Add LUN (Agregar LUN).**

   Se muestra la ventana Add LUN (Agregar LUN).



3. **Desde el menú desplegable RAID EU (UE de RAID), seleccione el número del controlador al que desea agregar un LUN.**

4. **Seleccione las unidades que se incluirán en el LUN haciendo clic en las imágenes de unidad.**

   Debe seleccionar como mínimo tres unidades. Las imágenes de las unidades muestran el estado de cada una de ellas.

TABLA 3-1 Indicadores de estado de las unidades del cuadro de diálogo Add LUN (Agregar LUN)

Unidad	Indicación
	La unidad de esta ranura es apta para incluirla en un LUN.
	Se ha seleccionado la unidad de esta ranura para incluirla en un LUN.
	No hay ninguna unidad en esta ranura.

5. **Elija una de las siguientes opciones de volumen.**

Opción	Descripción
New Volume (Nuevo volumen)	Seleccione esta opción para crear un nuevo volumen para este LUN. El LUN entero se utiliza para crear el volumen. Escriba el nombre del nuevo volumen en el espacio proporcionado.
Existing Volume (Volumen existente)	Seleccione esta opción si el propósito de este LUN es agregar espacio de disco a un volumen existente (para crear y adjuntar un segmento). A continuación, seleccione en la lista desplegable el volumen que desea ampliar.
None (Ninguno)	Seleccione esta opción para crear un nuevo LUN sin asignarle un nombre.

6. **Haga clic en Apply (Aplicar) para crear el nuevo LUN.**

   El sistema puede tardar varias horas en agregar el LUN.

Designación como unidad de reserva de otra unidad

Puede configurar como unidad de reserva para el dispositivo o el sistema de clúster Sun StorEdge 5310 otra unidad.

▼ Para designar otra unidad como unidad de reserva

1. **En el panel de navegación, seleccione RAID > Manage RAID (Gestionar RAID).**
2. **Haga clic en el botón Add HS (Agregar unidad de reserva), situado en la parte inferior de la pantalla.**
3. **Seleccione la unidad que desee haciendo clic en la imagen de la unidad.**

   Asegúrese de que el disco que va a utilizar como unidad de reserva sea, como mínimo, tan grande como el disco de mayor tamaño de los LUN en el servidor.

   Las imágenes de las unidades muestran el estado de cada una de ellas.

TABLA 3-2 Imágenes de estado de las unidades en Add Hot Spare (Agregar unidad de reserva)

Unidad	Indicación
	La unidad de esta ranura es apta para establecerla como unidad de reserva.
	La unidad de esta ranura se ha seleccionado para establecerla como unidad de reserva.
	No hay ninguna unidad en esta ranura.

4. **Haga clic en Apply (Aplicar) para agregar la nueva unidad de reserva.**

Creación de un volumen de archivo o un segmento

El tamaño máximo de los volúmenes de archivo nuevos es de 255 gigabytes. Para crear un volumen de archivo mayor, puede agregar hasta 63 segmentos al volumen principal. Si desea obtener un volumen de archivo de mayor tamaño, cree un volumen principal y hasta 63 segmentos. Después, adjunte los segmentos al volumen principal para aumentar su tamaño.

Los volúmenes de archivo y los segmentos se pueden crear desde el panel Create File Volume (Crear volumen de archivo) o System Manager (Gestor de sistema).

▼ Para crear un volumen de archivo o un segmento con el panel Create File Volume (Crear volumen de archivo)

1. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Create File Volumes (Crear volúmenes de archivo).**
2. **Si ha agregado recientemente nuevos discos al sistema conectado sin efectuar un reinicio, haga clic en el botón Scan For New Disks (Buscar discos nuevos).**
3. **En el cuadro LUN, haga clic en el LUN en el que desea crear el volumen de archivo principal.**

   El número de partición del volumen de archivo en el menú desplegable **Partition** (Partición) se incrementará automáticamente cuando se cree el volumen de archivo.
4. **Escriba el nombre del nuevo volumen o segmento en el campo Name (Nombre).**

   Los caracteres válidos son alfanuméricos (a–z, A–Z, 0–9). El nombre debe contener como máximo 12 caracteres y debe comenzar por una letra (a–z, A–Z).
5. **Seleccione en el menú desplegable si el tamaño del volumen de archivo debe registrarse en MB (megabytes) o en GB (gigabytes).**
6. **Escriba el tamaño del volumen de archivo utilizando números enteros.**

   El espacio total disponible se muestra justo debajo de este campo.
7. **Seleccione el tipo de volumen de archivo, que puede ser Primary (Principal) o Segment (Segmento).**

8. **Si el software Archiving Software está instalado y desea crear un volumen compatible, haga clic en Enable (Habilitar) en la sección Compliance (Compatibilidad). A continuación, especifique el tipo de compatibilidad que es necesario aplicar.**

   - Si selecciona Mandatory Enforcement (Aplicación obligatoria), el tiempo de retención predeterminado será permanente. No se permite su anulación administrativa.

Precaución – Una vez se ha activado el almacenamiento compatible en un volumen con aplicación obligatoria, no se podrá eliminar o renombrar el volumen, o desactivar la función de almacenamiento compatible, ni cambiar a la característica de aplicación recomendada.

   - Si selecciona Advisory Enforcement (Aplicación recomendada), el tiempo de retención predeterminado será de 0 días. Se permite su anulación administrativa.

Nota – El superusuario, desde un host de confianza, podrá reducir el tiempo de retención y borrar los archivos retenidos antes de vencer el periodo de retención. Consulte "Gestión de hosts de confianza" en la página 224.

   Para obtener más información, consulte "Compliance Archiving Software" en la página 133.

9. **Haga clic en Apply (Aplicar) para crear el nuevo volumen de archivo o segmento.**

▼ Para crear un volumen de archivo o un segmento con System Manager (Gestor de sistema)

1. **Haga clic con el botón derecho en System Manager (Gestor de sistema) en el panel de navegación.**
2. **Elija Create Volume (Crear volumen) o Create Segment (Crear segmento) en el menú emergente para abrir el cuadro de diálogo que proceda.**
3. **En el cuadro LUN, haga clic en el LUN en el que desea crear el volumen de archivo principal.**

   El número de partición del volumen de archivo en el menú desplegable **Partition** (Partición) se incrementará automáticamente cuando se cree el volumen de archivo.

4. **Escriba el nombre del nuevo volumen o segmento en el campo Name (Nombre).**

   Los caracteres válidos son alfanuméricos (a–z, A–Z, 0–9). El nombre debe contener como máximo 12 caracteres y debe comenzar por una letra (a–z, A–Z).

5. **Seleccione en el menú desplegable si el tamaño del volumen de archivo debe registrarse en MB (megabytes) o en GB (gigabytes).**

6. **Escriba el tamaño del volumen de archivo utilizando números enteros.**

   El espacio total disponible se muestra justo debajo de este campo.

7. **Seleccione el tipo de volumen de archivo, que puede ser Primary (Principal) o Segment (Segmento).**

8. **Si el software Archiving Software está instalado y desea crear un volumen compatible, haga clic en Enable (Habilitar) en la sección Compliance (Compatibilidad). A continuación, especifique el tipo de compatibilidad que es necesario aplicar.**

   - Si selecciona Mandatory Enforcement (Aplicación obligatoria), el tiempo de retención predeterminado será permanente. No se permite su anulación administrativa.

Precaución – Una vez se ha activado el almacenamiento compatible en un volumen con aplicación obligatoria, no se podrá eliminar o renombrar el volumen, o desactivar la función de almacenamiento compatible, ni cambiar a la característica de aplicación recomendada.

   - Si selecciona Advisory Enforcement (Aplicación recomendada), el tiempo de retención predeterminado será de 0 días. Se permite su anulación administrativa.

Nota – El superusuario, desde un host de confianza, podrá reducir el tiempo de retención y borrar los archivos retenidos antes de vencer el periodo de retención. Consulte "Gestión de hosts de confianza" en la página 224.

Para obtener más información, consulte "Compliance Archiving Software" en la página 133.

9. **Haga clic en Apply (Aplicar) para crear el nuevo volumen de archivo o segmento.**

Adición de segmentos a un volumen de archivo principal

Al agregar segmentos a un volumen de archivo principal, se aumenta el tamaño del volumen. El segmento pasa a estar asociado permanentemente al volumen y no se puede eliminar. Los segmentos se deben crear antes de adjuntarlos a un volumen. Consulte "Creación de un volumen de archivo o un segmento" en la página 45 para obtener instrucciones.

Precaución – No se puede deshacer la acción de adjuntar un segmento a un volumen de archivo principal.

Un volumen de archivo puede tener como máximo 255 gigabytes; sin embargo, se le pueden agregar hasta 63 segmentos de cualquier LUN. El tamaño de un segmento puede oscilar entre 8 megabytes y 255 gigabytes.

Un segmento se puede agregar usando el panel Attach Segments (Adjuntar segmentos) o System Manager (Gestor de sistema).

Precaución – Los volúmenes compatibles con la característica de aplicación obligatoria no pueden eliminarse. Si agrega un segmento a un volumen compatible con aplicación obligatoria, no podrá eliminar o recuperar el espacio utilizado por el segmento.

▼ Para adjuntar un segmento con el panel Attach Segments (Adjuntar segmentos)

1. **Acceda al panel Attach Segments (Adjuntar segmentos) haciendo clic en File Volume Operations (Operaciones con volúmenes de archivo) > Attach Segments (Adjuntar segmentos).**
2. **Seleccione el volumen que desee en el cuadro Existing Volumes (Volúmenes existentes).**
3. **Seleccione el segmento que desee en el cuadro Available Segments (Segmentos disponibles).**
4. **Haga clic en Apply (Aplicar) para adjuntarlos.**

▼ Para adjuntar un segmento con System Manager (Gestor de sistema)

1. **Haga clic en System Manager (Gestor de sistema) en el panel de navegación para ver los volúmenes existentes.**
2. **Haga clic con el botón derecho en el volumen de archivo que desee para acceder al menú emergente y seleccione Attach Segments (Adjuntar segmentos).**
3. **Haga clic para seleccionar el segmento que desee.**

   Sólo se puede seleccionar un segmento para adjuntarlo cada vez.
4. **Haga clic en Apply (Aplicar) para adjuntar el segmento seleccionado.**
5. **Repita los pasos 3 y 4 para adjuntar más segmentos.**

Reconstrucción de un LUN

Si alguna de las unidades en un LUN tiene un error, el LED de dicha unidad se iluminará de color amarillo para indicar que se encuentra en espera de ser sustituida por otra unidad.

Nota – La reconstrucción de LUN no es aplicable a las configuraciones del sistema de puerta de enlace Sun StorEdge 5310 NAS.

Si la unidad de reserva está disponible, el conjunto de RAID asociado con la unidad con error se reconstruirá haciendo uso de dicha unidad de reserva. Todas las unidades asociadas a la reconstrucción mostrarán el indicador LED destellando de color verde y no deben ser retiradas durante este proceso. Tiene lugar una reconstrucción parecida al reemplazar la unidad con fallo, cuando la unidad nueva se inserta en el conjunto de RAID y la unidad de reserva vuelve al modo de espera. La reconstrucción puede tardar varias horas en completarse.

Si su sistema no cuenta con una unidad de reserva, deberá sustituir la unidad que ha fallado por otra unidad que tenga una capacidad igual o superior. Consulte el Apéndice D para obtener información sobre cómo reemplazar la unidad con fallo.

Después de sustituir la unidad defectuosa, el controlador RAID reconstruye automáticamente el LUN. Dicha reconstrucción puede tardar varias horas, según la capacidad del disco. Los indicadores LED de la unidad con el LUN destellan de color ámbar durante este proceso.

Gestión de segmentos y de volúmenes de archivo

Las tareas de gestión del sistema de archivos incluyen:

- "Edición de las propiedades de los volúmenes de archivo" en la página 50
- "Eliminación de volúmenes de archivo" en la página 52
- "Visualización de particiones de volúmenes" en la página 52

Edición de las propiedades de los volúmenes de archivo

Puede cambiar las propiedades de un volumen de archivo con el panel Edit Properties (Editar propiedades).

Nota – No es posible cambiar el nombre a los volúmenes de almacenamiento compatible con aplicación obligatoria ni deshabilitar el almacenamiento compatible o cambiar su aplicación a recomendada.

▼ Para cambiar el nombre de un volumen, habilitar los puntos de control o las cuotas, y editar las propiedades de compatibilidad

1. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Edit Properties (Editar propiedades).**
2. **En la lista Volumes (Volúmenes), seleccione el nombre del volumen que desea modificar.**
3. **Si procede, especifique el nuevo nombre del volumen en el campo New Name (Nombre nuevo).**

   Los caracteres válidos son alfanuméricos (a–z, A–Z, 0–9). El nombre debe contener como máximo 12 caracteres y debe comenzar por una letra (a–z, A–Z).
4. **Seleccione una o las dos siguientes opciones para este volumen.**

Opción	Descripción
Enable Checkpoints (Habilitar puntos de control)	Seleccione esta casilla de verificación para crear los puntos de control del volumen de archivo. Los puntos de control están habilitados de forma predeterminada cuando se crea un volumen de archivo.
Enable Quotas (Habilitar cuotas)	Seleccione esta casilla de verificación para habilitar el uso de cuotas en el volumen seleccionado. Las cuotas están deshabilitadas de forma predeterminada cuando se crea un volumen de archivo.
Enable Attic (Habilitar Attic)	Seleccione esta casilla de verificación para guardar temporalmente los archivos eliminados en el directorio `.attic$` que se encuentra en la raíz de cada volumen. Esta opción está habilitada de forma predeterminada. En los sistemas que estén muy ocupados, serán pocas las ocasiones en las que el directorio `.attic$` se llene a una velocidad superior a la velocidad con que procesa las eliminaciones, lo que puede provocar una falta de espacio libre y un rendimiento inferior. En este caso, se debería deshabilitar el directorio `.attic$` desactivando la casilla de verificación.

5. **Si el volumen tiene la compatibilidad habilitada, se dispone de varias opciones en el software Compliance Archiving dependiendo del nivel de compatibilidad elegido.**

Precaución – Para los volúmenes compatibles con aplicación obligatoria, el tiempo de retención predeterminado es permanente. Para los volúmenes compatibles con aplicación recomendada, el tiempo de retención predeterminado es de 0 días. Si desea configurar un tiempo de retención predeterminado distinto, es necesario que especifique el periodo de tiempo *antes* de empezar a utilizar el volumen.

Precaución – Una vez se ha activado el almacenamiento compatible en un volumen con aplicación obligatoria, no se podrá eliminar o renombrar el volumen, o desactivar la función de almacenamiento compatible, ni cambiar a la característica de aplicación recomendada.

Para obtener más información, consulte "Compliance Archiving Software" en la página 133.

Opción	Descripción
Mandatory Enforcement (Aplicación obligatoria)	Si el volumen tiene la compatibilidad habilitada con aplicación recomendada, puede seleccionar esta opción para cambiar la compatibilidad a aplicación obligatoria.
Advisory Enforcement (Aplicación recomendada)	Si el volumen tiene la compatibilidad habilitada con aplicación obligatoria, no es posible su modificación y esta opción no se encuentra disponible.
Permanent Retention (Retención permanente)	Opción predeterminada. Si no desea que los datos se retengan de manera permanente, debe seleccionar la opción Retain for *nn* Days (Retener durante nn días) antes de utilizar el volumen. Seleccione esta opción para retener los datos de este volumen permanentemente.
Retain for *nn* Days (Retener durante nn días)	Seleccione esta opción y, en el menú desplegable, especifique el número de días que se retendrán los datos. Si el volumen tiene la compatibilidad habilitada con aplicación recomendada, puede aumentar o reducir el periodo de retención. Si el volumen tiene la compatibilidad habilitada con aplicación obligatoria, sólo puede incrementar el periodo de retención.

6. **Para guardar los cambios, haga clic en Apply (Aplicar).**

Eliminación de volúmenes de archivo

En algunos casos, después de eliminar archivos, el espacio libre del volumen no cambia, probablemente, debido a la función de puntos de control o la función de habilitación de attic. (Para obtener más información acerca de cómo habilitar attic, consulte la página 51).

Los puntos de control almacenan datos eliminados y modificados durante un periodo de tiempo determinado para que sea posible la recuperación de dichos datos por motivos de seguridad. Esto significa que los datos no se eliminan del disco hasta que vence el punto de control (dos semanas como máximo, excepto en el caso de los puntos de control manuales, que se pueden conservar de forma indefinida).

Si desea eliminar datos para liberar espacio, deberá eliminar los puntos de control o deshabilitarlos. Consulte "Para eliminar un punto de control" en la página 168 para obtener instrucciones acerca de cómo eliminar los puntos de control.

Nota – Los volúmenes compatibles con la característica de aplicación obligatoria no pueden eliminarse, como tampoco los volúmenes que estén desconectados.

▼ Para eliminar un volumen de archivo o un segmento

1. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Delete File Volumes (Eliminar volúmenes de archivo).**
2. **Seleccione el segmento o el volumen de archivo que desee eliminar.**
3. **Haga clic en Apply (Aplicar).**

Visualización de particiones de volúmenes

El panel View Volume Partitions (Ver particiones de volúmenes) es una pantalla de sólo lectura de los LUN definidos para el clúster o el dispositivo dispositivo Sun StorEdge 5310 NAS.

▼ Para ver las particiones de los volúmenes

1. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > View Volume Partitions (Ver particiones de volúmenes).**

2. **En la lista Volumes (Volúmenes), seleccione el volumen cuyas particiones desea ver.**

   Se muestra la siguiente información acerca del volumen seleccionado.

Campo	Descripción
LUN	Enumera todos los LUN del volumen de archivo seleccionado.
Partition (Partición)	Muestra las particiones del volumen de archivo seleccionado.
Use (Uso)	Muestra el porcentaje de la partición que está en uso.
Type (Tipo)	Muestra el tipo de partición, que puede ser sfs2 (primaria) o sfs2ext (segmento).
Free (Libre)	Muestra la cantidad de espacio sin utilizar de la partición.
Capacity (Capacidad)	Muestra el tamaño total de la partición.
Requests (Solicitudes)	Muestra el número total de solicitudes procesadas para la partición.
Active (Activa)	Indica las solicitudes activas que no se han procesado todavía para la partición.

Configuración de iSCSI

Es posible configurar el sistema para que utilice el protocolo iSCSI (Internet Small Computer Systems Interface) a fin de transportar datos desde las aplicaciones de host al dispositivo Sun StorEdge 5310. El protocolo iSCSI transporta comandos, datos y el estado de SCSI en redes TCP/IP. Cuando se habilita iSCSI, las aplicaciones de host pueden almacenar datos en el dispositivo Sun StorEdge 5310.

En un entorno de iSCSI, el dispositivo Sun StorEdge 5310 NAS actúa como destino SCSI para un cliente con iniciador iSCSI. Cada iniciador y destino iSCSI tiene un identificador exclusivo permanente. El identificador del iniciador iSCSI se genera por el software de iSCSI en el host. El destino iSCSI admite tanto identificadores EUI (del inglés Enterprise Unique Identifier, identificador exclusivo de empresa) como identificadores IQN (iSCSI Qualified Name, nombre calificado de iSCSI).

Configuración de un destino iSCSI

La configuración de un destino iSCSI para su conexión y acceso requiere que se efectúen los siguientes pasos:

- Configure el cliente del iniciador iSCSI (consulte la documentación proporcionada con el software del iniciador iSCSI).
- Cree una lista de acceso para que el iniciador iSCSI puede acceder al destino.
- Cree un LUN y asigne acceso al iniciador iSCSI a ese LUN.
- Configure el método de detección del destino y el iniciador iSCSI.

El destino iSCSI que está implementado en el dispositivo Sun StorEdge 5310 NAS se basa en la norma iSCSI RFC 3720 desarrollada por la Internet Engineering Task Force (IETF). El protocolo admitido incluye procesamiento de encabezados, el protocolo CHAP (Challenge Handshake Authentication Protocol) de iniciador, y recuperación de errores de nivel 0.

Configuración de acceso del iniciador iSCSI

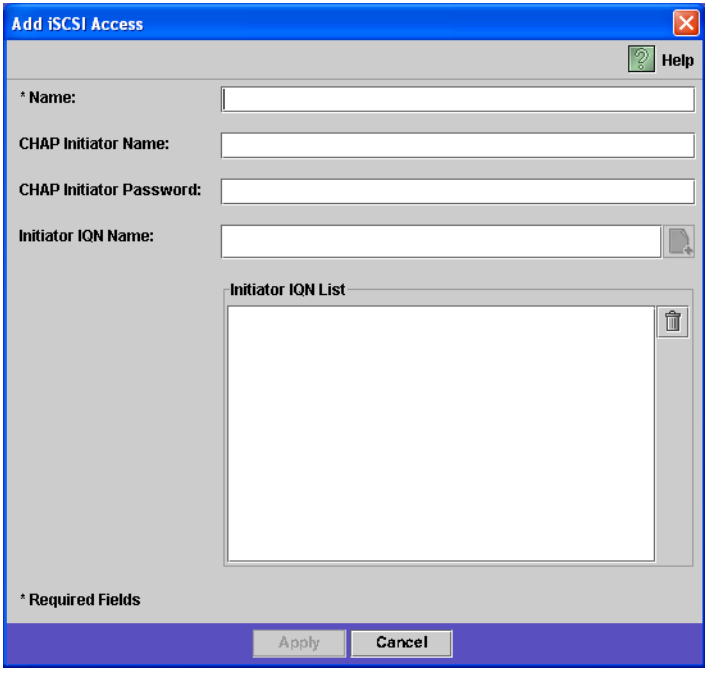
Puede definir los iniciadores iSCSI que tienen acceso a un LUN si crea una lista de acceso de iSCSI. La lista de acceso puede incluir uno o más iniciadores iSCSI y como opción, un iniciador CHAP y una contraseña. El protocolo CHAP garantiza que los datos se envían desde un iniciador iSCSI auténtico.

Precaución – Es posible configurar más de un iniciador iSCSI para acceder al LUN del mismo destino iSCSI. Sin embargo, la aplicación (clúster o base de datos) que se esté ejecutando en el servidor cliente del iniciador iSCSI debe ofrecer un acceso sincronizado para evitar que se corrompan los datos.

▼ Para crear una lista de acceso de iSCSI

1. **En el panel de navegación, seleccione iSCSI Configuration (Configuración de iSCSI) > Configure Access List (Configurar lista de acceso).**
2. **Para crear una lista de acceso, haga clic en Add (Agregar).**

   Se muestra el cuadro de diálogo Add iSCSI LUN (Agregar LUN iSCSI).



3. **Escriba la siguiente información:**

Campo	Descripción
Name (Nombre)	Escriba un nombre para la lista de acceso. Este nombre puede consistir en uno o más caracteres alfanuméricos (a–z, A–Z, 0–9) además del punto (.), guión (-) y dos puntos (:). Por ejemplo, `iscsiwinxp` es un nombre de lista de acceso válido.
CHAP Initiator Name (Nombre de iniciador CHAP)	Escriba el nombre completo del iniciador CHAP que está configurado por el software del iniciador de iSCSI. El nombre predeterminado de iniciador CHAP para un cliente iSCSI de Windows es: `iqn.1991-05.com.microsoft:iscsi-winxp` Si deja este campo en blanco, no se requerirá la autorización de CHAP. Consulte la documentación del iniciador iSCSI para obtener más información.
CHAP Initiator Password (Contraseña de iniciador CHAP)	Si ha especificado el nombre de iniciador CHAP, escriba la contraseña para este iniciador.
Initiator IQN Name (Nombre de iniciador IQN)	Escriba el nombre para el iniciador IQN y haga clic en el botón Add (Agregar) para agregar el iniciador a la lista. Si deja este campo en blanco, todos los iniciadores tendrán acceso al destino. El nombre puede consistir en uno o más caracteres alfanuméricos (a–z, A–Z, 0–9) además del punto (.), guión (-) y dos puntos (:). Para borrar un iniciador IQN de la lista, seleccione el nombre y haga clic en el botón Trash (Papelera).

4. **Para guardar la configuración, haga clic en Apply (Aplicar).**

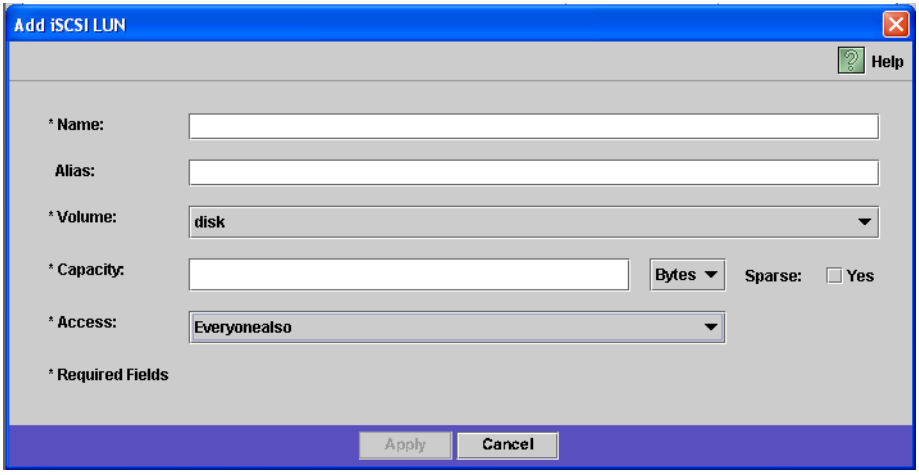
   Puede editar la lista de acceso de iSCSI si selecciona uno de los nombres de la lista y hace clic en Edit (Editar), o haciendo doble clic en ese nombre. Cambie los campos de texto que sea necesario y haga clic en Apply (Aplicar) para guardar la configuración.

▼ Para crear un LUN iSCSI

1. **En el panel de navegación, seleccione iSCSI Configuration (Configuración de iSCSI) > Configure iSCSI LUN (Configurar LUN iSCSI).**

2. **Para agregar un LUN de iSCSI a la lista, haga clic en Add (Agregar).**

   Se muestra el cuadro de diálogo Add iSCSI LUN (Agregar LUN iSCSI).



3. **Escriba la siguiente información para el LUN iSCSI:**

Campo	Descripción
Name (Nombre)	Escriba un nombre para el LUN iSCSI. El nombre puede consistir en uno o más caracteres alfanuméricos (a–z, A–Z, 0–9) además de un punto (.), guión (-) o dos puntos (:). El nombre de destino que se utilice tendrá como prefijo el nombre de IQN completo, que sigue esta convención de nomenclatura: `iqn.1986-03.com.sun:01:mac-address.timestamp.`*`nombre-especificado-usuario`* Por ejemplo, si escribe el nombre `lun1`, el LUN del destino iSCSI tendrá este nombre completo: `iqn.1986-03.com.sun:01:`*`dirección-mac.marca-de-tiempo`*`.lun1` Nota: la marca de tiempo es un número hexadecimal que representa el número de segundos después de la fecha 1/1/1970.
Alias (Alias)	Optativo. Escriba una breve descripción del destino.
Volume (Volumen)	Seleccione el nombre del volumen en que desea crear el LUN iSCSI.

Campo	Descripción
Capacity (Capacidad)	Especifique el tamaño máximo del LUN en bytes, KB, MB o GB.
Sparse (Sin densidad)	Marque la casilla Yes (Sí) cuando desee crear un LUN sin densidad. El LUN sin densidad define el atributo de tamaño de archivo en la capacidad especificada, aunque los bloques del disco no se asignan hasta que se escriben los datos en el disco. Si desea obtener más información, consulte "Nociones básicas sobre los LUN iSCSI sin densidad" en la página 58. Si se crea un LUN denso, los bloques del disco se asignarán dependiendo de la capacidad del LUN creado. Cuando se creen LUN iSCSI densos, deje aproximadamente un 10% del espacio del volumen para los metadatos del sistema de archivos. Por ejemplo, un LUN iSCSI de 100 GB debería residir en un volumen con espacio de 110 GB para que se creara el LUN denso. Si desea obtener más información para decidir si utilizar LUN sin densidad o densos, consulte "Nociones básicas sobre los LUN iSCSI sin densidad" en la página 58.
Access (Acceso)	Seleccione la lista de acceso (creada previamente) para este LUN en la lista desplegable.

4. **Para guardar la configuración, haga clic en Apply (Aplicar).**

Nociones básicas sobre los LUN iSCSI sin densidad

Como regla general, utilice los LUN densos siempre que esté disponible la suficiente capacidad de almacenamiento.

Los LUN iSCSI sin densidad no resultan útiles en todas las situaciones. Cuando se crea un LUN sin densidad, el espacio de disco no queda reservado antes del uso. Los LUN sin densidad son útiles cuando se ha previsto crear varios LUN que no van a utilizar toda su capacidad. Por ejemplo, si tiene previsto que cinco LUN iSCSI de 100 GB cada uno hagan uso sólo del 55% de su capacidad, puede crearlos todos en un volumen que tenga 5*100*0,55=275 GB, con algo más de espacio para crecer (50 TB) = 325 GB.

De acuerdo con este modelo, puede supervisar el uso dado al volumen y asignarle espacio adicional antes de que se llene por completo. Si se ha previsto que para el LUN iSCSI se requerirá utilizar la mayor parte del tamaño disponible, no debe utilizar la opción de LUN sin densidad. Algunos entornos operativos no pueden manejar correctamente la falta de espacio con un LUN sin densidad, por lo que habrá que evitar que el espacio se agote para mantener el rendimiento óptimo del sistema.

Métodos de detección del destino SCSI

Puede configurar el modo en que un iniciador iSCSI detecta el destino iSCSI con uno de los siguientes métodos:

- Configuración estática: escriba manualmente la dirección IP y el nombre de destino iSCSI en el host del iniciador iSCSI. Consulte la documentación del software del iniciador iSCSI para obtener más información.
- Solicitud SendTargets: añada la dirección IP o nombre DNS de portal del destino iSCSI a la configuración del iniciador iSCSI. El iniciador enviará una solicitud SendTargets para detectar la lista de destinos iSCSI con acceso en el portal del destino en cuestión. Consulte la documentación del software del iniciador iSCSI para obtener más información.
- Servidor iSNS (Internet Storage Name Service): configure un servidor iSNS para automatizar la detección tanto de los iniciadores como los destinos iSCSI. Este servidor permite que los iniciadores iSCSI detecten la existencia, ubicación y configuración de los destinos iSCSI. El cliente de iSNS es una función opcional que se puede configurar con la interfaz gráfica de Web Administrator como se describe en la sección a continuación.

Configuración de un servidor iSNS

Para habilitar un servidor iSNS, debe especificar la dirección IP o el nombre DNS (del inglés Domain Name Service, servicio de nombre de dominio) de dicho servidor. El cliente de iSNS puede operar con cualquier implementación estándar de servidor iSNS, como por ejemplo, Microsoft iSNS Server 3.0.

Consulte la documentación del servidor iSNS y el iniciador iSCSI para obtener más información.

▼ Para especificar el servidor iSNS

1. **En el panel de navegación, seleccione iSCSI Configuration (Configuración de iSCSI) > Configure iSNS Server (Configurar servidor iSNS).**
2. **Escriba la dirección IP o el nombre DNS del servidor iSNS y, a continuación, haga clic en Apply (Aplicar).**

   También puede cambiar el nombre del servidor iSNS si escribe una dirección IP o nombre DNS distintos en el campo iSNS Server (Servidor iSNS) y hace clic en Apply (Aplicar).

Qué debe hacer a continuación

En este momento, el sistema de archivos y los destinos iSCSI están configurados y listos para el uso. Ahora, debe configurar los privilegios de acceso, las cuotas y las estructuras de directorio que necesite. Estas funciones de gestión se describen al principio del Capítulo 4.

Las funciones de supervisión, que son fundamentales para gestionar los recursos, se tratan en el Capítulo 10. Las funciones de mantenimiento (como las copias de seguridad y las tareas de restauración) se describen en el Capítulo 11.

CAPÍTULO 4

Gestión del sistema

Este capítulo describe varias funciones básicas para la gestión del sistema. Muchas de estas funciones se utilizan sobre todo durante la configuración inicial del sistema, aunque siguen estando disponibles por si necesita restablecerlas.

Las funciones de gestión del sistema incluyen:

- "Definición de la contraseña del administrador" en la página 61
- "Control de la hora y la fecha" en la página 62
- "Uso de software antivirus" en la página 65

Definición de la contraseña del administrador

De forma predeterminada, el administrador del sistema no tiene una contraseña. Puede definir una si lo desea.

▼ Para definir la contraseña del administrador

1. **En el panel de navegación, seleccione System Operations (Operaciones de sistema) > Set Administrator Password (Configurar contraseña del administrador).**
2. **Escriba la contraseña antigua (si existe) en el campo Old Password (Contraseña antigua).**

   Si no hay ninguna contraseña previa, deje este campo en blanco.
3. **Escriba la contraseña nueva en el campo New Password (Contraseña nueva).**

   La contraseña debe tener entre 1 y 21 caracteres. No hay restricciones en cuanto al tipo de caracteres.

4. **Escriba otra vez la contraseña nueva en el campo Confirm Password (Confirmar contraseña).**

   Si desea deshabilitar las contraseñas, deje en blanco los campos New Password (Contraseña nueva) y **Confirm Password** (Confirmar contraseña).

5. **Para guardar los cambios, haga clic en Apply (Aplicar).**

Control de la hora y la fecha

Controlar la fecha y la hora en el sistema es fundamental para la gestión de los archivos. Esta sección describe las funciones disponibles para mantener la fecha y hora correctas.

Puede utilizar la sincronización de la hora o establecer la hora manualmente.

Nota – La primera vez que configura la fecha y la hora, también inicializa el *reloj seguro* del sistema. El software de administración de licencias y Compliance Archiving Software usan este reloj para controlar las operaciones que dependen del tiempo.

Precaución – Una vez inicializado el reloj seguro, no puede restablecerse. Por ello, es importante que defina la fecha y la hora con precisión al configurar el sistema.

Sincronización de la hora

El sistema admite dos tipos de sincronización de la hora: Protocolo de hora de red (NTP, del inglés Network Time Protocol) y protocolo de hora RDATE. Puede configurar el sistema para que sincronice la hora con NTP o con un servidor RDATE.

- NTP es un protocolo de Internet que se emplea para sincronizar los relojes de los equipos con una fuente de referencia para la hora, que puede ser un receptor de radio, de satélite o un módem. Las configuraciones NTP habituales tienen varios servidores redundantes y diversas rutas de red para conseguir una gran precisión y fiabilidad.
- El protocolo de hora RDATE proporciona una fecha y hora independientes del sitio. RDATE puede obtener la hora de otro equipo de la red. Los servidores RDATE se utilizan normalmente en sistemas UNIX y permiten sincronizar la hora del sistema con la hora del servidor RDATE.

Existe un tercer método, llamado de “sincronización manual”, que permite deshabilitar la sincronización de la hora. Con este método, el administrador define la hora del sistema y controla la hora con independencia de los demás nodos de la red.

Configuración de la sincronización de la hora

Puede configurar el método que desee para sincronizar la hora en el panel **Set Up Time Synchronization** (Configurar la sincronización de la hora).

▼ Para configurar la sincronización de la hora

1. **En el panel de navegación, seleccione System Operations (Operaciones de sistema) > Set Up Time Synchronization (Configurar la sincronización de la hora).**
2. **Elija una de estas tres opciones:**
   - **Manual Synchronization** (Sincronización manual): seleccione esta opción si no desea utilizar la sincronización de hora NTP o RDATE.
   - **NTP Synchronization** (Sincronización NTP): cuando desee utilizar la sincronización NTP y disponga de un servidor NTP en la red, como mínimo, seleccione esta opción e introduzca la siguiente información:
     - **Enable Server 1** (Habilitar servidor 1): para habilitar un servidor NTP, seleccione esta casilla de verificación y aporte la información necesaria en los campos correspondientes. Repita el procedimiento con un segundo servidor NTP, si procede. Puede configurar dos servidores NTP como máximo.
     - **Enable Server 2** (Habilitar servidor 2): para habilitar un segundo servidor NTP (o uno alternativo), seleccione esta casilla de verificación y aporte la información necesaria en los campos correspondientes. Puede configurar dos servidores NTP como máximo.
     - **NTP Server** (Servidor NTP): especifique el nombre o la dirección IP del servidor NTP al que recurrirá el sistema para obtener la hora actual.
     - **Auth Type** (Tipo de autenticación): la posibilidad de utilizar autenticación hace que el sistema pueda verificar que el servidor es conocido y de confianza mediante una clave y un identificador de clave. La clave y el identificador de clave del servidor NTP y del sistema deben coincidir para que se puedan autentificar sus mensajes. Elija el tipo de autenticación que desee usar, que puede ser **None** (Ninguna), para que no se use ningún esquema de autenticación, o **Symmetric Key** (Clave simétrica).
     - **Key ID** (ID de clave): si ha seleccionado **Symmetric Key** (Clave simétrica) como esquema de autenticación en el campo previo, escriba el identificador de clave para el servidor NTP. El valor debe estar comprendido entre **1** y **65534**.
     - **Min Poll Rate** (Frecuencia mínima de consulta): especifique la frecuencia mínima con que se deben consultar los mensajes NTP. Este valor, elevado a la segunda potencia, es el número mínimo de segundos para el intervalo de consulta. Por ejemplo, si especifica 4, significa que las consultas se efectuarán cada 16 segundos como mínimo. El valor de este campo debe estar entre **4** y **17**.
     - **Max Poll Rate** (Frecuencia máxima de consulta): especifique la frecuencia máxima con que se deben consultar los mensajes NTP. Este valor, elevado a la segunda potencia, es el número máximo de segundos para el intervalo de consulta. Por ejemplo, si especifica 4, significa que las consultas se efectuarán cada 16 segundos como máximo. El valor de este campo debe estar entre **4** y **17** y debe ser superior al valor especificado en el intervalo mínimo de consulta.

- **Enable Broadcast Client** (Habilitar cliente de difusión): marque esta casilla de verificación para que el sistema responda a los mensajes de difusión recibidos desde cualquier interfaz. Esta función está pensada para configuraciones que involucren uno o varios servidores NTP y que tengan un gran número de clientes que soliciten sincronizaciones de hora.
- **Require Broadcast Server Authentication** (Requerir autenticación del servidor de difusión): seleccione esta casilla para que el cliente NTP compruebe que el servidor que tiene mensajes de difusión para el sistema es un servidor conocido y de confianza.

- **RDATE Synchronization** (Sincronización RDATE): para configurar el servidor RDATE y la ventana de tolerancia, active esta casilla de verificación y escriba los siguientes datos:
  - **RDATE Server** (Servidor RDATE): escriba el nombre o la dirección IP del servidor RDATE.
  - **Tolerance** (Tolerancia): especifique el nivel máximo de tolerancia permitido para la hora recibida del servidor RDATE, que puede oscilar entre **0** y **3600** segundos. Si la hora del sistema tiene una diferencia con la hora del servidor RDATE de una cantidad de segundos menor a la indicada (+ o –), la hora del sistema se sincroniza con la hora del servidor RDATE. Si la diferencia es mayor, la hora del sistema no se sincroniza automáticamente con el servidor RDATE. Esta comprobación se produce todos los días a las 11:45 PM.

3. **Para guardar los cambios, haga clic en Apply (Aplicar).**

Configuración de la fecha y la hora manualmente

Si no utiliza la sincronización de hora, puede establecer la hora y la fecha manualmente.

▼ Para configurar la fecha y la hora manualmente

1. **En el panel de navegación, seleccione System Operations (Operaciones de sistema) > Set Time and Date (Configurar la fecha y la hora).**
2. **Seleccione el año correcto en el cuadro de menú desplegable situado a la izquierda encima del calendario.**
3. **Seleccione el mes correcto en el cuadro de menú desplegable situado a la derecha, encima del calendario.**
4. **Haga clic en la fecha correcta en el calendario.**
5. **Seleccione la hora correcta en el cuadro de lista desplegable situado a la izquierda encima del reloj. Los valores posibles oscilan entre 0 (medianoche) y 23 (11:00 PM).**

6. **Seleccione el minuto correcto (entre 0 y 59) en el cuadro de menú desplegable situado a la derecha encima del reloj.**

7. **Elija la zona horaria que proceda en el menú desplegable de la parte inferior de la pantalla.**

   Al seleccionar la zona horaria correcta, el sistema puede ajustar automáticamente la configuración del horario de verano.

8. **Para guardar las preferencias de fecha y hora, haga clic en Apply (Aplicar).**

Nota – Si es la primera vez que define la hora y la fecha en el sistema, este procedimiento configurará el reloj seguro con la misma información. Compruebe que define la hora y la fecha con precisión ya que puede configurar el reloj seguro una sola vez.

Uso de software antivirus

La protección antivirus se encuentra disponible mediante conexiones ICAP (del inglés Internet Content Adaptation Protocol, protocolo de adaptación de contenido) a "motores de búsqueda" que estén instalados en la red. Cuando se habilita la protección antivirus en el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310, el sistema se convierte en cliente del motor antivirus utilizado en la red.

Nota – Si se configura la protección antivirus del sistema, en necesario tener en todo momento al menos un motor de búsqueda operativo, o los clientes de Windows pueden quedar sin acceso.

▼ Para habilitar la protección antivirus

1. **En el panel de navegación, seleccione Configure Anti Virus (Configurar antivirus).**
2. **Marque la casilla de verificación Enable Anti Virus (Habilitar antivirus).**

Nota – Si necesita desactivar por el momento la protección antivirus, utilice la opción Scanning Suspended (Exploración suspendida), en vez de desactivar la casilla de verificación Enable Anti Virus (Habilitar antivirus).

---

3. **Seleccione el modo de exploración.**

Modo de exploración	Descripción
Scanning Suspended (Exploración suspendida)	Seleccione esta opción para suspender temporalmente la protección antivirus. Nota: la protección antivirus no tiene actividad cuando se selecciona esta opción.
Scan after Modify (Explorar al modificar)	Seleccione esta opción para que la exploración tenga lugar después de modificar cualquier archivo. Esta opción equilibra el rendimiento con la calidad de la protección antivirus y proporciona un rápido acceso de lectura, con protección antivirus sólo en el momento que se modifican los archivos. Cuando más adelante se acceda a esos archivos, no se tendrán en cuenta posibles cambios en las definiciones de virus.
Scan all Access (Explorar todo acceso)	Seleccione esta opción para que la exploración se realice después de un acceso del sistema. Esta opción ofrece la máxima protección contra virus, ya que permite acceder sólo a los datos analizados con las definiciones de virus más recientes.

4. **Escriba la dirección TCP/IP del motor de búsqueda que desee utilizar.**
5. **Introduzca el número de puerto TCP/IP por el que el servidor ICAP intenta detectar las conexiones; normalmente es el puerto 1344.**
6. **Especifique el número máximo de operaciones de exploración concurrentes de los archivos que el sistema expedirá al motor de búsqueda; el número típico es 2.**

7. **Especifique lo que se incluye o excluye en cada exploración seleccionando las opciones que se describen en la lista.**

Especificación	Descripción	Formato
File Types Included (Tipos de archivo incluidos)	Deje en blanco para incluir todos, o seleccione la extensión de cada tipo de archivo que incluirá la exploración.	Tres o menos caracteres. El signo ? sirve como comodín.
File Types Excluded (Tipos de archivo excluidos)	Seleccione la extensión de cada tipo de archivo que se excluirá en la exploración.	Tres o menos caracteres. El signo ? sirve como comodín.
Exempt Clients (Clientes exentos)	Nombre o dirección IP de cada cliente exento de la exploración.	
Exempt Groups (Grupos exentos)	Nombre de cada grupo de Windows/NT o grupo de directorio activo de Windows (no grupos de UNIX) exento de la exploración.	Puede incluir espacios.
Exempt Shares (Recursos compartidos exentos)	Nombre de cada recurso compartido del sistema de archivos comunes de Internet (CIFS) exento de la exploración. Nota: los recursos compartidos administrativos (`X$`) siempre se eximen de la exploración.	

Para agregar un elemento nuevo a la lista, escríbalo en el cuadro y haga clic en **Add** (Agregar).

Para quitar un elemento de la lista, selecciónelo y haga clic en **Remove** (Eliminar).

8. **Para guardar las preferencias, haga clic en Apply (Aplicar).**

Nota – Los archivos que están en la memoria no se someten a exploración. El mejor modo de habilitar por completo la exploración antivirus consiste en reiniciar el sistema.

Exploración antivirus

Con el funcionamiento normal, los usuarios de clientes CIFS pueden observar un ligero retraso cuando sucede la exploración contra virus; en particular, cuando se ha seleccionado la opción Scan all Access (Explorar todo acceso).

Cuando se detecta un virus, en el registro del sistema se agrega una entrada con el nombre del archivo infectado, el nombre del virus, y la disposición elegida para ese archivo. En muchos casos, esta disposición consiste en dejar el archivo infectado en "cuarentena" y denegar el acceso al cliente de CIFS. Los archivos en cuarentena se pueden ver en el directorio `/quarantine` de la raíz del sistema de archivos que contenga el archivo infectado. Con objeto de evitar conflictos de nombre en el directorio `/quarantine`, los archivos reciben nombres basados en un "número interno": *NNNNNN*`.vir` es un "vínculo fuerte" al archivo infectado, y *NNNNNN*`.log` es un archivo de texto que contiene el nombre original del archivo infectado con los datos de las infecciones detectadas.

Nota – De forma predeterminada, únicamente el administrador (o el superusuario de UNIX) pueden ver el contenido de los directorios `/quarantine`.

El modo de recuperación más sencillo consiste en borrar los archivos infectados (encuarentena).

▼ Para borrar los archivos en cuarentena

1. **Determine el nombre original utilizando el registro del sistema o el archivo *NNNNNN*`.log` del directorio de cuarentena, y borre esos archivos si todavía existen.**
2. **Examine en el directorio de cuarentena los dos archivos** *NNNNNN*`.vir` **y** *NNNNNN*`.log` **que correspondan al archivo infectado y bórrelos también.**

CAPÍTULO 5

Gestión de los puertos de sistema

Este capítulo describe los puertos de red y las direcciones IP alias. Puede enlazar dos o más puertos para crear un puerto enlazado. Un puerto de este tipo tiene un ancho de banda superior al de los puertos que lo componen.

Está dividido en las siguientes secciones:

- "Gestión de los puertos de sistema" en la página 69
- "Acerca de las direcciones IP alias" en la página 70
- "Puertos enlazados" en la página 71

Ubicaciones de los puertos

El dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310 identifican los puertos siguiendo un orden predefinido que se basa en el tipo de puerto y en su ubicación física y lógica en el servidor. Consulte la *Guía básica del sistema de puerta de enlace y el dispositivo Sun StorEdge 5310 NAS* para identificar las ubicaciones de los puertos del sistema.

Cada puerto debe tener asignada una función. Las funciones posibles son:

- **Primary** (Principal): si se asigna esta función a un puerto, significa que es el puerto de red activo. Como mínimo, uno de los puertos debe estar configurado como principal. El puerto principal es una parte integrante del proceso de recuperación tras error. Cuando asigna esta función a un puerto, el servidor asociado (servidor H2) gestiona las direcciones IP asignadas al puerto principal como una dirección IP alias de copia de seguridad no conectada. Se produce el proceso inverso cuando proporciona una dirección IP alias en el servidor asociado. La dirección IP asociada se mantiene como una dirección IP alias de copia de seguridad por el servidor principal (servidor H1). En caso de que se produzca una recuperación tras error, el servidor en funcionamiento activa las direcciones IP alias del servidor asociado, lo que permite continuar el acceso a la red como si el servidor que ha fallado estuviera activo.

Nota – Como mínimo, uno de los puertos de cada servidor debe tener asignada una función principal.

- Independent (Independiente): identifica un puerto de red activo que se utiliza para otros fines que proporcionar datos; por ejemplo, para copias de seguridad. En el clúster Sun StorEdge 5310, el puerto independiente no participa en el proceso de recuperación tras error. Los puertos independientes se utilizan normalmente para la copia de seguridad remota. No puede vincular (agregar) puertos independientes o agregar direcciones IP alias a ellos. Puede asignar cualquier número de funciones de puertos, pero debería asignar únicamente uno por unidad.
- Mirror (Duplicar): muestra que el puerto conecta este servidor con otro servidor para duplicar los volúmenes de archivo. Utilice el mismo puerto en los servidores de origen y de destino para la duplicación. Para obtener más información acerca de la duplicación, consulte "Sun StorEdge File Replicator" en la página 121.
- Private (Privado): (clúster StorEdge 5310 sólo) el puerto Private se reserva para la conexión privada, un puerto dedicado que supervisa constantemente el estado de la otra unidad.

Acerca de las direcciones IP alias

La función de alias de IP es una función de red que permite asignar varias direcciones IP a un mismo puerto. Todos los alias de IP del puerto seleccionado deben estar en la misma red física y deben compartir la misma *máscara de red* y *dirección de difusión* como la primera, o principal, dirección IP especificada en el puerto seleccionado.

Para los usuarios de un solo servidor (unidad), puede agregar hasta nueve direcciones IP alias a la dirección IP principal de cada puerto. En consecuencia, una tarjeta de interfaz de red (NIC) con dos puertos puede proporcionar hasta 20 direcciones IP para utilizarlas.

En un sistema de clúster Sun StorEdge 5310, la función de alias de IP está integrada en el proceso de recuperación tras error. En un sistema de doble unidad puede agregar hasta cuatro direcciones IP alias a la dirección IP principal de cada puerto. Las otras posiciones de alias de IP se reservan para realizar copias de seguridad de las direcciones IP principal y alias de los puertos principal y duplicado en el servidor asociado. En el caso de una recuperación de unidad tras error, el servidor en funcionamiento activa estas direcciones IP de seguridad reservadas, lo que permite continuar el acceso a la red con una mínima interrupción. Consulte "Habilitar la recuperación de unidad tras error" en la página 16 para obtener información sobre la recuperación tras error de las unidades.

En el caso de sistemas de dos servidores, puede agregar direcciones IP alias únicamente a los puertos que tienen asignados una función principal. Las opciones de funciones se describen en "Gestión de los puertos de sistema" en la página 69.

Nota – No confunda la función principal con la dirección IP principal. La función principal es una asignación que indica cómo funciona el puerto en un sistema de clúster Sun StorEdge 5310. La dirección IP principal es la primera dirección asignada a un puerto seleccionado. En Web Administrator, la dirección IP principal se muestra en el panel Network Configuration (Configuración de red) > Configure TCP/IP (Configurar TCP/IP) > Configure Network Adapters (Configurar adaptadores de red). Puede seleccionar la función de puerto en la parte inferior de la pantalla.

Puertos enlazados

Hay dos formas de enlazar puertos: adición de puertos y alta disponibilidad. La modalidad de adición de puertos combina dos o más puertos adyacentes para crear un puerto más rápido y con un ancho de banda mayor, mientras que el modo de alta disponibilidad combina dos o más puertos para proporcionar servicios de recuperación ante fallos para puertos NIC o puertos de copia de seguridad.

Nota – El dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310 son compatibles con el enlazado Etherchannel, un subgrupo de la especificación 802.3ad. Consulte la documentación del conmutador sobre el enlazado Etherchannel antes de configurar los puertos enlazados.

Un sistema puede tener hasta cuatro enlaces de cualquier tipo. Cada enlace puede tener seis puertos.

Enlaces de adición de puertos

Los enlaces de adición de puertos (también conocidos como "enlaces de canales", "adición" o "agrupamiento") le permiten escalar las E/S de red, puesto que unen puertos adyacentes. De esta forma, se crea un único canal de red de banda ancha a partir de dos o más canales con un ancho de banda inferior.

Un enlace de adición requiere como mínimo que haya dos puertos disponibles. Los puertos también deben estar en el mismo tipo de interfaz (por ejemplo, una interfaz rápida de Ethernet con Fast Ethernet), deben estar conectados a la misma subred y deben estar conectados a puertos adyacentes del mismo conmutador de red.

Nota – El conmutador conectado a los puertos configurados para los enlaces de canales deben admitir la adición de enlaces IEEE 802.3ad. Consulte la documentación del conmutador LAN para obtener más información acerca de cómo configurar esta función.

Enlaces de alta disponibilidad

Los enlaces de puertos de alta disponibilidad proporcionan al sistema funciones de recuperación ante fallos de los puertos. Se enlazan dos o más puertos para que si el principal falla, haya un segundo puerto que asuma automáticamente la función de puerto principal para que los servicios puedan continuar sin ninguna interrupción.

En un enlace de este tipo, se requieren como mínimo dos puertos. Sin embargo, no es necesario que estén en la misma tarjeta de interfaz, ni que estén conectados a puertos adyacentes.

Nota – En un enlace de alta disponibilidad se puede utilizar cualquier tipo de conmutadores. El único requisito es que los conmutadores deben estar conectados a la misma subred.

Puertos enlazados en un sistema de un servidor

Esta sección describe cómo enlazar puertos para un sistema de un solo servidor.

Los puertos se pueden enlazar después de configurarlos. Sin embargo, es posible que cambien las direcciones IP alias y otros aspectos de la configuración original. Después de crear un enlace de puerto, deberá volver a "Configuración de los puertos de red" en la página 18 para configurarlo. Una vez que haya enlazado dos o más puertos, no se podrán agregar direcciones IP alias a los puertos individuales: sólo se podrán agregar al puerto enlazado.

▼ Para enlazar puertos en el sistema de un servidor

1. **En el panel de navegación, seleccione Network Configuration (Configuración de red) > Bond NIC Ports (Enlazar puertos NIC).**
2. **Haga clic en Create (Crear).**

3. **Haga clic en Port Aggregation (Adición de puertos) o en High Availability (Alta disponibilidad) para indicar el tipo de enlace que desea crear.**

4. **Elija, como mínimo, dos puertos disponibles para enlazarlos. Para ello, haga clic en los puertos que desee del cuadro Available NIC Ports (Puertos NIC disponibles) y, a continuación, haga clic en > para agregarlos a la lista NIC Ports in This Bond (Puertos NIC de este enlace).**

   Si elige Port Aggregation (Adición de puertos) en el paso 3, deberá elegir los puertos que tengan el mismo tipo de interfaz y que estén conectados a puertos adyacentes.

   Para eliminar un puerto de la lista, selecciónelo y haga clic en <.

5. **Escriba la información necesaria en los campos IP Address (Dirección IP), Subnet Mask (Máscara de subred) y Broadcast Address (Dirección de difusión).**

   De forma predeterminada, estos campos contienen información del puerto principal, que es el primero que aparece en el cuadro NIC Ports in This Bond (Puertos NIC de este enlace).

6. **Haga clic en Apply (Aplicar) para completar el proceso de enlace de los puertos. Web Administrator le pide que confirme el reinicio automático.**

   Después del reinicio, todas las direcciones IP alias se habrán eliminado de los puertos en el enlace.

   Para agregar direcciones IP alias al enlace de puertos, consulte "Para configurar los adaptadores de red" en la página 19.

Puertos enlazados en el sistema de clúster Sun StorEdge 5310

Para enlazar puertos en sistemas de doble unidad, sólo necesitará completar el siguiente procedimiento en uno de los servidores. Todos los puertos enlazados deben ser del mismo tipo (por ejemplo, una interfaz rápida de Ethernet con Fast Ethernet), deben estar conectados a la misma subred y deben estar conectados a puertos adyacentes del mismo conmutador de red. El sistema se reinicia automáticamente después de cada enlace de puertos.

Los puertos se pueden enlazar después de configurarlos. Sin embargo, es posible que cambien las direcciones IP alias y otros aspectos de la configuración original. Después de crear un enlace de puerto, deberá volver a "Configuración de los puertos de red" en la página 18 para configurarlo.

Para obtener más información acerca de los puertos enlazados en sistemas de dos servidores, consulte "Ejemplo de enlaces de puertos en sistemas de dos servidores" en la página 75.

Nota – Sólo se pueden enlazar puertos con función principal. Para obtener más información acerca de las funciones de puertos, consulte "Gestión de los puertos de sistema" en la página 69.

▼ Para enlazar puertos en el sistema de dos servidores

1. **En el panel de navegación, seleccione Network Configuration (Configuración de red) > Bond NIC Ports (Enlazar puertos NIC).**
2. **Haga clic en Create (Crear).**
3. **Seleccione los puertos que desea enlazar en la lista Available NIC Ports (Puertos NIC disponibles), que muestra todos los puertos que no son parte de un enlace.**

   El cuadro de diálogo muestra la dirección IP, la máscara de subred y dirección de difusión del primer puerto en la lista.
4. **Seleccione un puerto y, a continuación, haga clic en > para agregarlo a la lista NIC Ports in This Bond (Puertos NIC en este enlace).**

   Para eliminar un puerto de la lista, selecciónelo y haga clic en <.

   Debe agregar al menos dos puertos a la lista. Todos los puertos en el enlace deben pertenecer a la misma subred.

   En el servidor asociado, los puertos correspondientes se enlazan también automáticamente después de hacer clic en Apply (Aplicar) y de que se reinicie el sistema. Por ejemplo, si enlaza los puertos 2 y 3 en el servidor H1, los puertos 2 y 3 en el servidor H2 también se enlazan.
5. **Haga clic en Apply (Aplicar) para terminar el proceso de enlace de puertos y reiniciar el sistema.**

   El sistema asigna automáticamente un ID de enlace al nuevo enlace de puertos. La dirección IP del enlace de puertos es la misma que la del primer puerto agregado al enlace.
6. **Para agregar direcciones IP alias al enlace de puertos, consulte "Para configurar los adaptadores de red" en la página 19.**

   Una vez que haya enlazado dos o más puertos, no se podrán agregar direcciones IP alias a los puertos individuales: sólo se podrán agregar al puerto enlazado.

Ejemplo de enlaces de puertos en sistemas de dos servidores

La FIGURA 5-1 ilustra un ejemplo de un sistema de clúster Sun StorEdge 5310 conectado a dos subredes distintas. Para mostrar todas las combinaciones posibles, este ejemplo muestra cada unidad con un puerto de conexión privada y cuatro puertos adicionales. Todos los puertos, excepto el de conexión privada, se han configurado con la función principal.

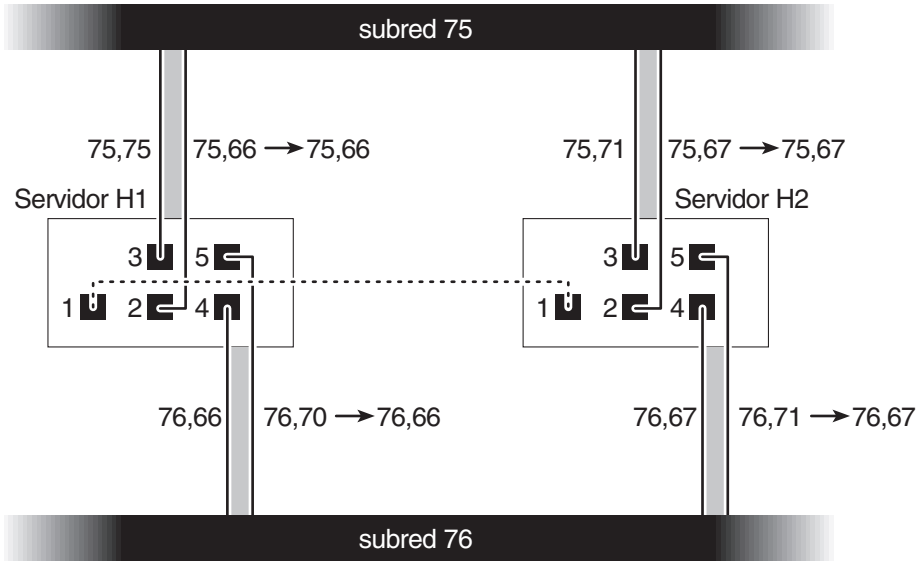


FIGURA 5-1 Enlaces de puertos en sistemas de dos servidores

Si los puertos 2 y 3 están enlazados, y los puertos 4 y 5 están enlazados, se producirá la configuración IP que se muestra en la TABLA 5-1.

TABLA 5-1 Ejemplo de enlaces de puertos en sistemas de dos servidores

	Puertos que se van a enlazar		Enlace de puertos		
Unidad	**Name**	**Dirección IP principal**	**Nombre**	**Dirección IP principal**	**Dirección IP de seguridad**
	Puerto 2	192.1xx.75.66	Enlace 1	192.1xx.75.66	192.1xx.75.67
	Puerto 3	192.1xx.75.70			
	Puerto 4	192.1xx.76.66	Enlace 2	192.1xx.76.66	192.1xx.76.67
1	Puerto 5	192.1xx.76.70			
	Puerto 2	192.1xx.75.67	Enlace 1	192.1xx.75.67	192.1xx.75.66
	Puerto 3	192.1xx.75.71			
	Puerto 4	192.1xx.76.67	Enlace 2	192.1xx.76.67	192.1xx.76.66
2	Puerto 5	192.1xx.76.71			

La dirección IP principal de cada puerto en el servidor H1 es la dirección IP de copia de seguridad del puerto correspondiente en el servidor 2, y viceversa.

En el caso de una recuperación tras error, el servidor en funcionamiento activa las direcciones IP del servidor que ha fallado. Puede agregar direcciones IP alias a la dirección IP principal de un enlace de puerto y a aquellas direcciones IP que participan en el procesos de recuperación tras error. Para obtener más información acerca de los alias de IP, consulte "Acerca de las direcciones IP alias" en la página 70.

CAPÍTULO 6

Servicio Active Directory y autenticación

En este capítulo se describen en detalle los servicios de Active Directory, la configuración del protocolo ligero de acceso a directorios (LDAP, del inglés Lightweight Directory Access Protocolo) y la forma de cambiar el orden de búsqueda de los servicios de nombres. Para obtener más información acerca de otros servicios de nombres, consulte "Servicios de nombres" en la página 21.

Las siguientes temas se describen en este capítulo:

- "Servicios de nombres admitidos" en la página 77
- "Servicio Active Directory" en la página 78
- "Configuración de LDAP" en la página 83
- "Cambio del orden de búsqueda de los servicios de nombres" en la página 84

Servicios de nombres admitidos

El sistema admite diferentes servicios de nombres tanto para redes de Windows como de UNIX. Dichos servicios de nombres incluyen:

- **ADS**: el Servicio Active Directory es un servicio de nombres de Windows 2000 integrado con el sistema de nombres de dominio (DNS). Consulte al respecto "Configuración de DNS" en la página 24. ADS se ejecuta sólo en los controladores de dominio. Además de almacenar los datos y hacer que estén disponibles, ADS protege los objetos de red para evitar accesos no autorizados y replica los objetos por la red para que los datos no se pierdan en caso de que falle un controlador de dominio. Cuando se habilita y configura ADS, el sistema realiza actualizaciones automáticas de este servicio Active Directory. Si desea obtener más información, consulte "Servicio Active Directory" en la página 78.

- **LDAP:** el protocolo ligero de acceso a directorios es un servicio de UNIX que habilita la autenticación.
- **WINS**: el servidor del sistema de nombres de Internet para Windows (WINS) convierte los nombres NetBIOS en direcciones IP, lo que permite que los equipos de la red puedan localizar otros dispositivos NetBIOS de forma rápida y eficaz. El servidor WINS realiza en los entornos Windows una función semejante a la que realiza el servidor DNS en los entornos UNIX. Si desea obtener más información, consulte "Configuración de WINS" en la página 23.
- **DNS**: el sistema de nombres de dominio traduce los nombres de dominio en direcciones IP para el sistema. Este servicio le permite identificar un servidor por su nombre o por su dirección IP. Si desea obtener más información, consulte "Configuración de DNS" en la página 24.
- **NIS**: Servicio de información de red, (del inglés Network Information Service) configura el sistema para importar la base de datos NIS. Administra el acceso a los recursos basándose en la información del host y del grupo de usuarios. Si desea obtener más información, consulte "Configuración de NIS" en la página 26.
- **NIS+**: Network Information Service Plus (NIS+) se ha creado para sustituir a NIS. NIS+ ofrece compatibilidad limitada a los clientes de NIS pero está pensado principalmente para resolver problemas que NIS no puede solucionar. NIS+ agrega, en líneas generales, credenciales y acceso seguro a la función NIS. Si desea obtener más información, consulte "Configuración de NIS+" en la página 27.

Servicio Active Directory

Para que el sistema se integre sin fisuras en un entorno Active Directory de Windows 2000, deben existir en la red los siguientes elementos:

- Un controlador de dominio de servidor de Windows 2000
- Aunque no es obligatorio para ejecutar ADS, se recomienda disponer de un servidor DNS integrado en Active Directory que permita las actualizaciones dinámicas (necesarias para utilizar la función de sistema de nombres de dominio dinámica).

Después de configurar el servicio Active Directory, puede realizar las acciones necesarias para que publique recursos compartidos específicos en el directorio ADS. Para ello, debe crear o actualizar recursos compartidos SMB y especificar el contenedor correspondiente para cada recurso compartido que desee publicar.

La configuración de ADS implica realizar las siguientes operaciones:

1. Habilitación del servicio Active Directory
2. Comprobación del orden de búsqueda de los servicios de nombres
3. Comprobación de que DNS está habilitado y configurado para admitir ADS
4. Publicación de recursos compartidos en ADS

▼ Para habilitar el servicio Active Directory

1. **En el panel de navegación, seleccione System Operations (Operaciones de sistema) > Set Time and Date (Configurar la fecha y la hora).**
2. **Compruebe que la diferencia de hora existente entre el sistema y los controladores de dominio de Windows 2000 de ADS no sea superior a 5 minutos.**
3. **Para guardar los cambios efectuados, haga clic en Apply (Aplicar).**

Nota – El restablecimiento de la fecha y hora cambiará el reloj del sistema, que se utiliza para la mayoría de operaciones relacionadas con el tiempo. No cambiará el reloj seguro que utiliza el software de administración de licencias y el software Compliance Archiving.

---

4. **En el panel de navegación, seleccione Windows Configuration (Configuración de Windows) > Configure Domains and Workgroups (Configurar dominios y grupos de trabajo).**
5. **Marque la casilla Enable ADS (Habilitar ADS).**
6. **En el campo Domain (Dominio), indique el dominio de Windows 2000 en el que se está ejecutando ADS.**

   El sistema debe pertenecer a este dominio.
7. **En el campo User Name (Nombre de usuario), escriba el nombre de un usuario de Windows 2000 que tenga derechos administrativos.**

   Debe ser el administrador de dominio o un usuario que sea miembro del grupo de administradores de dominio. El cliente ADS comprueba las actualizaciones ADS seguras con este usuario.

Nota – Si especifica aquí el nombre del administrador del dominio y falla la actualización de ADS, habrá que cambiar la contraseña de este administrador en el controlador de dominio. El usuario administrador es el único que debe hacer esto y puede reutilizar la misma contraseña. Para obtener más información, consulte el sitio Web de asistencia técnica de Microsoft (artículo Q248808).

---

8. **En el campo Password (Contraseña), escriba la contraseña del usuario administrativo de Windows 2000.**

9. **En el campo Container (Contenedor), escriba la ubicación de la ruta ADS del usuario administrativo de Windows 2000 en notación de nombre distinguido (DN) de protocolo ligero de acceso a directorios (LDAP).**

   Los objetos, incluidos los usuarios, están ubicados en los dominios Active Directory de acuerdo con una ruta jerárquica, que incluye cada nivel del objeto "contenedor". Escriba la ruta en términos de la carpeta **cn** (nombre común) o bien de la **ou** (unidad organizativa) del usuario.

   Por ejemplo, si el usuario reside en una carpeta "usuarios" que está en una carpeta principal llamada "contabilidad", deberá escribir lo siguiente:

   `ou=usuarios,ou=contabilidad`

   No incluya el nombre del dominio en la ruta.

10. **En el campo Site (Sitio), escriba el nombre del sitio ADS local si es diferente del dominio ADS.**

    Este campo se suele dejar en blanco.

11. **En la sección Kerberos Realm Info (Información del dominio Kerberos), escriba el nombre de dominio que se usa para identificar ADS.**

12. **Normalmente, se trata del dominio ADS o del dominio DNS. Al hacer clic en Apply (Aplicar), esta entrada se convierte en caracteres en mayúscula.**

13. **En el campo Server (Servidor), escriba el nombre de host del servidor de KDC de Kerberos.**

    Normalmente, se trata del nombre de host del controlador de dominio principal del dominio ADS. Puede dejar este campo en blanco si el sistema es capaz de localizar el servidor de KDC mediante DNS.

14. **Para guardar los cambios y que surtan efecto, haga clic en Apply (Aplicar).**

▼ Para comprobar el orden de búsqueda de los servicios de nombres

1. **Seleccione UNIX Configuration (Configuración de UNIX) > Configure Name Services (Configurar servicios de nombres).**

2. **Compruebe que el orden de búsqueda de los servicios de nombres para DNS está habilitado y configurado según la prioridad adecuada.**

   a. **Seleccione la ficha Hosts Order (Orden de hosts). Asegúrese de que el servicio DNS aparece en Services Selected (Servicios seleccionados) en el cuadro de la derecha. De lo contrario, seleccione el servicio DNS y haga clic en el botón >.**

   b. **Utilice los botones Arriba y Abajo para cambiar el orden en que se realizará la búsqueda en los servicios seleccionados.**

3. **Para guardar los cambios, haga clic en Apply (Aplicar).**

▼ Para comprobar la configuración DNS

1. **En el panel de navegación, seleccione Network Configuration (Configuración de red) > Configure TCP/IP (Configurar TCP/IP) > Set Up DNS (Configurar DNS).**
2. **Si DNS no está habilitado, seleccione la casilla de verificación Enable DNS (Habilitar DNS).**
3. **Si no ha especificado un nombre de dominio, escriba un valor en DNS Domain Name (Nombre de dominio DNS).**

   Este nombre debe coincidir con el del dominio ADS.
4. **En el campo Server (Servidor), escriba la dirección IP del servidor que desea que utilice el sistema y, a continuación, haga clic en el botón Add (Agregar) para que el servidor sea incluido en la DNS Server List (Lista de servidores DNS).**

   Puede agregar hasta dos servidores a la lista.
5. **Marque la casilla Enable Dynamic DNS (Habilitar DNS dinámico).**

   Si no activa esta función, deberá agregar manualmente el nombre de host y la dirección IP.
6. **En el campo DynDNS User Name (Nombre de usuario de DNS dinámico), escriba el nombre de usuario de un usuario de Windows 2000 que tenga derechos administrativos para realizar actualizaciones DNS dinámicas seguras.**

   Puede dejar este campo en blanco para las actualizaciones no seguras si el servidor DNS las permite.
7. **En el campo DynDNS Password (Contraseña de DNS dinámico), escriba la contraseña del usuario de DNS dinámico.**
8. **Para guardar los cambios, haga clic en Apply (Aplicar).**

   Si la función de DNS dinámico está habilitada, el sistema actualizará inmediatamente DNS con su nombre de host y dirección IP.

▼ Para publicar recursos compartidos en ADS

1. **En el panel de navegación, seleccione Windows Configuration (Configuración de Windows) > Configure Shares (Configurar recursos compartidos).**
2. **Haga clic en Add (Agregar).**
3. **Escriba un valor en Share Name (Nombre del recurso compartido).**
4. **(Optativo) Puede escribir un comentario para describir el recurso compartido.**

   Puede escribir hasta 60 caracteres alfanuméricos.

5. **En la lista desplegable, seleccione un volumen para compartirlo.**
6. **(Optativo) En el campo Directory (Directorio), especifique un directorio existente en el volumen seleccionado que desee compartir.**

Nota – Si no se especifica el directorio, se crea un recurso compartido en la raíz.

---

7. **En el campo Container (Contenedor), indique la ubicación del directorio ADS en el que se publicará el recurso compartido.**

   El campo Container (Contenedor) hace referencia al contenedor ADS. Especifique la ubicación ADS para el recurso compartido utilizando la notación de nombre distinguido (DN) de protocolo ligero de acceso a directorios (LDAP). Si desea obtener más información, consulte paso 9. en la página 80.

8. **Haga clic en Apply (Aplicar) para agregar el recurso compartido al contenedor especificado.**

Nota – Dicho contenedor debe existir de antemano para que se pueda publicar el recurso compartido. El sistema no crea objetos de contenedor en el árbol ADS.

▼ Para actualizar los contenedores de recursos compartidos de ADS

1. **En el panel de navegación, seleccione Windows Configuration (Configuración de Windows) > Configure Shares (Configurar recursos compartidos).**
2. **Seleccione el recurso compartido que desee actualizar.**
3. **Haga clic en Edit (Editar) para mostrar el cuadro de diálogo Edit Share (Editar recurso compartido).**
4. **Especifique el nuevo contenedor de recursos compartidos.**
5. **Haga clic en Apply (Aplicar).**

   El sistema actualiza el contenedor de recursos compartidos.

▼ Para eliminar recursos compartidos de ADS

1. **En el panel de navegación, seleccione Windows Configuration (Configuración de Windows) > Configure Shares (Configurar recursos compartidos).**
2. **Seleccione el recurso compartido que desee eliminar de ADS.**
3. **Haga clic en Edit (Editar) para mostrar el cuadro de diálogo Edit Share (Editar recurso compartido).**
4. **Elimine el contenedor de recursos compartidos del campo Container (Contenedor).**
5. **Haga clic en Apply (Aplicar).**

Configuración de LDAP

Para utilizar LDAP, es necesario que el servidor LDAP esté funcionando.

▼ Para habilitar el servicio LDAP

1. **En el panel de navegación, seleccione UNIX Configuration (Configuración de UNIX) > Set Up NSSLDAP (Configurar NSSLDAP).**
2. **Para habilitar LDAP, active la casilla Enable NSSLDAP (Habilitar NSSLDAP).**
3. **En el campo Domain (Dominio), escriba el nombre de dominio del servidor LDAP; por ejemplo, foo.com.**
4. **En el campo Password (Contraseña), escriba la contraseña del servidor LDAP.**
5. **En el campo Server (Servidor), escriba la dirección IP del servidor LDAP.**
6. **En el campo Proxy, escriba el dominio del servidor Proxy, de acuerdo con la configuración del servidor.**
7. **Para guardar la configuración, haga clic en Apply (Aplicar).**

Cambio del orden de búsqueda de los servicios de nombres

El orden de búsqueda de los servicios de nombres (NS) controla la secuencia que sigue el sistema a la hora de buscar los servicios de nombres para resolver una consulta. Entre estos servicios de nombres se encuentran LDAP, NIS, NIS+, DNS y Local. Para utilizarlos en la resolución de nombres deberá habilitar los servicios.

▼ Para establecer el orden de búsqueda del usuario, el grupo, el grupo de red y el host

1. **En el panel de navegación, seleccione UNIX Configuration (Configuración de UNIX) > Configure Name Services (Configurar servicios de nombres).**
2. **Haga clic en la ficha Users Order (Orden de usuarios) para seleccionar el orden de búsqueda de los usuarios.**
   a. **Seleccione un servicio en el cuadro Services Not Selected (Servicios no seleccionados).**
   b. **Para pasarlo al cuadro Services Selected (Servicios seleccionados), utilice el botón >.**

      Para eliminar un servicio de la búsqueda de usuarios, márquelo y haga clic en <.
   c. **Establezca el orden de los servicios de búsqueda en el cuadro Services Selected (Servicios seleccionados). Para ello, seleccione cada servicio y haga clic en los botones Arriba y Abajo para desplazarlo.**

      El servicio que se sitúe al comienzo de la lista será el primero que se utilice en la búsqueda de usuario.
3. **Haga clic en la ficha Groups Order (Orden de grupos) para seleccionar los servicios que se deben usar en la búsqueda de grupos y siga el procedimiento que se especifica en el paso 2.**
4. **Haga clic en la ficha Netgroups Order (Orden de grupos de red) para seleccionar los servicios que se deben usar en la búsqueda de grupos de red y siga el procedimiento que se especifica en el paso 2.**
5. **Haga clic en la ficha Hosts Order (Orden de hosts) para seleccionar los servicios que se deben usar en la búsqueda de hosts y siga el procedimiento que se especifica en el paso 2.**
6. **Para guardar los cambios, haga clic en Apply (Aplicar).**

CAPÍTULO 7

Seguridad de los grupos, los hosts y los directorios de archivos

Este capítulo describe las distintas preferencias para la seguridad de los grupos locales, los hosts, las asignaciones de grupos y usuarios, y los directorios de archivos.

Para configurar la seguridad de Windows, consulte "Configuración de la Seguridad de Windows" en la página 21.

El capítulo está dividido en las siguientes secciones:

- "Grupos locales" en la página 85
- "Configuración de hosts" en la página 89
- "Asignación de las credenciales de usuario y grupo" en la página 91
- "Definición de la seguridad de los directorios de archivos" en la página 98

Grupos locales

Los requisitos para los grupos locales integrados en el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310 son diferentes que para los grupos de un sistema Windows. Como se trata de un dispositivo NAS, no hay usuarios que inicien sesión localmente. Todos los usuarios se conectan a través de la red y se autentican mediante un controlador de dominio, por lo que no es necesario disponer de grupos locales como Usuarios o Invitados.

Nota – Los grupos locales se aplican sólo a las redes CIFS.

Los grupos locales se utilizan sobre todo para gestionar recursos y efectuar operaciones relacionadas con las copias de seguridad. Existen tres grupos locales: administradores, usuarios avanzados y operadores de copia de seguridad.

- **Administrators** (administradores): los miembros de este grupo pueden administrar con pleno derecho los archivos y directorios en el sistema.
- **Power Users** (usuarios avanzados): los miembros de este grupo pueden ser propietarios de los archivos y directorios del sistema, y hacerse cargo de las copias de seguridad y la restauración de archivos.
- **Backup Operators** (operadores de copia de seguridad): los miembros de este grupo pueden omitir los procedimientos de seguridad de los archivos para hacer copias de seguridad y restaurarlos.

El sistema también admite los grupos integrados de Authenticated Users (Usuarios autenticados) y de Network (Red). Todos los usuarios que inicien la sesión se convierten automáticamente en miembros de estos dos grupos integrados que se gestionan internamente. Puede agregar cualquier usuario de dominio principal o de confianza para que se convierta en miembro de alguno de estos grupos locales integrados.

Configuración de privilegios para los grupos locales

Los privilegios proporcionan un mecanismo seguro para asignar tareas de responsabilidad en todo el sistema. Cada privilegio tiene una función totalmente definida que asigna el administrador del sistema a un usuario o a un grupo. En el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310, como no hay usuarios locales, los privilegios se asignan sólo a los grupos.

A diferencia de los derechos de acceso, que se asignan como permisos en función de los objetos mediante descriptores de seguridad, los privilegios son independientes de los objetos. Los privilegios hacen caso omiso de las listas de control de acceso basadas en objetos y permiten al titular de los mismos realizar la función que se le ha asignado. Por ejemplo, los miembros del grupo de operadores de copia de seguridad, deben superar las comprobaciones habituales de seguridad para poder hacer copias de seguridad y restaurar los archivos a los que normalmente no tendrían acceso.

La diferencia entre un derecho de acceso y un privilegio queda de manifiesto en las siguientes definiciones:

- Un derecho de acceso se otorga o se deniega explícitamente a un usuario o grupo. Los derechos de acceso se asignan como permisos en una lista de control de acceso discrecional (DACL, del inglés Discretionary Access Control List) en función de los objetos.
- Un privilegio es una función que afecta al sistema entero y que faculta implícitamente a los miembros de un grupo para realizar operaciones predefinidas. Los privilegios sustituyen u omiten los derechos de acceso en función de los objetos.

Los privilegios admitidos se muestran en la TABLA 7-1. Puede asignar cualquiera de ellos a los grupos integrados. Dado que los usuarios de dominio se pueden convertir en miembros de los grupos integrados, podrá asignar estos privilegios a cualquier usuario de dominio.

TABLA 7-1 Privilegios admitidos

Privilegio	Descripción
Hacer copias de seguridad de archivos y directorios	Permite al usuario realizar copias de seguridad sin que se requiera permiso de acceso de lectura a los archivos y carpetas de destino.
Restaurar los archivos y directorios	Permite al usuario restaurar los archivos sin que se requiera permiso de acceso de escritura a los archivos y carpetas de destino.
Convertirse en propietario de los archivos y carpetas	Permite que los usuarios se conviertan en propietarios de un objeto sin que se requiera el permiso de acceso de propiedad. La propiedad sólo se puede definir en aquellos valores que el titular pueda asignar legítimamente a un objeto.

Los privilegios predeterminados asignados a los grupos integrados locales se muestran en la TABLA 7-2. En consecuencia, los miembros del grupo local de administradores pueden hacerse con la propiedad de cualquier archivo o carpeta y los miembros del grupo de operadores de copia de seguridad pueden realizar copias de seguridad y restauraciones.

TABLA 7-2 Privilegios de grupo predeterminados

Grupo	Privilegio predeterminado
Administradores	Convertirse en propietario
Operadores de copia de seguridad	Copia de seguridad y restauración
Usuarios avanzados	Ninguno

Asignación de la propiedad

De forma predeterminada, el grupo Domain Admins en el dominio del dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310 es un miembro del grupo de administradores local. Por ello, cuando un miembro del grupo Domain Admins (incluido el administrador de dominio) crea un archivo o carpeta o se convierte en su propietario, la propiedad se le asigna al grupo local de administradores. De esta forma se garantiza la máxima portabilidad en caso de que el sistema se mueva de un dominio a otro: los objetos que sean propiedad del grupo local de administradores siguen siendo accesibles para los miembros del nuevo grupo de administradores de dominio.

Las reglas de asignación de la propiedad descritas anteriormente también se cumplen en el caso de los usuarios normales que sean miembros del grupo local de administradores. Si algún miembro del grupo local de administradores crea un objeto o se convierte en su propietario, la propiedad se le asignará al grupo local de administradores en lugar de al miembro en concreto.

En los sistemas Windows, la pertenencia del administrador de dominio al grupo local de administradores se puede revocar. En estos casos, los miembros del grupo de administradores del dominio se consideran como usuarios normales. En el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310, sin embargo, el administrador del dominio siempre es miembro del grupo local de administradores. Además, el administrador del dominio no aparece como miembro de este grupo, por lo que no puede revocarlo. Dado que no hay usuarios locales y, en consecuencia, tampoco hay administradores locales de Windows, el grupo de administradores de dominio debe tener control administrativo sobre el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310.

Adición y eliminación de miembros del grupo y configuración de privilegios

El panel **Configure Groups** (Configurar grupos) le permite agregar usuarios de dominio a cualquiera de los tres grupos locales.

▼ Para agregar o eliminar un miembro de grupo

1. **En el panel de navegación, seleccione Windows Configuration (Configuración de Windows) > Configure Groups (Configurar grupos).**

   Los miembros existentes del grupo seleccionado aparecen en la lista del cuadro Group Members (Miembros del grupo).

2. **Para agregar un grupo, haga lo siguiente:**

   a. **Haga clic en Add Group (Agregar grupo).**

   b. **En el campo Group (Grupo), escriba el nombre del grupo.**

   c. **En el campo Comment (Comentario), especifique una descripción o comentario acerca del grupo.**

   d. **Para guardar los cambios, haga clic en Apply (Aplicar).**

3. **Para eliminar un grupo, haga lo siguiente:**

   a. **Seleccione el grupo que desee eliminar.**

   b. **Haga clic en Remove Group (Eliminar grupo).**

   c. **Para guardar los cambios, haga clic en Apply (Aplicar).**

4. **Para agregar o eliminar un miembro del grupo, haga lo siguiente:**

   a. **Resalte el grupo al que desea agregar miembros o el grupo del que desea eliminar miembros.**

      Los miembros existentes del grupo seleccionado aparecen en la lista del cuadro Group Members (Miembros del grupo).

   b. **En el cuadro Group Members (Miembros del grupo), resalte el miembro que desea agregar o eliminar y haga clic en el icono Add (Agregar) o Delete (Borrar).**

   c. **Para guardar los cambios, haga clic en Apply (Aplicar).**

Configuración de privilegios

El panel Configure Privileges (Configurar privilegios) permite a los administradores ver, otorgar y revocar privilegios de los grupos.

▼ Para configurar privilegios de NT

1. **En el panel de navegación, seleccione Windows Configuration (Configuración de Windows) > Configure Groups (Configurar grupos).**
2. **En el cuadro Groups (Grupos), seleccione el grupo al que desea asignar privilegios.**

Configuración de hosts

El panel **Set Up Hosts** (Configurar hosts) le permite agregar, editar y eliminar entradas del archivo host del sistema. La tabla muestra la información del host actual, incluido el nombre de host, la dirección IP y si se trata de un host de confianza.

Precaución – Hay que ser prudentes a la hora de asignar a un host el estado **de confianza**. Los hosts de confianza tienen acceso raíz al sistema de archivos, y acceso de lectura y escritura en todos los archivos y directorios del sistema.

Adición y edición de hosts

El panel **Set Up Hosts** (Configurar hosts) permite ver la información sobre el host y determinar si es de confianza o no. Un **superusuario** de un cliente NFS tendrá privilegios raíz en el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310 si ese cliente está definido como **host de confianza** y podrá acceder a todos los archivos sin tener en cuenta los permisos.

▼ Para agregar manualmente un host

1. **En el panel de navegación, seleccione UNIX Configuration (Configuración de UNIX) > Configure NFS (Configurar NFS) > Set Up Hosts (Configurar hosts).**
2. **Haga clic en Add (Agregar).**
3. **Escriba un valor en Host Name (Nombre del host).**

   Este nombre es por el que se conoce el host en el sistema. Dicho nombre de host sólo puede incluir letras y números (a-z, A-Z, 0-9), "-" (guiones), y "." (puntos). El primer carácter debe ser una letra (sólo a–z o A–Z).
4. **Escriba la dirección IP del nuevo host.**
5. **Si es necesario, seleccione la casilla de verificación para asignar al host el estado Trusted (De confianza).**

   Un host de confianza cuenta con un acceso raíz al dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310.
6. **Para guardar los cambios, haga clic en Apply (Aplicar).**

▼ Para editar la información del host

1. **En el panel de navegación, seleccione UNIX Configuration (Configuración de UNIX) > Configure NFS (Configurar NFS) > Set Up Hosts (Configurar hosts).**
2. **Seleccione los hosts cuya información desee editar y haga clic en Edit (Editar).**
3. **Revise la siguiente información si es necesario.**
   - **Host Name** (Nombre del host): es el nombre por el que se conoce el host en el sistema. Puede usar solamente letras en mayúscula o en minúscula, números, puntos (".") o guiones ("-"). El primer carácter debe ser una letra.
   - **IP Address** (Dirección IP): se trata de la dirección IP del host.
   - **Trusted** (De confianza): seleccione esta casilla para indicar que el host es de confianza. Hay que ser prudentes a la hora de asignar a un host este estado.
4. **Para guardar los cambios, haga clic en Apply (Aplicar).**

▼ Para eliminar una asignación de host para un host determinado

1. **En el panel de navegación, seleccione UNIX Configuration (Configuración de UNIX) > Configure NFS (Configurar NFS) > Set Up Hosts (Configurar hosts).**
2. **Haga clic en la entrada pertinente de la lista de hosts para seleccionar el host que desee eliminar.**
3. **Haga clic en Remove (Eliminar).**
4. **Haga clic en Apply (Aplicar).**

Asignación de las credenciales de usuario y grupo

Los servidores del dispositivo Sun StorEdge 5310 NAS, clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310 están diseñados para residir en un entorno de varios protocolos y para proporcionar un modelo integral que permita compartir datos entre sistemas Windows y UNIX. Aunque a los archivos se puede acceder simultáneamente desde ambos sistemas Windows y UNIX, no hay ningún mecanismo estándar en la industria que defina un usuario en ambos entornos (Windows y UNIX). Los objetos se pueden crear usando cada entorno, pero la sintaxis de control de acceso en cada entorno es muy diferente. Esta sección describe la asignación de credenciales. Para obtener información sobre la interacción entre la asignación de credenciales de usuario y grupo y los objetos seguros en el sistema, consulte "Asignación y objetos seguros" en la página 222.

La asignación de credenciales se utiliza para establecer una relación de equivalencia entre el usuario o grupo de UNIX definido en un archivo de configuración local o una base de datos NIS, y el usuario o grupo de dominio de Windows definido en una base de datos SAM de Windows. La asignación de usuarios y grupos es un modo de establecer equivalencia de credenciales en el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310 con el fin de proporcionar un acceso común en los dos entornos.

Usuarios y grupos de UNIX

Los usuarios y grupos de UNIX están definidos en archivos de configuración locales ('passwd' y 'group') o en una base de datos NIS. Cada usuario y grupo tiene un identificador de 32 que se llama el UID y el GID, respectivamente. La mayoría de sistemas UNIX hacen uso de identificadores de 16-bits, aunque se han ampliado a 32 bits en el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310 para evitar las restricciones que impone el rango de 16 bits. Aunque el UID y el GID identifican a cada usuario y grupo en un solo dominio UNIX, no existe un método que proporcione esta identificación exclusiva en todos los dominios. Por lo general, el valor de cero se aplica al usuario raíz o el grupo raíz. El usuario y el grupo raíz tienen un acceso casi ilimitado a fin de poder realizar tareas administrativas.

Usuarios y grupos de Windows

Los usuarios y grupos de Windows se encuentran definidos en una base SAM (del inglés Security Account Manager, gestor de cuenta de seguridad). Cada usuario y grupo tiene un identificador de seguridad (SID). Este identificador posee una estructura de longitud variable que permite identificar usuarios y grupos tanto en el dominio local, como en el resto de dominios de Windows.

El formato del SID es el siguiente:

```
typedef struct _SID_IDENTIFIER_AUTHORITY {
    BYTE Value[6];
} SID_IDENTIFIER_AUTHORITY;
typedef struct _SID {
    BYTE Revision;
    BYTE SubAuthorityCount;
    SID_IDENTIFIER_AUTHORITY IdentifierAuthority;
    DWORD SubAuthority[ANYSIZE_ARRAY];
} SID;
```

Los campos de la estructura del SID se pueden interpretar como muestra la TABLA 7-3.

TABLA 7-3 Campos en el SID

Campo	Value
Revision	La versión de SID. El valor de revisión actual es 1.
SubAuthorityCount	El número de entradas de subautoridad en el SID. Un SID puede contener hasta 15 entradas de subautoridades.
IdentifierAuthority	Una matriz de 6 bytes que identifica el subsistema que emite el SID.
SubAuthority	Una matriz de 32 bits de subautoridades identifica con exclusividad el objeto de seguridad adecuado: dominio, usuario, grupo o alias. El SID de dominio identifica un dominio entre todos los demás que pertenecen a la misma autoridad. Un SID de usuario, grupo o alias es un SID de dominio que adjunta su identificador relativo (RID) correspondiente. El RID es un identificador de 32 bits semejante a los UID y GID de UNIX.

Para facilitar su interpretación, los SID se muestran normalmente como una línea: S-1–5-32-500. Este SID contiene el número de versión 1, la autoridad del identificador es 5 y contiene dos subautoridades: 32 y 500. El valor 500 es el RID.

Cada dominio de Windows posee un SID exclusivo, y cada estación de trabajo y servidor de Windows también se encuentran en un dominio local que recibe el nombre de host respectivo. Por ello, todas las estaciones de trabajo y servidores de Windows tienen un SID propio. Los dominios de Windows que incluyen varias

máquinas están gestionados desde un controlador de dominio principal (PDC). Este controlador proporciona una administración centralizada de usuarios y grupos del dominio, además de definir un SID exclusivo para todo el dominio. De esta forma, el usuario de dominio y el usuario de estación de trabajo tienen diferente la parte sobre el dominio en el SID de usuario.

Para su integración en el modelo de dominios de Windows, cada dispositivo Sun StorEdge 5310 NAS, clúster Sun StorEdge 5310 y sistema de puerta de enlace Sun StorEdge 5310 también genera un SID para definir su dominio local. Este SID es generado con un algoritmo que produce cuatro subautoridades. La primera subautoridad tiene el valor 4, lo que representa una autoridad no exclusiva. Las tres subautoridades restantes se generan con un algoritmo que incluye la hora y una de las direcciones MAC3 del sistema para garantizar su carácter exclusivo. Este SID se empleará para representar tanto usuarios locales como de NIS, al anexar el UID o el GID de UNIX al SID del dominio. Este SID se almacena en lo equivalente a una base de datos SAM local.

Asignación de credenciales

Es posible definir asignaciones de usuario y grupo con el propósito de que todos los usuarios accedan a los archivos tanto desde sistemas Windows como UNIX. Esta sección describe los algoritmos que se utilizan para generar automáticamente las asignaciones de usuario y grupo, además de las políticas aplicadas durante el proceso de inicio de sesión. Las reglas de asignación para que los usuarios y grupos de UNIX sean asignados a los de Windows están especificadas en la configuración de políticas del sistema, y las asignaciones se guardan en la base de datos de políticas de sistema.

Cada asignación de usuario describe la manera en que el usuario de UNIX con un determinado UID es asignado a un usuario de Windows en un dominio con un RID específico. De manera parecida, cada asignación de grupo describe la manera en que el grupo de UNIX con un determinado GID es asignado a un grupo de Windows en un dominio con un RID específico.

El formato de asignación es como sigue:

```
<UNIX-nombre-usuario>:<UID>:<Windows-nombre-
usuario>:<NTDOMAIN>:<RID>
```

```
<UNIX-nombre-grupo>:<GID>:<Windows-nombre-grupo>:<NTDOMAIN>:<RID>
```

Los usuarios y grupos locales están definidos en los archivos `passwd` y de grupo locales. Estos archivos están definidos según el formato estándar de UNIX:

```
<nombre-usuario>:<contraseña>:<UID>:<GID>:<comentario>:<directorio
inicial>:<shell>
```

```
<nombre-grupo>:<contraseña>:<GID>:<lista-nombres-usuario-separada-
por-comas>
```

Asignación de usuarios

La asignación de usuarios permite crear una relación de equivalencia entre el usuario de UNIX y el usuario de Windows en que ambas credenciales tienen los mismos derechos en el sistema. Aunque el método de asignación puede ser bidireccional, no es necesario asignar los usuarios de UNIX a usuarios de Windows para el acceso de NFS al sistema. Esto es debido a la política de utilizar el dominio de UNIX como dominio de asignación básico.

Cada vez que el usuario de Windows inicia sesión en el sistema, los archivos de asignación se comprueban para determinar las credenciales UNIX de ese usuario. Para determinar el UID de UNIX de un usuario de Windows, se busca en la asignación de usuarios una entrada coincidente con el nombre de dominio y el nombre de usuario de Windows. Si se encuentra dicha entrada coincidente, pasa a componer el UID de UNIX. Si no existe esta entrada, la UID de UNIX del usuario se determina según la configuración de la política de asignación de usuarios.

Configuración de la política de asignaciones de usuario

La política de asignaciones de usuario tiene cuatro opciones.

- `MAP_NONE` especifica que no hay asignaciones predefinidas entre usuarios de Windows y de UNIX. Se asignará un UID de UNIX exclusivo al usuario de Windows. Se comprueba que este UID es exclusivo en la base de datos passwd configurada y el archivo de asignaciones de usuario antes de que sea elegido. Típicamente, el nuevo UID consistirá en el valor mayor encontrado en la búsqueda más uno. La base de datos passwd también puede incluir el archivo passwd NAS local y el archivo passwd de NIS, cuando NIS está habilitado. En este caso, es necesario modificar la entrada de asignación manualmente cuando el usuario de Windows debe asignarse a un usuario de UNIX existente.
- `MAP_ID` especifica que el UID de UNIX es el RID del usuario de Windows. No se efectúa ninguna búsqueda en la base de datos `passwd`.
- `MAP_USERNAME` especifica que el nombre del usuario de Windows se busca en la base de datos `passwd`. Si se encuentra una entrada coincidente entre el nombre del usuario de Windows y el de UNIX, el UID de UNIX se elige de dicha entrada. Si no se encuentra ninguna entrada, el UID de UNIX exclusivo se genera con el método descrito para `MAP_NONE`.
- `MAP_FULLNAME` especifica que el nombre completo de Windows para el usuario de Windows se busca en la base de datos passwd. Se busca una entrada coincidente con el campo de comentario de cada contraseña de UNIX. Sólo se compara con el nombre completo de Windows la entrada de nombre completo en el campo de comentario de la base de datos passwd. Si se encuentra una entrada coincidente, se utiliza el UID de UNIX de esa entrada. Si no se encuentra ninguna entrada, se genera un UID de UNIX exclusivo siguiendo el mismo método que con `MAP_NONE`.

Las credenciales de grupo para el usuario de Windows se obtienen por medio del algoritmo de asignaciones de grupo. Para obtener más información, consulte "Asignación de grupos" en la página 95.

Ejemplo de política de asignaciones de usuario

El siguiente ejemplo ilustra una asignación en que el usuario HOMEBASE\juanm de Windows pasa a ser equivalente al usuario juan de UNIX, y el usuario HOMEBASE\alanw de Windows pasa a equivaler al usuario amw de UNIX.

```
juan:638:juanm:HOMEBASE:1031
amw:735:alanw:HOMEBASE:1001
```

Asignación de grupos

La asignación de grupos se utiliza para crear una relación de equivalencia entre los grupos de UNIX y de Windows. Para determinar el GID de UNIX del usuario de Windows, la asignación de grupo se busca utilizando el nombre de dominio de Windows respectivo del usuario y el nombre de grupo principal de Windows. Cuando se encuentra una coincidencia, la entrada de asignación define el GID de UNIX al que se asignará el grupo de Windows a que pertenece el usuario. Si en la asignación de grupos no hay una entrada coincidente, el GID de UNIX se determina como esté configurada la política de asignaciones de grupo, y se crea una entrada nueva en la asignación del grupo, excepto cuando está aplicada la política de `MAP_UNIXGID`.

Configuración de la política de asignaciones de grupo

La política de asignaciones de grupo tiene cuatro opciones.

- `MAP_NONE` especifica que no hay asignaciones predefinidas entre usuarios de Windows y de UNIX. Se asignará un nuevo UID de UNIX exclusivo al grupo. Se comprueba que este GID es exclusivo en la base de datos group configurada y el archivo de asignaciones de grupo antes de elegirse un GID que consistirá en el mayor valor encontrado más uno. La base de datos group también puede incluir el archivo de grupo NAS local y el archivo de grupo de NIS, cuando NIS está habilitado. En este caso, es necesario modificar la entrada de asignación manualmente cuando el grupo de Windows debe asignarse a un grupo de UNIX existente.
- `MAP_ID` especifica que el GID de UNIX es el RID del grupo de Windows al que pertenece el usuario, tal como aparece en su testigo de acceso.
- `MAP_GROUPNAME` especifica que el nombre de grupo de Windows respectivo del usuario se busca en la base de datos group. Si se encuentra una entrada coincidente, pasa a componer el GID de UNIX. Si no se encuentra ninguna entrada, se genera un GID de UNIX exclusivo.
- `MAP_UNIXGID` especifica que el grupo de UNIX para el usuario de Windows está determinado por el campo de GID principal en el campo `passwd` que se ha obtenido durante la asignación del usuario.

  En este caso, no se consulta el archivo `group.map`. Si no es posible establecer un GID, se utiliza el GID del grupo sin usuarios de UNIX (60001).

El último paso consiste en determinar la lista de grupos UNIX a los que el usuario pertenece. En la base de datos group se buscan entradas del nombre de usuario de UNIX, según el procedimiento de asignaciones de usuario. El GID de cada grupo en que aparece el nombre del usuario de UNIX se agrega a la lista de grupo en las credenciales del usuario.

Ejemplo de la política de asignaciones de grupo

El siguiente ejemplo ilustra una asignación de grupo en que el grupo HOMEBASE\Domain Admins se convierte en equivalente del grupo wheel de UNIX, y el grupo HOMEBASE\Domain Users, en equivalente del grupo users de UNIX.

```
wheel:800:Domain Admins:HOMEBASE:1005
users:100:Domain Users:HOMEBASE:513
```

La regla de asignaciones predeterminada del sistema será `MAP_NONE` tanto para usuarios como para grupos:

```
map.users=MAP_NONE
map.groups=MAP_NONE
```

No es obligatorio que la regla para asignaciones de usuario sea la misma que para las asignaciones de grupo. A continuación, se muestra un ejemplo de configuración de asignaciones. En este ejemplo, la regla de asignaciones de usuario es `MAP_USERNAME` y la regla para asignaciones de grupo es `MAP_ID`.

```
map.users=MAP_USERNAME
map.groups=MAP_ID
```

Asignación de credenciales integrada

El identificador de superusuario UNIX, 0 (el UID o el GID), siempre está asignado al grupo local de administradores. El SID del grupo de administradores local se encuentra integrado (predefinido) en el SID de Windows: S-1-5-32-544. Esta asignación cumple la propiedad que asigna Windows de los archivos creados por el administrador del dominio. La propiedad de estos archivos siempre se asigna al grupo local de administradores integrado, a fin de proveer de independencia al dominio; es decir, para no perder el acceso a estos archivos si el sistema es desplazado de un dominio de Windows a otro. En el cuadro de permisos de Windows, este SID aparece como HOSTNAME\Administrators, donde HOSTNAME es el nombre de host del dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 o el sistema de puerta de enlace Sun StorEdge 5310.

▼ Para definir una política de asignaciones

1. **En el panel de navegación, seleccioneWindows Configuration (Configuración de Windows)> Manage SMB/CIFS Mapping (Administrar asignaciones SMB/CIFS)> Configure Mapping Policy (Configurar política de asignaciones).**
2. **Seleccione una de las preferencias de asignación de usuario en la sección Windows <--> UNIX User Mapping Choice (Elección de asignación de usuario entre Windows y UNIX).**
   - **Default Mapping** (Asignación predeterminada): seleccione esta opción si no hay ninguna regla de asignación definida entre los usuarios de Windows y UNIX. A los nuevos usuarios se les asignará un ID nuevo y exclusivo generado por el sistema.
   - **Map by User Name** (Asignar por nombre de usuario): seleccione esta opción para que el sistema asigne usuarios de UNIX y Windows que posean nombres de usuario idénticos. De este modo el usuario podrá acceder al dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310, o el sistema de puerta de enlace Sun StorEdge 5310 desde los dos entornos.
   - **Map by Full Name** (Asignar por nombre completo): seleccione esta opción para asignar usuarios de UNIX y Windows que posean nombres completos iguales.
3. **Seleccione una de las preferencias de asignación de grupo en la sección Windows <--> UNIX Group Mapping Choice (Elección de asignación de grupo entre Windows y UNIX).**
   - **Default Mapping** (Asignación predeterminada): seleccione esta opción si no hay ninguna regla de asignación predefinida entre los grupos de Windows y UNIX. A los nuevos grupos se les asignará un ID nuevo y exclusivo generado por el sistema.
   - **Map by Group Name** (Asignar por nombre de grupo): seleccione esta opción para asignar grupos de UNIX y Windows que posean nombres de grupo idénticos.
   - **Map to Primary Group** (Asignar al grupo principal): seleccione esta opción para crear una asignación con el grupo NFS en el campo de grupo principal del archivo `passwd` configurado.
4. **Para guardar los cambios, haga clic en Apply (Aplicar).**

   Para obtener más información sobre la interacción entre la asignación de credenciales de usuario y grupo y los objetos seguros en el sistema, consulte "Asignación y objetos seguros" en la página 222.

▼ Para asignar grupos y usuarios de Windows a grupos y usuarios de UNIX

1. **En el panel de navegación, seleccioneWindows Configuration (Configuración de Windows) > Manage SMB/CIFS Mapping (Administrar asignaciones SMB/CIFS) > Configure Maps (Configurar asignaciones).**
2. **Haga clic en Add (Agregar).**
3. **En el cuadro NT User (Usuario NT), especifique la siguiente información:**
   - **Account** (Cuenta): indique el nombre de cuenta de NT del usuario o el grupo que desee asignar.
   - **RID**: escriba el identificador relativo exclusivo para el usuario o grupo de NT dentro del dominio de NT.
4. **En el cuadro UNIX User (Usuario UNIX), especifique la siguiente información:**
   - **Name** (Nombre): escriba el nombre de grupo o usuario de UNIX al que desea asignar el grupo o usuario de NT especificado.
   - **ID**: escriba el identificador exclusivo para el usuario o grupo de UNIX dentro del dominio de UNIX.
5. **Para guardar los cambios, haga clic en Apply (Aplicar).**

   Para obtener más información sobre la interacción entre la asignación de credenciales de usuario y grupo y los objetos seguros en el sistema, consulte "Asignación y objetos seguros" en la página 222.

Definición de la seguridad de los directorios de archivos

Hay dos métodos para definir la seguridad en los directorios de archivos:

- "Definición de la seguridad de directorios de archivos en el modo de grupo de trabajo" en la página 99
- "Definición de la seguridad de los directorios de archivos en el modo de dominio" en la página 99

Definición de la seguridad de directorios de archivos en el modo de grupo de trabajo

En el modo de grupo de trabajo o de recursos compartidos seguros, todas las funciones de seguridad se definen en el propio recurso compartido (seguridad en el nivel de recurso compartido) utilizando Web Administrator.

En el modo de grupo de trabajo, el sistema asume que no se realiza ninguna autenticación en el cliente y solicita explícitamente los permisos, pidiendo una contraseña cada vez que se envía una solicitud de conexión al recurso compartido.

Consulte "Para agregar un nuevo recurso compartido SMB" en la página 103 para obtener instrucciones sobre cómo definir la seguridad en nivel de recurso compartido mientras se agrega un recurso de este tipo. Consulte "Para editar un nuevo recurso compartido SMB" en la página 106 para obtener instrucciones acerca de cómo definir la seguridad en nivel de recurso compartido mientras se edita un recurso de este tipo.

Definición de la seguridad de los directorios de archivos en el modo de dominio

Sólo se pueden gestionar derechos de acceso desde Windows 2000 o Windows XP.

Nota – Si el sistema está configurado en el modo de dominio, la configuración de permisos de objetos se realiza del mismo modo que los permisos de objetos en un controlador de dominio estándar de Windows. Hay más de una forma de ubicar los servidores y de asignar unidades para definir y gestionar los permisos de los recursos compartidos. Más abajo se muestra un ejemplo de este proceso.

Nota – El dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310 admiten funciones de seguridad en archivos y directorios solamente. La definición de seguridad para un recurso compartido pasará su asignación de seguridad al directorio inferior.

▼ Para definir la seguridad

1. **Abra el explorador de Windows.**
2. **Haga clic en Tools (Herramientas) > Map Network Drive (Conectar a unidad de red).**
3. **En el cuadro de diálogo Map Network Drive (Conectar a unidad de red), seleccione una letra de unidad en el cuadro de menú desplegable Drive (Unidad).**
4. **Localice y seleccione el servidor del dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 o el sistema de puerta de enlace Sun StorEdge 5310.**
5. **Haga clic en OK (Aceptar).**
6. **En la ventana del explorador de Windows, haga clic con el botón derecho en el recurso compartido del sistema para el cual desea definir permisos de nivel de usuario.**
7. **Seleccione Properties (Propiedades) en el menú desplegable.**
8. **Seleccione la ficha Security (Seguridad) en el cuadro de diálogo Properties (Propiedades).**
9. **Haga clic en el botón Permissions (Permisos).**
10. **Establezca los permisos que desee.**

    Consulte la documentación de Windows para obtener más información sobre la definición de los permisos.
11. **Haga clic en OK (Aceptar).**

CAPÍTULO 8

Recursos compartidos, cuotas y exportaciones

Este capítulo describe los distintos métodos disponibles para controlar el acceso de los usuarios a los volúmenes y archivos del dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310.

Se incluyen los siguientes temas:

- "Recursos compartidos" en la página 101
- "Gestión de cuotas" en la página 109
- "Configuración de exportaciones NFS" en la página 116

Recursos compartidos

El sistema de archivos comunes de Internet (CIFS, del inglés Common Internet File System) es una versión mejorada del protocolo de bloque de mensajes de servidor (SMB, del inglés Server Message Block) de Microsoft. SMB/CIFS permiten a los sistemas cliente de los entornos Windows acceder a los archivos del dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310.

Un **recurso compartido** es un recurso local en un servidor que está accesible para los clientes de Windows en la red. En un dispositivo Sun StorEdge 5310 NAS, clúster Sun StorEdge 5310 o sistema de puerta de enlace Sun StorEdge 5310, se trata normalmente de un volumen de sistema de archivos, o de un árbol de directorios dentro de un volumen. Cada recurso compartido se identifica mediante un nombre en la red. Para los clientes de la red, el recurso compartido aparece como un volumen completo en el servidor y no pueden ver la ruta de directorio local que existe por encima de la raíz del recurso compartido.

Nota – Los recursos compartidos y los directorios son entidades independientes. Si se elimina un recurso compartido, no afecta al directorio subyacente.

Los recursos compartidos se usan normalmente para proporcionar acceso de red a los directorios principales en un servidor de archivos de red. Cada usuario posee un directorio principal asignado dentro de un volumen de archivo.

Hay dos tipos de recursos compartidos: recursos compartidos SMB/CIFS **estáticos** y **autohome** (recursos temporales de creación automática). Los recursos compartidos estáticos son persistentes y permanecen definidos con independencia de si hay usuarios conectados al servidor o no. Los recursos compartidos autohome son recursos compartidos temporales que se crean cuando un usuario inicia una sesión en el sistema y se eliminan cuando finaliza dicha sesión.

Cuando el usuario explora el sistema, sólo aparecen mostrados los recursos compartidos definidos como estáticos y los recursos compartidos autohome de los usuarios que estén conectados.

Recursos compartidos estáticos

Se crea un recurso compartido estático que permite que el usuario asigne su directorio principal como unidad de red en una estación de trabajo cliente. Por ejemplo, un volumen llamado **vol1** puede contener un directorio principal llamado **principal** y, además, subdirectorios para los usuarios **pedro** y **sara**. Los recursos compartidos se definen como sigue:

TABLA 8-1 Ejemplos de rutas de recursos compartidos

Nombre de recurso compartido	Ruta de directorio
pedro	/vol1/principal/pedro
sara	/vol1/principal/sara

Si no resulta adecuado definir y mantener un recurso compartido de directorio principal estático para cada usuario de Windows que tenga acceso al sistema, puede utilizar la función de recursos temporales de creación automática (autohome). Si desea obtener más información, consulte "Recursos compartidos autohome" en la página 108.

Configuración de recursos compartidos estáticos

El panel **Configure Shares** (Configurar recursos compartidos) le permite agregar, ver y actualizar recursos compartidos SMB estáticos.

La tabla situada en la parte superior del panel **Configure Shares** (Configurar recursos compartidos) muestra información acerca de todos los recursos compartidos SMB existentes. Esta información incluye el nombre compartido y los

directorios compartidos, los nombres de contenedores y las llamadas a la base de datos de escritorio, así como la información relativa únicamente a los grupos de trabajo de Windows (usuario, grupo, umask y contraseñas).

Nota – Un directorio o volumen debe existir antes de poder compartirse.

De forma predeterminada, se crea un recurso compartido oculto para la raíz de cada volumen y sólo es accesible para los administradores de dominio. Normalmente, los administradores utilizan este tipo de recursos para migrar datos y crear estructuras de directorios. Los nombres de recursos compartidos se pueden encontrar en la pantalla Configure Shares (Configurar recursos compartidos). Los recursos compartidos del usuario no se crean hasta este pasos, ya que compartir directorios en un punto inferior a la raíz del volumen facilita la administración de la seguridad.

Creación de recursos compartidos estáticos

Para crear un recurso compartido, debe crear antes un volumen de archivo. Para obtener más información, consulte "Creación de un volumen de archivo o un segmento" en la página 45.

▼ Para agregar un nuevo recurso compartido SMB

1. **En el panel de navegación, seleccione Windows Configuration (Configuración de Windows) > Configure Shares (Configurar recursos compartidos).**
2. **Haga clic en Add (Agregar).**
3. **Escriba el nombre del recurso compartido que desee agregar en el campo Share Name (Nombre de recurso compartido).**

   Este nombre será el que verán los usuarios en la red. El nombre no podrá tener más de 15 caracteres. Los siguientes caracteres no se considerarán como válidos:

   = | : ; \ " ? < > * /
4. **(Optativo) Puede escribir un comentario para describir el recurso compartido.**

   Puede escribir hasta 60 caracteres alfanuméricos.
5. **Marque la casilla Desktop DB Calls (Llamadas a BD de escritorio) en la sección Mac Ext. (Extensiones de Mac) para que el sistema pueda acceder a la información de la base de datos de escritorio de Macintosh.**

   Esto acelera el acceso a los archivos a los clientes de Macintosh y permite a los no clientes acceder a archivos de Macintosh en el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310.

6. **Seleccione el volumen que se va a compartir en la lista de volúmenes disponibles que figura en el menú desplegable Volume Name (Nombre de volumen).**

7. **Especifique un directorio existente en el campo Directory (Directorio).**

   En este campo no puede crear un directorio. Los nombres de directorios distinguen mayúsculas de minúsculas.

   Nota – No deje el campo Directory (Directorio) en blanco.

   ---

8. **(Optativo) El campo Container (Contenedor) hace referencia al contenedor ADS en que se va a publicar el recurso compartido.**

   Si habilita ADS en el panel **Set Up ADS** (Configurar ADS), este campo estará disponible. No obstante, incluso si ADS está habilitado, no se le pedirá que especifique un contenedor ADS.

9. **Para especificar el contenedor, indique la ubicación de la ruta ADS para el recurso compartido en notación DN LDAP.**

   Si desea obtener más información, consulte "Para publicar recursos compartidos en ADS" en la página 81.

10. **Rellene los campos User ID (ID de usuario), Group ID (ID de grupo) y Password (Contraseña), si están disponibles.**

    Los campos **User ID** (ID de usuario), **Group ID** (ID de grupo) y **Password** (Contraseña) están disponibles únicamente si habilita el modo de grupo de trabajo de Windows (y no el modo de dominio NT). Consulte "Configuración de la Seguridad de Windows" en la página 21 para obtener información sobre cómo habilitar los modelos de seguridad de Windows.

    El modo de grupo de trabajo de Windows utiliza seguridad en nivel de recurso compartido. Los campos User ID (UID, ID de usuario), Group ID (GID, ID de grupo) y de contraseña en esta pantalla constituyen los únicos medios de seguridad para la propiedad de archivos en el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310, y para el acceso de los usuarios de grupos de trabajo de Windows. En otras palabras, los derechos para un directorio están determinados por la definición del recurso compartido y no por el usuario. El sistema da por hecho que el cliente no realiza ninguna autenticación y solicita explícitamente los permisos mediante el uso de una contraseña cada vez que se envía una solicitud de conexión al recurso compartido.

    Puede crear varios recursos compartidos para el mismo directorio con UID, GID y contraseñas diferentes. También puede dar a cada usuario una contraseña para un recurso compartido concreto. También puede utilizar cuotas para gestionar las restricciones de grupo y de usuario individuales en cuanto a cantidad de espacio de volumen de archivo o al número de archivos utilizados. Para obtener más información acerca de las cuotas, consulte "Gestión de cuotas" en la página 109.

Precaución – **User ID** (ID de usuario): especifique el UID del usuario que va a acceder al directorio especificado mediante este recurso compartido. El valor predeterminado para este campo es **0** (cero), que es el valor del superusuario UNIX. Sin embargo, hay que tener precaución a la hora de asignar este valor. En el modo de grupo de trabajo de Windows, si escribe un cero en este campo, se deshabilitará la seguridad en todos los archivos y directorios del recurso compartido en cuestión.

- **R/W Password** (Contraseña lectura/escritura): escriba la contraseña para los usuarios del grupo de trabajo de Windows que tengan acceso de lectura y escritura a los directorios especificados para este recurso compartido.
- **Confirm R/W Password** (Confirmar contraseña lectura/escritura): vuelva a escribir la contraseña de lectura y escritura para confirmarla.
- **R/O Password** (Contraseña de sólo lectura): escriba la contraseña para los usuarios del grupo de trabajo de Windows que tengan acceso de sólo lectura al recurso compartido.
- **Confirm R/O Password** (Confirmar contraseña de sólo lectura): vuelva a escribir la contraseña de sólo lectura para confirmarla.

11. En el campo Umask, escriba la máscara de creación de archivos (si procede) que desee aplicar a este recurso compartido.

La umask define la política de seguridad para los archivos y directorios creados en modo Share (Recurso compartido) y especifica los tipos de permisos que se deben desactivar cuando se crea un archivo.

La umask se define en octales ya que estos números constan de tres bytes; un sistema que se corresponde fácilmente con la representación de permisos de archivos de UNIX. La umask se aplica utilizando las reglas UNIX estándar, excepto para el atributo de sólo lectura de DOS. Si se configura el atributo de sólo lectura de DOS al crear un archivo, después de aplicar la umask, se eliminarán de los permisos de archivo todos los dígitos correspondientes a la escritura.

La siguiente tabla muestra cómo actúa la umask en distintos ejemplos de permisos, incluido el efecto del atributo de sólo lectura de DOS.

TABLA 8-2 Ejemplos de permisos con umask

Umask	Permisos de nuevo directorio		Permisos de nuevo archivo	
	DOS R/W (Lectura/Escritura de DOS)	DOS R/W (Sólo lectura de DOS)	DOS R/W (Lectura/Escritura de DOS)	DOS R/W (Sólo lectura de DOS)
000	777 (rwxrwxrwx)	555 (r-xr-xr-x)	666 (rw-rw-rw)	444 (r--r--r--)
777	000 (---------)	000 (---------)	000 (---------)	000 (---------)
022	755 (rwxr-xr-x)	555 (r-xr-xr-x)	644 (rw-r--r--)	444 (r--r--r--)
002	775 (rwxrwxr-x)	555 (r-xr-xr-x)	664 (rw-rw-r--)	444 (r--r--r--)

12. Para guardar los cambios, haga clic en Apply (Aplicar).

▼ Para editar un nuevo recurso compartido SMB

1. **En el panel de navegación, seleccione Windows Configuration (Configuración de Windows) > Configure Shares (Configurar recursos compartidos).**
2. **Seleccione el recurso compartido que desee actualizar.**
3. **Haga clic en Edit (Editar).**
4. **El campo Old Share Name (Nombre de recurso compartido antiguo) muestra el nombre actual del recurso compartido. Si desea cambiarlo, escriba el valor nuevo en el campo Share Name (Nombre de recurso compartido).**

   Los siguientes caracteres no se pueden incluir en el nombre del recurso compartido:

   = | : ; \ " ? < > * /
5. **Puede cambiar la descripción del recurso compartido en el campo Comment (Comentario). Puede escribir hasta 60 caracteres alfanuméricos.**
6. **Marque la casilla Desktop DB Calls (Llamadas a BD de escritorio) en la sección Mac Extensions (Extensiones de Mac) para permitir que el sistema acceda y defina la información de la base de datos de escritorio de Macintosh.**

   Esto acelera el acceso a los archivos a los clientes de Macintosh y permite a los no clientes acceder a archivos de Macintosh en el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310.
7. **Para cambiar la ruta del recurso compartido, indique un nombre de directorio existente en el campo Path (Ruta).**

   En este campo no puede crear un directorio. Los nombres de directorios distinguen mayúsculas de minúsculas.
8. **Especifique el nuevo valor en el campo Container (Contenedor), si es necesario.**

   El contenedor hace referencia al contenedor ADS en el que se va a publicar el recurso compartido. Este campo sólo estará disponible si ha habilitado ADS en el panel Set Up ADS (Configurar ADS). Indique la ubicación de la ruta ADS para el recurso compartido en notación DN LDAP. Si desea obtener más información, consulte "Para habilitar el servicio Active Directory" en la página 79.
9. **Rellene los campos User ID (ID de usuario), Group ID (ID de grupo) y Password (Contraseña), si están disponibles.**

   Consulte el paso 10. en la página 104 para obtener información detallada acerca de estos campos.
10. **Puede cambiar la configuración de Umask usando las reglas especificadas para el campo Umask que aparecen en el apartado "Creación de recursos compartidos estáticos" en el paso 11. en la página 105.**
11. **Para guardar los cambios, haga clic en Apply (Aplicar).**

▼ Para eliminar un recurso compartido SMB/CIFS

1. **En el panel de navegación, seleccione Windows Configuration (Configuración de Windows) > Configure Shares (Configurar recursos compartidos).**
2. **Seleccione el recurso compartido que desee eliminar de la tabla de recursos compartidos.**
3. **Haga clic en Remove (Eliminar).**
4. **Haga clic en Yes (Sí) para eliminar el recurso compartido.**

Configuración de clientes SMB/CIFS

Después de configurar las preferencias de red y de seguridad, el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 o el sistema de puerta de enlace Sun StorEdge 5310 pasa a estar visible para los clientes SMB/CIFS al registrarse automáticamente con el explorador principal en su red local.

Los clientes pueden conectarse de las siguientes formas.

Windows 98, XP y Windows NT 4.0

Los usuarios se conectan a la unidad de red desde el explorador de Windows, o bien, haciendo clic en el icono del dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 o el sistema de puerta de enlace Sun StorEdge 5310, situado en la ventana **Network Neighborhood** (Entorno de red).

Si los usuarios se conectan a la unidad de red, deberán emplear la ruta con formato de la convención de nomenclatura universal (UNC, del inglés Universal Naming Convention) para el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 o el sistema de puerta de enlace Sun StorEdge 5310, que consiste en el nombre de un equipo y el nombre de un recurso compartido, como se indica: `\\nombre_equipo\nombre_recurso_compartido`. Si se conectan mediante la ventana **Network Neighborhood** (Entorno de red), necesitarán el nombre de sistema que se utiliza para identificar al dispositivo Sun StorEdge 5310 NAS, clúster Sun StorEdge 5310 o sistema de puerta de enlace Sun StorEdge 5310 en la red.

Windows 2000, XP y 2003

Si ADS no está instalado, los usuarios se conectan a la unidad de red desde el explorador de Windows, o bien, haciendo clic en el icono del dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 o el sistema de puerta de enlace Sun StorEdge 5310, situado en la ventana **My Network Places** (Mis sitios de red).

Si los usuarios se conectan a la unidad de red, deberán utilizar la ruta con el formato UNC para el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310, que consiste en el nombre de un equipo y el nombre de un recurso compartido, como se indica: `\\nombre_equipo\nombre_recurso_compartido`. Si se conectan mediante la ventana **Network Neighborhood** (Entorno de red), necesitarán el nombre de sistema que se utiliza para identificar al dispositivo Sun StorEdge 5310 NAS, clúster Sun StorEdge 5310 o sistema de puerta de enlace Sun StorEdge 5310 en la red.

Si ADS está instalado, los usuarios se pueden conectar haciendo clic en un recurso compartido del dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 o el sistema de puerta de enlace Sun StorEdge 5310 publicado en ADS.

DOS

Los usuarios deben escribir el comando **net use** para conectase a una unidad en la línea de comandos. Deberán utilizar la ruta con el formato UNC para el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310, que consiste en el nombre de un equipo y el nombre de un recurso compartido como sigue: `\\nombre_equipo\nombre_recurso_compartido`.

Recursos compartidos autohome

La función de recursos compartidos SMB/CIFS autohome elimina las tareas administrativas necesarias para mantener los recursos compartidos de directorio principal de cada usuario de Windows que acceda al sistema. El sistema crea recursos compartidos autohome cuando un usuario inicia una sesión y los elimina cuando finaliza dicha sesión. De esta manera, se reduce el trabajo administrativo necesario para mantener las cuentas de usuario a la vez que aumenta la eficacia de los recursos del servidor.

Para configurar la función autohome, habilítela y escriba una ruta autohome. La ruta autohome es la ruta del directorio base para los recursos compartidos de directorio. Por ejemplo, si el directorio principal de un usuario es `/vol1/principal/sara`, la ruta autohome es `/vol1/principal`. El recurso compartido temporal se llamará sara. El nombre del directorio principal del usuario debe ser el mismo que el nombre de inicio de sesión del usuario.

Cuando un usuario inicia una sesión, el servidor comprueba que existe un subdirectorio que coincide con el nombre del usuario. Si encuentra una coincidencia y que el recurso compartido no existe, se agregará un recurso temporal. Cuando el usuario cierra la sesión, el servidor elimina el recurso compartido.

Los clientes de Windows pueden cerrar automáticamente la sesión de un usuario si transcurren 15 minutos de inactividad, lo que provoca que el recurso compartido autohome desaparezca de la lista de recursos compartidos publicados. Éste es el comportamiento normal del protocolo CIFS. Si el usuario hace clic en el nombre de un servidor o intenta acceder de otro modo al sistema (por ejemplo, mediante una ventana del explorador), el recurso compartido reaparecerá automáticamente.

Nota – Cuando el sistema se reinicia, se eliminan todos los recursos compartidos autohome.

Puesto que los recursos compartidos autohome se crean y se eliminan automáticamente, la configuración consiste, fundamentalmente, en habilitar la función.

▼ Para habilitar los recursos compartidos autohome

1. **En el panel de navegación, seleccione Windows Configuration (Configuración de Windows) > Configure Autohome (Configurar recursos compartidos autohome).**
2. **Marque la casilla Enable Autohome (Habilitar recurso compartido autohome).**
3. **Especifique un valor en Autohome Path (Ruta del recurso compartido autohome).**

   Para obtener más información sobre la ruta, consulte "Recursos compartidos autohome" en la página 108.
4. **Especifique un valor en ADS Container (Contenedor ADS).**

   Para obtener más información, consulte "Servicio Active Directory" en la página 78.
5. **Para guardar los cambios, haga clic en Apply (Aplicar).**

Gestión de cuotas

El panel **Manage Quotas** (Gestionar cuotas) le permite administrar cuotas en volúmenes de archivo y directorios del dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310. Las cuotas de grupos y usuarios determinan el espacio en disco que está disponible para un usuario o un grupo y cuántos archivos pueden escribir éstos en un volumen. Las cuotas de árbol de directorios determinan el espacio que está disponible para un directorio específico y cuántos archivos se pueden escribir en él.

Consulte "Configuración de las cuotas de grupos y usuarios" en la página 110 para definir las restricciones de espacio y archivo para los usuarios y los grupos. Consulte "Configuración de cuotas de árbol de directorios" en la página 113 para definir las restricciones de espacio y archivo para directorios específicos.

Configuración de las cuotas de grupos y usuarios

El panel **Configure User and Group Quotas** (Configurar cuotas de grupos y usuarios) le permite administrar cuotas en volúmenes para usuarios y grupos de NT y de UNIX. Muestra las cuotas raíz, predeterminadas e individuales para el volumen seleccionado. Las preferencias para el **usuario predeterminado** y el **grupo predeterminado** son las que se usan para todos los usuarios y grupos que no tienen cuotas individuales.

Límites máximos y flexibles

Un **límite máximo** es la cantidad máxima absoluta de espacio que está disponible para el usuario o el grupo.

Cuando se alcanza el **límite flexible**, que es igual o inferior al límite máximo, se inicia un periodo de gracia de 7 días, después del cual el usuario y el grupo no podrán escribir en el volumen hasta que la cantidad de espacio usada sea inferior al límite flexible.

El límite máximo debe ser igual o superior al límite flexible. En cuanto a espacio en disco, no puede ser superior a los 2 terabytes. Con respecto al número de archivos, el límite máximo no puede ser superior a cuatro mil millones de archivos.

El **superusuario** y el **grupo raíz** se definen automáticamente para que no tengan límites máximos ni flexibles, y no pueden poseer cuotas definidas.

▼ Para habilitar cuotas para un volumen de archivo

1. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Edit Properties (Editar propiedades).**
2. **En el menú desplegable Volume Name (Nombre de volumen), seleccione el volumen de archivo para el que va a habilitar las cuotas.**
3. **Asegúrese de que haya una marca de verificación en el cuadro Enable Quotas (Habilitar cuotas). Si no hay ninguna marca, active la casilla.**
4. **Haga clic en Apply (Aplicar).**

▼ Para agregar una cuota de usuario o grupo

1. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Manage Quotas (Gestionar cuotas) > Configure User and Group Quotas (Configurar cuotas de grupos y usuarios).**
2. **Haga clic en Users (Usuarios) si está configurando una cuota de usuario o en Groups (Grupos) si es una cuota de grupo.**
3. **En la lista desplegable Volume (Volumen), seleccione el nombre del volumen de archivo al que va a agregar cuotas.**

   La tabla de la pantalla muestra las cuotas de grupos y usuarios raíz, predeterminados e individuales para el volumen de archivo seleccionado.
4. **Para agregar una cuota para un grupo o usuario, haga clic en Add (Agregar).**
5. **Seleccione si el usuario o el grupo designados pertenecen a un entorno UNIX o NT. Para ello, haga clic en el botón de opción que proceda.**
6. **Seleccione el nombre de grupo o de usuario que proceda y el nombre de Domain (Dominio) para los grupos o los usuarios de NT.**
7. **Defina los límites de espacio en disco para el grupo o el usuario seleccionados.**

   Elija una de estas tres opciones:

   - **Default** (Predeterminado): elija esta opción para establecer que los límites máximos y flexibles sean los mismos que los del usuario o grupo predeterminados.
   - **No Limit** (Sin límite): elija esta opción para asignar un espacio ilimitado al usuario o grupo.
   - **Custom** (Personalizar): elija esta opción para definir un límite concreto. Seleccione si la cuota se debe mostrar en **kilobytes**, **megabytes** o **gigabytes**. A continuación, especifique los límites de espacio **flexibles** y **máximos** para el usuario o el grupo.

   Nota – Para definir las cuotas de usuario, hay que especificar el límite máximo y el flexible.

   ---

8. **Defina el límite en cuanto al número de archivos que puede escribir un usuario o un grupo en un volumen de archivo. Elija de entre las tres opciones siguientes:**

   - **Default** (Predeterminado): elija esta opción para establecer que los límites máximos y flexibles sean los mismos que los del usuario o grupo predeterminados.
   - **No Limit** (Sin límite): elija esta opción para que el usuario o el grupo puedan escribir un número ilimitado de archivos en el volumen de archivo.
   - **Custom** (Personalizar): elija esta opción para definir un límite concreto de archivos. A continuación, especifique los límites de espacio **flexibles** y **máximos** para el número de archivos.
9. **Para guardar los cambios, haga clic en Apply (Aplicar).**

▼ Para editar una cuota de usuario o grupo

1. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Manage Quotas (Gestionar cuotas) > Configure User and Group Quotas (Configurar cuotas de grupos y usuarios).**
2. **Haga clic en Users (Usuarios) para editar una cuota de usuario o en Groups (Grupos) para editar una cuota de grupo.**
3. **En la lista desplegable Volume (Volumen), seleccione el nombre del volumen cuyas cuotas desee editar.**

   La tabla de la pantalla muestra las cuotas de grupos y usuarios raíz, predeterminados e individuales para el volumen de archivo.
4. **Seleccione el usuario o el grupo cuyas cuotas desee editar y haga clic en Edit (Editar).**
5. **Modifique los límites de espacio en disco para el grupo o el usuario seleccionados.**

   Elija de entre las tres opciones siguientes:

   - **Default** (Predeterminado): elija esta opción para establecer que los límites máximos y flexibles sean los mismos que los del usuario o grupo predeterminados.
   - **No Limit** (Sin límite): elija esta opción para asignar un espacio ilimitado al usuario o grupo.
   - **Custom** (Personalizar): elija esta opción para definir un límite concreto. Seleccione si la cuota se debe ver en **kilobytes**, **megabytes** o **gigabytes**. A continuación, especifique los límites de espacio **flexibles** y **máximos** para el usuario o el grupo.
6. **Modifique el límite en cuanto al número de archivos que puede escribir un usuario o un grupo en un volumen de archivo. Elija de entre las tres opciones siguientes.**

   - **Default** (Predeterminado): elija esta opción para establecer que los límites máximos y flexibles sean los mismos que los del usuario o grupo predeterminados.
   - **No Limit** (Sin límite): elija esta opción para que el usuario o el grupo puedan escribir un número ilimitado de archivos en el volumen de archivo.
   - **Custom** (Personalizar): elija esta opción para definir un límite concreto de archivos. A continuación, especifique los límites de espacio **flexibles** y **máximos** para el número de archivos.
7. **Para guardar los cambios, haga clic en Apply (Aplicar).**

Eliminación de una cuota de usuario o grupo

Las cuotas raíz y predeterminadas no se pueden eliminar. Para eliminar una cuota individual, defina su espacio en disco y la cantidad de archivos en el valor predeterminado.

▼ Para borrar una cuota

1. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Manage Quotas (Gestionar cuotas) > Configure User and Group Quotas (Configurar cuotas de grupos y usuarios).**
2. **En el panel Configure User and Group Quotas (Configurar cuotas de grupos y usuarios), seleccione Users (Usuarios) para eliminar una cuota de usuario, o bien, seleccione Groups (Grupos) para eliminar una cuota de grupo.**
3. **Seleccione la cuota que desee eliminar en la tabla y haga clic en Edit (Editar).**
4. **En el cuadro de diálogo Edit Quota Setting (Editar configuración de cuota), haga clic en la opción Default (Predeterminado) en las secciones Disk Space Limits (Límites de espacio en disco) y File Limits (Límites de archivo).**
5. **Para eliminar la configuración de las cuotas, haga clic en Apply (Aplicar).**

Configuración de cuotas de árbol de directorios

El panel **Configure Directory Tree Quotas** (DTQ, Configurar cuotas de árbol de directorios) le permite administrar cuotas para directorios específicos en el sistema de archivos. Las cuotas de árbol de directorios determinan el espacio en disco que está disponible para un directorio y cuántos archivos se pueden escribir en él. Sólo se pueden configurar cuotas para directorios creados en este panel (no para directorios existentes).

▼ Para crear un árbol de directorios con una DTQ

1. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Manage Quotas (Gestionar cuotas) > Configure Directory Tree Quotas (Configurar cuotas de árbol de directorios).**
2. **En el menú desplegable, seleccione el volumen de archivo para el que va a configurar cuotas de árbol de directorios.**
3. **Haga clic en Add (Agregar).**
4. **En el campo DTQ Name (Nombre DTQ), escriba un nombre para identificar la cuota de árbol de directorios.**
5. **En el campo DirName (Nombre de directorio), especifique el nombre del directorio nuevo.**

6. **Bajo el campo Path (Ruta), hay un pequeño cuadro que muestra la estructura del árbol de directorios del volumen de archivo que ha seleccionado.**

   Para ver el contenido de una carpeta, haga clic en el símbolo que está al lado de la carpeta, o haga doble clic en el icono de la carpeta. Después, seleccione el directorio que incluirá el nuevo directorio que está creando. Continúe hasta que se muestre la ruta completa del directorio en el campo **Path** (Ruta).

7. **Seleccione el límite de espacio en disco del directorio en la sección Disk Space Limits (Límites de espacio en disco). Puede elegir No Limit (Sin límite) o Custom (Personalizar).**

   - Seleccione **No Limit** (Sin límite) para que el directorio tenga un espacio en disco ilimitado.
   - Seleccione **Custom** (Personalizar) para definir el espacio en disco máximo que puede ocupar el directorio.

8. **Elija si la cuota se debe mostrar en megabytes o gigabytes y escriba el límite de espacio en disco en el campo Max Value (Valor máximo).**

   Indicar un valor **personalizado** de **0** (cero) es igual que si elige **No Limit** (Sin límite).

9. **En el campo File Limits (Límites de archivo), seleccione el número máximo de archivos que se pueden escribir en el directorio. Puede optar por las opciones No Limit (Sin límite) y Custom (Personalizar).**

   - Seleccione **No Limit** (Sin límite) para que se pueda escribir una cantidad ilimitada de archivos en este directorio.
   - Elija **Custom** (Personalizar) si desea establecer un número máximo de archivos. Después, indique el límite de archivos en el campo **Max Value** (Valor máximo).

10. **Para agregar la cuota, haga clic en Apply (Aplicar).**

▼ Para editar una cuota de árbol de directorios existente

1. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Manage Quotas (Gestionar cuotas) > Configure Directory Tree Quotas (Configurar cuotas de árbol de directorios).**

2. **Seleccione la cuota que desee editar en la tabla y haga clic en Edit (Editar).**

3. **Modifique el nombre que identifica esta cuota de árbol de directorios en el campo DTQ Name (Nombre DTQ).**

   El campo **Path** (Ruta) es de sólo lectura y muestra la ruta al directorio.

4. **Seleccione el límite de espacio en disco del directorio en la sección Disk Space Limits (Límites de espacio en disco). Puede elegir No Limit (Sin límite) o Custom (Personalizar).**
   - Seleccione **No Limit** (Sin límite) para que el directorio tenga un espacio en disco ilimitado.
   - Elija **Custom** (Personalizar) si desea establecer una cantidad máxima de espacio en disco.
5. **Elija si la cuota se debe mostrar en megabytes o gigabytes y escriba el límite de espacio en disco en el campo Max Value (Valor máximo).**

   Indicar un valor **personalizado** de **0** (cero) es igual que si elige **No Limit** (Sin límite).
6. **En la secciónFile Limits (Límites de archivo), seleccione el número máximo de archivos que se pueden escribir en el directorio. Puede elegir entre No Limit (Sin límite) y Custom (Personalizar).**
   - Si selecciona **No Limit** (Sin límite) podrá escribir un número ilimitado de archivos en este directorio.
   - Elija **Custom** (Personalizar) si desea establecer un número máximo de archivos.
7. **Indique el límite de archivos en el campo Max Value (Valor máximo).**
8. **Para guardar los cambios, haga clic en Apply (Aplicar).**

Nota – Si desplaza un directorio que contenga una cuota de árbol de directorios (DTQ) o le cambia el nombre, el sistema actualizará automáticamente la especificación de la ruta de la DTQ.

▼ Para borrar una cuota de árbol de directorios

1. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Manage Quotas (Gestionar cuotas) > Configure Directory Tree Quotas (Configurar cuotas de árbol de directorios).**
2. **Seleccione la cuota que desee eliminar de la tabla.**
3. **Para eliminar la configuración de las cuotas, haga clic en Delete (Borrar).**

   Cuando se borra una cuota de árbol de directorios (DTQ), se elimina la configuración de las cuotas. Sin embargo, esto no elimina el directorio ni los archivos que contenga.

Nota – Si borra un directorio que contenga una configuración DTQ, tanto el directorio como la configuración DTQ se eliminarán.

Configuración de exportaciones NFS

Las exportaciones del sistema de archivos de red (NFS, del inglés Network File System) le permiten especificar privilegios de acceso para los usuarios de UNIX (y Linux). La tabla del panel **Configuring Exports** (Configuración de exportaciones) muestra la información sobre la exportación NFS actual, incluidos los directorios a los que se puede acceder, el nombre de host y el nivel de acceso (Lectura/Escritura o Sólo lectura) para cada exportación.

Los nombres de host que comienzan por "@" designan un grupo de hosts. Por ejemplo, un host llamado **@general** designa todos los hosts, y un host llamado **@trusted** designa todos los hosts de confianza. Consulte "Configuración de hosts" en la página 89 para obtener información acerca de los hosts de confianza.

Para especificar los privilegios de acceso para un host UNIX determinado

▼ Para crear las exportaciones

1. **En el panel de navegación, seleccione UNIX Configuration (Configuración de UNIX) > Configure NFS (Configurar NFS) > Configure Exports (Configurar exportaciones).**

   La tabla de este panel muestra la información sobre la exportación actual. Si no ha creado ninguna exportación, este espacio está en blanco.

2. **Haga clic en el botón Add (Agregar) para añadir una exportación.**

3. **En el cuadro Volume (Volumen), seleccione el volumen al que desea otorgar acceso al host NFS de UNIX.**

4. **En el cuadro Path (Ruta), especifique el directorio al que desea otorgar acceso al host NFS de UNIX.**

   Si deja este campo en blanco, se exporta el directorio raíz del volumen.

5. **En la sección Access (Acceso), especifique si los hosts dispondrán de privilegios de Read/Write (Lectura/Escritura), Read/Only (Sólo lectura) o No Access (Ningún acceso) con respecto al volumen seleccionado.**

6. **En la sección Hosts, seleccione los hosts para los que está definiendo una exportación NFS.**

   Elija una de las siguientes opciones:

   - **Host Netgroups** (Grupos de red del host): para seleccionar un grupo de red, active este botón de opción. Seleccione del menú desplegable el grupo de red para el que desee definir la exportación.
   - **Host Group** (Grupo de host): para seleccionar un grupo de host, active este botón de opción. En el menú desplegable, seleccione General (todos los hosts), Trusted (todos los hosts de confianza) o un grupo de host definido por el usuario.
   - **Known Host** (Host conocido): para asignar la exportación a un host agregado con el panel **Set Up Hosts** (Configurar hosts), seleccione esta opción. Seleccione, en el menú desplegable, el host para el que desee definir la exportación.
   - **Other Host** (Otros hosts): para asignar la exportación a un host que no haya agregado con el panel **Set Up Hosts** (Configurar hosts), seleccione esta opción y escriba el nombre del host.

7. **En la sección Map Root User (Asignar superusuario), seleccione un método de asignación del ID de usuario para los superusuarios.**

   Elija una de las siguientes opciones:

   - **Anonymous users** (Usuarios anónimos): para asignar el ID de superusuario al ID de usuarios anónimos, active este botón de opción.
   - **Root User** (Superusuario): para asignar el ID de superusuario al ID de raíz (UID= 0), active este botón de opción.
   - **Map to UID** (Asignar a UID): para asignar un ID de usuario específico, seleccione esta opción y escriba el ID de usuario.

8. **Para guardar la exportación, haga clic en Apply (Aplicar).**

9. **En el panel Configure Exports (Configurar exportaciones), compruebe que los datos de la ruta, el host y los derechos de acceso de la exportación que ha creado son correctos.**

▼ Para editar exportaciones

1. **En el panel de navegación, seleccione UNIX Configuration (Configuración de UNIX) > Configure NFS (Configurar NFS) > Configure Exports (Configurar exportaciones).**

2. **Seleccione la exportación que desee cambiar y haga clic en el botón Edit (Editar).**

3. **Para cambiar los derechos de acceso, haga clic en Read/Write (Lectura/Escritura), Read/Only (Sólo lectura) o No Access (Ningún acceso).**

   La sección **Hosts** es de sólo lectura.

4. **Para guardar los cambios, haga clic en Apply (Aplicar).**

5. **En el panel Configure Exports (Configurar exportaciones), compruebe que los datos de la ruta, el host y los derechos de acceso de la exportación que ha editado son correctos.**

Eliminación de exportaciones

Para eliminar una exportación NFS, haga clic en la exportación en el panel **Configure Exports** (Configurar exportaciones) y después en el botón Trash (Papelera).

CAPÍTULO 9

Opciones del sistema

Este capítulo proporciona las instrucciones para las opciones de activación que se pueden adquirir para el dispositivo Sun StorEdge 5310 NAS. Además, contiene información adicional acerca de las siguientes opciones:

- Sun StorEdge File Replicator, que permite duplicar datos de un volumen a otro volumen duplicado en un dispositivo Sun StorEdge 5310 NAS diferente (utilizado normalmente para sistemas orientados a las transacciones).
- Compliance Archiving Software, que permite activar volúmenes con el fin de seguir las directrices de almacenamiento compatible para la retención y protección de datos.

Está dividido en las siguientes secciones:

- "Activación de opciones del sistema" en la página 119
- "Sun StorEdge File Replicator" en la página 121
- "Compliance Archiving Software" en la página 133

Activación de opciones del sistema

Para activar las opciones del sistema, debe escribir una clave de activación en el panel **Activate Options** (Activar opciones). Si ha adquirido una opción, póngase en contacto con el representante del servicio de atención al cliente de Sun Microsystems para obtener la clave de activación.

▼ Para activar una opción

1. **En el panel de navegación, seleccione System Operations (Operaciones de sistema) > Activate Options (Activar opciones) y haga clic en Add (Agregar) para añadir la licencia.**
2. **En el cuadro de diálogo Add License (Agregar licencia), indique el nombre del módulo que le ha proporcionado Sun (por ejemplo, `Sun StorEdge File Replicator`).**
3. **Escriba la fecha indicada por Sun en el campo Origination (Inicio) con el formato AAAAMMDD.**

   Se trata de la fecha en que se activa la licencia (se inicia a las 00:00:00 horas). La fecha 00:00:00:00 indica que la licencia se activa inmediatamente.
4. **Escriba la fecha indicada por Sun en el campo Expiration (Caducidad) con el formato AAAAMMDD.**

   Se trata de la fecha en que caduca la licencia (a las 23:59:59 horas). La fecha 00:00:00:00 indica que la licencia no tiene fecha de caducidad.

Nota – Cuando una licencia de cumplimiento caduca o se elimina, el sistema mantiene las normativas relacionadas pero no es posible crear nuevos volúmenes de cumplimiento. Consulte "Compliance Archiving Software" en la página 133 para obtener información acerca del software Compliance Archiving.

---

5. **Indique la clave de licencia que le ha proporcionado Sun.**
6. **Haga clic en Apply (Aplicar) para activar la opción.**

   Para Sun StorEdge File Replicator debe seguir pasos adicionales en el servidor duplicado. Consulte "Para activar Sun StorEdge File Replicator en el servidor remoto" en la página 124 para obtener instrucciones.
7. **Si nunca ha ajustado la hora y fecha, defina la hora, la fecha y la información de zona horaria correctas.**

   Se establecerá la hora del sistema y el reloj seguro. El software de gestión de licencias y Compliance Archiving Software utilizan el reloj seguro para las operaciones que dependen del tiempo.

Nota – El reloj seguro sólo se puede configurar una vez. Asegúrese de que realiza la operación con precisión.

---

8. **Confirme que la nueva hora y fecha son exactas.**

   Si la nueva fecha y hora son correctas, haga clic en **Yes** (Sí). En caso contrario, haga clic en **No** y defina la fecha y hora correctas.

Sun StorEdge File Replicator

El software Sun StorEdge File Replicator le permite mantener duplicaciones de datos exactas en dos servidores.

Duplicación del dispositivo Sun StorEdge 5310 NAS

La duplicación permite replicar uno o todos los volúmenes de archivo de un sistema Sun StorEdge NAS a otro. El servidor de origen recibe el nombre de "activo" y el de destino se llama "servidor de duplicación".

Si todos los servidores activos fallan, podrá interrumpir la duplicación en el servidor y, a continuación, promocionar el volumen de archivo duplicado (ponerlo a disposición de los usuarios) en el servidor de duplicación.

El método utilizado es una duplicación asíncrona orientada a las transacciones. Se lleva a cabo mediante una memoria búfer de duplicación extensa que pone en cola las transacciones del sistema de archivos para transferirlas al sistema de duplicación. En la práctica, el servidor de duplicación mantiene una mínima diferencia temporal con respecto al servidor activo. Como la duplicación está orientada a las transacciones, la integridad del sistema de archivos duplicado está garantizada, incluso si se producen interrupciones en la red o en el sistema.

Pasos preliminares de la duplicación

Antes de comenzar a duplicar, asegúrese de que se cumplen los siguientes requisitos:

- Para duplicar, se requieren dos servidores Sun StorEdge NAS. Los servidores pueden ser de cualquier modelo y diferentes entre ellos.
- El servidor de duplicación debe contener una cantidad igual o superior de espacio de almacenamiento que los volúmenes de archivo que se estén duplicando.
- Entre los servidores activos y de duplicación debe haber una conexión de red fiable, que esté disponible continuamente y que tenga capacidad suficiente. El tipo de interfaz que conecte estos dos servidores puede ser Ethernet de 100 Mb o de 1.000 Mb. Los servidores pueden estar conectados con un conmutador o un router. Si conecta los servidores mediante un router, deberá configurar preferencias de ruta estática para garantizar que los datos de duplicación se conduzcan mediante una ruta privada. Si conecta los servidores mediante un conmutador, cree una LAN virtual (VLAN) para cada servidor con objeto de aislar el tráfico de red.

- Ambos servidores deben tener instaladas las mismas versiones del sistema operativo.
- Los volúmenes de archivo activos que se van a duplicar necesitan un tamaño mínimo de 1 gigabyte.

Nota – Una vez que se duplica un volumen de archivo, no se podrá cambiar el nombre del volumen de archivo original.

Requisitos y limitaciones de File Replicator con una configuración de clúster

La siguiente lista describe los requisitos y limitaciones de la duplicación con el clúster Sun StorEdge 5310:

- Ambas unidades en la configuración de clúster deben tener activada la licencia de Sun StorEdge File Replicator.
- Las duplicaciones deben establecerse sólo desde y al servidor H1. (No cree una duplicación del servidor H1 al servidor H2 del mismo clúster).
- Para realizar cualquier operación de administración de duplicación (incluida la creación de duplicaciones, cambiar funciones, promocionar o interrumpir), ambas unidades en el clúster deben encontrarse en el estado NORMAL.
- Cuando el clúster se encuentre en el modo de recuperación tras error (es decir, con un servidor en estado ALONE y el otro en estado QUIET) o tenga un rendimiento reducido, *no* realice operaciones de duplicación. Debería colocar el clúster en el estado NORMAL antes de realizar ninguna operación de administración de duplicación.
- Las duplicaciones existentes continuarán duplicando, incluso cuando se produzca un error en la configuración del clúster. Asimismo, continuarán duplicándose cuando el clúster se restablezca tras un error.

Configuración de sistemas activos y de duplicación

A la hora de configurar los sistemas, deberá establecer las funciones de los puertos que interconectan los servidores (consulte "Para configurar los puertos de red dedicados" en la página 123). A continuación, tendrá que configurar la duplicación en los sistemas activo y de duplicación utilizando la interfaz de Web Administrator (consulte "Configuración de volúmenes de archivo duplicados" en la página 123). Configure cada sistema de forma independiente.

▼ Para configurar los puertos de red dedicados

1. **En el panel de navegación del servidor activo, seleccione Network Configuration (Configuración de red) > Configure TCP/IP (Configurar TCP/IP) > Configure Network Adapters (Configurar adaptadores de red).**
2. **Si todavía no lo ha hecho, asigne las direcciones IP y la función de puerto principal para los puertos que estén conectados a una red local o subred.**

   Los puertos de los sistemas activos y de duplicación pueden estar en diferentes subredes locales. Para obtener más información acerca de la configuración TCP/IP, consulte "Configuración de los puertos de red" en la página 18.
3. **Asigne la dirección IP del puerto que se utiliza para la conexión de duplicación entre los sistemas activo y de duplicación.**

   Nota – No emplee subredes que contengan la interfaz principal para la duplicación.

   Si ha creado una red aislada para conducir el tráfico de duplicación, deberá utilizar direcciones que pertenezcan al grupo de uso privado del tipo 192.1xx.x.x. Por ejemplo, puede establecer 192.1xx.1.1 como interfaz de enlace de duplicación del sistema activo y asignar 192.1xx.1.2 como interfaz de enlace de duplicación del sistema de duplicación.
4. **En el campo Role (Función) del puerto que sirve para las conexiones entre el servidor activo y el de duplicación, seleccione Mirror (Duplicar).**
5. **Si las interfaces de duplicación de los sistemas activo y de duplicación no están conectados a la misma subred, tendrá que configurar una ruta estática entre ellos en la interfaz de línea de comandos.**

   Esto permite que los servidores puedan comunicarse entre sí mediante redes que no estén conectadas directamente a sus interfaces locales. Para obtener más información acerca de cómo finalizar este proceso, consulte "Rutas de gestión" en la página 205.
6. **Para guardar los cambios, haga clic en Apply (Aplicar).**

Configuración de volúmenes de archivo duplicados

La duplicación se lleva a cabo por volúmenes. Puede optar por duplicar algunos de los volúmenes o bien todos ellos.

Nota – Se pueden duplicar sólo los volúmenes de archivo cuyo tamaño sea igual o superior a 1 gigabyte. Una vez que se duplica un volumen de archivo, no se podrá cambiar el nombre del volumen de archivo original mientras esté activa la conexión de duplicación.

No puede haber actividad de E/S en el volumen de archivo que se está duplicando procedente del servidor activo durante la sincronización de duplicación inicial.

Búfer de duplicación

La memoria búfer de duplicación almacena las transacciones escritas del sistema de archivos a medida que se van transfiriendo al servidor de duplicación. El espacio libre del volumen de archivo del servidor activo se ve reducido por el tamaño de asignación de la memoria búfer de duplicación.

El tamaño del búfer de duplicación depende de una serie de factores, pero debe ser como mínimo de 100 megabytes, y el búfer de duplicación nunca puede mayor que la mitad del espacio libre restante en un volumen de archivos.

En una situación normal, se recomienda crear una memoria búfer de duplicación cuyo tamaño sea aproximadamente el 10% del tamaño del volumen de archivo que va a duplicar. El tamaño que elija dependerá de la cantidad de información que se escriba en el volumen de archivo y no del tamaño del volumen de archivo en sí. Como norma general, el tamaño del búfer de duplicación es directamente proporcional a la frecuencia de las escrituras en el archivo, e inversamente proporcional a la velocidad de la conexión de la red entre los dos servidores.

Si hay una alta actividad de escritura en el volumen de archivos y una conexión de red lenta entre los dos servidores de duplicación, se recomienda crear un búfer de duplicación que tenga entre el 25 y el 30% del tamaño del volumen de archivos que esté duplicando.

El tamaño del búfer de duplicación no se puede aumentar dinámicamente. Para incrementar el tamaño del búfer de duplicación, es necesario dividir la duplicación existente y crearla otra con el nuevo tamaño de búfer de duplicación.

▼ Para activar Sun StorEdge File Replicator en el servidor remoto

Después de activar la opción Sun StorEdge File Replicator (consulte "Activación de opciones del sistema" en la página 119), debe también activar la opción en el servidor remoto que contiene los volúmenes de archivo que desea duplicar.

1. **Inicie una sesión en Web Administrator en el servidor que contiene los volúmenes de archivo que desea duplicar.**
2. **En el cuadro de diálogo Add License (Agregar licencia), indique el nombre del módulo que le ha proporcionado Sun (`Sun StorEdge File Replicator`).**
3. **Escriba la fecha indicada por Sun en el campo Origination (Inicio) con el formato AAAAMMDD.**

   Se trata de la fecha en que se activa la licencia (se inicia a las 00:00:00 horas). La fecha 00:00:00:00 indica que la licencia se activa inmediatamente.
4. **Escriba la fecha indicada por Sun en el campo Expiration (Caducidad) con el formato AAAAMMDD.**

   Se trata de la fecha en que caduca la licencia (a las 23:59:59 horas). La fecha 00:00:00:00 indica que la licencia no tiene fecha de caducidad.

5. **Indique la clave de licencia que le ha proporcionado Sun.**
6. **Haga clic en Apply (aplicar) para activar Sun StorEdge File Replicator.**

▼ Para agregar un volumen de archivo

1. **En el panel de navegación, seleccione File Replicator (Replicador de archivos) > Manage Mirrors (Gestionar duplicaciones).**
2. **Haga clic en Add (Agregar).**
3. **Seleccione el volumen de archivo que se va a duplicar en el menú desplegable Volume (Volumen).**

   Este volumen de archivo debe tener un tamaño igual o superior a 1 gigabyte.
4. **Escriba un nombre distinto para el servidor de duplicación en el campo Mirror Host (Host de duplicación).**
5. **Escriba la dirección IP del sistema de duplicación.**

   Debe ser la dirección IP elegida para duplicar la tarjeta NIC en el sistema de duplicación.
6. **Si lo desea, introduzca un valor en Alternate IP Address (dirección IP alternativa), opcional.**

   Si la primera dirección IP deja de estar disponible, el servidor emplea la dirección IP alternativa para mantener la duplicación.
7. **Si se requiere una contraseña administrativa para acceder al servidor de duplicación, especifíquela en el campo Password (Contraseña).**

   Si no hay ninguna contraseña administrativa, deje este campo en blanco. Se aconseja proteger los servidores con contraseñas.
8. **Especifique el tamaño (en megabytes) en el campo Mirror Buffer (Búfer de duplicación).**

   El espacio libre del volumen de archivo del servidor activo se ve reducido por el tamaño de asignación de la memoria búfer de duplicación.
9. **Compruebe que no exista actividad de E/S hacia el volumen de archivo de origen en el servidor activo mientras se crea la duplicación y, a continuación, haga clic en Apply (Aplicar) para crearla.**

   Comienza el proceso de creación de la duplicación. Cuando la duplicación alcanza el estado **In Sync** (En sincronización) en el panel **Manage Mirrors** (Gestionar duplicaciones), el volumen de archivo duplicado se monta como de sólo lectura. La actividad de E/S puede resumirse cuando la duplicación alcanza el estado en sincronización.

   Puede editar las direcciones IP alternativas o la contraseña del administrador del servidor de duplicación de una duplicación existente.

▼ Para editar una duplicación

1. **En el panel de navegación, seleccione File Replicator (Replicador de archivos) > Manage Mirrors (Gestionar duplicaciones).**
2. **Seleccione en la tabla la duplicación que desee editar.**
3. **Haga clic en Edit (Editar).**

   Los campos del nombre del volumen de archivo y del host de la duplicación son campos de sólo lectura.
4. **Modifique la dirección IP que desee usar para la conexión de la duplicación y, después, edite el campo Alternate IP Address (Dirección IP alternativa).**
5. **Si es necesario, especifique la nueva contraseña de administrador para acceder al servidor host de la duplicación.**

   Si no hay ninguna contraseña administrativa, deje el campo Password (Contraseña) en blanco.
6. **Para guardar los cambios, haga clic en Apply (Aplicar).**

▼ Para corregir una duplicación con daños

En el caso de que una duplicación esté dañada (esto se produce si la conexión entre los dos servidores no está activa durante un tiempo o si el búfer de la duplicación es demasiado pequeño y hay muchas operaciones de escritura en el volumen maestro), realice las siguientes operaciones:

1. **Establezca una conexión de red más rápida entre los dos servidores.**
2. **Detenga toda la actividad de E/S hacia el sistema de archivos maestro hasta que la duplicación alcance el estado de sincronización.**
3. **Después de interrumpir y promocionar el volumen `nbd`, monte el sistema de archivos de destino en el servidor de duplicación como de sólo lectura para un cliente CIFS o NFS.**

   Este sistema de archivos se puede utilizar para las actividades de copia de seguridad o sólo lectura.

   También puede combinar los puntos de comprobación con la función de duplicación. Cuando se crea un punto de comprobación en el servidor activo, también se duplica en el servidor duplicado. Esto se puede utilizar para las copias de seguridad programadas o para conceder acceso de sólo lectura al punto de comprobación a otros usuarios y aplicaciones.

Definición de los umbrales de advertencia

En el panel **File Replicator (Replicador de archivos) > Set Threshold Alert (Establecer umbral de alerta)** puede definir los umbrales de alerta para todos los volúmenes de archivo duplicados. El umbral de alerta determina en qué porcentaje de uso de la memoria búfer de duplicación se envía una advertencia a los usuarios especificados.

La memoria búfer de duplicación almacena las transacciones escritas del sistema de archivos a medida que se van transfiriendo al servidor de duplicación. El aumento de las tareas de escritura en el servidor activo o los enlaces de red dañados puede provocar que se transfieran transacciones de escritura al servidor de duplicación para realizar una copia de seguridad en la memoria búfer de duplicación. Si se desborda la memoria búfer a causa de este proceso, la duplicación falla y no se producen más transacciones entre el servidor activo y el servidor de duplicación hasta que se restablezca la duplicación. Una vez que se restablece por completo la comunicación, el sistema comienza automáticamente el proceso de resincronización hasta que el volumen de archivo duplicado cuenta con una copia de seguridad en la sincronización.

Para evitar que se produzca esta situación, el sistema envía automáticamente advertencias mediante correos electrónicos, el archivo de registro del sistema, las capturas SNMP y la pantalla LCD cuando el búfer de duplicación alcanza determinados porcentajes.

▼ Para configurar los umbrales de alerta

1. **En el panel de navegación, seleccione File Replicator (Replicador de archivos) > Set Threshold Alert (Establecer umbral de alerta).**

2. **Especifique un valor para Mirroring Buffer Threshold 1 (Umbral 1 para la memoria búfer de duplicación).**

   Éste será el porcentaje de uso de la memoria búfer de duplicación que desencadenará la primera alerta. El valor predeterminado es el 70%. Esto significa que cuando el búfer de duplicación esté al 70% de su capacidad, se emitirá una alerta automática.

3. **Especifique un valor para Mirroring Buffer Threshold 2 (Umbral 1 para la memoria búfer de duplicación).**

   Éste será el porcentaje de uso de la memoria búfer de duplicación que desencadenará la segunda alerta. El valor predeterminado es el 80%.

4. **Especifique un valor para Mirroring Buffer Threshold 3 (Umbral 1 para la memoria búfer de duplicación).**

   Éste será el porcentaje de uso de la memoria búfer de duplicación que desencadenará la tercera alerta. El valor predeterminado es el 90%.

5. **Seleccione un valor para Alert Reset Interval (Hours) (Intervalo para el restablecimiento de las alertas [en horas]).**

   Hace referencia a la cantidad de tiempo que debe esperar antes de volver a generar una alerta si se produce de nuevo la misma circunstancia dentro del intervalo de tiempo.

   Por ejemplo, si establece que **Mirroring Buffer Threshold 1** (Umbral 1 para la memoria búfer de duplicación) es el 10% y que **Alert Reset Interval (Hours)** (Intervalo para el restablecimiento de las alertas [en horas]) es dos horas, la primera alerta se genera cuando el búfer de duplicación está al 10% de su capacidad. El sistema no volverá a generar la misma alerta de umbral 1 hasta que transcurran dos horas. Si, pasado este tiempo, el uso del búfer de duplicación sigue siendo superior al umbral del 10% (pero sin llegar al umbral 2 o 3), se volverá a generar la alerta número 1.

   El valor predeterminado para este campo es 24 horas.

6. **Para guardar los cambios, haga clic en Apply (Aplicar).**

Interrupción de la conexión entre servidores de duplicación

Para promocionar un volumen de archivo en el servidor de duplicación (por ejemplo, si el volumen de archivo del servidor activo no está disponible), en primer lugar debe interrumpir la conexión de duplicación. Interrumpa dicha conexión en el servidor activo en lugar de hacerlo en el servidor de duplicación, tal y como se describe en el siguiente procedimiento. Sin embargo, si el servidor activo no está en funcionamiento y no puede acceder a él para interrumpir la conexión, deberá hacerlo desde el servidor de duplicación.

▼ Para interrumpir una conexión de duplicación

1. **En el panel de navegación del servidor activo, seleccione File Replicator (Replicador de archivos) > Manage Mirrors (Gestionar duplicaciones).**

2. **Seleccione la duplicación en la tabla y haga clic en Break (Interrumpir).**

   Se le solicitará que confirme esta acción. Una vez que haya interrumpido la conexión de duplicación, ésta desaparecerá de la tabla de duplicaciones de este panel. Para promocionar el volumen de archivo, debe acceder al panel **Manage Mirrors** (Gestionar duplicaciones) en el servidor de duplicación. Para obtener más información, consulte "Promoción de un volumen de archivo duplicado" en la página 129.

Promoción de un volumen de archivo duplicado

Si el servidor activo falla, el servidor de duplicación proporciona funciones de alta disponibilidad para los volúmenes de archivo duplicados. Para hacer que un volumen de archivo duplicado esté disponible para los usuarios de red, debe **promocionar** el volumen de archivo. En primer lugar, debe interrumpir la conexión de duplicación y, después, promocionar el volumen de archivo duplicado y configurar los derechos de acceso pertinentes. Una vez que se interrumpe una conexión de duplicación y se promociona el volumen de archivo duplicado, los volúmenes de archivo original y duplicado pasan a ser completamente independientes.

Precaución – No se puede generar la duplicación de un volumen con compatibilidad habilitada.

Si necesita un acceso temporal a un volumen de duplicación compatible, expórtelo como sistema de archivos de sólo lectura sin promocionarlo.

Para promocionar un volumen de archivo en el servidor de duplicación, en primer lugar debe interrumpir la conexión de duplicación. Consulte "Interrupción de la conexión entre servidores de duplicación" en la página 128 para obtener instrucciones.

▼ Para promocionar un volumen de archivo en el servidor de duplicación

1. **En el panel de navegación del servidor de duplicación, seleccione File Replicator (Replicador de archivos) > Manage Mirrors (Gestionar duplicaciones).**
2. **Haga clic en Promote (Promocionar).**
3. **En el cuadro de diálogo Promote Volume (Promocionar volumen), seleccione el volumen que desea promocionar y haga clic en Apply (Aplicar).**

   Este proceso puede tardar varios minutos en completarse. Para promocionar un volumen de archivo duplicado, el volumen debe haber alcanzado el estado **In Sync** (En sincronización) en algún momento. Si el volumen de archivo duplicado estaba fuera de la sincronización cuando se promocionó correctamente, el volumen se establecerá como de sólo lectura. Antes de habilitar el volumen para que se pueda escribir, ejecute el comando `fsck` para llevar a cabo las reparaciones necesarias.

   Después de interrumpir la conexión de duplicación, el sistema realiza una comprobación del sistema de archivos. Si el sistema encuentra errores durante esta comprobación, el proceso de promoción del volumen puede tardar más en completarse. La integridad de los datos no está garantizada si la duplicación está fuera de la sincronización durante el proceso de promoción.

   Después de promocionar el volumen de archivo, puede que sea necesario volver a configurar los derechos de acceso. La información de los recursos compartidos SMB se traslada automáticamente, pero será necesario configurar de nuevo el acceso a los volúmenes de archivo NFS y las exportaciones NFS para dicho volumen de archivo. Para obtener información acerca de cómo configurar las exportaciones NFS, consulte "Configuración de exportaciones NFS" en la página 116.

Restablecimiento de la conexión de duplicación

Este procedimiento describe cómo se restablece la conexión de duplicación cuando el servidor haya fallado y el volumen de archivo esté promocionado en el servidor de duplicación. El volumen de archivo promocionado es ahora la versión más actualizada y funciona de forma independiente del volumen de archivo desfasado del sistema activo. Para volver a crear la conexión de duplicación, debe volver a duplicar el volumen de archivo actualizado en el servidor activo y, a continuación, duplicar el volumen de archivo de nuevo en el servidor de duplicación, tal y como hizo al principio.

Nota – Si el volumen de archivo duplicado no llegó a promocionarse, no deberá seguir estas instrucciones. El sistema activo pone automáticamente la duplicación en estado **In Sync** (En sincronización) cuando vuelva a estar conectado.

En el ejemplo que aparece a continuación, el *Servidor 1* es el que está activo y el *Servidor 2* es el de duplicación.

▼ Para restablecer una conexión de duplicación

1. **Asegúrese de que la conexión de la duplicación del Servidor 1 está interrumpida.**

   Consulte "Interrupción de la conexión de duplicación en el servidor activo" en la página 130.

2. **Elimine el volumen de archivo desfasado del Servidor 1.**

   Consulte "Para eliminar el volumen de archivo desfasado del Servidor 1" en la página 131.

3. **Haga una duplicación del volumen de archivo actualizado del Servidor 2 al Servidor 1. Consulte "Para duplicar el volumen actualizado del Servidor 2 en el Servidor 1" en la página 131.**

4. **Cambie la función del Servidor 2.**

   Consulte "Cambio de las funciones de los volúmenes" en la página 132.

   En este momento, el Servidor 1 estará activo de nuevo y el número 2 será el servidor de destino duplicado.

▼ Interrupción de la conexión de duplicación en el servidor activo

1. **Abra una ventana del explorador web para acceder al Servidor 1.**

2. **En el panel de navegación, seleccione File Replicator (Replicador de archivos) > Manage Mirrors (Gestionar duplicaciones).**

3. **Seleccione la conexión de duplicación que desea interrumpir.**

4. **Haga clic en Break (Interrumpir).**

▼ Para eliminar el volumen de archivo desfasado del Servidor 1

1. **En el panel de navegación del Servidor 1, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Delete File Volumes (Eliminar volúmenes de archivo).**
2. **Elija el volumen de archivo que se estaba duplicando.**

   Como el volumen de archivo del servidor de duplicación se ha promocionado y ahora es la versión más actual, el que corresponde al servidor activo está desfasado y es necesario borrarlo.

Precaución – Antes de llevar a cabo el siguiente paso, asegúrese de que lo que va a eliminar es el volumen de archivo original desfasado del **servidor activo**. También, asegúrese primero de que el volumen de archivo actualizado del servidor de duplicación se ha verificado y promocionado.

3. **Haga clic en Apply (Aplicar) para eliminar el volumen de archivo desfasado.**

▼ Para duplicar el volumen actualizado del Servidor 2 en el Servidor 1

1. **Abra una ventana del explorador web para acceder al Servidor 2.**
2. **En el panel de navegación, seleccione File Replicator (Replicador de archivos) > Manage Mirrors (Gestionar duplicaciones).**
3. **Haga clic en Add (Agregar).**
4. **Seleccione el volumen de archivo que se va a duplicar en el menú desplegable Volume (Volumen).**
5. **Especifique el nombre de duplicación del Servidor 1 en el campo Mirror Host (Host de duplicación).**
6. **Escriba la dirección IP del puerto del Servidor 1 que se utiliza para la conexión de duplicación.**
7. **Si lo desea, especifique un valor en Alternate IP Address (Dirección IP alternativa).**
8. **Si necesita una contraseña administrativa para acceder al Servidor 1, escríbala en el campo Password (Contraseña).**

   Si no hay ninguna contraseña administrativa, deje este campo en blanco.

9. **Especifique el tamaño en el campo Mirror Buffer (Búfer de duplicación).**

   Para obtener más información acerca de la memoria búfer de duplicación, consulte "Duplicación del dispositivo Sun StorEdge 5310 NAS" en la página 121.

   Asegúrese de que no haya actividad de E/S hacia el volumen de archivo de origen en el *Servidor 2* durante la sincronización de duplicación.

10. **Para crear la duplicación, haga clic en Apply (Aplicar).**

    Comienza el proceso de creación de la duplicación. Cuando la duplicación alcance el estado **In Sync** (En sincronización), habrá una copia exacta del volumen de archivo tanto en el Servidor 1 como en el Servidor 2.

11. **En el panel Manage Mirrors (Gestionar duplicaciones) del Servidor 1, seleccione el volumen de archivo promocionado y haga clic en Change Roles (Cambiar funciones).**

    Si desea obtener más información, consulte "Cambio de las funciones de los volúmenes" en la página 132.

    Ha restablecido la conexión de duplicación original.

Cambio de las funciones de los volúmenes

Un administrador puede cambiar las funciones entre un volumen activo y uno duplicado. Al cambiar dichas funciones, el volumen activo puede funcionar como el duplicado y viceversa. Sin embargo, la configuración original de cada volumen no se modifica. El cambio de funciones no es una operación de recuperación de fallos.

Nota – Los volúmenes deben estar en una perfecta sincronización para cambiar las funciones.

El cambio de funciones se puede iniciar desde el panel Manage Mirror (Gestionar duplicaciones) del servidor activo o de duplicación.

▼ Para cambiar las funciones

1. **En el panel de navegación, seleccione File Replicator (Replicador de archivos) > Manage Mirrors (Gestionar duplicaciones).**
2. **Seleccione un volumen en la columna Volume (Volumen).**
3. **Haga clic en Change Roles (Cambiar funciones).**
4. **Haga clic en Yes (Sí) para confirmar.**

Compliance Archiving Software

Compliance Archiving Software permite que una empresa cumpla con las normativas y utilice las prácticas empresariales recomendadas relativas a la retención y protección de la información. Dichas normas y marcos de trabajo para la retención y protección de registros incluye la normativa de seguridad e intercambio (SEC) 17 CFR § 240.17a-4 (17a-4), la ley Sarbanes Oxley, BASEL II y numerosas directivas de privacidad y protección de datos.

Compliance Archiving Software se ha diseñado partiendo de cero contando con la ayuda de expertos del sector de gestión del contenido empresarial y de cumplimiento de normas en gestión de la información con el fin de satisfacer los más estrictos requisitos en cuanto a protección y retención de medios de almacenamiento electrónico. Compliance Archiving Software hace uso de archivos WORM (escritura una vez, lectura múltiple) de acuerdo con las normas de cumplimiento.

Activación de Compliance Archiving

El software Compliance Archiving se encuentra disponible sin algunas restricciones (denominado de "aplicación recomendada") y con restricciones (de "aplicación obligatoria").

Si el software Compliance Archiving está activado (consulte "Activación de opciones del sistema" en la página 119), en el momento de crear un volumen se puede elegir entre habilitar la compatibilidad con aplicación recomendada o aplicación obligatoria.

Nota – Las configuraciones del sistema de puerta de enlace Sun StorEdge 5310 admiten la compatibilidad con aplicación recomendada, pero no aplicación obligatoria.

Nota – Compliance Archiving Software requiere la correcta configuración del hardware del dispositivo Sun StorEdge 5310 NAS o el clúster Sun StorEdge 5310 para su funcionamiento correcto. En concreto, las matrices de controladores de unidad de expansión RAID del Sun StorEdge 5300 no deberían conectarse a ningún otro dispositivo o red que no sea la conexión privada Fibre Channel con la unidad NAS, o cualquier armario de expansión de Sun StorEdge 5300 EU.

Nota – Para asegurar la máxima aplicación de las políticas de retención de datos, también deberá tener en cuenta la seguridad física del dispositivo Sun StorEdge 5310 NAS o clúster Sun StorEdge 5310. La retención de datos controlada por software no puede ser más sólida que las medidas preventivas físicas utilizadas para controlar el acceso al hardware del sistema.

Precaución – No debería habilitar el archivo compatible en los volúmenes que utilizarán las aplicaciones (y usuarios) que no estén al tanto de las distintas normas de retención de datos impuestas por Compliance Archiving Software.

Compliance Archiving Software permite a los administradores activar el archivo compatible en cualquier volumen nuevo que creen pero sólo cuando estos volúmenes se han creado inicialmente. Siga las instrucciones que se indican en "Para crear un volumen de archivo o un segmento con el panel Create File Volume (Crear volumen de archivo)" en la página 45 para crear un volumen con compatibilidad habilitada.

Compatibilidad con aplicación obligatoria

La compatibilidad de aplicación obligatoria cumple las directivas de protección, retención de datos y privacidad, incluidas las siguientes:

- No se puede destruir un volumen con compatibilidad de aplicación obligatoria.
- Un archivo WORM no se puede destruir hasta que haya vencido el periodo de retención.
- El periodo de retención de un volumen se puede acortar o alargar; para un archivo WORM sólo es posible alargarlo.
- No se puede restaurar un archivo WORM desde un punto de comprobación.

Precaución – Una vez se ha activado el almacenamiento compatible en un volumen con aplicación obligatoria, no se podrá eliminar o renombrar el volumen, o desactivar la función de almacenamiento compatible, ni cambiar a la característica de aplicación recomendada.

Compatibilidad con aplicación recomendada

La compatibilidad con aplicación recomendada incluye lo siguiente:

- Un administrador autorizado puede destruir archivos WORM y volúmenes compatibles (utilizando la función 'borrar auditados').

Nota – Antes de eliminar un volumen, es necesario que los registros de auditoría de este volumen se retengan en una copia de seguridad efectuada en un sistema de archivos distinto. De lo contrario, estos registros se perderán.

- Un administrador autorizado puede incrementar o reducir el tiempo de retención.
- El administrador autorizado puede restaurar archivos WORM desde un punto de comprobación (utilizando la función 'borrar auditados').
- El tiempo de retención predeterminado de fábrica es de 0 días aunque es posible cambiarlo.

Nota – El superusuario, desde un host de confianza, podrá reducir el tiempo de retención y eliminar los archivos retenidos antes de vencer el periodo de retención. Consulte "Gestión de hosts de confianza" en la página 224.

Cuando un volumen con compatibilidad habilitada de aplicación recomendada se actualiza a su aplicación obligatoria, el periodo de retención de ese volumen se convierte en permanente. Esto se puede cambiar en el panel Edit Properties (Editar propiedades).

Nota – La actualización de un volumen con compatibilidad de aplicación recomendada no es posible en configuraciones de puerta de enlace.

Auditoría de la compatibilidad

La auditoría de la compatibilidad proporciona un registro de texto con todos los intentos por modificar o eliminar datos (con o sin la autoridad necesaria) y se puede habilitar mediante la API de DRAS (del inglés Data Retention Audit Service, servicio de auditoría de retención de datos), que incluye las siguientes funciones:

- Registro de los cambios e intentos de modificación de los archivos retenidos
- Un método de registro con el que se guardan los eventos auditables
- Protección y conservación del registro de auditoría durante toda la vida útil del sistema
- Información del registro de auditoría en un formato visible, y acceso seguro a este registro mediante protocolos de acceso estándar del sistema

Los eventos auditables son los siguientes:

- Retención de un archivo
- Ampliación del periodo de retención del archivo retenido
- Solicitudes para desvincular (borrar) un archivo retenido
- Solicitudes para escribir en un archivo retenido
- Solicitudes para cambiar el nombre de un archivo retenido
- Solicitudes para eliminar un directorio
- Solicitudes para cambiar el nombre de un directorio

Restricciones del tamaño de archivo

Los volúmenes compatibles reservan una cantidad de espacio libre con el fin de garantizar que se registran las operaciones auditables en el volumen. Cuando el espacio libre del volumen con compatibilidad caiga por debajo del límite, las operaciones de auditoría no se ejecutarán. Se registra un mensaje que indica que no hay espacio suficiente para ejecutar la operación y la auditoría, y se enviará un correo electrónico de advertencia si está configurado el correo electrónico en el sistema.

Registro de auditoría

El registro de auditoría de los volúmenes con compatibilidad habilitada reside en el directorio raíz de cada volumen.

Estos registros se basan en texto y se puede acceder a ellos mediante los protocolos de red, incluidos NFS y CIFS. El directorio `.audit$` debe estar incluido en la ruta de recursos compartidos para que los clientes de Windows 2000 o XP puedan ver el contenido. Consulte "Recursos compartidos" en la página 101 para obtener información sobre cómo crear los recursos compartidos.

El formato del registro de auditoría se muestra en la TABLA 9-1.

TABLA 9-1 Formato del registro de auditoría

Campo	Longitud	Descripción
Version (Versión)	7	Número de versión del servicio de auditoría de retención de datos
Serial Number (Nº de serie)	11	Un número de secuencia exclusivo
Length (Longitud)	5	Longitud del registro de auditoría
Timestamp (Marca de tiempo)	21	Fecha y hora en que ocurrió el evento
TID	11	ID del subproceso desde el que se ejecutó el evento
Volume ID (ID de volumen)	11	ID del volumen en el que se realizó la auditoría
Protocol (Protocolo)	9	Protocolo de red con el que se solicitó la operación
Inode (Inodo)	11	Número inodo de sistema de archivos para el archivo
Client IP Address (Dirección IP cliente)	16	Dirección IP del cliente desde el que se solicitó la operación
Server IP Address (Dirección IP servidor)	16	Dirección IP mediante la que se recibió la solicitud del cliente
UID	11	Credencial de usuario
GID	11	Credencial de grupo principal
Operation (Operación)	8	El evento de auditoría
Status (Estado)	variable	Resultado de la operación
Domain (Dominio)	variable	El dominio de Windows al que pertenece el usuario, si está disponible
File/Directory Name (Nombre de archivo/directorio)	variable	Nombre del archivo o el directorio en que se realizó la operación, si está disponible
Path/Extra Data (Ruta/datos adicionales)	variable	Información adicional de la auditoría, si está disponible

Funcionales adicionales de Compliance Archiving

Para obtener una descripción técnica de las funciones y la interfaz de programación de Compliance Archiving Software, consulte Apéndice C.

Para modificar la configuración en el almacenamiento compatible, consulte "Configuración de Compliance Archiving Software" en la página 248.

CAPÍTULO 10

Supervisión del sistema

Este capítulo describe las funciones de supervisión del dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310. La supervisión del sistema está muy relacionada con las funciones de mantenimiento y muchas de las tareas que se describen aquí hacen referencia a otros capítulos en los que hay que realizar determinadas acciones para solucionar aspectos relacionados con las funciones de supervisión. Dichas funciones también muestran el estado de gestión o de las actividades de mantenimiento.

Se incluyen los siguientes temas:

- "Supervisión del protocolo simple de administración de red (SNMP)" en la página 140
- "Visualización del estado del sistema" en la página 141
- "Registro del sistema" en la página 142
- "Auditoría del sistema" en la página 145
- "Estado del entorno" en la página 147
- "Información de uso" en la página 151
- "Visualización de las rutas de red" en la página 154
- "Supervisión de los componentes de sistema" en la página 155
- "Visualización del estado de trabajos de copia de seguridad" en la página 159

Supervisión del protocolo simple de administración de red (SNMP)

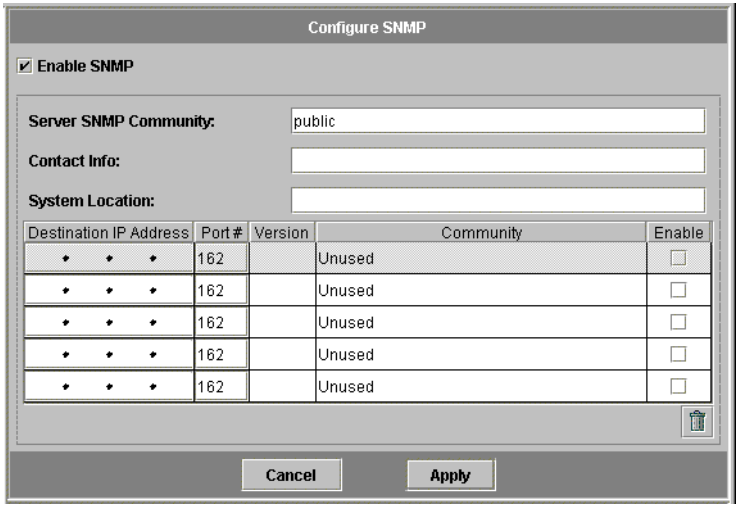
Para conducir la supervisión SNMP es necesario habilitar las comunicaciones de SNMP. El dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310 admiten sólo la supervisión SNMP (no la administración de SNMP).

Para interpretar los bloques de información sobre mensajes (MIB, del inglés Message Information Blocks) se necesitan los archivos MIB. Los archivos MIB están instalados con la imagen en el *directorio_arranque*/www/data/mib. Por ejemplo, `/cvol/nf1/www/data/mib`.

Los archivos MIB también se encuentran disponibles para descargarlos en `http://sunsolve.sun.com`. Si desea obtener más información sobre cómo utilizar estos archivos, consulte la documentación relativa a la aplicación de gestión de red.

▼ Para configurar SNMP

1. **En el panel de navegación, seleccione Monitoring and Notification (Supervisión y notificación) > Configure SNMP (Configurar SNMP).**



2. **Marque la casilla Enable SNMP (Habilitar SNMP).**

3. **Especifique la comunidad SNMP a la que pertenece el dispositivo Sun StorEdge 5310 NAS en el campo Server SNMP Community (Comunidad del servidor SNMP).**
4. **En el campo Contact Info (Información de contacto), especifique el nombre de la persona que es responsable del sistema.**
5. **En el campo System Location (Ubicación del sistema), escriba la ubicación de red.**

   Esta ubicación puede ser física o lógica.
6. **Para añadir una nueva dirección de destino, escriba la siguiente información en una fila vacía de la tabla SNMP:**
   - **Destination IP Address** (Dirección IP de destino): escriba la dirección TCP/IP del servidor que desea configurar como destino de las capturas SNMP en el caso de que se produzcan errores de sistema.
   - **Port #** (Nº de puerto): escriba el puerto al que enviará capturas el sistema. El valor predeterminado es 162.
   - **Version** (Versión): elija la versión del protocolo SNMP (que es 1 o 2) en el menú desplegable.
   - **Community** (Comunidad): escriba la línea de la comunidad para el destino de captura.
   - **Enable** (Habilitar): seleccione la casilla de esta columna para habilitar esta dirección de destino como destino de capturas.
7. **Para eliminar una dirección de destino, seleccione la línea que desea eliminar y pulse el botón Trash (Papelera).**
8. **Para guardar los cambios, haga clic en Apply (Aplicar).**

Visualización del estado del sistema

Web Administrator muestra información básica sobre el estado del sistema la primera vez que se accede a él. Las pantallas de estado varían de un modelo a otro, según las funciones y las características físicas del modelo.

La información que se proporciona en esta pantalla resulta útil cuando se llama al servicio técnico, puesto que puede proporcionar una primera pista sobre qué ha fallado en algunos casos.

▼ Para visualizar el estado del sistema

Haga clic en el botón Home (Inicio) de la barra de herramientas.

Esta pantalla proporciona una visualización de sólo lectura de los datos indicados en la TABLA 10-1.

TABLA 10-1 Pantalla de estado del sistema

Nombre	Visualización
Name (Nombre)	El nombre del servidor
Model (Modelo)	El modelo del sistema
Serial # (Nº de serie)	El número de serie exclusivo del sistema
Up Time (Tiempo de actividad)	La cantidad de tiempo que ha transcurrido desde que se encendió por última vez el sistema
CPU Load (Carga de CPU)	La carga actual del procesador y los picos de carga
OS Version (Versión SO)	La versión del sistema operativo instalado en el servidor
Web Admin Version (Versión de Web Admin)	La versión de Web Administrator que se ejecuta en el sistema
Head Status (Estado de unidad)	El estado del servidor H1 (sólo clúster): NORMAL, QUIET, ALONE
Partner Status (Estado asociado)	El estado del servidor H2 (sólo clúster): NORMAL, QUIET, ALONE
Features Enabled (Funciones habilitadas)	Cualquiera de las funciones opcionales habilitadas en el sistema

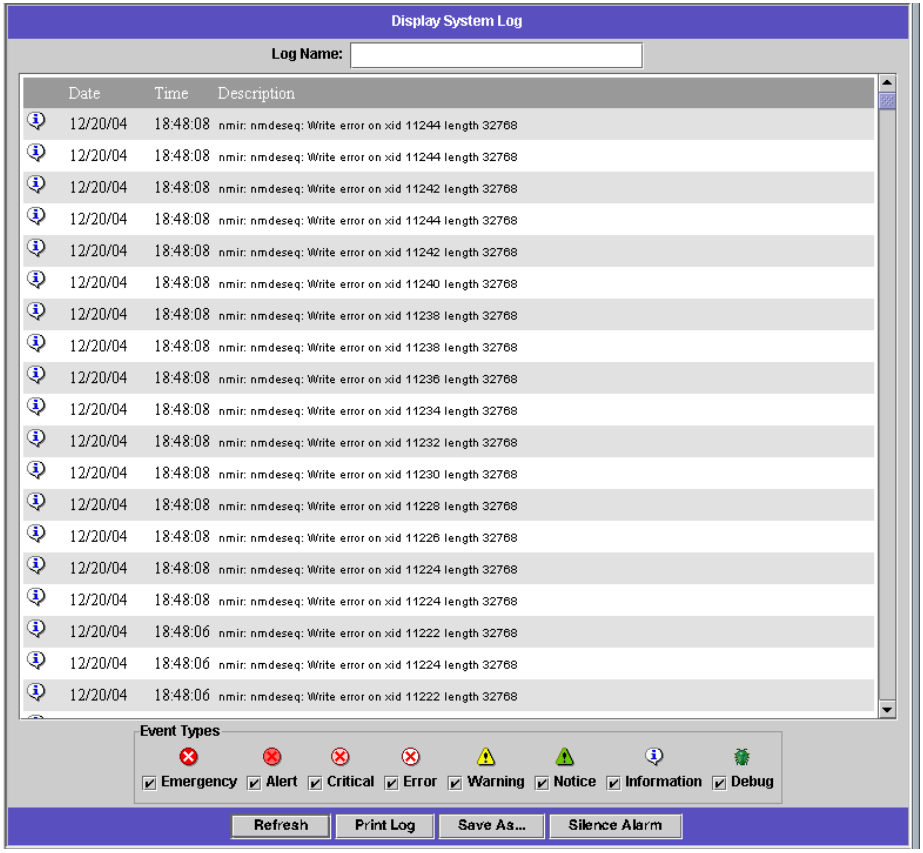
Registro del sistema

El registro del sistema proporciona información básica relacionada con todos los eventos del sistema. El registro proporciona información importante a la hora de determinar qué errores se han producido y cuándo.

Precaución – Debe habilitar el registro remoto o bien crear un archivo de registro en el disco local para evitar que el registro desaparezca cuando se cierre el sistema. Al iniciarlo por primera vez, el sistema crea un archivo de registro temporal en la memoria volátil para registrar los errores que se puedan producir durante el inicio.

El panel **Display System Log** (Mostrar registro del sistema) permite ver todos los eventos del sistema, las advertencias y los errores, incluidas la fecha y la hora a la que se produjeron. Este panel muestra automáticamente los eventos del sistema más recientes y se pueden ver los eventos anteriores con la barra de desplazamiento.

Nota – Los cambios en la configuración de las unidades (como el hecho de eliminar o insertar una unidad) pueden tardar hasta 30 segundos en aparecer en el registro de eventos. En consecuencia, si se producen muchos cambios en el mismo intervalo de tiempo, es posible que algunos eventos no se registren.



▼ Para ver el registro del sistema

1. **En el panel de navegación, seleccione Monitoring and Notification (Supervisión y notificación) > View System Events (Ver eventos de sistema) > Display System Log (Mostrar registro del sistema).**
2. **Active las opciones que desee ver de la sección Event Types (Tipos de eventos).**

   Si desea obtener más información, consulte "Eventos de sistema" en la página 144.
3. **Haga clic en Refresh (Actualizar).**

Nota – Si el registro del sistema contiene mensajes de error que indican volúmenes "Unowned SFS2", llame al servicio técnico para obtener ayuda.

Eventos de sistema

El registro de sistema incluye 8 tipos de eventos de sistema. Cada evento se representa mediante un icono como se muestra en la TABLA 10-2.

TABLA 10-2 Iconos de los eventos de sistema

	**Emergency** (Emergencia): especifica cuáles son los mensajes de emergencia. Este tipo de mensajes no se distribuyen a todos los usuarios. Los mensajes de emergencia prioritarios se registran en un archivo separado para revisarlos.
	**Alert** (Alerta): hace referencia a mensajes importantes que exigen una atención inmediata. Este tipo de mensajes sí se distribuyen a todos los usuarios.
	**Critical** (Crítico): especifica los mensajes críticos que no se clasifican como errores, por ejemplo, los problemas de hardware. Los mensajes críticos y los que tienen una mayor prioridad se envían a la consola del sistema.
	**Error**: especifica qué mensajes representan condiciones de error, como por ejemplo, cuando se intenta escribir en un disco y no se consigue.
	**Warning** (Advertencia): pertenecen a esta categoría los mensajes de condiciones anómalas pero que se pueden recuperar.
	**Notice** (Aviso): pertenecen a esta categoría los mensajes informativos importantes. Los mensajes que no tienen asignada una prioridad se incluyen en esta categoría de mensajes.
	**Information** (Información): especifica cuáles son los mensajes informativos. Estos mensajes son útiles a la hora de analizar el sistema.
	**Debug** (Depuración): especifica cuáles son los mensajes de depuración.

Auditoría del sistema

La auditoría del sistema permite al administrador auditar los eventos de sistema que desee almacenando las entradas de estos eventos en archivos de registro. La auditoría es una función independiente de `syslog`; el registro de auditoría se escribe en archivos binarios del sistema local.

El administrador del sistema debe habilitar esta función de auditoría mediante un volumen de archivo configurado como el volumen de almacenamiento del registro de auditoría. Es posible configurar y habilitar la auditoría utilizando Web Administrator, los menús de operador, o comandos CLI.

Configuración de auditoría

Debe especificar el volumen de auditoría, que puede ser cualquier volumen no del sistema. Aunque el sistema no exige que este volumen sirva sólo para auditorías, los volúmenes de auditoría no deben utilizarse para el almacenamiento en general.

El archivo de registro de auditoría tiene un tamaño máximo predeterminado, aunque el usuario lo puede modificar. Cuando el registro de auditoría en uso alcanza este tamaño aproximado (puede variar en 1 kilobyte), este archivo de registro se cierra y se crea uno nuevo.

▼ Para configurar la auditoría del sistema

1. **En el panel de navegación, seleccione Monitoring and Notification (Supervisión y notificación) > Enable System Auditing (Habilitar auditoría del sistema).**
2. **Para habilitar la auditoría del sistema, seleccione la casilla Enable System Auditing (Habilitar auditoría del sistema).**
3. **Seleccione un volumen donde se almacenarán los registros de las auditorías del sistema.**

   Puede elegir volúmenes que no sean de sistema. Debería crear volúmenes con propósitos de auditoría específicos. Consulte "Para crear un volumen de archivo o un segmento con el panel Create File Volume (Crear volumen de archivo)" en la página 45 para obtener instrucciones.

4. **Escriba el tamaño máximo del archivo de registro de auditoría, entre 1 y 1.024 megabytes.**

   El archivo de registro crecerá desde 0 megabytes hasta el tamaño máximo que haya especificado antes de crear un archivo nuevo. Los archivos de registro de auditoría existentes no se eliminarán. Cuando el volumen alcanza el 90% de espacio ocupado, se envían alertas y se dejan de escribir archivos de registro.

5. **Para guardar las preferencias, haga clic en Apply (Aplicar).**

Archivos de registro de auditoría

El formato de los archivos de registro de auditoría incluye la fecha/marcas de tiempo y el nombre de host del sistema. El archivo de registro actual tendrá el formato *AAAAMMDDhhmmss*`.not_terminated.nombre host`.

Las marcas de tiempo son en formato de GMT. Por ejemplo, si el archivo de registro actual se creó el 21 de octubre, 2005, a las 1:15 PM GMT en el host del dispositivo Sun StorEdge 5310 NAS =`host prueba`, sería el archivo `20051021131500.not_terminated.host prueba`.

Una vez que el archivo de registro se cierra, el nombre se convierte según el mismo formato de marca de tiempo. Por ello, si este mismo archivo de ejemplo alcanzó el tamaño máximo el 30 de octubre, 2005, a las 7:35 PM GMT, el nombre se habrá convertido en `20051021131500.20051030193500.host prueba`.

Los archivos de registro de auditoría poseen atributos especiales. Además de tener permisos de nivel cero, están marcados como imborrables e inmutables, lo que impide eliminarlos, renombrarlos o que sean escritos de otra manera que no sea por el propio sistema. El administrador puede eliminar estos atributos utilizando el comando `chattr`.

Nota – En este momento, la interfaz gráfica de usuario no admite la lectura ni la eliminación de archivos de auditoría.

Eventos auditados

Es posible auditar un número reducido de eventos: encendido y apagado del sistema, creación y eliminación de particiones del disco, y creación y eliminación de volúmenes.

Estos eventos no son configurables.

Lectura de registros de auditoría

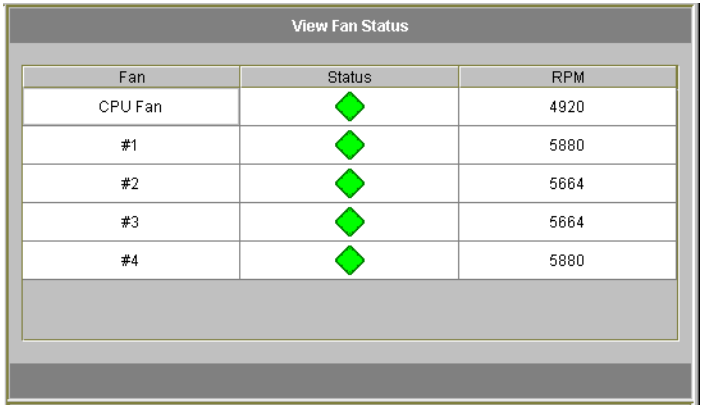
Debido a que los registros de auditoría se almacenan con formato binario, para leerlos se utiliza el comando `praudit`. El comando `praudit` convierte la información binaria de estos registros en texto legible.

Estado del entorno

Puede ver la información del ventilador, la temperatura, el suministro eléctrico y el consumo de voltaje del sistema.

▼ Para ver el estado del ventilador

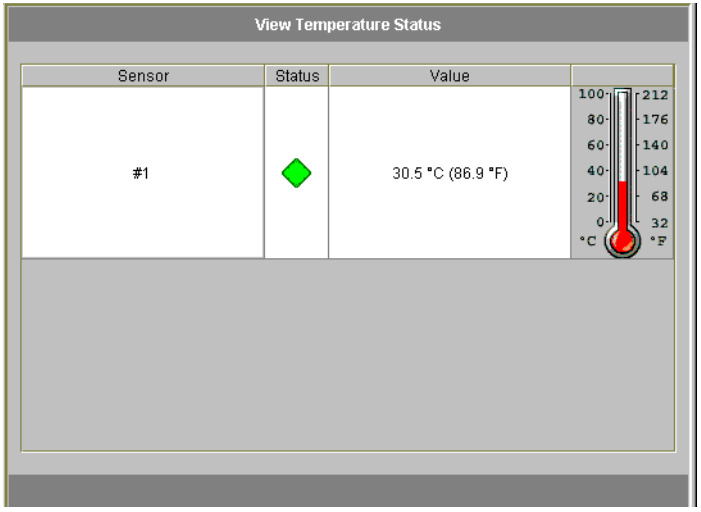
- **Para ver el estado operativo y las revoluciones por minuto (RPM) de todos los ventiladores en la unidad del dispositivo Sun StorEdge 5310 NAS, en el panel de navegación seleccione Monitoring and Notification (Supervisión y notificación) > View Environmental Status (Ver estado del entorno) > View Fan Status (Ver estado de los ventiladores).**



La tabla muestra el estado actual de cada ventilador. Cuando aparece un rombo verde en la columna **Status** (Estado), indica que las RPM del ventilador son normales. Si el rombo es rojo, significa que las RPM han superado el rango de funcionamiento aceptable. Si las RPM de un ventilador son inferiores a 1.800 o algún ventilador queda inactivo, se envía un correo electrónico a los destinatarios que estén especificados. Para obtener información acerca de cómo configurar las notificaciones de correo electrónico, consulte "Configuración de la notificación por correo electrónico" en la página 30.

▼ Para ver el estado de la temperatura

- **Para ver el estado de la temperatura, en el panel de navegación seleccione Monitoring and Notification (Supervisión y notificación) > View Environmental Status (Ver estado del entorno) > View Temperature Status (Ver estado de la temperatura).**

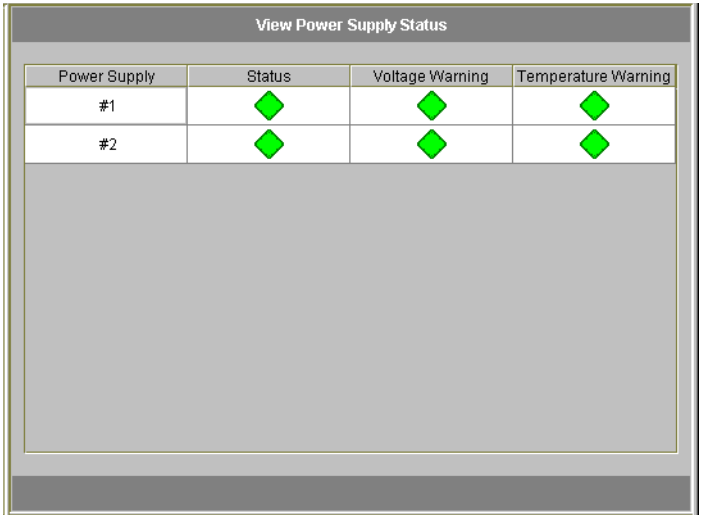


Esta pantalla muestra la temperatura de los sensores de la unidad. Cuando aparece un rombo verde en la columna **Status** (Estado), indica que la unidad está funcionando dentro del rango de temperatura normal. Si el rombo es rojo, significa que la temperatura ha superado el rango aceptable de funcionamiento. Si la temperatura supera los 55° Celsius (131° Fahrenheit), se envía un mensaje de correo electrónico a los destinatarios que se especifiquen. Para obtener información acerca de cómo configurar las notificaciones de correo electrónico, consulte "Configuración de la notificación por correo electrónico" en la página 30.

Nota – Los umbrales de temperatura no se pueden modificar.

▼ Para ver el estado de suministro eléctrico

- **Para ver el estado del suministro eléctrico, en el panel de navegación seleccione Monitoring and Notification (Supervisión y notificación) > View Environmental Status (Ver estado del entorno) > View Power Supply Status (Ver estado del suministro eléctrico).**

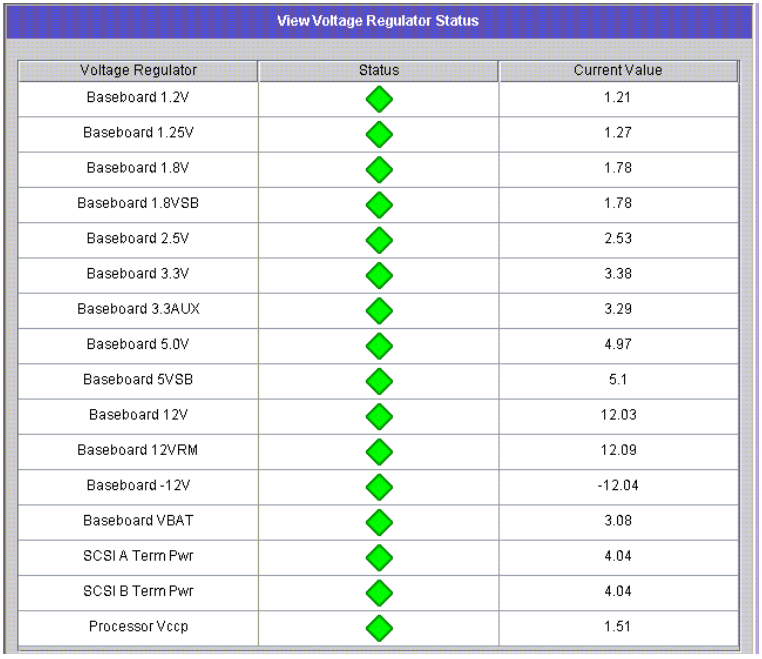


Hay tres columnas que muestran el estado del suministro eléctrico. La columna **Status** (Estado) indica si el suministro eléctrico está funcionando normalmente. Las columnas **Voltage Warning** (Advertencia sobre voltaje) **Temperature Warning** (Advertencia sobre temperatura) indican si el voltaje y la temperatura están en los niveles adecuados.

Un rombo verde en una de estas columnas indica que el voltaje o la temperatura son normales. Si es un rombo de color rojo, significa que la temperatura o el voltaje han superado el rango aceptable de funcionamiento. En este caso, se envía una notificación por correo electrónico a los destinatarios especificados. Para obtener información acerca de las notificaciones por correo electrónico, consulte "Configuración de la notificación por correo electrónico" en la página 30.

▼ Para ver el estado del voltaje

- **Para ver las lecturas del voltaje actual, en el panel de navegación seleccione Monitoring and Notification (Supervisión y notificación) > View Environmental Status (Ver estado del entorno) > View Voltage Regulator Status (Ver estado del regulador de voltaje).**



Consulte la TABLA 10-3 para conocer el rango aceptable de cada voltaje.

TABLA 10-3 Rangos de voltaje aceptables

Valor del voltaje	Intervalo aceptable
Placa base 1,2 V	1,133 V a 1,250 V
Placa base 1,25 V	1,074 V a 1,406 V
Placa base 1,8 V	1,700 V a 1,875 V
Placa base 1,8 VSB (en espera)	1,700 V a 1,875 V
Placa base 2,5 V	2,285 V a 2,683 V
Placa base 3,3 V	3,096 V a 3,388 V

TABLA 10-3 Rangos de voltaje aceptables *(continuación)*

Placa base 3,3 AUX	3,147 V a 3,451 V
Placa base 5,0 V	4,784 V a 5,226 V
Placa base 5 VSB (en espera)	4,781 V a 5,156 V
Placa base 12 V	11,50 V a 12,56 V
Placa base 12 VRM	11,72 V a 12,80 V
Placa base –12 V	–12,62 V a –10,97 V
Placa base VBAT	2,859 V a 3,421 V
SCSI A Term Pwr	4,455 V a 5,01 V
SCSI B Term Pwr	4,455 V a 5,01 V
Procesador Vccp	1,116 V a 1,884 V

Información de uso

Se puede ver la información de uso tanto de volúmenes de archivo como de la actividad de la red y el sistema, y de los puertos de red.

▼ Para ver el uso de un volumen de archivo

- **Para ver qué cantidad de espacio libre y de espacio utilizado tiene un volumen de archivo, seleccione Monitoring and Notification (Supervisión y notificación) en el panel de navegación. Después, seleccione View File Volume Usage (Ver uso del volumen de archivo) para mostrar la capacidad del volumen y el espacio utilizado.**

  Si el uso de un volumen de archivo supera el 95%, se enviará un correo electrónico a los destinatarios especificados.

▼ Para ver la actividad de red

- **Para que se muestre el número de solicitudes de E/S por segundo de todos los clientes del dispositivo Sun StorEdge 5310 NAS, seleccione System Activity (Actividad del sistema) > View Networking Activity (Ver actividad de red) en el panel de navegación.**

▼ Para ver la actividad del sistema

El dispositivo Sun StorEdge 5310 NAS supervisa la actividad y la carga de varios dispositivos mediante el sistema de almacenamiento. Tenga en cuenta que los nombres y el número de los dispositivos que se supervisan dependen de la configuración de hardware de que disponga.

- **Para mostrar las solicitudes de E/S de los dispositivos de sistema, seleccione System Activity (Actividad del sistema) > View System Activity (Ver actividad del sistema) en el panel de navegación.**

  Los dispositivos de red y del sistema figuran en la TABLA 10-4.

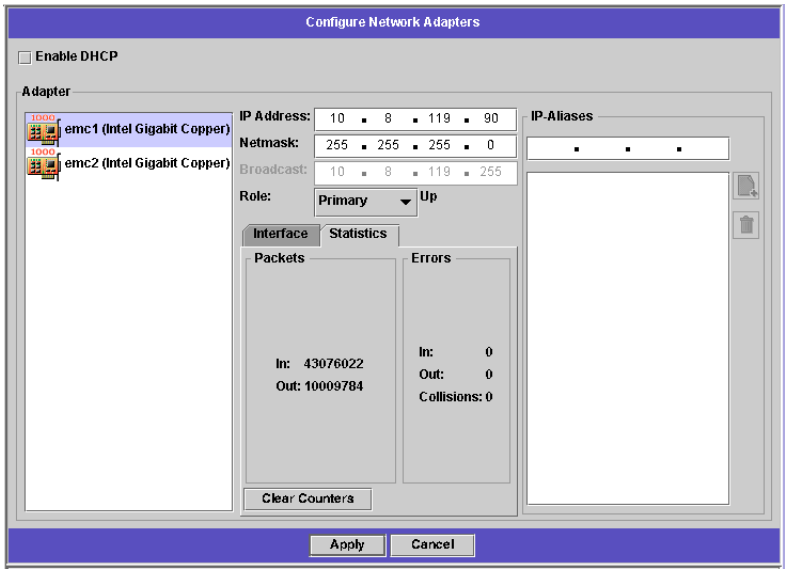
TABLA 10-4 Dispositivos de red y del sistema

Código de dispositivo	Dispositivo
CPU	Unidad central de proceso (CPU) del dispositivo Sun StorEdge 5310 NAS
Memory (Memoria)	Memoria de acceso aleatorio (RAM) del dispositivo Sun StorEdge 5310 NAS
Port Aggregation *x* (Adición de puertos)	Puerto enlazado *x*
Controller *x* (Controlador)	Controlador RAID *x*
dac010*xx*	Números de unidad lógica (LUN) *xx*
PORT*x*	Puerto *x*
Host Adapter *x*(Adaptador de host)	Adaptador de host SCSI *x* (para el dispositivo de copia en cinta)

▼ Para ver las estadísticas de red (puertos)

1. **En el panel de navegación, seleccione Network Configuration (Configuración de red) > Configure TCP/IP (Configurar TCP/IP) > Configure Network Adapters (Configurar adaptadores de red).**

   Se muestra la pantalla de estadísticas de red.



2. **Seleccione el puerto en la lista Adapter (Adaptador).**

   La ficha **Interface** (Interfaz) muestra la siguiente información:

   - **Description** (Descripción): ofrece una descripción del puerto seleccionado.
   - **H/W Address** (Dirección H/W): muestra la dirección de hardware (H/W) o la de control de acceso de dispositivos (MAC, del inglés Media Access Control), que es una dirección única, en notación hexadecimal (hex) que emplea el software de red para distinguir esta tarjeta de red de las demás tarjetas que haya en la red. La dirección está codificada en la tarjeta de red de fábrica.
   - **Speed** (Velocidad): especifica la velocidad (Mbit/segundo) a la que se transmiten los datos por la red.
   - **MTU**: especifica la unidad de transmisión máxima (MTU, del inglés Maximum Transmission Unit) actual del adaptador seleccionado. MTU es la longitud de marco máxima que se puede enviar en un dispositivo físico. El mayor valor MTU posible es el valor predeterminado 1500. El valor mínimo que se puede utilizar es 552.

     El tamaño del segmento máximo TCP coincide con el tamaño del datagrama máximo IP menos 40. El tamaño del datagrama máximo IP es 576. El tamaño del segmento máximo TCP predeterminado es 536.

3. **Haga clic en la ficha Statistics (Estadísticas) para mostrar la siguiente información de entrada y salida acerca del puerto seleccionado:**
   - **Packets In/Out** (Entrada/salida de paquetes): número de entradas y salidas (envíos y recepciones) de paquetes registrado por este puerto.
   - **Errors In/Out** (Entrada/salida de errores): número de entradas y salidas de errores registrado por este puerto.
   - **Collisions** (Colisiones): número de colisiones de transmisión que se han producido en este puerto.

Visualización de las rutas de red

El panel **View the Routing Table** (Ver la tabla de rutas) permite mostrar las rutas por las que se envían los paquetes a la red y los hosts. Dichas rutas consisten en una referencia de entrada de ruta y una red de destino.

Acerca de las rutas

Existen dos tipos diferentes de rutas: **rutas de red** y **rutas de hosts**. Las primeras se utilizan para enviar paquetes a los hosts de una red concreta. Las rutas de host se usan en pocas ocasiones y se implementan para enviar paquetes a un host que no está conectado a ninguna red conocida, sólo a otro host o a otra puerta de enlace.

A continuación, aparecen algunos ejemplos de indicadores de ruta que se muestran en la tabla de rutas:

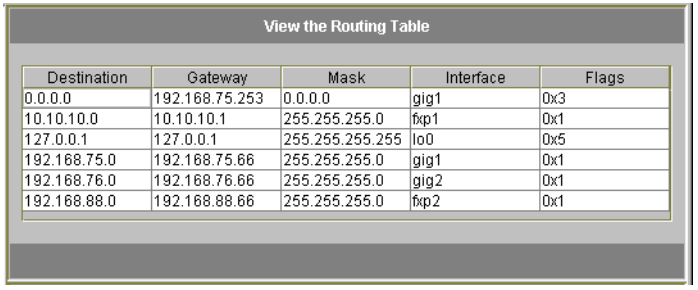
- **0x1**: indica que la ruta se puede utilizar.
- **0x2**: indica que el destino es una puerta de enlace.
- **0x4**: indica que el destino es una entrada de host.
- **0x8**: indica que no se puede establecer contacto con el host o la red.
- **0x10**: indica que el destino se creó dinámicamente.
- **0x20**: indica que el destino se modificó dinámicamente.

Algunos indicadores pueden ser la suma de indicadores individuales. Por ejemplo, **0x3** representaría que la ruta se puede utilizar (**0x1**) e indicaría la presencia de una puerta de enlace (**0x2**), como resultado de la suma de estos dos valores.

▼ Para ver las rutas

Para ver el estado de todas las rutas de la red local, en el panel de navegación, seleccione **Network Configuration (Configuración de red) > View the Routing Table (Ver la tabla de rutas)**.

Se muestra el panel View the Routing Table (Ver la tabla de rutas).



Esta pantalla muestra la siguiente información sobre cada ruta de red:

- **Destination** (Destino): se trata de la dirección IP del destino de la ruta y puede hacer referencia a una red o a un host. Debe haber una ruta predeterminada (destinatario 0.0.0.0), una ruta de bucle inverso (destinatario 127.0.0.1) y, como mínimo, una ruta de red y otra de host.
- **Gateway** (Puerta de enlace): se trata de la dirección de la puerta de enlace por la que viajan los paquetes a su destino.
- **Mask** (Máscara): se trata de la máscara de red para la red de destino.
- **Interface** (Interfaz): indica el tipo de interfaz que se utiliza para enviar paquetes por la red.
- **Flags** (Indicadores): muestran el estado de la ruta. Cada tipo de indicación de estado se representa mediante un número en notación hexadecimal. Si desea obtener más información, consulte "Acerca de las rutas" en la página 154.

Supervisión de los componentes de sistema

Puede supervisar el estado de un dispositivo de suministro ininterrumpido de alimentación (UPS), los controladores y la duplicación.

Supervisión de UPS

Si ha instalado con la unidad un dispositivo de suministro ininterrumpido de alimentación (UPS), puede supervisar el UPS.

Nota – Debe conectar el dispositivo UPS al sistema dispositivo Sun StorEdge 5310 NAS antes de habilitar la supervisión de UPS. De lo contrario, el sistema de supervisión notificará que se ha producido un fallo UPS. Tenga en cuenta también que el dispositivo Sun StorEdge 5310 NAS no admite la gestión UPS, sólo la supervisión UPS. Consulte la Guía básica del *dispositivo Sun StorEdge 5310 NAS y el sistema de puerta de enlace* para obtener información sobre el uso de UPS.

Capacidad de supervisión UPS

La función de supervisión UPS proporciona notificaciones cuando se producen las siguientes circunstancias:

- **Power failure** (Fallo en el suministro eléctrico): indica que se ha producido un fallo en el suministro eléctrico y que el sistema está funcionando con la batería.
- **Power restoration** (Restauración de la alimentación): señala el restablecimiento de la alimentación.
- **Low battery** (Batería baja): indica que la batería tiene poca carga.
- **Recharged battery** (Batería recargada): indica que el dispositivo UPS ha cargado la batería hasta el nivel normal.
- **Battery replacement** (Sustitución de las baterías): indica que el dispositivo UPS ha detectado un problema en la batería y que es necesario sustituirla.
- **UPS alarms** (Alarma UPS): indica que el dispositivo UPS ha detectado que la temperatura ambiente o la humedad sobrepasan los umbrales de seguridad.
- **UPS failure** (Fallo de UPS): indica que el sistema no se puede comunicar con el dispositivo UPS.

Todos los errores (excepto el de batería recargada) se le comunican mediante notificaciones de correo electrónico, notificaciones al servidor SNMP, visualizaciones en la pantalla LCD y visualizaciones en el registro de sistema. La notificación de batería recargada se envía mediante correo electrónico, notificación SNMP y visualización en el registro de sistema (no se genera notificación en la pantalla LCD).

▼ Para habilitar la supervisión UPS

1. **En el panel de navegación, seleccione Monitoring and Notification (Supervisión y notificación) > Enable UPS Monitoring (Habilitar supervisión de UPS).**
2. **Marque la casilla Enable UPS monitoring (Habilitar supervisión de UPS).**
3. **Para guardar los cambios, haga clic en Apply (Aplicar).**

Visualización de la información del controlador

El panel de sólo lectura **View Controller Information** (Visualizar información del controlador) muestra información sobre el proveedor del controlador, el modelo y la versión de firmware.

▼ Para ver el fabricante, el modelo y la versión de firmware del controlador

En el panel de navegación, seleccione **RAID > View Controller Information (Ver información del controlador).**

Visualización del estado de duplicación

El dispositivo Sun StorEdge 5310 NAS elabora una serie de estadísticas de red acerca de los volúmenes de archivo duplicados. Estas estadísticas están disponibles sólo en el servidor activo y en el servidor duplicado de cada volumen de archivo de la duplicación.

▼ Para ver las estadísticas de duplicación

1. **En el panel de navegación, seleccione File Replicator (Replicador de archivos) > View Mirror Statistics (Ver estadísticas de duplicación).**
2. **Seleccione el volumen de archivo que desee en la lista Select Volume (Seleccionar volumen).**

   El sistema muestra la siguiente información acerca del volumen de archivo duplicado:

   - **Status** (Estado): este campo indica el estado de la duplicación. Para obtener definiciones de los indicadores de estado, consulte "Estados de una duplicación" en la página 159.
   - **Incoming Transactions** (Transacciones entrantes): esta sección muestra las siguientes estadísticas acerca del volumen seleccionado:
     - **Average** (Promedio): indica el promedio de transacciones por segundo que viajan hacia el servidor activo.
     - **Minimum** (Mínimo): el menor número de transacciones por segundo que se han recibido en el servidor activo. A la derecha se muestra la fecha y la hora en la que se ha registrado este valor mínimo.
     - **Maximum** (Máximo): el mayor número de transacciones por segundo que se han recibido en el servidor activo. A la derecha se muestra la fecha y la hora en la que se ha registrado este valor máximo.

- **Outgoing Transactions** (Transacciones salientes): esta sección indica las siguientes estadísticas acerca del volumen seleccionado:
  - **Average** (Promedio): indica el promedio de transacciones por segundo que viajan desde el servidor activo hasta el servidor de duplicación.
  - **Minimum** (Mínimo): indica el número mínimo de transacciones por segundo que han viajado desde el servidor activo hasta el servidor de duplicación. A la derecha se muestra la fecha y la hora en la que se ha registrado este valor mínimo.
  - **Maximum** (Máximo): indica el número máximo de transacciones por segundo que han viajado desde el servidor activo hasta el servidor de duplicación. A la derecha se muestra la fecha y la hora en la que se ha registrado este valor máximo.
- **Mirror Buffer** (Búfer de duplicación): esta sección indica el estado de la memoria búfer de duplicación como sigue:
  - **Size** (Tamaño): el número máximo de transacciones que puede contener la memoria búfer.
  - **Free** (Libre): la cantidad de transacciones que quedan en la memoria búfer.
  - **Utilization** (Uso): el porcentaje de transacciones que se emplean en el búfer de duplicación.
  - **Fill Rate** (Tasa de llenado): velocidad a la que se llena la memoria búfer de duplicación (en transacciones por segundo). Si esta tasa es superior a cero, deberá comprobar que todos los enlaces de red estén funcionando correctamente. Esto significa que todas las transacciones están viajando hacia el sistema activo a una velocidad superior que con la que viajan hacia el sistema duplicado, por lo que se llena la memoria búfer.
- **Network Statistics** (Estadísticas de red): esta sección muestra las estadísticas de red de la memoria búfer de duplicación como sigue:
  - **Host**: el nombre de host y el estado de la conexión de la memoria búfer de duplicación.
  - **Link** (Enlace): el estado, la calidad y otras estadísticas del enlace de la memoria búfer de duplicación.
  - **Request Control Blocks** (Bloques de control de solicitudes): el número de bloques de control enviados con el total de bytes enviados, el tamaño medio y la tasa.
  - **Transfer Rate** (Tasa de transferencia): la velocidad media a la que sucede una transferencia, la velocidad máxima y la hora en que se produce la velocidad máxima.
  - **Response Time** (Tiempo de respuesta): el tiempo medio de respuesta, el tiempo máximo y la hora a la que se produce el tiempo de respuesta máximo.

Estados de una duplicación

El estado de una duplicación se muestra en el panel **Manage Mirrors** (Gestionar duplicaciones). Los estados son los siguientes:

- **New** (Nuevo): se está creando una nueva duplicación.
- **Creating mirror log** (Creando registro de la duplicación): se está iniciando la memoria búfer de duplicación.
- **Connecting to host** (Conectando con el host): el servidor activo está conectando con el servidor remoto de la duplicación.
- **Creating extent** (Creando particiones): el servidor de duplicación está creando las particiones de disco.
- **Ready** (Listo): el sistema está preparado y esperando a que los otros sistemas estén listos.
- **Down** (Inactivo): el enlace de red está inactivo.
- **Cracked** (Dañado): la duplicación está dañada.
- **Syncing Volume** (Sincronizando el volumen): el servidor de la duplicación está sincronizando el volumen de archivo.
- **In Sync** (En sincronización): la duplicación está sincronizada.
- **Out of Sync** (Sin sincronización): la duplicación no está sincronizada.
- **Error**: se ha producido un error.

Visualización del estado de trabajos de copia de seguridad

Es posible ver la información sobre los trabajos de copia de seguridad, como el registro, el estado de cada trabajo y el estado de la cinta.

▼ Para ver el registro de copia de seguridad

En el panel de navegación, seleccione **System Backup (Copia de seguridad del sistema) > Manage Backup Jobs (Gestionar trabajos de copia de seguridad) > View Backup Log (Ver registro de copia de seguridad)**.

El registro de copia de seguridad muestra una lista completa de eventos que han sucedido en los procesos de copia de seguridad del sistema e incluye la fecha, la hora y la descripción de cada evento. Desplácese hacia abajo para ver los eventos de copia de seguridad anteriores.

El tamaño total del archivo se muestra en la parte superior de la pantalla. Haga clic en **Refresh** (Actualizar) para actualizar la visualización del archivo de registro.

▼ Para ver el estado del trabajo de copia de seguridad

En el panel de navegación, seleccione **System Backup (Copia de seguridad del sistema) > Manage Backup Jobs (Gestionar trabajos de copia de seguridad) > View Backup Status (Ver estado de copia de seguridad)**.

Esta pantalla muestra los procesos más recientes de copia de seguridad, restauración y limpieza.

Si se está llevando a cabo un proceso de copia de seguridad o de restablecimiento, el botón **Abort Job** (Cancelar trabajo) estará habilitado. Haga clic en este botón para detener un proceso que esté en ejecución y compruebe el panel de eventos de sistema para confirmar que el trabajo se ha cancelado. Deberá esperar varios minutos para que la cancelación surta efecto.

▼ Para ver el estado de la cinta

1. **En el panel de navegación, seleccione System Backup (Copia de seguridad del sistema) > Manage Backup Jobs (Gestionar trabajos de copia de seguridad) > View Tape Status (Ver estado de la cinta).**
2. **Seleccione la información de la cinta que desee ver.**
   - Para ver la información acerca de una cinta en concreto, seleccione la opción **Choose Tape Slot (Elegir ranura de cinta)**. A continuación, seleccione en la lista la ranura correspondiente a la cinta que desee ver.

     La numeración de las ranuras en esta pantalla comienza con el número 1. Sin embargo, es posible que la numeración de las ranuras de su dispositivo particular de copia de seguridad en cinta sea diferente. Si la numeración de las ranuras de su dispositivo de cinta comienza por el cero, seleccione el número 1 en esta pantalla para ver la información sobre la ranura cero de su dispositivo de cinta.
   - Para ver información sobre todas las cintas del dispositivo de cinta, seleccione **All Slots** (Todas las ranuras).

     El sistema tarda uno o dos minutos por ranura para recuperar la información de la cinta, la cual se muestra en la parte inferior de la pantalla. Si selecciona **All Slots** (Todas las ranuras), se incrementa el tiempo necesario para recuperar la información. El dispositivo de cinta no puede recuperar información de las ranuras cuando se está llevando a cabo un proceso de copia de seguridad, de restauración o de limpieza de la unidad.
3. **Haga clic en Apply (Aplicar) para iniciar la recuperación de la cinta.**

Nota – Estos datos no se pueden ver cuando se está llevando a cabo un proceso de copia de seguridad, de restauración o de limpieza de la unidad.

CAPÍTULO 11

Mantenimiento del sistema

En este capítulo se describen las distintas tareas de mantenimiento del sistema.

Incluye los siguientes temas:

- "Ajuste de las opciones de acceso remoto" en la página 161
- "Configuración del acceso a FTP" en la página 162
- "Apagado del servidor" en la página 163
- "Puntos de control de archivo" en la página 164
- "Copia de seguridad y restauración" en la página 170
- "Limpieza de los cabezales" en la página 172
- "Traducción de caracteres CATIA V4/V5" en la página 171
- "Actualización del software del dispositivo Sun StorEdge 5310 NAS" en la página 173
- "Actualización de niveles de revisión del firmware para matriz y unidad de disco" en la página 174

Ajuste de las opciones de acceso remoto

Las funciones de seguridad del sistema incluyen la posibilidad de definir opciones de acceso remoto. Es posible habilitar o deshabilitar los servicios de red utilizados para acceder de forma remota al sistema. Puede ejecutar el sistema en el modo seguro para garantizar la máxima seguridad o también puede habilitar explícitamente ciertas funciones de acceso remoto como, por ejemplo, Telnet, el inicio de sesión remoto y Remote Shell.

Los servicios seguros son Secure Web Admin, que utiliza el nivel de socket seguro (SSL, del inglés Secure Socket Layer) mediante http y Secure Shell (ssh).

▼ Para definir la seguridad de acceso remoto

1. **En el panel de navegación, seleccione System Operations (Operaciones de sistema) > Set Remote Access (Definir acceso remoto).**
2. **Marque la casilla de verificación Secure Mode (Modo seguro) para garantizar la máxima seguridad. En este modo, debe marcar las casillas de verificación asociadas para habilitar Secure Web Admin y Secure Shell.**
3. **Si no emplea el modo seguro, active la casilla de cada servicio que desee habilitar:**
   - Web Admin
   - Telnet
   - Remote Login (Inicio de sesión remoto)
   - Remote Shell (Shell remoto)
4. **Haga clic en Apply (Aplicar).**
5. **Si ha seleccionado el modo seguro, deberá reiniciar el servidor para que la configuración entre en vigor. Consulte** **"Apagado del servidor" en la página 163****.**

Configuración del acceso a FTP

El protocolo de transferencia de archivos (FTP, del inglés File Transfer Protocol) es un protocolo de Internet utilizado para copiar archivos entre un cliente y un servidor. FTP requiere que cada cliente que solicite acceder al servidor se identifique con un nombre de usuario y una contraseña.

Puede establecer tres tipos de usuarios:

- **Administrators** (Administradores), cuyo nombre de usuario es "admin" y tienen la misma contraseña que los clientes de la interfaz gráfica de usuario.

  El administrador tiene acceso "raíz" a todos los volúmenes, directorios y archivos del sistema. El directorio principal del administrador se define con el signo "/".
- **Users** (Usuarios), que tienen un nombre de usuario y una contraseña que se especifica en el archivo de contraseña local o en un servidor NIS o NIS+ remoto.

  El usuario tiene acceso a todos los directorios y archivos dentro del directorio principal del usuario. El directorio principal está definido como parte de la información de la cuenta del usuario y se recupera por el servicio de nombre.
- **Guests** (Invitados), que acceden con el nombre de usuario "ftp" o su alias "anónimo". En este caso se precisa una contraseña pero no es autenticada. Todos los usuarios invitados tienen acceso a todos los directorios y archivos que se encuentran en el directorio principal del usuario "ftp".

Nota – Los usuarios invitados no pueden cambiar el nombre, sobrescribir o eliminar archivos; no pueden crear o eliminar directorios y tampoco pueden cambiar los permisos de los archivos o directorios existentes.

▼ Para configurar los usuarios de FTP

1. **En el panel de navegación, seleccione UNIX Configuration (Configuración de UNIX) > Set Up FTP (Configurar FTP).**
2. **Seleccione la casilla de verificación Enable FTP (Habilitar FTP).**
3. **Seleccione el tipo de acceso FTP activando las casillas de verificación correspondientes:**
   - Allow Guest Access (Permitir acceso a invitado) hace posible que los usuarios anónimos accedan al servidor FTP.
   - Allow User Access (Permitir acceso a usuario) hace posible que todos los usuarios accedan al servidor FTP. Esto no incluye el usuario admin o raíz.

Nota – Los nombres de usuario y las contraseñas deben especificarse en el archivo de contraseña local o en un servidor NIS, NIS+ o LDAP remoto.

   - Allow Admin Access (Permitir acceso de administración) hace posible el acceso raíz a todos los que tengan la contraseña de administración (utilícese con precaución).

Nota – El usuario raíz es aquel cuyo UID es igual a 0 y el usuario especial admin del dispositivo Sun StorEdge 5310 NAS.

---

4. **Para permitir el inicio de sesión, seleccione la casilla de verificación Enable Logging (Habilitar inicio de sesión) y especifique el nombre del archivo de registro.**
5. **Para guardar la configuración, haga clic en Apply (Aplicar).**

Apagado del servidor

El panel **Shut Down the Server** (Apagar el servidor) le permite apagar, detener y reiniciar el servidor. (Consulte "Para apagar el sistema" en la página 242 para obtener información sobre cómo apagar el sistema utilizando Telnet.)

▼ Para apagar, detener o reiniciar el servidor

1. **En el panel de navegación, seleccione System Operations (Operaciones de sistema) > Shut Down the Server (Apagar el servidor).**

2. **Elija una de las siguientes opciones:**
   - **None** (Ninguno): seleccione esta opción si no desea apagar el servidor.
   - **Halt Both Heads** (Detener ambas unidades): seleccione esta opción para apagar los dos servidores en una configuración de clúster. Para reiniciar los servidores, deberá encenderlos manualmente.
   - **Reboot Both Heads** (Reiniciar ambas unidades): seleccione esta opción para apagar y reiniciar los dos servidores en una configuración de clúster.
   - **Reboot Previous Version** (Reiniciar versión previa): seleccione esta opción para apagar el servidor y reiniciarlo con la versión del software previamente cargada. Utilice esta opción si, por ejemplo, ha detectado problemas al actualizar el software. Le permite reiniciar con el software que se instaló la última vez antes de actualizar.

Precaución – Póngase en contacto con el servicio técnico antes de seleccionar la opción Reboot Previous Version (Reiniciar versión previa).

   - **Halt This Head** (Detener esta unidad): seleccione la opción para apagar el servidor en que tiene iniciada la sesión actualmente. El otro servidor permanecerá conectado. Para reiniciar el servidor, deberá encenderlo manualmente.
   - **Reboot This Head** (Reiniciar esta unidad): seleccione la opción para apagar y reiniciar el servidor en que tiene iniciada la sesión actualmente. El otro servidor permanecerá conectado.

3. **Haga clic en Apply (Aplicar).**

Puntos de control de archivo

Los puntos de control, también llamados “puntos de referencia” (en inglés, “c-spot”) son copias virtuales de sólo lectura de un volumen de archivo principal. Mientras que un volumen de archivo esté en un proceso de lectura o escritura, todos los datos existentes en el momento en que se creó el punto de control estarán disponibles. Los puntos de control se utilizan para recuperar archivos eliminados o modificados por error y también para estabilizar las copias de seguridad.

Nota – Un punto de control es una copia virtual del volumen del archivo que se almacena en la misma ubicación física que el propio volumen. No es una copia de seguridad en línea. Si el volumen de archivo se pierde, se perderán también los puntos de control.

Para utilizar los puntos de control de archivo, debe habilitar esta función y crear puntos de control individuales o programados.

Creación de puntos de control de archivo

Puede elegir si desea programar la creación de un punto de control o si desea crear uno inmediatamente. Consulte "Programación de puntos de control de archivo" en la página 166 para obtener información acerca de cómo programar la creación de puntos de control periódicos.

En el panel **Manage Checkpoints** (Gestionar puntos de control), puede crear puntos de control inmediatamente, así como cambiar el nombre de los existentes o eliminarlos. Además de los puntos de control programados, que se crean en días y horas preestablecidos, puede crear puntos de control inmediatos en esta pantalla en cualquier momento.

▼ Para crear un nuevo punto de control manualmente

1. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Edit Properties (Editar propiedades).**
2. **Seleccione el volumen para el que desea crear un punto de control en el menú desplegable Volume Name (Nombre de volumen).**
3. **Asegúrese de que haya una marca de verificación en el cuadro Enable Checkpoints (Habilitar puntos de control).**

   Si no hay ninguna marca, haga clic en Apply (Aplicar).
4. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Configure Checkpoints (Configurar puntos de control) > Manage Checkpoints (Gestionar puntos de control).**
5. **Para crear un punto de control nuevo, haga clic en Create (Crear).**
6. **Seleccione el volumen para el que desea crear un punto de control en el menú desplegable Volume Name (Nombre de volumen).**
7. **Elija una de estas opciones de punto de control:**
   - **Auto Delete** (Eliminación automática): seleccione esta opción para eliminar manualmente el punto de control una vez que los valores de **Keep Days** (Conservar días) y **Keep Hours** (Conservar horas) hayan transcurrido. En esta opción, es el sistema el que asigna automáticamente el nombre al punto de control. Si activa esta opción, deberá seleccionar el número de días y de horas que se debe conservar el punto de control.
   - **Backup** (Copia de seguridad): en esta opción, el nombre predeterminado del punto de seguridad es **Backup**. El punto de control se utiliza para las copias de seguridad locales del sistema de archivos del dispositivo Sun StorEdge 5310 NAS. El punto de control no se elimina automáticamente cuando transcurra un periodo de tiempo determinado.
   - **Manual**: si desea asignar al punto de control un nombre distinto de **Backup** (Copia de seguridad), seleccione esta opción. A continuación, escriba el nombre en el campo **Name** (Nombre). El punto de control no se elimina automáticamente cuando transcurra un periodo de tiempo determinado.
8. **Para crear el punto de control, haga clic en Apply (Aplicar).**

Programación de puntos de control de archivo

El panel **Schedule Checkpoints** (Programar puntos de control) muestra los puntos de control programados y le permite agregar otros nuevos y editar o eliminar los existentes. Para cada punto de control programado, esta pantalla indica el nombre del volumen de archivo, la descripción, la hora y el día programados y la cantidad de tiempo que se debe conservar el punto de control. El valor del campo **Keep** (Conservar) indica el número de días más el número de horas que se debe conservar el punto de control.

Al agregar una línea de programación, el sistema configura automáticamente un punto de control para las fechas y las horas requeridas.

Es posible programar un máximo de cinco puntos de control para cada volumen. En una programación, sin embargo, se pueden especificar muchos.

A continuación, se muestra un ejemplo con varios puntos de control.

			Días	Horas A.M.	Horas P.M.	Mantener	
	Habilitado	Descripción	SMTWTFS	M1234567890E	M1234567890E	Días + Horas	
1.	Y	MTWTF5am5pm	-*****-	-----*------	-----*------	1	0
2.	Y	SunWed1pm	*--*---	----------	-*----------	0	12
3.	Y	MWFmidnight	-*-*-*-	*----------	----------	0	3
4.	Y	Weekend	*-----*	*-----*-----	*-----*-----	0	6
5.	Y	FriEvery2hrs	-----*-	*-*-*-*-*-*-	*-*-*-*-*-*-	0	2

▼ Para agregar un punto de control a la programación

1. **Habilite los puntos de control para el volumen de archivo.**
   a. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Edit Properties (Editar propiedades).**
   b. **Seleccione el volumen en el que desea añadir un punto de control en el menú desplegable Volume Name (Nombre de volumen).**
   c. **Asegúrese de que haya una marca de verificación en el cuadro Enable Checkpoints (Habilitar puntos de control).**

      Si no hay ninguna marca, haga clic en Apply (Aplicar).
2. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Configure Checkpoints (Configurar puntos de control) > Schedule Checkpoints (Programar puntos de control).**
3. **Para agregar un punto de control a la programación, haga clic en Add (Agregar).**
4. **Seleccione el volumen de archivo para el que desea programar puntos de control.**

5. **En el campo Description (Descripción), escriba detalles sobre el punto de control.**

   Este campo es obligatorio. Puede especificar información acerca de la periodicidad de los puntos de control como, por ejemplo, “semanal” o “diario”.

6. **En los cuadros Keep Days + Hours (Conservar Días +Horas), seleccione el número de días y de horas que se deben conservar los puntos de control.**

7. **En el campo Days (Días), especifique cuándo se deben crear los puntos de control.**

   Para seleccionar más de un día en la lista, mantenga pulsada la tecla Ctrl mientras selecciona los demás días con el ratón.

8. **En la lista AM Hours (Horas antes de mediodía), seleccione las horas de la mañana en que se deben crear los puntos de control.**

   Para seleccionar más de un elemento en la lista, mantenga pulsada la tecla Ctrl mientras selecciona los demás elementos con el ratón.

9. **En la lista PM Hours (Horas después de mediodía), seleccione las horas de la tarde o de la noche en que se deben crear los puntos de control.**

   Para seleccionar más de un elemento en la lista, mantenga pulsada la tecla Ctrl mientras selecciona los demás elementos con el ratón.

10. **Para guardar los cambios, haga clic en Apply (Aplicar).**

▼ Para editar un punto de control existente en la programación

1. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Configure Checkpoints (Configurar puntos de control) > Schedule Checkpoints (Programar puntos de control).**

2. **Seleccione la línea de la programación que desea editar y haga clic en Edit (Editar).**

3. **La información que se muestra en esta pantalla es idéntica a la del cuadro de diálogo Add Checkpoint Schedule (Agregar programación de puntos de control), excepto que no se puede cambiar el nombre del volumen.**

4. **Edite la información que proceda.**

   Para obtener más información, consulte “Para agregar un punto de control a la programación” en la página 166.

5. **Para guardar los cambios, haga clic en Apply (Aplicar).**

▼ Para eliminar una línea de la programación

1. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Configure Checkpoints (Configurar puntos de control) > Schedule Checkpoints (Programar puntos de control).**

2. **Haga clic en la línea de la programación que desee eliminar y haga clic en Remove (Eliminar).**

▼ Para cambiar el nombre de un punto de control

1. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Configure Checkpoints (Configurar puntos de control) > Manage Checkpoints (Gestionar puntos de control).**
2. **Seleccione el punto de control cuyo nombre desee cambiar y haga clic en Rename (Cambiar nombre).**

   Los campos **Volume Name** (Nombre de volumen) y **Old Name** (Nombre antiguo) son de sólo lectura.
3. **En el campo New Name (Nombre nuevo), escriba el nombre nuevo del punto de control.**

Precaución – Si cambia el nombre de un punto de control de eliminación automática por un nombre común, este punto de control no se eliminará.

4. **Para guardar los cambios, haga clic en Apply (Aplicar).**

▼ Para eliminar un punto de control

1. **En el panel de navegación, seleccione File Volume Operations (Operaciones con volúmenes de archivo) > Configure Checkpoints (Configurar puntos de control) > Manage Checkpoints (Gestionar puntos de control).**
2. **Seleccione el punto de control que desee eliminar y haga clic en Remove (Eliminar).**

Cómo compartir puntos de control de archivo

Los puntos de control se pueden compartir, lo que permite que todos los usuarios accedan a los datos existentes cuando se creó el punto de control.

▼ Para compartir los puntos de control de archivo

1. **En el panel de navegación, seleccione Windows Configuration (Configuración de Windows) > Configure Shares (Configurar recursos compartidos).**
2. **Haga clic en Add (Agregar).**
3. **Escriba el nombre de recurso compartido del punto de control en el cuadro Share Name (Nombre del recurso compartido).**

   El nombre del recurso compartido se utiliza para acceder al punto de control desde la red.

4. **La opción Mac Extensions (Extensiones de Mac) está activada de forma predeterminada.**

5. **Haga clic en el cuadro de menú desplegable Volume Name (Nombre de volumen) y seleccione el volumen del punto de control en la lista.**

   Los volúmenes de puntos de control tienen la extensión ".chkpnt".

6. **Deje en blanco el campo Directory (Directorio).**

7. **Si ADS está habilitado y configurado, escriba un contexto ADS en el cuadro de texto Container (Contenedor).**

8. **Los siguientes campos y opciones aparecerán deshabilitados si el sistema está configurado para el modo de dominio NT; de lo contrario, complete la información como se indica:**

   a. **Escriba 0 en el cuadro User (Usuario).**

   b. **Escriba 0 en el cuadro Group (Grupo).**

   c. **Deje en blanco los cuadros R/W Password (Contraseña lectura/escritura) y R/O Password (Contraseña de sólo lectura).**

      Los volúmenes de punto de control son de sólo lectura.

9. **Haga clic en Apply (Aplicar).**

   Observe que el nuevo punto de control aparece como un recurso compartido en el panel Configure Share (Configurar recurso compartido).

Acceso a los puntos de control de archivo

Los usuarios pueden acceder a los puntos de control, lo que les permite acceder a los datos existentes cuando se creó el punto de control.

▼ Para acceder a un punto de control

1. **Utilizando una estación de red, haga clic en el menú Start (Inicio) de Windows.**

2. **Seleccione Run (Ejecutar).**

3. **En el cuadro Run (Ejecutar), escriba la dirección IP del servidor de dispositivo Sun StorEdge 5310 NAS y el nombre del punto de control compartido.**

   Por ejemplo, escriba `\\xxx.xxx.xxx.xxx\recursocompartido`.

4. **Haga clic en OK (Aceptar).**

Copia de seguridad y restauración

El dispositivo Sun StorEdge 5310 NAS admite copias de seguridad NDMP de la red.

Configuración de NDMP

El protocolo de gestión de datos de red (NDMP, del inglés Network Data Management Protocol) es un protocolo abierto para copias de seguridad basadas en red. La arquitectura NDMP le permite usar aplicaciones de administración de copias de seguridad compatibles con el protocolo NDMP para realizar copias de seguridad de su dispositivo de almacenamiento conectado a red.

Nota – La aplicación de administración de copias de seguridad debe configurarse para iniciar sesión con el nombre de usuario "administrator" y con la contraseña del administrador de consola (interfaz de línea de comandos).

Nota – Los puntos de control deben estar habilitados para realizar copias de seguridad NDMP de volúmenes. Consulte "Creación de puntos de control de archivo" en la página 165.

▼ Para configurar NDMP

1. **En el panel de navegación, seleccione System Backup (Copia de seguridad del sistema) > Set Up NDMP (Configurar NDMP).**
2. **Seleccione la tarjeta NIC NDMP que se debe usar para transferir los datos a la unidad de cinta de copia de seguridad.**
3. **En la pantalla aparece la dirección de la puerta de enlace para cada puerto.**

   Si el dispositivo de cinta de copia de seguridad NDMP está ubicado en otra red, asegúrese de seleccionar el puerto que conecta con la puerta de enlace correcta.
4. **Haga clic en Apply (Aplicar).**

Traducción de caracteres CATIA V4/V5

El dispositivo Sun StorEdge 5310 NAS y el sistema de puerta de enlace interoperan con los productos CATIA V4/V5 (desarrollados por Dessault Systemes).

CATIA V4 es un producto sólo para UNIX, mientras que CATIA V5 está disponible tanto para plataformas de UNIX como de Windows. CATIA V4 puede utilizar determinados caracteres en los nombres de archivo que no son válidos en Windows. Cuando los clientes de CATIA migran del producto V4 al V5, se puede perder el acceso a los archivos de V4 en Windows si los nombres de tales archivos contienen caracteres no válidos en Windows. Por este motivo, se ha incluido una opción de traducción de caracteres para la interoperabilidad de CATIA V4/V5 en UNIX y Windows.

La traducción de caracteres se muestra en la TABLA 11-1.

TABLA 11-1 Tabla de traducción de caracteres CATIA

Carácter CATIA V4 de UNIX	Carácter CATIA V5 de Windows	Descripción de caracteres de CATIA V5
Comillas dobles abiertas tipográficas (no ilustrado)	¨	Diéresis
*	¤	Signo de moneda
/	ø	La O minúscula latina con barra
:	÷	Signo de división
<	«	Corchetes dobles en ángulo izquierdos
>	»	Corchetes dobles en ángulo derechos
?	¿	Signo de interrogación invertido
\	ÿ	La y minúscula latina con diéresis
|	Barra dividida (no ilustrado)	Barra dividida

La interoperabilidad de CATIA V4/V5 está deshabilitada de forma predeterminada. Puede habilitar esta función manualmente desde la interfaz de línea de comandos o después de un reinicio del sistema.

▼ Para habilitar CATIA desde la interfaz de línea de comandos

- **Envíe el comando** `load catia` **utilizando la interfaz de línea de comandos. Con este método, es necesario habilitar CATIA después de cada reinicio del sistema.**

▼ Para habilitar CATIA automáticamente tras un reinicio

1. **Edite el archivo** `/dvol/etc/inetload.ncf` **para añadir la palabra** `catia` **en una línea aparte dentro del archivo.**
2. **En la interfaz de línea de comandos, envíe los dos comandos siguientes para reiniciar el servicio** `inetload`**:**

   ```
   unload inetload
   load inetload
   ```

   Si la compatibilidad de CATIA V4/V5 está habilitada con éxito, en el registro del sistema se muestra una entrada similar a la siguiente:

   ```
   07/25/05 01:42:16 I catia: $Revision: 1.1.4.1
   ```

Limpieza de los cabezales

Puede ver información acerca de la última limpieza realizada o configurar la próxima limpieza de cabezales del dispositivo de cinta local:

▼ Para ejecutar la limpieza de cabezales

1. **En el panel de navegación, seleccione System Backup (Copia de seguridad del sistema) > Assign Cleaning Slot (Asignar ranura de limpieza).**
2. **Seleccione el número de ranura que contiene la cinta limpiadora para limpiar el cabezal en cuestión.**

   La numeración de las ranuras en esta pantalla comienza con el número 1. Sin embargo, es posible que la numeración de las ranuras de su dispositivo particular de copia de seguridad en cinta sea diferente. Si la numeración de las ranuras de su dispositivo de cinta comienza por el cero, seleccione el número 1 en esta pantalla para ver la información sobre la ranura cero de su dispositivo de cinta.

3. **Asigne un número de recuento de limpieza para realizar un seguimiento del número de veces que se usa una cinta limpiadora para limpiar los cabezales.**

   Antes de desechar una cinta limpiadora, debe usarla 10 veces como máximo. Este número aumenta gradualmente cada vez que se lleva a cabo una limpieza de cabezales.

4. **Para realizar ahora una limpieza, seleccione la casilla de verificación Run Immediately (Ejecutar inmediatamente) para comenzar la limpieza con el número de ranura y el recuento de limpieza especificados.**

5. **Para guardar los cambios, haga clic en Apply (Aplicar). Si activa la casilla Run Immediately (Ejecutar inmediatamente), el trabajo de limpieza comienza ahora mismo.**

Actualización del software del dispositivo Sun StorEdge 5310 NAS

Póngase en contacto con el servicio de asistencia técnica de Sun Microsystems con el fin de obtener los archivos de actualización de la configuración del sistema. Cuando tenga los archivos, utilice el panel **Update Software** (Actualizar software) para actualizar el software del dispositivo Sun StorEdge 5310 NAS.

Precaución – No actualice el software del sistema ni el firmware de RAID cuando el subsistema RAID esté en estado crítico, creando un volumen nuevo o reconstruyendo uno existente.

▼ Para actualizar el software

En el siguiente procedimiento, es necesario reiniciar el sistema una vez completado el proceso de actualización. El reinicio del sistema exige que se detengan todas las E/S; por esto, actualice el software durante un periodo de mantenimiento planeado.

Nota – En una configuración de clúster, siga este procedimiento con ambos servidores del clúster.

1. **En el panel de navegación, seleccione System Operations (Operaciones de sistema) > Update Software (Actualizar software).**

2. **En el panel Update Software (Actualizar software), escriba la ruta en la que se encuentran los archivos de actualización.**

   Si necesita buscar la ruta, haga clic en **Browse** (Examinar).

3. **Haga clic en Update (Actualizar) para comenzar el proceso.**

4. **Cuando haya terminado el proceso de actualización, haga clic en Yes (Sí) para reiniciar, o en No para continuar sin reiniciar.**

   La actualización no surte efecto hasta que se reinicie el sistema.

Actualización de niveles de revisión del firmware para matriz y unidad de disco

Esta sección explica cómo se determinan los niveles de revisión del firmware de la matriz y la unidad de disco, y la manera de actualizar el firmware. Incluye los siguientes temas:

- "Cómo determinar si se necesita la actualización del firmware" en la página 174
- "Actualización del firmware para matriz y unidad de disco (exige el reinicio)" en la página 175
- "Actualización del firmware para matriz (no exige el reinicio)" en la página 177
- "Actualización del firmware para unidades de disco (exige el reinicio)" en la página 181

Cómo determinar si se necesita la actualización del firmware

Para decidir si se requiere una actualización del firmware, en primer lugar debe determinar el nivel de revisión del firmware actual de cada componente de la matriz.

Puede utilizar el comando `raidctl profile` para capturar y registrar el nivel de revisión del firmware de cada controlador RAID, unidad de expansión, NVSRAM de controlador y unidad de disco. Si desea obtener más información, consulte "Captura de la salida del comando `raidctl`" en la página 183.

Actualización del firmware para matriz y unidad de disco (exige el reinicio)

Utilice este procedimiento para actualizar el firmware de matriz RAID y unidad de disco. En este procedimiento es necesario reiniciar el servidor NAS.

Si no es posible reiniciar el servidor NAS y debe actualizar sólo el firmware para la matriz, consulte "Actualización del firmware para matriz (no exige el reinicio)" en la página 177.

El periodo de tiempo que se tarda en completar la actualización del firmware puede variar y depende de la configuración. Por ejemplo, llevará unos 50 minutos actualizar y reiniciar un servidor NAS con dos controladores RAID, su unidad de expansión Fibre Channel (FC) y su unidad de expansión SATA (Serial Advanced Technology Attachment). Consulte la TABLA 11-3 para determinar el tiempo que requerirá su configuración.

Nota – Al actualizar el firmware de la unidad de disco, se requiere reiniciar el servidor NAS.

Nota – Todas las unidades de cada tipo se actualizarán, incluso las que ya posean el nivel de revisión del archivo de firmware actual.

Precaución – No realice este procedimiento si alguna unidad ha fallado y se encuentra en estado de reconstrucción. La información puede verse en el registro del sistema o en la página RAID de Web Administrator.

Antes de iniciar el procedimiento, asegúrese de que está instalada la versión 4.10, build 18, (como mínimo) de software del servidor NAS. No intente actualizar el firmware de las matrices y unidades en un servidor NAS que ejecute una versión anterior del sistema operativo.

1. **Descargue el último parche de `www.sunsolve.sun.com` y descomprima el archivo.**
2. **Lea el archivo `readme` del parche para determinar cuáles son los niveles de revisión del firmware asociados con el parche.**
3. **Desde un cliente NAS, habilite FTP.**

   Para obtener más información acerca de cómo habilitar FTP con la interfaz gráfica de usuario, consulte "Configuración del acceso a FTP" en la página 162. Consulte "Configuración del acceso a FTP" en la página 239 si está utilizando la interfaz de línea de comandos.
4. **Desplácese al directorio en que ha descargado el parche.**

5. **Utilice FTP para conectarse al servidor NAS, e inicie la sesión como el usuario admin.**

6. **Escriba `bin` para el modo binario.**

7. **En el indicador `ftp`, cree los siguientes directorios en `/cvol` utilizando estos comandos:**

```
mkdir /cvol/firmware
mkdir /cvol/firmware/2882
mkdir /cvol/firmware/2882/ctlr
mkdir /cvol/firmware/2882/nvsram
mkdir /cvol/firmware/2882/jbod
mkdir /cvol/firmware/2882/drive
```

8. **Cambie al directorio que ha creado para el firmware y copie el archivo de firmware (consulte la TABLA 11-2) con el comando `put`.**

   Por ejemplo, si quiere cargar el firmware para el controlador RAID, ejecute estos comandos:

```
cd /cvol/firmware/2882/ctlr
put SNAP_288X_06120910.dlp
```

9. **Prosiga con la carga del archivo de firmware en los directorios correctos.**

   La TABLA 11-2 muestra el directorio y el archivo de firmware de ejemplo para cada componente.

TABLA 11-2 Directorios y archivos de firmware de los componentes

Componente	Directorio	Nombre de archivo de ejemplo
Controlador RAID	`/cvol/firmware/2882/ctlr`	`SNAP_288X_06120910.dlp`
NVSRAM de controlador RAID	`/cvol/firmware/2882/nvsram`	`N2882-612843-503.dlp`
Unidad de expansión FC	`/cvol/firmware/2882/jbod`	`esm9631.s3r`
Unidad de expansión SATA	`/cvol/firmware/2882/jbod`	`esm9722.dl`
Tipos de unidades:		
Seagate ST314680	`/cvol/firmware/2882/drive`	`D_ST314680FSUN146G_0407.dlp`
Seagate 10K	`/cvol/firmware/2882/drive`	`D_ST314670FSUN146G_055A.dlp`
Hitachi 400GB HDS724040KLSA80	`/cvol/firmware/2882/drive`	`D_HDS7240SBSUN400G_AC7A.dlp`
Fujitsu MAT3300F 300GB	`/cvol/firmware/2882/drive`	`D_MAT3300FSUN300G_1203.dlp`
Seagate 10K 300GB	`/cvol/firmware/2882/drive`	`D_ST330000FSUN300G_055A.dlp`

10. **Cierre la sesión de FTP.**

11. **Utilice Telnet para conectarse al servidor NAS, e inicie sesión con una cuenta de usuario con privilegios admin.**

12. **Reinicie el sistema. En una configuración de clúster, reinicie los dos servidores.**

    La TABLA 11-3 indica el tiempo aproximado que tarda la actualización del firmware de cada componente.

TABLA 11-3 Tiempo de actualización del firmware

Componente	Tiempo para finalizar la actualización
Controlador RAID	Reinicio más 15 minutos
NVSRAM de controlador RAID	Reinicio más 5 minutos
Unidad de expansión FC o SATA	Reinicio más 5 minutos
Unidades	Reinicio más 1,5 minutos por cada unidad

13. **Confirme que el firmware nuevo se ha cargado con este comando:**

    `raidctl get type=lsi target=profile ctlr=0`

    También puede comprobar si hay errores en el registro del sistema.

Actualización del firmware para matriz (no exige el reinicio)

Con este procedimiento se actualiza el firmware de la matriz RAID sin necesidad de reiniciar el servidor NAS.

Antes de empezar, tenga en cuenta lo siguiente:

- El servidor NAS debe tener instalada la versión 4.10, build 18, (como mínimo) del software. No intente actualizar el firmware en un servidor NAS que ejecute una versión anterior del sistema operativo.
- Este procedimiento da el mejor resultado con una actividad de E/S limitada. El controlador detendrá las E/S durante el proceso.

Precaución – No realice este procedimiento si alguna unidad ha fallado y se encuentra en estado de reconstrucción. Puede ver esta información en el registro del sistema.

1. **Descargue el último parche de `www.sunsolve.sun.com` y descomprima el archivo.**

2. **Lea el archivo `readme` del parche para determinar cuáles son los niveles de revisión del firmware asociados con el parche.**

3. **Desplácese al directorio en que ha descargado el parche.**

4. **Desde un cliente NAS, habilite FTP.**

   Para obtener más información acerca de cómo habilitar FTP con la interfaz gráfica de usuario, consulte "Configuración del acceso a FTP" en la página 162. Consulte "Configuración del acceso a FTP" en la página 239 si está utilizando la interfaz de línea de comandos.

5. **Utilice FTP para conectarse al servidor NAS, e inicie sesión con una cuenta de usuario con privilegios admin.**

6. **Escriba `bin` para el modo binario.**

7. **En el indicador `ftp`, cree los siguientes directorios en `/cvol` utilizando estos comandos:**

```
mkdir /cvol/firmware
mkdir /cvol/firmware/2882
mkdir /cvol/firmware/2882/ctlr
mkdir /cvol/firmware/2882/nvsram
mkdir /cvol/firmware/2882/jbod
```

8. **Cambie al directorio que ha creado para el firmware y copie el archivo de firmware (consulte la TABLA 11-4) con el comando `put`.**

   Por ejemplo, si quiere cargar el firmware para el controlador RAID, ejecute estos comandos:

```
cd /cvol/firmware/2882/ctlr
put SNAP_288X_06120910.dlp
```

9. **Prosiga con la carga del archivo de firmware en los directorios correctos.**

   La TABLA 11-4 muestra el directorio y el archivo de firmware de ejemplo para cada componente.

TABLA 11-4 Directorios y archivos de firmware de los componentes

Componente	Directorio	Nombre de archivo de ejemplo
Controlador RAID	`/cvol/firmware/2882/ctlr`	`SNAP_288X_06120910.dlp`
NVSRAM de controlador RAID	`/cvol/firmware/2882/nvsram`	`N2882-612843-503.dlp`
Unidad de expansión FC	`/cvol/firmware/2882/jbod`	`esm9631.s3r`
Unidad de expansión SATA	`/cvol/firmware/2882/jbod`	`esm9722.dl`

10. **Cierre la sesión de FTP.**

11. **Utilice Telnet para conectarse al servidor NAS, e inicie sesión con una cuenta de usuario con privilegios admin.**

12. **Utilice el comando** `raidctl download` **para cargar cada archivo en el directorio de destino.**

    Por ejemplo, si desea cargar el firmware de controlador desde el directorio `ctlr` al controlador 0 y 1, envíe este comando:

    ```
    raidctl download type=lsi target=ctlr ctlr=0
    ```

    Este comando descarga el archivo de firmware en los dos controladores y elimina el archivo del directorio.

    Nota – El comando `raidctl download` elimina el archivo de firmware cada vez que se invoca. Por ello, deberá volver a copiar el archivo del firmware después de actualizar cada componente (controlador, NVSRAM de controlador, unidad de expansión, unidades de disco).

    Para descargar el firmware situado en el directorio `jbod` al armario de expansión 0, envíe este comando:

    ```
    raidctl download type=lsi target=jbod ctlr=0
    ```

13. **Supervise el progreso de cada descarga desde la sesión de Telnet.**

    El tiempo aproximado para completar cada una de las descargas es el siguiente:

Componente	Minutos por componente
UE de controlador RAID	15 minutes
NVSRAM de controlador RAID	5 minutes
Unidad de expansión FC o SATA	5 minutes

    Nota – Cuando termina la actualización, el cursor de `telnet` puede demorar hasta 5 minutos en aparecer. Aguarde hasta que vuelva a mostrarse el cursor.

    ---

14. **Antes de continuar con el siguiente componente, compruebe si la descarga está completa en el registro del sistema.**

    El siguiente ejemplo muestra la salida del registro del sistema:

```
Ctrl-

Firmware Download  90% complete
Firmware Download  95% complete
Firmware Download 100% complete
Waiting for controllers to become ACTIVE
Controller 0 - now ACTIVE
Controller 1 - now ACTIVE
Controllers are now active
nvsram-

raidctl download type=lsi target=nvsram ctlr=0
Flashing C0 NVSRAM: /cvol/nf2/../firmware/2882/nvsram/n2882-
61.dlp (48068)
Firmware Download 100% complete
Waiting for controllers to become ACTIVE
Controller 0 - now ACTIVE
Controller 1 - now ACTIVE
Controllers are now active
ESM-
```

```
>> raidctl download type=lsi target=jbod ctlr=0 tray=1

Flashing C0 JBOD 1 with
/cvol/nf1/../firmware/2882/jbod/esm9631.s3r (663604)
Firmware Download  20% complete
Firmware Download  30% complete
Firmware Download  50% complete
Firmware Download  60% complete
Firmware Download  90% complete
Firmware Download 100% complete
Waiting for controllers to become ACTIVE
Controller 0 - now ACTIVE
Controller 1 - now ACTIVE
Controllers are now active
Drive-
10/26/05 10:57:42 I Firmware Download  20% complete
10/26/05 10:57:46 I Firmware Download  30% complete
10/26/05 10:57:50 I Firmware Download  40% complete
10/26/05 10:57:54 I Firmware Download  50% complete
10/26/05 10:57:58 I Firmware Download  60% complete
10/26/05 10:58:03 I Firmware Download  70% complete
10/26/05 10:58:08 I Firmware Download  80% complete
10/26/05 10:58:13 I Firmware Download  90% complete
10/26/05 10:58:18 I Bytes Downloaded: 628224 (2454 256 chunks),
imageSize=62804
                    8
10/26/05 10:59:01 I Flashed OK - drive in tray 2 slot 12
10/26/05 10:59:01 I Downloaded firmware version 0407 to 27 drives
```

Actualización del firmware para unidades de disco (exige el reinicio)

Utilice este procedimiento para actualizar el firmware de unidad de disco exclusivamente. En este procedimiento es necesario reiniciar el servidor NAS.

Nota – Al actualizar el firmware de la unidad de disco, se requiere reiniciar el servidor NAS.

Nota – Todas las unidades de cada tipo se actualizarán, incluso las que ya posean el nivel de revisión del archivo de firmware actual.

El tiempo que se requiere para terminar una actualización puede variar según el número de unidades que estén instaladas, a lo que se suma el tiempo que tarda el reinicio del servidor NAS. Consulte TABLA 11-3 para determinar el tiempo que requerirá su configuración.

Precaución – No realice este procedimiento si alguna unidad ha fallado y se encuentra en estado de reconstrucción. Puede ver esta información en el registro del sistema.

Antes de empezar a actualizar el firmware de las unidades, asegúrese de que está instalada la versión 4.10, build 18, (como mínimo) de software del servidor NAS. No intente actualizar el firmware en un servidor NAS que ejecute una versión anterior del sistema operativo.

1. **Descargue el último parche de `www.sunsolve.sun.com` y descomprima el archivo.**
2. **Lea el archivo `readme` del parche para determinar cuáles son los niveles de revisión del firmware asociados con el parche.**
3. **Desplácese al directorio en que ha descargado el parche.**
4. **Desde un cliente NAS, habilite FTP.**

   Para obtener más información acerca de cómo habilitar FTP con la interfaz gráfica de usuario, consulte "Configuración del acceso a FTP" en la página 162. Consulte "Configuración del acceso a FTP" en la página 239 si está utilizando la interfaz de línea de comandos.
5. **Utilice FTP para conectarse al servidor NAS, e inicie la sesión como el usuario `admin`.**
6. **Escriba `bin` para el modo binario.**
7. **En el indicador `ftp`, cree el siguiente directorio en `/cvol` utilizando este comando:**

   ```
   mkdir /cvol/firmware/2882/drive
   ```
8. **Cambie al directorio que ha creado para el firmware de unidades y copie los archivos de firmware (consulte la TABLA 11-2) con el comando `put`.**

   Por ejemplo, si quiere cargar el firmware de la unidad Seagate ST314680, ejecute estos comandos:

   ```
   cd /cvol/firmware/2882/drive
   put D_ST314680FSUN146G_0407.dlp
   ```
9. **Cierre la sesión de FTP.**
10. **Utilice Telnet para conectarse al servidor NAS, e inicie la sesión como el usuario `admin`.**

11. **Reinicie el sistema. En una configuración de clúster, reinicie los dos servidores.**

    El tiempo aproximado requerido para terminar la actualización es el tiempo del reinicio más 1,5 minuto para cada unidad.

12. **Confirme que el firmware nuevo se ha cargado con este comando:**

    `raidctl get type=lsi target=profile ctlr=0`

    También puede comprobar si hay errores en el registro del sistema.

Captura de la salida del comando `raidctl`

Puede utilizar el comando `raidctl profile` para determinar el nivel de revisión del firmware de cada controlador RAID, unidad de expansión, NVSRAM de controlador y unidad de disco. Esta sección contiene las instrucciones de los siguientes procedimientos:

- "Para capturar la salida del comando `raidctl` desde un cliente de Solaris" en la página 183
- "Para capturar la salida del comando `raidctl` desde un cliente de Windows" en la página 194

▼ Para capturar la salida del comando `raidctl` desde un cliente de Solaris

1. **Desde un cliente de Solaris, escriba el comando `script` y un nombre de archivo. Por ejemplo:**

   > **`script raidctl`**

2. **Utilice Telnet para conectarse al servidor NAS.**

3. **Escriba el siguiente comando `raidctl` para capturar la salida:**

   `raidctl get type=lsi target=profile ctlr=0`

4. **Escriba `exit` para cerrar la sesión de Telnet.**

5. **Escriba `exit` otra vez para cerrar el archivo llamado `raidctl`**

El siguiente ejemplo ilustra la salida del comando, resaltado en negrita con los niveles de firmware respectivos:

```
telnet 10.8.1xx.x2
Trying 10.8.1xx.x2...
Connected to 10.8.1xx.x2.
Escape character is '^]'.
connect to (? for list) ? [menu] admin
password for admin access ? *********
5310 > raidctl get type=lsi target=profile ctlr=0

SUMMARY---------------------------------
Number of controllers: 2
Number of volume groups: 4
Total number of volumes (includes an access volume): 5 of 1024 used
   Number of standard volumes: 4
   Number of access volumes: 1
Number of drives: 28
Supported drive types: Fibre (28)
Total hot spare drives: 2
   Standby: 2
   In use: 0
Access volume: LUN 31
Default host type: Sun_SE5xxx (Host type index 0)
Current configuration
   Firmware version: PkgInfo 06.12.09.10
   NVSRAM version: N2882-612843-503
Pending configuration
```

```
CONTROLLERS ---------------------------------
Number of controllers: 2

Controller in Tray 0, Slot B
   Status: Online
   Current Configuration
      Firmware version: 06.12.09.10
         Appware version: 06.12.09.10
         Bootware version: 06.12.09.10
      NVSRAM version: N2882-612843-503
   Pending Configuration
      Firmware version: None
         Appware version: None
         Bootware version: None
      NVSRAM version: None
      Transferred on: None
   Board ID: 2882
   Product ID: CSM100_R_FC
   Product revision: 0612
   Serial number: 1T44155753
   Date of manufacture: Sat Oct 16 00:00:00 2004
   Cache/processor size (MB): 896/128
   Date/Time: Thu Nov  2 19:15:49 2006
   Associated Volumes (* = Perferred Owner):
      lun4* (LUN 3)
Ethernet port: 1
      Mac address: 00.A0.B8.16.C7.A7
      Host name: gei
      Network configuration: Static
      IP address: 192.168.128.106
      Subnet mask: 255.255.255.0
      Gateway: 192.168.128.105
      Remote login: Enabled
   Drive interface: Fibre
      Channel: 2
      Current ID: 124/0x7C
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Fixed
      Link status: Up
      Topology: Arbitrated Loop - Private
      World-wide port name: 20:02:00:A0:B8:16:C7:A7
      World-wide node name: 20:00:00:A0:B8:16:C7:A7
      Part type: HPFC-5400      revision 6
```

```
 Drive interface: Fibre
      Channel: 2
      Current ID: 124/0x7C
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
Data rate control: Fixed
      Link status: Up
      Topology: Arbitrated Loop - Private
      World-wide port name: 20:02:00:A0:B8:16:C7:A7
      World-wide node name: 20:00:00:A0:B8:16:C7:A7
      Part type: HPFC-5400      revision 6
   Host interface: Fibre
      Channel: 2
      Current ID: 255/0x3
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Auto
      Link status: Down
      Topology: Unknown
      World-wide port name: 20:07:00:A0:B8:16:C6:FB
      World-wide node name: 20:06:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6
   Host interface: Fibre
      Channel: 2
      Current ID: 255/0x3
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Auto
      Link status: Down
      Topology: Unknown
      World-wide port name: 20:07:00:A0:B8:16:C6:FB
      World-wide node name: 20:06:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6

Controller in Tray 0, Slot A
   Status: Online
   Current Configuration
      Firmware version: 06.12.09.10
         Appware version: 06.12.09.10
         Bootware version: 06.12.09.10
      NVSRAM version: N2882-612843-503
   Pending Configuration
      Firmware version: None
         Appware version: None
         Bootware version: None
      NVSRAM version: None
      Transferred on: None
```

```
 Board ID: 2882
   Product ID: CSM100_R_FC
   Product revision: 0612
   Serial number: 1T44155741
   Date of manufacture: Sun Oct 10 00:00:00 2004
   Cache/processor size (MB): 896/128
   Date/Time: Thu Nov  2 19:15:45 2006
   Associated Volumes (* = Perferred Owner):
lun1* (LUN 0), lun2* (LUN 1), lun3* (LUN 2)
   Ethernet port: 1
      Mac address: 00.A0.B8.16.C6.F9
      Host name: gei
      Network configuration: Static
      IP address: 192.168.128.105
      Subnet mask: 255.255.255.0
      Gateway: 192.168.128.105
      Remote login: Enabled
   Drive interface: Fibre
      Channel: 1
      Current ID: 125/0x7D
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Fixed
      Link status: Up
      Topology: Arbitrated Loop - Private
      World-wide port name: 20:01:00:A0:B8:16:C6:F9
      World-wide node name: 20:00:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6
Drive interface: Fibre
      Channel: 1
      Current ID: 125/0x7D
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Fixed
      Link status: Up
      Topology: Arbitrated Loop - Private
      World-wide port name: 20:01:00:A0:B8:16:C6:F9
      World-wide node name: 20:00:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6
Host interface: Fibre
      Channel: 1
      Current ID: 255/0x0
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Auto
```

```
 Link status: Down
      Topology: Unknown
      World-wide port name: 20:06:00:A0:B8:16:C6:FA
      World-wide node name: 20:06:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6
   Host interface: Fibre
      Channel: 1
      Current ID: 255/0x0
      Maximum data rate: 200 MB/s
      Current data rate: 200 MB/s
      Data rate control: Auto
      Link status: Down
      Topology: Unknown
World-wide port name: 20:06:00:A0:B8:16:C6:FA
      World-wide node name: 20:06:00:A0:B8:16:C6:F9
      Part type: HPFC-5400      revision 6

VOLUME GROUPS-------------------------
   Number of volume groups: 4
   Volume group 1 (RAID 5)
      Status: Online
      Tray loss protection: No
      Associated volumes and free capacities:
         lun1 (681 GB)
      Associated drives (in piece order):
      Drive at Tray 0, Slot 7
      Drive at Tray 0, Slot 6
      Drive at Tray 0, Slot 5
      Drive at Tray 0, Slot 4
      Drive at Tray 0, Slot 3
      Drive at Tray 0, Slot 8
Volume group 2 (RAID 5)
      Status: Online
      Tray loss protection: No
      Associated volumes and free capacities:
         lun2 (681 GB)
      Associated drives (in piece order):
      Drive at Tray 0, Slot 14
      Drive at Tray 0, Slot 13
      Drive at Tray 0, Slot 12
      Drive at Tray 0, Slot 11
      Drive at Tray 0, Slot 10
      Drive at Tray 0, Slot 9
```

```
 Volume group 3 (RAID 5)
      Status: Online
      Tray loss protection: No
      Associated volumes and free capacities:
         lun3 (817 GB)
      Associated drives (in piece order):
      Drive at Tray 11, Slot 5
      Drive at Tray 11, Slot 4
      Drive at Tray 11, Slot 3
      Drive at Tray 11, Slot 2
      Drive at Tray 11, Slot 1
      Drive at Tray 11, Slot 7
      Drive at Tray 11, Slot 6
   Volume group 4 (RAID 5)
      Status: Online
      Tray loss protection: No
      Associated volumes and free capacities:
         lun4 (817 GB)
      Associated drives (in piece order):
      Drive at Tray 11, Slot 13
Drive at Tray 11, Slot 12
      Drive at Tray 11, Slot 11
      Drive at Tray 11, Slot 10
      Drive at Tray 11, Slot 9
      Drive at Tray 11, Slot 8
      Drive at Tray 11, Slot 14

STANDARD VOLUMES----------------------------

SUMMARY
   Number of standard volumes: 4
   NAME    STATUS    CAPACITY  RAID LEVEL  VOLUME GROUP
   lun1    Optimal   681   GB    5            1
   lun2    Optimal   681   GB    5            2
   lun3    Optimal   817   GB    5            3
   lun4    Optimal   817   GB    5            4
```

```
DETAILS

   Volume name: lun1
      Volume ID: 60:0A:0B:80:00:16:C6:F9:00:00:23:B4:43:4B:53:3A
      Subsystem ID (SSID): 0
      Status: Optimal
      Action: 1
      Tray loss protection: No
      Preferred owner: Controller in slot A
      Current owner: Controller in slot B
      Capacity: 681 GB
      RAID level: 5
      Segment size: 64 KB
      Associated volume group: 1
      Read cache: Enabled
      Write cache: Enabled
      Flush write cache after (in seconds): 8
      Cache read ahead multiplier: 1
      Enable background media scan: Enabled
      Media scan with redundancy check: Disabled
DRIVES------------------------------

SUMMARY

   Number of drives: 28
      Supported drive types: Fiber (28)
   BASIC:
CURRENT    PRODUCT      FIRMWARE
   TRAY,SLOT  STATUS  CAPACITY   DATA RATE     ID          REV
      0,1     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,7     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,6     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,5     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,4     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,3     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,2     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,14    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,13    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,12    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,11    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,10    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,9     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      0,8     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
```

```
 11,5     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,4     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,3     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,2     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,1     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,13    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,12    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,11    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,10    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,9     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,8     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,7     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,6     Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307
      11,14    Optimal  136 GB    2 Gbps   ST314680FSUN146G 0307

   HOT SPARE COVERAGE:

      The following volume groups are not protected:

      Total hot spare drives: 2
         Standby: 2
         In use: 0

   DETAILS:

      Drive at Tray 0, Slot 1 (HotSpare)
         Available: 0
         Drive path redundancy: OK
         Status: Optimal
         Raw capacity: 136 GB
         Usable capacity: 136 GB
         Product ID: ST314680FSUN146G
         Firmware version: 0307
         Serial number: 3HY90HWJ00007510RKKV
Vendor: SEAGATE
         Date of manufacture: Sat Sep 18 00:00:00 2004
         World-wide name: 20:00:00:11:C6:0D:BA:3E
         Drive type: Fiber
         Speed: 10033 RPM
         Associated volume group: None
         Available: No
```

```
 Vendor: SEAGATE
         Date of manufacture: Sat Sep 18 00:00:00 2004
         World-wide name: 20:00:00:11:C6:0D:CA:12
         Drive type: Fiber
         Speed: 10033 RPM
         Associated volume group: 3
         Available: No

      Drive at Tray 11, Slot 1
         Drive path redundancy: OK
         Status: Optimal
         Raw capacity: 136 GB
         Usable capacity: 136 GB
         Product ID: ST314680FSUN146G
         Firmware version: 0307
         Serial number: 3HY90JEW00007511BDPL
         Vendor: SEAGATE
         Date of manufacture: Sat Sep 18 00:00:00 2004
         World-wide name: 20:00:00:11:C6:0D:C8:8B
         Drive type: Fiber
         Speed: 10033 RPM
         Associated volume group: 3
         Available: No
Drive Tray 1 Overall Component Information
      Tray technology: Fibre Channel
      Minihub datarate mismatch: 0
      Part number: PN 54062390150
      Serial number: SN 0447AWF011
      Vendor: VN SUN
      Date of manufacture: Mon Nov  1 00:00:00 2004
      Tray path redundancy: OK
      Tray ID: 11
Tray ID Conflict: 0
      Tray ID Mismatch: 0
      Tray ESM Version Mismatch: 0
      Fan canister: Optimal
      Fan canister: Optimal
      Power supply canister
         Status: Optimal
         Part number: PN 30017080150
         Serial number: SN A6847502330F
         Vendor: VN SUN
         Date of manufacture: Sun Aug  1 00:00:00 2004
```

```
 Power supply canister
         Status: Optimal
         Part number: PN 30017080150
         Serial number: SN A6847502330F
         Vendor: VN SUN
         Date of manufacture: Sun Aug  1 00:00:00 2004
      Power supply canister
         Status: Optimal
         Part number: PN 30017080150
         Serial number: SN A68475023N0F
         Vendor: VN SUN
         Date of manufacture: Sun Aug  1 00:00:00 2004
      Temperature: Optimal
Temperature: Optimal
      Esm card
         Status: Optimal
         Firmware version: 9631
         Maximum data rate: 2 Gbps
         Current data rate: 2 Gbps
         Location: A (left canister)
         Working channel: -1
         Product ID: CSM100_E_FC_S
         Part number: PN 37532180150
         Serial number: SN 1T44462572
         Vendor: SUN
         FRU type: FT SBOD_CEM
         Date of manufacture: Fri Oct  1 00:00:00 2004
      Esm card
         Status: Optimal
         Firmware version: 9631
         Maximum data rate: 2 Gbps
         Current data rate: 2 Gbps
         Location: B (right canister)
         Working channel: -1
```

▼ Para capturar la salida del comando `raidctl` desde un cliente de Windows

1. **Haga clic en Start (Inicio) > Run (Ejecutar) y escriba `cmd`. Haga clic en OK (Aceptar).**
2. **Haga clic con el botón derecho en la parte superior de la ventana y elija Properties (Propiedades).**

   Se muestra el cuadro de diálogo Properties (Propiedades).
3. **Cambie el tamaño del búfer de pantalla (altura) a 3.000.**
4. **Haga clic en la ficha Options (Opciones) y desactive Insert Mode (Modo de inserción).**
5. **Utilice Telnet para conectarse al servidor NAS, y escriba el siguiente comando `raidctl` para capturar la salida:**

   ```
   raidctl get type=lsi target=profile ctlr=0
   ```
6. **Copie el texto a un archivo con cualquier editor de texto. Por ejemplo:**
   a. **Seleccione el texto de salida y pulse Ctrl-C para copiar los datos.**
   b. **Haga clic en Start (Inicio) > Programs (Programas) > Accessories (Accesorios) > Wordpad para abrir este editor de texto.**
   c. **Haga clic en la ventana y pulse Ctrl-V para pegar los datos.**
   d. **Guarde el archivo.**
7. **Abra este archivo y busque la versión de firmware actual de cada uno de los componentes.**

APÉNDICE **A**

Administración de consola

La consola es el método alternativo a Web Administrator para gestionar el dispositivo Sun StorEdge 5310 NAS, el clúster Sun StorEdge 5310 y el sistema de puerta de enlace Sun StorEdge 5310. Puede utilizar diversos protocolos como Telnet, Secure Shell (SSH) y RLogin para conectarse a la consola del administrador, siempre que la aplicación que utilice posea un emulador de terminal compatible con ANSI (del inglés American National Standards Institute). En este apéndice, utilizamos el protocolo Telnet ya que está listo para su uso en Windows.

Nota – Es posible que deba modificar la configuración de las funciones de seguridad del acceso remoto para acceder a la interfaz de línea de comandos. Consulte "Para definir la seguridad de acceso remoto" en la página 162 para obtener información sobre el acceso remoto.

Este apéndice incluye los siguientes temas:

- "Acceso al administrador de consola" en la página 196
- "Elementos básicos del menú de la consola" en la página 197
- "Visualización del menú principal" en la página 198
- "Copia de seguridad de la configuración" en la página 198
- "Gestión del sistema" en la página 199
- "Rutas de gestión" en la página 205
- "Servicios de nombres" en la página 205
- "Gestión del sistema de archivos del servidor" en la página 210
- "Gestión de recursos compartidos y cuotas" en la página 213
- "Seguridad" en la página 218
- "Duplicación de volúmenes de archivo" en la página 226
- "Supervisión" en la página 234
- "Mantenimiento del sistema" en la página 238

Acceso al administrador de consola

En este ejemplo se utiliza el protocolo Telnet de Windows. No obstante, puede utilizar otro protocolo siempre que cuente con el emulador de terminal compatible con ANSI.

▼ Para acceder a Telnet de Windows

1. **Haga clic en el botón Start (Inicio) de la barra de tareas de su escritorio.**
2. **Seleccione Run (Ejecutar).**
3. **En la ventana Run (Ejecutar), escriba `Telnet` y haga clic en OK (Aceptar).**
4. **En el indicador de comandos, escriba `telnet` *dirección-ip*, donde *dirección-ip* es la dirección IP del servidor, y pulse Intro.**
5. **Si el acceso administrativo está protegido con contraseña, escriba la contraseña.**

   Una vez conectado, la pantalla Telnet mostrará el siguiente mensaje de línea de comandos:

   ```
   connect to (? for list) ? [menu]
   ```

   En este punto, puede ir al menú principal o acceder a la interfaz de línea de comandos (CLI) para ejecutar los comandos.

   Para acceder al menú principal, pulse Intro.

▼ Para acceder a la interfaz de línea de comandos

1. **En el indicador de conexión, escriba `admin` y pulse Intro.**
2. **Escriba la contraseña administrativa y pulse Intro.**

   Aparecerá el indicador de línea de comandos. Puede escribir un comando o seleccionar `menu` para acceder al menú principal de la consola.

Precaución – Utilice los comandos con cuidado para evitar resultados no deseados.

Para volver a la línea de comandos, pulse Esc en el menú principal.

Elementos básicos del menú de la consola

Esta sección describe los componentes de la pantalla Telnet que se utilizan para configurar y mantener el sistema.

Directrices básicas

Éstas son algunas directrices básicas que debe tener en cuenta al utilizar la consola:

- Para seleccionar un menú, pulse el número o la letra asociado al elemento. Por ejemplo, pulse **1** para seleccionar la pantalla 1. Activity Monitor (Monitor de actividad).
- Las casillas que aparecen en la parte inferior de las pantallas indican las tareas que puede realizar y la letra que debe seleccionar para cada acción.
- Utilice la barra espaciadora para desplazarse por la lista.

Descripciones de las teclas

Las teclas que sirven para editar campos de pantalla se enumeran en la siguiente tabla.

TABLA A-1 Teclas de pantalla activa

Teclas	Descripción
Tecla de retroceso, Supr, Ctrl+H	Borra el carácter anterior
Ctrl+U	Borra el campo completo
Intro, Ctrl+M, Ctrl+J, Ctrl+I, Tabulación	La entrada está completa y el cursor pasa al siguiente campo
Esc	Abandona la pantalla sin realizar cambios

Si no desea cambiar el valor de un campo, pulse Intro. El cursor se mueve al siguiente cambio sin modificar la información.

Visualización del menú principal

El menú principal consta de las siguientes secciones:

- **Operations** (Operaciones): pulse cualquier número para realizar la operación de servidor correspondiente.
- **Configurations** (Configuración): pulse cualquier letra para activar el comando de configuración de servidor correspondiente.
- **Access Control** (Control de acceso): pulse cualquier letra para configurar el acceso a los elementos del menú correspondientes.
- **Extensions** (Extensiones): pulse cualquier letra para seleccionar la extensión correspondiente. Utilice la barra espaciadora para desplazarse por las listas de extensiones.

▼ Para utilizar el menú

1. **Elija un elemento de menú pulsando la letra o el número correspondiente.**
2. **Pulse la barra espaciadora para ver más opciones de la lista Extension (Extensiones).**

Copia de seguridad de la configuración

Después de configurar el sistema, es aconsejable que cree una copia de seguridad de la configuración.

Precaución – El sistema almacena copias redundantes de la información de configuración, pero deberá hacer una copia de seguridad en caso de que falle.

▼ Para realizar una copia de la información de configuración

En una configuración de clúster, siga este procedimiento con un solo servidor. La configuración se sincroniza automáticamente entre los servidores; por ello, no es necesario crear una copia de seguridad de la configuración de cada servidor.

1. **Siga las instrucciones para "Para acceder a la interfaz de línea de comandos" en la página 196.**

Precaución – Utilice los comandos con cuidado para evitar resultados no deseados.

2. **En la línea de comandos, escriba `load unixtools`.**
3. **Escriba `cp r v /dvol/etc` *ruta-de-copia-de-seguridad* donde *ruta-de-copia-de-seguridad* es la ruta completa, incluido el nombre del volumen, de la ubicación del directorio para la copia de seguridad de archivos de configuración. El directorio debe existir y estar vacío.**

   Esto copia toda la información de configuración almacenada en el directorio `/dvol/etc` a la ubicación indicada.

Gestión del sistema

Puede utilizar el administrador de consola para llevar a cabo las tareas de gestión del sistema.

▼ Para configurar TCP/IP

1. **En el menú Configuration (Configuración), seleccione Host Name & Network (Nombre de host y red).**
2. **Seleccione 1. Edit fields (Editar campos).**
3. **Escriba el nombre de host del servidor y, a continuación, pulse Intro.**
4. **Escriba la Unidad máxima de transferencia (MTU, del inglés Maximum Transfer Unit) o pulse Intro para mantener el valor predeterminado.**
5. **Escriba la dirección IP del servidor y pulse Intro.**
6. **Escriba la máscara de subred IP y pulse Intro.**
7. **Escriba la difusión IP de la red, y pulse Intro.**

8. **Seleccione 1. Setup (Configurar) para configurar las direcciones IP alias, y pulse Intro.**
9. **Repita del paso 3 al paso 8 para los demás puertos. Para continuar, pulse Intro.**

Nota – Si existen puertos adicionales, utilice la barra espaciadora para desplazarse hacia abajo.

---

10. **Escriba la dirección de puerta de enlace y pulse Intro.**
11. **Seleccione 7. Save changes (Guardar cambios).**

▼ Para modificar la contraseña del administrador

1. **En el menú Access Control (Control de acceso) seleccione Admin Access (Acceso de administrador).**
2. **Seleccione Y. Yes (Sí) para habilitar la protección con contraseña o N. No para deshabilitarla.**

Nota – Se aconseja proteger el sistema con una contraseña.

---

3. **Si ha seleccionado Yes (Sí) realice estos pasos en respuesta a los mensajes:**
   a. **Escriba la contraseña para acceso administrativo dos veces para confirmarla.**
   b. **Para activar la nueva contraseña, seleccione 7. Save changes (Guardar cambios).**

Control de la hora y la fecha

Utilice la opción de menú **Timezone, Time, Date** (Zona horaria, hora, fecha) para cambiar la zona horaria, la hora y la fecha establecidas en el servidor. El reloj en tiempo real de la placa principal guarda un registro de la hora local.

Nota – La primera vez que configura la fecha y la hora en el sistema, también inicializa el reloj seguro del sistema. El software de administración de licencias y de Compliance Archiving utilizan este reloj para controlar las operaciones que dependen del tiempo.

Precaución – Una vez inicializado el reloj seguro, no puede restablecerse. Por ello, es importante que defina la fecha y la hora con precisión al configurar el sistema.

▼ Para configurar la zona horaria, la hora y la fecha

1. **En el menú Configuration (Configuración) seleccione Timezone, Time, Date (Zona horaria, hora, fecha).**
2. **Seleccione la zona horaria adecuada y, a continuación, pulse Intro.**
3. **Seleccione la configuración de horario de verano, Y (Sí) o N (No), según proceda.**
4. **Escriba la nueva fecha y, a continuación, pulse Intro.**

   El formato utilizado es AAAAMMDD, donde AAAA corresponde al año, MM corresponde al mes y DD corresponde al día. Por ejemplo, **`20051001`** es el 1 de octubre, 2005.
5. **Escriba la hora actual y, a continuación, pulse Intro.**

   El sistema utiliza un reloj de veinticuatro horas.
6. **Seleccione 7. Save changes (Guardar cambios).**

Configuración de la sincronización de la hora

Puede configurar el sistema para que sincronice la hora con el protocolo NTP o con un servidor RDATE.

NTP es un protocolo de Internet que se utiliza para conectar los relojes de los equipos informáticos a una fuente horaria de referencia y sincronizarlos con dicha fuente. Las configuraciones NTP habituales tienen varios servidores redundantes y diversas rutas de red para conseguir una gran precisión y fiabilidad.

Los servidores RDATE se utilizan normalmente en sistemas UNIX y permiten sincronizar la hora del servidor del sistema con la hora del servidor RDATE.

▼ Para configurar NTP

1. **En el menú Extensions (Extensiones) seleccione NTP Configuration (Configuración de NTP).**
2. **Para configurar las preferencias de NTP seleccione 1. Edit fields (Editar campos).**
3. **Seleccione Y. Yes (Sí) para habilitar NTP.**

4. **Realice estos pasos con cada uno de los servidores NTP que esté configurando.**

   Puede configurar dos servidores NTP como máximo.

   a. **Seleccione Y. Yes (Sí) para habilitar el primer servidor NTP.**

   b. **Escriba el nombre o la dirección IP del servidor NTP al que consultará el dispositivo Sun StorEdge 5310 NAS para obtener la hora actual, y pulse Intro.**

   c. **Elija el tipo de autenticación que desee utilizar, ya sea 0. none (ninguna) o 1. symmetric-key (clave simétrica).**

      La autenticación mediante clave simétrica permite al dispositivo Sun StorEdge 5310 NAS verificar que el servidor NTP es conocido y de confianza. Para ello se utiliza una clave y un ID de clave. Para autenticar los mensajes, la clave y el ID de clave del servidor NTP deben coincidir con la clave y el ID de clave del dispositivo Sun StorEdge 5310 NAS.

   d. **Si selecciona en el campo anterior Symmetric Key (Clave simétrica) como esquema de autorización, escriba el Key ID (ID de clave) asociado a la clave privada del archivo de claves que se va a utilizar con este servidor NTP.**

      El valor debe estar comprendido entre 1 y 65534.

5. **En el campo Min. Polling Interval (Intervalo mínimo de consulta) escriba el índice mínimo de consulta para los mensajes de NTP.**

   Este valor, elevado a la segunda potencia, es el número mínimo de segundos para el intervalo de consulta. Por ejemplo, si escribe 4, el tiempo que transcurrirá entre consultas será de 16 segundos. El valor de este campo debe estar entre 4 y 17.

6. **En el campo Max. Polling Interval (Intervalo máximo de consulta) escriba el índice máximo de consulta para los mensajes de NTP.**

   Este valor, elevado a la segunda potencia, es el número máximo de segundos para el intervalo de consulta. Por ejemplo, si escribe 4, el tiempo que transcurrirá entre consultas será de 16 segundos. El valor de este campo debe estar entre 4 y 17 y debe ser superior al valor especificado en el intervalo mínimo de consulta.

7. **En el campo Broadcast Client Enabled (Cliente de difusión habilitado) seleccione Y. Yes (Sí) para que el dispositivo Sun StorEdge 5310 NAS responda a los mensajes de difusión del servidor que se reciban en cualquier interfaz.**

8. **En el campo Require Server authentication (Solicitar autenticación del servidor), seleccione Y. Yes (Sí) para solicitar autenticación a los servidores que utilicen el cliente de difusión.**

   No se aceptarán los servidores NTP que no utilicen autenticación.

9. **Seleccione 7. Save changes (Guardar cambios).**

▼ Para configurar el servidor RDATE y la ventana de tolerancia

1. **En el menú Extensions (Extensiones) seleccione RDATE time update (Actualización de hora de RDATE).**
2. **Seleccione 1. Edit fields (Editar campos).**
3. **Escriba el nombre o la dirección IP del servidor RDATE y pulse Intro.**
4. **Escriba la tolerancia y pulse Intro.**

   Si la hora del dispositivo Sun StorEdge 5310 NAS es distinta a la del servidor RDATE en una cantidad de segundos inferior al número indicado (+ o -), la hora de sistema del dispositivo Sun StorEdge 5310 NAS se sincroniza con la hora del servidor RDATE. Esta comprobación ocurre todos los días a las 11:45 p.m.
5. **Seleccione 7. Save changes (Guardar cambios).**

Configuración de la protección antivirus

Si tiene un motor de exploración antivirus que se ejecuta en la red, puede configurar la protección antivirus para el sistema. Para obtener más información acerca de la protección antivirus, consulte "Uso de software antivirus" en la página 65.

▼ Para habilitar la protección antivirus

1. **En el menú Extensions (Extensiones) seleccione Anti-Virus Configuration (Configuración de antivirus).**
2. **Seleccione 1. Edit fields (Editar campos).**
3. **En el campo AVA Enable (Habilitar AVA), especifique Yes (Sí) para activar la protección antivirus.**
4. **En el campo de modo de exploración, seleccione el modo.**

   Consulte "Para habilitar la protección antivirus" en la página 66 para obtener información sobre las opciones del modo de exploración.
5. **Especifique la dirección TCP/IP del motor de búsqueda que desee utilizar.**
6. **Especifique el número de puerto TCP/IP por el que el servidor ICAP intenta detectar las conexiones; normalmente es el puerto 1344.**
7. **Indique el número máximo de operaciones de exploración concurrentes de los archivos que el sistema expedirá al motor de búsqueda; el número típico es 2.**

8. **Especifique los tipos de archivos que desea incluir y excluir, además de los clientes, los grupos o los recursos compartidos exentos.**

Especificación	Descripción	Formato
File Types Included (Tipos de archivo incluidos)	La extensión de cada tipo de archivo que incluirá la exploración. Deje en blanco para incluir todos.	Tres o menos caracteres separados por coma. El signo ? sirve como comodín.
File Types Excluded (Tipos de archivo excluidos)	La extensión de cada tipo de archivo que se excluirá en la exploración.	Tres o menos caracteres separados por coma. El signo ? sirve como comodín.
Exempt Clients (Clientes exentos)	Nombre o dirección IP de cada cliente exento de la exploración.	Separado por comas.
Exempt Groups (Grupos exentos)	Nombre de cada grupo de Windows/NT o grupo de directorio activo de Windows (no grupos de UNIX) exento de la exploración.	Puede incluir espacios, separado por coma.
Exempt Shares (Cuotas exentas)	Nombre de cada recurso compartido del CIFS exento de la exploración. Nota: los recursos compartidos administrativos (`X$`) siempre se eximen de la exploración.	Separado por comas.

9. **Seleccione 7. Save changes (Guardar cambios).**

Selección de idioma

Puede especificar el idioma para NFS y CIFS.

▼ Para seleccionar el idioma

1. **En el menú Extensions (Extensiones) seleccione Language Selection (Selección de idioma).**
2. **Escriba el idioma que desee y, a continuación, pulse Intro.**

   Los idiomas admitidos aparecen en una lista en la parte superior de la pantalla.

Rutas de gestión

La tabla de rutas contiene un listado con las rutas de red por las que el sistema envía paquetes de red a determinados destinos. Cada entrada de ruta se compone de una dirección de destino y una ruta. El destino puede ser una red o un host. La ruta es el dispositivo de puerta de enlace por el que el paquete llega a su destino.

▼ Para gestionar rutas estáticas en la red local

1. **En el menú Configuration (Configuración), seleccione Host Name & Network (Nombre de host y red).**
2. **Seleccione 2. Manage Routes (Gestionar rutas).**
3. **Seleccione 1. Add route (Agregar ruta) y, a continuación, 1. Edit (Editar).**
4. **Especifique si el tipo de ruta es para un host, una red, un host con puerta de enlace o una red con puerta de enlace.**
5. **Escriba la dirección IP de destino y, a continuación, pulse Intro.**
6. **Escriba la ruta o la dirección de la puerta de enlace que se va a utilizar para conectar el dispositivo Sun StorEdge 5310 NAS con el destino y, a continuación, pulse Intro.**

   El dispositivo de puerta de enlace debe estar conectado a la misma subred que el dispositivo Sun StorEdge 5310 NAS.
7. **Seleccione 7. Save changes (Guardar cambios).**

Servicios de nombres

El nombre, los servicios y las funciones disponibles mediante la interfaz de la consola difieren del nombre, los servicios y las funciones disponibles mediante la interfaz gráfica de usuario.

Configuración de DNS, `syslogd` e inicio de sesión local

DNS es un sistema de nomenclatura jerárquico que traduce los nombres de dominios en direcciones IP. `syslogd` es la utilidad que ofrece asistencia para el inicio de sesión remoto. Sólo podrá habilitar el inicio de sesión remoto si dispone de un sistema UNIX con la utilidad `syslogd` en la red que pueda recibir el registro de sistema del dispositivo Sun StorEdge 5310 NAS. Todas las funciones que se detallan a continuación se configuran en la misma pantalla.

Tras configurar `syslogd`, todos los mensajes de registro se enviarán al servidor seleccionado. Esto le permitirá centralizar un archivo de mensajes de registro de todos los servidores en un sistema.

▼ Para configurar DNS, DNS dinámico, `syslogd` y el inicio de sesión local

1. **En el menú Configuration (Configuración) seleccione DNS & SYSLOGD (DNS y SYSLOGD).**
2. **Seleccione 1. Edit fields (Editar campos).**
3. **Seleccione Y. Yes (Sí) para habilitar DNS (Domain Name Service).**
4. **Escriba la dirección IP del servidor DNS que se deba consultar en primer lugar para resolver nombres. A continuación pulse Intro.**
5. **Escriba la dirección IP del servidor que se consultará en segundo lugar para resolver nombres y, a continuación, pulse Intro.**

   Si no posee un servidor DNS secundario, deje este campo en blanco.
6. **Escriba el nombre de dominio del servidor DNS y, a continuación, pulse Intro.**
7. **Escriba el número máximo de veces que el sistema debe intentar realizar una consulta DNS a cada servidor DNS. A continuación, pulse Intro.**
8. **Escriba el número de segundos de retraso entre los intentos de consulta a cada servidor DNS y, a continuación, pulse Intro.**
9. **Para habilitar el inicio de sesión remoto, seleccione Y. Yes (Sí). Si no hay ningún servidor `syslogd` en la red, seleccione N. No y vaya al paso 15.**

   Esta función permite que el dispositivo Sun StorEdge 5310 NAS envíe mensajes de registro a un servidor `SYSLOGD` remoto.
10. **Escriba el nombre o la dirección IP del servidor `syslogd` y, a continuación, pulse Intro.**

11. **Seleccione la utilidad adecuada y, a continuación, pulse Intro. La utilidad identifica la aplicación o el componente de sistema que genera los mensajes. Las utilidades incluyen:**
    - **Kern** (Núcleo): los mensajes son generados por el núcleo. Estos mensajes no los puede generar ningún proceso de usuario.
    - **User** (Usuario): los mensajes son generados por procesos de usuarios aleatorios. Es el valor predeterminado si no se especifica ninguno.
    - **Mail** (Correo): el sistema de correo.
    - **Daemon**: daemons de sistema o de red.
    - **Auth** (Autorización): sistemas de autorización como, por ejemplo, el inicio de sesión.
    - **Syslog** (Registro de sistema): mensajes generados internamente por syslogd.
    - **Local0–Local7**: reservado para el uso local.
12. **Seleccione el tipo de eventos de sistema que desea incluir en los registros del dispositivo Sun StorEdge 5310 NAS:**
    a. **Seleccione el tipo de evento adecuado.**
    b. **Seleccione Y. Yes (Sí) para habilitar el informe de eventos de ese tipo. Los tipos de eventos incluyen los siguientes:**
        - **Emerg –** (Emergencia): los mensajes de emergencia. Este tipo de mensajes no se distribuyen a todos los usuarios. Los mensajes de emergencia prioritarios se pueden registrar en un archivo separado para revisarlos.
        - **Alert –** (Alerta): mensajes importantes que exigen una atención inmediata. Este tipo de mensajes sí se distribuyen a todos los usuarios.
        - **Crit –** (Crítico): mensajes críticos que no se clasifican como errores; por ejemplo, los problemas de hardware. Los mensajes críticos y los que tienen una prioridad superior se envían a la consola del sistema.
        - **Err –** : mensajes que representan condiciones de error, por ejemplo, un intento de escribir en el disco sin éxito.
        - **Warning –** (Advertencia): mensajes de condiciones anómalas pero que se pueden recuperar.
        - **Notice –** (Aviso): mensajes informativos importantes. Los mensajes que no tienen asignada una prioridad se incluyen en esta categoría de mensajes.
        - **Info –** (Información): mensajes informativos. Estos mensajes son útiles a la hora de analizar el sistema.
        - **Debug –** (Depuración): mensajes de depuración.
    c. **Pulse Intro para pasar al siguiente tipo de evento.**
13. **Seleccione Y. Yes (Sí) para habilitar actualizaciones DNS dinámicas.**

    Estas actualizaciones permiten que se produzcan actualizaciones dinámicas que no son seguras durante el reinicio.

14. **Para habilitar actualizaciones seguras, escriba el nombre de un usuario de Windows con el que el cliente DNS dinámico puede comprobar las actualizaciones y, a continuación, pulse Intro.**

    Este usuario debe tener derechos administrativos.

15. **Escriba la contraseña del usuario DNS dinámico y, a continuación, pulse Intro.**

16. **Seleccione Y. Yes (Sí) para habilitar el inicio de sesión local.**

17. **Escriba la ruta del archivo de registro (directorio) y el nombre de archivo en el campo Log File (Archivo de registro).**

18. **Indique el número máximo de archivos de almacenamiento en el campo Archives (Archivos de almacenamiento).**

    Puede indicar un valor entre 1 y 9.

19. **Especifique el tamaño máximo de archivo en kilobytes para cada archivo de almacenamiento en el campo Archives (Archivos de almacenamiento).**

    Puede indicar un valor entre 1.000 y 999.999 kilobytes.

20. **Seleccione 7. Save changes (Guardar cambios).**

Configuración de NIS y NIS+

Nota – Una vez configurado NIS (Network Information Service) revise periódicamente el servidor para comprobar si se han producido cambios en los archivos maestros. Cuando un archivo sufre modificaciones, se copia del servidor NIS al archivo local. El campo **Enable** (Habilitar) le permitirá deshabilitar las actualizaciones NIS sin perder los datos de la configuración. De este modo, podrá recuperar la información cuando vuelva a habilitarlo.

▼ Para habilitar NIS o NIS+

1. **En el menú Configuration (Configuración) seleccione NIS & NIS+ (NIS y NIS+).**

2. **Seleccione 1. Edit fields (Editar campos).**

3. **Seleccione Y. Yes (Sí) para habilitar la opción que permite al dispositivo Sun StorEdge 5310 NAS actualizar periódicamente los archivos de los hosts, los usuarios y los grupos mediante un servidor NIS.**

4. **Escriba el nombre del dominio de NIS y, a continuación, pulse Intro.**

5. **Escriba el nombre o la dirección IP del servidor NIS y, a continuación, pulse Intro.**

6. **Seleccione Y. Yes (Sí) para actualizar el archivo de los hosts mediante el servidor NIS.**

7. **Seleccione Y. Yes (Sí) para actualizar el archivo de los usuarios mediante el servidor NIS.**
8. **Seleccione Y. Yes (Sí) para actualizar el archivo de los grupos mediante el servidor NIS.**
9. **Seleccione Y. Yes (Sí) para actualizar el archivo de los grupos de red mediante el servidor NIS.**
10. **Especifique el número de minutos que desea que transcurran entre las actualizaciones de NIS. Este número debe estar comprendido entre 0 y 9; después, pulse Intro.**
11. **Seleccione Y. Yes (Sí) para habilitar NIS+ para el dispositivo Sun StorEdge 5310 NAS.**
12. **Escriba la dirección de dominio principal del servidor NIS+ y, a continuación, pulse Intro.**
13. **Escriba el nombre de dominio principal de NIS+ y, a continuación, pulse Intro.**
14. **Introduzca la contraseña para RPC seguro del servidor NIS+. Pulse Intro.**
15. **Introduzca la ruta de búsqueda en forma de lista de dominios separados por dos puntos (":"). Si desea buscar solamente el dominio principal y los que tiene relacionados, deje este espacio en blanco. Pulse Intro.**
16. **Seleccione 7. Save changes (Guardar cambios).**

Configuración del orden de búsqueda de los servicios de nombres

Puede elegir el servicio que desea utilizar en primer lugar para las funciones de búsqueda de usuario, grupo y host.

▼ Para configurar las órdenes de búsqueda

1. **En el menú Configuration (Configuración) seleccione Lookup orders (Órdenes de búsqueda).**
2. **Seleccione 1. Edit fields (Editar campos).**
3. **Seleccione el orden para resolver la información de usuario (entre NIS y NIS+) y, a continuación, pulse Intro.**
4. **Seleccione el orden para resolver la información de grupo (entre NIS y NIS+) y, a continuación, pulse Intro.**
5. **Seleccione el orden de los cuatro servicios para resolver la información de host y, a continuación, pulse Intro.**
6. **Seleccione 7. Save changes (Guardar cambios).**

Gestión del sistema de archivos del servidor

Existen varios procedimientos en la consola que le permitirán gestionar los volúmenes del sistema de archivos del servidor (SFS, del inglés Server File System). Los procedimientos más habituales son:

- Configurar las letras de las unidades
- Configurar un nuevo volumen de disco
- Cambiar el nombre de una partición de disco
- Borrar un volumen de disco
- Habilitar y deshabilitar cuotas y puntos de control

Configurar las letras de las unidades

Las letras de las unidades se asignan de forma automática a los volúmenes de archivo disponibles para compartir mediante un bloque de mensajes de servidor (SMB)/CIFS. Puede asignar manualmente las asignaciones de letras de unidad a través de la consola, excepto para la unidad `C:`, que sólo puede asignarse a `\cvol`.

Es posible que todas las letras de unidades válidas no sean suficientes, en cuyo caso se muestra el siguiente mensaje de registro:

```
No drive letter available
```

Este mensaje es a título informativo. El sistema de archivos se creará, aunque para asignarle una letra de unidad, tendrá que reasignar la letra de unidad actual de otro sistema de archivos.

▼ Para asignar manualmente una letra de unidad a un volumen de archivo

1. **En el menú Configuration (Configuración) seleccione Drive Letters (Letras de unidades).**
2. **Escriba la letra de unidad que desee cambiar y, a continuación, pulse Intro.**
3. **Escriba el nombre del volumen de archivo que desee asignar a la nueva letra de unidad, y pulse Intro.**

   Recuerde que sólo puede asignar volúmenes de archivo existentes a las letras de unidades.
4. **Para abandonar esta pantalla pulse Esc.**

▼ Para crear un nuevo volumen de disco

1. **En el menú Configuration (Configuración) seleccione Disks & Volumes (Discos y volúmenes).**
2. **Escriba la letra de la unidad que desea configurar.**
3. **Seleccione 1. Edit (Editar).**
4. **Seleccione 1. Create partition (Crear partición).**
5. **Seleccione el tipo de partición para la unidad, o pulse Intro para aceptar el tipo predeterminado, como por ejemplo,** `sfs2` **(volumen principal) o** `sfs2ext` **(segmento).**
6. **Escriba la etiqueta del volumen de disco y, a continuación, pulse Intro.**

   El sistema le solicitará que confirme si desea habilitar el almacenamiento compatible en este volumen.
7. **Si dispone una licencia del software Compliance Archiving y desea crear un volumen con compatibilidad habilitada, pulse Y.**

Nota – Las configuraciones del sistema de puerta de enlace Sun StorEdge 5310 admiten la aplicación recomendada, pero no la aplicación obligatoria, de la compatibilidad.

Precaución – Una vez se ha activado el almacenamiento compatible en un volumen con aplicación obligatoria, ese volumen no se podrá eliminar o renombrar, ni se podrá deshabilitar el almacenamiento compatible o hacerlo de aplicación recomendada.

---

8. **Si desea seleccionar el tamaño predeterminado pulse Intro. Si lo prefiere, puede escribir el tamaño del volumen de disco en MB y, a continuación, pulsar Intro.**
9. **Seleccione 7. Proceed with create (Proceder con la creación).**

   Espere a que aparezcan los siguientes mensajes: `Initialization OK` (Inicialización correcta) y `Mount OK` (Montaje correcto); después pulse Esc para volver al menú Configure Disk (Configurar disco).
10. **Una vez finalizado el proceso pulse Esc hasta regresar al menú principal.**

▼ Para cambiar el nombre de una partición

1. **En el menú Configuration (Configuración) seleccione Disks & Volumes (Discos y volúmenes).**
2. **Escriba la letra de la unidad a la que desea cambiar el nombre.**
3. **Seleccione 1. Edit (Editar).**
4. **Seleccione 3. Rename (Cambiar nombre).**
5. **Escriba el nuevo nombre de la partición y, a continuación, pulse Intro.**

Nota – No es posible cambiar el nombre de los volúmenes con compatibilidad habilitada estricta.

▼ Para agregar un segmento de extensión

Para agregar una extensión, primero debe crear una partición `sfs2ext` en el volumen.

Nota – Una vez adjuntado el volumen de extensión al volumen de archivo `sfs` ya no podrá separarlo. Esta operación no se puede deshacer. El único modo de separarlos es borrando el volumen de archivo `sfs`.

---

1. **En el menú Configuration (Configuración) seleccione Disks & Volumes (Discos y volúmenes).**
2. **Escriba la letra de la unidad que desea configurar.**

Nota – Si tiene más de 26 unidades de disco (volúmenes de disco), pulse la barra espaciadora para realizar la búsqueda.

---

3. **Escriba el número al lado de la partición que va a cambiar.**
4. **Seleccione 5. Segments (Segmentos).**
5. **Seleccione 1. Add an extension segment.(Agregar un segmento de extensión).**
6. **Seleccione la letra que está al lado de la unidad de extensión que desee.**
7. **Seleccione 7. Proceed (Proceder).**

▼ Para borrar un volumen de disco

Nota – Los volúmenes de compatibilidad habilitada con aplicación obligatoria no se pueden borrar.

Precaución – Al borrar un volumen se perderán todos los datos contenidos en dicho volumen.

▼ Para borrar un volumen de disco

1. **En el menú Configuration (Configuración) seleccione Disks & Volumes (Discos y volúmenes).**
2. **Escriba la letra de la unidad que desea configurar.**

   Nota – Si tiene más de 26 unidades de disco (volúmenes de disco), pulse la barra espaciadora para realizar la búsqueda.

3. **Seleccione 1. Edit (Editar).**
4. **Seleccione 8. Delete (Borrar).**
5. **Escriba el nombre del volumen de disco y, a continuación, pulse Intro.**
6. **Seleccione 7. Proceed with delete (Proceder con el borrado). Aguarde hasta que aparezcan los mensajes** `Delete OK` **(Borrado correcto) y** `Delpart OK` **(Borrado de partición correcto).**
7. **Pulse la tecla Esc para volver al menú Configure Disk (Configurar disco).**
8. **Pulse Esc hasta regresar al menú principal.**

Gestión de recursos compartidos y cuotas

Puede gestionar los recursos compartidos y las cuotas desde la consola.

Configuración de los recursos compartidos SMB/CIFS

CIFS es un servicio para compartir archivos de Windows que utiliza el protocolo SMB. CIFS ofrece un mecanismo para los sistemas de cliente Windows que permite acceder a archivos del dispositivo Sun StorEdge 5310 NAS.

▼ Para configurar los recursos compartidos

1. **En el menú Extensions (Extensiones) seleccione CIFS/SMB Configuration (Configuración de CIFS/SMB).**
2. **Seleccione A. Domain Configuration (Configuración de dominio).**
3. **Escriba un nombre de grupo de trabajo o de dominio en el campo Domain (Dominio).**
4. **Defina el ámbito del dominio, si procede.**
5. **Escriba una descripción de texto para el servidor del dispositivo Sun StorEdge 5310 NAS.**
6. **Escriba la dirección IP de los servidores principal y secundario del sistema de nombres de Internet para Windows (WINS), si procede.**
7. **Asigne un parámetro Keep Alive (Mantener activo).**

   Este parámetro designa el número de segundos tras los cuales el sistema da por finalizadas las conexiones inactivas.
8. **Asigne un modo de seguridad de Secure Share Level (Nivel de recurso compartido seguro) y NT Domain Auto UID (UID automático de dominio NT).**
9. **Si utiliza el modo NT Domain Auto UID (UID automático de dominio NT), escriba el nombre y la contraseña del usuario administrativo.**
10. **Seleccione 7. Save changes (Guardar cambios).**

    Si cambia el modo de seguridad entre Secure Share Level (Nivel de recurso compartido seguro) y NT Domain Auto UID (UID automático de dominio NT), el dispositivo Sun StorEdge 5310 NAS se reiniciará.

Configuración de los recursos compartidos autohome SMB/CIFS

Los recursos compartidos autohome son recursos temporales que se crean cuando un usuario inicia sesión en el sistema y se eliminan cuando cierra la sesión.

La función de recurso compartido autohome precisa de dos parámetros de configuración, que son el estado y la ruta de autohome, definidos como se indica:

- El parámetro de estado define si la función está habilitada o desactivada. La variable de entorno `smb.autohome.enable` establece el estado actual de la función; el valor debe ser “yes” o “no”.
- El parámetro de ruta autohome establece la ruta del directorio base para los recursos compartidos temporales. Está definido por la variable de entorno `smb.autohome.path`. Por ejemplo, si el directorio principal de un usuario es `/vol1/home/juan`, la ruta autohome debe definirse en `/vol1/home`. El nombre del recurso compartido temporal será `juan`. El nombre del directorio principal del usuario debe ser el mismo que el nombre de inicio de sesión del usuario.

Si esta función permanece deshabilitada, el parámetro de ruta autohome no tiene relevancia y no será validado.

Si está habilitada y la ruta es una línea de longitud cero, la configuración será ignorada. De lo contrario, se validará la ruta. Si el parámetro de ruta autohome no representa una ruta de directorio existente, se escribe un mensaje informativo en el registro del sistema. Por ejemplo, si la ruta base especificada fuese `/vol1/home`, el mensaje de registro sería como sigue:

```
SMB autohome: /vol1/home: no such directory
```

Este mensaje de registro tiene el propósito de informar al administrador del sistema sobre la situación, pues la configuración se sigue considerando válida. El sistema funcionará de manera normal aunque no se crearán recursos compartidos autohome. Si la ruta del directorio se crea más adelante, los recursos compartidos autohome se agregarán y eliminarán como sea necesario a partir de ese momento.

▼ Para habilitar los recursos compartidos autohome

1. **En el menú Extensions (Extensiones) seleccione CIFS/SMB Configuration (Configuración de CIFS/SMB).**
2. **Seleccione F. Autohome Setup (Configuración de autohome).**
3. **Seleccione 1. Edit fields (Editar campos).**
4. **Seleccione Y. Yes (Sí) para habilitar los recursos compartidos autohome.**
5. **Especifique un valor en Autohome Path (Ruta del recurso compartido autohome).**

   La ruta autohome es la ruta del directorio base para los recursos compartidos. Por ejemplo, si el directorio principal de un usuario es`/usr/home/juan`, tendría que definir el parámetro de ruta autohome como `/usr/home`. El recurso compartido temporal se llamará `juan`. El sistema asume que el nombre del directorio principal del usuario es el mismo que su nombre de inicio de sesión.
6. **Seleccione 7. Save changes (Guardar cambios).**

▼ Para definir un recurso compartido

Una vez completada la configuración de SMB/CIFS, deberá definir los recursos compartidos SMB/CIFS. Los recursos compartidos permiten a los usuarios de Windows acceder a los directorios del dispositivo Sun StorEdge 5310 NAS.

1. **En el menú Extensions (Extensiones) seleccione CIFS/SMB Configuration (Configuración de CIFS/SMB).**
2. **Seleccione E. Shares (Recursos compartidos).**
3. **Seleccione 8. Add a share (Agregar un recurso compartido).**
4. **Escriba el nombre del recurso compartido.**
5. **Escriba una ruta en el** *directorio* **siguiendo la estructura de volumen/directorio.**
6. **Escriba un comentario sobre este directorio, si procede.**
7. **Si el sistema está configurado para modo de grupo de trabajo, realice estos pasos:**
   a. **En el menú desplegable Password Protection (Protección con contraseña) seleccione Yes (Sí) o No.**
      Si está habilitada la función, existe una opción de lectura/escritura o sólo lectura.
   b. **Rellene los campos User ID (ID de usuario), Group ID (ID de grupo) y Umask.**
8. **Seleccione 7. Save changes (Guardar cambios).**

▼ Para editar un recurso compartido

1. **En el menú Extensions (Extensiones) seleccione CIFS/SMB Configuration (Configuración de CIFS/SMB).**
2. **Seleccione E. Shares (Recursos compartidos).**
3. **Escriba la letra correspondiente al recurso compartido que va a editar.**
4. **Seleccione 1. Edit fields (Editar campos).**
5. **Escriba el nombre, directorio, comentario, información de contraseña, ID de usuario e ID de grupo del nuevo recurso compartido.**
6. **Especifique el contenedor ADS siguiendo el procedimiento descrito en el paso 7 de la sección anterior,** **"Para definir un recurso compartido" en la página 216****.**
7. **Seleccione 7. Save changes (Guardar cambios).**

▼ Para borrar un recurso compartido

1. **En el menú Extensions (Extensiones) seleccione CIFS/SMB Configuration (Configuración de CIFS/SMB).**
2. **Seleccione E. Shares (Recursos compartidos).**
3. **Escriba la letra correspondiente al recurso compartido que va a borrar.**
4. **Seleccione 8. Delete (Borrar).**

Configuración del servicio Active Directory

Cuando se habilita y se configura el servicio Active Directory (ADS) en esta pantalla, el dispositivo Sun StorEdge 5310 NAS realiza actualizaciones de ADS automáticamente.

▼ Para habilitar el servicio ADS

1. **En el menú Extensions (Extensiones) seleccione ADS Setup (Configuración de ADS).**
2. **Seleccione 1. Edit fields (Editar campos).**
3. **Seleccione Y. Yes (Sí) para permitir al cliente ADS publicar recursos compartidos del dispositivo Sun StorEdge 5310 NAS para ADS.**
4. **Escriba el dominio de Windows en el que se está ejecutando ADS.**

   El dispositivo Sun StorEdge 5310 NAS también debe pertenecer a este dominio.
5. **Escriba el nombre de un usuario de Windows con derechos administrativos.**

   El cliente ADS comprueba las actualizaciones ADS seguras con este usuario.
6. **Escriba la contraseña del usuario administrativo de Windows.**
7. **En el campo User Container (Contenedor de usuario) escriba la ruta ADS del usuario administrativo de Windows en notación DN LDAP.**

   Para obtener más información, consulte "Para habilitar el servicio Active Directory" en la página 79.
8. **Escriba el nombre de ADS local en el campo Site (Sitio).**
9. **Escriba en letras mayúsculas el nombre del dominio Kerberos que se va a utilizar para identificar ADS.**

   Normalmente es el dominio ADS.

10. **Escriba el nombre de host del servidor del centro de distribución de claves (KDC, del inglés Key Distribution Center) de Kerberos.**

    Normalmente, se trata del nombre de host del controlador de dominio principal del dominio ADS. Puede dejar este campo en blanco si el cliente ADS o el cliente DNS dinámico puede localizar el servidor de KDC mediante DNS.

11. **Seleccione 7. Save changes (Guardar cambios).**

Habilitación y deshabilitación de cuotas

Las cuotas registran y limitan la cantidad de espacio de disco que cada usuario o grupo utiliza. La función de seguimiento de cuota se puede activar y desactivar. Esta función sólo habilita y deshabilita las cuotas. No configura los límites de cuotas.

Nota – La inicialización de cuotas puede tardar varios minutos. Durante este tiempo el volumen permanece bloqueado y no está disponible para los usuarios.

▼ Para habilitar o deshabilitar las cuotas

1. **En el menú Configuration (Configuración) seleccione Disks & Volumes (Discos y volúmenes).**
2. **Seleccione la unidad para la que está habilitando las cuotas.**
3. **Seleccione 1. Edit (Editar).**
4. **Seleccione 4. Quotas on/off (Cuotas activadas/desactivadas).**
5. **Seleccione 1. Turn quotas on (Activar cuotas) o 8.Turn quotas off (Desactivar cuotas).**

Seguridad

Puede configurar los grupos y asignaciones de credenciales para garantizar la seguridad.

Configuración de grupos de usuarios

Los requisitos de los grupos locales integrados son diferentes que en un sistema Windows NT. Si desea obtener una descripción completa de los grupos de usuarios, consulte "Grupos locales" en la página 85.

▼ Para agregar un grupo

1. **En el menú Extensions (Extensiones) seleccione CIFS/SMB Configuration (Configuración de CIFS/SMB).**
2. **Seleccione B. Local Groups (Grupos locales).**
3. **Seleccione 8. Add a Group (Agregar un grupo) para añadir un grupo local.**
4. **Escriba el nombre del grupo y, a continuación, pulse Intro.**
5. **Escriba una descripción del grupo (si procede) y, a continuación, pulse Intro.**
6. **Para guardar el nuevo grupo, pulse en 7. Save Changes (Guardar cambios).**

▼ Para agregar un miembro a un grupo

1. **En el menú Extensions (Extensiones) seleccione CIFS/SMB Configuration (Configuración de CIFS/SMB).**
2. **Seleccione B. Local Groups (Grupos locales).**
3. **Seleccione la letra del grupo que desee modificar.**
4. **Seleccione 2. Members (Miembros) para cambiar la condición de miembro del grupo.**
5. **Seleccione 8. Add (Agregar) para añadir un miembro.**
6. **Escriba el nombre del dominio y de usuario siguiendo la estructura** *dominio*`\` *nombre-usuario***.**

   El dominio identifica el dominio en el que puede autenticarse el nombre de usuario. Por ejemplo, si escribe `BENCHLAB\juan` el dominio `BENCHLAB` será donde podrá autenticarse el usuario `juan`.
7. **Pulse Intro.**
8. **Para guardar el nuevo miembro, pulse 7. Save Changes (Guardar cambios).**

▼ Para eliminar el miembro de un grupo

1. **En el menú Extensions (Extensiones) seleccione CIFS/SMB Configuration (Configuración de CIFS/SMB).**
2. **Seleccione B. Local Groups (Grupos locales).**
3. **Seleccione la letra del grupo que desee modificar.**
4. **Seleccione 2. Members (Miembros) para cambiar la condición de miembro del grupo.**
5. **Pulse la letra correspondiente al miembro del grupo que desee eliminar.**
6. **Para responder al mensaje, haga clic en Y (S).**

Privilegios de grupo

En "Configuración de privilegios para los grupos locales" en la página 86 encontrará una descripción de los privilegios de los grupos de usuarios.

▼ Para modificar los privilegios de los grupos locales

1. **En el menú Extensions (Extensiones) seleccione CIFS/SMB Configuration (Configuración de CIFS/SMB).**
2. **Seleccione B. Local Groups (Grupos locales).**
3. **Seleccione la letra del grupo que desee modificar.**
4. **Seleccione 3. Privileges (Privilegios) para cambiar los privilegios de los miembros del grupo.**
5. **Pulse la letra del privilegio que desee añadir o eliminar.**
6. **Para guardar los cambios realizados, seleccione 7. Save Changes (Guardar cambios).**

Asignaciones del usuario y de grupo

Si desea obtener una descripción completa de las credenciales de usuarios y grupos, consulte "Asignación de las credenciales de usuario y grupo" en la página 91.

▼ Para agregar una asignación de usuario

1. **En el menú Extensions (Extensiones) seleccione CIFS/SMB Configuration (Configuración de CIFS/SMB).**
2. **Seleccione C. User Mapping (Asignación de usuario).**
3. **Haga clic en 8. Add a map (Agregar una asignación).**
4. **En el campo Account (Cuenta), escriba el dominio y el nombre del usuario NT que desea asignar a un usuario UNIX.**

   Utilice la estructura de *dominio\nombre-usuario*.
5. **En el campo Name (Nombre), escriba el nombre del usuario UNIX que desea asignar al usuario NT.**
6. **Pulse en 7. Save Changes (Guardar cambios).**

▼ Para editar una asignación de usuario

1. **En el menú Extensions (Extensiones) seleccione CIFS/SMB Configuration (Configuración de CIFS/SMB).**
2. **Seleccione C. User Mapping (Asignación de usuario).**
3. **Pulse la letra de la asignación que desee editar.**
4. **Haga clic en 1. Edit fields (Editar campos).**
5. **Escriba los cambios y, a continuación, pulse Intro.**
6. **Pulse en 7. Save Changes (Guardar cambios).**

▼ Para eliminar una asignación de usuario

1. **En el menú Extensions (Extensiones) seleccione CIFS/SMB Configuration (Configuración de CIFS/SMB).**
2. **Seleccione C. User Mapping (Asignación de usuario).**
3. **Pulse la letra de la asignación de usuario que desee eliminar.**
4. **Haga clic en 8. Delete (Borrar).**

▼ Para agregar una asignación de grupo

1. **En el menú Extensions (Extensiones) seleccione CIFS/SMB Configuration (Configuración de CIFS/SMB).**
2. **Seleccione D. Group Mapping (Asignación de grupo).**
3. **Haga clic en 8. Add a map (Agregar una asignación).**
4. **En el campo Account (Cuenta), escriba el dominio y el nombre del grupo NT que desea asignar a un grupo de UNIX. Siga la estructura de** *dominio**nombre-usuario*.
5. **En el campo Name (Nombre), escriba el nombre del grupo UNIX que desea asignar al grupo NT.**
6. **Pulse en 7. Save Changes (Guardar cambios).**

▼ Para editar una asignación de grupo

1. **En el menú Extensions (Extensiones) seleccione CIFS/SMB Configuration (Configuración de CIFS/SMB).**
2. **Seleccione D. Group Mapping (Asignación de grupo).**
3. **Pulse la letra de la asignación de grupo que desee editar.**

4. **Haga clic en 1. Edit fields (Editar campos).**
5. **Escriba los cambios y, a continuación, pulse Intro.**
6. **Pulse en 7. Save Changes (Guardar cambios).**

▼ Para eliminar una asignación de grupo

1. **En el menú Extensions (Extensiones) seleccione CIFS/SMB Configuration (Configuración de CIFS/SMB).**
2. **Seleccione D. Group Mapping (Asignación de grupo).**
3. **Pulse la letra de la asignación de grupo que desee borrar.**
4. **Haga clic en 8. Delete (Borrar).**

Asignación y objetos seguros

Esta sección describe cómo interactúan las asignaciones de credenciales de usuario y grupo y los objetos seguros, tal como archivos y directorios del sistema de archivos, en el sistema.

Los objetos que residen en el sistema se clasifican según el dominio desde el que se definieron los atributos de seguridad. Los objetos creados con el protocolo NFS poseen sólo atributos de seguridad de UNIX, por lo que están clasificados como objetos de UNIX. Los objetos creados con el protocolo SMB poseen atributos de seguridad tanto de UNIX como de Windows, por lo que están clasificados como objetos de Windows. Aunque es posible hacer migrar los objetos de un dominio a otro, como sus atributos de seguridad cambian, existe una política para que se permita sólo una de las migraciones. Un objeto de UNIX se convierte en objeto de Windows cuando se utiliza SMB para cambiar sus atributos de seguridad. De forma predeterminada, los atributos de seguridad de un objeto de Windows no se pueden modificar con NFS. Esto se debe a que la seguridad en Windows está basada en descriptores que no siempre se pueden representar correctamente con los atributos de seguridad de UNIX. Si se permite que un objeto de Windows se convierta en objeto de UNIX, el control de acceso que lo protege se debilita.

Existen dos métodos para cambiar los atributos de un objeto de Windows por medio de NFS: el comando `chsmb` y la variable de entorno `acl.overwrite.allowed`.

Si la variable `acl.overwrite.allowed` no está presente o se define en `no`, se aplicará el comportamiento predeterminado; es decir, los atributos del objeto de Windows no se podrán modificar con NFS.

Si la variable `acl.overwrite.allowed` se define en `yes`, los comandos de UNIX como `chown`, `chgrp` y `chmod` estarán permitidos, conforme a las reglas de acceso estándar de UNIX. Si los atributos del objeto de Windows se modifican utilizando NFS, el descriptor de seguridad se elimina y el objeto se convierte en uno de UNIX.

El comando `chsmb` permite eliminar un solo descriptor de seguridad o toda la base de datos de descriptores de seguridad de Windows para un volumen. Para aplicar el comando `chsmb` a un archivo o directorio en particular, debe especificar la ruta absoluta a ese objeto. Tenga en cuenta que `chsmb` no realiza operaciones recursivas, por lo que los subdirectorios y los archivos que contiene un directorio no se ven afectados cuando este comando se aplica al directorio. Los siguientes ejemplos ilustran el uso del comando `chsmb`.

Para borrar el descriptor de seguridad y volver a los permisos de UNIX en `/vol1/shared/bin/file.doc`, utilice el siguiente comando:

```
chsmb /vol1/shared/bin/file.doc
```

Para borrar todos los descriptores de seguridad en `/vol1` y revertir todos los archivos a sus permisos de UNIX, utilice el siguiente comando:

```
chsmb /vol1
```

El comando `chsmb` afecta a la seguridad de los archivos por lo que debe ser utilizado con cuidado. Cuando se especifica un volumen, `chsmb` envía una advertencia y solicita su confirmación antes de realizar cualquier otra acción.

No se realizan asignaciones cuando el usuario de Windows accede a un objeto de Windows. Tampoco ocurren asignaciones cuando el usuario de UNIX accede a un objeto de UNIX. Se consideran condiciones de acceso nativo. Además, los objetos de Windows poseen atributos de seguridad tanto de Windows como de UNIX, por lo que no se requieren asignaciones cuando el usuario de UNIX accede a un objeto de Windows, aunque se trate de una situación de acceso no nativo. Es una ventaja directa que proviene de la decisión diseñada de elegir uno de los dominios como de asignación predeterminada, en vez de crear asignaciones independientes neutras. Así, el único momento en que se requiere una asignación es cuando el usuario de Windows accede a un objeto de UNIX. Cuando este usuario accede al objeto de UNIX, los atributos de seguridad de dicho objeto se asignan al dominio de Windows y empiezan a aplicarse las políticas de seguridad de Windows.

Configuración de la lista de hosts

La consola le permite configurar la información de host.

▼ Para agregar un host

1. **En el menú Configuration (Configuración) seleccione Hosts.**
2. **Escriba el nombre del nuevo host y, a continuación, pulse Intro.**

   El sistema comprueba que el nombre de host no concuerda con ninguno de los existentes.
3. **Para agregar el host pulse Intro.**

4. **Escriba la dirección IP del nuevo host.**
5. **Seleccione 7. Save changes (Guardar cambios).**

▼ Para editar un host existente

1. **En el menú Configuration (Configuración) seleccione Hosts.**
2. **Escriba el nombre del host que desee editar y, a continuación, pulse Intro.**
3. **Seleccione 1. Edit (Editar).**
4. **Escriba el nombre o la dirección IP del nuevo host.**
5. **Seleccione 7. Save changes (Guardar cambios).**

▼ Para borrar un host

1. **En el menú Configuration (Configuración) seleccione Hosts.**
2. **Escriba el nombre del host que desee borrar y, a continuación, pulse Intro.**
3. **Seleccione 8. Delete (Borrar).**

Gestión de hosts de confianza

Utilice la opción de menú **Trusted Hosts** (Hosts de confianza) para gestionar los hosts que poseen acceso ilimitado a todos los recursos.

▼ Para designar un host de confianza

1. **En el menú Access Control (Control de acceso) seleccione Trusted Hosts (Hosts de confianza).**
2. **Escriba un nombre de host y pulse Intro.**

Nota – Para añadir un host de confianza, debe estar presente en la lista de host o en NIS.

El sistema comprueba que el nombre del host de confianza no concuerda con ninguno de los existentes. Si ya existe el host de confianza, aparecerá en la pantalla la información del host. Si el host no es de confianza, el sistema emitirá una señal de advertencia.

3. **Seleccione 7. Add to list (Agregar a la lista).**

   El nuevo host de confianza queda añadido y el sistema muestra el nombre en la parte superior de la pantalla.

▼ Para borrar un host de confianza

1. **En el menú Access Control (Control de acceso) seleccione Trusted Hosts (Hosts de confianza).**
2. **Escriba el nombre del host de confianza que desee borrar y, a continuación, pulse Intro.**
3. **Seleccione 8. Delete (Borrar).**

   Se elimina de la lista el host de confianza.

Gestión de acceso a volúmenes

Cuando haya guardado los cambios, se actualizarán los NFS existentes de los clientes para mostrar los nuevos parámetros.

No permita ningún tipo de acceso (ni de lectura, ni de escritura) al volumen `cvol`.

Nota – Los hosts de confianza adquieren automáticamente acceso de lectura/escritura a los volúmenes de archivo independientemente de la configuración de acceso de los volúmenes.

▼ Para gestionar un acceso a volumen para los clientes NFS

1. **En el menú Access Control (Control de acceso) seleccione Volume Access (Acceso a volumen).**
2. **Para cambiar el acceso a un volumen, escriba la letra correspondiente a dicho volumen.**
3. **Escriba el número correspondiente al tipo de acceso que desee asignar: read/write access (acceso de lectura/escritura), read-only access (acceso de sólo lectura) o no access (ningún acceso).**

   Nota – Los hosts de la lista de hosts de confianza tienen acceso de lectura/escritura sean cuales sean los parámetros de acceso a volúmenes.

   ---

4. **Seleccione 7. Save changes (Guardar cambios).**

Bloqueo y desbloqueo de la consola

Puede utilizar la consola para deshabilitar o habilitar casi todas las opciones del menú principal, con el fin de que no se acceda a la consola sin autorización. Para asegurar la consola deberá configurar la contraseña administrativa.

▼ Para bloquear la consola

1. **En el menú Operations (Operaciones) seleccione Lock Console (Bloqueo de consola).**
2. **Escriba la contraseña administrativa.**
3. **Seleccione Y (Yes) (Sí).**

▼ Para desbloquear la consola

1. **En el menú principal seleccione Unlock Console (Desbloqueo de consola).**
2. **Escriba la contraseña administrativa.**
3. **Seleccione Y (Yes) (Sí).**

Duplicación de volúmenes de archivo

Esta sección explica cómo duplicar los volúmenes de archivo de un sistema de dispositivo Sun StorEdge 5310 NAS activo a un sistema de dispositivo Sun StorEdge 5310 NAS duplicado. Para obtener más información sobre la duplicación, consulte el Capítulo 9.

Nota – Si se utiliza la replicación de archivos en un clúster Sun StorEdge 5310 no haga operaciones de duplicación, como un cambio de función, cuando el clúster tenga un rendimiento reducido.

Configuración de servidores activos y de duplicación

Una vez que las direcciones IP principales estén configuradas en los servidores activo y de duplicación, y haya designado las funciones de los puertos que conectan entre sí los servidores duplicados del dispositivo Sun StorEdge 5310 NAS, podrá configurar la duplicación en ambos servidores utilizando la interfaz de la consola.

▼ Para configurar un nuevo servidor activo con un nuevo servidor de duplicación

1. **En el menú Configuration (Configuración), seleccione Host Names and Network (Nombres de host y red).**
2. **Seleccione 1. Edit Fields (Editar campos).**
3. **Si aún no lo ha hecho, configure los puertos que estén conectados a una subred o red local.**

   Para obtener información acerca de la configuración de TCP/IP desde la consola, consulte "Para configurar TCP/IP" en la página 199. Para obtener más información sobre la configuración de los puertos, consulte el Capítulo 5.
4. **Asigne el nombre y la dirección IP del servidor al puerto utilizado para la conexión entre el sistema activo y el de duplicación.**
5. **En el campo Role (Función) del puerto de conexión entre el servidor activo y el servidor de duplicación, seleccione Mirror (Duplicar).**
6. **Seleccione Save (Guardar) para almacenar los cambios y volver al menú principal.**
7. **Configure el DNS y NIS/NIS+, si están disponibles estos servicios, y el orden de búsqueda del servicio de nombres.**

   Para obtener información acerca de cómo configurar los servicios de nombres, consulte "Servicios de nombres" en la página 205.
8. **Abra una ventana de Telnet para el sistema de duplicación y repita del paso 1 al paso 6.**

   Ahora las conexiones de red del sistema activo y de duplicación están configuradas. Continúe en la siguiente sección.

▼ Para configurar un servidor activo existente con un nuevo servidor de duplicación

1. **En el menú Configuration (Configuración) del servidor activo, seleccione Host Names and Network (Nombres de host y red).**
2. **Seleccione 1. Edit Fields (Editar campos).**
3. **Asigne el nombre y la dirección IP del servidor al puerto utilizado para la conexión entre el sistema activo y el de duplicación.**
4. **En el campo Role (Función) del puerto de conexión entre el servidor activo y el servidor de duplicación, seleccione Mirror (Duplicar).**
5. **Abra una ventana de Telnet para el sistema de duplicación y repita del paso 1 al paso 4.**

6. **En la ventana de Telnet del servidor activo, pulse Esc hasta llegar a la siguiente línea de comandos:**

   ```
   connect to (? for list) ? [menu]
   ```

7. **Inicie una sesión de administrador y escriba lo siguiente:**

   `ping` *xxx.xxx.xx.xx*

   donde *xxx.xxx.xx.xx* es la dirección IP del servidor de duplicación.

8. **Repita el paso 7. en el servidor de duplicación y escriba la dirección IP del servidor activo.**

   Ahora las conexiones de red del sistema activo y de duplicación están configuradas. Continúe con la configuración de los volúmenes de archivo para duplicación.

Configuración de volúmenes de archivo

La duplicación se lleva a cabo por volúmenes. Puede duplicar algunos o todos los volúmenes.

Nota – Una vez que se duplica un volumen de archivo, no es posible cambiar el nombre de dicho volumen mientras se mantenga la conexión de duplicación. Se pueden duplicar los volúmenes de archivo con un tamaño igual o superior a 1 gigabyte.

▼ Para configurar un volumen de archivo para duplicación

Realice estos pasos en el sistema activo y después en el sistema de duplicación.

1. **Cree un volumen de archivo pequeño (por ejemplo, de 32 MB) con el nombre `SYS` antes de crear otros volúmenes.**

   Si ya existen volúmenes de archivo en el sistema activo, este paso es optativo.

2. **En el menú Configuration (Configuración), seleccione Disks and Volumes (Discos y volúmenes).**

3. **Seleccione la unidad en que desea crear un volumen de archivo nuevo.**

4. **Seleccione Create & init partition (Crear e iniciar partición). Ahora seleccione 1. sfs2.**

5. **Escriba SYS para el nombre y 64 para el tamaño en MB.**

   Esto obliga a que el directorio `/etc` y los archivos de configuración del dispositivo Sun StorEdge 5310 NAS que contiene residan en el volumen `SYS`.

   No cree otros volúmenes de archivo en el sistema de duplicación.

▼ Para duplicar volúmenes de archivo

1. **Utilice Telnet para conectarse al sistema activo y acceda al menú principal.**
2. **En el menú Operations (Operaciones), seleccione Licenses (Licencias) y la letra correspondiente de Mirroring (Duplicación).**
3. **Escriba la clave de activación que le ha proporcionado Sun Microsystems.**
4. **Pulse Esc hasta llegar al menú principal.**
5. **En el menú Extensions (Extensiones) seleccione Mirrors (Duplicaciones).**
6. **Seleccione Add mirror (Agregar duplicación) para crear una nueva duplicación.**
7. **Seleccione el volumen de archivo que se va a duplicar pulsando la letra correspondiente.**

   Este volumen de archivo debe ser igual o mayor que 1 GB.
8. **Escriba el nombre de host del sistema de duplicación.**
9. **Escriba la dirección IP privada, si es necesario.**

   Se trata de la dirección IP utilizada para la conexión de duplicación con el servidor duplicado.
10. **Escriba las direcciones IP alternativas en los campos Alt IP Address (Direcciones IP alternativas).**
11. **Si se requiere una contraseña administrativa para acceder al servidor de duplicación, escríbala en el campo Remote admin password (Contraseña de administrador remoto).**
12. **Escriba el tamaño de reserva de la memoria búfer de transacciones, y pulse Intro.**
13. **Seleccione 7. Proceed (Proceder) a fin de agregar el volumen de archivo de la duplicación.**

    Cuando este volumen alcanza el estado de sincronización con el volumen activo, se monta como un volumen de sólo lectura.

    Nota – No puede haber actividad de E/S procedente del servidor activo durante la sincronización de duplicación inicial.

    Durante y una vez creada la duplicación, el sistema muestra la pantalla Mirror Creation (Creación de duplicación).
14. **Para ver el estado de la duplicación, seleccione A.**
15. **Para editar las direcciones IP alternativas o la contraseña de administrador, seleccione 1. Edit (Editar).**

Definición de los umbrales de advertencia

Si la reserva de memoria búfer de transacciones se llena y se desborda, la duplicación "falla". Esta pantalla permite definir los porcentajes en que se enviarán las advertencias. Los porcentajes predeterminados son el 70, 80 y 90%.

▼ Para definir los porcentajes del umbral en que se comunican advertencias

1. **En el menú Extensions (Extensiones) del sistema activo, seleccione Mirrors (Duplicaciones).**
2. **Seleccione 3. Threshold Config. (Configuración de umbral).**
3. **Seleccione 1. Edit (Editar) para cambiar los porcentajes mostrados en la pantalla.**
4. **Escriba los porcentajes que desee.**
5. **En el campo Alert Silent Period (Periodo de silencio de alertas), escriba el número de horas que esperará el sistema antes de que emita otra vez la misma advertencia de umbral.**
6. **Seleccione 7. Proceed (Proceder).**

Promoción de un volumen de archivo duplicado

Si el servidor activo falla, el servidor de duplicación proporciona alta disponibilidad. Para que un volumen de archivo duplicado esté a disposición de los usuarios de red, debe promocionar el volumen de archivo. Primero es necesario interrumpir la duplicación desconectando la conexión entre los volúmenes de archivo activo y de duplicación. Después, promocione el volumen y configure los derechos de acceso del volumen de archivo duplicado. Una vez que se interrumpe la duplicación y se promociona el volumen de archivo duplicado, los dos volúmenes de archivo pasan a ser independientes.

▼ Para promocionar un volumen de archivo en el sistema de duplicación

1. **En el sistema de duplicación, seleccione Disks & Volumes (Discos y volúmenes) en el menú Configuration (Configuración) para ver el estado del volumen de archivos.**

   Un asterisco (*) mostrado después del nombre del volumen de archivo duplicado indica que, en estos momentos, ese volumen se está duplicando.

Nota – Debe interrumpir el volumen de archivo duplicado desde el sistema de duplicación únicamente cuando el sistema activo no se encuentre disponible. Para promocionar el volumen de archivo cuando está disponible el sistema activo, interrumpa la duplicación siempre desde el sistema activo, no desde el sistema de duplicación.

---

2. **En el menú Extensions (Extensiones) seleccione Mirrors (Duplicaciones).**
3. **Seleccione la letra correspondiente del volumen de archivo duplicado que va a interrumpir.**
4. **Seleccione 8. Break (Interrumpir).**
5. **Cuando se le solicite que confirme la interrupción, seleccione Y. Yes (Sí) para continuar.**
6. **Pulse la tecla Esc para volver a la pantalla principal Mirrors (Duplicaciones).**
7. **En el menú Extensions (Extensiones) seleccione Mirrors (Duplicaciones).**
8. **Seleccione 1. Promote Volume (Promocionar volumen)**
9. **Seleccione la letra correspondiente del volumen de archivo que desea promocionar.**
10. **Seleccione 7. Proceed (Proceder) para promocionar el volumen de archivo.**

    Este proceso puede tardar varios minutos en completarse. Para que un volumen de archivo de duplicación se pueda promocionar, es necesario que haya alcanzado al menos una vez el estado de sincronización.
11. **Cuando el sistema termine de promocionar el volumen, pulse Esc para volver al menú principal.**
12. **(Optativo) Para configurar el acceso a un volumen de archivo NFS, seleccione Volume Access (Acceso a volumen) en el menú Access Control (Control de acceso).**
13. **Defina los derechos de acceso al volumen de archivo seleccionando la letra correspondiente.**
14. **Elija el derecho de lectura/escritura, sólo lectura o ninguno.**
15. **Seleccione 7. Save changes (Guardar cambios) para continuar.**

    El volumen ha sido promocionado. Para restablecer una duplicación, consulte la siguiente sección, "Restablecimiento de una duplicación" en la página 231.

Restablecimiento de una duplicación

Este procedimiento describe cómo restablecer una duplicación cuando el servidor activo ha fallado y ha promocionado un volumen de archivo en el servidor de la duplicación. El volumen de archivo promocionado es ahora la versión más actualizada y funciona de forma independiente del volumen de archivo desfasado del sistema activo. Para volver a crear la duplicación, es necesario que duplique otra vez el volumen de archivo actualizado en el servidor activo y, a continuación, en el servidor de duplicación, tal y como hizo al principio.

Nota – Si el volumen de archivo duplicado no está promocionado, no siga estas instrucciones. El sistema activo pone automáticamente la duplicación en estado In Sync (En sincronización) cuando se conecta de nuevo.

En los ejemplos que aparecen a continuación, el Servidor 1 es activo y el Servidor 2 es de duplicación.

Restablecer una duplicación incluye los siguientes pasos:

1. Interrumpir la duplicación en el Servidor 1
2. Borrar el volumen de archivo desfasado del Servidor 1
3. Duplicar el volumen de archivo actualizado desde el Servidor 2 al Servidor 1
4. Cambiar las funciones para convertir el Servidor 1 en activo y el Servidor 2 en el de duplicación

Cuando el servidor activo se conecte de nuevo, intentará restablecer la duplicación. Por lo tanto, debe interrumpir la duplicación en el Servidor 1.

▼ Para interrumpir la duplicación en el Servidor 1

1. **En el Servidor 1, en el menú Extensions (Extensiones), seleccione Mirrors (Duplicaciones).**
2. **Seleccione la letra respectiva del volumen de archivo de la duplicación.**
3. **Seleccione 8. Break (Interrumpir).**
4. **Seleccione Y. Yes (Sí) para confirmar que interrumpe la duplicación.**

▼ Para borrar el volumen de archivo desfasado del Servidor 1

1. **Pulse la tecla Esc para volver al menú principal.**
2. **En el menú Configuration (Configuración) seleccione Disks & Volumes (Discos y volúmenes).**
3. **Seleccione el número que corresponda al volumen de archivo de la duplicación.**

Precaución – Antes de proseguir en el siguiente paso, asegúrese de que ha borrado el volumen de archivo desfasado en el Servidor 1 y de que primero se promociona y verifica el volumen de archivo actualizado en el Servidor 2.

4. **Seleccione 8. Delete (Borrar).**
5. **Escriba el nombre del volumen de archivo desfasado.**
6. **Seleccione 7. Proceed with delete (Proceder con borrado) a fin de eliminar el volumen de archivo desfasado.**

▼ Para duplicar el volumen de archivo actualizado del Servidor 2 en el Servidor 1

1. **En el Servidor 2, en el menú Extensions (Extensiones), seleccione Mirrors (Duplicaciones).**
2. **Seleccione 8. Add mirror (Agregar duplicación).**
3. **Seleccione la letra correspondiente del volumen de archivo que va a duplicar.**
4. **Escriba el nombre de host privado del Servidor 1.**
5. **Escriba la dirección IP privada, si es necesario, y la contraseña de administrador.**
6. **Escriba la reserva del búfer de transacciones.**

   Para obtener más información, consulte "Para duplicar volúmenes de archivo" en la página 229.
7. **Seleccione 7. Proceed (Proceder).**
8. **Durante la creación de duplicaciones, seleccione la letra respectiva del nuevo volumen de archivo duplicado.**

   Cuando la duplicación alcance el estado In Sync (En sincronización), habrá una copia exacta del volumen de archivo tanto en el Servidor 1 como en el Servidor 2. Consulte las secciones a continuación.

▼ Para cambiar las funciones

Nota – Compruebe que los volúmenes se encuentran en perfecta sincronización antes de cambiar las funciones.

---

1. **En el menú principal, seleccione la opción Mirror (Duplicación) en el Servidor 1.**
2. **Seleccione el volumen que desee pulsando la letra respectiva.**
   Por ejemplo, pulse A si quiere seleccionar el volumen de archivo `cvol1`.
3. **En el menú Mirror Status (Estado de duplicación), seleccione la opción Change Role (Cambiar función).**
4. **Seleccione Yes (Sí) para confirmar.**

Supervisión

Puede utilizar la consola para realizar las funciones de supervisión.

Configuración SNMP

El menú SNMP le permite enviar mensajes a un monitor SNMP (Simple Network Management Protocol) remoto, además de poder modificar la línea de comunidad, la información de contacto y la ubicación del monitor SNMP.

▼ Para configurar SNMP

1. **En el menú Extensions (Extensiones) seleccione SNMP Configuration (Configuración de SNMP).**

   El nombre predeterminado de la comunidad es Public (Pública). Puede especificar el nombre que desee.

2. **Seleccione 1-5. Edit a Trap Destination (Editar un destino de captura) para añadir, editar o borrar un destino de captura; 6. Edit Community (Editar comunidad) para editar la línea de la comunidad; 7. Edit Contact (Editar contacto) para editar la información de contacto, o 8. Edit Location (Editar ubicación) para editar la ubicación del monitor SNMP remoto.**

3. **Seleccione Y. Yes (Sí) para guardar los cambios.**

Configuración de la notificación por correo electrónico

Cuando se produce un problema en el sistema, el dispositivo Sun StorEdge 5310 NAS envía mensajes de correo electrónico a una serie de destinatarios.

Nota – Para que la notificación por correo electrónico funcione correctamente debe configurar DNS.

▼ Para configurar la notificación por correo electrónico

1. **En el menú Extensions (Extensiones) seleccione EMAIL Configuration (Configuración de correo electrónico).**

2. **Seleccione 1. Edit fields (Editar campos).**

3. **Escriba la información pertinente en el campo correspondiente. Para pasar de un campo a otro pulse Intro.**
   - **SMTP Server** (Servidor SMTP): el servidor de correo electrónico al que se dirigen todos los mensajes de correo electrónico. El archivo de host o el servidor de DOS deben incluir el nombre del servidor.

Nota – Puede utilizar la dirección IP o el nombre. El servidor DNS debe resolver el nombre.

   - **Recipient 1–4** (Destinatarios 1-4): son las direcciones de correo electrónico de las cuatro personas que recibirán una notificación automática si ocurre algún problema.
   - **Notification Level** (Nivel de notificación): el nivel que debe alcanzar un problema para que los destinatarios reciban la notificación por correo electrónico. Elija uno de los siguientes valores:
     - **Errors** (Errores): sólo se envían notificaciones en caso de errores.
     - **Errors and warnings** (Errores y advertencias): se envían notificaciones en caso de errores y advertencias de baja prioridad.
     - **None** (Ninguno): no se envían notificaciones.
4. **Para guardar la configuración actual, seleccione 7. Save changes (Guardar cambios).**
5. **Pulse la tecla Esc para volver al menú principal.**

Visualización de información del sistema

Puede ver la información del sistema en la consola.

▼ Para ver el estado de los servidores

1. **En el menú Operations (Operaciones) seleccione Activity Monitor (Monitor de actividad).**

   La pantalla Activity Monitor (Monitor de actividad) muestra la siguiente información:
   - **Volume** (Volumen): los 22 primeros volúmenes de archivo.
   - **Use%** (Porcentaje utilizado): la cantidad de espacio utilizado en el volumen.
   - **Reqs** (Solicitudes): el número de solicitudes procesadas para el volumen en los últimos 10 segundos.
   - **Device** (Dispositivo): el nombre del dispositivo.
   - **Load** (Carga): el porcentaje de carga de la CPU.
   - **Peak** (Pico): el momento de mayor uso por segundo en los 10 minutos anteriores.
   - **Client** (Cliente): el nombre o la dirección del usuario.
   - **Reqs** (Solicitudes): el número de solicitudes procesadas para el volumen en los últimos 10 segundos.
2. **Pulse la tecla Esc para volver al menú principal.**

▼ Para ver el registro del sistema

- **En el menú Operations (Operaciones) seleccione Show Log (Mostrar registro).**

  En el registro aparecen dos tipos de entradas:

  - **System Startup Log Entries** (Entradas de registro de inicio de sistema): informa sobre la configuración y los volúmenes del dispositivo y tiene otra información importante.
  - **Normal Operation Log Entries** (Entradas de registro de funcionamiento normal): informa de los errores del dispositivo, las violaciones de seguridad y otro datos sobre el estado de las rutas. En último lugar aparecen el número de versión y el número de serie del software.

▼ Para ver los puertos enlazados

1. **En el menú Configuration (Configuración), seleccione Host Name & Network (Nombre de host y red).**
2. **Para pasar a la página siguiente pulse la barra espaciadora.**

   La columna bond1 (enlazado1) muestra el primer puerto enlazado. La información de entrada/salida que aparece en esta columna es la suma de la información de entrada/salida de ambos puertos que ha enlazado.

▼ Para ver el análisis de los puntos de control

1. **En el menú Configuration (Configuración) seleccione Disks & Volumes (Discos y volúmenes).**
2. **Escriba la letra correspondiente a la unidad que va a configurar.**
3. **Seleccione Change/Delete *nombre-volumen* (Cambiar/Borrar).**
4. **Seleccione 6. Checkpoints (Puntos de control).**
5. **Seleccione 3. Analysis (Análisis). Para desplazarse por esta pantalla utilice la barra espaciadora.**
6. **Para salir de esta pantalla seleccione 0. End Analysis (Finalizar análisis).**

▼ Para ver el estado de un volumen de archivo duplicado

1. **En el sistema activo, seleccione Mirrors (Duplicaciones) en el menú Extensions (Extensiones).**
2. **Seleccione el volumen de archivo duplicado.**

   La pantalla de estado tiene tres partes:

- La primera línea muestra la información del estado de la duplicación, incluyendo el nombre del volumen de archivo, la duplicación, un indicador de progreso y un mensaje de estado. Existen diez estados de la duplicación:
  - ERR**:** ha sucedido un error.
  - NEW**:** se está creando una nueva duplicación.
  - INIT**:** la memoria búfer de duplicación se está inicializando.
  - MKPT**:**se están creando particiones de disco en el sistema de duplicación.
  - RDY**:** es sistema está preparado y aguardando a que esté preparado el otro sistema.
  - DOWN**:** el enlace de red no se encuentra disponible.
  - CRK**:** la duplicación está interrumpida.
  - RPL**:** está sucediendo la fase de replicación.
  - OOS**:** la duplicación no está sincronizada.
  - SYNC**:** la duplicación está sincronizada.

  El indicador de progreso muestra el porcentaje de actividad de cada estado. El mensaje de estado también ofrece un mensaje de texto corto en que se describe el estado de la duplicación.
- La segunda línea muestra la condición de la reserva de memoria búfer de transacciones. La información que aporta es el número máximo de transacciones del búfer, el siguiente ID de transacción, el ID de transacción de sincronización, el ID de transacción de unidades, y un indicador de porcentaje que describe el estado de la sincronización entre el sistema activo y el sistema de duplicación.

  En el sistema activo, la información es la siguiente:
  - El siguiente xid (ID de siguiente transacción) identifica la próxima transacción del sistema de archivos.
  - El xid de sincronización (ID de transacción de sincronización) identifica la última transacción transferida al sistema de duplicación.
  - El xid de unidad (ID de transacción de unidad) identifica la última transacción reconocida por el sistema de duplicación.
  - Cuando el indicador de porcentaje de la sincronización alcanza el 100%, significa que el sistema de duplicación posee una copia completa del sistema activo. Si este indicador de porcentaje muestra el 0, significa que la duplicación está interrumpida y el servidor activo realiza automáticamente una resincronización bloque por bloque. Cuando la duplicación no se encuentra sincronizada, el volumen de duplicación es volátil.

  En el sistema de la duplicación, la información es la siguiente:
  - El siguiente xid (ID de siguiente transacción) identifica la próxima transacción prevista desde el sistema activo.
  - El xid de sincronización (ID de transacción de sincronización) identifica la última transacción de escritura programada en disco.
  - El xid de unidad (ID de transacción de unidad) identifica la última transacción reconocida en disco.
  - Cuando el indicador de porcentaje de la sincronización alcanza el 100%, significa que todas las transacciones de duplicación se han escrito en el disco y que el volumen del sistema de duplicación es una copia exacta del volumen del sistema activo.

3. **Para editar las direcciones IP alternativas o la contraseña de administrador, seleccione 1. Edit (Editar).**

4. **Edite los campos y después seleccione 7. Proceed (Proceder) para guardar los cambios.**

5. **Para ver las estadísticas de red del volumen de archivo duplicado, seleccione 2. Statistics (Estadísticas).**

   La pantalla muestra las estadísticas del sistema activo, incluido el número de transacciones hacia el volumen de archivo activo (IN) y fuera del sistema activo hacia el volumen de archivo duplicado (OUT). En la pantalla se indican las transacciones promedio, mínimas y máximas por segundo (t/s) de cada sistema.

   El sistema muestra la cantidad de espacio libre en la reserva del búfer de transacciones, además de su tasa de llenado. Si esta tasa es superior a cero, deberá comprobar que todos los enlaces de red estén funcionando correctamente. Esto significa que las transacciones están viajando hacia el sistema activo a una velocidad superior que con la que viajan hacia el sistema duplicado, por lo que la memoria búfer se llena. Cuando la memoria búfer se desborda, la duplicación "falla".

▼ Para ver las estadísticas de red de todos los volúmenes de archivo duplicados

1. **En el sistema activo, seleccione Mirrors (Duplicaciones) en el menú Extensions (Extensiones).**

2. **Seleccione 2. Network Statistics (Estadísticas de red).**

   La pantalla muestra el número total de bloques de control de solicitud (RCB) que se han enviado, el número de bloques enviado por segundo y el tamaño promedio de los bloques, además del tiempo de respuesta promedio y la tasa de transferencia.

3. **Seleccione 1. Reset (Reiniciar) para reiniciar esta pantalla.**

Mantenimiento del sistema

Existen varias funciones de mantenimiento y configuración del sistema que se pueden realizar únicamente desde la consola. Se describen en las siguientes secciones:

- "Configuración del acceso a FTP" en la página 239
- "Gestión de los controladores RAID" en la página 240
- "Montaje de sistemas de archivos" en la página 242

En estas secciones se explican tareas adicionales que se pueden realizar tanto desde el administrador de consola como desde Web Administrator:

- "Apagado del sistema" en la página 242
- "Gestión de recuperación tras error" en la página 243
- "Configuración de rutas LUN" en la página 244
- "Programación de puntos de control de archivo" en la página 247
- "Configuración de copias de seguridad" en la página 248
- "Configuración de Compliance Archiving Software" en la página 248
- "Configuración de la auditoría del sistema" en la página 249

Configuración del acceso a FTP

El protocolo de transferencia de archivos (FTP, del inglés File Transfer Protocol) es un protocolo de Internet utilizado para copiar archivos entre un cliente y un servidor. FTP requiere que cada cliente que solicite acceder al servidor esté identificado con un nombre de usuario y una contraseña.

Puede establecer tres tipos de usuarios:

- **Administrators** (Administradores), cuyo nombre de usuario es `admin` y utilizan la misma contraseña que los clientes de la interfaz gráfica de usuario.

  El administrador tiene acceso "raíz" a todos los volúmenes, directorios y archivos del sistema. El directorio principal del administrador se define como "/".

- **Users** (Usuarios), que tienen un nombre de usuario y una contraseña que se especifica en el archivo de contraseña local o en un servidor NIS o NIS+ remoto.

  El usuario tiene acceso a todos los directorios y archivos dentro del directorio principal del usuario. El directorio principal está definido como parte de la información de la cuenta del usuario y se recupera por el servicio de nombre.

- **Guests** (Invitados), que acceden con el nombre de usuario `ftp` o su alias `anónimo`. En este caso se precisa una contraseña pero no es autenticada. Todos los usuarios invitados tienen acceso a todos los directorios y archivos que se encuentran en el directorio principal del usuario `ftp`.

Nota – Los usuarios invitados no pueden cambiar el nombre, sobrescribir o eliminar archivos; no pueden crear o eliminar directorios y tampoco pueden cambiar los permisos de los archivos o directorios existentes.

▼ Para configurar el acceso de FTP

1. **En el menú Extensions (Extensiones) seleccione FTP Configuration (Configuración de FTP).**
2. **Seleccione 1. Edit Fields (Editar campos).**
3. **Seleccione Y. Yes (Sí) para habilitar FTP o N. No para deshabilitarlo.**

   Si se habilita el servicio FTP, el servidor FTP aceptará las solicitudes de conexión entrantes.
4. **En Allow guest access (Permitir acceso a invitado) seleccione Yes (Sí) para habilitar el acceso al servidor FTP a usuarios anónimos o No para deshabilitar dicho acceso.**
5. **En Allow user access (Permitir acceso a usuario) seleccione Yes (Sí) para habilitar el acceso al servidor FTP a todos los usuarios o No para deshabilitar dicho acceso.**

   Esto no incluye el usuario `admin` o `raíz`.

Nota – Los nombres de usuario y las contraseñas deben especificarse en el archivo de contraseña local o en un servidor NIS o NIS+ remoto.

---

6. **En Allow admin access (Permitir acceso de administración), seleccione Yes (Sí) para permitir el acceso como superusuario a aquellos que tengan la contraseña administrativa del dispositivo Sun StorEdge 5310 NAS (utilícese con precaución), o No para deshabilitar el acceso.**

Nota – El superusuario es aquel cuyo UID (ID de usuario) es igual a 0 y el usuario especial `admin` del dispositivo Sun StorEdge 5310 NAS.

---

7. **En Enable logging (Habilitar inicio de sesión) seleccione Yes (Sí) para habilitar el inicio de sesión o No para deshabilitar dicho inicio.**
8. **Si habilita el inicio de sesión, en Log filename (Nombre de archivo de registro) especifique el nombre del archivo de registro.**
9. **Seleccione 7. Save changes (Guardar cambios).**

Gestión de los controladores RAID

El comando `raidctl` permite gestionar los controladores RAID desde la interfaz de línea de comandos.

Para todos los comandos `raidctl`, siga las instrucciones de "Para acceder a la interfaz de línea de comandos" en la página 196.

Precaución – Utilice los comandos con cuidado para evitar resultados no deseados.

▼ Para obtener ayuda sobre los subcomandos

1. **En la línea de comandos, escriba `raidctl help`.**

▼ Para controlar los LED

- **Para hacer que destellen todos los LED de una bandeja, escriba este comando:**

  `raidctl locate type=lsi target=tray ctlr=0..`*`n`* `tray=0..`*`n`*

- **Para hacer que el LED de la unidad especificada, escriba este comando:**

  `raidctl locate type=lsi target=drive ctlr=0..`*`n`* `tray=0..`*`n`* `slot=1..`*`n`*

- **Para hacer que no destellen los LED de un controlador especificado, escriba este comando:**

  `raidctl locate type=lsi action=stop ctlr=0..`*`n`*

▼ Para obtener información de eventos y configuración

- **Para obtener todos los eventos del controlador especificado, escriba este comando:**

  `raidctl get type=lsi target=events ctlr=0..`*`n`*

  El registro de todos los eventos se escribirá en el archivo `/cvol/log/2882ae.log`. Si este archivo ya existe, se le pedirá que lo sobrescriba, que especifique un nombre de archivo nuevo o que cancele la operación.

- **Para obtener los eventos críticos del controlador especificado, escriba este comando:**

  `raidctl get type=lsi target=events ctlr=0..`*`n`* `etype=critical`

  El registro de eventos críticos se escribirá en el archivo `/cvol/log/2882ce.log`. Si este archivo ya existe, se le pedirá que lo sobrescriba, que especifique un nombre de archivo nuevo o que cancele la operación.

- **Para obtener la información de configuración de un controlador especificado, escriba este comando:**

  `raidctl get type=lsi target=profile ctlr=0..`*`n`*

▼ Para definir la hora del controlador y la edad de la batería

- **Para restablecer la edad de la batería de un controlador especificado, escriba este comando:**

  `raidctl set type=lsi target=battery-age ctlr=0..`*`n`*

- **Para sincronizar la hora de un controlador con la hora del servidor, escriba este comando:**

  `raidctl set type=lsi target=ctlr_time-age ctlr=0..`*`n`*

▼ Para descargar el firmware

Utilice el comando `raidctl download` para descargar el firmware.

Nota – Consulte el Capítulo 11 para ver los procedimientos detallados de actualización del firmware.

Montaje de sistemas de archivos

Después de varios reinicios continuos, uno o más sistemas de archivos pueden quedar desmontados. Para montar los sistemas de archivos otra vez, utilice el siguiente comando:

```
mount -f volume_name
```

Apagado del sistema

El dispositivo Sun StorEdge 5310 NAS se ha diseñado para un funcionamiento continuo, aunque si necesita apagar el sistema, deberá hacerlo desde Web Administrator, la consola o la pantalla LCD.

▼ Para apagar el sistema

1. **En el menú Operations (Operaciones) seleccione Shutdown (Apagar).**
2. **Para seleccionar la opción que desee escriba la letra correspondiente.**
   - **R. Reboot** (Reinicio): escriba la letra "R" para reiniciar el sistema.
   - **H. Halt (Detener):** escriba la letra "H" para detener el sistema.
   - **P. Boot Previous Version 4.x.xx.xxx** (Iniciar versión anterior 4.x.xx.xxx): escriba la letra "P" para reiniciar el sistema utilizando la versión anterior disponible del sistema operativo. Esta opción se encuentra disponible en los sistemas que tengan instalada más de una versión de sistema operativo.
   - **ESC:**pulse la tecla Esc para cancelar y volver al menú principal.

Si elige reiniciar, detener o iniciar con la versión de sistema operativo anterior, el servidor se reiniciará o apagará después de haber completado todo el proceso de escritura retardada en los discos.

Gestión de recuperación tras error

Se produce una recuperación tras error cuando uno de los dos controladores RAID o unidades es inestable y todos los LUN bajo su control deben moverse al controlador o unidad estable. El menú Failover (Recuperación tras error) administra los recursos de disco cuando se produce un error de RAID recuperable.

▼ Para configurar la recuperación tras error

1. **En el menú Extensions (Extensiones), seleccione Failover/Move LUNs (Recuperación tras error/Mover LUN).**

   La recuperación tras error está configurada de forma predeterminada y no se puede desactivar.

2. **Si la opción está disponible, seleccione 3. Edit Failover (Editar recuperación tras error).**

   Nota – No puede habilitar o deshabilitar la recuperación de controlador tras error para el dispositivo Sun StorEdge 5310 NAS de una sola unidad.

   ---

3. **Seleccione Y. (Sí) para habilitar la recuperación de controlador o unidad tras error.**

4. **Si está utilizando el clúster Sun StorEdge 5310 o un servidor doble del sistema de puerta de enlace Sun StorEdge 5310 en una configuración de clúster, realice estos pasos:**

   a. **Seleccione Y. Yes (Sí) para habilitar la recuperación de enlaces tras error.**

      La recuperación de enlace tras error garantiza que habrá un enlace de red alternativo si falla el enlace principal.

   b. **Escriba el número de segundos antes de que se produzca la recuperación de enlace tras error en caso de que un enlace de red no sea fiable.**

   c. **Escriba el número de segundos antes de que se produzca la restauración del enlace en el caso de que el enlace original se repare o se vuelva a conectar.**

5. **Para los usuarios del clúster Sun StorEdge 5310 y la configuración en clúster del sistema de puerta de enlace Sun StorEdge 5310 sólo: Seleccione 2. Modify (Modificar) para redistribuir la propiedad de LUN por adaptador.**

   Los valores que especifique determinan la configuración que se utilizará cuando suceda el proceso de recuperación.

   a. **Introduzca los LUN propiedad de cada adaptador.**

   b. **Separe los números por un espacio (por ejemplo, `0 2 8 10`).**

   c. **Pulse Intro.**

6. **Seleccione Y. Yes (Sí) para guardar los cambios.**

▼ Para restablecer el sistema al iniciarse la recuperación tras error

1. **Sustituya o repare el componente defectuoso y asegúrese de que esté conectado.**
2. **En el menú Extensions (Extensiones), seleccione Failover/Move LUNs (Recuperación tras error/Mover LUN).**
3. **Seleccione 1. Restore (Restaurar).**
4. **Select Y. Yes (Sí) para realizar el proceso de restauración.**

Configuración de rutas LUN

Consulte "Configuración de las rutas LUN" en la página 10 para obtener más información acerca de las rutas de número de unidad lógica (LUN) y el uso de la GUI para configurar las rutas LUN.

▼ Para configurar o editar una ruta LUN

1. **En el menú Extensions (Extensiones), pulse la barra espaciadora hasta que se muestre la opción LUN Ownership (Propiedad de LUN) y selecciónela.**

   La pantalla LUN Ownership (Propiedad de LUN) muestra todos los LUN para los que se puede cambiar su ruta. Sólo se puede reasignar un LUN si no dispone de sistemas de archivos. En un clúster Sun StorEdge 5310 o un sistema de puerta de enlace Sun StorEdge 5310 en una configuración de clúster, sólo la unidad "propietaria" de un LUN podrá reasignarlo a otra unidad.

Nota – En un sistema de clúster de Sun StorEdge 5310 o un sistema de puerta de enlace Sun StorEdge 5310 en una configuración de clúster, cuando arranca el sistema por primera vez, todos los LUN se asignan a una unidad (Head 1). Utilice la unidad Head 1 para reasignar algunos LUN a la unidad Head 2 y obtener una distribución homogénea.

Nota – Los LUN que no tienen una ruta LUN asignada aparecerán inicialmente varias veces en la pantalla LUN Ownership (Propiedad de LUN) ya que su presencia se señala mediante varios controladores en varias rutas. Cuando un LUN tiene una ruta asignada, se muestra una vez, en la ruta actual.

---

2. **Seleccione una ruta LUN escribiendo la letra a la izquierda de la ruta deseada.**
3. **Select 1. Edit (Editar) para editar la ruta LUN.**

   La pantalla Configure LUN Path (Configurar ruta LUN) muestra todas las rutas disponibles para el LUN. La ruta LUN actual o activa está marcada como activa. Si la ruta principal se define para el LUN, se marcará como PRIMARY (Principal).

4. **Escriba el número de la ruta LUN deseada que desea cambiar y pulse Intro.**

   Divida homogéneamente los LUN entre las dos rutas disponibles. Por ejemplo, asigne el primer y tercer LUN a la ruta 1 y el segundo y cuarto LUN a la ruta 2.

5. **Seleccione Y. Yes (Sí) para guardar los cambios.**

Procedimientos de desasignación y reasignación para el sistema de puerta de acceso

Realice este procedimiento si desea desasignar un LUN que esté asignado al sistema de puerta de enlace Sun StorEdge 5310 NAS. También puede reasignar el LUN si necesita acceder a los datos en el futuro.

A continuación se resume el procedimiento de desasignación y reasignación:

1. Desasignacion de un LUN
   a. Desmonte los volúmenes que residen en el LUN que quiere desasignar.
   b. Desasigne el LUN utilizando el software de gestión SAN del host.
   c. Explore otra vez los LUN del sistema de puerta de enlace.
2. Reasignación de un LUN
   a. Reasigne el LUN utilizando el software de gestión SAN del host.
   b. Explore otra vez los LUN del sistema de puerta de enlace.
   c. Vuelva a montar los volúmenes a los que desea acceder.

En los siguientes procedimientos se ha ilustrado como ejemplo la matriz Sun StorEdge 6130.

▼ Para desasignar un LUN

1. **Desmonte el volumen en el sistema de puerta de enlace:**
   a. **Utilice Telnet para conectarse al sistema de puerta de enlace NAS.**
   b. **En el primer indicador, escriba** `admin` **para iniciar la CLI.**
   c. **Escriba** `mount` **para ver la lista de los volúmenes que están montados en el LUN que va a desasignar. La columna "Origin" (Origen) indica el nombre de los dispositivos sin procesar que contienen los volúmenes. Apunte los nombres de los volúmenes (en la columna del extremo izquierdo) que desea desmontar.**
   d. **Desmonte todos los volúmenes que residen en el LUN que quiere desasignar utilizando el comando** `umount`**. Escriba** `mount` **y compruebe que ninguno de los volúmenes que pertenecen al LUN están montados.**

2. **Desde el host de gestión de Sun StorEdge 6130, desasigne el LUN de la matriz conectada directamente.**

   a. **Abra un explorador en** `https://hostname:6789` **y acceda al software de gestión.**

   b. **Haga clic en Sun StorEdge 6130 Configuration Service (Servicio de configuración).**

   c. **Haga clic en la matriz cuyo LUN quiere desasignar.**

   d. **Haga clic en el nombre del LUN quiere desasignar.**

   e. **Haga clic en el botón Unmap (Desasignar).**

   f. **Haga clic en el ventana emergente para confirmar que desea borrar el LUN.**

3. **Explore otra vez el sistema de puerta de enlace.**

   a. **Seleccione el LUN que quiere desasignar.**

   b. **Utilice Telnet para conectarse al sistema de puerta de enlace NAS.**

   c. **En el primer indicador, escriba** `menu` **para iniciar la interfaz de menú basada en caracteres.**

   d. **Escriba la letra** `d` **para mostrar el menú Disks and Volumes (Discos y volúmenes).**

   e. **En este menú, escriba** `9` **para buscar nuevos discos (o LUN). Espere a que desaparezca el mensaje "Scanning for new disks, please wait..."**

▼ Para reasignar un LUN

1. **Desde el host de gestión de Sun StorEdge 6130, reasigne el LUN de la matriz conectada directamente.**

   a. **Abra un explorador en** `https://<hostname>:6789` **y acceda al software de gestión.**

   b. **Haga clic en Sun StorEdge 6130 Configuration Service (Servicio de configuración).**

   c. **Haga clic en la matriz cuyo LUN quiere reasignar.**

   d. **Haga clic en la casilla al lado del nombre del LUN que desea reasignar.**

   e. **Pulse el botón Map (Asignar).**

      Aparece la ventana Map Volumes (Asignar volúmenes).

   f. **Seleccione el host al que desea asignar el LUN.**

2. **Explore los LUN otra vez en el sistema de puerta de enlace:**

   a. **Utilice Telnet para conectarse al sistema de puerta de enlace.**

   b. **En el primer indicador, escriba** `menu` **para iniciar la interfaz de menú basada en caracteres.**

   c. **Escriba la letra** `d` **para mostrar el menú Disks and Volumes (Discos y volúmenes).**

   d. **En este menú, escriba** `9` **para buscar nuevos discos (o LUN). Espere a que desaparezca el mensaje "Scanning for new disks, please wait..."**

3. **Monte otra vez los volúmenes en el sistema de puerta de enlace.**

   a. **Utilice Telnet para conectarse al sistema de puerta de enlace.**

   b. **En el primer indicador, escriba** `admin` **para iniciar la CLI.**

   c. **Monte todos los volúmenes que residen en el LUN reasignado.**

   d. **Escriba** `mount` **para comprobar que todos los volúmenes están reasignados.**

Programación de puntos de control de archivo

Un punto de control es una copia virtual de sólo lectura de un volumen de archivo principal. Consulte "Puntos de control de archivo" en la página 164 para obtener información detallada sobre los puntos de control.

▼ Para programar puntos de control

1. **En el menú Configuration (Configuración) seleccione Disks & Volumes (Discos y volúmenes).**
2. **Seleccione la unidad para la que está programando los puntos de control.**

Nota – Si tiene más de 26 unidades de disco (volúmenes de disco), pulse la barra espaciadora para realizar la búsqueda.

---

3. **Seleccione 1. Edit (Editar).**
4. **Seleccione 6. Checkpoints (Puntos de control).**
5. **Siga las instrucciones que aparecen en la parte inferior de la pantalla y pulse Intro para pasar de un campo a otro.**
6. **Cuando haya especificado la información relativa a los puntos de control, seleccione 7. Save changes (Guardar cambios).**

Configuración de copias de seguridad

Para la copia de seguridad de los volúmenes del sistema, debe agregar un trabajo de copia de seguridad y después programarlo o ejecutarlo. Compruebe que el dispositivo de copia de seguridad está conectado antes de proceder.

Nota – Los puntos de control deben estar habilitados para realizar copias de seguridad NDMP (Network Data Management Protocol) de los volúmenes. Consulte "Creación de puntos de control de archivo" en la página 165.

▼ Para configurar NDMP

1. **En el menú Extensions (Extensiones) seleccione NDMP Setup (Configuración de NDMP).**
2. **Seleccione el puerto de la tarjeta de interfaz de red (NIC) que se debe utilizar para transferir los datos a la unidad de cinta para la copia de seguridad.**

   Todos los puertos disponibles se muestran debajo de este campo.
3. **Seleccione una ruta de volumen de reserva, por ejemplo `/vol_ndmp`, con al menos 2 GB de espacio para guardar los archivos de datos y de registro NDMP.**

   Debe utilizar un volumen de archivo separado que no sea ninguno de los volúmenes programados de la copia de seguridad.
4. **Guarde los cambios.**

Configuración de Compliance Archiving Software

Si ha adquirido, activado y habilitado la opción Compliance Archiving Software (consulte "Para activar una opción" en la página 120), existen configuraciones adicionales que puede establecer desde la interfaz de línea de comandos.

Nota – Las configuraciones del sistema de puerta de enlace Sun StorEdge 5310 admiten la compatibilidad de aplicación recomendada, pero no la de aplicación obligatoria.

Precaución – Utilice los comandos con cuidado para evitar resultados no deseados.

▼ Para cambiar el periodo de retención predeterminado

1. **Siga las instrucciones para "Para acceder a la interfaz de línea de comandos" en la página 196.**
2. **En la línea de comandos, escriba `fsctl compliance` *volumen* `drt` *tiempo***

   donde *volumen* es el nombre del volumen para el que desea definir el tiempo de retención predeterminado y *tiempo* es la duración del tiempo de retención en segundos.

   Para definir la retención predeterminada en "permanent" (permanente), debería utilizar el valor máximo permitido, `2147483647`.

Habilitación de compatibilidad CIFS

En su configuración inicial, Compliance Archiving Software sólo admitirá las solicitudes de retención de datos procedentes de clientes NFS. El acceso de CIFS a esta función se puede habilitar desde la interfaz de línea de comandos.

Precaución – Utilice los comandos con cuidado para evitar resultados no deseados.

▼ Para permitir que los clientes de Windows utilicen la función de almacenamiento compatible

1. **Siga las instrucciones para "Para acceder a la interfaz de línea de comandos" en la página 196.**
2. **En la línea de comandos, escriba:**

   ```
   fsctl compliance wte on
   ```

Configuración de la auditoría del sistema

La auditoría del sistema es un servicio que permite auditar los eventos de sistema que desee almacenando las entradas de estos eventos en archivos de registro. Para obtener más información sobre la auditoría del sistema, consulte "Auditoría del sistema" en la página 145.

▼ Para configurar la auditoría del sistema

1. **En el menú Extensions (Extensiones) seleccione System Audit Configuration (Configuración de auditoría del sistema).**
2. **Seleccione 1. Edit fields (Editar campos).**
3. **Habilite la auditoría y especifique la ruta para el registro de auditoría y el tamaño máximo del archivo de registro.**
4. **Seleccione 7. Save changes (Guardar cambios).**

APÉNDICE **B**

Mensajes de error del dispositivo Sun StorEdge 5310 NAS

En este apéndice se detallan los mensajes de error específicos que se envían por correo electrónico, mediante notificación SNMP, la pantalla LCD o el registro de sistema al administrador en caso de que se produzca un error de sistema. *SysMon*, el subproceso de supervisión de dispositivo Sun StorEdge 5310 NAS, supervisa el estado de los dispositivos RAID, UPS, así como de los sistemas de archivos, las unidades, los subsistemas de cierre y las variables del entorno. Los mensajes de error y de supervisión varían en función del modelo y de la configuración.

En las tablas de este apéndice, las columnas que no tienen entradas se han eliminado.

Acerca de la notificación de error `SysMon`

`SysMon`, el subproceso de supervisión del dispositivo Sun StorEdge 5310 NAS, captura eventos generados como resultado de los errores del subsistema. A continuación, ejecuta la acción pertinente: enviar un mensaje de correo electrónico, informar al servidor SNMP, mostrar el error en la pantalla LCD, escribir un mensaje de error en el registro de sistema o una combinación de todas estas acciones. Las notificaciones por correo electrónico y el registro de sistema incluyen la hora del evento.

Mensajes de error del dispositivo Sun StorEdge 5310 NAS

Los siguientes apartados muestran mensajes de error de los dispositivos UPS y RAID, del uso del sistema de archivos y de los sistemas IPMI del dispositivo Sun StorEdge 5310 NAS.

Errores del subsistema UPS

Consulte la TABLA B-1 para obtener descripciones de las condiciones de error de UPS.

TABLA B-1 Mensajes de error de UPS

Evento	Asunto de correo electrónico: texto	Captura SNMP	Pantalla LCD	Registro
Fallo del suministro eléctrico	**AC Power Failure: (Fallo del suministro eléctrico CA)** AC power failure (Fallo en el suministro eléctrico CA). System is running on UPS battery (El sistema se está ejecutando mediante UPS). Action (Acción): Restore system power (Restablezca el suministro eléctrico). Severity = Error (Gravedad=Error)	EnvUpsOn Battery	U20 on battery (Batería en U20)	UPS: AC power failure (Fallo en el suministro eléctrico CA). System is running on UPS battery (El sistema se está ejecutando mediante UPS).
Power Restored (Suministro eléctrico restaurado)	**AC power restored: (Suministro eléctrico de CA restaurado)** AC power restored (Suministro eléctrico de CA restaurado). System is running on AC power (El sistema se está ejecutando mediante suministro eléctrico de CA). Severity = Notice (Gravedad=Aviso)	EnvUpsOff Battery	U21 power restored (Suministro eléctrico restaurado U21)	UPS: AC power restored (Suministro eléctrico de CA restaurado).
Low Battery (Batería baja)	**UPS battery low (Batería UPS baja):** UPS battery is low (La batería UPS está baja). The system will shut down if AC power is not restored soon (El sistema se cerrará si el suministro eléctrico CA no se restaura pronto). Action (Acción): Restore AC power as soon as possible (Restaure lo antes posible el suministro eléctrico de CA). Severity = Critical (Gravedad=Crítica)	EnvUpsLow Battery	U22 low battery (Batería baja U22)	UPS: Low battery condition (Condición de batería baja).

TABLA B-1 Mensajes de error de UPS *(continuación)*

Evento	Asunto de correo electrónico: texto	Captura SNMP	Pantalla LCD	Registro
Normal Battery (Batería normal)	**UPS battery recharged: (Batería UPS recargada)** The UPS battery has been recharged (La batería UPS se ha recargado). Severity = Notice (Gravedad=Aviso)	EnvUps Normal Battery	U22 battery normal (Batería normal U22)	UPS: Battery recharged to normal condition (Batería recargada a su estado normal).
Replace Battery (Sustituir batería)	**Replace UPS Battery: (Sustituir la batería UPS)** The UPS battery is faulty (La batería UPS está defectuosa). Action (Acción): Replace the battery (Sustituya la batería). Severity = Notice (Gravedad=Aviso)	EnvUps Replace Battery	U23 battery fault (Batería U23 defectuosa)	UPS: Battery requires replacement (Es necesario sustituir la batería).
UPS Alarms - Ambient temperature or humidity outside acceptable thresholds (Alarmas UPS: la temperatura ambiente o la humedad exceden los umbrales aceptables)	**UPS abnormal temperature/humidity: (Temperatura/humedad anormal en UPS)** Abnormal temperature/humidity detected in the system (Se ha detectado una temperatura/humedad anormales en el sistema). Action (Acción): 1. Check UPS unit installation, OR (Compruebe la instalación de la unidad UPS, O 2. Contact technical support (Póngase en contacto con el servicio técnico). Severity = Error (Gravedad=Error)	EnvUps Abnormal	U24 abnormal ambient (Ambiente anormal U24)	UPS: Abnormal temperature and/or humidity detected (Se ha detectado una temperatura o humedad anormales).
Write-back cache is disabled (La caché de escritura de respaldo se deshabilitará).	**Controller Cache Disabled: (Caché de controlador deshabilitada)** Either AC power or UPS is not charged completely (El suministro eléctrico de CA o el dispositivo UPS no se han cargado completamente). Action (Acción): 1 - If AC power has failed, restore system power (Si ha fallado el suministro de CA, restáurelo). 2 - If after a long time UPS is not charged completely, check UPS (Si el dispositivo UPS no se ha cargado completamente después de bastante tiempo, compruébelo). Severity = Warning (Gravedad= Advertencia)		Cache Disabled (Caché deshabilitada)	write-back cache for ctrl *x* disabled (Caché de escritura de respaldo para controlador X deshabilitada)

TABLA B-1 Mensajes de error de UPS *(continuación)*

Evento	Asunto de correo electrónico: texto	Captura SNMP	Pantalla LCD	Registro
Write-back cache is enabled (Caché de escritura de respaldo habilitada).	**Controller Cache Enabled: (Caché de controlador habilitada)** System AC power and UPS are reliable again (El suministro eléctrico de CA y el dispositivo UPS son fiables de nuevo). Write-back cache is enabled (Caché de escritura de respaldo habilitada). Severity = Notice (Gravedad=Aviso)		Cache Enabled (Caché habilitada)	write-back cache for ctlr *n* enabled (Caché de escritura de respaldo para controlador N habilitada)
The UPS is shutting down (El dispositivo UPS se está apagando).	**UPS shutdown: (Apagado del dispositivo UPS)** The system is being shut down because there is no AC power and the UPS battery is depleted (El sistema se está apagando porque no hay suministro de CA y la batería del dispositivo UPS está agotada). Severity = Critical (Gravedad=Crítica)			!UPS: Shutting down (Apagándose)
UPS Failure (Fallo de UPS)	**UPS failure: (Fallo de UPS)** Communication with the UPS unit has failed (Ha fallado la comunicación con la unidad UPS). Action (Acción): 1. Check the serial cable connecting the UPS unit to one of the CPU enclosures, OR (Compruebe el cable serie que conecta la unidad UPS a uno de los dispositivos de cierre de la CPU, O) 2. Check the UPS unit and replace if necessary (Compruebe la unidad UPS y sustitúyala si es necesario). Severity = Critical (Gravedad=Crítica)	EnvUpsFail	U25 UPS failure (Fallo UPS U25)	UPS: Communication failure (Fallo de comunicación).

Errores del sistema de archivos

Los mensajes de error del sistema de archivos se producen cuando el uso del sistema de archivos supera un umbral definido. El umbral de uso predeterminado es el 95 %.

TABLA B-2 Errores del sistema de archivos

Evento	Asunto de correo electrónico: texto	Captura SNMP	Pantalla LCD	Registro
File System Full (Sistema de archivos lleno)	File system full: (Sistema de archivos lleno) File system <name> is *xx*% full: (El sistema de archivos está lleno al xx%) Action (Acción): 1. Delete any unused or temporary files, OR (Elimine los archivos temporales o los que no sirvan, O) 2. Extend the partition by using an unused partition, OR (Amplíe las particiones usando una partición que no esté en uso, O) 3. Add additional disk drives and extend the partition after creating a new partition (Agregue unidades de disco adicionales y amplíe la partición después de crear una nueva). Severity=Error (Gravedad=Error)	PartitionFull	F40 FileSystemName full (NombreSistema Archivos lleno F40)	File system <name> usage capacity is *xx*% (El sistema de archivos X está lleno al xx%).

Errores del subsistema RAID

La TABLA B-3 muestra eventos y mensajes de error sobre el dispositivo Sun StorEdge 5310 NAS.

TABLA B-3 Mensajes de error de RAID

Evento	Asunto de correo electrónico: texto	Captura SNMP	Pantalla LCD	Registro
LUN Failure (Fallo de LUN)	RAID LUN failure: (Fallo de LUN RAID) RAID LUN *N* failed and was taken offline (El LUN RAID ha fallado y no está conectado). Slot *n* is offline (La ranura N no está conectada). Action (Acción): Replace bad drives and restore data from backup (Sustituya las unidades dañadas y restaure los datos desde la copia de seguridad). Severity = Error (Gravedad=Error)	RaidLunFail	R10 Lun failure (Fallo de LUN R10)	RAID LUN *N* failed and was taken offline (El LUN RAID ha fallado y no está conectado). Slot *n* is offline (La ranura N no está conectada). Severity=Error (Gravedad=Error)
Disk Failure (Fallo en el disco)	Disk drive failure: (Fallo en la unidad de disco) Disk drive failure (Fallo en la unidad de disco). Failed drives are (Las unidades que han fallado son): Slot no., Vendor, Product ID, Size (Nº de ranura, proveedor, ID de producto, tamaño) Severity = Error (Gravedad=Error)	RaidDiskFail	R11 Drive failure (Fallo de unidad R11)	Disk drive failure (Fallo en la unidad de disco). Failed drives are: (Las unidades que han fallado son) Slot#, Vendor, Product ID, Size (N.º de ranura, proveedor, ID de producto, tamaño) Severity=Error (Gravedad=Error)
Controller Failure (Fallo de controlador)	RAID controller failure: (Fallo de controlador) RAID controller *N* has failed (El controlador N RAID ha fallado). Action (Acción): Contact technical support (Póngase en contacto con el servicio técnico). Severity = Error (Gravedad=Error)	Raid Controller Fail	R12 Ctlr failure (Fallo de controlador R11)	RAID controller *N* failed (El controlador N RAID ha fallado).

Eventos IPMI

El dispositivo Sun StorEdge 5310 NAS utiliza placas IPMI para supervisar el entorno de los sistemas y enviar mensajes relacionados con anomalías en el suministro de energía o en la temperatura.

Nota – La ubicación de los dispositivos se muestra en el Apéndice D.

La TABLA B-4 muestra mensajes de error de IPMI para el dispositivo Sun StorEdge 5310 NAS.

TABLA B-4 Mensajes de error de IPMI

Evento	Asunto de correo electrónico: texto	Captura SNMP	Pantalla LCD	Registro
Fan Error (Error del ventilador)	Fan Failure: (Error del ventilador) Blower fan *xx* has failed (El ventilador xx ha fallado). Fan speed = xx RPM (Velocidad del ventilador= xx RPM). Action (Acción): The fan must be replaced as soon as possible (Debe sustituir el ventilador lo antes posible). If the temperature begins to rise, the situation could become critical (Si la temperatura comienza a subir, la situación puede volverse crítica). Severity = Error (Gravedad=Error)	envFanFail trap	P11 Fan *xx* failed (El ventilador xx ha fallado P11)	Blower fan *xx* has failed! (El ventilador ha fallado)
Power Supply Module Failure (Fallo del módulo de suministro eléctrico)	Power supply failure: (Fallo del suministro eléctrico) The power supply unit xx has failed (Ha fallado el suministro eléctrico de la unidad xx). Action (Acción): The power supply unit must be replaced as soon as possible (Debe restaurar el suministro eléctrico lo antes posible). Severity = Error (Gravedad=Error)	envPowerFail trap	P12 Power *xx* failed (Ha fallado el suministro xx P12)	Power supply unit *xx* has failed (Ha fallado el suministro eléctrico de la unidad xx).
Power Supply Module Temperature (Temperatura del módulo de suministro eléctrico)	Power supply temperature critical: (La temperatura del suministro eléctrico es crítica) The power supply unit *xx* is overheating (La unidad de suministro eléctrico xx tiene sobrecalentamiento). Action (Acción): Replace the power supply to avoid any permanent damage (Sustituya el suministro eléctrico para evitar que se produzcan daños permanentes). Severity = Critical (Gravedad=Crítica)	envPowerTemp Critical trap	P22 Power *xx* overheated (El suministro xx tiene sobrecalenta miento P22)	Power supply unit *xx* is overheating (La unidad de suministro eléctrico xx tiene sobrecalenta miento).

TABLA B-4 Mensajes de error de IPMI *(continuación)*

Evento	Asunto de correo electrónico: texto	Captura SNMP	Pantalla LCD	Registro
Temperature Error (Error de temperatura)	Temperature critical: (La temperatura es crítica) Temperature in the system is critical (La temperatura del sistema es crítica). It is xxx Degrees Celsius (Es de xxx grados Celsius). Action (Acción): 1. Check for any fan failures, OR (Verifique si hay algún fallo en el ventilador, O) 2. Check for blockage of the ventilation, OR (Compruebe si hay algún bloqueo en la ventilación, O) 3. Move the system to a cooler place (Desplace el sistema a un sitio más frío). Severity = Error (Gravedad=Error)	envTemperatue Error trap	P51 Temp error (Error de temperatura P51)	The temperature is critical (La temperatura es crítica).
Primary Power Cord Failure (Fallo en el cable de alimentación principal)	Power cord failure: (Fallo en el cable de alimentación) The primary power cord has failed or been disconnected (El cable de alimentación principal ha fallado o está desconectado). Action (Acción): 1. Check the power cord connections at both ends, OR (Compruebe las conexiones de los extremos del cable de alimentación, O) 2. Replace the power cord (Sustituya el cable de alimentación). Severity = Error (Gravedad=Error)	envPrimary PowerFail trap	P31 Fail PWR cord 1 (Fallo del cable de alimentación 1 P31)	The primary power cord has failed (El cable de alimentación principal ha fallado).
Secondary Power Cord Failure (Fallo en el cable de alimentación secundario)	Power cord failure: (Fallo en el cable de alimentación) The secondary power cord has failed or been disconnected (El cable de alimentación secundario ha fallado o está desconectado). Action (Acción): 1. Check the power cord connections at both ends, OR (Compruebe las conexiones de los extremos del cable de alimentación, O) 2. Replace the power cord (Sustituya el cable de alimentación). Severity = Error (Gravedad=Error)	envSecondary PowerFail trap	P32 Fail PWR cord 2 (Fallo del cable de alimentación 2 P32)	The secondary power cord has failed (El cable de alimentación secundario ha fallado).

APÉNDICE **C**

API de Compliance Archiving Software

El dispositivo Sun StorEdge 5310 NAS admite el almacenamiento de datos de normativas como una extensión de software habilitada con clave de licencia que se denomina Compliance Archiving Software.

El software Compliance Archiving se encuentra disponible con restricciones (de "aplicación obligatoria") y sin algunas restricciones (de "aplicación recomendada"). Para obtener información acerca de Compliance Archiving Software, consulte "Compliance Archiving Software" en la página 133.

Este apéndice es una descripción técnica de las funciones y la interfaz de programación de Compliance Archiving Software con aplicación obligatoria.

Nota – Compliance Archiving Software requiere la correcta configuración del hardware del sistema del dispositivo Sun StorEdge 5310 NAS para su funcionamiento correcto. En concreto, las matrices del controlador Sun StorEdge 5300 RAID EU no deberían conectarse a ningún dispositivo o red distinto a una conexión de canal de fibra privada a la unidad NAS o cualquier armario de expansión Sun StorEdge 5300 EU.

Nota – Para asegurar la máxima aplicación de las directivas de retención de datos, también deberá tener en cuenta la seguridad física del dispositivo Sun StorEdge 5310 NAS. La retención de datos controlada por software no puede ser más sólida que las medidas preventivas físicas utilizadas para controlar el acceso al hardware del sistema.

Características de cumplimiento de normativas

Compliance Archiving Software proporciona garantías en el ámbito del almacenamiento relativas a la precisión, integridad y retención de los archivos. Esta función consta de las siguientes tres características principales:

- Archivos WORM (Escribir una vez, leer muchas)
- Periodos de retención por archivo
- Bloqueo administrativo

Archivos WORM

Los archivos WORM permiten un mayor control de acceso que las semánticas de acceso a archivos tradicionales que proporcionan los protocolos NFS y CIFS. Cuando una aplicación designa un archivo como WORM, el archivo no podrá modificarse. Los archivos WORM no se pueden modificar, ampliar ni cambiarles el nombre, independientemente de la identidad o privilegios del cliente o usuario que intente la operación. Además, los archivos WORM sólo se pueden eliminar de acuerdo con las normas de retención de archivos que se describen a continuación.

Nota – Aunque estos archivos se llaman "WORM", para mantener la nomenclatura habitual de almacenamiento que no se puede escribir ni borrar, sería más adecuado llamarlos "sólo lectura permanente". El dispositivo Sun StorEdge 5310 NAS no restringe la forma en que un archivo está escrito o el número de veces que se pueden modificar los contenidos antes de que el archivo se convierta en un archivo WORM.

Periodos de retención por archivo

Compliance Archiving Software asocia un periodo de retención para cada archivo WORM. Un archivo WORM no se puede eliminar hasta que se haya agotado su periodo de retención. Los periodos de retención se pueden ampliar, pero no reducir. Se puede asignar un nuevo periodo de retención a un archivo para el que haya terminado su periodo de retención anterior.

Bloqueo administrativo

Para asegurar las garantías de retención y preservación de los archivos WORM y los periodos de retención, algunas funciones de administración del sistema, como la eliminación o edición de volúmenes de archivos, están desactivadas o restringidas en volúmenes de sistemas con el cumplimiento habilitado. Estas restricciones afectan a las funciones de administración del sistema que podrían utilizarse para sortear la retención de un archivo (por ejemplo, eliminando el volumen del archivo).

Acceso a la función de compatibilidad

Para mantener la compatibilidad con los sistemas operativos y aplicaciones existentes, las funciones de Compliance Archiving Software se implementan como ampliaciones de los protocolos de acceso a los archivos existentes compatibles con el dispositivo Sun StorEdge 5310 NAS (NFS y CIFS). En concreto, el dispositivo Sun StorEdge 5310 NAS sobrecarga los atributos de archivo existentes para indicar el estado WORM de un archivo y al final de su periodo de retención. Esto simplifica la asignación de puertos de las aplicaciones de gestión de registro y documentos existentes, ya que estos campos de metadatos se pueden definir y ver utilizando API y utilidades de clientes estándar.

Volúmenes compatibles

Los volúmenes se deben diseñar con la compatibilidad habilitada en el momento en que se crean; los volúmenes existentes no se pueden convertir en volúmenes compatibles. Es posible tener varios volúmenes en un único dispositivo Sun StorEdge 5310 NAS con sólo algunos con la compatibilidad habilitada.

No debería habilitar el archivo compatible en los volúmenes que utilizarán las aplicaciones (y usuarios) que no estén al tanto de las distintas semánticas de retención de datos impuestas por Compliance Archiving Software.

Archivos WORM

Los archivos WORM no se pueden modificar o actualizar. Una vez que un archivo se convierte en WORM, será de sólo lectura hasta que se elimine.

Creación de archivos WORM

Compliance Archiving Software utiliza un desencadenante WORM para convertir un archivo normal en WORM. Cuando una aplicación cliente o un usuario ejecuta la acción desencadenante en un archivo, el Compliance Archiving Software interpreta que esto significa que el archivo de destino debería convertirse en WORM.

El desencadenante WORM para los clientes UNIX define el modo de permiso del archivo en 4000. Las aplicaciones cliente o los usuarios pueden invocar este desencadenante WORM con el comando chmod o una llamada del sistema.
Al recibir esta solicitud, Compliance Archiving Software convierte el archivo de destino en un archivo WORM de la siguiente manera:

- Definiendo el bit setuid
- Eliminando los bits de escritura definidos para el archivo
- Manteniendo los bits de acceso de lectura para el archivo

Nota – Los archivos ejecutables no pueden convertirse en archivos WORM. Para los archivos creados a partir de clientes de Windows, esto significa que un archivo no se puede convertir a WORM si su lista de control de acceso (ACL) tiene alguna entrada de control de acceso (ACE) que conceda permiso de ejecución para el archivo.

En el siguiente ejemplo, un archivo con un modo de acceso 640 se convierte a WORM. Después de emitir el desencadenante WORM, el modo de acceso al archivo es 4440.

```
$ ls -l testfile
-rw-r-----   1 smith    staff      12139 Dec  2 13:18 testfile
$ chmod 4000 testfile
$ ls -l testfile
-r-Sr-----   1 smith    staff      12139 Dec  2 13:18 testfile
```

Compliance Archiving Software utiliza este desencadenante WORM porque es una operación que probablemente las aplicaciones existentes no utilizarán.

El desencadenante WORM para los clientes de Windows define el bit del sistema y de sólo lectura en el archivo. El desencadenante WORM define el bit de sólo lectura del archivo, pero no cambia su bit de sistema.

Una vez que un archivo se convierte en WORM, no se puede modificar. Desde los clientes de Windows, el bit de sólo lectura no se puede eliminar y el bit de sistema no se puede cambiar. Desde clientes de UNIX, el bit setuid no se puede eliminar, ni se pueden agregar permisos de ejecución o escritura al modo de acceso del archivo.

Los volúmenes con compatibilidad habilitada traducen esta configuración WORM entre CIFS y NFS. Por ejemplo, si un cliente UNIX visualiza un archivo WORM creado por un cliente de Windows, verá un modo de acceso WORM como se ha descrito anteriormente.

Comportamiento de los archivos WORM

Los archivos WORM no se pueden modificar, sobrescribir o ampliar. Cualquier intento de escribir en un archivo WORM producirá un fallo y devolverá un error con independencia de la identidad del usuario del cliente y los privilegios de acceso.

Ni el propietario de un archivo WORM o un usuario con privilegios administrativos (incluso privilegios de superusuario) puede modificar un archivo WORM. No es posible cambiar el nombre a los archivos WORM ni tampoco volver a convertirlos a archivos normales (no WORM).

Metadatos de los archivos WORM

Compliance Archiving Software no permite modificar los metadatos que contengan, protejan, describan o nombren los datos del cliente. Sólo se permite modificar un subconjunto restringido de campos de metadatos, en función del sistema operativo, como se muestra en la TABLA C-1.

TABLA C-1 Metadatos del archivo WORM que se pueden o no se pueden modificar

Sistema operativo	Puede	No puede
UNIX	• Definir o eliminar los bits de permiso de lectura • Cambiar el propietario del archivo y del grupo	• Habilitar los bits de escritura y ejecución • Borrar el bit setuid • Modificar el tamaño o la hora de modificación (mtime)
Windows	• Definir o eliminar los bits de permiso de lectura • Cambiar el bit de archivo • Crear y modificar las listas de control de acceso (aunque un archivo WORM no se puede modificar independientemente de la configuración de ACL)	• Cambiar los bits de oculto, sistema y sólo lectura • Modificar el tamaño o la hora de modificación (mtime)

Restricciones de espacio de nombre

Compliance Archiving Software no permite cambiar el nombre a los archivos WORM. Además, no se puede cambiar el nombre a los directorios que no estén vacíos. Esta norma garantiza que el nombre completo de la ruta de un archivo WORM no se puede cambiar durante la vida del archivo.

Advertencias

Cuando un cliente UNIX define el modo de archivo en 4000 (invocando el desencadenante WORM), el modo de acceso resultante para el archivo no será 4000. Esto viola la semántica de norma del comando `chmod` y la llamada del sistema. Como resultado, la versión GNU del comando `chmod(1)` (utilizado en muchas versiones de Linux) genera un mensaje de advertencia cuando se utiliza para emitir el desencadenante WORM. Puede ignorar este mensaje.

Periodos de retención de archivos

Todos los archivos WORM tienen un periodo de retención en el que no se pueden eliminar. El periodo de retención se especifica utilizando una marca de tiempo que indica cuándo debería terminar. Este tiempo de retención se puede definir explícitamente por las aplicaciones cliente o los usuarios. Si el cliente no especifica un periodo de retención, Compliance Archiving Software utiliza el *periodo de retención predeterminado* especificado para el volumen cuando se crea dicho volumen. Cualquier intento de eliminar un archivo WORM antes del fin de este periodo de retención producirá un error; sin embargo, puede eliminar un archivo en cualquier momento después de que el periodo de retención haya finalizado.

Nota – Los periodos de retención sólo controlan la capacidad para eliminar archivos. Un archivo WORM no se puede modificar, independientemente de si ha finalizado el periodo de retención.

Configuración de marcas de tiempo de retención

Las marcas de tiempo de retención del sistema de archivo de cumplimiento se guardan en el atributo de tiempo de acceso (atime) de los archivos WORM. Normalmente, los clientes definen el atributo atime antes de cambiar un archivo a sólo lectura. Cuando un archivo se transforma en WORM, su valor de atime se redondea a la baja al número de segundos más cercano para determinar la marca de tiempo de retención.

Si el atributo atime representa un momento en el pasado, el periodo de tiempo predeterminado del sistema de archivos se utiliza para calcular la marca de tiempo de retención añadiendo el periodo de tiempo de retención al tiempo actual.

Retención permanente

Las aplicaciones cliente o los usuarios pueden especificar que un archivo debe retenerse permanentemente. Esta permanencia se obtiene definiendo el atributo atime de un archivo en el valor legal máximo para un entero de 32 bits con signo. Este valor (0x7fffffff) es igual a 2.147.483.647. En los sistemas UNIX se define como `INT_MAX` en el archivo de encabezado limits.h y se traduce en una marca de tiempo de 03:14:07 GMT, 19 enero, 2038.

Cambio de periodos de retención

Los periodos de retención se pueden ampliar y se pueden definir nuevos periodos de retención para los archivos cuya retención ha terminado. Esto se consigue restableciendo el atributo atime en un archivo WORM. Dichos cambios se permiten siempre que el nuevo valor represente un momento posterior a la hora de tiempo de retención anterior.

Tiempo de acceso ignorado

Debido a que Compliance Archiving Software utiliza el atributo de tiempo de acceso (atime) para guardar las marcas de tiempo de retención, este atributo no se actualiza como un efecto secundario del funcionamiento estándar del sistema de archivos, independientemente de si un archivo es o no un archivo WORM.

Determinación del estado de un archivo

Las aplicaciones cliente y los usuarios pueden determinar el estado de retención de un archivo leyendo los metadatos del archivo con herramientas y API estándar. En clientes UNIX, por ejemplo, los atributos de un archivo se pueden leer mediante la llamada de sistema `stat(2)` o verse utilizando el comando `ls .` (`ls -lu` mostrará los archivos con sus permisos de acceso y marcas de tiempo atime).

Comportamiento de las llamadas de sistema de UNIX

Las aplicaciones cliente de UNIX acceden a Compliance Archiving Software mediante su interfaz de llamada de sistemas locales. Estas llamadas invocan la implementación NFS del cliente, que traducen las llamadas de sistema en solicitudes de protocolo NFS estándar. Debido a que los sistemas de archivos con el cumplimiento habilitado se comportan de manera distinta que los sistemas de archivos estándar NAS, existen diferencias entre el comportamiento de las llamadas de sistema de clientes.

Esta sección describe las llamadas de sistema estándar de UNIX que se comportan de forma distinta cuando un cliente las ejecuta en un dispositivo Sun StorEdge 5310 NAS compartido con compatibilidad habilitada. Las llamadas de sistema que no se indiquen en esta sección se comportan de manera normal.

Es importante recordar que las interfaces del dispositivo Sun StorEdge 5310 NAS son protocolos de acceso a archivos NFS y CIFS. Por tanto, esta sección incorpora el comportamiento relacionado con el cumplimiento del dispositivo Sun StorEdge 5310 NAS de acuerdo con las solicitudes estándar de protocolo y la asignación desde las llamadas de sistema a solicitudes NFS. El comportamiento de estas llamadas se ha verificado en clientes del sistema operativo Solaris y debería ser el mismo en otros clientes UNIX.

access(2)

Cualquier comprobación de permiso de escritura en un archivo WORM (es decir, una llamada a `access(2)` donde el argumento `amode` incluye el bit `W_OK`) produce un error (`EPERM`).

chmod(2), fchmod(2)

Si el archivo de destino es un archivo normal no WORM sin ningún bit de permiso de ejecución definido, y el nuevo permiso de acceso es 4000 (`S_ISUID`), el archivo de destino se convierte en WORM. Cuando esto sucede, el archivo recibe un nuevo modo de acceso que se calcula agregando el bit setuid a cualquier bit de lectura existente en el modo de acceso del archivo. Concretamente, dado un modo de acceso antiguo, oldmode, un nuevo modo de acceso del archivo tras recibir el desencadenante WORM se puede computar como:

```
newmode = S_ISUID | (oldmode & 0444)
```

Los archivos ejecutables no se pueden convertir a WORM. La aplicación del desencadenante WORM (modo 4000) a un archivo con uno o más bits de permiso de ejecución producirá un error (`EACCES`).

Los bits de acceso de lectura se pueden definir o eliminar en los archivos WORM. Cualquier intento para habilitar el permiso de escritura o ejecución en un archivo WORM, para definir el bit setgid (`S_ISGID`) o el bit sticky (`S_ISVTX`), o para eliminar el bit setuid en un archivo WORM dará un error (`EPERM`).

`chown(2), fchown(2)`

Estas llamadas se comportan de la misma manera en archivos WORM que en los archivos normales.

`link(2)`

Los clientes pueden crear nuevos vínculos fuertes a los archivos WORM. Los vínculos fuertes a un archivo WORM no se pueden eliminar hasta que termina el periodo de retención del archivo. (Consulte `unlink(2)`, en la página 268).

`read(2), readv(2)`

Los clientes pueden leer archivos WORM. Dado que las marcas de tiempo de retención se guardan en el atributo atime, este valor no se actualiza para reflejar el acceso de lectura a los archivos WORM.

`rename(2)`

Cualquier intento para cambiar el nombre a un archivo WORM o a un directorio no vacío en un sistema de archivos con cumplimiento habilitado dará un error (`EPERM`).

stat(2), fstat(2)

Cuando se utilizan estas llamadas para obtener información acerca de los archivos normales, la estructura `stat` devuelta contiene valores relacionados con cumplimiento. El campo `st_mode` contiene (como siempre) el modo y permisos del archivo. Un archivo WORM tiene el bit setuid definido y no tiene bits de escritura o ejecución. El campo `st_atime` contiene una marca de tiempo que indica el periodo de retención del archivo. Si este valor es igual a `INT_MAX`, como se define en limits.h, el archivo se mantiene permanentemente.

unlink(2)

Los archivos WORM sólo se pueden desvincular si el tiempo actual, reflejado por el reloj seguro del dispositivo Sun StorEdge 5310 NAS, es posterior a la fecha guardada en el atributo atime del archivo (es decir, la marca de tiempo de retención). Si esta condición no se mantiene, `unlink(2)` produce un error (`EPERM`).

utime(2), utimes(2)

Estas llamadas se utilizan para definir los atributos de tiempo de acceso de un archivo (atime) y de tiempo de modificación (mtime). Cuando se utiliza en un archivo no WORM, se comportan normalmente y proporcionan un mecanismo para especificar la marca de tiempo de retención antes de que un archivo se convierta a WORM.

Cuando se invoca en un archivo WORM, estas llamadas se pueden utilizar para ampliar el periodo de retención de un archivo o para asignar un nuevo periodo de retención a un archivo con la retención caducada. Estas llamadas tienen éxito en un archivo WORM si el nuevo valor de atime es superior (es decir, posterior) al valor de atime existente del archivo. Si el nuevo valor de atime es menor o igual que el valor actual de atime, estas llamadas darán un error (`EPERM`). Cuando se utilizan en un archivo WORM, el argumento mtime se ignora.

write(2), writev(2)

Cualquier intento de escritura en un archivo WORM producirá un error (`EPERM`).

Comportamiento de los clientes de Windows

Creación de archivos WORM

Un archivo normal no WORM sólo se puede convertir a WORM desde Windows cuando se han definido los bits de sólo lectura y del sistema en un archivo. Este desencadenante WORM establecerá el bit de sólo lectura del archivo, pero no cambiará el estado del bit del sistema del archivo.

Una vez que un archivo se convierte en WORM, no se puede modificar. Desde los clientes de Windows, el bit de sólo lectura no se puede eliminar y el bit de sistema no se puede cambiar.

Restricciones de metadatos en archivos WORM

Los clientes de Windows pueden cambiar el bit de archivo en un archivo WORM. No pueden cambiar los bits de sistema, ocultos o de sólo lectura. Los clientes de Windows pueden cambiar las ACL en los archivos WORM, pero se ignorarán los permisos de escritura en la ACL de un archivo WORM. Cualquier intento de modificar los datos en un archivo WORM dará un error independientemente de los permisos en la ACL.

Establecimiento de periodos de retención

Al igual que los clientes de UNIX, los clientes de Windows definen los periodos de retención almacenando las marcas de tiempo de retención en el atributo de tiempo de acceso (atime) de un archivo.

Advertencias para los clientes de Windows

Precauciones con el bit de sólo lectura

Es especialmente importante que los volúmenes de archivo con el cumplimiento habilitado sólo los utilicen las aplicaciones y usuarios de Windows que conozcan el comportamiento especial de los archivos WORM. Numerosas utilidades estándar de Windows para copiar archivos incluirán los bits de sistema y de sólo lectura en un archivo. Si se utilizan estas herramientas para hacer copias de los archivos WORM en un volumen con el cumplimiento habilitado, los archivos resultantes serán WORM debido a que tendrán sus bits de sistema y de sólo lectura definidos.

Software antivirus

Muchos programas de detección de virus intentan preservar el tiempo de acceso en los archivos que examinan. Normalmente, estos programas leen el atributo atime del archivo antes de verificar si tienen virus, y después restablecen atime al valor que tenía antes de la exploración. Esto puede dar lugar a una situación de carrera si el programa de comprobación de virus explora un archivo a la vez que otra aplicación está definiendo un tiempo de ejecución en el archivo. Como resultado, el archivo puede terminar con el tiempo de retención incorrecto.

Una manera sencilla de evitar este problema es asegurarse de que los programas antivirus no se ejecutan en sistemas de archivos con cumplimiento habilitado o que no se ejecutan a la vez que las aplicaciones que crean archivos WORM.

Las aplicaciones personalizadas también pueden evitar este problema utilizando un periodo de retención predeterminado corto y definiendo el verdadero periodo de retención del archivo tras aplicar el desencadenante WORM.

Otras API

Se puede acceder a Compliance Archiving Software mediante muchas otras API de cliente, incluidas Java, Perl y C++. Todos estos idiomas se basan en las mismas llamadas de sistema para acceder a los recursos compartidos montados mediante NFS o CIFS.

APÉNDICE **D**

Componentes del dispositivo Sun StorEdge 5310 NAS

Este apéndice describe algunos de los componentes de hardware del servidor (unidad) de dispositivo Sun StorEdge 5310 NAS y clúster Sun StorEdge 5310, el armario de controladores RAID Sun StorEdge 5300 EU y el armario de expansión Sun StorEdge 5300 EU.

Precaución – Sólo un técnico cualificado tiene autorización para retirar las cubiertas de la unidad y acceder a los componentes internos.

Incluye la siguiente información:

- "Suministros eléctricos del servidor" en la página 271
- "Botones del panel frontal del servidor" en la página 272
- "Panel trasero del servidor" en la página 274
- "Componentes del armario de controladores RAID Sun StorEdge 5300 EU y el armario de expansión Sun StorEdge 5300 EU" en la página 275

Suministros eléctricos del servidor

Un suministro eléctrico de sistema proporciona alimentación eléctrica a todos los componentes. Los sistemas de alimentación eléctrica de las unidades son dispositivos de detección automática con adaptación automática a los voltajes de línea de 100 a 240 voltios, 50 a 60 Hz.

El sistema de suministro eléctrico de un servidor consta de dos módulos redundantes de intercambio en caliente dispuestos en una configuración 1 + 1-. Cada módulo es capaz de mantener una carga de 500 vatios. Para un buen funcionamiento del sistema es preciso contar al menos con una fuente de alimentación, aunque se necesitan dos para llegar al suministro eléctrico redundante.

Una luz roja en la parte trasera del módulo de suministro eléctrico indica que el cable de alimentación está desconectado.

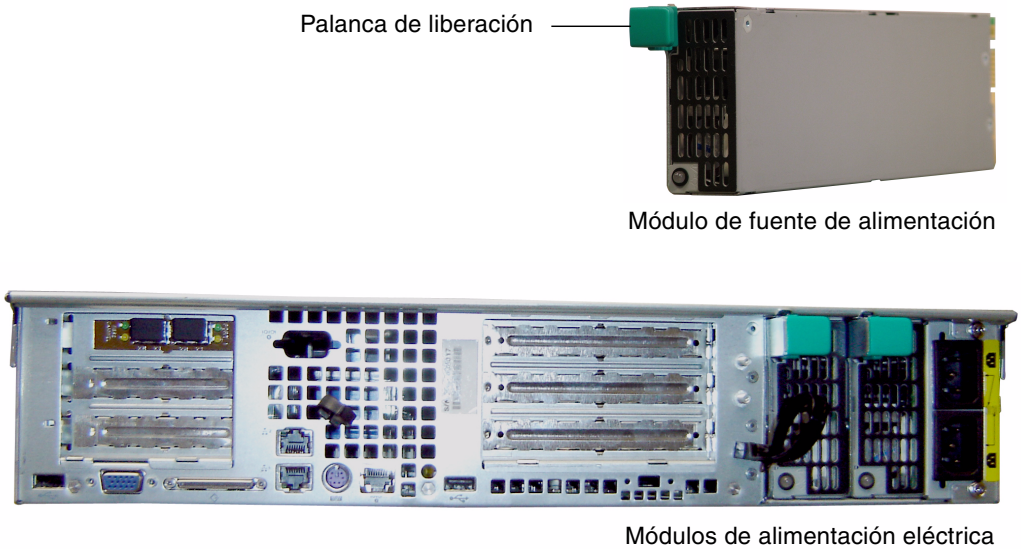


FIGURA D-1 Suministro eléctrico

Las características del suministro eléctrico son:

- Capacidad de 500 W
- Indicadores LED de estado
- Ventiladores de refrigeración internos de varias velocidades
- Función de carga integrada compartida
- Función de protección contra sobrecargas integrada
- Mango integral para inserción/extracción

Botones del panel frontal del servidor

Botón de alimentación eléctrica: el conmutador momentáneo (cumple la normativa APCI) que enciende y apaga el sistema.

Precaución – No utilice el botón de encendido para apagar el sistema. Siga siempre el procedimiento de apagado correcto descrito en "Apagado del servidor" en la página 163. Si se cierra la sesión incorrectamente pueden perderse datos.

Botón de ID del sistema: el botón que enciende la luz azul de la parte delantera y trasera del sistema para localizar las unidades en un rack.

Botón de reinicio: el botón que reinicia el sistema.

Precaución – No utilice este botón para reiniciar el sistema. Siga siempre el procedimiento de apagado que corresponda.

Indicadores LED de estado

Los indicadores LED de estado del panel frontal señalan las actividades de la corriente que se producen en el sistema.

TABLA D-1 Indicadores LED de estado

LED de alimentación eléctrica	Si el LED presenta una luz verde fija indica que el sistema está encendido. La luz amarilla indica que uno de los cables está desconectado. Si no hay ninguna luz encendida, quiere decir que el sistema está apagado.
LED NIC 1 integrado	Cuando el LED es de color verde indica que existe actividad de red por el puerto NIC 1 integrado.
LED NIC 2 integrado	Cuando el LED es de color verde indica que existe actividad de red por el puerto NIC 2 integrado.
LED de estado del disco duro	• No se aplica.
LED de estado del sistema	• Si el LED muestra una luz verde fija, indica que el sistema está funcionando de forma correcta. • Cuando el LED muestra una luz verde destellante indica que el sistema está funcionando en un modo degradado. • Una luz amarilla fija indica que el sistema está en un estado crítico o irrecuperable. • Una luz amarilla destellante indica que el sistema se encuentra en un estado no crítico. • La luz roja indica que uno de los cables está desconectado. • Si no hay ninguna luz encendida, significa que el sistema se ha detenido pero se considera que el LED es verde.
LED de ID del sistema	• Cuando el LED muestra una luz azul fija, significa que el botón de ID está pulsado. • Si no hay ninguna luz encendida, significa que el botón de ID no está pulsado.

Panel trasero del servidor

A continuación, se muestran los distintos puertos y conectores del panel trasero del servidor.

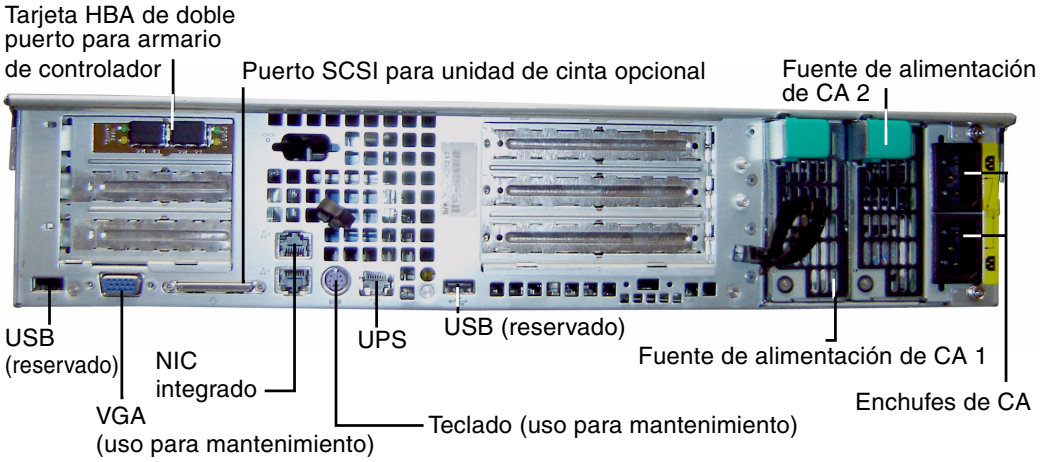


FIGURA D-2 Panel trasero con una tarjeta HBA

Nota – No utilice los puertos VGA de los paneles delantero y trasero. Estos conectores se reservan para el servicio de asistencia técnica de Sun Microsystems.

Nota – El panel trasero del dispositivo Sun StorEdge 5310 NAS que se conecta a dos armarios de controlador tiene dos tarjetas HBA de doble puerto.

Biblioteca de cintas directamente conectada

Se puede conectar una unidad de copia de seguridad de cinta local al puerto SCSI en la zona inferior izquierda de la parte trasera del servidor.

Nota – Asegúrese de que la unidad de cinta figura en la lista de unidades de cinta compatibles. Para obtener la información más reciente sobre los dispositivos de cinta admitidos, póngase en contacto con el representante de ventas de Sun.

La ID de SCSI de la biblioteca de cintas debe ser menor que la de la unidad de cinta. Por ejemplo, configure la ID de la biblioteca como **0** y otorgue a la ID de la unidad un valor no conflictivo, como **5**.

Si desea más información sobre el sistema de unidad de cinta que está utilizando, consulte la documentación que se adjunta con el sistema.

Componentes del armario de controladores RAID Sun StorEdge 5300 EU y el armario de expansión Sun StorEdge 5300 EU

El armario de controladores y los armarios de expansión proporcionan almacenamiento para el dispositivo Sun StorEdge 5310 NAS y el clúster Sun StorEdge 5310.

Los armarios de controladores RAID Sun StorEdge 5300 EU se pueden utilizar con armarios de expansión Fibre Channel (EU F) o armarios de expansión SATA (EU S).

Precaución – Sin embargo, es necesario apagar el sistema para añadir o retirar los armarios de expansión.

El panel delantero del armario de controladores Fibre Channel contiene 14 discos duros intercambiables en caliente organizados como dos grupos RAID 5 de seis unidades, más dos unidades de reserva globales. Cada unidad de 146 gigabytes (capacidad bruta) tiene una capacidad disponible de 133 gigabytes, para una capacidad total disponible de 1,3 terabytes para el armario.

La configuración RAID de unidades FC de 300 GB consiste en un grupo RAID 5 de seis unidades (5+1) y un grupo RAID 5 de siete unidades (6+1), más la unidad de reserva global.

El armario de controlador que se utiliza con un sistema SATA se entrega sin discos duros. En su lugar, todas las unidades SATA están contenidas en armarios de expansión EU S.

Precaución – No mezcle las unidades de disco SATA con las unidades Fibre Channel en un armario de controladores o una matriz.

Nota – En una configuración de doble matriz, una matriz puede contener unidades de disco Fibre Channel (en los armarios de expansión y el armario de controlador) y la otra matriz puede contener las unidades de disco SATA (sólo en los armarios de expansión).

Los armarios de expansión permiten ampliar las capacidades de almacenamiento del sistema. El panel delantero de cada armario de expansión EU F contiene 14 unidades de disco Fibre Channel intercambiables en caliente organizadas como dos grupos RAID 5 de siete unidades. Cada unidad de 146 gigabytes (capacidad bruta) tiene una capacidad disponible de 133 gigabytes, para una capacidad total disponible de 1,6 terabytes por armario de expansión EU F.

El panel delantero del primer armario de expansión EU S contiene 14 unidades SATA intercambiables en caliente organizadas como dos grupos RAID 5 de seis unidades, más dos unidades de reserva globales. Cada unidad de 400 gigabytes (capacidad bruta) tiene una capacidad disponible de 360 gigabytes, para una capacidad total disponible de 3,6 terabytes para el primer armario de expansión EU S.

Los siguientes armarios de expansión EU S contienen 14 discos duros SATA intercambiables en caliente organizados como dos grupos RAID 5 de siete unidades, que proporcionan prácticamente 4,4 terabytes de capacidad disponible adicional.

Precaución – No mezcle unidades de disco Fibre Channel y SATA en un armario de expansión.

Unidades de expansión FC y SATA mixtas

También se ha incorporado compatibilidad con las configuraciones de unidades SATA (Mixed Serial Advanced Technology Attachment) y unidades de expansión Fibre Channel, si se cumplen las siguientes condiciones.

- Todas las unidades de expansión deben consistir en unidades Fibre Channel o unidades SATA. No es posible combinar distintos tipos de unidades en la unidad de expansión.
- La unidad de expansión RAID puede contener unidades Fibre Channel, aunque otras unidades de expansión contengan unidades SATA. La unidad de expansión RAID no puede contener unidades SATA.
- Es necesario tener disponible una unidad de reserva, tanto para unidades SATA como Fibre Channel, con la misma capacidad que la matriz.
- Los LUN no pueden incluir a la vez unidades SATA y Fibre Channel.

Carcasas de disco

Precaución – Sólo las unidades Fibre Channel suministradas por Sun Microsystems funcionarán con el dispositivo Sun StorEdge 5310 NAS y el clúster Sun StorEdge 5310. Para solicitar información de asistencia técnica, póngase en contacto con el representante de ventas de Sun.

Cada disco está incrustado en su carcasa de disco. Estas carcasas se pueden sustituir de forma individual sin necesidad de apagar el armario de expansión, el armario de controladores, el dispositivo Sun StorEdge 5310 NAS o el clúster.

Precaución – No mezcle las unidades de disco Fibre Channel y SATA en un armario de expansión, un armario de controlador o una matriz.

Precaución – Recuerde que sólo puede cambiar una carcasa cada vez. Confirme que el subsistema RAID ha completado las reconstrucciones necesarias antes de extraer otra carcasa.

Precaución – No actualice el software del sistema o el firmware de RAID cuando el subsistema RAID se encuentre en un estado crítico, cuando esté creando un nuevo conjunto de RAID o esté reconstruyendo un conjunto de RAID existente.

▼ Para localizar una unidad o un armario

1. **En el panel de navegación de Web Administrator, seleccione RAID > Manage RAID (Gestionar RAID).**
2. **Haga clic en el botón Locate Drive (Localizar unidad) o Locate Drive Tray (Localizar bandeja de unidades), lo que causará que destelle el indicador del LCD de ese armario o esa unidad.**

FIGURA D-3 Carcasa de la unidad de canal de fibra

▼ Para identificar una unidad que requiere sustituirse

Si ocurre un fallo en unidades de disco, utilice la entrada del registro para identificar el disco defectuoso. (Las ubicaciones de los discos tienen la misma interpretación en el registro de sistema y los informes de diagnóstico.) A continuación se muestra un ejemplo de entrada del registro:

```
Controller 0  enclosure 0  row 0  column 6
```

Antes de interpretar las entradas del registro, tenga en cuenta lo siguiente:

- Ignore todos los números de canal y de destino.
- La numeración de los controladores comienza en 0. Por ejemplo, los controladores en la primera matriz son 0 (ranura A) y 1 (ranura B), y en la segunda matriz son 2 y 3.
- La numeración de los armarios comienza en 0 y está relacionada con la matriz a la que pertenecen. Por ejemplo, si la primera matriz tiene 2 armarios, se identificarán como armario 0 y 1.
- La numeración de filas siempre es 0 para el clúster Sun StorEdge 5310.
- La numeración de las columnas comienza en 0 y especifica el número de ranura del armario.

Así, puede interpretar que el ejemplo indica la ranura 7 del primer armario de la primera matriz.

Nota – No hay una forma estándar de identificar cuál es la primera matriz y cuál es la segunda. Normalmente, el primer puerto HBA está conectado a la primera matriz, el segundo está conectado a la segunda, y así sucesivamente.

Suministros eléctricos

El armario de controlador y los armarios de expansión utilizan los mismos módulos de fuente de alimentación.

Módulo de fuente de alimentación

Armario de controlador

Módulo de fuente de alimentación Módulo de fuente de alimentación

Armario de expansión

Módulo de fuente de alimentación Módulo de fuente de alimentación

FIGURA D-4 Módulos de fuente de alimentación

APÉNDICE **E**

Envío de un correo electrónico de diagnóstico

La función de correo electrónico de diagnóstico le permite enviar mensajes de correo electrónico al servicio técnico de Sun Microsystems o a cualquier otro destinatario que corresponda. Estos mensajes de correo electrónico incluyen información acerca de diversos aspectos del dispositivo Sun StorEdge 5310 NAS, como la configuración del sistema, el subsistema de disco, el sistema de archivos, la configuración de red, los recursos compartidos SMB, los procesos de copias de seguridad y de restablecimiento, la información del directorio `/etc`, el registro del sistema, los datos de entorno y la información sobre el administrador.

Todos los mensajes de diagnóstico que se envíen incluirán esta información, con independencia de la naturaleza del problema.

En una configuración de clúster, es necesario definir el correo electrónico de diagnóstico en cada servidor del clúster.

Para configurar el correo electrónico de diagnóstico:

1. **En la barra de herramientas de la parte superior de la pantalla, seleccione el botón**  **.**

   Se muestra el cuadro de diálogo Diagnostic Email (Correo electrónico de diagnóstico).

2. **En el campo Problem Description (Descripción del problema), describa en qué consiste el problema.**

   Se trata de un campo obligatorio y está limitado a 256 caracteres.

3. **Compruebe que la casilla de verificación Diagnostics (Diagnósticos) está activada para al menos un destinatario de correo.**

   Si necesita agregar o realizar modificaciones en los destinatarios, consulte las instrucciones en "Configuración de la notificación por correo electrónico" en la página 30.

4. **Haga clic en Send (Enviar) para proceder con el envío del mensaje.**

Índice alfabético

A

acceso
  puntos de control 169
activación, opciones 119
actualización
  contenedores de recursos compartidos de ADS 82
  software 173
adaptadores, red
  configuración 19
  configuración telnet 199
adición
  consulte Puertos enlazados
  cuotas de árbol de directorios 113
  cuotas de grupo 111
  cuotas de usuario 111
  exportaciones NFS 116
  hosts 89
    telnet 223
  hosts de confianza
    GUI 90
    telnet 224
  LUN 40
  miembros del grupo
    GUI 88
    telnet 219
  puntos de control
    GUI 165
    telnet 247
  RAID 40
  recursos compartidos estáticos
    GUI 103
    telnet 216
  segmento
    telnet 212
  volumen de archivo
    telnet 211
adjuntar segmentos
  telnet 212
administradores
  grupo 86
ADS
  acerca de 77, 78
  actualización de contenedores de recursos compartidos 82
  configuración 22
    clientes de Windows 2000 108
    GUI 79
    telnet 217
  definición 7
  eliminación de recursos compartidos 83
  habilitación 79
  nombres de contenedor 80
  publicación de recursos compartidos 81
agrupamiento
  consulte Puertos enlazados
alerta
  eventos, registro de sistema 144
  umbrales de la memoria búfer de duplicación 127
alias de IP
  acerca de 70
  sistema con dos servidores 71
alta disponibilidad, recuperación tras error 15
  enlace, habilitar 16

apagado 163
  telnet 242
apagado del servidor 163
  telnet 242
archivos en cuarentena
  borrado 68
archivos MIB 140
armario de expansión
  carcasa de disco 276
asignación
  credenciales 91
  funciones de los puertos 20
  idioma 32
  letras de unidades, telnet 210
  nombre del servidor 10
  propiedad, privilegio de grupo 87
  unidad de reserva 44
asistente
  ejecución 6
  inicio 7
  variaciones 7
ayuda en línea, uso 6
ayuda, uso 6

B

barra de herramientas
  iconos 2
  uso 2
Bloque de mensajes de servidor
  consulte SMB
bloqueo de la consola 226
borrado
  archivos en cuarentena 68
  cuotas de árbol de directorios 115
  cuotas de usuario 113
  exportaciones NFS 118
  hosts
    GUI 90
    telnet 224
  hosts de confianza
    GUI 90
    telnet 225
  miembros del grupo
    GUI 88
    telnet 219
  punto de control 168
  punto de control programado 167
  recursos compartidos estáticos
    GUI 107
    telnet 217
  volumen de archivo
    telnet 213
  volumen de archivo desfasado
    GUI 131
    telnet 232
  volumen de archivo duplicado
    telnet 232

C

cambio
  cuotas de árbol de directorios 114
  cuotas de grupo 112
  cuotas de usuario 112
  duplicación 125
  exportaciones NFS 117
  hosts 89
    telnet 224
  idioma
    telnet 204
  nombre de particiones, telnet 212
  orden de búsqueda de los servicios de nombres
    84
    telnet 209
  punto de control programado 167
  recursos compartidos estáticos
    GUI 106
    telnet 216
cambio de nombre
  particiones, telnet 212
  punto de control 168
carcasa de disco 276
centro de distribución de claves
  consulte KDC
CIFS
  asignación de letras de unidades 210
  Compliance Archiving Software 248
  configuración de clientes
    DOS 108
    Windows 107
  definición 101
  recur compartid estát
    acerca de 101
    configuración, telnet 214
  recur compartidos autohome
    configuración, telnet 214

recursos compartidos autohome
configuración 109
recursos compartidos estáticos
adición 103
configuración 102
creación 103
edición 106
eliminación 107
seguridad 104
restricciones, nombres recur compartid 103, 106
clientes
configuración 107
DOS 108
Windows 107
clúster
funciones de los puertos 20
habilitar la recuperación de unidad tras error 15
comando raidctl profile 183
Compliance Archiving Software 133
API 259
configuración 248
componentes de hardware 274
componentes del panel trasero 274
comprobación
configuración DNS 81
orden de búsqueda de los servicios de nombres 80
configuración
adaptadores de red 19
ADS 22
GUI 79
telnet 217
clientes SMB/CIFS 107
Compliance Archiving Software 248
comprobación de DNS para ADS 81
contraseña del administrador 61
copia de seguridad
telnet 248
copia de seguridad, telnet 248
cuotas de árbol de directorios 113
cuotas de grupo 110
cuotas de usuario 110
dirección de la puerta de enlace 20
DNS
GUI 24
telnet 206
DNS dinámico
telnet 206
duplicación
telnet 226, 229
duplicación de volúmenes de archivo 123
GUI 123
telnet 228
ejecución del asistente 6
exportaciones NFS 116
fecha 64
telnet 200
FTP 162, 239
grupo
cuotas 110
privilegios 86
privilegios, telnet 220
grupos de usuarios, telnet 218
hora 64
telnet 200
hosts 89
GUI 89
idioma 32
GUI 32
telnet 204
inicio de sesión 31
inicio de sesión local
telnet 206
inicio del asistente 7
inicio sesión remoto
telnet 206
LDAP 83
letras de unidades en telnet 210
NDMP
GUI 170
telnet 248
NIC 19
NIS 26
telnet 208
NIS+ 27
telnet 208
nombre del servidor 10
notificación mediante correo electrónico 30
telnet 234
NTP 63
telnet 201
orden de búsqueda de los servicios de nombres 28
telnet 209
privilegios 89
GUI 89
telnet 220
privilegios de grupo 86

puertos
duplicación 123
GUI 19
telnet 199
RDATE 64
telnet 201
recuperación 17
telnet 244
recuperación de controlador 17
recuperación de unidad 17
recuperación tras error
telnet 243
recuperación tras error, telnet 243
recur compartid estát
telnet 214
recur compartidos autohome
telnet 214
recursos compartidos autohome
GUI 109
telnet 214
recursos compartidos estáticos
GUI 102
telnet 214
seguridad 100
seguridad de Windows 21
servicios de nombres 28
telnet 205
servidor activo
GUI 122
telnet 226, 227
servidor de destino
GUI 122
telnet 226, 227
servidor de duplicación
GUI 122
telnet 226, 227
servidor de origen
GUI 122
telnet 226, 227
sincronización de hora 63
GUI 63
telnet 201
SMTP
telnet 235
SNMP
GUI 140
telnet 234
TCP/IP
telnet 199
TCP/IP, telnet 199
telnet, letras de unidades 210
umbrales de advertencia 127
GUI 127
telnet 230
variaciones del asistente 7
WINS 23
zona horaria 64
GUI 64
telnet 200
configuración de iSCSI 53
conmutadores 272
alimentación 272
panel frontal 272
consola 195
bloqueo 226
contenedores, actualización de recursos
compartidos de ADS 82
contraseña
administrador, configuración 61
controlador
información, visualización 157
recuperación tras error, habilitar 17
convenciones
nombres de servidores 10
copia de seguridad
configuración, telnet 248
grupo de operadores 86
limpieza, cabezales 172
NDMP
GUI 170
telnet 248
visualización
estado de la cinta 160
estado del trabajo 160
registro 159
correo electrónico de diagnóstico, envío 281
creación
cuotas de árbol de directorios 113
cuotas de grupo 111
cuotas de usuario 111
exportaciones NFS 116
hosts 89
telnet 223
hosts de confianza
GUI 90
telnet 224
LUN 40

punto de control programado
telnet 247
puntos de control
GUI 165
telnet 247
RAID 40
recursos compartidos estáticos
GUI 103
telnet 216
segmento 45
telnet 212
volumen de archivo 45
telnet 211
creación de sistema de archivos 40
credenciales, asignación 91
c-spots, acerca de 164
cuotas
árbol de directorios
adición 113
borrado 115
configuración 113
edición 114
gestión 109
grupo
adición 111
configuración 110
edición 112
predeterminado 110
raíz 110
habilitación
telnet 218
límite flexible 110
límite máximo 110
superusuario 110
usuario
adición 111
borrado 113
configuración 110
edición 112
predeterminado 110
cuotas de árbol de directorios
adición 113
borrado 115
configuración 113
edición 114
cuotas predeterminadas
grupo 110
usuario 110

D

definición
LUN 40
RAID 40
segmento 45
volumen de archivo 45
derechos de acceso, definición 86
desbloqueo de la consola 226
desplazamiento
telnet 197
Web Administrator 1
detener servidor 164
DHCP
deshabilitación con recuperación de unidad tras error 15
dirección de la puerta de enlace
configuración 20
Dirección IP
alias 70
dirección IP alias
acerca de 70
disco, carcasa 276
dispositivo Sun StorEdge 5310 NAS
componentes del panel trasero 274
conmutadores 272
Indicadores LED de estado 273
DN, definición 23
DNS
acerca de 78
comprobación de la configuración 81
configuración
GUI 24
telnet 206
DNS dinámico
configuración, telnet 206
habilitación 25
dominio
seguridad 21
DOS, configuración para SMB/CIFS 108
DTQ
consulte Cuotas de árbol de directorios
definición 113
duplicac
configuración
servidor de destino, telnet 226

duplicación
acerca de 121
antes de comenzar 121
cambio 125
configuración
puerto dedicado 123
servidor activo, telnet 226, 227
servidor de destino, telnet 227
servidor de duplicación, telnet 226, 227
servidor de origen, telnet 226, 227
telnet 229
umbrales de advertencia, telnet 230
volúmenes de archivo 123
volúmenes de archivo, telnet 228
edición 125
eliminación del volumen de archivo, telnet 232
estadísticas de uso 157
estados 159
función de puerto 70
interrupción
duplicación 128
telnet 232
memoria búfer
alertas, umbrales 127
definición 121
duplicación, definición 121
promoción de un volumen de archivo
GUI 129
telnet 230
requisitos 121
restablecimiento de una duplicación
GUI 130
telnet 231
servidor
configuración 122
configuración, telnet 226, 227
definición 121
servidor activo, definición 121
servidor de destino, definición 121
servidor de duplicación, definición 121
servidor de origen, definición 121
telnet 226
visualización, telnet
estadísticas 238
estado individual 236
duplicación individual, visualización del estado
desde telnet 236
duplicación, RAID
definición 36

E

edición
cuotas de árbol de directorios 114
cuotas de grupo 112
cuotas de usuario 112
duplicación 125
exportaciones NFS 117
hosts 89
telnet 224
punto de control programado 167
recursos compartidos estáticos
GUI 106
telnet 216
teclas que se utilizan en telnet 197
ejecución
asistente de configuración 6
limpieza de cabezal 172
eliminación
cuotas de árbol de directorios 115
exportaciones NFS 118
hosts
GUI 90
telnet 224
hosts de confianza
GUI 90
telnet 225
miembros del grupo
GUI 88
telnet 219
punto de control 168
punto de control programado 167
recursos compartidos de ADS 83
recursos compartidos estáticos
GUI 107
telnet 217
volumen de archivo
telnet 213
enlace de canales
consulte Puertos enlazados
envío de un correo electrónico de diagnóstico 281
errores del sistema de archivos 255
errores del subsistema RAID 256
Errores del subsistema UPS 252
estadísticas de uso
actividad de red 152
actividad del sistema 152
duplicación 157
volúmenes de archivo 151

estado 141
actividad de red 152
actividad del sistema 152
cintas de copia de seguridad 160
duplicación
GUI 157
telnet 236
duplicación individual, telnet 236
entorno, visualización 147
estadísticas de duplicación, telnet 238
estados de la duplicación 159
indicadores, LED 273
información del controlador 157
rutas de red 154
suministro eléctrico 149
temperatura 148
trabajos de copia de seguridad 160
UPS 156
uso de un volumen de archivo 151
ventiladores 147
voltaje 150
estado de la temperatura 148
estado del entorno
suministro eléctrico del sistema 149
temperatura 148
ventiladores del sistema 147
visualización 147
voltaje 150
estado del sistema 273
estado del voltaje 150
eventos
inicio de sesión en telnet 207
IPMI 257
registro de sistema 144
eventos críticos, registro de sistema 144
eventos de advertencia, registro de sistema 144
eventos de aviso, registro de sistema 144
eventos de depuración, registro de sistema 144
eventos de emergencia, registro del sistema 144
eventos de error, registro de sistema 144
eventos de información, registro de sistema 144
eventos IPMI 257
exploración antivirus 68
exportaciones
configuración 116
creación 116
edición 117
eliminación 118

F

fecha, configuración 64
telnet 200
File Replicator 121
firmware
actualización 174
directorios y archivos 176
matriz RAID 175
firmware de unidad, actualización 174
flexible, límite 110
FTP
acceso 163, 240
configuración 162, 239

G

gestión
acceso a volúmenes de archivo, telnet 225
cuotas 109
hosts de confianza, telnet 224
recuperación tras error, telnet 243
rutas, telnet 205
GID, definición 104
grupo
adición de miembros
GUI 88
telnet 219
administradores 86
credenciales, asignación 91
cuotas
adición 110
configuración 110
edición 112
predeterminadas 110
eliminación de miembros
GUI 88
telnet 219
operadores de copia de seguridad 86
privilegios
GUI 86
telnet 220
raíz
cuotas 110
usuario, acerca de 85
usuarios avanzados 86
grupo de trabajo
seguridad
habilitación 22

grupo de usuarios avanzados 86
grupo raíz
  cuotas 110
GUI
  ayuda en línea 6
  barra de herramientas 2
  definición 1
  panel de contenido 5
  Panel de estado 6
  panel de navegación 3
  uso 2

H

habilitación
  ADS
    GUI 79
    telnet 217
  cuotas
    telnet 218
  cuotas de grupo
    GUI 110
    telnet 218
  cuotas de usuario
    GUI 110
    telnet 218
  DNS
    GUI 24
    telnet 206
  DNS dinámico 25
    telnet 206
  idiomas extranjeros
    GUI 32
    telnet 204
  inicio de sesión 31
  inicio de sesión local
    telnet 206
  inicio sesión remoto
    telnet 206
  LDAP 83
  NIS 26
    telnet 208
  NIS+ 27
    telnet 208
  notificación mediante correo electrónico 30
    telnet 234
  protección antivirus 66
  puntos de control
    telnet 247
  recuperación de controlador tras error
    GUI 17
  recuperación de enlace tras error
    GUI 16
  recuperación tras error
    GUI 15
  recursos compartidos autohome
    GUI 109
    telnet 214
  recursos compartidos estáticos
    GUI 103
    telnet 214
  seguridad para dominio 21
  seguridad para grupos de trabajo 22
  servicios de nombres 28
    telnet 205
  SNMP
    GUI 140
    telnet 234
  supervisión de UPS 156
  WINS 23
habilitar
  recuperac controlador tras error
    telnet 243
  recuperac enlace tras error
    telnet 243
  recuperac tras error
    telnet 243
  recuperac unidad tras error
    telnet 243
hora
  configuración 64
    telnet 200
  sincronización
    acerca de 62
    configuración 63
    configuración, telnet 201
    NTP 62
    RDATE 62
  zona, configuración 64
    telnet 200
hosts
  adición 89
    telnet 223
  asignación de nombres 90
  borrado, telnet 224
  configuración 89

de confianza 89
adición, telnet 224
borrado, telnet 225
configuración 89
eliminación 90
telnet 224
edición 89
telnet 224
eliminación 90
rutas 154
hosts de confianza
acerca de 89
adición
GUI 90
telnet 224
borrado, telnet 225
eliminación 90
gestión, telnet 224

I

iconos, barra de herramientas 2
identificación de ubicaciones de puertos 18, 69
idioma
asignación 32
selección, telnet 204
Independiente, función de puerto 70
indicadores
LED de estado 273
indicadores LED de estado 273
iniciación
recuperación
GUI 17
recuperación de controlador 17
recuperación de unidad 17
inicio de sesión
configuración 31
eventos críticos 144
eventos de advertencia 144
eventos de alerta 144
eventos de aviso 144
eventos de depuración 144
eventos de emergencia 144
eventos de error 144
eventos de información 144
eventos de sistema 144
local, configuración
telnet 206
registro de copia de seguridad
GUI 159
remoto, configuración
telnet 206
tipos de eventos 207
utilidades 31
telnet 207
visualización del registro 143
visualización del registro del sistema
GUI 143
telnet 236
inicio de sesión local
consulte inicio de sesión
inicio de sesión remoto
configuración
telnet 206
consulte inicio de sesión
inmediatamente
puntos de control, creación 165
interfaz de línea de comandos 195
interfaz gráfica de usuario
consulte GUI
interrupción de duplicaciones
GUI 128
servidor 1
GUI 130
telnet 232
telnet 232

K

KDC, definición 23

L

LDAP
acerca de 78
configuración 83
habilitación 83
letras de unidades, configuración, telnet 210
límite
flexible 110
máximo 110
LUN
acerca de 38
adición 40
creación 40
definición 38
reconstrucción 49

M

Macintosh
- compatibilidad 103, 106
- llamadas a BD de escritorio 103, 106

matriz RAID
- firmware 175

Matriz redundante de discos independientes
- consulte RAID

máximo, límite 110

mensajes
- idioma de visualización 32

mensajes de error 251
- errores del sistema de archivos 255
- errores del subsistema RAID 256
- Errores del subsistema UPS 252
- eventos IPMI 257
- SysMon 251

menú principal, telnet 198

modificación, telnet
- privilegios de grupo 220

monitor de actividad, visualización, telnet 235

N

NDMP
- configuración 170
- configuración en telnet 248
- definición 170

NFS
- definición 116
- exportaciones
  - configuración 116
  - creación 116
  - edición 117
  - eliminación 118

NIC
- configuración 19
- definición 18

NIS
- acerca de 78
- configuración 26
  - telnet 208
- definición 8

NIS+
- acerca de 78
- configuración 27
  - telnet 208
- definición 8

niveles de notificación, notificación de correo electrónico 30

niveles de RAID admitidos 35

nombre
- ámbito 24
- contenedor, límites 80
- dominio 22
- hosts 90
- restricción de NetBIOS 22
- restricciones, nombres recur compartid 103, 106
- segmento 45
- servidor
  - configuración 10
  - convenciones 10
- volumen de archivo 45

nombres de rutas, ADS 80

notificación mediante correo electrónico
- configuración 30
- configuración, telnet 234
- diagnóstico, envío 281
- niveles de notificación 30

NSSLDAP, consulte LDAP

NTP
- configuración 63
  - telnet 201
- definición 62
- sincronización de hora 62
  - telnet 201

número de unidad lógica
- consulte LUN

O

opciones
- activación 119
- Compliance Archiving Software 133, 248
  - API 259
- duplicación 121

orden de búsqueda
- cambio 84
- configuración en telnet 209
- servicios de nombres, verificación 80

organización en secciones, definición 36

P

panel
- frontal, conmutadores 272
- trasero, componentes 274

panel de contenido
uso 5
panel de navegación
uso 3
panel frontal
conmutadores 272
paridad, definición 37
partición
acerca de 38
cambio de nombre, telnet 212
periodo retención, Compliance Archiving Software 248
Preferencias de UNIX
asignación 97, 98
orden de búsqueda de los servicios de nombres 29
principal, función de puerto 69
privado, función de puerto 70
privilegios
asignación de la propiedad 87
configuración 89
definición 86
grupos de usuarios 86
superusuario 89
programación
puntos de control 166
edición 167
eliminación 167
telnet 247
promoción
volumen de archivo
GUI 129
telnet 230
Protección antivirus 65
configuración 65
Protocolo de gestión de datos de red
consulte NDMP
Protocolo de hora de red
consulte NTP
Protocolo de transferencia de archivos
consulte FTP
Protocolo ligero de acceso a directorios
consulte LDAP
Protocolo simple de administración de red
consulte SNMP
Protocolo simple de transferencia de correo
consulte SMTP
publicación de recursos compartidos en ADS 81
puerto dedicado
configuración de la función de los puertos 123
duplicación 123
puertos
configuración
telnet 199
duplicación
configuración 123
enlazados 71
sistema con dos servidores 73
funciones 70
asignación 20
configuración de puertos dedicados 123
duplicación 70
independiente 70
principal 69
privado 70
ubicación
identificación 18, 69
visualización de puertos enlazados, telnet 236
puertos enlazados 71
sistema con dos servidores 73
visualización, telnet 236
puntos de control
acceso 169
acerca de 164
adición a una programación
telnet 247
análisis, visualización desde telnet 236
cambio de nombre 168
compartidos 168
creación 165
edición de la programación 167
eliminación 168
eliminación de un elemento programado 167
programación
GUI 166
telnet 247
Puntos de control de archivo Sun StorEdge
consulte Puntos de control
puntos de referencia, acerca de 164

R

RAID
- acerca de 35
- adición 40
- conjuntos 35
- creación 40
- duplicación, definición 36
- mensajes de error 256
- niveles admitidos 35
- organización en secciones, definición 36
- paridad, definición 37

RDATE
- configuración 64
  - telnet 201
- sincronización de hora 62
  - telnet 201

reconstrucción, LUN 49

recuperación
- configuración
  - telnet 244
- definición 15
- iniciación 17
  - GUI 17

recuperación de enlace tras error, habilitar 16

recuperación tras error
- configuración, telnet 243
- controlador
  - habilitación 17
- definición 15
- enlace 16
- gestión, telnet 243
- habilitación 15
- unidad, definición 15

recur compartid 101
- estáticos
  - acerca de 101
  - configuración, telnet 214
- restricciones nombres 103, 106

recur compartid estát
- acerca de 101
- restricciones nombres 103, 106

recursos compartidos
- acerca de 101
- actualización de contenedores de ADS 82
- asignación de letras de unidades 210
- autohome
  - acerca de 108
  - configuración 109
  - configuración, telnet 214
- eliminación de ADS 83
- estáticos
  - adición, telnet 216
  - borrado, telnet 217
  - configuración 102
  - creación 103
  - edición 106
  - edición, telnet 216
  - eliminación 107
  - seguridad 104
- publicación en ADS 81
- puntos de control 168

recursos compartidos autohome
- acerca de 108
- configuración 109
- configuración, telnet 214

recursos compartidos estáticos
- configuración 102
- creación 103
- edición 106
- eliminación 107
- seguridad 104

red
- actividad, estadísticas de uso 152
- rutas 154
  - estadísticas 154
  - visualización 155
- tarjeta de interfaz
  - consulte NIC

reinicio
- servidor 164
- telnet 242

requisitos
- duplicación 121
- nombre del servidor 10

restablecimiento de una duplicación
- duplicación del volumen de archivo actualizado
  - GUI 131
  - telnet 233
- eliminación del volumen de archivo desfasado
  - GUI 131
  - telnet 232
- GUI 130

interrupción de la duplicación
GUI 130
telnet 232
telnet 231
restauración
limpieza, cabezales 172
tiempo de espera, definición 16
restricciones
nombres
ámbito 24
contenedor 80
contenedor ADS 80
dominio 22
host 90
NetBIOS 22
recur compartid 103, 106
segmento 45
servidor 10
volumen de archivo 45
Ruta LUN 12
acerca de 10
configuración 14
sistema con dos servidores 13
rutas
acerca de 154
gestión en telnet 205
host 154
indicadores 154
visualización 155

S

segmento
acerca de 39
adición, telnet 212
anexión
telnet 212
creación 45
restricciones del nombre 45
seguridad
acceso a volúmenes de archivo, telnet 225
bloqueo de la consola 226
configuración 100
contraseña del administrador 61
desbloqueo de la consola 226
directorios de archivos 99
recursos compartidos estáticos 104
Windows 21
selección de idioma, telnet 204
Servicio Active Directory
consulte ADS
Servicio de información de red
consulte NIS
Servicio de información de red Plus
consulte NIS+
servicios de nombres
cambio del orden de búsqueda 84
comprobación del orden de búsqueda 80
configuración 28
configuración del orden de búsqueda, telnet 209
DNS 28
local 28
NIS 28
NIS+ 28
servidor
detención 164
nombre
configuración 10
convenciones 10
recuperación 15
recuperación tras error de unidad 15
reinicio 164
unidad, definición 15
servidor activo
configuración
GUI 122
telnet 226
duplicación
definición 121
telnet 226
servidor de destino
configuración
GUI 122
telnet 226
definición 121
duplicac, telnet 226
servidor de origen
configuración
GUI 122
telnet 226
duplicación
definición 121
telnet 226
servidor iSNS 59
sincronización 62

sincronización de hora
acerca de 62
configuración 63
telnet 201
sistema
apagado
GUI 163
telnet 242
estadísticas de uso de actividades 152
estado
panel, uso 6
eventos
visualización 144
registro
visualización 143
visualización, telnet 236
sistema con dos servidores
alias de IP 71
funciones de los puertos 20
habilitar la recuperación de unidad tras error 15
puertos enlazados 73
sistema de archivos
creación 40
gestión en telnet 210
mensajes de error 255
Sistema de archivos comunes de Internet
consulte CIFS
Sistema de archivos de red
consulte NFS
sistema dos servidores
habilitar recuperac unidad tras error
telnet 243
SMB
asignación de letras de unidades 210
configuración
clientes 107
clientes de DOS 108
clientes de Windows 107
recur compartid estát, telnet 214
recur compartidos autohome, telnet 214
definición 101
recur compartid estát
acerca de 101
recursos compartidos autohome
configuración 109
habilitación 109
recursos compartidos estáticos
adición 103
borrado 107
cambio 106
configuración 102
creación 103
edición 106
eliminación 107
habilitación 103
restricciones, nombres recur compartid 103, 106
seguridad, recursos compartidos estáticos 104
SMTP
definición 30
SNMP
configuración
GUI 140
telnet 234
definición 140
software
actualización 173
duplicación 121
File Replicator 121
suministro eléctrico 279
estado 149
Suministro ininterrumpido de alimentación
consulte UPS
superusuario
cuotas 110
privilegios definidos por el estado del host 89
supervisión
configuración SNMP 140
UPS 156
habilitación 156
syslogd, definición 31
SysMon, acerca de 251

T

TCP/IP
configuración
telnet 199
telnet
adición
hosts 223
hosts de confianza 224
miembros del grupo 219
puntos de control 247
recursos compartidos 216
segmentos 212

apagado 242
bloqueo de la consola 226
borrado
  hosts 224
  hosts de confianza 225
  recursos compartidos 217
  volumen de archivo 213
  volumen de archivo duplicado 232
cambio de nombre de particiones 212
configuración
  ADS 217
  copia de seguridad 248
  DNS 206
  DNS dinámico 206
  duplicación 229
  fecha 200
  grupos de usuarios 218
  hora 200
  inicio de sesión local 206
  inicio sesión remoto 206
  letras de unidades 210
  NDMP 248
  NIS 208
  NIS+ 208
  notificación mediante correo electrónico 234
  NTP 201
  orden de búsqueda de los servicios de nombres 209
  RDATE 201
  recuperación 244
  recuperación tras error 243
  recur compartid estát 214
  recur compartidos autohome 214
  servidor activo 226
  servidor de destino 226, 227
  servidor de duplicación 226, 227
  servidor de origen 226
  sincronización de hora 201
  SNMP 234
  TCP/IP 199
  umbrales de advertencia 230
  volúmenes de archivo duplicados 228
  zona horaria 200
creación de volúmenes de archivo 211
desbloqueo de la consola 226
desplazamiento 197
duplicación 226
  interrupción de duplicaciones 232
  promoción de volúmenes de archivo 230
  visualización del estado 236
edición
  hosts 224
  recursos compartidos 216
eliminación de miembros de grupos 219
gestión
  acceso a volúmenes de archivo 225
  hosts de confianza 224
  recuperación tras error 243
  rutas 205
  sistema de archivos 210
habilitación de cuotas 218
inicio de sesión
  eventos 207
  utilidades 207
interrupción de duplicaciones 232
menú principal 198
menús 197
modificación
  privilegios de grupo 220
programación
  puntos de control 247
reinicio 242
restablecimiento de una duplicación 231
selección, idioma 204
teclas de edición 197
visualización
  análisis de puntos de control 236
  estadísticas de duplicación 238
  estado de duplicación 236
  estado duplicación individual 236
  monitor de actividad 235
  puertos enlazados 236
  registro del sistema 236
tiempo de espera de inactividad, definición 16

U

UID, definición 104
umask 105
umbrales 127
umbrales de advertencia
  acerca de 127
  configuración
    GUI 127
    telnet 230
umbrales, configuración
  GUI 127
  telnet 230

unidad
definición 15
limpieza 172
unidad de reserva
asignación 44
UPS
definición 155
habilitación de la supervisión 156
mensajes de error 252
supervisión 156
uso
ayuda en línea 6
barra de herramientas 2
GUI 2
panel de contenido 5
Panel de estado 6
panel de navegación 3
usuario
credenciales
asignación 91
cuotas
adición 111
borrado 113
configuración 110
edición 112
predeterminadas 110
grupos
acerca de 85
adición de miembros, telnet 219
configuración, telnet 218
eliminación de miembros, telnet 219
modificación de privilegios, telnet 220
privilegios 86
raíz
cuotas 110
utilidades
telnet 207

V

variaciones, asistente de configuración 7
ventiladores
estado 147
virus
exploración 68
visualización
actividad de red 152
actividad del sistema 152
análisis de puntos de control, telnet 236
copia de seguridad
estado de la cinta 160
estado del trabajo 160
copia de seguridad, registro
GUI 159
estadísticas de duplicación
GUI 157
telnet 238
estado 141
estado de duplicación, telnet 236
estado de la temperatura 148
estado de los ventiladores 147
estado del entorno 147
estado del suministro eléctrico 149
estado del voltaje 150
estado duplicación individual, telnet 236
eventos de sistema 144
información del controlador 157
monitor de actividad, telnet 235
puertos enlazados, telnet 236
registro del sistema 143
GUI 143
telnet 236
rutas 155
rutas de red 155
uso de un volumen de archivo 151
volumen de archivo
acerca de 39
borrado
telnet 213
creación 45
telnet 211
duplicación
GUI 123
telnet 228
duplicación del volumen actualizado
GUI 131
telnet 233
eliminación del volumen desfasado
GUI 131
telnet 232
estadísticas de uso 151
expansión
telnet 212
gestión de acceso, telnet 225
promoción
GUI 129
telnet 230

recur compartid estát
acerca de 101
recursos compartidos autohome
acerca de 108
telnet 214
recursos compartidos estáticos
telnet 214
restablecimiento de una duplicación
GUI 130
telnet 231
restricciones del nombre 45

W

Web Administrator
ayuda en línea 6
barra de herramientas 2
desplazamiento 1
GUI 2
panel de contenido 5
Panel de estado 6
panel de navegación 3
Windows
asignación de credenciales 97
configuración de SMB/CIFS 107
dominio
habilitación 21
grupo de trabajo
habilitación 22
seguridad 104
seguridad de los directorios de archivos 99
recur compartid estát, acerca de 101
recursos compartidos autohome, acerca de 108
seguridad
modelos 21
WINS
acerca de 78
configuración 23