

ADIC Management Console™ Manual de usuario

ADVANCED DIGITAL INFORMATION CORPORATION

Copyright © 2002-2004 ADIC®

La información contenida en este documento está sujeta a cambios sin previo aviso.

Este documento contiene información de propietario protegida por copyright. Todos los derechos reservados. Ninguna parte de este documento se podrá fotocopiar, reproducir ni traducir a otro idioma sin el permiso previo por escrito de ADIC.

ADIC no será responsable de los errores contenidos en este documento ni de los daños incidentales o imprevistos (entre ellos, la pérdida de ganancias) en relación con suministros, rendimiento o uso de este material, ya sea basándose en una garantía, contrato u otro documento legal.

Todas las marcas comerciales contenidas en este documento son propiedad de sus respectivos propietarios.

Copyright © 2002-2004 ADIC Europe™

Reservados todos los derechos. Prohibida la copia o reproducción de este documento de cualquier forma y por cualquier medio, sin el consentimiento previo por escrito de ADIC Europe, ZAC des Basses Auges, 1 rue Alfred de Vigny, 78112 Fourqueux, Francia.

ADIC Europe declina toda responsabilidad por los errores que puedan existir en este documento y se reserva el derecho a realizar cambios en estas especificaciones y descripciones en cualquier momento sin previo aviso.

Es posible que esta publicación describa diseños cuyas patentes estén pendientes o hayan sido otorgadas. Al publicar esta información, ADIC Europe no cede licencia bajo ninguna patente ni ningún otro derecho.

ADIC Europe no representa ni ofrece garantías respecto a los contenidos de este documento y específicamente niega cualquier garantía implícita de comerciabilidad o conveniencia para cualquier propósito particular. Además, ADIC Europe se reserva el derecho de revisar o cambiar esta publicación sin la obligación de notificar a ninguna persona u organización tal revisión o cambio.

Se han realizado todos los esfuerzos para reconocer las marcas comerciales y a sus propietarios. Los nombres de marcas comerciales se han utilizado con el único propósito de identificación o ejemplo, cualquier omisión es involuntaria.

ADIC es una marca comercial registrada y ADIC Europe es una marca comercial de Advanced Digital Information Corporation.

ADIC USA
Telef.: +1-303-705-3900
Fax: +1-303-792-2465
ATAC: 1-800-827-3822
<http://www.adic.com>

ADIC Europe
ZAC des Basses Auges 1,
rue Alfred de Vigny
78112 Fourqueux, Francia
Telef.: +33.1.3087.5300
Fax: +33.1.3087.5301

ADIC Germany Beteiligungs GmbH, KG
Eschenstraße 3
D-89558 Böhmenkirch, Alemania
Telef.: +00.800.9999.3822

Publicado: Junio de 2004

Número de documento: 6-00064-04 Rev. A

Sommario

1	Introducción	1
	Usuarios objetivo	1
	Documentos asociados	1
	Explicación de símbolos	1
	Ayuda	2
	Ayuda en pantalla	2
<hr/>		
2	Descripción	3
	Funciones de ADIC Management Console	4
	Utilización del cliente SAN	4
	Utilización de un cliente de gestión de bibliotecas	4
	Características de ADIC Management Console	4
	Gestión de la biblioteca	5
	Registro de eventos	5
	Informes	5
	Latido	5
	Comprobaciones de estado	5
	Zonificación por canales	5
	Organizador de datos	5
	Scalar® Firewall Manager / Virtual Private SAN®	6
	extended VPS®	6
	Asignación privada virtual	6
	SNMP	6
	Soporte de la RMU de la biblioteca	6
	Seguridad	6
	Detección de red	7
	Opciones de configuración	7
	Actualización del Firmware	7
<hr/>		
3	Información preliminar	9
	Requisitos de instalación	9
	Requisitos del sistema para el servidor	9
	Requisitos del sistema para el cliente	10
	Antes de instalar AMC	11
	Instalación del servidor AMC	11
	Instalación del servidor en un sistema Windows	11

Instalación del servidor en un sistema UNIX	12
Inicio del servidor AMC	13
Inicio de un servidor Windows	14
Inicio de un servidor UNIX	14
Instalación del cliente AMC	15
Antes de instalar el cliente	15
Instalación de un cliente AMC en Windows	15
Instalación de un cliente UNIX	15
Inicio del cliente AMC	16
Inicio de un cliente Windows	17
Inicio de un cliente UNIX	17
Conexión al servidor	18
Inicio de sesión	18
Cierre de sesión	19
Salir del cliente AMC	20
Apagar el servidor AMC	20

4 Preguntas frecuentes 21

¿Qué es una red SAN?	21
¿Qué sucede si no aparece ningún componente de SAN después de instalarlo?	21
¿Se puede gestionar una red SAN desde una biblioteca Scalar i2000 o un sistema Pathlight VX?	21
¿Es necesario instalar un servidor o un cliente?	21
¿Es posible configurar el correo electrónico si salté ese paso durante la instalación?	22
¿Cómo se interpretan los componentes de la interfaz?	22
¿Cómo se crea una cuenta de administrador de red SAN?	22
¿Qué es un portal?	22
¿Cómo se crean portales para los usuarios?	22
¿Cómo se crean las cuentas de usuario?	22
¿Qué privilegios presenta cada tipo de usuario?	22
¿Cómo se actualiza el firmware?	22
¿Cómo se modifica la configuración de detección?	22
¿Cómo se crean políticas?	23

5 La interfaz de gestión de la red SAN 25

Menús	25
Barra de herramientas	25
Paneles	26
Ventana Received Event Traps	26
Lectura de los paneles de información de gestión de la red SAN	26
Panel de árbol	26
Numeración de los dispositivos	32
Panel gráfico	33
Panel de datos	33
Área de estado/mensajes	36
Gestión de la biblioteca o gestión de la red SAN	36
Opciones de gestión de red SAN comunes	39
Categorización automática	39
Creación de una nueva categoría	39
Desplazamiento de elementos	39
Búsquedas	39

6 Gestión de cuentas de usuario 41

Cambio de la contraseña de administrador	41
Descripción de los niveles de privilegios de usuario	41
Creación, modificación y eliminación de cuentas de usuario	43
Agregar una nueva cuenta de usuario	43
Modificación de una cuenta de usuario	44
Eliminación de una cuenta de usuario	44

7 El trabajo con portales 47

Creación de un nuevo portal	47
Modificación de un portal	48
Eliminación de un portal	49
Establecimiento de permisos para acceder al portal	49

8 El trabajo con categorías y vistas 51

El trabajo con categorías de SAN	51
Categorización automática de la SAN	51
Creación de una nueva categoría	52
Cambio del nombre de una categoría	52
Eliminación de una categoría	53
Reubicación de una categoría	53
El trabajo con componentes de categorías	54
Reubicación de elementos usando la función de arrastrar y soltar	54
Reubicación de elementos mediante el menú	55
El trabajo con vistas	56
Abrir vistas guardadas	56
Creación de vistas	56
Guardar vistas	58
Eliminación de vistas	58
Búsquedas en la vista actual	59
Informes sobre la vista actual	59

9 Realización de tareas administrativas 61

Configuración del correo electrónico	61
Configuración de políticas	62
Detección de la red SAN	63
Configuración de cadenas de comunidad SNMP	65
Lectura de información sobre una biblioteca	66
Visualización de los datos de la RMU	66
Utilización de la comprobación de estado	66
Realización de la comprobación de estado	66
Configuración de la comprobación de estado	67
Comprobación del latido	68
Seguimiento y gestión de registros de eventos	68
Ajuste del límite de captura de eventos	69
Recepción de capturas de eventos	70

Seguimiento de las capturas de evento recibidas	70
Seguimiento del panel de LEDs	71
Utilización del comando Identify	73
Gestión del equipo de red SAN	75
Actualización de datos	76
Guardar la configuración	76
Carga de un archivo local	77
Carga de un archivo desde el servidor	77
Actualización del firmware	77
Utilización del comando Restart	78
Seguimiento de datos de entorno	79

10 Configuración de canales y dispositivos 81

Gestión del canal SCSI	81
Volver a escanear el canal SCSI	81
Restablecer el canal SCSI	82
Configuración del canal SCSI	82
Gestión de Fibre Channel	83
Volver a escanear Fibre Channel	83
Restablecer Fibre Channel	84
Configuración de Fibre Channel	84
Descripción de las opciones de modo de puerto	85
Descripción de las opciones de tipo de conexión	86
Tipo de host	86
ID de bucle	86
Tamaño de trama	86
Gestión de dispositivos	87
Edición de mapas de dispositivos	87
Asignación previa de números de dispositivos	88

11 Configuración del acceso a la red SAN 91

Habilitación de funciones sujetas a licencia	91
Módulo organizador de datos	92
Utilización de la zonificación por canales	92
Instalación de HRS	93
Instalación del servicio de registro de host en sistemas Windows	93
Instalación del servicio de registro de host en sistemas Solaris	94
Instalación del servicio de registro de host en sistemas HP-UX	95
Instalación del servicio de registro de host en sistemas AIX	96
Utilización de Scalar Firewall Manager (SFM)	96
Instalación de SFM	97
Configuración del acceso a través de SFM	98
Agregar hosts SFM	100
Eliminación de hosts SFM	100
Utilización de eVPS	101
Instalación de eVPS	101
Configuración del acceso a través de eVPS	102
Agregar o modificar hosts eVPS	105
Eliminación de hosts eVPS	106
Utilización del menú View de eVPS	106
Utilización de VPM	107

12 Solución de problemas de la red SAN	109
Comprobación del registro de eventos	109

A Glosario	113
------------	-----

1

Introducción

Este manual contiene la información y las instrucciones necesarias para manejar ADIC Management Console (AMC).

Usuarios objetivo

Este manual está dirigido a administradores del sistema, operadores o a cualquier persona interesada en conocer el funcionamiento de AMC. AMC se utiliza para gestionar redes de áreas de almacenamiento (SAN) mediante una conexión por controlador de red de almacenamiento (SNC) o por tarjeta de control de gestión (MCB), como pueden ser los modelos Scalar 24, Scalar 100, Scalar 1000, Scalar i2000 o Scalar 10K.

Documentos asociados




El manual de usuario del hardware del SNC de la biblioteca Scalar que utilice.

Manual de Referencia de SNC Firmware 4: documento 6-00676-xx

Manual de usuario de Scalar i2000: documento 6-00421-xx

Explicación de símbolos

Los siguientes símbolos, que aparecerán en el transcurso de este documento, ofrecen información importante:

Símbolo	Descripción	Definición	Consecuencia
	ADVERTENCIA:	Situación inminente de riesgo eléctrico	Muerte o lesión grave
	ATENCIÓN:	Posible situación de daño	Posible daño en el equipo o pérdida de datos
	NOTA:	Indica información importante que permite realizar un mejor uso del sistema.	Sin consecuencias de daño o peligro

Ayuda

Si no encuentra la solución a sus dudas en este documento o desea realizar un curso de formación, póngase en contacto con el centro de asistencia técnica de ADIC (ADIC Technical Assistance Center, ATAC).

En Estados Unidos: 800.827.3822

Fuera de Estados Unidos
(llamada gratuita): 00.800.9999.3822

Internet: support@adic.com

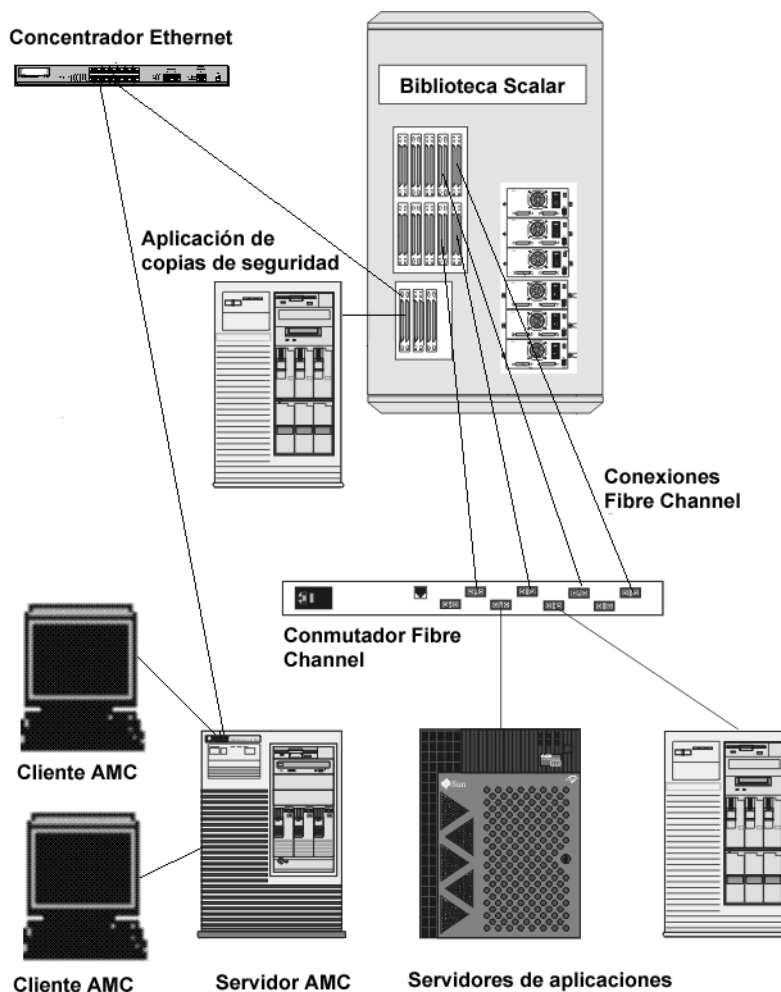
Ayuda en pantalla

AMC ofrece una ayuda en pantalla mediante el menú **Help** y los botones o cuadros de diálogo **Help**.

2

Descripción

En este capítulo se describe AMC (ADIC Management Console). AMC es una herramienta de gestión con todas las características posibles para las redes de áreas de almacenamiento (SAN) que tengan una conexión por controlador de red de almacenamiento (SNC) o por tarjeta de control de gestión (MCB). Una SAN es una red que conecta servidores o estaciones de trabajo con matrices de discos, sistemas de copia de seguridad en cinta, conmutadores, puentes y otros dispositivos, como pueden ser las redes de transmisión a gran velocidad (fibra óptica o Gigabit Ethernet). Las redes SAN evitan que el tráfico de almacenamiento se mezcle con el tráfico de la red sin que ello suponga un retraso en el tiempo de acceso a los datos almacenados.



AMC ofrece varios niveles de derechos de acceso y la posibilidad de personalizar vistas y portales. Si se realiza un seguimiento de las distintas vistas de los clientes, siempre se podrá recuperar las vistas guardadas de estos. El servidor ofrece características de seguridad registrando los nombres de cuenta y contraseñas en nombre de la aplicación cliente. AMC también dispone de funciones para poder realizar copias de seguridad sin servidor, herramientas para la asignación del LUN y una sencilla zonificación por canales.

Funciones de ADIC Management Console

AMC utiliza un modelo de cliente/servidor de tres niveles. Las tres partes son el agente, el servidor y el cliente. El agente en un modelo Scalar i2000 es la tarjeta de control de gestión (MCB). En los modelos Pathlight VX, Scalar 24, Scalar 100, Scalar 1K y Scalar 10K, el agente es el controlador de red de almacenamiento (SNC). El agente se comunica con el servidor y con otros agentes gestionados mediante los protocolos SNMP (Simple Network Management Protocol) y SOIP (SCSI over IP). Además de comunicarse con los clientes, el servidor también se comunica con el agente.

La API de invocación de método remoto (Remote Method Invocation, RMI) de Java se utiliza para establecer comunicación desde el cliente al servidor. En sistemas de la red SAN, puede instalar una o más instancias del servidor que se ejecuten en software de las plataformas UNIX o Windows que sean remotas de los MCB o SNC. No instale más de un servidor por sistema cliente.

Utilización del cliente SAN

AMC es el cliente SAN de la serie Scalar de bibliotecas. Un modo sencillo para gestionar bibliotecas Scalar como parte de una solución SAN es mediante AMC. Cuando se instalan tanto un servidor como un cliente desde el CD del producto (esto se denomina instalación **Full**, completa), el cliente predeterminado es el cliente SAN AMC. El cliente AMC predeterminado se compone de una ventana de la interfaz de usuario basada en Java y una ventana de captura de eventos. En una red SAN se pueden instalar una o más instancias del cliente AMC.

Utilización de un cliente de gestión de bibliotecas

Si la red SAN incluye una biblioteca en la serie de plataformas inteligentes, por ejemplo la Scalar i2000, haga clic con el botón derecho del ratón en el icono Scalar i2000 del panel de árbol de AMC para luego iniciar el cliente LMC (Library Management Console). El cliente LMC tendrá la misma apariencia que la interfaz que se ejecute en la pantalla táctil de la biblioteca Scalar i2000. Sólo está disponible para el modelo de bibliotecas Scalar i2000. Si hace clic con el botón derecho del ratón en el icono de Pathlight VX, se inicia la Virtual Library Interface (VLI), la herramienta de gestión de bibliotecas para este sistema. Si se exceptúa la gestión de la red SAN, la gestión de bibliotecas de las otras bibliotecas Scalar sólo se realiza mediante sus paneles de operador respectivos.

Para obtener más información acerca de la consola LMC, consulte el *Manual de usuario de Scalar i2000*. Para obtener más información acerca de la VLI, consulte la ayuda en pantalla de Pathlight VX.

Características de ADIC Management Console

AMC ofrece el estado y los controles de las características de la biblioteca y del SNC. Las capacidades de gestión de AMC se definen mediante las siguientes características:

Gestión de la biblioteca

AMC ofrece la posibilidad de gestionar las operaciones de biblioteca en bibliotecas Scalar de plataformas inteligentes mediante una vinculación al LMC o a la VLI. Mediante el botón **Library Manager** de la pantalla táctil de la biblioteca inteligente Scalar i2000, se accede a todas las funciones disponibles. Mediante el botón **VLI** de AMC, se accede a todas las funciones disponibles en el sistema Pathlight VX.

Para obtener más información sobre las operaciones de gestión de bibliotecas, consulte el *Manual de usuario de Scalar i2000*. Para obtener más información acerca de la VLI, consulte la ayuda en pantalla del sistema Pathlight VX.

Registro de eventos

Puede recuperar y ver los registros de eventos. Para evitar los fallos, se pueden realizar filtros según la importancia de los eventos. Para obtener más información, consulte [Seguimiento y gestión de registros de eventos](#) en la página 68 y [Configuración de políticas](#) en la página 62.

Informes

Para cumplir los requisitos de informes, se pueden imprimir o guardar informes que se hayan configurado. Para obtener más información, consulte [Informes sobre la vista actual](#) en la página 59.

Latido

AMC realiza un seguimiento de los componentes del sistema para garantizar la continuidad del servicio. Si ya no están disponibles ni un SNC o un MCB, el componente del servidor notifica el seguimiento de los clientes. Para obtener más información, consulte [Comprobación del latido](#) en la página 68.

Comprobaciones de estado

Las comprobaciones instantáneas y periódicas de estado permiten realizar un seguimiento de cada equipo de red y los dispositivos conectados al mismo. Para obtener más información, consulte [Utilización de la comprobación de estado](#) en la página 66.

Zonificación por canales

La zonificación por canales es una manera de gestionar la seguridad de acceso entre conexiones SAN y los dispositivos SCSI o FC por canales.

- Esta zonificación se utiliza para asegurar el acceso entre un servidor y su almacenamiento, separándolos, por ejemplo, de otros servidores y de sus almacenamientos respectivos.
- La configuración predeterminada permite que todas las conexiones SAN accedan a todos los dispositivos SCSI o FC.

Organizador de datos

El SNC puede mover datos directamente entre los dispositivos de almacenamiento que estén conectados al mismo. El organizador de datos libera valiosos recursos del sistema en el servidor y mejora significativamente la velocidad de las operaciones de copia de seguridad y restauración.

El organizador de datos es el motor de las operaciones de copia de seguridad y restauración, y de las aplicaciones de gestión del almacenamiento jerárquico que admiten la especificación de copia ampliada (ANSI T10/99-143r1).

Scalar[®] Firewall Manager / Virtual Private SAN[®]

Las tecnologías Scalar[®] Firewall Manager (SFM) y Virtual Private SAN[®] (VPS) permiten a las redes SAN con varios usuarios compartir los mismos canales de conexión para acceder a los mismos o a distintos elementos de almacenamiento mediante la creación de varias conexiones privadas virtuales.

SFM y VPS gestionan el acceso entre un iniciador (usuario, host, sistema) y un número de unidad lógica/objetivo (LUN).

extended VPS[®]

Las funciones de extended Virtual Private SAN[®] (eVPS) permiten controlar y asignar los dispositivos FC y SCSI. También ofrece flexibilidad para asignar los dispositivos conectados a cualquier LUN definido por el usuario de forma separada e individual a cada host Fibre Channel conectado. Como eVPS es compatible de la otra manera, los usuarios actuales de VPS y SFM pueden mantener sus asignaciones cuando actualicen sus licencias.

Asignación privada virtual

La tecnología de asignación privada virtual (Virtual Private Map, VPM) permite que los sistemas antiguos y nuevos equipados con los adaptadores de bus de host SCSI accedan a los dispositivos Fibre Channel. VPM permite que los dispositivos objetivo Fibre Channel y SCSI se asignen a canales de host SCSI privados.

SNMP

Las cadenas de comunidad SNMP (Simple Network Management Protocol) forman parte de la función de mensajería del software agente que sirve para agrupar los dispositivos de red en grupos lógicos con objetivos de gestión. Las cadenas de comunidad del servidor se deben corresponder con las de los equipos en red que se deseen gestionar.

Se definen tres cadenas:

- Read: para consultar al equipo
- Write: para controlar el equipo
- Trap: para recibir mensajes de eventos desde el equipo

El equipo puede mantener 32 cadenas de comunidad de lectura, otras 32 de escritura y una sola cadena de comunidad de captura.

Para manipular las cadenas de comunidad SNMP de lectura y escritura, se ofrece un conjunto de comandos. Estas cadenas agrupan lógicamente dispositivos en comunidades de gestión.

Soporte de la RMU de la biblioteca

Los datos obtenidos a partir de una RMU (unidad de gestión remota) de la biblioteca Scalar incluyen datos globales sobre el estado, la unidad y el organizador. Estos datos se muestran en el panel de datos de AMC. Los datos de la RMU también se muestran en el menú contextual que aparece al hacer clic con el botón derecho del ratón en la biblioteca.

Seguridad

Se han definido cuatro niveles de privilegios de usuario, cada uno con derechos específicos. Para obtener más información, consulte la [tabla 2](#) en la página 42.

Detección de red

La detección de red permite localizar cualquier equipo de la red basándose en direcciones e intervalos de red. Así se permite la gestión de un equipo sin antes conocer la dirección IP específica.

Opciones de configuración

Puede configurar un equipo de red con varios parámetros no predeterminados, valores de canal y variables de gestión de eventos. Para obtener más información, consulte [Realización de tareas administrativas](#) en la página 61 y [Configuración del acceso a la red SAN](#) en la página 91.

Actualización del Firmware

Puede actualizar el firmware del dispositivo y del equipo en red a partir del cliente. Para obtener más información, consulte [Actualización del firmware](#) en la página 77.

3

Información preliminar

El servidor de AMC se comunica mediante una red Ethernet con sus clientes. Para gestionar una red SAN, instale una instancia del servidor en un sistema cualquiera de plataforma abierta que esté conectado mediante Ethernet a cada SNC y a cada cliente AMC. Para gestionar la red SAN con AMC, hay que instalar al menos una instancia del servidor. El cliente AMC se puede iniciar desde cualquier sistema conectado en el que esté instalado. Es posible iniciar un cliente LMC (Library Management Console) si el cliente de AMC se ha conectado al servidor de una biblioteca Scalar i2000. La interfaz VLI (Virtual Library Interface) se puede iniciar si el cliente AMC está conectado al servidor de un sistema Pathlight VX.



Nota

Los servidores incluidos en los modelos Scalar i2000 y Pathlight VX se encargan de gestionar las operaciones de la biblioteca. Los clientes conectados a estos servidores inician la LMC y la VLI respectivamente. Un cliente capaz de gestionar la SAN no se podrá iniciar a partir de la consola LMC ni de la interfaz VLI.

Requisitos de instalación

A continuación se presentan los requisitos mínimos de configuración de cada plataforma de sistema.

Requisitos del sistema para el servidor

Java Runtime Environment 1.4.1 se encuentra instalado en AMC. La versión del sistema operativo debe ser compatible con este nivel.

Windows

Los requisitos de instalación para Microsoft® Windows NT®, Windows® 2000 y Windows® XP son los siguientes:

- Windows NT 4.0 Server o Workstation, Service Pack 6a, Windows 2000 o Microsoft® Windows® XP
- Memoria mínima: 96 MB
- Espacio libre en disco duro: 40 MB
- Ethernet con protocolo TCP/IP instalado

AIX

Los requisitos mínimos de instalación para AIX son los siguientes:

- AIX® 4.3.3 (paquete de mantenimiento 10) o AIX 5.1
- 128 MB de memoria de sistema
- 60 MB de espacio libre en la partición de destino

HP-UX

Los requisitos mínimos de instalación para HP-UX son los siguientes:

- HP-UX™ 11.0 o superior
- 80 MB o más de memoria de sistema
- 60 MB de espacio libre en disco en la partición de destino

Solaris

Los requisitos de instalación para Solaris son los siguientes:

- Solaris™ 2.7 ó 2.8. El nivel de mantenimiento debe admitir JDK 1.4.1.
- 80 MB o más de memoria de sistema
- 60 MB de espacio libre en disco en la partición de destino
- Entorno de escritorio común (CDE)



Nota

Las limitaciones en el entorno de escritorio OpenWindows afectan a las funciones de edición “arrastrar y soltar” en los cuadros de diálogo **Device Mapping** y **VPM** de AMC. Si necesita utilizar estas funciones de AMC, debe utilizar la CDE en lugar del entorno OpenWindows.

Linux

Los requisitos de instalación para Red Hat Linux son los siguientes:

- Red Hat Linux 8
- Memoria mínima: 80 MB
- Espacio libre en disco duro: 60 MB
- Ethernet con protocolo TCP/IP instalado
- Tarjeta de adaptador de vídeo para entrada gráfica

Requisitos del sistema para el cliente

Windows

- Windows NT 4.0 Server o Workstation, Service Pack 6a, Windows 2000 o Windows XP
- Memoria mínima: 96 MB
- Espacio libre en disco duro: 30 MB
- Ethernet con protocolo TCP/IP instalado

Plataformas UNIX

Deben cumplirse los mismos requisitos descritos anteriormente para la plataforma servidor correspondiente.

Antes de instalar AMC

AMC utiliza Ethernet para la comunicación. Antes de instalar AMC debe haber una red Ethernet.



ATENCIÓN

Compruebe que tiene suficiente espacio (100 MB aproximadamente) en el directorio temporal para poder finalizar la instalación.

Para instalar una red Ethernet

- 1 Consulte en la SAN los parámetros de red del cliente, servidor y otras bibliotecas Scalar.
 - Utilice direcciones IP estáticas.
 - Si las bibliotecas Scalar de la red SAN no se encuentran en la misma subred TCP/IP que el servidor, asigne una dirección de pasarela de red predeterminada o entradas de tabla de ruta.
- 2 Guarde esta información de configuración para referencia futura.
- 3 Conecte un cable Ethernet desde el servidor hasta el concentrador o conmutador.
- 4 Conecte otros cables Ethernet desde los clientes hasta el concentrador de red.
- 5 Tienda un cable Ethernet desde el concentrador de red hasta las bibliotecas Scalar en la red SAN.
- 6 Configure la red de forma apropiada en función del sistema operativo que esté usando.

Instalación del servidor AMC

Para gestionar la red SAN, debe instalar una instancia del servidor en un sistema conectado a través de Ethernet a los productos de almacenamiento ADIC y a los sistemas en que se estén ejecutando los clientes. Este servidor no puede ser igual al servidor incluido en el modelo Scalar i2000 o en el servidor web del modelo Pathlight VX.



Nota

Es posible iniciar un cliente Library Management Console (LMC) desde el cliente AMC. Para ver las instrucciones de funcionamiento de LMC, consulte el *Manual de operador de Scalar i2000*.



Nota

La Virtual Library Interface (VLI) se puede iniciar desde el cliente AMC. Para ver las instrucciones de funcionamiento de la interfaz VLI, consulte la ayuda en pantalla del sistema Pathlight VX.

Instalación del servidor en un sistema Windows

Instale el servidor AMC cuando haya llevado a cabo los pasos descritos en [Antes de instalar AMC](#) en la página 11.

Para instalar el servidor AMC en un sistema Windows

- 1 Cargue el CD con el producto.
- 2 Haga clic en el vínculo para la instalación que aparece debajo de ADIC Management Console 4.2.

3 Haga clic en **OK**.

Así se iniciará el programa "InstallAnywhere", que realizará varias preguntas durante la instalación.

4 Cuando se le solicite que elija una opción de instalación, seleccione **Server Only** si no desea ejecutar el cliente AMC en ese host o **Full** si desea hacerlo.



ATENCIÓN

El servidor AMC debe coincidir con la versión del cliente AMC. Si el cliente y el servidor tienen versiones distintas, es posible que no puedan comunicarse.

5 Cuando se le pida que configure la detección de red, asegúrese de que el segmento de red definido incluye los componentes SAN identificados en el [paso 2](#) descrito en [Antes de instalar AMC](#) en la página 11.

6 Para instalar la parte de configuración de correo electrónico es necesaria la siguiente información:

- Nombre de red del servidor de correo electrónico; por ejemplo, MiServidorCorreo.
- Cuenta de correo válida para el servidor SMTP; por ejemplo, Juan.Perez.
- Contraseña válida para la cuenta de correo electrónico; por ejemplo, *u!nBe.
- Dirección de correo que deben recibir los destinatarios cuando AMC se ponga en contacto con ellos. No tiene por qué ser una dirección previamente validada por un servidor de correo en funcionamiento; por ejemplo, AlertaAMC@MiEmpresa.com.

7 Continúe con [Inicio del servidor AMC](#) en la página 13.

Instalación del servidor en un sistema UNIX

Instale el servidor AMC cuando haya llevado a cabo los pasos descritos en [Antes de instalar AMC](#) en la página 11.

Para instalar el servidor AMC en un sistema UNIX

- 1 Cargue el CD con el producto.
- 2 Haga clic en el vínculo para la instalación que aparece debajo de ADIC Management Console 4.2.
- 3 Haga clic en **OK**.
- 4 Abra la carpeta y copie el archivo de imagen en una carpeta temporal del host.



ATENCIÓN

Compruebe que tiene suficiente espacio (100 MB aproximadamente) en el directorio temporal para poder finalizar la instalación. Para los sistemas Solaris, si el directorio /tmp no es lo suficientemente grande para que InstallAnywhere se ejecute, la instalación fallará aunque el directorio se cambie de tamaño después.

Ajuste la variable de entorno IATEMPDIR al nombre de un directorio que sea lo bastante grande. InstallAnywhere utilizará ese directorio en lugar de /tmp.

Para ajustar la variable para Bourne shell (sh), ksh, bash y zsh, realice los siguientes pasos:

```
$IATEMPDIR=/your/free/space/directory $ export
IATEMPDIR -
```

Para ajustar la variable para C shell (csh) y tcsh, realice los siguientes pasos:

```
$ setenv IATEMPDIR /your/free/space/directory
```

- 5 Desde la carpeta temporal, escriba: `chmod 777 <filename>`; por ejemplo,

```
chmod 777 MC400SOL.bin
```

y pulse **Enter**.

- 6 Si la carpeta temporal NO se encuentra en la ruta del usuario, escriba `[espacio] ./<nombre de archivo>`; por ejemplo,

```
./MC400HPX.bin
```

y pulse **Enter**.

De esta forma se iniciará la instalación desde el directorio actual.

Si la carpeta temporal está en la ruta del usuario, sólo tendrá que escribir: `<nombre de archivo>` (incluyendo la extensión); por ejemplo,

```
MC400LIN.bin
```

y pulse **Enter**.

Así se iniciará el programa "InstallAnywhere", que realizará varias preguntas durante la instalación.

- 7 Cuando se le solicite que elija una opción de instalación, seleccione **Server Only** si no desea ejecutar el cliente AMC en ese host o **Full** si desea hacerlo.



ATENCIÓN

El servidor AMC debe coincidir con la versión del cliente AMC. Si el cliente y el servidor tienen versiones distintas, es posible que no puedan comunicarse.

- 8 Cuando se le pida que configure la detección de red, asegúrese de que el segmento de red definido incluya los componentes SAN identificados en el [paso 2](#) descrito en [Antes de instalar AMC](#) en la página 11.
- 9 Para instalar la parte de configuración de correo electrónico es necesaria la siguiente información:
- Nombre de red del servidor de correo electrónico; por ejemplo, MiServidorCorreo.
 - Cuenta de correo válida para el servidor SMTP; por ejemplo, Juan.Perez.
 - Contraseña válida para la cuenta de correo electrónico; por ejemplo, *u!nBe.
 - Dirección de correo que deben recibir los destinatarios cuando AMC se ponga en contacto con ellos. No tiene por qué ser una dirección previamente validada por un servidor de correo en funcionamiento; por ejemplo, AlertaAMC@MiEmpresa.com.
- 10 Continúe con [Inicio del servidor AMC](#) en la página 13.

Inicio del servidor AMC

Una vez iniciado el servidor, antes de iniciar el cliente asegúrese de que la detección de red haya finalizado. Cuando el servidor termina la detección de red y está listo para recibir las conexiones, el mensaje `Ready . Waiting for commands` aparece encima de la línea de comandos en la ventana del servidor.

Inicio de un servidor Windows

Inicie el servidor al principio de la sesión de gestión SAN, pero no salga de él cuando haya terminado, déjelo encendido.

Para iniciar el servidor AMC en un sistema Windows

- 1 Seleccione **Inicio, Programas**.
- 2 A continuación, seleccione **ADIC Management Console**. Finalmente, elija **Server**.

Si ha instalado el servidor AMC en una ruta no predeterminada, inícielo desde allí.

Una vez iniciado el servidor, se abrirá una ventana en el monitor. Cuando aparezca el mensaje `Ready . Waiting for commands` delante de la línea de comandos sabrá que ha finalizado la detección de red.

Si su configuración consta de un gran número de segmentos de red grandes o remotos, la detección puede tardar varios minutos en finalizar.



Nota

No cierre la ventana del servidor. Para apagar el servidor, siga el procedimiento descrito en [Apagar el servidor AMC](#) en la página 20.

- 3 Continúe con [Inicio del cliente AMC](#) en la página 16.

Inicio de un servidor UNIX

Inicie el servidor al principio de la sesión de gestión SAN, pero no salga de él cuando haya terminado, déjelo encendido.

Para iniciar el servidor AMC en un sistema UNIX

- 1 Escriba `Server` en una ventana del terminal y pulse **Enter**.

```
Server <enter>
```



Nota

Es necesario que la "S" de "Server" esté en mayúscula.

Aparecerá la ventana del servidor.

Si su configuración consta de un gran número de segmentos de red grandes o remotos, la detección puede tardar varios minutos en finalizar.



Nota

No cierre la ventana del servidor. Para apagar el servidor, siga el procedimiento descrito en [Apagar el servidor AMC](#) en la página 20.

- 2 Continúe con [Inicio del cliente AMC](#) en la página 16.

Instalación del cliente AMC

El cliente AMC se utiliza para gestionar la red SAN.

Antes de instalar el cliente

Si ya ha instalado una instancia del cliente y desea instalar otra, o si ya ha instalado una instancia del servidor AMC utilizando la opción **Server Only**, continúe con [Instalación de un cliente AMC en Windows](#) en la página 15 o con [Instalación de un cliente UNIX](#) en la página 15.

Si ya ha instalado una instancia de AMC utilizando la opción **Full** y no desea instalar otro cliente, continúe con [Inicio del cliente AMC](#) en la página 16.

Si no lo ha hecho, siga los pasos descritos en [Antes de instalar AMC](#) en la página 11 e [Instalación del servidor AMC](#) en la página 11 antes de continuar con la instalación del cliente.

Instalación de un cliente AMC en Windows

Los clientes AMC se pueden ejecutar con Windows NT, Windows 2000 o Windows XP.

Para instalar el cliente en un sistema Windows

- 1 Cargue el CD con el producto.
- 2 Haga clic en el vínculo para la instalación que aparece debajo de ADIC Management Console 4.2.
- 3 Haga clic en **OK**.

Así se iniciará el programa "InstallAnywhere", que realizará varias preguntas durante la instalación.

- 4 Cuando se le pida que elija una opción de instalación, seleccione **Client Only**.
- 5 Continúe con [Inicio del cliente AMC](#) en la página 16.

Instalación de un cliente UNIX

Los clientes AMC se pueden ejecutar con Solaris, Linux, HP-UX o AIX.

Para instalar el cliente en un sistema UNIX

- 1 Cargue el CD con el producto.
- 2 Haga clic en el vínculo para la instalación que aparece debajo de ADIC Management Console 4.2.
- 3 Haga clic en **OK**.
- 4 Abra la carpeta y copie el archivo de imagen en una carpeta temporal del host.



ATENCIÓN

Compruebe que tiene suficiente espacio (80 MB aproximadamente) en el directorio temporal para poder finalizar la instalación. Para los sistemas Solaris, si el directorio /tmp no es lo suficientemente grande para que InstallAnywhere se ejecute, la instalación fallará aunque el directorio se cambie de tamaño después.

Ajuste la variable de entorno IATEMPDIR para obtener un nombre de directorio lo bastante grande. El programa “InstallAnywhere” utilizará ese directorio en lugar de /tmp.

Para ajustar la variable para Bourne shell (sh), ksh, bash y zsh, realice los siguientes pasos:

```
$IATEMPDIR=/your/free/space/directory $ export
IATEMPDIR -
```

Para ajustar la variable para C shell (csh) y tcsh, realice los siguientes pasos:

```
$ setenv IATEMPDIR /your/free/space/directory
```

- 5 Desde la carpeta temporal, escriba: `chmod 777 <nombre de archivo>;` por ejemplo,
`chmod 777 MC400SOL.bin`
- 6 Si la carpeta temporal NO se encuentra en la ruta del usuario, escriba `[espacio] ./<nombre de archivo>;` por ejemplo,
`./MC400SOL.bin`
De esta forma se iniciará la instalación desde el directorio actual.
Si la carpeta temporal se encuentra en la ruta del usuario, sólo tiene que escribir: `<nombre de archivo>` (incluyendo la extensión); por ejemplo,
`MC400SOL.bin`
Así se iniciará el programa “InstallAnywhere”, que realizará varias preguntas durante la instalación.
- 7 Cuando se le pida que elija una opción de instalación, seleccione **Client Only**.
- 8 Continúe con [Inicio del cliente AMC](#) en la página 16.

Inicio del cliente AMC

Para gestionar la red SAN, conecte el cliente a una instancia del servidor AMC remoto respecto a Scalar i2000 o Pathlight VX.



Nota

Cuando un servidor está listo para recibir conexiones, el mensaje `Ready .` `Waiting for commands` aparece encima de la línea de comandos en la ventana del servidor.

Utilice uno de los siguientes procedimientos para iniciar el cliente según el sistema operativo que éste utilice:

Inicio de un cliente Windows

Si inicia el cliente antes de que el servidor remoto haya completado la detección, el cliente no se conectará al servidor.

Para iniciar un cliente Windows

- 1 Si ha aceptado los ajustes predeterminados durante la instalación, seleccione el grupo de programas **ADIC Management Console** en el menú **Inicio** para ver el icono del cliente. Si eligió un grupo de programas distinto al predeterminado, acceda a él.
- 2 Seleccione **Client** para iniciar el programa.

Cuando se inicie el cliente, aparecerán las ventanas **ADIC Management Console** y **Receive Event Traps**. Cuando se reciben capturas de eventos, los mensajes correspondientes aparecen en la ventana **Received Event Traps**. No es posible cerrar la ventana **Received Event Traps** mientras el cliente se está ejecutando. No obstante, sí se puede minimizar.

- 3 Si el servidor remoto se está ejecutando en un sistema que también es remoto respecto al cliente, la ventana del cliente mostrará un aviso para que se conecte a un servidor. Continúe con [Conexión al servidor](#) en la página 18.

Si el servidor remoto se está ejecutando en el mismo sistema que el cliente, la conexión al servidor será automática. La ventana del cliente mostrará el cuadro de diálogo de inicio de sesión. Continúe con [Inicio de sesión](#) en la página 18.



ATENCIÓN

Después de iniciar la sesión, configure otro administrador de SAN. Al configurar un administrador de SAN, el nombre de usuario predeterminado admin quedará inhabilitado. Consulte [Agregar una nueva cuenta de usuario en la página 43](#).

Inicio de un cliente UNIX

Si inicia el cliente antes de que el servidor remoto haya completado la detección, el cliente no se conectará al servidor.

Para iniciar un cliente UNIX

- 1 Para iniciar un cliente HP-UX, AIX, Solaris o Linux, inicie una ventana del terminal y escriba

```
Client <enter>
```

y pulse **Enter**.



Nota

Es necesario que la "C" de "Client" esté en mayúscula.

Cuando se inicie el cliente, aparecerán las ventanas **ADIC Management Console** y **Received Event Traps**. Cuando se reciben capturas de eventos, los mensajes correspondientes aparecen en la ventana **Received Event Traps**. No es posible cerrar la ventana **Received Event Traps** mientras el cliente se está ejecutando. No obstante, sí se puede minimizar.

- 2 Si el servidor remoto se está ejecutando en un sistema que también es remoto respecto al cliente, la ventana del cliente le pedirá que se conecte a un servidor. Continúe con [Conexión al servidor](#) en la página 18.

Si el servidor se está ejecutando en un sistema local respecto al cliente, la conexión al servidor será automática. La ventana del cliente mostrará el cuadro de diálogo de inicio de sesión. Continúe con [Inicio de sesión](#) en la página 18.

Conexión al servidor

Si el cliente es local respecto al servidor, la conexión será automática.

Para conectarse a un servidor AMC remoto una vez iniciado el cliente

- 1 En el cuadro de diálogo **Connect to Server**, escriba el nombre de la red o la dirección IP del servidor remoto.



Nota

Si escribe la dirección IP de una biblioteca Scalar i2000 o Pathlight VX, no podrá gestionar la red SAN. Los servidores instalados en estas bibliotecas se utilizan únicamente para gestionar sus operaciones.

- 2 Seleccione **OK**.



Nota

Si el cliente ya está iniciado, puede visualizar el cuadro de diálogo seleccionando el menú **Session** y a continuación, **Connect to Server**.

- 3 Continúe con [Inicio de sesión](#) en la página 18.

Inicio de sesión

El cuadro de diálogo **Log On** aparece automáticamente cuando se establece una nueva conexión al servidor. También puede aparecer si se selecciona **Session** y a continuación, **Log On**. El cuadro de diálogo **Logon** también aparece al hacer clic en el botón **Log On** de la barra de herramientas.



Para iniciar una sesión

En el cuadro de diálogo **Logon**, escriba “admin” como nombre de usuario. En el campo de contraseña, escriba “password” si es la primera vez que inicia una sesión.



ATENCIÓN

Después de iniciar la sesión, configure otro administrador de SAN. Al configurar un administrador de SAN, el nombre de usuario predeterminado admin quedará inhabilitado. Consulte [Agregar una nueva cuenta de usuario en la página 43](#).

Si comete un error al iniciar una sesión, el cuadro de diálogo desaparecerá y en el área **Status/Message Area** de la pantalla aparecerá el mensaje *Unsuccessful log on*. Consulte [Área de estado/mensajes](#) en la página 36. Seleccione **Session > Log On** y vuelva a escribir el nombre de usuario y la contraseña.

Si la sesión se inicia correctamente, el cliente muestra una barra de estado mientras descarga datos del Master Portal (Portal principal). Para obtener más información sobre este portal principal y los portales en general, consulte [El trabajo con portales](#) en la página 47.

El portal principal predeterminado incluye todos los dispositivos detectados, según el archivo de configuración de detección. Cuando se completa la descarga, la pantalla de AMC aparece llena de datos. Para obtener más información sobre esta pantalla, consulte [Lectura de los paneles de información de gestión de la red SAN](#) en la página 26.

Name	Value
World Wide Node Name	10000060:4517045B
IP Address	172.16.76.166
Firmware Revision	4.40.11
Serial Number	601115
Log Size	2047
Serial Baud Rate	19200
Health Check Level	2
Health Check Interval	60
Receive Event Traps	Enabled
Ethernet Type	100 base-T
UDP Port	164
Extended SFM Enabled	Yes
VPM Enabled	No
Data Mover Module Enabled	No

Up Time: 15 days 23:58:42

TRAP !

Cierre de sesión

Cierre su sesión cuando haya terminado de utilizar AMC. No es necesario reiniciar el cliente para iniciar la siguiente sesión de gestión.

Para cerrar la sesión

- 1 Seleccione el menú **Session** y a continuación, **Log Off**.

Aparecerá un cuadro de diálogo de advertencia.

También puede iniciar el cuadro de diálogo **Log Off** seleccionando el botón **Log Off** de la barra de herramientas.



Aparecerá el cuadro de diálogo de advertencia.

- 2 Si realmente desea cerrar la sesión, haga clic en **Yes**. Si elige **Yes** y ha cambiado la vista actual, se le pedirá que la guarde.
Aparecerá el cuadro de diálogo **Save Current View**.
Seleccione **No** si ha decidido no cerrar la sesión. Si elige **No**, regresará a la vista.
- 3 Seleccione **Yes** si ha realizado cambios en la vista que desee guardar.
Seleccione **No** si no desea guardar los cambios.

Salir del cliente AMC

El comando **Exit** detiene la aplicación cliente AMC y cierra su ventana.

Utilice el comando **Exit** si desea reiniciar la aplicación cliente la próxima vez que utilice AMC. Generalmente, sólo se cerrará la sesión y el cliente continuará ejecutándose entre sesiones.

Para salir de AMC

- 1 Una vez cerrada la sesión, seleccione **Session > Exit**.
Aparecerá el cuadro de diálogo **Exit**.
- 2 Haga clic en **Yes** para salir. La vista se cerrará.
Seleccione **No** si ha cambiado de opinión.
Si hace clic en **No**, regresará a la vista cerrada anteriormente.

Apagar el servidor AMC

El procedimiento para apagar el servidor AMC es igual para todas las plataformas.



Nota

No es posible apagar el servidor incluido en los modelos Scalar i2000 o Pathlight VX.

- 1 Cuando haya cerrado la sesión (consulte [Cierre de sesión](#) en la página 19) y salido del cliente (consulte [Salir del cliente AMC](#) en la página 20), coloque el puntero en la línea de comando de la ventana del servidor.
- 2 Escriba "exit" y pulse la tecla **Enter**.
La ventana del servidor desaparecerá.

4

Preguntas frecuentes

En esta sección se ofrece respuesta a las preguntas planteadas con mayor frecuencia.

¿Qué es una red SAN?

Una SAN (Storage Area Network) es una red que conecta servidores o estaciones de trabajo con matrices de discos, sistemas de copia de seguridad en cinta, conmutadores, puentes y otros dispositivos, como pueden ser las redes de transmisión a gran velocidad (Fibre Channel o Gigabit Ethernet).

¿Qué sucede si no aparece ningún componente de SAN después de instalarlo?

Si no cambia la cadena de ejemplo de segmento de red (1.1.1.1 - 1.1.1.2) que aparece en la pantalla **Configure Discovery Settings** del asistente de instalación, los componentes de SAN no se detectarán.

Siga las instrucciones que se ofrecen en [Detección de la red SAN](#) en la página 63 para cambiar esta cadena y para agregar otras sobre el entorno de red. Agregue una cadena independiente por cada subred. Esa sección también ofrece información sobre cómo volver a detectar la red SAN.

¿Se puede gestionar una red SAN desde una biblioteca Scalar i2000 o un sistema Pathlight VX?

No. En los modelos i2000 y Pathlight VX, AMC sólo está disponible desde un cliente remoto.

¿Es necesario instalar un servidor o un cliente?

Para gestionar la red SAN, debe instalar al menos una instancia del servidor y del cliente AMC y, como mínimo, un sistema remoto. Consulte [Antes de instalar AMC](#) en la página 11. No instale más de una instancia de servidor por equipo cliente. En caso de efectuar una actualización, debe actualizar el servidor y el cliente, de forma que ambos se comuniquen con la mayor eficacia.

Para gestionar una biblioteca Scalar i2000 remotamente (es decir, sin utilizar el panel táctil), debe instalar un cliente SAN.

¿Es posible configurar el correo electrónico si salté ese paso durante la instalación?

Consulte [Configuración del correo electrónico](#) en la página 61.

¿Cómo se interpretan los componentes de la interfaz?

Consulte [Lectura de los paneles de información de gestión de la red SAN](#) en la página 26. Para ver en qué se diferencia la interfaz AMC de la interfaz LMC, consulte la [tabla 1](#) en la página 37.

¿Cómo se crea una cuenta de administrador de red SAN?

Consulte [Agregar una nueva cuenta de usuario](#) en la página 43.

¿Qué es un portal?

Un portal es un conjunto de dispositivos de red de área de almacenamiento que representan el universo particular de un usuario determinado. El portal predeterminado del administrador de una red SAN es el conjunto completo de dispositivos y su almacenamiento asociado en la subred a la que accede AMC. Este portal se conoce como portal principal. El administrador de SAN puede otorgar a otros usuarios privilegios sobre subconjuntos del portal principal.

¿Cómo se crean portales para los usuarios?

Consulte [Creación de un nuevo portal](#) en la página 47.

¿Cómo se crean las cuentas de usuario?

Consulte [Creación, modificación y eliminación de cuentas de usuario](#) en la página 43.

¿Qué privilegios presenta cada tipo de usuario?

Consulte la [tabla 2](#) en la página 42.

¿Cómo se actualiza el firmware?

En el caso del modelo Scalar i2000, utilice LMC. En el caso del modelo Pathlight VX, utilice VLI. Para otros componentes de SAN ADIC, consulte [Actualización del firmware](#) en la página 77.

¿Cómo se modifica la configuración de detección?

Consulte [Detección de la red SAN](#) en la página 63.

¿Cómo se crean políticas?

En el caso del modelo Scalar i2000, utilice LMC. Consulte el *Manual de operador de Scalar i2000*. En el caso del modelo Pathlight VX, utilice VLI. Para otros componentes de SAN, consulte [Configuración de políticas](#) en la página 62.

5

La interfaz de gestión de la red SAN

La interfaz AMC presenta cierto número de menús y botones de barras de herramientas.

Menús

AMC clasifica los comandos de usuario en distintos menús:

- El menú **Session** está formado por comandos que afectan a la conexión establecida en ese momento: conectar al servidor, iniciar y cerrar la sesión, cambiar la contraseña y salir del programa.
- El menú **View** contiene comandos que modifican las representaciones gráficas lógicas de un portal: abrir, guardar, borrar y crear vistas; buscar una vista para un componente determinado así como también, averiguar si otros usuarios pueden acceder a la vista o imprimir informes basados en vistas.
- El menú **Admin** presenta los comandos que afectan a la configuración de la red SAN, como crear y gestionar usuarios, portales, cadenas de comunidad y políticas.
- El menú **Category** está formado por comandos con los que se pueden modificar las categorías (componentes de la SAN organizados en grupos lógicos).
- El menú **Help** permite acceder a la ayuda en pantalla, al cuadro de diálogo con los números de compilación del servidor y el cliente, y al copyright.

Barra de herramientas

La barra de herramientas está formada por seis botones que representan los comandos más utilizados, que están también disponibles en los menús.

- **Log On** abre el cuadro de diálogo **Log On**. Si hay iniciada una sesión de usuario, primero aparecerá un cuadro de diálogo de confirmación para cerrar dicha sesión.
- **Log Off** cierra la sesión del usuario actual tras aceptar la petición de confirmación.
- **Open View** abre un explorador de vistas después de confirmar el cierre de la vista actual.
- **Save Current View** guarda inmediatamente la vista actual. Este botón sólo está habilitado cuando se han realizado cambios en la vista.
- **Close Current View** cierra la vista actual tras confirmar la petición de cierre. Si se han producido cambios en la vista, se le pedirá que los guarde primero.
- **Find** abre un cuadro de diálogo en el que se puede buscar un componente de la SAN determinado.

Paneles

La interfaz de AMC está formada por tres paneles de información:

- El panel de árbol muestra una representación jerárquica de los componentes de la red SAN, utilizando convenciones gráficas especiales e información textual para representar la estructura de la red.
- El panel gráfico ofrece una representación no textual de la red SAN, a excepción de los menús que incluyen texto asignados a zonas activas.
- En el panel de datos se enumeran las características de componente, configuración y compilación de los componentes de la red SAN.

Ventana Received Event Traps

Siempre que se está ejecutando AMC, se abre una ventana independiente que muestra las capturas de eventos recibidas. Esta ventana se puede minimizar, pero no cerrar.

Cuando se inicia el cliente SAN AMC, además de la ventana de gestión de la SAN aparece una ventana **Received Event Traps**. Si se reciben capturas de eventos, los mensajes indicándolo aparecen en esta ventana. No es posible cerrar esta ventana si se está ejecutando el cliente, aunque sí se puede minimizar. Para obtener más información sobre las capturas, consulte [Seguimiento y gestión de registros de eventos](#) en la página 68.

Lectura de los paneles de información de gestión de la red SAN

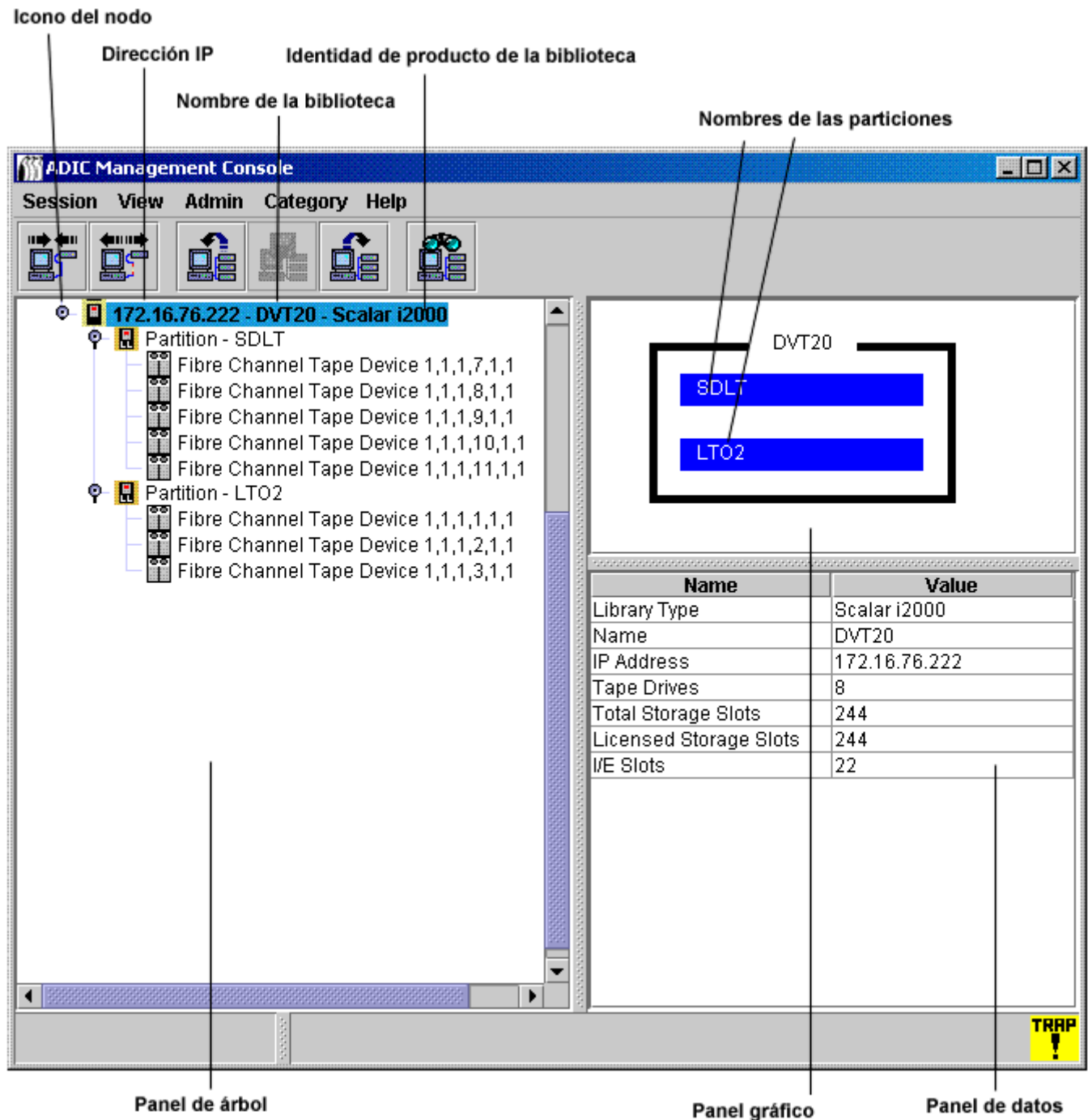
La pantalla principal de AMC está formada por tres paneles.

- El panel de vista de árbol enumera los controladores SNC y las bibliotecas Scalar con SNCs ordenándolos según su dirección IP. En la pantalla aparece codificada información detallada sobre cada configuración, tanto verbal como gráficamente.
- Cuando un SNC o una biblioteca Scalar se selecciona en la vista de árbol, el panel gráfico representa información de configuración para esa unidad en formato no verbal.
- Cuando un SNC o una biblioteca Scalar se selecciona en la vista de árbol, el panel de datos presenta información de estado sobre esa unidad en formato de tabla.

Panel de árbol

El panel izquierdo de la pantalla interactiva se conoce como panel de árbol. En él se ordenan jerárquicamente los componentes de la red SAN. La pantalla de los productos de la serie de plataforma inteligente, como los modelos Scalar i2000 o Pathlight VX, funcionan de forma distinta a las pantallas de otros componentes de la red SAN.

Figura 1 Representación de AMC en el modelo Scalar i2000



Scalar i2000

La cadena del panel de árbol que representa la biblioteca física Scalar i2000 está formada por tres elementos: la dirección IP, el nombre de la biblioteca (por ejemplo, **adilib**) y la identidad de producto de la biblioteca (**Scalar i2000**). Haga clic en el icono del nodo situado a la izquierda de la biblioteca Scalar i2000 para mostrar los dispositivos (unidades) y particiones asociados. En la [figura 1](#), todos los nodos aparecen ampliados. El icono del nodo sirve además para expandir y contraer la visualización de sus elementos.

La biblioteca Scalar i2000 de la [figura 1](#) está formada por una biblioteca física dividida en dos particiones. En la línea situada bajo la línea de la biblioteca física, la cadena que representa la partición consta de dos elementos: la palabra **Partition** y el nombre de la partición. Las particiones de la [figura 1](#) se llaman **SDLT** y **LTO**. Las cadenas de los dispositivos de cinta están formadas por la frase **SCSI Tape Device** seguida de las coordenadas de ubicación de la unidad. También puede aparecer la frase **Fibre Channel Tape Device**. Para ver una descripción más detallada de estas características, consulte el *Manual de usuario de Scalar i2000*.

Figura 2 Representación de AMC en el modelo Pathlight VX

Icono del nodo

Dirección IP

Nombre de la biblioteca

Producto de la biblioteca

Nombres de las bibliotecas virtuales

The screenshot shows the ADIC Management Console interface. The main window title is "ADIC Management Console" with a menu bar containing "Session", "View", "Admin", "Category", and "Help". Below the menu bar is a toolbar with several icons. The main content area is divided into three panels:

- Panel de árbol (Tree Panel):** Displays a hierarchical tree structure. The root node is "172.16.76.200 - nywp1.adic.com - Pathlight VX". Underneath, there are three "Virtual Library" nodes:
 - Virtual Library - i2k: Contains four drives (i2k_DRIVE_001 to i2k_DRIVE_004).
 - Virtual Library - s100: Contains four drives (s100_DRIVE_001 to s100_DRIVE_004).
 - Virtual Library - s1k: Contains three drives (s1k_DRIVE_001 to s1k_DRIVE_003).
- Panel gráfico (Graphic Panel):** Shows a graphical representation of the library structure. It displays the IP address "nywp1.adic.com" and three blue horizontal bars representing the virtual libraries: "i2k", "s100", and "s1k".
- Panel de datos (Data Panel):** A table with the following data:

Name	Value
Library Type	Pathlight VX
Name	nywp1.adic.com
IP Address	172.16.76.200
Total Virtual Libraries	3
Total Virtual Drives	11

TRRP

Pathlight VX

La cadena del panel de árbol que representa el modelo Pathlight VX es similar tanto en estructura como en funcionamiento a la cadena del modelo Scalar i2000. La [figura 2](#) muestra la biblioteca Pathlight VX como nodo ampliado. Está formada por una biblioteca virtual llamada **nyvp1_lib1**. Esta biblioteca consiste en tres unidades. Para obtener más información acerca de las bibliotecas virtuales y las unidades, consulte la ayuda en pantalla de Pathlight VX.



Nota

Para llevar a cabo las operaciones de la biblioteca, a diferencia de las operaciones de la red SAN, debe hacer clic con el botón derecho del ratón en el panel de árbol de la biblioteca Scalar i2000 o Pathlight VX. Aparecerá un menú formado únicamente por **Library Manager** o **VLI**. Haga clic en **Library Manager** (o **VLI**) para que se inicie.

SNCs y bibliotecas Scalar 24, 100, 1000 y 10K

La cadena del panel de árbol que representa un SNC independiente o un modelo Scalar 24, Scalar 100, Scalar 1000 o Scalar 10K está formada por tres elementos: la dirección IP de la unidad, su nombre y su familia de productos.

Haga clic en el icono del nodo situado a la izquierda del gráfico de la biblioteca para mostrar los controladores de almacenamiento en red (SNC) agregados.



Nota

Un SNC se considera agregado cuando se ha instalado en una biblioteca, a diferencia de los SNC que funcionan como unidades independientes.

El icono del nodo sirve además para expandir y contraer la visualización de sus elementos.

- Las bibliotecas de cintas Scalar 10K contienen múltiples SNCs.
- Las bibliotecas de cintas Scalar 1000 contienen tres SNCs.
- Las bibliotecas de cintas Scalar 100 contienen un SNC.
- Las bibliotecas de cintas Scalar 24 contienen un SNC.

Los nodos de SNC se expanden para mostrar canales. Los canales se expanden para mostrar los hosts y dispositivos conectados. Los iconos de nodo de canales y SNCs también permiten expandir y contraer su visualización haciendo clic sobre ellos. Consulte la [figura 3](#).

Figura 3 Representación en AMC de SNCs y componentes del sistema

The screenshot displays the ADIC Management Console interface. On the left, a tree view shows the system hierarchy under 'Default View - Portal1.2 - local'. The selected node is '172.16.76.215 - SN601193 - Pathlight 5000', which is highlighted in blue. Below it, several SCSI channels and Fibre Channels are listed, along with their associated devices like 'Medium Changer', 'Tape Device', and various switches and hosts.

On the right, a graphical representation shows the physical layout of the system components, including 'Cambiador de medios', 'Dispositivos de cinta', 'SNC', and 'Hosts'. The selected SNC (172.16.76.215) is highlighted in a blue box.

Name	Value
World Wide Node Name	10000060:451704A9
IP Address	172.16.76.215
Firmware Revision	4.40.13
Serial Number	601193
Log Size	2047
Serial Baud Rate	19200
Health Check Level	2
Health Check Interval	3
Receive Event Traps	Enabled
Ethernet Type	100 base-T
UDP Port	164
Extended VPS Enabled	Yes
VPM Enabled	Yes
Data Mover Module Enabled	Yes

Up Time: 12 days 17:55:50

La [figura 3](#) en la página 30 muestra un panel de árbol con diversos elementos expandidos. Como se ha seleccionado el SNC 5100 con la dirección IP 172.16.76.215, aparece resaltado en azul en el panel de árbol. Este controlador está agregado a una biblioteca Scalar 1000. Si desea ver una lista de los iconos utilizados en el panel gráfico y en el panel de árbol, consulte la [figura 4](#).

Figura 4 Iconos utilizados en el panel gráfico y en el panel de árbol

Símbolo	Nombre
	Dispositivo de disco
	Dispositivo de cinta
	Cambiador de medios
	SNC 4XXX, 5XXX, 6XXX
	SNC 3000
	Scalar i2000, Pathlight VX
	Host
	Biblioteca de cintas Scalar
	Categoría

Para ver un resumen de los gráficos de modo de canal, consulte la [figura 5](#).

Figura 5 Gráficos de modo de canal

Icono del panel de árbol	Modo	Tipo de canal
Azul	Objetivo	Diferencial de alto voltaje SCSI
Verde	Iniciador	Diferencial de alto voltaje SCSI
Azul	Objetivo	Diferencial de bajo voltaje SCSI
Verde	Iniciador	Diferencial de bajo voltaje SCSI
Azul	Objetivo	Fibra óptica de onda corta
Verde	Iniciador	Fibra óptica de onda corta
Morado	Objetivo/Iniciador	Fibra óptica de onda corta

Target es el modo predeterminado para Fibre Channel. Se muestran en color azul. Cuando los canales están ajustados en modo **Target**, es posible ver los host conectados. Primero debe ejecutar el software de registro de host (HRS). Para instalarlo, póngase en contacto con su representante del servicio técnico.

El color verde señala que el canal se encuentra en modo **Initiator**. **Initiator** es el modo predeterminado para los canales SCSI. Cuando los canales se ajustan a **Initiator** podrá ver los dispositivos conectados.

Además de los modos **Target** e **Initiator**, los canales Fibre Channel pueden funcionar en modo **Target and Initiator**. Cuando ése es el caso, el icono de Fibre Channel es de color morado.

AMC muestra los hosts SCSI y Fibre Channel que ejecutan el software HRS. Consulte el *Manual de usuario* del controlador SNC para obtener información sobre la instalación del software HRS.

En el panel de árbol, haga clic con el botón derecho del ratón en un canal Fibre Channel, un canal SCSI, un dispositivo o el controlador SNC para ver el menú contextual correspondiente al elemento elegido. Para obtener información sobre estos menús, consulte las siguientes secciones:

- [Lectura de información sobre una biblioteca](#) en la página 66
- [Gestión del equipo de red SAN](#) en la página 75
- [Gestión de Fibre Channel](#) en la página 83
- [Gestión del canal SCSI](#) en la página 81
- [Gestión de dispositivos](#) en la página 87

Si se actualizan los datos en el panel de árbol, también se actualizarán el panel gráfico y el de datos.

Numeración de los dispositivos

La [figura 3](#) en la página 30 muestra dispositivos en distintos canales. Todos ellos están numerados de acuerdo con un esquema estándar. Para interpretar la numeración, consulte la [figura 6](#).

- El número situado delante de los dos puntos dentro de los paréntesis angulares representa el ID objetivo (o ID SCSI).
- El número situado tras los dos puntos dentro de los paréntesis angulares representa el LUN (número de unidad lógica) de dispositivo. Este número también se conoce como LUN objetivo.
- El número situado tras el guión es el LUN asignado. Este número también se conoce como LUN interno.

Figura 6 Convenciones para la numeración de dispositivos



En los canales SCSI se utilizan los ID 0 a 15; los LUN de dispositivo 0 a 31 se asocian a cada ID. El LUN asignado es el LUN que el dispositivo asigna durante la detección. El ID objetivo y el LUN de dispositivo son conceptos físicos.

El LUN asignado es un concepto de gestión y el usuario lo puede manipular para crear mapas de dispositivos privados. Consulte los comandos enumerados bajo **Setup > Device** en el *Manual de operador de Scalar i2000* de la biblioteca Scalar i2000. En el caso de bibliotecas con SNCs, consulte [Edición de mapas de dispositivos](#) en la página 87, [Utilización de Scalar Firewall Manager \(SFM\)](#) en la página 96, [Utilización de eVPS](#) en la página 101 o [Utilización de VPM](#) en la página 107.

En el caso de unidades Scalar i2000, compare la designación de dispositivos de cintas en el panel gráfico de AMC con el cuadro de diálogo **Monitor > Drives** que muestra la consola LMC. Para más información acerca de las convenciones de numeración para el modelo Scalar i2000, consulte el *Manual de usuario de Scalar i2000*.

En cuanto al modelo Pathlight VX, las unidades virtuales se crean y numeran secuencialmente dentro de las bibliotecas virtuales. Los sistemas Pathlight VX integran unidades virtuales, bibliotecas y medios con sus equivalentes físicos. Para más información sobre cómo interpretar la interfaz del sistema Pathlight VX, consulte la ayuda en pantalla del modelo Pathlight VX.

Panel gráfico

En el lado derecho de la pantalla, por encima del panel de datos, hay una representación gráfica de la configuración en red del SNC seleccionado. Esta representación es el panel gráfico.

En el caso de los SNC independientes y las bibliotecas Scalar que incluyen algún dispositivo de almacenamiento en red, al seleccionar el SNC, un canal, un host o un dispositivo en el panel de árbol, el icono asociado aparecerá resaltado en azul en el panel gráfico. Los canales SCSI no seleccionados se dibujan en color negro. Consulte la [figura 3](#) en la página 30. Los canales Fibre Channel se dibujan en color amarillo.

Si se selecciona el sistema Scalar i2000 o el Pathlight VX también aparece una imagen en el panel gráfico. Un rectángulo marcado en negro representa la biblioteca física Scalar i2000, dentro de la cual un determinado número de barras azules representa el número de particiones asociado. También se utiliza un rectángulo marcado en negro para representar la biblioteca física de la solución Pathlight VX, dentro de la cual un número determinado de barras azules representa el número de bibliotecas virtuales asociado. Consulte la [figura 1](#) en la página 27 y la [figura 2](#) en la página 28.

En el panel gráfico, haga clic con el botón derecho del ratón en un canal Fibre Channel, un canal SCSI, un dispositivo o el controlador SNC para ver el menú contextual correspondiente al elemento elegido. Para obtener información sobre estos menús, consulte las siguientes secciones:

- [Lectura de información sobre una biblioteca](#) en la página 66
- [Gestión del equipo de red SAN](#) en la página 75
- [Gestión de Fibre Channel](#) en la página 83
- [Gestión del canal SCSI](#) en la página 81
- [Gestión de dispositivos](#) en la página 87

Panel de datos

En la parte derecha de la pantalla, bajo el panel gráfico, aparece una representación de la información de estado seleccionada en forma de tabla. Se trata del panel de datos.



Nota

LMC permite acceder a los datos de estado de la biblioteca Scalar i2000. Los datos que ofrece la Library Management Console (LMC) no son iguales a los datos ofrecidos por el panel de datos de la interfaz AMC, y se muestran en tablas individuales. Para más información, consulte el *Manual de operador de Scalar i2000*. Para acceder a la información de estado del modelo Pathlight VX se utiliza la interfaz VLI. Para más información al respecto, consulte la ayuda en pantalla de la VLI.

Cuando se selecciona una biblioteca en el panel de árbol, en el panel de datos aparece la siguiente información recopilada por la unidad de gestión remota (RMU) de la biblioteca:

Global Status	Estado de resumen actual de la biblioteca: Unknown, OK, Degraded o Failure
Last Global Status	Último estado de resumen de la biblioteca: Unknown, OK, Degraded o Failure
SNMP Timeout	Consulte la documentación de la biblioteca correspondiente.
Agent Modifiers	Consulte la documentación de la biblioteca correspondiente.

Refresh rate	Consulte la documentación de la biblioteca correspondiente.
IP Address	Una dirección única de protocolo de Internet
Host Name	Nombre de host DNS (Domain Name Server) de la RMU
RMU Version	Nivel actual del firmware de la biblioteca
Shutdown State	Estado de apagado actual de la biblioteca: Other, Unknown, Normal, Powerfail, Errorreboot
Last Shutdown State	Último estado de apagado de la biblioteca: Other, Unknown, Normal, Powerfail, Errorreboot
Error Code	Valor entero suministrado por algunos códigos de acción de servicio
Error Data	Parámetro que hace más preciso el código de acción de servicio
Service Action Code	Código utilizado para el diagnóstico
Service Tag	Número de identificación de la configuración original

Cuando se selecciona un SNC, la parte inferior del panel de datos muestra la siguiente información:

World Wide Name	Un nombre de nodo único global
IP Address	Una dirección única de protocolo de Internet
Firmware Revision	Un número en formato xx.xx.xx que indica el nivel del firmware del SNC
Número de serie	Número asignado al SNC durante la fabricación
Log Size	Tamaño del archivo de registro del SNC
Serial Baud Rate	Velocidad de la conexión HyperTerminal
Health Check Level	Nivel al que se establece la comprobación de estado, 0-4
Health Check Interval	Intervalo entre comprobaciones de estado, en minutos
Receive Event Traps	Estado -- Enabled o Disabled
Ethernet Type	10-base T o 100-base T
UDP Port	Puerto del Protocolo de datagrama de usuario (UDP) en el que se reciben las capturas SNMP
VPS Enabled SFM Enabled	Yes (habilitado) o No (inhabilitado)
VPM Enabled	Yes (habilitado) o No (inhabilitado)
Data Mover Module Enabled	Yes (habilitado) o No (inhabilitado)

Cuando se selecciona un canal SCSI, la parte inferior del Panel de datos muestra la siguiente información:

Channel Type	Low Voltage o High Voltage, Single-Ended o Differential
Channel Mode	Target o Initiator
Host ID (si el canal está en modo Initiator)	SCSI Bus Channel ID
Termination	Estado -- Enabled o Disabled
Max Width	Ancho de bus, en bits
Max Speed	Velocidad del bus en megahercios
Status	Estado -- Operational u Offline
Max IDs per Bus (si el canal está en modo Initiator)	Número de IDs SCSI permitidos
Max LUNs per ID (si el canal está en modo Initiator)	Número de LUNs SCSI permitidos

Cuando se selecciona Fibre Channel, la parte inferior del panel de datos muestra la siguiente información:

World Wide Port Name	Identificador de 64 bits único asignado a este puerto
World Wide Node Name	Identificador de 64 bits único asignado por el fabricante
Número de serie	Número asignado al conector de FC durante la fabricación
Media	Short Wave o Long Wave, Dual PMC o Single PMC o tipo GBIC
Firmware Revision	Versión de firmware del controlador de FC
Port Type	Point-to-Point (N_Port), Fabric loop (NL_Port), Fabric_Attached (N_Port) o None
Port Mode	Public o Private, Initiator o Target
Address Identifier	Dirección arbitrada de bucle físico (AL_PA)
Host Type	Sistema operativo del host conectado
Loop ID	0-125
Tamaño de trama	512, 1024 o 2048
Frame Buffer Size	Espacio de almacenamiento, generalmente más grande que un cuadro simple
Connection	Opciones de conexión para chips de FC
Max Speed	1 GB o 2 GB
Status	Ready o Not Ready
Link Error Statistics	Encabezado: los números subsiguientes son errores contados por el SNC en canal full duplex entre dos conexiones Fabric de red.
Link Failure Count	Conteos utilizados en el diagnóstico

Loss of Sync Count	Conteos utilizados en el diagnóstico
Loss of Signal Count	Conteos utilizados en el diagnóstico
Primitive Sequence Protocol Error Count	Palabra de transmisión que contiene información especial de control. Se reconoce una secuencia primitiva cuando se reciben tres palabras de transmisión del mismo valor.
Invalid Transmission Word Count	La palabra de transmisión tiene 40 bits, la menor unidad de información transmitida.
Invalid CRC Count	Comprobación de redundancia cíclica, un algoritmo de detección de errores.

Cuando se selecciona un dispositivo, la parte inferior del panel de datos muestra la siguiente información:

Vendor ID	Nombre del proveedor
Product ID	Nombre del producto, asignado por el proveedor
Revision	Número de versión del proveedor
Número de serie	Número asignado al dispositivo durante la fabricación
Removable	Yes o No
Capacidad	Para dispositivos de disco, número de bloques
Block Size	Para dispositivos de disco, el tamaño del bloque
Width	Para dispositivos de cinta, la anchura del bus en bits
Speed	Para dispositivos de cinta, la velocidad del bus

Área de estado/mensajes

El área situada en el extremo inferior de la pantalla se utiliza para presentar los mensajes de estado. Se denomina **Status/Message Area (área de estado/mensajes)**.

En la esquina inferior izquierda del **Status/Message Area** se muestra el tiempo de encendido del SNC. **Up Time** indica cuántas horas, minutos y segundos han transcurrido desde la última inicialización.

Gestión de la biblioteca o gestión de la red SAN

Ciertas utilidades de la red SAN disponibles en LMC o VLI pueden estar también disponibles en AMC con un nombre distinto.

Si desea ver un resumen de las distintas herramientas y su disponibilidad, consulte la [tabla 1](#).

Tabla 1 Herramientas de configuración y utilidades análogas por el tipo de interfaz

Funciones	ADIC Management Console	Library Management Console	Virtual Library Interface
Ajuste de ID SCSI	Para canales: menú SCSI Channel ¹	Para unidades: Setup > Device > IDs ²	No aplicable
Ajuste de ID de bucle de FC	Para canales: menú Fibre Channel ¹	Para unidades: Setup > Device > IDs ²	No aplicable
Zona de canales	menú SNC ¹ > Access options	(sólo biblioteca con tarjetas de E/S) Setup > Device > FC Host	No aplicable
SFM	menú SNC ¹ > Access options	No aplicable	No aplicable
eVPS	menú SNC ¹ > Access options	Setup > Device > Access > FC Host	No aplicable
VPM	menú SNC ¹ > Access options menú SCSI Channel ¹	Setup > Device > Access > SCSI Host	No aplicable
Ajustes del canal SCSI	menú SCSI Channel ¹	Setup > Connectivity > Port Configuration	No aplicable
Ajustes de Fibre Channel	menú Fibre Channel ¹	Setup > Connectivity > Port Configuration	Setup > Port Configuration
Actualización de firmware de dispositivo	menú Device ¹	Tools > Update Software	No aplicable
Actualización de firmware de SNC	menú SNC ¹	Tools > Update Software	No aplicable
Actualización de firmware de biblioteca	No aplicable	Tools > Update Software ³	No aplicable
Registro de eventos	menú SNC ¹ > Events	No aplicable	No aplicable
Notificación de eventos	menú Admin > Policy configuration	Setup > Notification	Setup > Notification
Estado de capturas	No aplicable	Tools > Capture Snapshot	Tools> Capture State
Comprobación de estado	menú SNC ¹ > Health Check	Setup > Connectivity > Datapath conditioning	Tools > System Status

1 Haga clic con el botón derecho del ratón en el componente (SNC) para que aparezca el menú contextual. Scalar i2000 sólo dispone de una opción de menú contextual, Library Manager. Pathlight VX sólo tiene una opción de menú contextual, la interfaz VLI. 2 Debe estar offline. 3 RCU, MCB y firmware de la unidad.

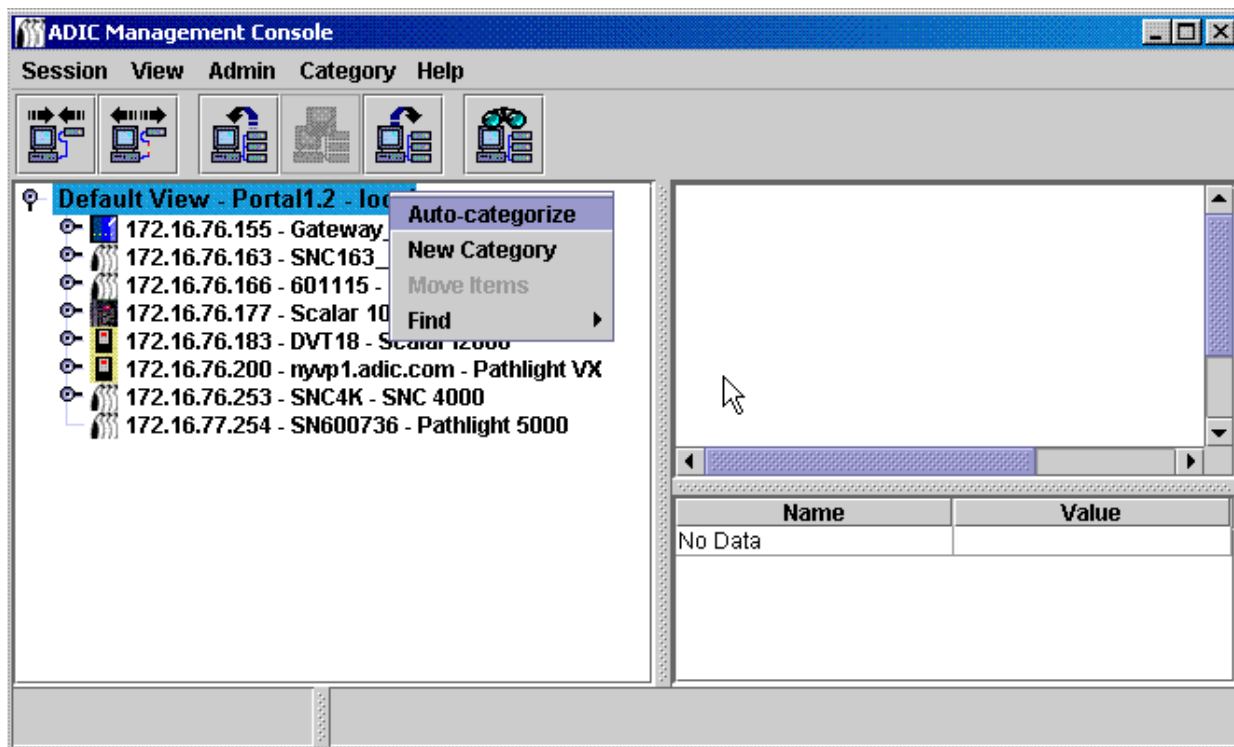
Tabla 1 Herramientas de configuración y utilidades análogas por el tipo de interfaz (continuación)

Latido	menú SNC ¹ > Health Check > Check Heartbeat	No aplicable	No aplicable
Reinicio	menú SNC ¹ menú SCSI Channel ¹ menú Fibre Channel ¹	Change Mode Tools > Connectivity	Operations > System Shutdown
Identificación	menú SNC ¹ > Identify	Tools > Drives Tools > Connectivity	No aplicable
Visualización de panel de LEDs	menú SNC ¹ > Show LED Panel	No aplicable	No aplicable
Actualización de datos	menú SNC ¹ menú SCSI Channel ¹ menú Fibre Channel ¹	No aplicable	No aplicable
Habilitación de funciones	menú SNC ¹ > Feature Enable	Setup > Licenses	Setup > License
Obtención de datos ambientales	menú SNC ¹ > Get Environmental Data	No aplicable	Tools > System Status
<p>1 Haga clic con el botón derecho del ratón en el componente (SNC) para que aparezca el menú contextual. Scalar i2000 sólo dispone de una opción de menú contextual, Library Manager. Pathlight VX sólo tiene una opción de menú contextual, la interfaz VLI. 2 Debe estar offline. 3 RCU, MCB y firmware de la unidad.</p>			

Opciones de gestión de red SAN comunes

Cuando selecciona una vista en el panel de árbol, no se dibuja ninguna representación topológica. Si hace clic con el botón derecho del ratón en el panel de árbol, aparecerán algunas de las operaciones de gestión de SAN más comunes. Consulte la [figura 7](#).

Figura 7 Comandos en la vista inicial del panel de árbol



El panel de datos no muestra dato alguno. Para obtener más información sobre el panel gráfico y el panel de datos, consulte [Lectura de los paneles de información de gestión de la red SAN](#) en la página 26.

Categorización automática

Consulte [Categorización automática de la SAN](#) en la página 51.

Creación de una nueva categoría

Consulte [El trabajo con componentes de categorías](#) en la página 54.

Desplazamiento de elementos

Consulte [Reubicación de elementos mediante el menú](#) en la página 55.

Búsquedas

Consulte [El trabajo con vistas](#) en la página 56.

6

Gestión de cuentas de usuario

AMC permite crear cuentas de usuario con distintos privilegios para cada usuario.

Cambio de la contraseña de administrador

Los administradores de red SAN deben seguir este procedimiento para modificar la contraseña de administrador. Para cambiar la contraseña de un usuario, consulte [Modificación de una cuenta de usuario](#) en la página 44.

Asegúrese de cambiar la contraseña del administrador de red SAN periódicamente.



Nota

Después de utilizar admin/password para iniciar una sesión por primera vez, cree un nuevo usuario en el nivel de administrador de SAN. Consulte [Creación, modificación y eliminación de cuentas de usuario](#) en la página 43.

Para cambiar la contraseña de administrador de SAN

- 1 Inicie la sesión como administrador SAN.
- 2 Seleccione el menú **Session** y a continuación, **Change Password**.
Aparecerá el cuadro de diálogo **Change Password**.
- 3 En la primera línea escriba la contraseña original.
- 4 Apunte la nueva contraseña.
- 5 Escriba la nueva contraseña en la segunda línea.
- 6 Confirme la nueva contraseña escribiéndola otra vez en la tercera línea.
- 7 Si está satisfecho con la nueva contraseña, seleccione **OK**.
Seleccione **Cancel** para cerrar el cuadro de diálogo sin aplicar los cambios.

Descripción de los niveles de privilegios de usuario

Todas las tareas de AMC se asignan a uno o varios de los cuatro perfiles de usuario específicos:

- Administrador de SAN
- Administrador del portal
- Usuario avanzado
- Usuario básico

El usuario básico tiene los derechos de usuario más limitados, sólo incluyen acceso y visualización de los portales asignados a él.

Los usuarios avanzados tienen los mismos derechos que los usuarios básicos más la capacidad de clasificar por categorías los portales asignados, guardar distintas vistas y utilizar todas las herramientas de AMC (a excepción de Virtual Private Map, VPM) para configurar el acceso. No obstante, no pueden crear, modificar ni eliminar usuarios, portales o políticas.



Nota

Todas las SAN que incluyen los sistemas Scalar i2000 y Pathlight VX presentan opciones de configuración distintas de aquellas SAN que no incluyen los sistemas Scalar i2000 y Pathlight VX. Consulte la [tabla 2](#) para ver una comparación comando a comando.

Los administradores de portal pueden llevar a cabo las tareas propias de los usuarios básicos y avanzados, y utilizar todas las herramientas de configuración de AMC. También pueden crear, modificar o eliminar usuarios básicos y avanzados, así como subportales de los portales a los que tengan acceso. No pueden crear políticas. Tampoco pueden crear usuarios en el nivel de administrador de portal ni en el de administrador de SAN. No pueden acceder al portal principal.

Los administradores de SAN pueden llevar a cabo todas las tareas asignadas al resto de usuarios, así como crear políticas y agregar usuarios en los niveles de administrador de SAN y de administrador de portal. De forma predeterminada, los administradores de SAN tienen acceso al portal principal. La [tabla 2](#) en la página 42 resume las actividades propias de cada usuario según sus privilegios.

Tabla 2 Derechos de usuario según su nivel de privilegios

Derecho	AS ¹	AP ²	UA ³	UB ⁴
Acceder al portal principal	Sí	No	No	No
Crear, modificar o eliminar cualquier AS o AP	Sí	No	No	No
Crear, modificar o eliminar un portal o subportal al que tiene acceso el usuario	Sí	Sí	No	No
Crear, modificar o eliminar cualquier UA o UB	Sí	Sí	No	No
Otorgar acceso de usuario a los portales	Sí	Sí	No	No
Crear, modificar o eliminar cualquier vista de los portales a los que tiene acceso el usuario	Sí	Sí	Sí	No
Crear vistas en los portales a los que tiene acceso el usuario	Sí	Sí	Sí	Sí
Eliminar vistas creadas por el usuario	Sí	Sí	Sí	Sí
Otorgar acceso de usuario a las vistas	Sí	Sí	Sí	No
Configurar, reinicializar, ver y suspender políticas	Sí	No	No	No
Crear nuevas categorías, cambiar el nombre de una categoría, borrarla, mover elementos o mover categorías	Sí	Sí	Sí	No
Configurar la zona de canales	Sí	Sí	Sí	No
Configurar SFM/eVPS	Sí	Sí	Sí	No
Configurar VPM	Sí	Sí	No	No

Tabla 2 Derechos de usuario según su nivel de privilegios (continuación)

Habilitar el organizador de datos	Sí	Sí	Sí	No
Asignar dispositivos	Sí	Sí ⁵	Sí ⁵	No
Configurar canales	Sí	Sí	Sí	No
Cargar configuración	Sí	Sí ⁵	Sí ⁵	No
Cargar firmware	Sí	Sí ⁵	Sí ⁵	No
Reiniciar el equipo de red	Sí	Sí ⁵	Sí ⁵	No
¹ AS=administrador de la red SAN ² AP=administrador del portal ³ UA=usuario avanzado ⁴ UB=usuario básico ⁵ Si el portal definido por el AP o el UA sólo incluye parte del equipo de red al que se aplicará la acción, el derecho sólo se asignará al administrador de la red SAN.				

Creación, modificación y eliminación de cuentas de usuario

A todos los usuarios que no sean administradores de SAN se les deben asignar privilegios para uno o varios portales. Estos subportales se tienen que crear antes de agregar los usuarios. Consulte [El trabajo con portales](#) en la página 47.

Agregar una nueva cuenta de usuario



Nota

Para conocer los privilegios asociados a los distintos comandos, consulte la [tabla 2](#) en la página 42.

Para agregar una nueva cuenta de usuario

- 1 Inicie una sesión como administrador de SAN o administrador de portal.
- 2 Seleccione el menú **Admin**, elija **User** y a continuación, **New**.
- 3 Aparecerá el cuadro de diálogo **New User Account**. Escriba un nombre para la nueva cuenta de usuario.

En los nombres de usuario se distingue entre mayúsculas y minúsculas.



Nota

No puede haber dos usuarios con el mismo nombre de usuario.



ATENCIÓN

Después de iniciar la sesión, configure otro administrador de SAN. Al configurar un administrador de SAN, el nombre de usuario predeterminado admin quedará inhabilitado.

- 4 Escriba la contraseña detrás de **Enter Password** y, después, detrás de **Confirm Password**. Si la contraseña no es idéntica las dos veces, aparecerá una advertencia.
- 5 Asigne al usuario un nivel de privilegios. Las opciones son: SAN Administrator, Portal Administrator, Power User y Basic User. Cuando haya elegido el nivel de privilegios para el usuario, utilice los botones de opciones del cuadro de diálogo **New User Account** para asignarlo.
- 6 Cuando haya terminado de rellenar el cuadro de diálogo **New User Account** dialog box , seleccione **Next**.

Aparecerá el cuadro de diálogo **Grant Portal Access Permission**.

Seleccione o anule la selección de las casillas de verificación según sea necesario hasta asignar el acceso correcto.

Seleccione **Back** para asignar al nuevo usuario un nivel de privilegios distinto.

Seleccione **Cancel** si decide no agregar un nuevo usuario.

- 7 Cuando el acceso esté correctamente asignado, seleccione **Finish**.

Modificación de una cuenta de usuario

Los administradores de SAN y administradores de portal llevan a cabo este procedimiento para modificar los privilegios de otros usuarios. Si desea cambiar su propia contraseña, consulte [Cambio de la contraseña de administrador](#) en la página 41.

Para cambiar la contraseña o los privilegios de un usuario

- 1 Inicie una sesión como administrador de SAN o administrador de portal.
- 2 En el menú **Admin**, seleccione **User** y a continuación, **Modify**.
- 3 Seleccione el nombre del usuario cuyos privilegios desee modificar en el área **Modify User Account**.
- 4 Seleccione **Next**.

Aparecerá el cuadro de diálogo **Password** del proceso **Modify User Account**. De forma predeterminada, aparece seleccionado el botón de opción del nivel de privilegio del tipo de usuario actual.

- 5 Si desea cambiar la contraseña, introduzca la nueva contraseña y vuelva a escribirla para confirmarla. Si no lo desea, continúe con el [paso 6](#).
- 6 Si desea cambiar el nivel de privilegios, seleccione el botón de opción correspondiente al nivel que desee asignar al usuario.

Cuando haya terminado de realizar cambios en el cuadro de diálogo, seleccione **Next**.

- 7 Seleccione la casilla de verificación situada delante de un portal o subportal disponible para permitir el acceso del usuario.

Para eliminar el acceso a un portal, anule la selección de la casilla de verificación.

- 8 Cuando el acceso esté correctamente asignado, seleccione **Finish**.
Seleccione o anule la selección de las casillas de verificación según sea necesario hasta asignar el acceso correcto.
Seleccione **Back** si decide modificar una cuenta de usuario distinta.
Seleccione **Cancel** si decide no modificar ningún privilegio de usuario.

Eliminación de una cuenta de usuario

Para eliminar una cuenta de usuario

- 1 Inicie una sesión como administrador de SAN o administrador de portal.
- 2 En el menú **Admin**, seleccione **User** y a continuación, **Delete**.
- 3 Seleccione el nombre de la cuenta de usuario que desee eliminar.
- 4 Seleccione **Delete**.
- 5 Se actualizará el cuadro de diálogo **Delete User Account**.

El nombre del usuario que acaba de eliminar ya no aparecerá en la lista.

6 Seleccione **OK** para eliminar la cuenta de usuario.

Seleccione **Cancel** para detener el proceso de eliminación.

7

El trabajo con portales

En esta sección se describen los procedimientos de administración de portales. Los portales son conjuntos físicos de bibliotecas y equipos de red SAN disponibles para los usuarios, según los haya definido el administrador de la SAN. El administrador de la SAN puede acceder a todos los equipos y bibliotecas descritos como portal principal.

Creación de un nuevo portal

Los portales se crean para dar acceso a dispositivos, canales, vistas y subportales.

El portal principal está formado inicialmente por todos los componentes de la red SAN detectados cuando el servidor realizó la detección inicial. Generalmente, los administradores de las SAN conservan su acceso al portal principal y al resto de usuarios se le otorga privilegios de acceso a subconjuntos.

Además, se crean grupos lógicos como categorías y se guardan como vistas. Consulte [El trabajo con categorías y vistas](#) en la página 51.

Para crear un nuevo portal

- 1 Inicie una sesión como administrador de SAN o administrador de portal.
- 2 En el menú **Admin**, seleccione **Portal** y a continuación, **New**.
- 3 Seleccione el portal que desee dividir y haga clic en **Next**.

Aparecerá el cuadro de diálogo **New Portal** con una jerarquía de los portales existentes en el servidor. Inicialmente no existen subportales del portal principal predeterminado. Cuando haya creado subportales, haga clic en el nivel de jerarquía apropiado para el nuevo subportal que esté creando.

Poco después se actualizará el cuadro de diálogo **New Portal** para mostrar todos los equipos conectados pertenecientes al portal seleccionado. Los SNC agregados a bibliotecas Scalar se muestran en este cuadro de diálogo, pero no aparecen las bibliotecas propiamente dichas. No obstante, sí se muestran las bibliotecas de plataforma inteligentes, como los sistemas Scalar i2000 y Pathlight VX.

Cuando el usuario asignado a este portal inicia una sesión, las bibliotecas de cinta Scalar asociadas a los SNC aparecen como resultado del proceso de detección.

- 4 Haga clic en el icono de nodo situado delante de la dirección IP o del canal para ver los dispositivos asociados.

Para cerrar el nodo, selecciónelo. Los nodos expandidos pueden estar en la misma pantalla que los nodos contraídos.

- 5 Seleccione las casillas de verificación asociadas a los elementos que desee incluir en el nuevo portal.
Las casillas de verificación de nodo se rellenan automáticamente en los niveles de canal y equipo cuando se seleccionan las casillas de verificación de dispositivos. Aquí se muestran los dispositivos seleccionados para un nuevo portal.
- 6 Seleccione **Next**. Aparecerá el cuadro de diálogo **Portal Name**.
- 7 Escriba un nombre para el nuevo portal. El nombre no debe repetirse.
- 8 Si está satisfecho con el nombre, seleccione **Finish**.
Los nuevos portales aparecerán como subportales en la lista del portal principal.

Modificación de un portal



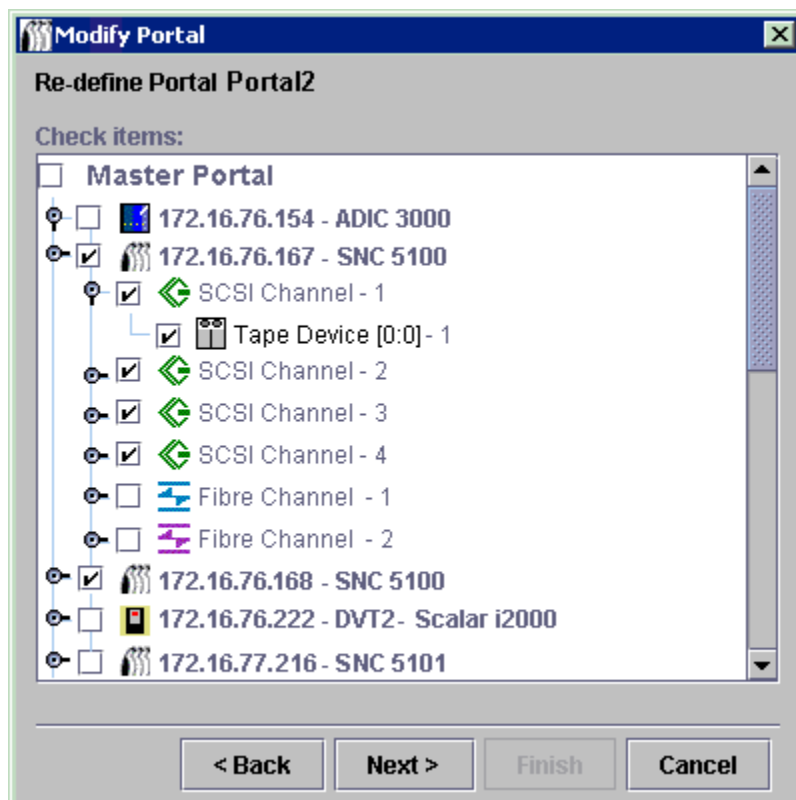
Nota

Los usuarios no pueden modificar el portal principal usando esta herramienta.

Para reasignar el acceso de un portal a dispositivos y canales

- 1 Inicie una sesión como administrador de SAN o administrador de portal.
- 2 En el menú **Admin**, seleccione **Portal** y, a continuación, **Modify**.
- 3 Haga clic en el portal que desee modificar.
- 4 Seleccione **Next**.
- 5 Seleccione o anule la selección de las casillas situadas delante de los equipos de la red SAN para modificar apropiadamente la definición del portal.

En el ejemplo, acceda a todos los canales SCSI en 172.16.76.167 y aparecerán todos los canales del equipo en 172.16.76.168.



Los dispositivos conectados a canales Fibre Channel en 172.16.76.167 no están disponibles.

- 6 Si está satisfecho con los cambios realizados, seleccione **Finish**.

El mensaje *Portal successfully modified* aparecerá en el **Status/Message Area**.

Eliminación de un portal

Un portal se puede eliminar sin perder los datos almacenados. Si se elimina el único portal de un usuario, dicho usuario quedará sin acceso a la red SAN.

Para eliminar un portal

- 1 Inicie una sesión como administrador de SAN o administrador de portal.
- 2 En el menú **Admin**, seleccione **Portal** y a continuación, **Delete**.
- 3 Haga clic en el portal que desee eliminar. El botón **Delete** quedará habilitado.
- 4 Seleccione **Delete** y **OK**. El portal se eliminará.

Establecimiento de permisos para acceder al portal

El administrador de la SAN puede establecer permisos para todos los usuarios. Un administrador de portal puede establecer permisos para los usuarios avanzados y usuarios básicos dentro de los portales que tenga asignado.

Para establecer permisos de acceso a un portal o subportal

- 1 Inicie una sesión como administrador de SAN o administrador de portal.
- 2 En el menú **Admin**, seleccione **Portal** y, a continuación, **Permissions**.
- 3 Seleccione el portal cuyo acceso desee asignar o revocar.
- 4 Seleccione **Next**.
Aparecerá una lista con todos los usuarios con privilegios sobre el portal seleccionado.
- 5 Haga clic en las casillas de verificación de la columna **Assign** para otorgar o revocar el acceso al portal seleccionado.
- 6 Seleccione **Finish**.

8

El trabajo con categorías y vistas

Los componentes de SAN se pueden organizar en grupos lógicos para facilitar la gestión de SAN. Cuando se categoriza la SAN, se seleccionan las categorías (subred, departamento, ubicación, tipo de host, etc.). AMC utiliza el icono de carpeta de archivos para representar una categoría. Consulte la [figura 4](#) en la página 31 para obtener más información sobre los iconos utilizados en el panel de árbol.

El trabajo con categorías de SAN

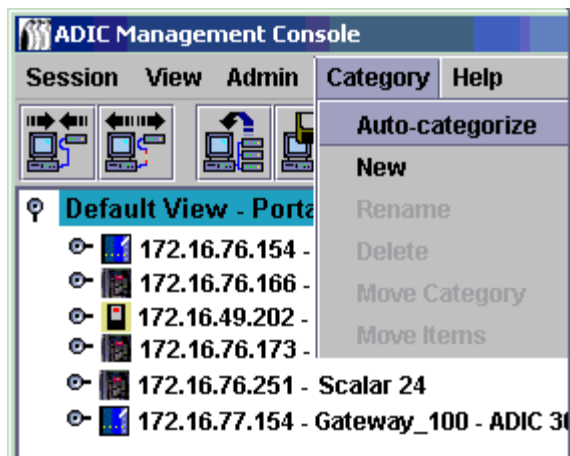
Crear categorías de los equipos de SAN es un método sencillo para ayudarle a gestionar su SAN. Agrupe los equipos por subred, características del host, similitudes por lo que respecta a la conectividad u otras características distintivas. Puede categorizar el portal de diversas formas, cada una de ellas adecuada a una tarea o un usuario distinto, y guardar luego cada categorización como una vista independiente. Puede otorgar derechos de acceso a determinadas vistas a usuarios específicos.

Categorización automática de la SAN

La categorización automática agrupa automáticamente los componentes de SAN por subred.

Para agrupar equipos por subred

- 1 Inicie la sesión como administrador de la SAN, administrador del portal o usuario avanzado.
- 2 Seleccione la vista que se encuentre en la raíz de la pantalla.



- 3 Seleccione el menú **Category** y la opción **Auto-categorize**.
Aparecerá un cuadro de diálogo de advertencia.
- 4 Haga clic en **Yes** para continuar.
De lo contrario, seleccione **No**.
El panel de árbol se actualiza para incluir líneas para las categorías.
- 5 Guarde las categorías como una vista. Consulte [Guardar vistas](#) en la página 58.

Creación de una nueva categoría

Las categorías se utilizan para agrupar componentes de SAN de forma visual en el panel de árbol y el panel gráfico.

Para crear una nueva categoría

- 1 Inicie la sesión como administrador de la SAN, administrador del portal o usuario avanzado.
- 2 Seleccione la vista que se encuentre en la raíz de la pantalla o la categoría que desee subcategorizar.
- 3 Seleccione el menú **Category** y la opción **New**.
- 4 En el cuadro de diálogo **New Category**, escriba un nombre para la nueva categoría.
Seleccione **OK**.
Se actualiza la ventana para incluir una línea para la nueva categoría.
- 5 Arrastre y suelte los equipos en el icono de carpeta de la categoría nueva.
Para obtener más información sobre la función de arrastrar y soltar equipos, consulte [El trabajo con componentes de categorías](#) en la página 54.
Subcategorice una categoría existente haciendo clic con el botón derecho del ratón en la categoría y seleccionando la opción **New**. También puede utilizar el menú **Category**. Consulte [Creación de una nueva categoría](#) en la página 52.
- 6 Arrastre y suelte elementos en la nueva categoría según proceda.
Consulte también [El trabajo con componentes de categorías](#) en la página 54.
- 7 Guarde las categorías como una vista. Consulte [Guardar vistas](#) en la página 58.

Cambio del nombre de una categoría

Es posible cambiar el nombre de las categorías sin perder los datos almacenados.

Para cambiar el nombre de una categoría

- 1 Inicie la sesión como administrador de la SAN, administrador del portal o usuario avanzado.
- 2 Seleccione la categoría cuyo nombre desee modificar.
- 3 Haga clic con el botón derecho del ratón en la categoría. Seleccione **Rename**.
O bien, seleccione la categoría en el panel de árbol y elija el menú **Category** y la opción **Rename**.
- 4 En el cuadro de diálogo **Rename Category**, escriba un nuevo nombre.
- 5 Seleccione **OK**.
Se actualiza la ventana y aparece el nombre nuevo.
- 6 Guarde las categorías como una vista. Consulte [Guardar vistas](#) en la página 58.

Eliminación de una categoría

Si elimina una categoría, no se eliminarán los datos almacenados. Si la categoría no está vacía, mueva primero todos sus elementos a otra categoría. Consulte [El trabajo con componentes de categorías](#) en la página 54.

Para eliminar una categoría

- 1 Inicie la sesión como administrador de la SAN, administrador del portal o usuario avanzado.
- 2 Seleccione la categoría que desee eliminar.
- 3 Haga clic con el botón derecho del ratón en la categoría. Seleccione **Delete**.
- 4 O bien, seleccione la categoría en el panel de árbol y elija el menú **Category** y la opción **Delete**.
La ventana del panel de árbol se actualiza automáticamente.

Reubicación de una categoría

En esta sección se describen los diversos modos para mover categorías:

- Función de arrastrar y soltar
- Comando **Move Categories**

Para arrastrar y soltar una categoría en un nivel distinto de la jerarquía del panel de árbol

- 1 Inicie la sesión como administrador de la SAN, administrador del portal o usuario avanzado.
- 2 Seleccione la categoría que desee mover.
- 3 Arrástrela y suéltela en la categoría adecuada.

Si desea mover la categoría a la carpeta raíz, puede señalar cualquier sitio de la línea de la carpeta raíz.

Si desea mover la categoría para que se anide dentro de otra categoría, asegúrese de que el puntero esté señalando dentro del icono de carpeta de la categoría objetivo.

- 4 Guarde las categorías como una vista. Consulte [Guardar vistas](#) en la página 58.

Para mover una categoría a un nivel distinto de la jerarquía mediante el menú

- 1 Inicie la sesión como administrador de la SAN, administrador del portal o usuario avanzado.
- 2 Seleccione la categoría que desee mover.
- 3 Seleccione el menú **Category** y la opción **Move Category**.

Aparecerá el cuadro de diálogo **Move Category**.

En la parte superior del cuadro de diálogo **Move Category**, detrás del texto **Source Category**, aparece el nombre de la categoría seleccionada para la reubicación en el [paso 2](#).

- 4 Seleccione la categoría a la que desee mover la categoría seleccionada en el [paso 2](#).

Se habilitará el botón **OK**.

- 5 Seleccione **OK**.

Se actualiza el panel de árbol para mostrar los equipos y las categorías del nivel raíz.

- 6 Seleccione el nodo situado a la izquierda de la nueva categoría principal para ver la categoría anidada.
- 7 Guarde las categorías como una vista. Consulte [Guardar vistas](#) en la página 58.

El trabajo con componentes de categorías

En esta sección se describen las diversas formas de mover elementos para sacarlos o introducirlos en categorías:

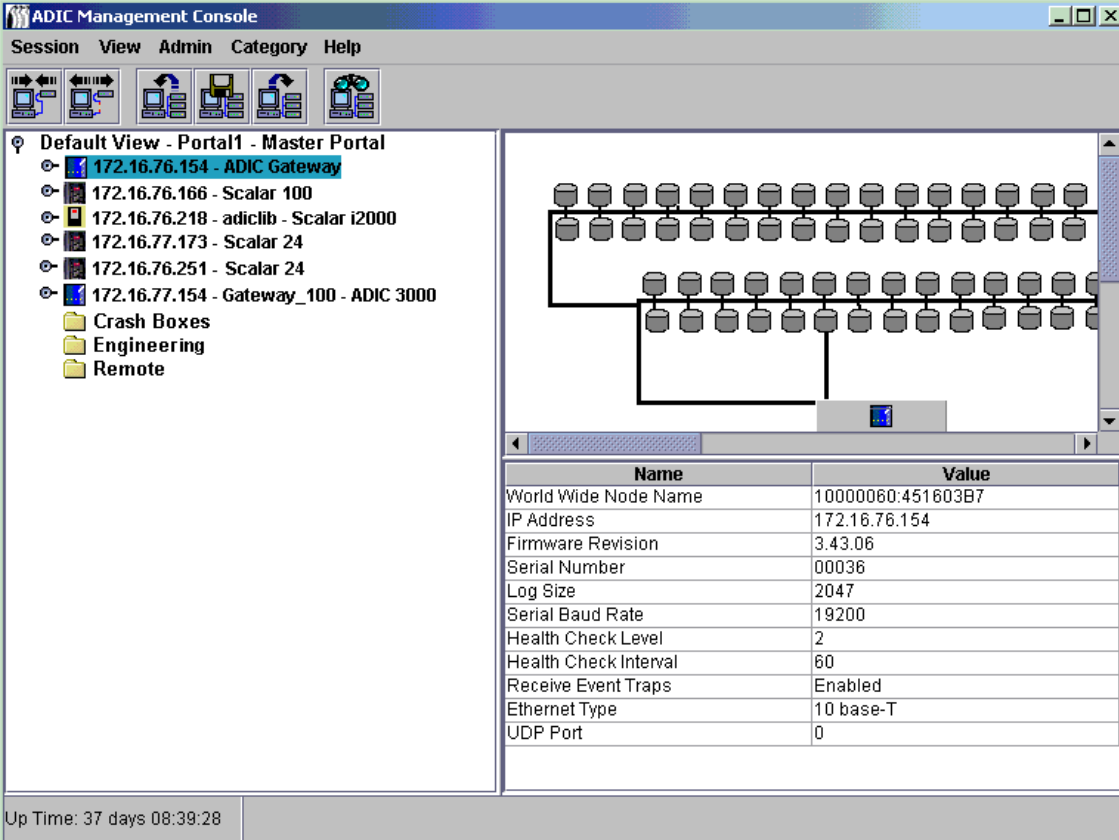
- Función de arrastrar y soltar
- Comando **Move Items**

Reubicación de elementos usando la función de arrastrar y soltar

Para arrastrar y soltar equipos con la finalidad de introducirlos o sacarlos de categorías

- 1 Inicie la sesión como administrador de la SAN, administrador del portal o usuario avanzado.
- 2 Seleccione el equipo que desee mover dentro de una categoría.

En el ejemplo, se selecciona el equipo con la dirección IP 172.16.76.154.



The screenshot shows the ADIC Management Console interface. On the left, a tree view displays the hierarchy: Default View - Portal1 - Master Portal, with sub-items for various devices and folders like Crash Boxes, Engineering, and Remote. The device '172.16.76.154 - ADIC Gateway' is selected. On the right, a network diagram shows a central switch connected to two rows of server racks. Below the diagram is a configuration table with the following data:

Name	Value
World Wide Node Name	10000060:451603B7
IP Address	172.16.76.154
Firmware Revision	3.43.06
Serial Number	00036
Log Size	2047
Serial Baud Rate	19200
Health Check Level	2
Health Check Interval	60
Receive Event Traps	Enabled
Ethernet Type	10 base-T
UDP Port	0

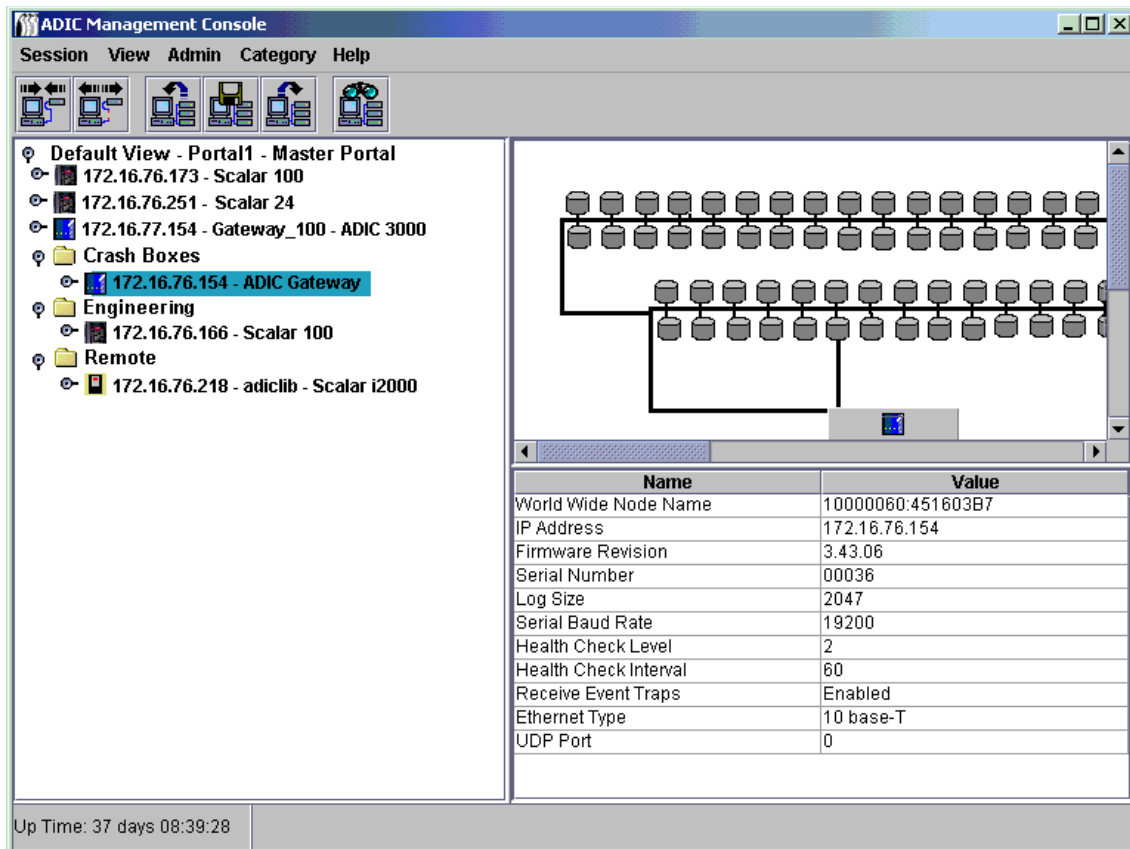
At the bottom left, the status 'Up Time: 37 days 08:39:28' is displayed.

- 3 Arrástrelo y suéltelo en la categoría adecuada.

Asegúrese de que el puntero señale dentro del icono de carpeta de la categoría objetivo.

Si desea mover el elemento a la raíz, puede señalar en cualquier sitio de la línea de la vista raíz.

- 4 Continúe hasta que haya movido todos los elementos que desee mover.



- 5 Guarde las categorías como una vista. Consulte [Guardar vistas](#) en la página 58.

Reubicación de elementos mediante el menú

Para mover elementos con el fin de introducirlos o sacarlos de las categorías mediante el menú

- 1 Inicie la sesión como administrador de la SAN, administrador del portal o usuario avanzado.
- 2 Seleccione la categoría a la que desee mover los elementos.
- 3 Seleccione el menú **Category** y la opción **Move Items**.
- 4 Aparecerá el cuadro de diálogo **Move Items**.

En la parte superior del cuadro de diálogo, seleccione todos los equipos que desee mover (mediante el ratón y las teclas Mayús y Ctrl).

- 5 En la parte inferior del cuadro de diálogo, seleccione la categoría a la que desee mover los elementos.
- 6 Seleccione **OK**.

Seleccione **Cancel** para detener el proceso de reubicación.

El trabajo con vistas

Una **View** es una representación gráfica con nombre de un portal, generalmente guardada para conservar una categorización particular. Los administradores de SAN otorgan a los usuarios acceso a una vista concreta asociada a un portal determinado. Cuando un usuario inicia una sesión, aparece esta vista predeterminada. Puede crear perfiles de usuario que permitan el acceso a más de una vista.

Abrir vistas guardadas

Para abrir una vista guardada anteriormente

- 1 Seleccione el menú **View** y la opción **Open**.

El procedimiento **Open View** también se puede iniciar seleccionando el botón **Open View** de la barra de herramientas.



- 2 Si ya tiene una vista abierta, el sistema pedirá confirmación para cerrarla.

Si hay cambios sin guardar en la vista actual, el sistema le pedirá que los guarde.

Seleccione **Yes** para guardar la vista actual. La vista se guardará. Todos los componentes de SAN desaparecerán de la visualización del panel de árbol. Aparecerá el cuadro de diálogo **Open View**.

- 3 Si no ha seleccionado **Cancel**, aparecerá el cuadro de diálogo **Open View**.

Seleccione el nombre del portal que contenga la vista guardada que desee abrir. A continuación, seleccione **Next**.

En el cuadro de diálogo, aparecerá una lista de las vistas guardadas asociadas al portal seleccionado.

- 4 Para abrir una vista, seleccione su nombre y la opción **Finish**.

Si la vista deseada no se encuentra en el portal seleccionado, elija **Back** y repita el [paso 3](#).

Una vez seleccionada la vista que se desee utilizar, se actualizará la ventana. Se visualiza la nueva vista.

Consulte [El trabajo con categorías y vistas](#) en la página 51.

Creación de vistas

Cree el portal apropiado antes de crear una vista. Consulte [El trabajo con portales](#) en la página 47.

Una vista es una representación lógica de una SAN física. Tal vez desee categorizar el portal antes de guardar la vista.

Consulte [El trabajo con componentes de categorías](#) en la página 54.

Para crear una nueva vista

- 1 Inicie la sesión como administrador de la SAN, administrador del portal o usuario avanzado.

- 2 Seleccione el menú **View** y la opción **New**.

Deberá guardar todos los cambios realizados en la vista actual y cerrarla antes de crear una vista nueva.

Aparecerá el cuadro de diálogo **Create a View**.

- 3 Introduzca un nombre para la vista.
- 4 Seleccione el portal que se asociará a la vista.

OK estará disponible.

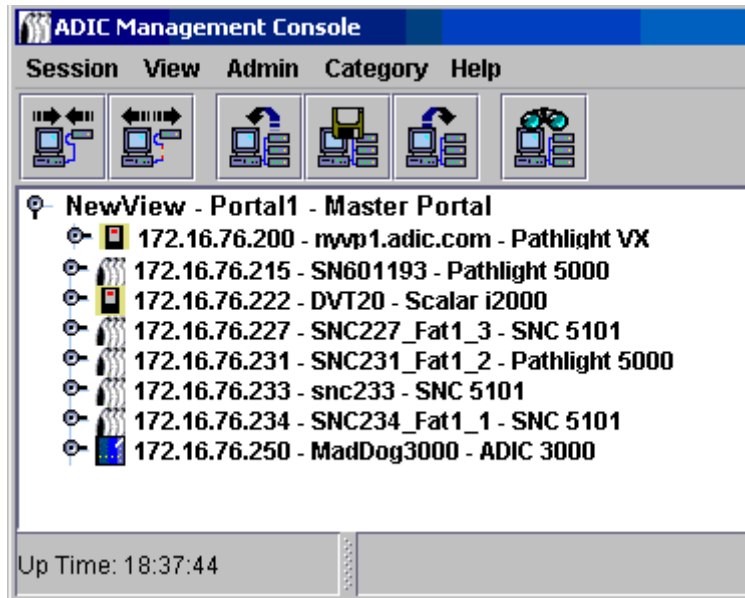
Se mostrarán todos los portales disponibles para el usuario para el que se esté creando la vista.

Para obtener más información sobre los portales, consulte [El trabajo con portales](#) en la página 47.

- 5 Haga clic en **OK**.

Se crea la vista y se actualiza la ventana para mostrar la nueva vista.

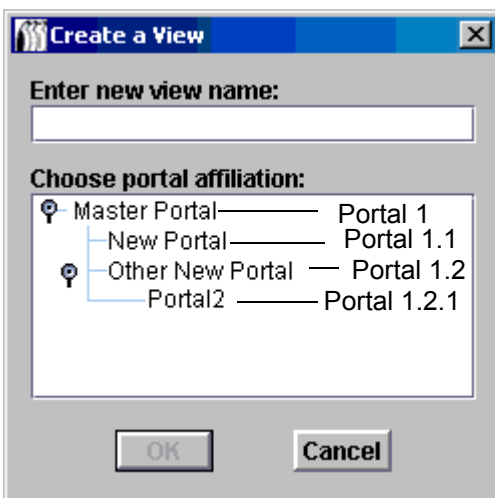
Figura 8 Vista nueva en el nivel de portal principal predeterminado



Como la vista se ha creado directamente bajo el portal principal, **Portal1** se muestra entre el nombre y la afiliación del portal.

Si la vista se hubiera creado bajo el nivel **NewPortal** o **OtherNewPortal** (portales subordinados al portal predeterminado), el nivel numerado sería **Portal1.1**, **Portal1.2**, etc.

Figura 9 Niveles numerados para las vistas



Si no ha categorizado la vista, hágalo ahora.

Consulte [El trabajo con componentes de categorías](#) en la página 54.

- 6 Guarde la vista. Consulte [Guardar vistas](#) en la página 58.

Guardar vistas

La creación de vistas, que son organizaciones lógicas de componentes de SAN, permite un trabajo más eficaz. Es conveniente guardar las vistas creadas para no tener que crearlas de nuevo.

Para guardar la vista actual

Si no se han realizado cambios en la vista, o si la vista no se acaba de crear, el comando **Save** no estará disponible.

- 1 Inicie la sesión como administrador de la SAN, administrador del portal o usuario avanzado.
- 2 Seleccione el menú **View** y la opción **Save**.

El procedimiento **Save Current View** también se puede iniciar mediante el botón **Save Current View** de la barra de herramientas.



Aparece el mensaje *View successfully saved* en el **Status/Message Area**.



Nota La vista predeterminada no se puede guardar con el comando **Save**.

Si intenta guardar la vista predeterminada con el comando **Save**, se le informará de que no es posible.

Para guardar la vista actual con otro nombre

- 1 Inicie la sesión como administrador de la SAN, administrador del portal o usuario avanzado.
- 2 Seleccione el menú **View** y la opción **Save as**.
- 3 En el cuadro de diálogo **Save View As**, escriba un nombre para la vista.

Este nombre aparecerá después cuando abra el cuadro de diálogo **Select View**.

Eliminación de vistas

Si elimina una vista, no se eliminarán los datos almacenados.

Para eliminar la vista actual

- 1 Seleccione el menú **View** y la opción **Delete**.
Aparecerá un mensaje que advierte de que se va a eliminar la vista actual.
- 2 Seleccione **Yes** para confirmar que desea eliminar la vista actual.
Seleccione **No** para detener el proceso de eliminación.

Búsquedas en la vista actual

En una red SAN de grandes dimensiones, se puede utilizar el comando Find para buscar rápidamente un componente de SAN.

Para buscar un equipo concreto u otro componente de SAN

- 1 Seleccione el menú **View** y la opción **Find**.

El comando se ajusta de forma predeterminada a **First Occurrence**.

También puede utilizar el botón **Find** de la barra de herramientas para iniciar una búsqueda en la red SAN.



Escriba la cadena de búsqueda en el cuadro de diálogo. Seleccione **OK**.

Se actualiza el panel de árbol para mostrar la línea que contiene la primera aparición de la cadena de búsqueda, resaltada en color azul.

- 2 Para continuar la búsqueda, seleccione **Next Occurrence** en el submenú **Find** del menú **View**. Se actualiza el panel de árbol para mostrar la línea que contiene la siguiente aparición de la cadena de búsqueda, resaltada en color azul.

Si la cadena no aparece más veces, se abre un cuadro de diálogo.

El comando **Find** también se puede utilizar para buscar dispositivos de disco y otros componentes de SAN.

Informes sobre la vista actual

Puede crear una serie de informes distintos que le ayudarán a gestionar la red SAN.

Para generar informes

- 1 Seleccione el menú **View** y la opción **Report Data**.
- 2 Utilice las casillas de verificación y los botones de opción para seleccionar el informe necesario.

Se pueden generar informes para SNC, controladores de biblioteca de cinta o controladores de matrices de discos, dispositivos de disco, dispositivos de cinta o todos los dispositivos.



Nota Las direcciones IP de las RMU Scalar no aparecen en la lista de selección.

Haga clic en el botón **Preview** para acceder a una vista previa del informe que se puede generar según los parámetros seleccionados.

9

Realización de tareas administrativas

En este capítulo se describen los procedimientos para realizar distintas tareas administrativas. Ciertas tareas son aplicables a toda la red SAN:

- Configuración del correo electrónico
- Configuración de políticas
- Detección de la red SAN

Otras tareas se centran en el SNC como equipo de red:

- Configuración de cadenas de comunidad SNMP
- Visualización de datos de RMU de una biblioteca
- Comprobaciones de estado
- Registros de eventos
- Identificación de componentes de SAN
- Actualización de datos
- Almacenamiento y carga de archivos de configuración
- Actualización del firmware
- Reinicio
- Seguimiento de datos de entorno

Configuración del correo electrónico

AMC se puede configurar para que utilice el correo electrónico para informar de ciertas condiciones.

Para configurar los ajustes de correo electrónico

- 1 En el menú **Admin**, seleccione **Email configuration**.

Aparecerá el cuadro de diálogo **Email Configuration Setting**.

Si introdujo datos en la parte de configuración de correo electrónico durante la instalación, esos datos aparecerán en el cuadro de diálogo. De otro modo, el cuadro diálogo aparecerá vacío.



Nota

Para obtener más información sobre la configuración de correo electrónico en los modelos Scalar i2000 y Pathlight VX, consulte el *Manual de usuario de Scalar i2000* o la ayuda en pantalla de la interfaz VLI.

- 2 Edite el nombre del servidor SMTP para que coincida con el servidor SMTP de su red.
- 3 Edite los campos **Account** y **Password** para reflejar la existencia de una cuenta válida y su contraseña asociada para el servidor SMTP mencionado en el [paso 2](#).
- 4 Edite el campo **Sender Address** para indicar el remitente que desee que vean los usuarios cuando el software AMC envíe un mensaje; por ejemplo, AMC@MyCompany.com.
- 5 Seleccione **OK** para continuar.
Seleccione **Cancel** para cerrar el cuadro de diálogo sin llevar a cabo ninguna acción.
Si selecciona **OK**, en el **Status/Message Area** aparecerá *Email configuration successfully set*.

Configuración de políticas

El generador de políticas es un sistema experto que permite que AMC alerte a ciertas personas especificadas por el administrador de que se cumplen ciertas condiciones de la red SAN. Estas condiciones se definen en términos de capturas de eventos. Para obtener más información sobre la generación de informes de eventos, consulte [Seguimiento y gestión de registros de eventos](#) en la página 68.

Para crear una nueva política

- 1 En el menú **Admin**, seleccione **Policy Configurations** y, a continuación, **New Policy**.
Aparecerá el cuadro de diálogo **Add New Rule**.
- 2 Seleccione **Check traps when they arrive**.
Esto hará que el botón **Next** quede habilitado.
- 3 Seleccione **Next**.
- 4 Escriba el nombre de la nueva regla en el cuadro de texto.
- 5 Seleccione **High**, **Medium** o **Low** en el cuadro de lista desplegable para asignar un nivel de prioridad. Si se generan muchas alertas, se ordenarán por prioridad antes de enviarse.
- 6 Haga clic en **Next**.
- 7 Seleccione una o las dos condiciones de notificación de eventos seleccionando las casillas de verificación:
 - Specify Trap Number
 - Specify the appliance IP that the trap is from
- 8 Seleccione **Specify Trap Number** para visualizar una lista de capturas por número y descripción. Recorra la lista para verla en su totalidad.
- 9 Haga clic en la condición que cumpla los requisitos del nombre de regla que ha elegido.
- 10 Realice uno de los pasos siguientes:
Haga clic en **OK** para asociar esta captura a la nueva regla.
- 11 Seleccione **Specify the appliance IP that the trap is from** para mostrar una lista de los equipos disponibles.
- 12 Seleccione las direcciones IP de los equipos que necesite. Utilice para ello el botón izquierdo del ratón y las teclas Ctrl o Mayús.

- 13 Haga clic en **OK** para asociar estos SNC a la nueva regla.
Las condiciones elegidas se escribirán en el panel inferior del cuadro de diálogo **Add New Rule**. Recorra la lista para revisar la regla completa.
- 14 Seleccione **Next** para abrir la configuración de correo electrónico.
- 15 Seleccione la casilla de verificación de correo electrónico situada en el extremo superior del cuadro de diálogo **Mail Address of Trap Notice**. Aparecerá un segundo cuadro de diálogo por encima de la ventana de configuración de correo.
- 16 Escriba las direcciones de correo electrónico de los destinatarios previstos y una línea con el asunto del mensaje. Si introduce varias direcciones, sepárelas con punto y coma.
- 17 Seleccione **OK** para continuar.
- 18 Tras seleccionar **OK**, revise la regla y las direcciones de correo electrónico en el panel inferior del cuadro de diálogo **Add New Rule**. Seleccione **Finish**.
- 19 Confirme que desea agregar la regla a la base de datos.
- 20 Haga clic en **Yes** para agregar la regla.
El mensaje *Policy added successfully* aparecerá en el **Status/Message Area**.

Detección de la red SAN

En esta sección se describen los pasos para establecer y modificar los elementos de la red SAN.

Para modificar la configuración de detección

- 1 Inicie una sesión como administrador de SAN.
- 2 En el menú **Admin**, seleccione **Discover SAN** y, a continuación, **Modify Discovery Configuration**.
Se abrirá el cuadro de diálogo **Discovery Configuration**.
Todas las direcciones IP se introducen en formato de cuatro grupos separados por puntos:
xxx.xxx.xxx.xxx.
- 3 Seleccione un segmento.
- 4 Realice uno de los pasos siguientes:
Para agregar un segmento de red para su detección, seleccione **Add**. Se mostrará el cuadro de diálogo **Segment Configuration**. Continúe con el [paso 5](#).
Para volver a configurar un segmento existente, haga clic en el segmento. A continuación, seleccione **Change**. Se mostrará el cuadro de diálogo **Segment Configuration**. Continúe con el [paso 5](#).
Para eliminar un segmento existente, selecciónelo. A continuación, haga clic en **Delete**. Continúe con el [paso 10](#).
- 5 Asigne un nombre al segmento o cámbielo escribiéndolo directamente en el cuadro de texto **Segment Name**. No es necesario asignar un nombre a un segmento de red.
- 6 Según sea necesario, seleccione el botón de opción **Single IP Address** o **IP Address Range**; el número de casillas de entrada se completará correspondientemente. Introduzca las direcciones IP que desee detectar. Haga esto si está agregando un segmento o si está modificando un segmento existente.
- 7 Seleccione **Add**. El nuevo segmento pasará a la lista **IP Addresses to be discovered** situada en el extremo inferior del cuadro de diálogo. Si está agregando un segmento nuevo, continúe con el [paso 12](#). Si está modificando un segmento existente, continúe con el [paso 8](#).

- 8 Seleccione la cadena del segmento que ya no desee detectar y haga clic en **Delete**. El botón **Delete** sólo está habilitado cuando hay seleccionado un segmento en el cuadro de su izquierda (**IP Addresses to be discovered**).

Si está agregando un nuevo segmento, complete la configuración con el [paso 12](#).

Si está modificando una configuración y desea cambiar los parámetros avanzados de configuración de detección, prosiga con el [paso 12](#).

Si está modificando una configuración y está satisfecho con los parámetros avanzados de configuración, prosiga con el [paso 9](#).

- 9 Seleccione OK en el cuadro de diálogo **Segment Configuration**.
- 10 Seleccione OK en el cuadro de diálogo **Discovery Configuration**.
Aparecerá un mensaje de advertencia.
- 11 Seleccione **Yes** para aceptar la actualización o **No** para cerrar el cuadro de diálogo sin aplicar los cambios.
- 12 Para configurar los parámetros avanzados de configuración de detección, seleccione la ficha **Advanced** del cuadro de diálogo **Segment Configuration**.
- 13 Cuando configure los parámetros, tenga en cuenta lo siguiente:
 - Escriba las direcciones IP de los sistemas que no desee detectar en el cuadro intermedio de la ficha **Advanced**.
 - Los parámetros opcionales, como el valor **SNMP Timeout** o el ajuste **Read Community** para un segmento nuevo, no se asocian a ningún segmento de detección nuevo a menos que se escriban en los cuadros de texto de la ficha **Advanced**.
 - La función **ICMP Ping Timeout** está inhabilitada en esta versión.
 - Los valores **SNMP Timeout** se introducen en milisegundos. Limitan el tiempo asignado a la espera de una respuesta en cada dirección IP que se esté verificando. El valor predeterminado se ha establecido a un número grande deliberadamente para garantizar que se detecten todos los dispositivos aunque la red sea lenta. Puede ajustar un valor de tiempo de espera mucho más bajo que el valor predeterminado de 5.000 milisegundos para que la detección sea más rápida.
 - El ajuste **SNMP Read Community** en los SNC Scalar se establece en **public** de forma predeterminada. A menos que haya cambiado ese valor en los equipos de su red, el valor del servidor también se tendrá que ajustar a **public**. Los valores para **SNMP Read Community** del equipo deben coincidir con los del servidor.
- 14 Cuando esté satisfecho con los datos de la ficha **Advanced**, regrese al [paso 9](#).

Para volver a detectar los equipos de un segmento de red determinado

- 1 En el menú **Admin**, seleccione **Discover SAN** y, a continuación, **Re-Discover Segment(s)**.
Aparecerá el cuadro de diálogo **Re-Discover Segments**.
 - a. Haga clic en la columna **View** para ver los parámetros de configuración de detección de segmentos.
 - b. Haga clic en **OK** para cerrar el cuadro de diálogo emergente.
- 2 En la columna **Discover**, seleccione la casilla de verificación del segmento que desee volver a detectar. A continuación, haga clic en **OK**.

Si hace clic en **OK**, aparecerá un mensaje de advertencia.

Los mensajes del **Status/Message Area** le mantendrán informado durante la detección.

Para obtener más información sobre esta área, consulte [Área de estado/mensajes](#) en la página 36.

Una vez finalizada la detección, en el **Status/Message Area** aparecerá el mensaje *Discovery Process Finished*.

Para detectar un equipo determinado

- 1 En el menú **Admin**, seleccione **Discover SAN** y, a continuación, **Discover Appliance**.

Aparecerá el cuadro de diálogo **Discover Appliance**.

- 2 En el cuadro de texto, escriba la dirección IP del equipo de red que desea detectar.

- 3 Seleccione **OK** para continuar.

Si el equipo ya se encuentra en la vista actual del portal actual, aparecerá un mensaje indicándolo.

Si el equipo no está en la vista activa, se agregará al portal principal asociado a la vista activa.

Aparecerá un mensaje indicando que el equipo se ha agregado.



Nota

Los equipos agregados a una vista mediante **Discover Appliance** no se convierten automáticamente en miembros de esa vista, incluso si dicha vista se guarda una vez detectados los equipos. Para que se conviertan en miembros permanentes, utilice **Modify Discovery Configuration** para agregar sus direcciones IP a la cadena de configuración de detección.

Configuración de cadenas de comunidad SNMP

Las cadenas de comunidad SNMP forman parte de la función de mensajería del software agente y sirven para agrupar los dispositivos de red en grupos lógicos con fines de gestión. Las cadenas de comunidad del servidor se deben corresponder con las de los equipos en red que se deseen gestionar.



ATENCIÓN

Antes de modificar los valores de las cadenas de comunidad SNMP, consulte a su representante de servicio de atención al cliente de ADIC.

Hay definidas dos cadenas configurables:

- **Read** permite que AMC obtenga información sobre equipos con cadenas de comunidad **Read** coincidentes.
- **Write** permite que AMC modifique los ajustes de los equipos con cadenas de comunidad **Write** coincidentes.

El equipo puede mantener 32 cadenas de comunidad **Read** y 32 cadenas **Write**.



ATENCIÓN

El ajuste incorrecto de las cadenas de comunidad SNMP puede impedir que AMC gestione el sistema.

Para asignar ajustes de cadenas de comunidad SNMP a un equipo en la red SAN

- 1 Inicie una sesión como administrador de SAN.



Nota

Los administradores de portal, los usuarios avanzados y los usuarios básicos no están autorizados para utilizar este comando. Para obtener información sobre los privilegios de usuario, consulte la [tabla 2](#) en la página 42.

- 2 Seleccione un equipo en la lista del panel de árbol.
- 3 En el menú **Admin**, seleccione el comando **SNMP Community Strings**.

Aparecerá el cuadro de diálogo **Change SNMP Community Strings**.

- 4 Modifique los ajustes que desee y haga clic en **OK**.

Para cancelar los cambios en los ajustes de las cadenas de comunidad SNMP, haga clic en **Cancel**.

Lectura de información sobre una biblioteca

Es posible acceder a los datos de la RMU de una biblioteca Scalar haciendo clic en la biblioteca y seleccionando el comando **Show RMU Data**.

Para obtener más información sobre la visualización de datos de la RMU, consulte [Visualización de los datos de la RMU](#) en la página 66.



Nota

La biblioteca Scalar i2000 y la solución Pathlight VX no tienen RMUs.

Visualización de los datos de la RMU

No todos los equipos de la red SAN pueden ofrecer este tipo de datos. Si el equipo seleccionado no es capaz de proporcionar esta información, el menú del equipo no mostrará **Show RMU Data**.

Para realizar un seguimiento de los datos de la RMU de un equipo seleccionado

- 1 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.
- 2 Seleccione **Show RMU Data**.

Si el equipo es capaz de ofrecer datos de RMUs pero no hay RMUs conectadas, aparecerá un cuadro de diálogo. Introduzca la dirección IP de la RMU en él.

Una vez conectada la RMU, aparecerá la información correspondiente. La ficha predeterminada es **Global Status**.

La ficha **Mover** muestra información sobre la automatización de la biblioteca.

La última ficha es la ficha **Drives**. Muestra información detallada sobre las unidades gestionadas.

- 3 Cuando haya terminado de visualizar los datos de la RMU, haga clic en **OK**.

Utilización de la comprobación de estado



Nota

En los modelos Scalar i2000 y Pathlight VX, las comprobaciones de estado se llevan a cabo automáticamente y de forma proactiva.

La **Health Check (comprobación de estado)** permite comprobar periódicamente el estado operacional de las conexiones de un SNC a las interfaces que controla. Si se deshabilita la **Health Check**, el SNC no realizará otra comprobación periódica que el seguimiento las líneas de estado de entorno, que indican las condiciones de alimentación y de temperatura. La función de **Health Check** envía capturas SNMP cuando es necesario para mostrar información de estado en la interfaz de usuario.

Realización de la comprobación de estado

El comando **Perform Health Check** solicita una comprobación inmediata del estado en el nivel actual especificado. Esta comprobación se realiza independientemente del ajuste Health Check Interval.

Para realizar una comprobación de estado

- 1 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.
- 2 En el menú **Health Check**, seleccione **Perform Health Check**.

A menos que haya restablecido el nivel, la comprobación de estado se lleva a cabo en el nivel **Interface Test**. Consulte la [tabla 3](#).

Tabla 3 Niveles de comprobación de estado

Nombre del nivel	Funciones
Ninguno	Comprobación de estado desactivada
Basic Function	Comprobar el estado del suministro eléctrico y la temperatura
Interface Test	Todas desde el nivel básico, además de realizar la comprobación de todas las interfaces
Device Test	Todas desde el nivel Interface Test, además de realizar una consulta en todos los dispositivos objetivo
Device Ready	Todas desde el nivel Device Test, además de realizar una comprobación de preparación de la unidad en todos los dispositivos objetivo (exclusivo para los medios no extraíbles)



Nota

Los niveles de comprobación de estado en AMC no son iguales a los niveles en LMC o VLI. Para más información, consulte el *Manual de usuario de Scalar i2000* o la ayuda en pantalla de VLI.

Si la comprobación tiene éxito, aparece un mensaje en el **Status/Message Area**, por ejemplo, *Successful Health Check*.

Configuración de la comprobación de estado

Es posible configurar los ajustes de la **Health Check**.

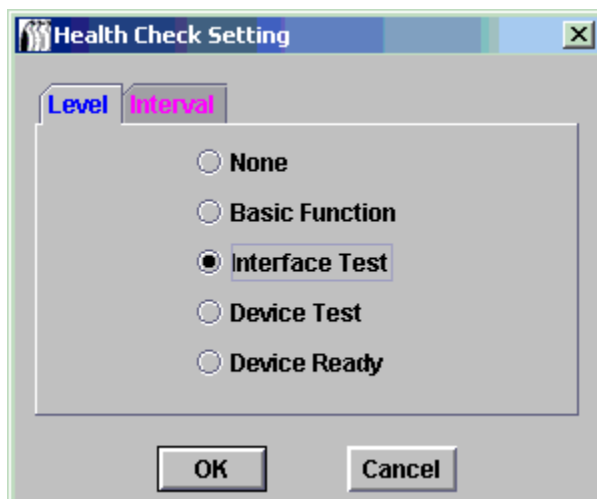
Para examinar o modificar los ajustes de comprobación de estado

- 1 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.
- 2 En el menú **Health Check**, seleccione **Health Check Settings**.

La ficha predeterminada es **Level**. Consulte la [tabla 3](#) en la página 67. Las opciones de esta ficha permiten elegir la exhaustividad con que se realizará la comprobación de estado. Compare la [tabla 3](#) con la [figura 10](#).

- 3 Si está satisfecho con el nivel, haga clic en **OK**.
Si decide no cambiar los ajustes de nivel de comprobación de estado, haga clic en **Cancel**.

Figura 10 Ficha Level del cuadro de diálogo Health Check Setting



- Si hace clic en **Cancel** y desea ajustar el intervalo con que se realizan las comprobaciones de estado, repita la secuencia del [paso 1](#) al [paso 3](#).
 - Ahora seleccione la ficha **Interval**.
- 4 En la ficha **Interval**, indique el tiempo que debe transcurrir entre las comprobaciones de estado automáticas del equipo seleccionado. El intervalo puede variar desde 0 hasta 65.535 minutos. El intervalo predeterminado es 60 minutos. Si elige 0, no se realizará ninguna comprobación de estado.

Comprobación del latido

El latido es una simple comprobación de la comunicación entre un equipo y un dispositivo.

Para comprobar el latido en un equipo seleccionado

- 1 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.
- 2 En el menú **Health Check**, seleccione **Check Heartbeat**.

Si el resultado de la comprobación es correcto, en el **Status/Message Area** aparecerá el mensaje *xxx.xxx.xxx.xxx is responding*, donde las "x" representarán una dirección IP.

Las comprobaciones de latido se realizan automáticamente cada cinco minutos.

Seguimiento y gestión de registros de eventos

En las bibliotecas que disponen de un SNC, los submenús de **Events** permiten controlar el modo en que se muestra el registro de eventos y en que se generan las capturas. Las capturas (mensajes) se generan cuando ocurre un evento a una frecuencia específica. Consulte [Ajuste del límite de captura de eventos](#) en la página 69. Los eventos también se pueden gestionar desde el generador de políticas, de modo que el usuario reciba avisos por correo electrónico sobre las condiciones de captura de eventos. Consulte [Configuración de políticas](#) en la página 62.

Para ver el registro de eventos

- 1 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.
- 2 En el menú **Events**, seleccione **View Event Log**.

Aparecerá el nivel de registro de eventos.

- 3 Seleccione **Warning** para visualizar los eventos del tipo **Warning** y **Notice**.
Seleccione **Information** para visualizar los eventos del tipo **Information**, **Warning** y **Notice**.
Si selecciona **All Events**, obtendrá el mismo resultado que si selecciona **Information**.
- 4 Seleccione **OK** para continuar. Si hace clic en **OK**, aparecerá el registro de eventos. Utilice las barras de navegación para desplazarse por el registro.
 - a. Seleccione los eventos que desee en el registro utilizando el ratón en combinación con las teclas Ctrl o Mayús, también puede seleccionar la opción **Select All** en el menú **Edit**.
 - b. Para copiar los eventos seleccionados en un archivo de texto, seleccione el comando **Copy** del menú **Edit**.
 - c. Para guardar los eventos en un archivo de texto, seleccione el comando **Save** del menú **File**.

Para imprimir una copia del registro de eventos

- 1 Siga los pasos descritos en [Para ver el registro de eventos](#) en la página 68.
- 2 Seleccione la ventana del registro de eventos y, en el menú **File**, haga clic en **Print**.

Se abrirá el cuadro de diálogo de la impresora.

- 3 Confirme el envío del registro a la impresora.

De forma predeterminada se envían todas las páginas a la impresora.

- Si no desea imprimir todas las páginas de un registro de eventos largo, seleccione con el ratón y las teclas Ctrl o Mayús las líneas que desee imprimir.
- Pegue estas líneas en un editor de textos.
- Seleccione el menú **File** y el comando **Print**.

Para guardar una copia de las entradas visualizadas actualmente

- 1 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.
- 2 En el menú **Events**, seleccione **Save Event Log**.
- 3 Escriba un nombre para el archivo en el cuadro de diálogo del examinador.
Si no desea guardar el archivo en el directorio predeterminado, elija un nuevo directorio.
- 4 Una vez guardado el registro, se le preguntará si desea borrar el registro de eventos del equipo seleccionado.

Haga clic en **Yes** para borrar el registro de eventos.

Haga clic en **No** para conservar el registro de eventos.

Ajuste del límite de captura de eventos

El **Trap Threshold Level (nivel de captura de eventos)** determina cuántas veces se puede producir un evento en un intervalo de diez minutos. Si se rebasa ese límite, se envía una captura a los clientes que realizan el seguimiento del equipo. Para recibir mensajes de correo electrónico, consulte [Configuración de políticas](#) en la página 62.

Para establecer el límite de captura de eventos

- 1 Inicie una sesión como administrador de SAN.



Nota

Los administradores de portal, los usuarios avanzados y los usuarios básicos no están autorizados para cambiar los límites de captura de eventos. Para obtener información sobre los privilegios de usuario, consulte la [tabla 2](#) en la página 42.

2 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.

3 En el menú **Events**, seleccione **Set Event Trap Threshold**.

Aparecerá el cuadro de diálogo **Event Trap Thresholds**.

4 Seleccione el evento.

5 Haga clic en el botón **Change**.

Se mostrará el cuadro de diálogo **Event Threshold**.

Cuando se produce un bucle descendente FCAL, no se registra ningún evento, ya que el límite está ajustado a "0".

La mayoría de eventos tiene un límite de "1", lo que significa que se registra un evento cuando se cumple la condición.

El evento **FCAL LIP Occurred** es el único evento que tiene ajustado un límite distinto de "0" o "1". Está ajustado a "10". Los usuarios no suelen tener interés en la aparición de LIPs FCAL, a menos que aparezcan con una frecuencia superior a un minuto.

6 Ajustar el límite de captura de eventos al número determinado por usted optimizará el rendimiento.

No cambie los límites de captura a menos que lo recomiende el representante del servicio técnico.

7 Seleccione **OK**.

Recepción de capturas de eventos

De forma predeterminada, las capturas se envían al cliente.

Para dejar de recibir capturas de eventos

1 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.

2 En el menú **Events**, seleccione **Receive Event Traps**.

3 Anule la selección de la casilla de verificación **Receive Event Traps**.

La marca de verificación se borrará y aparecerá un cuadro de diálogo de confirmación.

4 Haga clic en **Yes** si no desea recibir capturas de eventos.

Haga clic en **No** si desea continuar recibiendo capturas de eventos.



Nota

Si sale de AMC y vuelve a iniciarlo, volverá a recibir las capturas hasta que desactive la casilla de nuevo.

Seguimiento de las capturas de evento recibidas

Cuando se recibe una captura aparece un icono en el **Status/Message Area** situada en la parte inferior de la ventana principal.

Para ver las capturas de eventos recibidas

- 1 Seleccione la ventana **Received Event Traps**, que permanece activa mientras se ejecuta una instancia del cliente, aunque se puede minimizar.

Para obtener más información sobre la ventana **Received Event Traps**, consulte [Lectura de los paneles de información de gestión de la red SAN](#) en la página 26.

- 2 Consulte la ventana **Received Event Traps** para ver los mensajes de capturas.

Los mensajes identifican el equipo por su dirección IP. También incluyen una marca de fecha y hora, un código de evento y una descripción del evento que causó la captura.

- 3 Haga doble clic en un evento de la ventana para mostrar información detallada sobre él.
Haga clic en **OK** para cerrar la vista detallada.

Seguimiento del panel de LEDs

Cuando E/S se está ejecutando, el panel de LEDs del SNC permanece activo. Si se producen problemas cuando el SNC está pasando a modo online, los LED se congelarán con configuraciones específicas con significado. Para conocer el significado de los LEDs y de sus combinaciones, consulte el *Manual de usuario del hardware* del equipo. La biblioteca Scalar i2000 y el sistema Pathlight VX tienen paneles de LEDs distintos que la consola AMC no puede mostrar. Para obtener información sobre los LED, consulte su documentación.

Para ver el panel de LEDs de un equipo seleccionado

- 1 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.
- 2 Seleccione **Show LED Panel**.

Se abrirá una nueva ventana con una representación gráfica del panel de LEDs del equipo de red. Observando esta ventana puede realizar un seguimiento en tiempo real de la actividad de los LED. Consulte de la [figura 11](#) a la [figura 15](#).

Figura 11 Panel de LEDs del SNC 5101

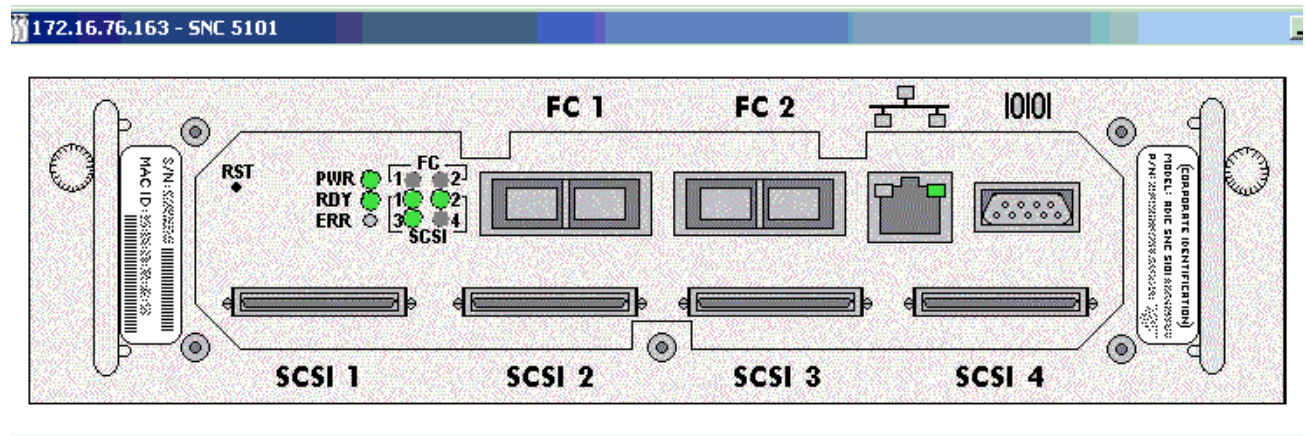


Figura 12 Panel de LEDs del ADIC SNC 3000

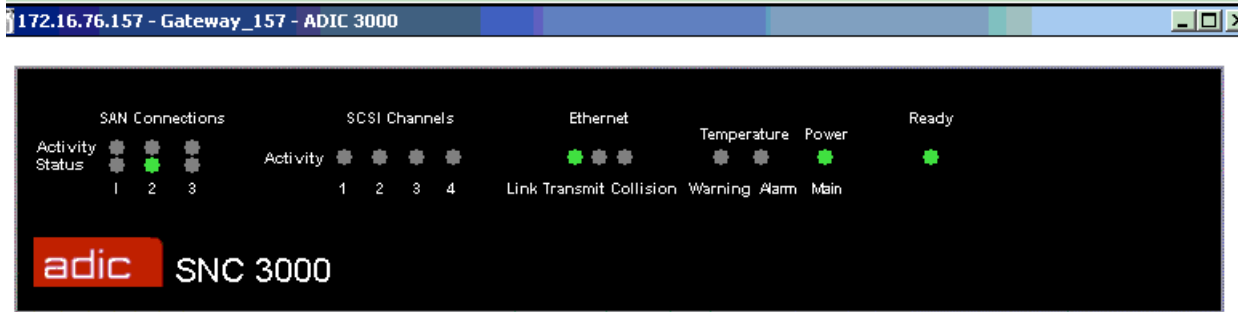


Figura 13 Panel de LEDs del SNC 4000

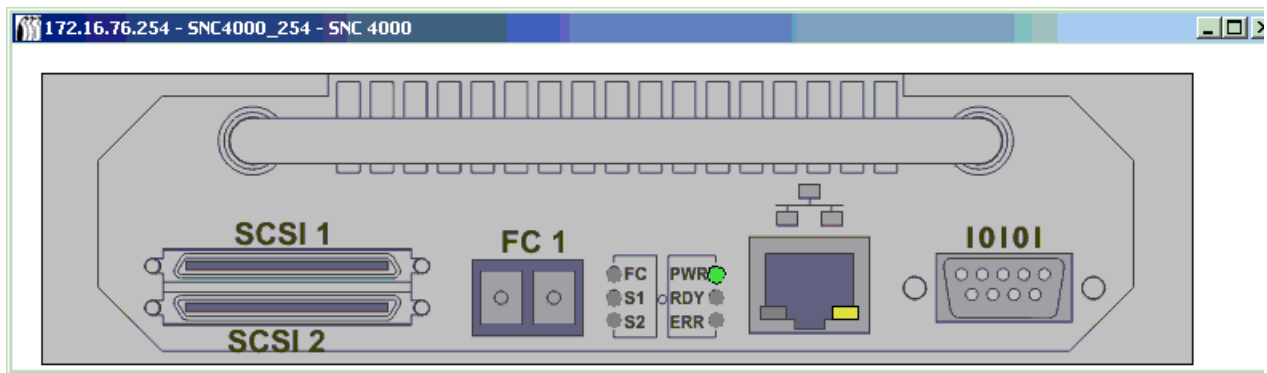


Figura 14 Panel de LEDs del SNC 5100

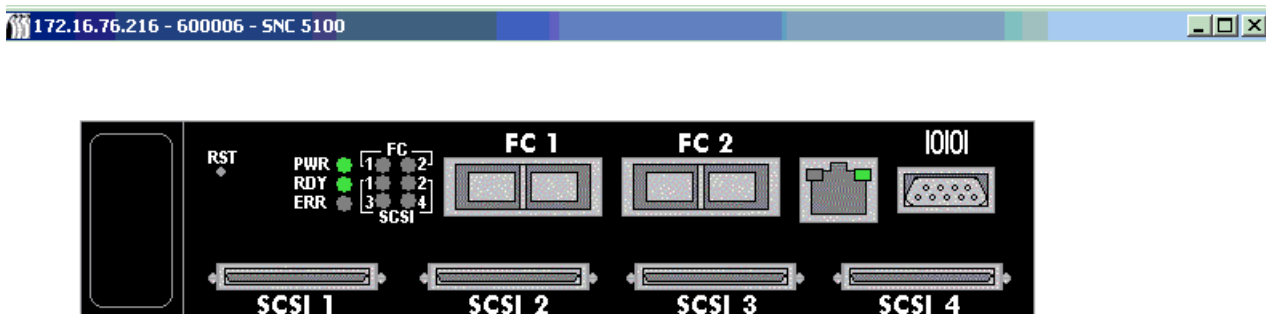
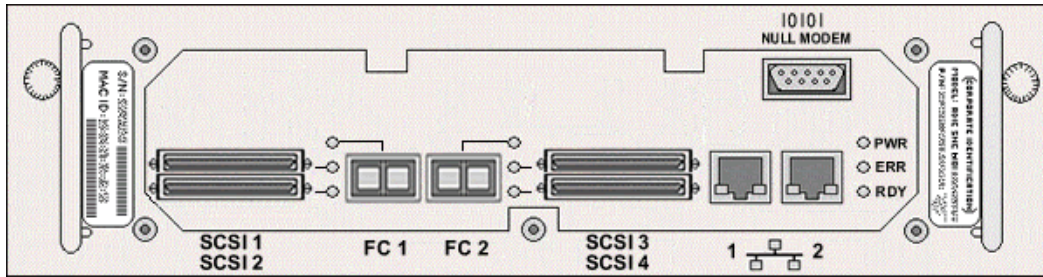


Figura 15 Panel de LEDs del SNC 6101



Utilización del comando Identify

El comando **Identify** hace que el LED **RDY** (ready) del equipo seleccionado parpadee rápidamente, de forma que pueda distinguirlo fácilmente del resto de equipos en funcionamiento.

Para identificar visualmente el equipo seleccionado

- 1 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.
- 2 Seleccione **Identify**.
Aparecerá el cuadro de diálogo **Flash Ready LED**.
- 3 Seleccione **Turn Ready LED On**.
- 4 Para ver la posición del LED **RDY** en varios equipos, consulte de la [figura 16](#) a la [figura 19](#).

Figura 16 LED Ready en el SNC 5101

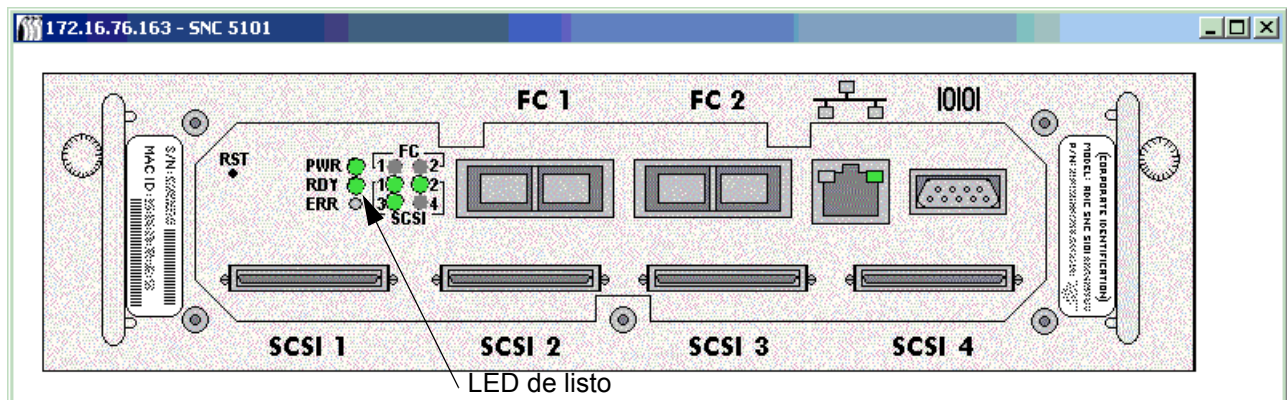


Figura 17 LED Ready en el SNC 5100

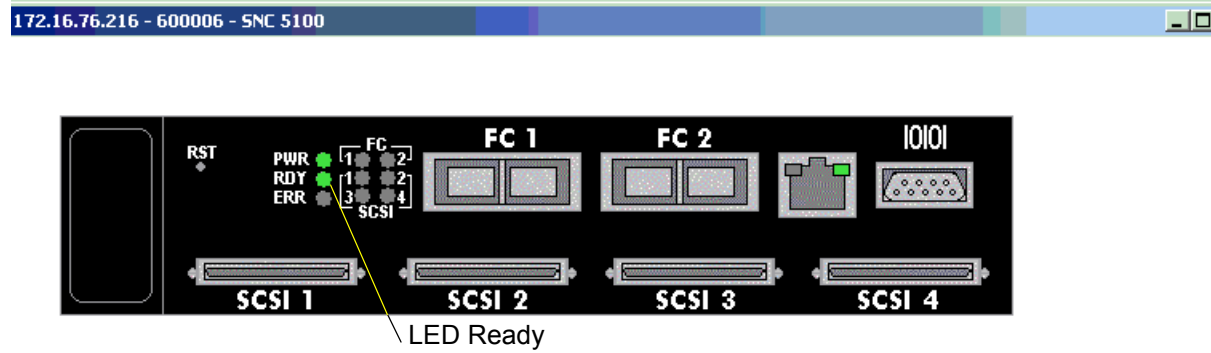


Figura 18 LED Ready en el SNC 4000

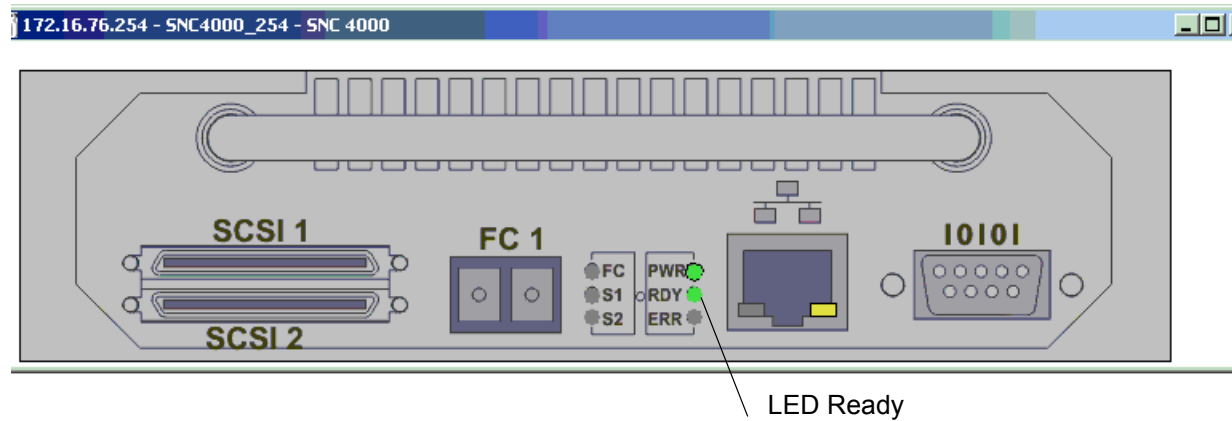
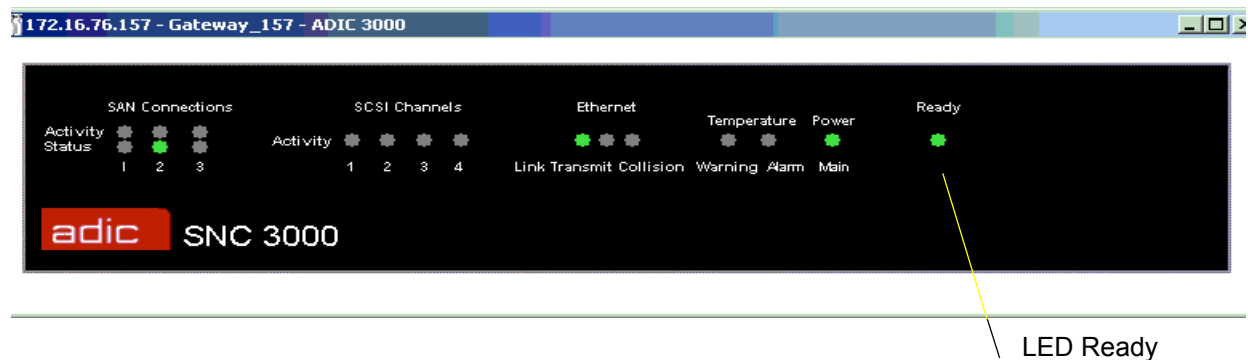


Figura 19 LED Ready en el ADIC SNC 3000



- 5 Una vez identificado el equipo, seleccione **Cancel** en el cuadro de diálogo **Flash Ready LED** para que el LED **RDY** vuelva a funcionar normalmente.

Gestión del equipo de red SAN

Ciertas funciones están disponibles haciendo clic con el botón derecho del ratón en el equipo deseado. Puede seleccionar el equipo haciendo clic con el botón derecho del ratón en el panel de árbol o en el panel gráfico. Consulte [figura 20](#) y [figura 21](#).

Figura 20 Selección con el botón derecho en la representación del equipo del panel gráfico

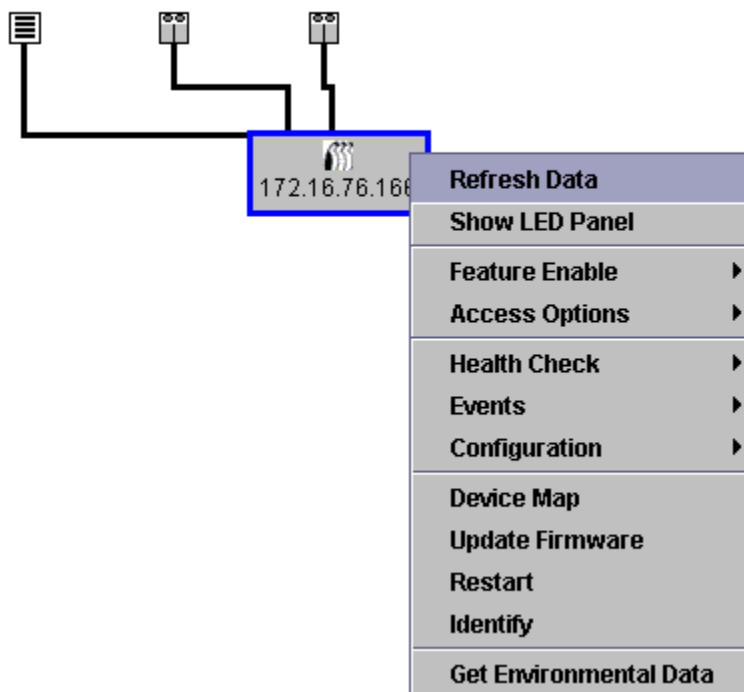
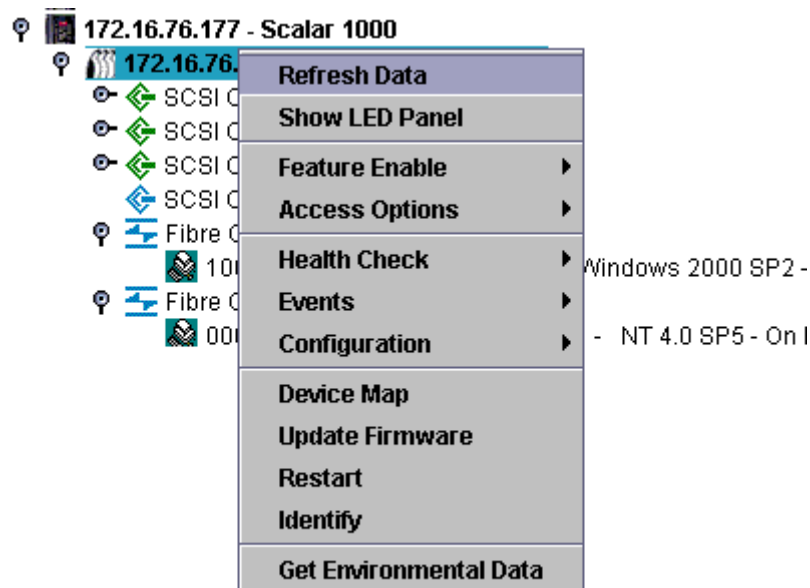


Figura 21 Selección con el botón derecho en la representación del equipo del panel de árbol



Actualización de datos

Al actualizar datos se visualizan los cambios de estado del host, el dispositivo y la conexión.



Nota

Después de agregar un dispositivo a un canal, debe volver a escanear el canal y a actualizar los datos del equipo.

Para actualizar el panel de árbol, el panel gráfico y el panel de datos

- 1 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.
- 2 Seleccione **Refresh Data**.

Los datos visualizados se actualizarán.



Nota

Si ha desactivado los avisos de captura de eventos, el comando **Refresh** no los activará. Para hacerlo deberá seguir los pasos descritos en [Recepción de capturas de eventos](#) en la página 70.

Guardar la configuración



ATENCIÓN

La mejor opción es guardar los archivos de configuración en una carpeta de un servidor que esté disponible continuamente. De esta forma, si se produce un fallo en el SNC, se podrá volver a configurar un SNC de repuesto rápidamente.

Los archivos que se guardan de esta forma incluyen el mapa de dispositivos, ajustes de puertos Fibre Channel y SCSI, ajustes de VPM, SFM y eVPS, y ajustes de zonificación por canales. El mapa de dispositivos es un registro de los ID de objetivo, LUNs de dispositivo y LUNs asignados.

Para copiar información de configuración esencial desde el equipo seleccionado

- 1 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.
- 2 Seleccione el menú **Configuration** y a continuación, **Save Configuration**.
- 3 Escriba un nombre para la configuración que desee guardar, o seleccione uno en la lista de configuraciones existentes en el servidor, si es posible.

Unos segundos después aparecerá el mensaje *Successfully received configuration from xxx.xxx.xxx.xxx* en el **Status/Message Area**.

- 4 Seleccione **Save Locally**.
- 5 Se abrirá un explorador de archivos.

De forma predeterminada muestra la subcarpeta “cfg” de la carpeta “Client”.

- 6 Seleccione **Save**.
- 7 Seleccione **Save on Server**.

Pocos segundos después aparecerá el mensaje *Configuration file saved successfully* en el **Status/Message Area**.



Nota

Es recomendable guardar la configuración localmente y en el servidor para garantizar el acceso al archivo.

- 8 Cuando haya terminado, haga clic en **Close**.

**ATENCIÓN**

Es importante guardar la configuración de cada equipo al principio y cuando se realicen cambios en los mapas de direcciones de dispositivo, en los parámetros de Fibre Channel o en los parámetros de canal SCSI.

Carga de un archivo local

Su representante del servicio técnico puede aconsejarle cargar en el SNC un archivo guardado.

Para cargar en un equipo de red SAN un archivo de configuración guardado localmente

- 1 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.

**ATENCIÓN**

Si reemplaza el equipo y no carga la configuración guardada, es posible que no pueda usar los dispositivos de almacenamiento conectados a él o que pierda los datos.

- 2 Seleccione el menú **Configuration** y a continuación, **Load a Local File**.
Se abrirá un explorador de archivos con los contenidos de la carpeta **Client**.
- 3 Si el archivo local se guardó en el directorio predeterminado, haga doble clic en la subcarpeta "cfg". También puede ir hasta la ubicación correspondiente. Seleccione el archivo que desee cargar.
- 4 Seleccione **Open** para cargar el archivo. Aparecerá un mensaje.
- 5 Haga clic con el botón derecho del ratón en el equipo para el que haya cargado la configuración, ya sea en el panel de árbol o en el panel gráfico.
- 6 Seleccione **Restart**. Consulte [Utilización del comando Restart](#) en la página 78.
En el **Status/Message Area** aparecerá *Restarting...Please Wait*.

Carga de un archivo desde el servidor

Si el servidor no es accesible, guarde las copias de la configuración en el servidor y en una ubicación a la que se pueda acceder.

Para cargar desde el servidor la configuración guardada

- 1 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.
- 2 Seleccione el menú **Configuration** y a continuación, **Load from Server**.
- 3 Seleccione el archivo que desee cargar.
- 4 Haga clic en **Load** para continuar con la carga.

Actualización del firmware

El comando **Update Firmware** sólo se puede utilizar con equipos. Para actualizar el firmware de un dispositivo conectado a un equipo, consulte [Gestión de dispositivos](#) en la página 87.

**Nota**

Para actualizar el firmware de algún componente de un sistema Scalar i2000 o Pathlight VX, consulte la documentación correspondiente.

Para actualizar el firmware de un equipo

- 1 Interrumpa toda actividad de E/S al equipo. Para ello, consulte el *Manual de usuario del hardware* del equipo.
- 2 Inicie la sesión como administrador de SAN, administrador del portal o usuario avanzado.



Nota

Los usuarios básicos no están autorizados para cargar firmware. Si el administrador del portal o el usuario avanzado tienen acceso a un portal, pero su acceso al equipo en el que se va a cargar el firmware es sólo parcial, únicamente podrá cargar el firmware el administrador de la red SAN.

- 3 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.
- 4 Una vez elegido el equipo, seleccione **Update Firmware**.
Se muestra un explorador de archivos.
- 5 Si el archivo de firmware que desea visualizar no se encuentra en la carpeta predeterminada, desplácese a la carpeta correcta.
- 6 Seleccione el archivo que desee cargar.
- 7 Haga clic en el botón **Open**.
Aparecerá un mensaje de advertencia.
- 8 Seleccione **Yes** para continuar.
El firmware tarda algunos minutos en cargarse. Cuando el firmware se termine de cargar aparecerá un mensaje en el **Status/Message Area**. Se le pedirá que reinicie el equipo.
- 9 **Reinicie (Restart)** el equipo. Consulte [Utilización del comando Restart](#) en la página 78.

Utilización del comando Restart

El comando **Restart** se utiliza cuando se ha actualizado el firmware o se han realizado cambios en las configuraciones del mapa de dispositivos, zonificación por canales, SFM o VPS.

Para reiniciar el equipo

- 1 Interrumpa toda actividad de E/S al equipo. Para ello, consulte el *Manual de usuario del hardware* del equipo.
- 2 Inicie la sesión como administrador de SAN, administrador del portal o usuario avanzado.



Nota

Los usuarios básicos no están autorizados para reiniciar un equipo. Si el administrador del portal o el usuario avanzado tienen acceso a un portal, pero su acceso al equipo que se va a reiniciar es sólo parcial, únicamente podrá reiniciar el equipo el administrador de la red SAN.

- 3 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.
- 4 Seleccione **Restart**.
Aparecerá un mensaje de advertencia.
- 5 Seleccione **Yes** para continuar.
Seleccione **No** para cancelar el reinicio.
Restarting...Please Wait aparecerá en el **Status/Message Area**.

Seguimiento de datos de entorno

No todos los equipos de la red SAN pueden ofrecer este tipo de datos. Si el equipo seleccionado no es capaz de proporcionar esta información, el menú del equipo no mostrará la opción **Get Environmental Data**.



Nota

Los datos de entorno de la biblioteca Scalar i2000 aparecen al seleccionar los botones de estado del sistema **Power** o **Cooling** situados en el extremo inferior de la pantalla de LMC. Los datos de entorno del sistema Pathlight VX aparecen en la interfaz VLI.

Para realizar un seguimiento de los datos de entorno de un equipo seleccionado

- 1 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.
- 2 Seleccione **Get Environmental Data**.
- 3 Se mostrará el cuadro de diálogo **Environmental Data**.

Las mediciones de tiempo real aparecen indicadas en cada gráfico por medio de agujas blancas.

El intervalo nominal de cada parámetro comprende todos los valores entre las barras amarillas.

Los intervalos de advertencia de cada parámetro comprenden los intervalos limitados por una barra amarilla y una roja en cada extremo.

Los intervalos de alarma de cada parámetro comprenden los intervalos limitados por una barra roja en un lado y nada en el otro en cada extremo.

- 4 Cuando haya terminado de visualizar los datos, haga clic en **OK**.

Los intervalos de datos de entorno pueden variar de un tipo de equipo a otro.

10

Configuración de canales y dispositivos

Cuando gestione la red SAN, es posible que desee volver a escanear o restablecer canales, cambiar el modo y las opciones de conexión o actualizar el firmware de dispositivos o unidades. AMC dispone de la estructura necesaria para satisfacer estas necesidades. Con AMC también se puede ajustar el mapa de dispositivos.

Gestión del canal SCSI

Si hace clic con el botón derecho del ratón en un canal SCSI de un equipo en red, podrá configurar directamente los parámetros del canal SCSI o volver a escanear y restablecer el canal al instante. Si se ha activado VPM, se podrán configurar sus parámetros. Consulte [Habilitación de funciones sujetas a licencia](#) en la página 91.

Volver a escanear el canal SCSI

Vuelva a escanear el bus SCSI después de agregar o quitar dispositivos.

Para volver a escanear el bus SCSI

- 1 En el panel de árbol o en el panel gráfico, amplíe el equipo.
- 2 Haga clic con el botón derecho del ratón en el gráfico del canal SCSI adecuado.
- 3 Seleccione **Rescan**.

Aparecerá un mensaje de advertencia.

- 4 Seleccione **Yes** para continuar.

En el **Status/Message Area** se mostrará el mensaje siguiente:

Rescanning SCSI Channel n on xxx.xxx.xxx.xxx. Please wait several minutes before doing a 'Refresh.'

En este ejemplo, la letra "n" corresponde al número de canal SCSI y xxx.xxx.xxx.xxx a la dirección IP del equipo.

- 5 Si ha vuelto a realizar un escaneado porque se ha agregado un dispositivo, continúe en [Actualización de datos](#) en la página 76.

Restablecer el canal SCSI

Mediante el comando **Reset** el equipo cancelará todos los comandos pendientes, se restablecerá el canal y se volverá a realizar un escaneado. Restablezca el canal SCSI después de realizar cambios a la configuración del canal.



ATENCIÓN

Utilice con cuidado la opción de restablecer ya que hace que los comandos de E/S pendientes devuelvan un estado de fallo al sistema operativo host y se pueden producir resultados inesperados. Antes de utilizar este comando, compruebe que se haya detenido toda actividad de E/S. Consulte el manual de usuario del hardware del equipo para obtener instrucciones y poder realizar estas acciones.

Para restablecer el canal SCSI

- 1 En el panel de árbol o en el panel gráfico, amplíe el equipo.
- 2 Haga clic con el botón derecho del ratón en el gráfico del canal SCSI adecuado.
- 3 Seleccione **Reset**.
Aparecerá un mensaje de advertencia.
- 4 Seleccione **Yes** para continuar.

En el **Status/Message Area** se mostrará el mensaje siguiente:

Resetting SCSI Channel n on xxx.xxx.xxx.xxx. Please wait several minutes before doing a 'Refresh'.

En este ejemplo, la letra "n" corresponde al número de canal SCSI y xxx.xxx.xxx.xxx a la dirección IP del equipo.

Configuración del canal SCSI

El comando **Configure** se utiliza para cambiar el modo de un canal SCSI, el ID del host, ajustes de restablecimiento y el estado de finalización.

Para ajustar los parámetros del canal SCSI

- 1 Inicie la sesión como administrador de SAN, administrador del portal o usuario avanzado.



Nota

Los usuarios básicos no están autorizados para configurar canales SCSI.



ATENCIÓN

Si cambia algún ajuste de los parámetros del canal SCSI, hay que restablecer el canal SCSI o reiniciar el equipo para hacer efectivos tales ajustes.

- 2 En el panel de árbol o en el panel gráfico, amplíe el equipo.
- 3 Haga clic con el botón derecho del ratón en el gráfico del canal SCSI adecuado.
- 4 Seleccione **Configure**.
Se mostrará el cuadro de diálogo **SCSI Channel Parameters**.
- 5 Utilice los cuadros desplegables y las casillas de verificación para realizar cambios en la configuración según sean necesarios.

Consulte los apartados [Modo de canal](#), [ID de host](#), [Restablecer bus al encendido](#), [Activar terminación](#) o [ID de iniciador alternativo](#) que aparecen a continuación.

- 6 Cuando haya termine de repasar o de establecer los parámetros del canal SCSI, seleccione **OK** para continuar.

En el **Status/Message Area** se mostrará el mensaje siguiente:

Pending changes on xxx.xxx.xxx.xxx.

En este ejemplo, xxx.xxx.xxx.xxx corresponde a la dirección IP del equipo.

Para cancelar todos los cambios y volver a la pantalla principal, seleccione **Cancel**.

- 7 Restablezca el canal. Consulte [Restablecer el canal SCSI](#) en la página 82.

Modo de canal

El **Channel Mode (modo de canal)** identifica el canal como un iniciador o un objetivo. Cuando se cambia un canal SCSI de modo objetivo a modo iniciador, los valores predeterminados que aparecen en los cuadros de ID de host y de ID de host alternativo no son 0. Los valores predeterminados que aparecen serán los que el equipo haya utilizado de forma más reciente.

ID de host

El **Host ID (ID de host)** normalmente tiene asignado un valor de 7.

Restablecer bus al encendido

La opción de **Bus Reset on Power Up (restablecer bus al encendido)** normalmente está activada. Si se anula la selección de esta casilla, se desactivará la opción de restablecer el bus al encendido.

Activar terminación

La opción **Enable Termination (Activar terminación)** normalmente está activada. Si se anula la selección de esta casilla, se desactivarán los circuitos internos de terminación.

ID de iniciador alternativo

Al **Alternate Initiator ID (ID de iniciador alternativo)** predeterminado lo ajusta automáticamente el equipo. Cuando el equipo escanea el bus SCSI, determina los ID que estén en ese momento en uso por los dispositivos objetivo y establece el ID alternativo al ID más alto que no esté en uso. Para cambiar el ID alternativo hay que utilizar la lista desplegable o escribir un número nuevo. Para restaurar el valor predeterminado automático, seleccione **Automatic** en la lista desplegable. Esta opción está desactivada cuando el canal SCSI está en modo objetivo.

Gestión de Fibre Channel

Para configurar directamente los parámetros Fibre Channel o volver a escanear y restablecer Fibre Channel al instante, hay que hacer clic con el botón derecho del ratón en el equipo de red Fibre Channel.

Volver a escanear Fibre Channel

Vuelva a escanear el bus Fibre Channel después de agregar o quitar dispositivos.

Para volver a escanear el bus Fibre Channel

- 1 En el panel de árbol o en el panel gráfico, amplíe el equipo.
- 2 Haga clic con el botón derecho del ratón en el gráfico de Fibre Channel adecuado.

3 Seleccione **Rescan**.

Aparecerá un mensaje de advertencia.

4 Seleccione **Yes** para continuar.

En el **Status/Message Area** se mostrará el mensaje siguiente:

Rescanning Fibre Channel n on xxx.xxx.xxx.xxx. Please wait several minutes before doing a 'Refresh.'

En este ejemplo, la letra “n” corresponde al número de Fibre Channel y xxx.xxx.xxx.xxx a la dirección IP del equipo.

Si ha vuelto a realizar un escaneado porque se ha agregado un dispositivo, continúe en [Actualización de datos](#) en la página 76.

Restablecer Fibre Channel

Mediante el comando **Reset** se cancelarán todos los comandos pendientes, se restablecerá el canal y se volverá a realizar un escaneado. Utilice este comando después de realizar cambios en la configuración de canal.



ATENCIÓN

Utilice con cuidado la opción de restablecer ya que hace que los comandos de E/S pendientes devuelvan un estado de fallo al sistema operativo host y se pueden producir resultados inesperados. Antes de utilizar este comando, compruebe que se haya detenido toda actividad de E/S. Consulte el manual de usuario del hardware del equipo para obtener instrucciones y poder realizar estas acciones.

Para restablecer Fibre Channel

1 En el panel de árbol o en el panel gráfico, amplíe el equipo.

2 Haga clic con el botón derecho del ratón en el gráfico de Fibre Channel adecuado.

3 Seleccione **Reset**.

Aparecerá un mensaje de advertencia.

4 Seleccione **Yes** para continuar.

En el **Status/Message Area** se mostrará el mensaje siguiente:

Resetting Fibre Channel n on xxx.xxx.xxx.xxx. Please wait several minutes before doing a 'Refresh.'

En este ejemplo, la letra “n” corresponde al número de Fibre Channel y xxx.xxx.xxx.xxx a la dirección IP del equipo.

Configuración de Fibre Channel

Los parámetros Fibre Channel que se pueden ajustar son el tipo de host, el ID de bucle, el tamaño de trama, el tipo de conexión y el modo de puerto.

Para ajustar los parámetros de Fibre Channel

1 Inicie la sesión como administrador de SAN, administrador del portal o usuario avanzado.



Nota

Los usuarios básicos no están autorizados para configurar canales Fibre Channel.



ATENCIÓN

Si cambia algún ajuste de los parámetros de Fibre Channel, habrá que restablecer el canal o reiniciar el equipo para hacer efectivos tales ajustes.

- 2 En el panel de árbol o en el panel gráfico, amplíe el equipo.
- 3 Haga clic con el botón derecho del ratón en el gráfico de Fibre Channel adecuado.
- 4 Seleccione **Configure**.
Se mostrará el cuadro de diálogo **Fibre Channel Parameters**.
- 5 Utilice los cuadros desplegados y las casillas de verificación para realizar cambios en la configuración según sean necesarios. Consulte [Descripción de las opciones de modo de puerto](#) en la página 85 y [Descripción de las opciones de tipo de conexión](#) en la página 86.
- 6 Cuando haya terminado de repasar o de establecer los parámetros de Fibre Channel, seleccione **OK** para continuar.

Aparecerá un mensaje de advertencia.

- 7 Seleccione **Yes** para continuar con el proceso de **Reset**.

En el **Status/Message Area** se mostrará el mensaje siguiente:

Resetting Fibre Channel n on xxx.xxx.xxx.xxx. Please wait several minutes before doing a 'Refresh.'

En este ejemplo, la letra “n” corresponde al número de Fibre Channel y xxx.xxx.xxx.xxx a la dirección IP del equipo.

Descripción de las opciones de modo de puerto

Los puertos Fibre Channel admiten conexiones Fibre Channel **Private (privadas)** y **Public (públicas)**. El modo de puerto predeterminado es **Public Target**. En este modo se pueden ver los ajustes y modificar los parámetros de puerto.

INICIADOR

En este modo, el puerto funciona a modo de iniciador, lo que permite la conexión de los objetivos Fibre Channel (discos, dispositivos de cinta o conmutadores FC).

OBJETIVO

En este modo el puerto funciona a modo de objetivo, lo que permite la conexión de un iniciador Fibre Channel (host o conmutador FC).

OBJETIVO E INICIADOR

En este modo, el equipo puede acceder a los dispositivos objetivo de Fibre Channel y los iniciadores del canal Fibre Channel pueden acceder a los objetivos conectados al equipo. El puerto funciona simultáneamente como objetivo e iniciador.

PRIVADO

Con esta opción, el equipo escanea el bucle local buscando dispositivos, pero sin considerar los dispositivos Fabric. Se aconseja seleccionar esta opción si conecta dispositivos objetivo directamente al puerto.

PÚBLICO

Mediante esta opción, el equipo escanea el bucle en busca de dispositivos Fabric. Si encuentra alguno, inicia la sesión y consulta al servidor de nombres si hay dispositivos objetivo disponibles para el dispositivo Fabric. Si encuentra dispositivos objetivo conectados al Fabric, los incluirá todos en el mapa de dispositivos. Se aconseja seleccionar esta opción si conecta un conmutador Fibre Channel al puerto y desea que el equipo acceda a todos los dispositivos objetivo disponibles conectados al conmutador. De lo contrario, si hay dispositivos objetivo conectados directamente al puerto, se cambiará automáticamente al modo **privado**.

Descripción de las opciones de tipo de conexión

Los puertos Fibre Channel admiten las conexiones de **Loop (bucle)** y **Point-to-Point (punto a punto)**. El ajuste de conexión predeterminado es **Loop**. En este modo se pueden ver los ajustes y modificar los parámetros de puerto.

BUCLE

Con esta opción, el puerto funcionará con dispositivos conectados capaces de formar bucle. Si se conecta un dispositivo punto a punto, el equipo no podrá establecer comunicación con el puerto.

PUNTO A PUNTO

Con esta opción, el puerto acepta la conexión Fabric punto a punto (F_Port Login). También funciona en “modo de puerto antiguo” para poder ser compatible con los dispositivos N_Port que no aceptan **Loop**. Si hay conectados dispositivos capaces de formar bucle, el equipo no podrá establecer una comunicación con ellos.

BUCLE PREFERIDO

Con esta opción, el puerto funciona en modo **Loop** a menos que detecte una conexión a un dispositivo N_Port. En tal caso, se cambia automáticamente al modo **Point-to-Point**.

Tipo de host

El **Host Type (tipo de host)** tiene muchos valores: **AIX**, **AS400**, **Gateway**, **HP-UX**, **Linux**, **NT** (incluye Windows 2000), **Netware**, **Generic**, **Solaris** y **Autosense/NT** (igual que “NT”). Los equipos host que se ejecuten en otros sistemas operativos utilizan el ajuste **Generic**. El ajuste predeterminado es **NT**. El tipo de host es el nombre del sistema operativo host o el tipo del equipo conectado al puerto. Con este ajuste se controla el modo con que el equipo conectado traduce los comandos SCSI (como el formato de los datos SCSI) que se tienen que presentar de una manera diferente a otros hosts. Si eVPS OR SFM está activado, se utilizará el ajuste del tipo de host mostrado en el panel de control eVPS OR SFM en lugar de este ajuste.

ID de bucle

El ajuste predeterminado del **Loop ID (ID de bucle)** es **Soft** y normalmente no se debería modificar. Cuando se utilizan conmutadores Fibre Channel, es conveniente utilizar un ajuste distinto del de **Loop ID**. Si elimina la selección de la casilla de verificación, puede escribir un valor de **Loop ID** de 0 a 125.

Tamaño de trama

El **Frame Size (tamaño de trama)** tiene tres valores posibles: 512, 1024 y 2048. El tamaño de trama de Fibre Channel lo especifica cada nodo receptor y no tiene que coincidir con otros nodos. Generalmente se debe fijar el tamaño de trama en 2048. Puede ser conveniente utilizar otro tamaño de trama si así lo requiere una aplicación particular de software.

Gestión de dispositivos

Este procedimiento sólo se aplica al firmware de dispositivos. Para actualizar el firmware del equipo, consulte [Actualización del firmware](#) en la página 77.

Para actualizar el firmware de un dispositivo

- 1 Interrumpa toda actividad de E/S al dispositivo. Para consultar instrucciones al respecto, consulte el *Manual de usuario del hardware* del equipo.
- 2 Inicie la sesión como administrador de SAN, administrador del portal o usuario avanzado.



Nota

Los usuarios básicos no están autorizados para cargar firmware. Si el administrador del portal o el usuario avanzado tienen acceso a un portal, pero su acceso al equipo en el que se va a cargar el firmware es sólo parcial, únicamente podrá cargar el firmware el administrador de la red SAN.

- 3 En el panel de árbol o en el panel gráfico, amplíe el equipo. Amplíe el canal adecuado.
- 4 Haga clic con el botón derecho del ratón en el gráfico del dispositivo.
- 5 Seleccione **Update Firmware**.
Se muestra un explorador.
Si el archivo de firmware que desea visualizar no se encuentra en la carpeta predeterminada, desplácese a la carpeta correcta.
- 6 Seleccione el archivo que desee cargar.
- 7 Haga clic en el botón **Open**.
Aparecerá un cuadro de diálogo de advertencia.
Asegúrese de que se ha interrumpido toda actividad de E/S al dispositivo.
- 8 Seleccione **Yes** para continuar.
Si no se puede detener la actividad de E/S al dispositivo o si desea realizar otra acción, seleccione **No** para cancelar la carga del firmware.
Si ha seleccionado **Yes**, se pedirá que **Restart** el equipo. Consulte [Utilización del comando Restart](#) en la página 78.

Edición de mapas de dispositivos

Algunas aplicaciones necesitan que los LUN se presenten en un orden distinto del que tienen cuando la rutina de detección los presenta al controlador SNC.

Para editar una base de datos de asignación de direcciones permanentes del equipo

- 1 Inicie la sesión como administrador de la SAN, administrador del portal o usuario avanzado.



Nota

Los usuarios básicos no están autorizados para configurar el mapa de dispositivos. Si el administrador del portal o el usuario avanzado tienen acceso a un portal, pero su acceso a la configuración de la asignación de dispositivos es sólo parcial, únicamente podrá modificar el acceso el administrador de la red SAN.

- 2 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en el equipo.

3 Seleccione **Device Map**.



ATENCIÓN

Si realiza cambios en las asignaciones de LUN de la base de datos de asignación de direcciones permanentes, estos cambios podrán afectar a los ajustes de acceso a SFM, eVPS y VPM. Si asigna distintos LUN a los dispositivos cuyo control de acceso se puede realizar por más de uno de estos métodos, un mismo LUN se podrá asociar a distintos dispositivos y se perderán los datos.

Se mostrará el cuadro de diálogo **Device Mapping**.

El cuadro de diálogo **Device Mapping** utiliza el formato de numeración de dispositivo “canal [ID objetivo:LUN de dispositivo]” tras el tipo de canal, “SCSI” o “Fibre”.

En la columna de la derecha aparecen imágenes desactivadas de estos mismos dispositivos, sin los LUN asignados.

El LUN 0 normalmente se asigna al “LUN de control” del equipo, a menos que se haya asignado manualmente a otro LUN.

Los dispositivos son LUN asignados por la detección inicial. Aparecen con letra en negrita a la izquierda.

- 4 Para reasignar el LUN, arrastre un dispositivo de la columna de la izquierda a la columna de la derecha o directamente a un lugar de la columna de la izquierda.



Nota

La columna de la derecha puede mantener temporalmente un elemento mientras se desplaza a un espacio abierto apropiado de la columna de la izquierda. No obstante, no se puede mantener ningún elemento en la columna de la derecha. Todos los elementos tienen que estar asignados a una posición de LUN en la columna de la izquierda.

Para eliminar un dispositivo, arrastre y suéltelo en el icono de la papelera de reciclaje.

- 5 Continúe hasta que se asignen todos los dispositivos.
- 6 Si está satisfecho con las asignaciones realizadas, seleccione **OK**.
- 7 Reinicie el equipo. Consulte [Utilización del comando Restart](#) en la página 78.
- 8 Reinicie el host o utilice otro método para garantizar que el host reconoce el nuevo mapa de dispositivos.

Asignación previa de números de dispositivos

El comando **New Device** se utiliza para asignar un LUN a un dispositivo que no esté presente en el sistema en ese momento y para el que no es adecuado un LUN de software (un LUN registrado por el controlador SND durante la detección).

El cambiador de medios normalmente será el primer LUN con número distinto (1) si está disponible o el primer LUN distinto disponible después de la última cinta.

Las aplicaciones o herramientas particulares pueden necesitar ajustes distintos de los predeterminados. Para codificar un LUN determinado para un dispositivo concreto, agréguelo al mapa de dispositivos en primer lugar. A continuación, pase el dispositivo a modo online.

Normalmente, los dispositivos pasan a modo online antes de que lo haga el controlador SNC. Cuando se inicia el controlador SNC, escanea todos los dispositivos y determina la ubicación de estos. Al final del proceso de inicio, el equipo de red reconocerá los LUN disponibles y podrá utilizarlos.

Para asignar un LUN a un dispositivo que ya no se encuentre en el sistema

- 1 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.
- 2 Seleccione **Device Map**.
- 3 Seleccione el cuadro de diálogo **Device Mapping**, acceda al menú **Tools** y seleccione **New Device**.
El nuevo dispositivo predeterminado es un dispositivo SCSI en el puerto (canal) 1, con el ID objetivo 0 y el LUN objetivo (LUN del dispositivo) 0.
- 4 Utilice los cuadros desplegados situados al final de cada campo para identificar el dispositivo de la forma correcta.
Si el dispositivo que se va a agregar es un dispositivo Fibre Channel, hay que incluir el ID de unidad correcto.
- 5 Seleccione **OK**.
Los dispositivos nuevos se mostrarán en la columna derecha del cuadro de diálogo **Device Mapping**.
- 6 Arrastre y suelte el dispositivo nuevo en una asignación de LUN.
- 7 Seleccione **OK**.
- 8 Vuelva a escanear el canal.
Consulte [Volver a escanear el canal SCSI](#) en la página 81 o [Volver a escanear Fibre Channel](#) en la página 83 según proceda.
- 9 Vuelva a detectar el segmento de red. Consulte [Detección de la red SAN](#) en la página 63.
- 10 Actualice los datos del equipo. Consulte [Actualización de datos](#) en la página 76.

Configuración del acceso a la red SAN

Además de proporcionar seguridad gracias a la asignación de privilegios, AMC permite configurar el acceso a la red SAN para un canal particular o grupo de LUNs, o desde la perspectiva de un determinado host.

Habilitación de funciones sujetas a licencia

Utilice el menú **Feature Enable** para habilitar las funciones sujetas a licencia para el equipo seleccionado. Las funciones que se deben habilitar antes de su uso son:

- Scalar® Firewall Manager (SFM)
- extended Virtual Private SAN® (eVPS)
- Asignación privada virtual (Virtual Private Map, VPM)
- Módulo organizador de datos (Data Mover Module)



Nota

Si la función ya está habilitada o no está disponible, el elemento de menú aparecerá sombreado en gris en la barra de menús.

Para habilitar funciones sujetas a licencia

- 1 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.
- 2 Seleccione el menú **Feature Enable**. A continuación, elija en el submenú la función que desee habilitar.



Nota

Las funciones opcionales disponibles para SNCs en la red SAN no son las mismas que las funciones opcionales de las bibliotecas Scalar i2000.

Si una función ya está habilitada o no está disponible para un equipo determinado, aparecerá sombreada en gris en el menú.

- 3 Escriba la clave de licencia de la función que desee habilitar. Si la función ha sido habilitada de fábrica, escriba la palabra **enable**.
- 4 Seleccione **OK** para continuar.
- 5 Si ha habilitado SFM, continúe con [Utilización de Scalar Firewall Manager \(SFM\)](#) en la página 96.
Si ha habilitado eVPS, continúe con [Utilización de eVPS](#) en la página 101.
Si ha habilitado VPM, continúe con [Utilización de VPM](#) en la página 107.
Si ha habilitado el módulo organizador de datos, no es necesario configurar otros ajustes.

Módulo organizador de datos



Nota

Los usuarios básicos no están autorizados para habilitar el módulo organizador de datos. Para obtener información sobre los privilegios de usuario, consulte la [tabla 2](#) en la página 42.

El módulo organizador de datos permite utilizar aplicaciones de copia de seguridad en cinta sin servidor que sean compatibles con el comando de copia ampliada SCSI de SNIA. Si se habilita esta función, el equipo de red podrá mover bloques de datos directamente entre los dispositivos de almacenamiento a los que está conectado.

Utilización de la zonificación por canales

La zonificación por canales (o “zonificación por puertos”) configura el acceso a un canal objetivo completo y a todos los LUN de ese canal para el uso exclusivo de un host o grupo de hosts en un único canal iniciador. Cada canal iniciador puede conectarse a un máximo de 64 hosts.

Un LUN (número de unidad lógica) es un identificador de 3 bits utilizado en un bus SCSI para distinguir hasta ocho dispositivos con el mismo ID SCSI.

En una situación donde los dispositivos son dispositivos de cinta y hay más de un host conectado al canal iniciador, la aplicación de biblioteca de cintas suele gestionar las peticiones del host al canal zonificado.

Para configurar la zonificación por canales

- 1 Inicie la sesión como administrador de la SAN, administrador del portal o usuario avanzado.



Nota

Los usuarios básicos no están autorizados para configurar la zonificación por canales. Si el administrador del portal o el usuario avanzado tienen acceso a un portal, pero su acceso a la configuración de la zonificación por canales es sólo parcial, únicamente podrá modificar el acceso el administrador de la red SAN.

- 2 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en un equipo.
- 3 En el menú **Access Options**, seleccione **Channel Zoning**.

La configuración predeterminada permite que todas las conexiones de la red SAN accedan a todos los canales objetivo.

- 4 Utilice las casillas de verificación para crear o eliminar zonas de acceso restringido para las conexiones deseadas en la SAN y los canales objetivo.

Todas las combinaciones son posibles.

Tenga en cuenta que cuando se marca una casilla de verificación se zonifica el canal entero.

Si realiza cambios en los ajustes de zonificación por canales, deberá reiniciar el equipo de red para que los nuevos parámetros se apliquen.

- 5 Para copiar o imprimir en un archivo de texto los ajustes de zonificación por canales, seleccione el menú **Tools** en el cuadro de diálogo **Channel Zoning**. A continuación, seleccione **Copy Channel Zoning** o **Print Channel Zoning**.



ATENCIÓN

Si crea zonas de acceso restringido con la zonificación por canales, SFM, eVPS y VPM sólo podrán asignar permisos de acceso dentro de cada zona accesible. Para más información, consulte [Utilización de Scalar Firewall Manager \(SFM\)](#) en la página 96, [Utilización de eVPS](#) en la página 101 o [Utilización de VPM](#) en la página 107.

- Haga clic en **OK** para aplicar los cambios realizados.
Haga clic en **Cancel** para no aplicar los cambios en la zonificación por canales.

Instalación de HRS

El servicio de registro de host (Host Registration Service, HRS) presenta información de host que los SNC y MCB utilizan para gestionar el acceso de hosts y la recuperación de datos. La información presentada incluye el nombre, el tipo y la conexión de host, así como el estado online u offline. Esta información se envía periódicamente a través de la conexión de canal Fibre Channel del host. De forma predeterminada, el HRS repite el registro del host cada cinco minutos. Puede cambiar este intervalo a cualquier valor entre 1 y 255 minutos.

Una vez instalado el servicio HRS, para obtener ayuda sólo tiene que escribir

```
hrs -h
```

en la línea de comandos y pulsar **Enter**.

AMC utiliza HRS para facilitar el uso de **SFM**, **eVPS** y **VPM**, que son esquemas de asignación de LUNs. Para obtener más información sobre estas herramientas, consulte [Utilización de Scalar Firewall Manager \(SFM\)](#) en la página 96, [Utilización de eVPS](#) en la página 101 y [Utilización de VPM](#) en la página 107.



Nota

Si desea utilizar **SFM**, **eVPS** o **VPM**, instale HRS en los hosts apropiados. Si no va a utilizar **SFM**, **eVPS** ni **VPM**, puede gestionar la red SAN sin instalar HRS. No obstante, HRS garantiza que el condicionamiento de rutas de datos incluya la parte del host de la ruta de datos.

Instalación del servicio de registro de host en sistemas Windows

Este software se instala en un equipo host con Windows conectado a un SNC, MCB o a un chasis de red.

Para instalar HRS en Windows

- Compruebe que el host Windows que está configurando tiene instalado un adaptador de bus de host (HBA).
- Solicite a su representante del servicio técnico el archivo `HstRegSrv.exe`.
- Haga clic en el botón **Inicio** de Windows y seleccione **Ejecutar**.
- Indique `HstRegSrv.exe`.
- Seleccione **OK**.
- Una vez finalizada la instalación, reinicie el sistema.
HRS se ejecutará como un servicio, por lo que se iniciará al arrancar el equipo.

**Nota**

En un sistema Windows, el intervalo de repetición del registro no se puede modificar, ya que HRS se ejecuta como servicio, y no como programa independiente.

Instalación del servicio de registro de host en sistemas Solaris

Este software se instala en un equipo host con Solaris conectado a un SNC, MCB o a un chasis de red.

**Nota**

Antes de instalar HRS, debe desinstalar cualquier versión anterior en el equipo Solaris.

Para instalar HRS en Solaris

- 1 Compruebe que el host Solaris que está configurando tiene instalado un adaptador de bus de host (HBA).
- 2 Solicite a su representante del servicio técnico el archivo `HstRegSrv.tar`.
- 3 En la línea de comandos, escriba

```
ps -A | grep hrs
```

y pulse **Enter**.

Si se encuentra una versión anterior de HRS, aparecerá un mensaje parecido a éste:

```
<219 ? 0:00 hrs>
```

- 4 Si no aparece ningún mensaje similar al indicado en el [paso 3](#), continúe con el [paso 6](#).
Si aparece el mensaje, escriba

```
pkgrm <nombre del paquete>
```

y pulse **Enter**.

- 5 Si ha eliminado un paquete, reinicie el host:

```
reboot -- -r
```

- 6 Inserte el CD del producto en el host Solaris.
- 7 Localice el archivo `HstRegSrv.tar`.
- 8 Copie `HstRegSrv.tar` en un directorio temporal.
- 9 En el directorio que contenga el archivo `HstRegSrv.tar`, escriba

```
tar xf HstRegSrv.tar
```

y pulse **Enter**.

- 10 Escriba el siguiente comando

```
pkgadd -d .
```

y pulse **Enter**.

- 11 Escriba el siguiente comando

```
reboot -- -r
```

y pulse **Enter**.

El HRS se ejecuta cuando arranca el sistema. El archivo que controla este proceso es `s99hrs`, que se encuentra en la carpeta `/etc/rc2.d`

El intervalo predeterminado de repetición del registro es de 5 minutos.

Para cambiar el intervalo

- 1 Localice el PID del proceso de HRS actual. Escriba

```
ps -ef | grep hrs
```

y pulse **Enter**.

- 2 De esta forma se cancelará el proceso de HRS. Escriba

```
kill -9 [PID]
```

y pulse **Enter**.

- 3 Reinicie HRS. En la frase entre paréntesis, escriba el número de minutos que desee que transcurran entre los registros. Escriba

```
hrs -i[intervalo en minutos] -D &
```

y pulse **Enter**.

Esto hará que HRS se ejecute en segundo plano como demonio, registrándose según el intervalo especificado.

Instalación del servicio de registro de host en sistemas HP-UX

Este software se instala en un equipo host con HP-UX conectado a un SNC, MCB o a un chasis de red.

Para instalar HRS en un sistema HP-UX

- 1 Compruebe que el host HP-UX que está configurando tiene instalado un adaptador de bus de host (HBA).

- 2 Solicite a su representante del servicio técnico el archivo HstRegSrv.depot.

- 3 En la línea de comandos, escriba

```
sam
```

y pulse **Enter**.

- 4 En el menú **Software Management**, seleccione **Install Software on the Local Host**.

- 5 Detrás de **Source Host Name**: escriba el nombre de su host.

- 6 Detrás de **Source Depot Path**: escriba el nombre del directorio que contenga el archivo *.depot.

Escriba el nombre completo del archivo, HstRegSrv.depot.

- 7 Seleccione **OK**.

- 8 En el menú **Action**, seleccione **Install (analysis...)**

- 9 En la ventana de confirmación, seleccione **Yes**.

- 10 Haga clic en **Done** cuando termine el proceso de instalación.

El software HRS quedará ubicado en **/usr/contrib/bin**

- 11 Reinicie el equipo.

- 12 De forma opcional puede cambiar el intervalo de repetición del registro. Para ello, escriba

```
hrs -i[intervalo en minutos] -D &
```

y pulse **Enter**.

Esto hará que HRS se ejecute en segundo plano como demonio, registrándose según el intervalo especificado.

El intervalo predeterminado de repetición del registro es de 5 minutos.

Instalación del servicio de registro de host en sistemas AIX

Este software se instala en un equipo host con AIX conectado a un SNC, MCB o a un chasis de red.

Para instalar HRS en un sistema AIX

- 1 Compruebe que el host AIX que está configurando tiene instalado un adaptador de bus de host (HBA).
- 2 Solicite a su representante del servicio técnico el archivo `HstRegSrv.bff`.

- 3 En la línea de comandos, escriba

```
smit
```

y pulse **Enter**.

- 4 En el menú **Software Installation and Maintenance**, seleccione **Install and Update Software**. A continuación, seleccione **Install and Update Software by Package Name (includes devices and printers)**.

- 5 Indique la ruta de acceso al archivo `HstRegSrv.bff` en la línea de comandos, o seleccione el botón **List** en la parte derecha de la pantalla para seleccionar este archivo.

Si introduce la ruta, asegúrese de incluir el nombre de archivo `HstRegSrv.bff`.

- 6 Cuando se le pida que seleccione los paquetes (**Select Packages to List**), seleccione **package**.
- 7 Cuando se le pida que seleccione el software para su instalación (**Select Software to Install**), seleccione **1.13.0.0 ADIC Host Registration Service**.

El software se instalará.

- 8 Reinicie el equipo.

- 9 De forma opcional puede cambiar el intervalo de repetición del registro. Para ello, escriba

```
hrs -i[intervalo en minutos] -D &
```

y pulse **Enter**.

Esto hará que HRS se ejecute en segundo plano como demonio, registrándose según el intervalo especificado.

El intervalo predeterminado de repetición del registro es de 5 minutos.

Utilización de Scalar Firewall Manager (SFM)

Scalar® Firewall Manager (SFM) es una función de software que recopila toda la información de host y objetivo y gestiona el control de acceso en toda la red SAN. Permite al administrador del sistema controlar los privilegios de acceso entre adaptadores de bus de host (HBA) y los dispositivos objetivo conectados a los canales SCSI y Fibre Channel del equipo.



Nota

Si utiliza un SNC fuera de una biblioteca Scalar, la función SFM se llamará Virtual Private SAN (VPS). Estas instrucciones también son aplicables al uso de VPS. Cuando se especifique "SFM", sólo tiene que cambiarlo por "VPS".

SFM permite un mayor control del acceso que la zonificación por canales. La función **Channel Zoning** permite asignar un canal entero a uno o varios hosts especificados. SFM asigna los LUN seleccionados en canales determinados a un host especificado de la red SAN.

SFM se puede utilizar para permitir que múltiples hosts Fibre Channel conectados a través de conmutadores y concentradores compartan los mismos canales SCSI o Fibre Channel, restringiendo a la vez su acceso a los LUN seleccionados en esos canales.

No es necesario adquirir una licencia de SFM si se va a utilizar para gestionar el control del acceso en redes SAN formadas por bibliotecas FC ADIC.



Nota

Si migra a extended VPS (eVPS), las asignaciones se deberán gestionar a través de eVPS. La pantalla de SFM está inhabilitada como resultado de la migración.

Instalación de SFM

La instalación de SFM en un sistema con una red SAN desarrollada es distinta de la instalación de SFM en un nuevo sistema.

Para instalar SFM

- 1 Inicie la sesión como administrador de la SAN, administrador del portal o usuario avanzado.



Nota

Los usuarios básicos no están autorizados para configurar SFM. Si el administrador del portal o el usuario avanzado tienen acceso a un portal, pero su acceso a la configuración de SFM es sólo parcial, únicamente podrá modificar el acceso el administrador de la red SAN.

- 2 Si desea instalar el servicio de registro de host (HRS) en los hosts correspondientes, consulte al representante del servicio técnico.
- 3 Si instala SFM como parte de una nueva instalación de red SAN, continúe con el [paso 4](#). Para instalar HRS en una red SAN ya existente, continúe con el [paso 5](#).
- 4 Si instala SFM en una red SAN ya existente, siga estos pasos:
 - a. Instale HRS en los hosts.
 - b. Deje que se ejecuten los hosts.
 - c. Habilite SFM. Consulte [Habilitación de funciones sujetas a licencia](#) en la página 91.
 - d. Haga clic con el botón derecho del ratón en el equipo que tiene habilitado SFM.
 - e. Seleccione **Refresh Data**. Consulte [Actualización de datos](#) en la página 76.
 - f. Continúe con el [paso 6](#).
- 5 Si instala SFM en una red SAN nueva, siga estos pasos:
 - a. Cargue HRS en los hosts.
 - b. Apague los hosts.
 - c. Reinicie el equipo. Consulte [Utilización del comando Restart](#) en la página 78.
 - d. Inicie los hosts.
 - e. Habilite SFM. Consulte [Habilitación de funciones sujetas a licencia](#) en la página 91.
 - f. Una vez haya finalizado el inicio de los hosts, haga clic con el botón derecho del ratón en el equipo con SFM habilitado.
 - g. Seleccione **Refresh Data**. Consulte [Actualización de datos](#) en la página 76.
 - h. Continúe con el [paso 6](#).
- 6 Amplíe todos los iconos de nodos para mostrar todos los hosts, dispositivos y sus LUN asignados. Consulte [Numeración de los dispositivos](#) en la página 32.

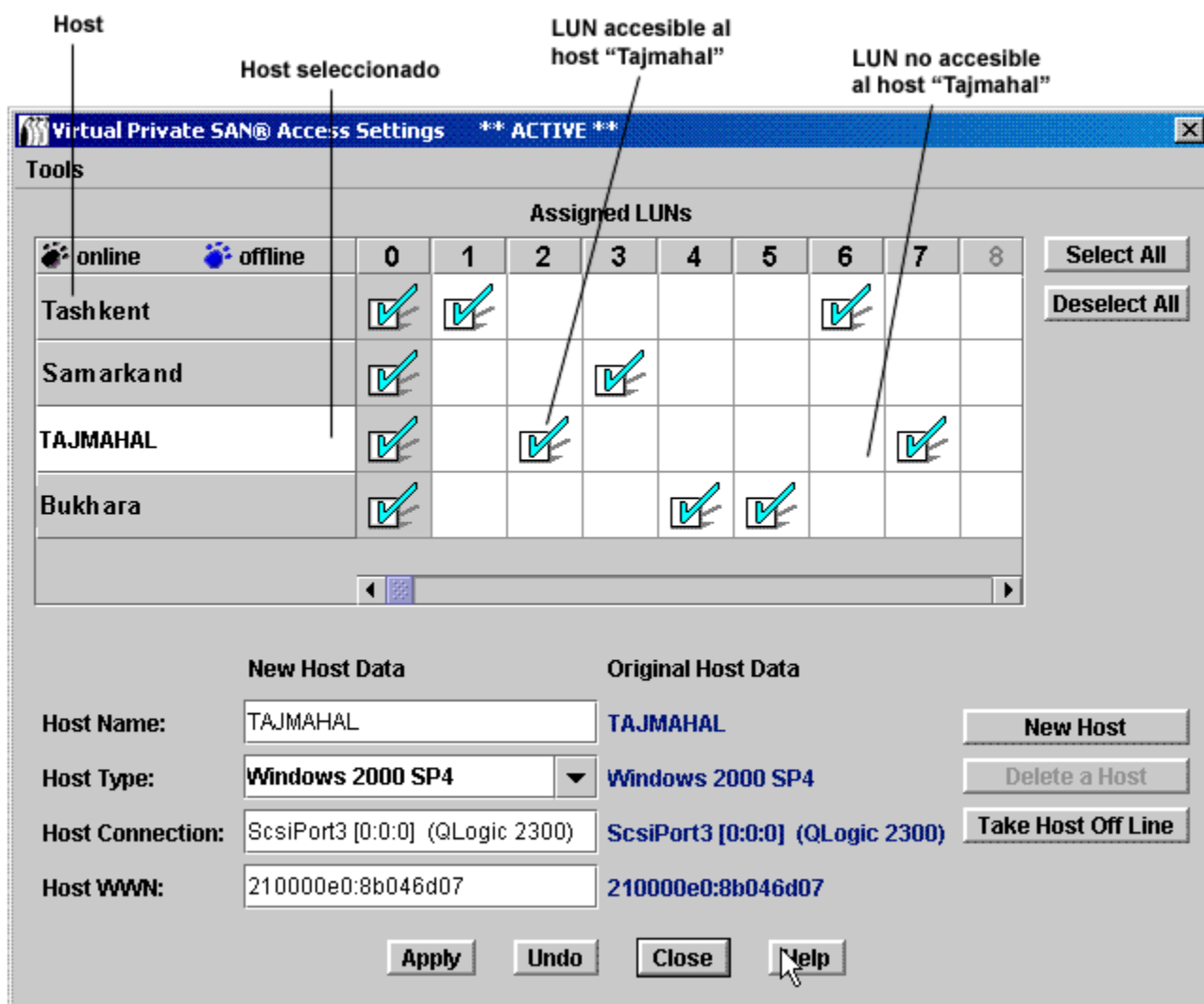
Configuración del acceso a través de SFM

Configure el acceso a ciertos LUN para ciertos hosts. El resto no podrá ver estos LUN.

Para asignar LUNs a hosts

- 1 Realice una lista con los LUN que desee asignar y a qué hosts.
- 2 En el panel de árbol o en el panel gráfico, haga clic con el botón derecho del ratón en el equipo que tenga SFM habilitado.
- 3 En el menú **Access Options**, seleccione **Scalar® Firewall Manager**.
Se abrirá el cuadro de diálogo **Scalar® Firewall Manager Access Settings**. Consulte la [figura 22](#) en la página 98.

Figura 22 Cuadro de diálogo de configuración de acceso de Scalar Firewall Manager




La [figura 22](#) identifica los componentes del cuadro de diálogo **Scalar® Firewall Manager Access Settings**.

Los hosts registrados se muestran en la columna de la izquierda. Cuando un host está online, su nombre aparece en negro.

Cuando un host está registrado pero no está online en este momento, aparece en azul.

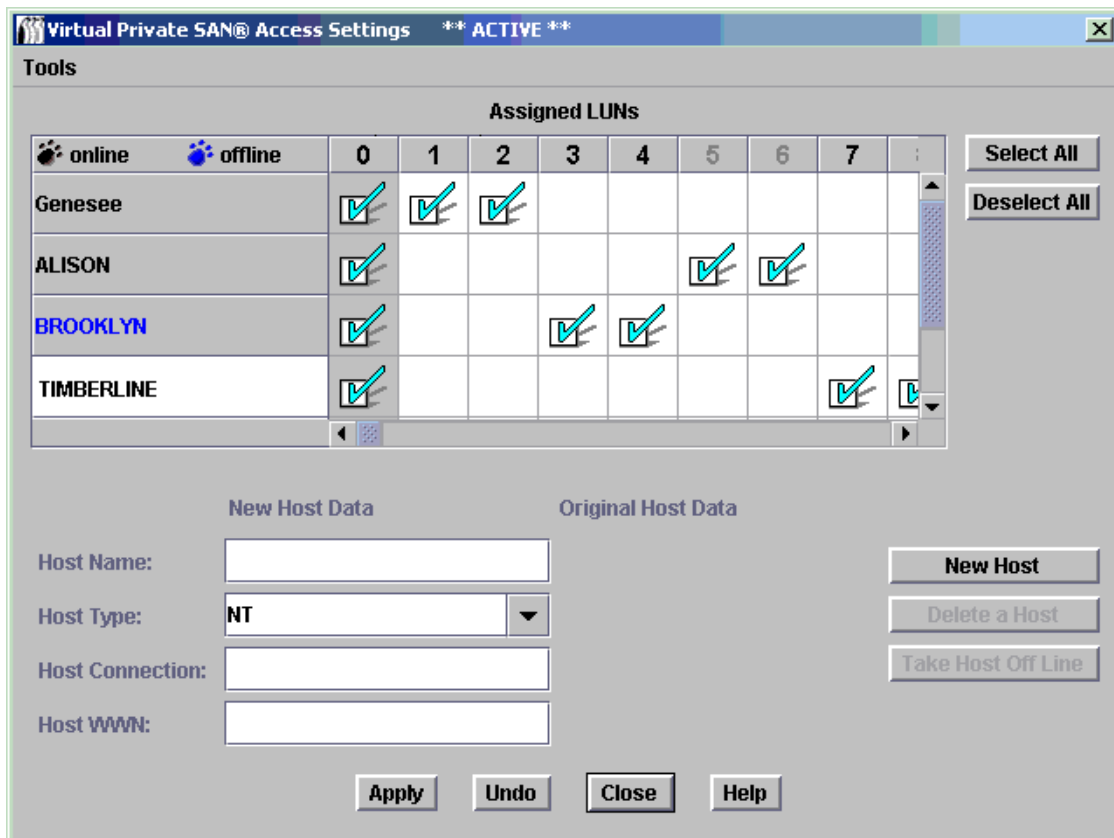
Para que toda la información de host aparezca en pantalla, primero debe ejecutar HRS. Póngase en contacto con su representante del servicio técnico.

 **Nota** Mueva el puntero sobre un LUN o un host para ver los detalles en una ventana emergente azul.

- 4 Seleccione las casillas situadas bajo **Assigned LUN** para indicar que un LUN puede acceder al host correspondiente. Vuelva a seleccionar una casilla para revocar el acceso.
 - Para seleccionar o anular los LUN de una la línea de host particular se utilizan los botones **Select All** o **Deselect All** situados en la parte derecha de la ventana.
 - Para seleccionar o anular el acceso a todos los LUN de un host, localice su nombre en la lista de hosts situada en la esquina superior izquierda de la pantalla y selecciónelo. A continuación, haga clic en **Select All** o **Deselect All**.

La [figura 23](#) en la página 99 muestra LUNs asignados de forma que ningún otro host pueda acceder a ellos.

Figura 23 LUNs limitados a acceso selectivo por parte de cuatro hosts



- 5 Seleccione **Apply** para aplicar los cambios realizados en los campos de datos de hosts y en las asignaciones de LUNs.

Seleccione el botón **Undo** para desechar todos los cambios realizados desde la última vez que se seleccionó **Apply**.

Para cerrar el cuadro de diálogo, haga clic en **Close** o seleccione el botón **x** situado en la esquina superior derecha del cuadro de diálogo. Si ha realizado algún cambio, aparecerá un cuadro de diálogo ofreciendo la posibilidad de aplicar los cambios antes de cerrar el cuadro.

Haga clic en **Help** si desea ayuda contextual.

- 6 Guarde la configuración. Consulte [Guardar la configuración](#) en la página 76.

Agregar hosts SFM

Los hosts se pueden agregar a la red SAN tras la configuración inicial de SFM.

Para agregar nuevos hosts a la SAN

- 1 Seleccione el botón **New Host** para agregar manualmente un nuevo host al sistema.

Los cuadros de texto situados en la esquina inferior izquierda quedarán habilitados. Si no dispone de los datos para esos campos, el servicio de registro de host (HRS) los detectará automáticamente. Para instalarlo, póngase en contacto con su representante del servicio técnico.

- 2 Rellene el campo **Host Name** y el resto de cuadros de texto.
 - Seleccione el **tipo de host**, es decir, el sistema operativo o tipo de equipo adecuado, en la lista desplegable **Host Type**.
 - En el campo **Host Connection** se indica el número de puerto al que se conecta el host, la dirección IP del host y la información sobre el HBA.
 - Debe conocer el número World Wide Name para introducirlo manualmente.
- 3 Cuando haya acabado, seleccione **Accept New Host** o **Quit New Host**.
- 4 Haga clic en el botón **Apply** para aplicar los cambios realizados en los campos de datos del host y en las asignaciones de LUNs.
- 5 Guarde la configuración. Consulte [Guardar la configuración](#) en la página 76.

Eliminación de hosts SFM

Los hosts se pueden eliminar de la red SAN tras la configuración inicial de SFM.

Para eliminar permanentemente un host de una red SAN

- 1 Seleccione el nombre del host en el cuadro de diálogo **SFM Access Settings**.

En la [figura 23](#) en la página 99, los hosts online son Genesee, Alison y Timberline.

Si un host está online, no se podrá eliminar hasta que se seleccione el botón **Take Host Off Line**.

Una vez seleccionado un host, sus datos aparecerán en la parte inferior del cuadro de diálogo.

- 2 Seleccione el botón **Delete a Host**.
- 3 Haga clic en el botón **Apply** para aplicar los cambios realizados en los campos de datos del host y en las asignaciones de LUNs.

Seleccione el botón **Undo** para desechar todos los cambios realizados desde la última vez que se seleccionó **Apply**.

Para cerrar el cuadro de diálogo, haga clic en **Close** o seleccione el botón **x** situado en la esquina superior derecha del cuadro de diálogo. Si ha realizado algún cambio, aparecerá un cuadro de diálogo ofreciendo la posibilidad de aplicar los cambios antes de cerrar el cuadro.

- 4 Guarde la configuración. Consulte [Guardar la configuración](#) en la página 76.

Utilización de eVPS

El control del acceso conseguido con SFM para la asignación de LUNs en la red SAN se puede ampliar a la asignación de LUNs por host utilizando eVPS (extended Virtual Private SAN).



Nota

Si migra a eVPS, las asignaciones se deberán gestionar a través de eVPS. Las pantallas de SFM están inhabilitadas como resultado de la migración.

Con eVPS se consigue un acceso de gestión más rápido y sencillo a los LUN asignados. Todos los hosts ven los LUN a los que tienen acceso comenzando por LUN 1, en lugar de comenzar por un número de LUN potencialmente alto, como es el LUN del dispositivo. Al igual que SFM, eVPS se puede utilizar para permitir que múltiples hosts Fibre Channel conectados a través de conmutadores y concentradores compartan los mismos canales SCSI o Fibre Channel, restringiendo a la vez su acceso a los LUN seleccionados en esos canales.

- Utilice eVPS para asignar LUNs a un determinado host.
- El número total de LUNs que se puede asignar es 2.048.
- El número total de LUNs que se puede asignar por host es 256.

Para utilizar eVPS es necesario adquirir una licencia.



ATENCIÓN

Los productos Windows Server admiten hasta 254 LUNs por ID de objetivo.

Instalación de eVPS

La instalación de eVPS en un sistema con una red SAN desarrollada es distinta de la instalación de eVPS en un nuevo sistema.



Nota

Los usuarios básicos no están autorizados para configurar eVPS. Si un administrador del portal o usuario avanzado tiene acceso a un portal, pero su acceso a la configuración de eVPS es sólo parcial, únicamente podrá modificar el acceso el administrador de la red SAN.

Para instalar eVPS

- 1 Inicie la sesión como administrador de la SAN, administrador del portal o usuario avanzado.



ATENCIÓN

Si ha realizado asignaciones de zonificación por canales, revíselas para asegurarse de que no provocan problemas al coexistir con las asignaciones de eVPS. Si la red SAN tiene un gran número de hosts, no se debe ejecutar la zonificación por canales simultáneamente con eVPS.

- 2 Si desea instalar el servicio de registro de host (HRS) en los hosts correspondientes, consulte al representante del servicio técnico.
- 3 Si instala eVPS como parte de una nueva instalación SAN, continúe con el paso 5. Para obtener información sobre la instalación en una red SAN ya existente, continúe con el [paso 4](#).
- 4 Si instala eVPS en una red SAN ya existente, siga estos pasos:

- a. Instale HRS en los hosts.
 - b. Deje que se ejecuten los hosts.
 - c. Habilite eVPS. Consulte [Habilitación de funciones sujetas a licencia](#) en la página 91.
 - d. Haga clic con el botón derecho del ratón en el equipo que tiene habilitado eVPS.
 - e. Seleccione **Refresh Data**. Consulte [Actualización de datos](#) en la página 76.
 - f. Continúe con el [paso 6](#).
- 5 Si instala eVPS en una red SAN nueva, siga estos pasos:
- a. Cargue HRS en los hosts.
 - b. Apague los hosts.
 - c. Reinicie el equipo. Consulte [Utilización del comando Restart](#) en la página 78.
 - d. Inicie los hosts.
 - e. Habilite eVPS. Consulte [Habilitación de funciones sujetas a licencia](#) en la página 91.
 - f. Una vez haya finalizado el inicio de los hosts, haga clic con el botón derecho del ratón en el equipo con eVPS habilitado.
 - g. Seleccione **Refresh Data**. Consulte [Actualización de datos](#) en la página 76.
 - h. Continúe con el [paso 6](#).
- 6 Amplíe todos los iconos de nodos para mostrar todos los hosts, dispositivos y sus LUN asignados. Consulte [Numeración de los dispositivos](#) en la página 32.

Configuración del acceso a través de eVPS

Configure el acceso a ciertos LUN para un host determinado, comenzando la numeración de LUNs por 1. El host ya no tendrá que escanear todo el bus para ver los dispositivos con LUNs altos a los que tiene acceso. Estos LUN aparecerán para el host como si su numeración empezara por 1. Una vez realizada la asignación, el resto de hosts dejará de ver los LUN asignados a un host determinado. Esta asignación se puede llevar a cabo desde dos puntos de vista:

- El punto de vista del equipo
- El punto de vista del host

Para asignar LUNs a hosts desde el punto de vista del equipo

- 1 Realice una lista con los LUN que desee asignar y a qué hosts. Se puede conectar a Fibre Channel un máximo de 64 hosts.
- 2 Haga clic con el botón derecho del ratón en el equipo que tiene habilitado eVPS.
- 3 En el menú **Access Options**, seleccione **Extended Virtual Private SAN®**.
Aparecerá el cuadro de diálogo **eVPS Access Settings**.

Figura 24 Asignaciones de eVPS para los LUN 0-9

Extended Scalar® Firewall Manager Access Summary ** ACTIVE **

Host View

Internal LUNs

<input checked="" type="checkbox"/> online <input type="checkbox"/> offline	0	1	2	3	4	5	6	7	8	9	10
<input checked="" type="checkbox"/> ASAHI	0	1	2	3							
<input checked="" type="checkbox"/> malloy	0				1	2	3				
<input checked="" type="checkbox"/> malone	0							1	2	3	

OK Cancel Help

Compare los LUN internos en la [figura 24](#) con los LUN asignados en el panel de árbol que aparece en la [figura 25](#) en la página 103.

Figura 25 LUNs 1-9 asignados en el panel de árbol

ADIC Management Console

Session View Admin Category Help

SFMView - Portal1 - Master Portal

- 172.16.76.166 - Scalar 100
 - 172.16.76.166 - SNC 5101
 - SCSI Channel - 1
 - Medium Changer [6:0] - 1
 - SCSI Channel - 2
 - Tape Device [1:0] - 2
 - SCSI Channel - 3
 - Tape Device [0:0] - 3
 - SCSI Channel - 4
 - Fibre Channel - 1
 - Fibre Channel - 2
 - 172.16.76.157 - Gateway_157 - ADIC 3000
 - SCSI Channel - 1
 - Disk Device [0:0] - 4
 - Disk Device [0:1] - 5
 - Disk Device [0:2] - 6
 - Disk Device [0:3] - 7
 - Disk Device [0:4] - 8
 - Disk Device [0:5] - 9
 - SCSI Channel - 2
 - SCSI Channel - 3
 - SCSI Channel - 4
 - Fibre Channel - 1
 - Fibre Channel - 2
 - Fibre Channel - 3
 - Fibre Channel - 6

Up Time: 61 days 02:58:28

Genesee Malloy

Name	Value
World Wide Node Name	10006045:1745B
IP Address	172.16.76.166
Firmware Revision	4.20.02
Serial Number	601115
Log Size	190
Serial Baud Rate	19200
Health Check Level	2
Health Check Interval	30
Receive Event Traps	Enabled
Ethernet Type	UNK base-T
UDP Port	162
Extended SFM Enabled	Yes
VPM Enabled	No

TRAP !

En la [figura 24](#) en la página 103, los hosts registrados se muestran en la columna de la izquierda. Cuando un host está online, su nombre aparece en negro. Cuando un host está registrado pero no está online en este momento, aparece en azul.

El número en la fila "Internal LUN" aparece en negro si el LUN está online. De lo contrario, su número aparecerá sombreado en gris.

Para que toda la información de host aparezca en pantalla, primero debe ejecutar HRS. Póngase en contacto con su representante del servicio técnico.

- 4 Escriba un número en una casilla de verificación de LUN interno para indicar que el acceso entre un LUN y el host correspondiente está habilitado.

Borre el número para cancelar el acceso.

En la [figura 24](#) en la página 103, a cada host se le han asignado LUNs a los que reconocerá como LUNs 0 a 3.

- 5 Haga clic en el botón **OK** para aplicar los cambios realizados en los campos de datos del host y en las asignaciones de LUNs.

Haga clic en el botón **Cancel** para cancelar todos los cambios.

Haga clic en el botón **Help** si desea ver una ayuda contextual.

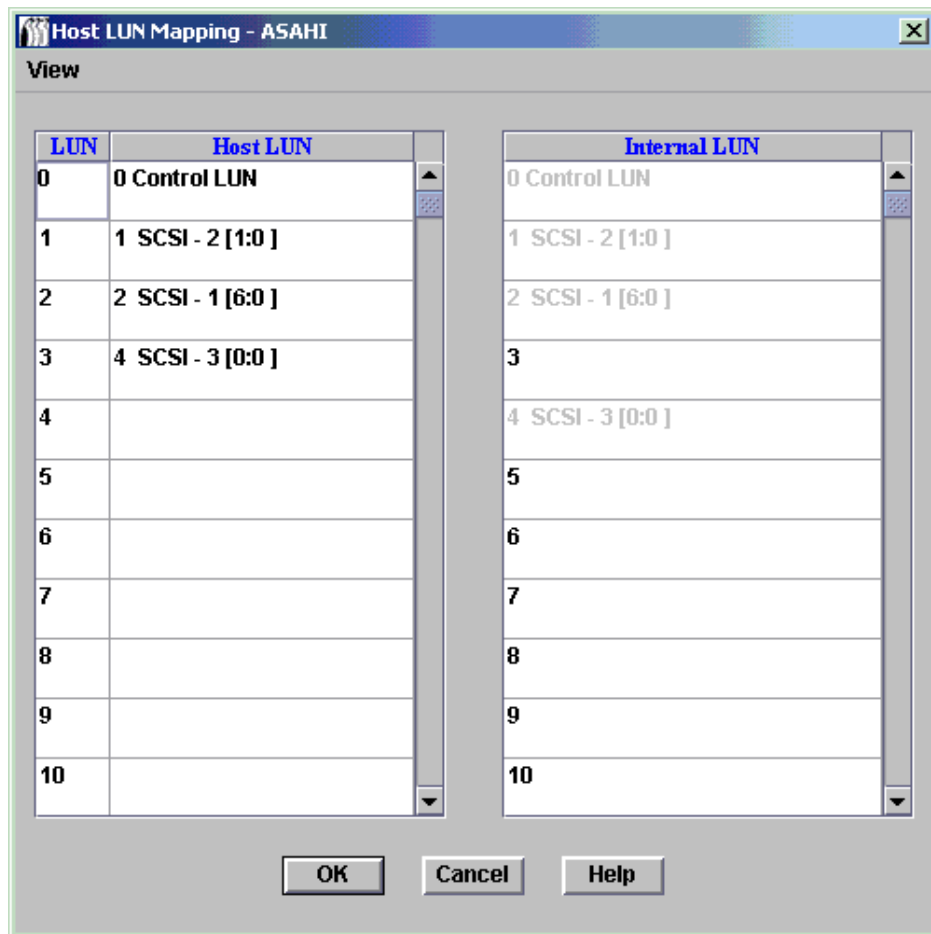
- 6 Guarde la configuración. Consulte [Guardar la configuración](#) en la página 76.

Para asignar LUNs a hosts desde el punto de vista del host

- 1 Seleccione el comando **Host LUN Mapping** en el menú **Host** del cuadro de diálogo **eVPS Access Summary**.

Se mostrará el cuadro de diálogo **Host LUN Mapping**.

Figura 26 Cuadro de diálogo Host LUN mapping



Los LUNs de la [figura 26](#) se asignan a un host llamado “Asahi”. Compare las asignaciones mostradas en la [figura 24](#) en la página 103 con las asignaciones de los LUNs del host de la [figura 26](#) . Los LUNs 0-3 asignados al host de la [figura 26](#) en la página 105 se corresponden a los LUNs internos 0, 1, 2 y 4.

- 2 Realice los cambios necesarios.
- 3 Seleccione **OK**.

El comando **View** del cuadro de diálogo **Host LUN Mapping** funciona a modo de alternador del mismo modo que el menú **View** funciona en el cuadro de diálogo **eVPS Access Summary**.

Consulte también [Utilización del menú View de eVPS](#) en la página 106.

Agregar o modificar hosts eVPS

Los hosts se pueden agregar a la red SAN tras la configuración inicial de eVPS.

Para agregar un host o modificar uno existente en una configuración eVPS

- 1 En el cuadro de diálogo **eVPS Access Summary**, seleccione **Add Host** o **Modify Host** del menú **Host**.
- 2 Complete los campos **Host Name**, **Host Type**, **Host Connection** y **Host WWN**.

Consulte [Agregar hosts SFM](#) en la página 100 para obtener información sobre cómo completar estos campos. El cuadro de diálogo **eVPS Host Configuration** sirve para que AMC conozca qué hosts está utilizando SFM.

- Haga clic en el botón **OK** para aplicar los cambios realizados en los campos de datos del host y en las asignaciones de LUNs.
- Guarde la configuración. Consulte [Guardar la configuración](#) en la página 76.

Eliminación de hosts eVPS

Los hosts se pueden eliminar de la red SAN tras la configuración inicial de SFM.



ATENCIÓN

Compruebe que el host que desee eliminar está offline. Los hosts offline se muestran en color azul.

Para eliminar un host

- Si el host no se encuentra offline, seleccione **Take Host Offline** del menú **Host** del cuadro de diálogo **eVPS Access Summary**.
- Seleccione **Delete a Host** del menú **Host** del cuadro de diálogo **eVPS Access Summary**.
- Seleccione **OK** para continuar con el proceso de eliminación de hosts.
- Guarde la configuración. Consulte [Guardar la configuración](#) en la página 76.

Utilización del menú View de eVPS

Los comandos **Show Details** y **Show All LUNs** se utilizan para obtener información rápida en el mapa de dispositivos de eVPS.

Para obtener información resumida de los LUNs asignados

Active y anule la activación de las casillas situadas junto a las selecciones cambiadas **Show Details** y **Show All LUNs** del comando **View** en el cuadro de diálogo **eVPS Access Summary**.

La [figura 27](#) y la [figura 28](#) en la página 107 muestran una vista de todos los espacios de LUNs disponibles en eVPS y una vista de sólo los LUNs que controla eVPS, respectivamente.

Figura 27 Comando **Show all LUNs** de eVPS

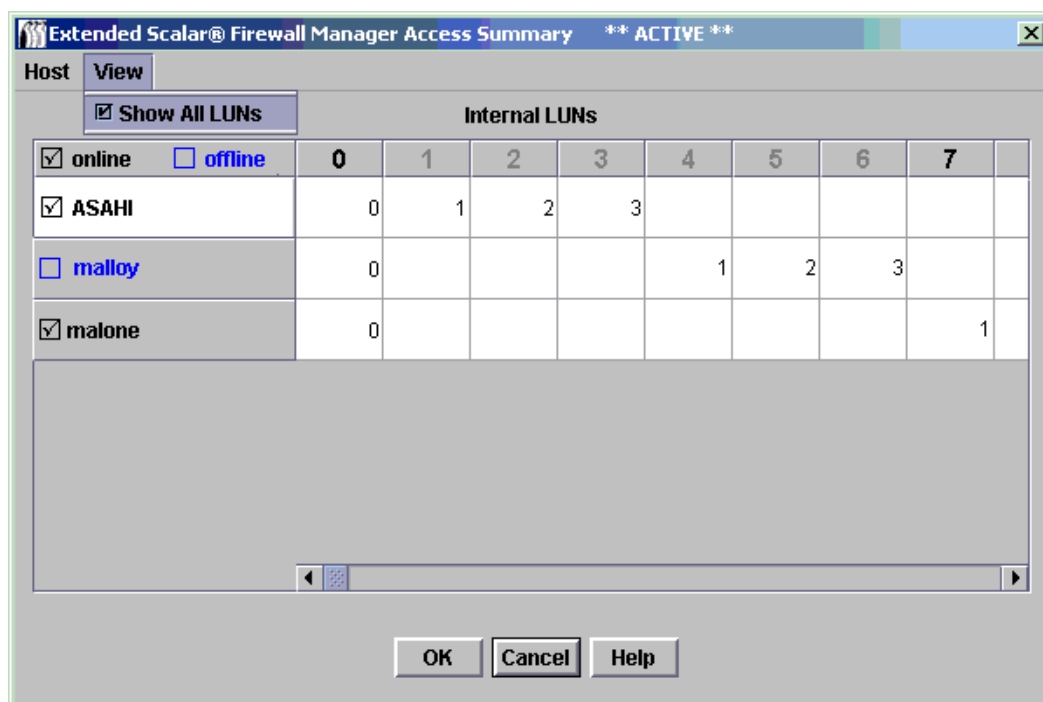
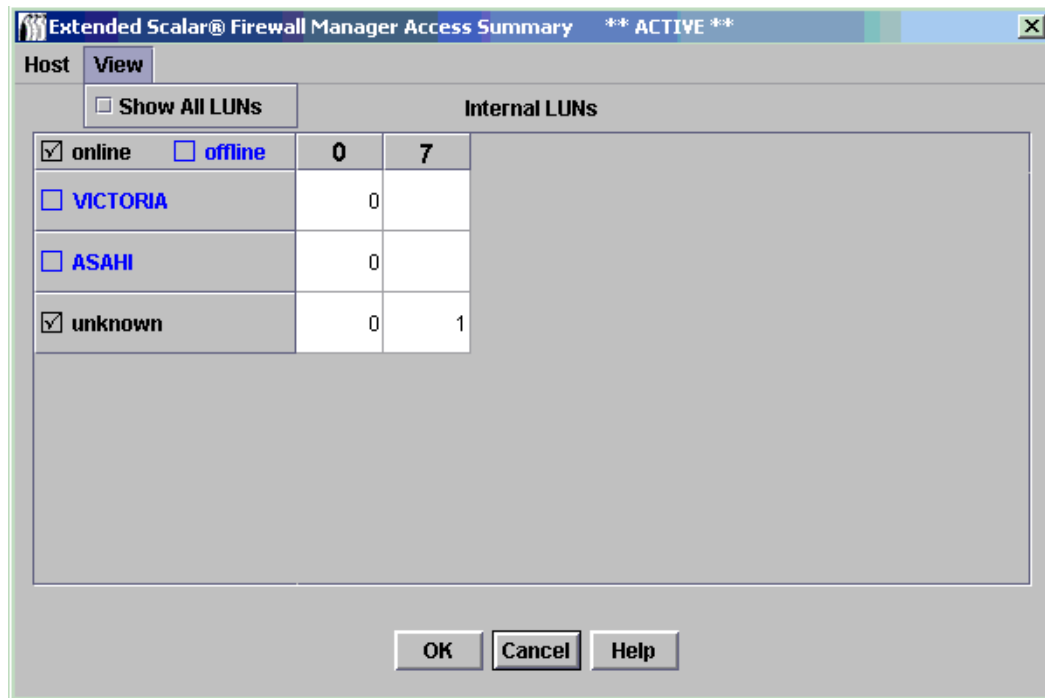


Figura 28 Comando Do Not Show All LUNs de eVPS



Utilización de VPM

La tecnología VPM (Virtual Private Map, asignación privada virtual) permite a los hosts conectados SCSI asignar LUNs Fibre Channel a dispositivos Fibre Channel.

Si ha realizado asignaciones de zonificación por canales, revíselas para asegurarse de que no provocan problemas al coexistir con las asignaciones de VPS. No se recomienda realizar la zonificación por canales a la vez que con VPM.

Para instalar VPM

- 1 Inicie una sesión como administrador de SAN o administrador de portal.



Nota

Los usuarios básicos y los avanzados no están autorizados para configurar VPM.

- 2 Si desea instalar el servicio de registro de host (HRS) en los hosts correspondientes, consulte al representante del servicio técnico.
- 3 Haga clic con el botón derecho del ratón en el canal SCSI al que se vaya a conectar el host.
- 4 Cambie el modo del puerto del canal SCSI a **Target**. Consulte [Configuración del canal SCSI](#) en la página 82.



ATENCIÓN

No olvide de restablecer el canal, que es el último paso del procedimiento de configuración del canal SCSI.

- 5 Reinicie el host.
- 6 Active VPM. Consulte [Habilitación de funciones sujetas a licencia](#) en la página 91.

Realización de asignaciones de VPM

- 1 Haga clic con el botón derecho del ratón en el canal SCSI al que se ha cambiado el modo a **Target**.
- 2 Seleccione **Virtual Private Map**.



Nota

Si hace clic con el botón derecho del ratón en un canal SCSI que no tiene el modo **Target** o si no se ha activado VPM, el comando VPN del canal SCSI seleccionado no estará activo.

Se abrirá el cuadro de diálogo **VPM**.

La columna **ID/LUN/Device** de la pantalla de VPM muestra el espacio de asignación de los IDs 0-15 asignados al canal SCSI seleccionado, los LUNs 0-7 asociados con cada ID y un cuadro que se completará arrastrando y soltando los dispositivos de la columna **Device**. De esta manera, los dispositivos tendrán un ID y un LUN concretos en el canal del host SCSI. Para obtener más información sobre la numeración de dispositivos, consulte [Numeración de los dispositivos](#) en la página 32.

Arrastre y suelte los dispositivos de la columna **Device** al LUN apropiado en la columna **ID/LUN/Device**.

Cuando se haya asignado un dispositivo objetivo, se mostrará sombreado en la columna **Device**.

Para visualizar las imágenes sombreadas de los canales Fibre Channel, desplácese por la columna **Device** hasta el rango de LUNs superior al cual se asignaron estos dispositivos durante la detección.

- 3 Seleccione **OK** para guardar la asignación.

La asignación VPM se guarda automáticamente como parte de la configuración.

En el **Status/Message Area** aparecerá el mensaje *Made Virtual Private Mapping changes*.

12

Solución de problemas de la red SAN

En esta sección se describen los códigos de eventos y los mensajes de error que pueden aparecer en la ventana de captura de eventos o en el registro de eventos conservado por el servidor AMC. Para obtener información detallada sobre el mantenimiento, la reparación y la solución de problemas, consulte el manual de mantenimiento de la biblioteca o el manual de hardware del SNC.

Comprobación del registro de eventos

Para determinar qué eventos se han incluido en el registro de eventos

- 1 Desde el panel de árbol o el panel gráfico, haga clic con el botón derecho del ratón en el equipo cuyo registro de eventos desee consultar.



Nota

Los registros de eventos Scalar i2000 y Pathlight VX no están disponibles para un acceso directo. Para guardar una copia de todos los registros de bibliotecas en un Scalar i2000, seleccione **Tools > Capture Snapshot**. Para guardar una copia de los registros de eventos en un Pathlight VX, seleccione **Tools > Capture State**.

- 2 Vaya a **Events > View Event Log**. El nivel de informes de eventos.
- 3 Seleccione **Warning** para visualizar los eventos del tipo **Warning** y **Notice**.
- 4 Seleccione **Information** para visualizar los eventos del tipo **Information**, **Warning** y **Notice**.
Si selecciona **All Events**, obtendrá el mismo resultado que si selecciona **Information**.
- 5 Seleccione **OK** para continuar.
- 6 Seleccione **Cancel** para anular todos los cambios realizados en el nivel de informe de eventos.
- 7 Seleccione **OK**.
- 8 Aparecerá el registro de eventos. Para navegar por él, utilice las barras de desplazamiento.
- 9 Utilice la [tabla 4](#) en la página 110 para interpretar los eventos enumerados. Tome nota de los códigos de eventos relevantes y consulte el *Manual de referencia de SNC Firmware 4* para averiguar las medidas necesarias para la solución del problema.

Si no hay ningún evento anormal, pero el comportamiento sigue siendo inaceptable, consulte [Realización de la comprobación de estado](#) en la página 66.

Tabla 4 Códigos de eventos y acciones

Código de eventos	Descripción
8	Datos de orientación registrados a continuación de una condición de comprobación. Nota: Normalmente, el sistema host solicita y procesa los datos de orientación y efectúa a continuación la recuperación de errores.
9	LUN notifica una condición de “atención a la unidad” en un dispositivo de medios no extraíble.
11	El controlador SNC notifica un cambio de temperatura (el mensaje del evento indica el cambio a alto, muy alto, reducido a alto o aceptable).
13	El equipo se cierra a petición de AMC (se solicitó un reinicio).
14	Información de estado adicional utilizada para el diagnóstico.
16	Un bus SCSI notifica una interrupción inesperada.
17	La interfaz Fibre Channel indica una acción de restablecimiento de LIP recibida desde un host.
18	La interfaz Fibre Channel indica un error del sistema.
19	La interfaz Fibre Channel indica un error al procesar una solicitud.
20	La interfaz Fibre Channel indica un error al procesar una respuesta.
21	Se ha detectado un fallo en la memoria del procesador del equipo.
22	La interfaz Fibre Channel ha detectado un LIP.
23	La interfaz Fibre Channel indica un bucle ascendente.
24	La interfaz Fibre Channel indica un bucle descendente.
25	Se ha detectado un error de paridad en el bus PCI del equipo de red.
26	Se ha detectado un error de interfaz PCI del equipo de red.
27	Se ha agregado un dispositivo al bus SCSI.
28	Un bus SCSI notifica que se ha detectado una acción de restablecimiento.
29	El equipo de red ha agregado un dispositivo a su tabla de configuración. Nota: La captura no se realizará hasta que el equipo lleve 60 segundos conectado.
30	El equipo en red ha eliminado un dispositivo de su configuración.
31	Se ha iniciado el servicio de registro del equipo.
33	Una interfaz ha detectado un fallo en un bus (el mensaje del evento indica la interfaz específica).
34	Una interfaz ha detectado un fallo en un dispositivo (el mensaje del evento indica la interfaz específica).
35	Una interfaz SCSI ha indicado la desconexión inesperada de un dispositivo.

Tabla 4 Códigos de eventos y acciones

Código de eventos	Descripción
36	Se ha detectado un error de paridad en un bus SCSI.
37	Cambio en la base de datos de puertos Fibre Channel.
39	Ha cambiado el servidor de directorios en Fabric.
40	Se ha superado el límite máximo de LUN.
41	Fallo de transferencia en Fibre Channel. Nota: Es posible que la recuperación de errores se haya completado.
42	Se ha superado el límite máximo de dispositivos (la base de datos del mapa de direcciones persistente está completa).
43	El controlador de la interfaz Fibre Channel ha indicado un volcado de archivos de depuración (el registro de eventos contiene información adicional).
58	El suministro eléctrico ha vuelto al estado nominal desde un nivel de advertencia o alarma.
59	El suministro eléctrico ha alcanzado el intervalo de advertencia desde el intervalo nominal (fallo en el suministro) o el intervalo de alarma (mejora en el suministro).
60	El suministro eléctrico ha alcanzado el intervalo de alarma.
61	Las temperaturas del aire de entrada, del aire de salida y del procesador de E/S han alcanzado el intervalo nominal desde un intervalo de advertencia o alarma.
62	La temperatura del aire de entrada ha alcanzado el intervalo de advertencia desde el intervalo nominal (caliente) o de alarma (frío).
63	La temperatura del aire de entrada ha alcanzado el intervalo de alarma.
64	La temperatura del aire de salida o del procesador de E/S ha alcanzado el intervalo de advertencia desde el intervalo nominal o de alarma.
65	La temperatura del aire de salida o la temperatura del procesador de E/S ha alcanzado el intervalo de alarma.
66	El ventilador está funcionando en el intervalo nominal después de funcionar en un estado de fallo.
67	La velocidad del ventilador ha alcanzado el intervalo de advertencia (sólo ventiladores de tacómetro).
68	La velocidad del ventilador ha alcanzado el intervalo de alarma (ventiladores de tacómetro) o se ha detenido (el rotor detiene los ventiladores).
70	Se ha completado el reinicio del equipo.
71	Se ha completado la carga del firmware.
72	Más de 64 iniciadores por canal FC
73	Se ha producido una conmutación por error de la ruta de datos en FCn WWPN=nnnnnnnn:nnnnnnnn lun=nxn loopId=nxn.
150	El registro de eventos sobrescribirá los eventos más antiguos.

Tabla 4 Códigos de eventos y acciones

Código de eventos	Descripción
	Descripciones de los eventos de la comprobación de estado
100	La fuente de alimentación no cumple las especificaciones.
102	Se ha detectado un cambio de temperatura desde la última notificación (el mensaje del evento indica el cambio a alto, muy alto, reducido a alto o aceptable).
106	La interfaz Fibre Channel no ha superado la comprobación de estado.
107	La interfaz SCSI no ha superado la comprobación de estado.
109	El dispositivo objetivo no ha superado la comprobación de estado.
110	Se ha modificado el estado de conexión de Fibre Channel.
111	Se han detectado errores de transferencia de Fibre Channel desde el último informe. Nota: Es posible que la recuperación de errores se haya completado.
112	El soplador/ventilador está funcionando en el intervalo de advertencia o alarma.
113	El suministro eléctrico se encuentra en el intervalo de advertencia o alarma.
114	La temperatura se encuentra en el intervalo de advertencia o alarma.
115	La red funciona a 10 Mbps.
	Descripciones de eventos de transacciones de control Nota: Estos códigos de evento no se incluyen en el registro de eventos. La notificación de estos eventos se produce desde AMC.
200	El servidor no pudo verificar la conexión al equipo.
201	El cliente no pudo establecer la comunicación con el servidor.
202	El servidor no pudo establecer la comunicación con el cliente.
203	Se ha restaurado la comunicación de la transacción de control.



Glosario

Este glosario contiene términos que se utilizan con los componentes de la red SAN.

Agregación

Representación del panel de árbol de un controlador SNC, de manera que está subordinado a la biblioteca Scalar en la que se encuentra.

AMC (ADIC Management Console)

Software cliente-servidor. El servidor AMC se utiliza para gestionar la red SAN y la biblioteca. La versión de AMC proporcionará acceso a dos clientes: el cliente AMC (que gestiona la red SAN) y el cliente LMC (que gestiona la biblioteca Scalar i2000).

ATAC

Centro de asistencia técnica de ADIC (ADIC Technical Assistance Center). Se trata del servicio de atención al cliente de ADIC.

Biblioteca

Biblioteca de cintas ADIC. Las bibliotecas son la Scalar 24, Scalar 100, Scalar 1000, Scalar 10K y Scalar i2000.

Biblioteca virtual

Para Pathlight VX, almacenamiento en disco que aparece como si fuera una unidad o biblioteca de cintas.

Cadenas de comunidad

Sentencias que describen las relaciones administrativas entre los agentes SNMP y los miembros de la comunidad.

Captura

Se envía una alerta SNMP al cliente AMC cuando se cumplen las condiciones predefinidas.

Categoría

Agrupación lógica de componentes de la red SAN que pertenecen a una vista específica. Por ejemplo, subred, departamento, ubicación, etc.

CE (técnico del servicio al cliente)

Miembro del equipo de ADIC que ofrece servicios de instalación, configuración, mantenimiento preventivo y reparaciones de una solución ADIC en el lugar de trabajo.

Comprobación de estado

Función de AMC que muestra alertas sobre posibles situaciones, advertencias de pérdida de conectividad o fallos en dispositivos mediante alertas locales o remotas. La comprobación de estado permite a los administradores corregir fallos antes de que estos afecten a operaciones de copia de seguridad o a otras operaciones de transferencia de datos.

Dispositivo virtual

Para Pathlight VX, se trata de un dispositivo presentado a un entorno de funcionamiento por un software de control o un gestor de volúmenes. Desde el punto de vista de las aplicaciones, un dispositivo virtual equivale a uno físico.

DNS (servicio de nombres de dominio)

Servicio que traduce los nombres de dominio en direcciones IP.

Equipo de red

Controlador SNC integrado o independiente. La Scalar i2000 no lo es y no contiene ningún equipo de red. La Scalar 100 contiene un equipo de red integrado. El Pathlight 5000 es un equipo de red independiente.

Evento

Condición que cumplen un conjunto predefinido y determinado de circunstancias. Se puede configurar el cliente AMC para que se muestren eventos de niveles específicos de gravedad y para que se generen capturas (también denominadas “capturas de eventos”) en casos específicos.

eVPS (extended Virtual Private SAN)

Esquema de asignación virtual de LUN de los hosts Fibre Channel que funcionan en el controlador SNC. Permite que todos los hosts consideren la asignación de LUN como si empezara en “1”, sujeto a un número total de dispositivos de 2.048 en todo el sistema y a un número total de dispositivos de 256 por cada host.

FC (Fibre Channel)

Arquitectura de transferencia de datos a gran velocidad. Mediante el uso de fibra óptica para conectar los dispositivos, las comunicaciones Fibre Channel son comunicaciones en serie que se producen a full duplex y logran velocidades de transferencia de datos de 200 Mbps.

HRS (servicio de registro de host)

Presenta información sobre el host que el servidor AMC utiliza para gestionar el acceso al host y la recuperación de datos. Esta información incluye el nombre, el tipo y la conexión de host, así como el estado online u offline.

ID objetivo

Dirección del bus SCSI. Véase también LUN.

Iniciador host

Adaptador de bus de host que proporciona al host un puerto Fibre Channel capaz de iniciar comandos SCSI a petición del host.

IP (protocolo de Internet)

Protocolo que especifica los formatos de los paquetes y las direcciones. Las direcciones se formulan en un formato de cuatro grupos separados por puntos, por ejemplo 123.456.789.123.

LMC (Library Management Console)

LMC es el software de gestión de la biblioteca Scalar i2000 que se ejecuta en la pantalla táctil de esa biblioteca. También se puede ejecutar de forma remota si hay una biblioteca Scalar i2000 en la red SAN. Es el software cliente que se comunica con el servidor AMC.

LUN (número de unidad lógica)

Identificador único que se utiliza en un bus SCSI para distinguir los dispositivos que comparten el mismo bus. SCSI es una interfaz paralela que admite hasta ocho dispositivos (IDs objetivo) conectados a un único cable. Cada uno de estos ocho dispositivos tiene acceso a 16 espacios de dirección única (LUN). El LUN asignado puede considerarse una intersección especificada de ID y LUN objetivo.

LVD (diferencial de bajo voltaje)

Tipo de unidad.

MAP (plan de acción de mantenimiento)

Rutina CLI que muestra a los usuarios los pasos que hay que realizar para solucionar los problemas del sistema o los errores de los componentes.

Menú Device

Menú de AMC que aparece cuando se hace clic con el botón derecho del ratón en un dispositivo de un disco o cinta en el panel de árbol o en el panel gráfico.

Menú Library

Menú de AMC que aparece cuando se hace clic con el botón derecho del ratón en una biblioteca en el panel de árbol o en el panel gráfico.

Menú SCSI Channel

Menú AMC que permite al usuario configurar los parámetros del canal SCSI de un controlador SNC. Aparecerá cuando se hace clic con el botón derecho del ratón en un canal SCSI en el panel de árbol o del panel gráfico.

Menú SNC

Menú AMC que permite al usuario configurar los parámetros del equipo de red de un controlador SNC. Aparecerá cuando se hace clic con el botón derecho del ratón en un controlador SNC en el panel de árbol o del panel gráfico.

MIB (base de datos de información de gestión)

Base de datos de los objetos que se pueden controlar por SNMP u otro sistema de gestión de bases de datos.

NDMP

Network Data Management Protocol

Panel de árbol

Parte izquierda de la ventana de AMC en la que se muestran los componentes en un formato visual/textual muy convencional.

Panel de datos

Cuadro situado en la parte inferior derecha de la ventana de la interfaz de AMC en el que se muestra información en formato de tablas.

Panel de LEDs

Representación de AMC de la superficie de LEDs del controlador SNC. Por ejemplo, en Pathlight 5000, se encuentra en el mismo lado que los conectores. En ADIC 3000, se encuentra en el lado contrario a los conectores.

Panel gráfico

Cuadro situado en la parte superior derecha de la ventana de la interfaz de AMC en el que se muestra información sobre la configuración en formato de gráficos.

Partición

Para la Scalar i2000, una partición es una abstracción de una biblioteca física subyacente que un host puede considerar como que tiene una personalidad diferente, una capacidad diferente o ambas características diferentes. Se trata de una representación de elementos físicos reales combinados para crear un grupo distinto de la biblioteca física.

Política

Norma del sistema de notificación experto AMC que permite que AMC alerte a ciertas personas especificadas por el administrador de que se han cumplido condiciones de error de la red SAN.

Portal

Conjunto de dispositivos de red de área de almacenamiento que representan el universo particular de un usuario determinado. El portal predeterminado del administrador de una red SAN es el conjunto completo de dispositivos y su almacenamiento asociado en la subred a la que accede AMC. Este portal se conoce como portal principal. El administrador de SAN puede otorgar a otros usuarios privilegios sobre subconjuntos del portal principal.

POST (autocomprobación de encendido)

Secuencia de comprobación de diagnóstico realizada por la BIOS MCB o SNC (sistema básico de entrada/salida) cuando se conecta el equipo por primera vez.

Punto a punto

Topología de Fibre Channel.

RAS (fiabilidad, disponibilidad y servicio)

Tres atributos clave del diseño del sistema de computación.

RCU (unidad de control de robótica)

PCB que forma parte del LMM y controla las funciones del accesor, selector y dispositivo de sujeción.

Realización

Para Pathlight VX, escritura de información de un disco a un medio de cinta físico

Recepción de capturas de eventos

Ventana así denominada que siempre se abre cuando funciona el cliente AMC. En él se mostrarán los eventos configurados para provocar capturas. Estos eventos se deben haber configurado antes para producir capturas y así poder verlas en esta ventana.

Registro de eventos

Lista de todos los eventos predefinidos registrados por el servidor AMC, aun habiendo configurado el cliente AMC para que el usuario visualice tales eventos.

RMU (unidad de gestión remota)

Función de la biblioteca que permite a los usuarios controlar las operaciones de la biblioteca de forma remota. Scalar i2000 y Pathlight VX no disponen de RMU. LMC se utiliza para manejar la Scalar i2000 tanto de forma local como remota. El VLI se utiliza para manejar el Pathlight VX de forma remota.

Ruta de datos

Una de las múltiples rutas posibles por la que se pueden trasladar datos en el entorno de la red SAN, que incluye potencialmente a muchos componentes o conexiones entre iniciadores y objetivos que se han utilizado desde que se realizó la primera configuración.

SAN (red de área de almacenamiento)

Una SAN es una red dedicada de gran rendimiento cuyo principal objetivo es transferir datos mediante conexiones de FC o de Ethernet a gran velocidad entre servidores, dispositivos interconectados y periféricos de almacenamiento.

SCSI (interfaz estándar de equipos pequeños)

Estándar de interfaces paralelas.

SE (técnico de sistemas)

Miembro del equipo de ADIC que ofrece servicios y mantenimiento continuo de una solución ADIC.

Servidor remoto

Instancia del servidor AMC distinta del servidor incluido en el MCB o en Pathlight VX.

SFM (Scalar Firewall Manager)

Esquema de asignación virtual de LUN para los hosts Fibre Channel que permiten reasignar virtualmente un número total de LUN de 2.048 en toda la red SAN.

SNC (controlador de almacenamiento en red)

Término de ADIC para los equipos de almacenamiento en red. El controlador SNC permite establecer comunicaciones en red de gran rendimiento que admiten funciones inteligentes en los sistemas de almacenamiento Scalar. En la biblioteca Scalar i2000, las funciones del controlador SNC las realiza la MCB.

SNMP (Simple Network Management Protocol)

SNMP es el protocolo que realiza la gestión de la red y el control de los dispositivos de red y sus funciones.

Status/Message Area (Área de estado/mensajes)

Parte inferior de la ventana de la interfaz de AMC en donde se muestran las capturas de eventos y otros mensajes.

Virtualización

Para Pathlight VX, escritura de datos de medios de cintas en discos.

Vista

En AMC, una vista es una representación gráfica con nombre de un portal, generalmente guardada para conservar una categorización particular.

VLI (Virtual Library Interface)

Interfaz de gestión de Pathlight VX.

VPM (Virtual Private MAP)

Esquema de asignación virtual de LUN para los hosts conectados por SCSI. Permite que todos los hosts consideren la asignación de LUN como si empezara en "1", sujeto a un número total de dispositivos de 2.048 en todo el sistema y a un número total de dispositivos de 256 por cada host.

VPS (Virtual Private SAN)

Esquema de asignación virtual de LUN en toda la red SAN para los hosts conectados mediante FC. Permite disponer de un número total de LUN de 2.048 dispositivos en toda la red.

WWN

World Wide Name, número único asignado por una entidad normalizadora de nombres reconocida. El WWN se incluye en todas las operaciones con Fibre Channel.

Zonificación por canales

Método que se utiliza para subdividir una red SAN en zonas separadas por canales para mejorar la seguridad y el acceso de personal cualificado.

Índice

- A -

Actualizar datos	76
Área de estado/mensajes	36
Asignación privada virtual. Véase VPM	
ATAC	2
Ayuda	2
en pantalla	2, 25

- B -

Bibliotecas	
datos de RMU. Véase también Cliente de gestión de bibliotecas.	66
Buscar	39, 59
Búsquedas	59

- C -

Canal SCSI	
configurar	82
restablecer	82
Categorías	
cambiar nombre	52
categorización automática	39, 51
crear	39, 52
eliminar	53
mover	53
mover elementos de componentes	39, 54
Cerrar sesión	19
Cliente	
barra de herramientas	25
cerrar sesión	19
gestión de bibliotecas	4
gestión de SAN	4
iniciar	
plataformas UNIX	17
Windows	17
iniciar sesión	18
instalación	
plataformas UNIX	15
Windows	15
leer la interfaz	26
menús	25

paneles	26, 33
requisitos del sistema	
plataformas UNIX	11
Windows	10
salir	20
ventana de captura de eventos.	
Véase también Eventos.	26
Comprobación de estado	
configurar	67
realizar	66
Configuración del sistema	76
Contraseña	
administrador	41
valor predeterminado	18
Correo electrónico	
configurar	61
Cuentas de usuario	
crear	43
eliminar	44
modificar	44

- D -

Datos de entorno	79
Datos de RMU	66
Datos, actualizar	76
Dispositivos	
editar mapas de dispositivos	87
gestión	87
numeración	32

- E -

Eventos	
configurar capturas	69
recibir capturas	70
registrar	5
registros	68, 109
eVPS	101
configurar	102
hosts	105
instalación	101
extended Virtual Private SAN. Véase eVPS	

- F -	
<hr/>	
FAQ. Véase Preguntas frecuentes	
Fibre Channel	
configurar	84
restablecer	84
volver a escanear	83
Firmware	
actualizar	76, 77, 87
- H -	
<hr/>	
HRS	93
- I -	
<hr/>	
ID de bucle	86
ID de host	83
ID de iniciador alternativo	83
Identificar	73
Informes	5, 59
Iniciar sesión	18
- L -	
<hr/>	
Latido	5
Localizar	39
- M -	
<hr/>	
MAP	109
Modo de canal. Véase también modos de puerto.	83
Modos de puerto	85
- N -	
<hr/>	
Niveles de privilegio	41
- O -	
<hr/>	
Organizador de datos	92
- P -	
<hr/>	
Panel de árbol. Véase también Cliente paneles.	26
Panel de datos. Véase también Cliente paneles	33
Panel de LEDs	71
Panel gráfico. Véase también Cliente paneles	33
Planes de acciones de mantenimiento. Véase MAP	
Políticas	
configurar	62
Portal	
eliminar	49

Portales	
crear	47
modificar	48
permisos	49
Preguntas frecuentes	21

- R -

<hr/>	
Requisitos de instalación	9
Restablecer bus al encendido	83
Restart	78
RMU	6

- S -

<hr/>	
Scalar Firewall Manager. Véase SFM	
Servicio de registro de host. Véase HRS	
Servidor	
conectar	18
iniciar	
plataformas UNIX	14
Windows	14
instalar	
plataformas UNIX	12
Windows	11
requisitos del sistema	
AIX	10
HP-UX	10
Solaris	10
Windows	9
salir	20
SMTP	62
configurar	65
SFM	96
configurar	98
hosts	100
instalación	97
Sistema, configuración	76
canal SCSI	82
cargar archivos	77
Fibre Channel	84
modo de canal	83
modo de puerto. Véase también Modo de canal	85
Solución de problemas	109

- T -

<hr/>	
Tamaño de trama	86
Terminación	83
Tipo de host	86

- V -

<hr/>	
Vistas	
abrir	56
buscar componentes específicos	39, 59

crear	56
crear informes	59
eliminar	58
guardar	58
VPM	107
configuración	108
instalación	107

- Z -

Zonificación por canales	92
--------------------------------	----

