(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 359 558**

(51) Int. Cl.:
H04L 12/24 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03796056 .4**
(96) Fecha de presentación : **25.11.2003**
(97) Número de publicación de la solicitud: **1573962**
(97) Fecha de publicación de la solicitud: **14.09.2005**

(54) Título: **Sistema y método seguros para gestión de SAN en un entorno de servidor no seguro.**

(30) Prioridad: **20.12.2002 EP 02102852**

(45) Fecha de publicación de la mención BOPI:
24.05.2011

(45) Fecha de la publicación del folleto de la patente:
24.05.2011

(73) Titular/es: **INTERNATIONAL BUSINESS MACHINES CORPORATION**
New Orchard Road
Armonk, New York 10504, US

(72) Inventor/es: **Raisch, Christoph**

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Antecedentes del Invento

1. Campo del Invento

El presente invento se refiere en general a redes de área de almacenamiento. Particularmente, el presente invento se refiere a un método y un sistema para hacer funcionar una red de área de almacenamiento en un entorno de servidor en el que múltiples servidores comparten un adaptador de Canal de Fibra.

2. Descripción de la Técnica Relacionada

El canal de fibra es una tecnología de comunicaciones en serie, dúplex-completa, de alta velocidad usada para interconectar dispositivos (I/O) de entrada/salida y sistemas anfitriones que pueden estar separados por decenas de kilómetros. Incorpora las mejores características de interfaces I/O tradicionales, como el rendimiento y la fiabilidad encontrados en SCSI y PCI, con las mejores características de interfaces de red, como conectividad y escalabilidad encontradas en Ethernet y Token Ring. Proporciona un mecanismo de transporte para la entrega de órdenes o comandos existentes, y proporciona una arquitectura que consigue un alto rendimiento permitiendo que una cantidad significativa de tratamiento sea realizada en hardware. Puede funcionar con protocolos antiguos y controladores como SCSI e IP, permitiéndole ser introducido fácilmente en infraestructuras existentes.

El canal de fibra transfiere información entre las fuentes y los usuarios de la información. Esta información puede incluir órdenes, controles, archivos, gráficos, video y sonido. Las conexiones del canal de fibra están establecidas entre los puertos de canal de Fibra que residen en los dispositivos I/O, sistemas anfitriones, y la red que los interconecta. La red se consiste de elementos como conmutadores, bobinas, puentes y repetidores que son usados para interconectar los puertos de Canal de Fibra.

Hay tres topologías de Canal de Fibra definidas en la arquitectura de Canal de Fibra. Estas son Punto a Punto, Tejido Conmutado y Bucle Arbitrado.

Los conmutadores de canal de Fibra (o tejidos conmutados) también incluyen funciones comúnmente denominadas Zonificación o Zonificación. Estas funciones permiten al usuario separar o dividir los puertos de conmutación en grupos de puertos. Los puertos dentro de un grupo de puertos, o zona, pueden sólo comunicar con otros puertos del mismo grupo de puertos (zona). Usando la zonificación, la I/O de un grupo de anfitriones y dispositivos puede estar completamente separada de aquel de cualquier otro grupo, impidiendo así la posibilidad de cualquier interferencia entre los grupos.

Esto es también denominado como “zonificación suave”. El modo en que esta zonificación suave trabaja es que el usuario asigna nodos a una zona de acuerdo con el Nombre de Ámbito Mundial del Nodo – o bien el Nombre de Puerto de Ámbito Mundial (WWPN) o bien el Nombre de Nodo de Ámbito Mundial (WWNN). El servidor de nombre captura esta información, que es una función embebida dentro del conmutador. A continuación, siempre que un puerto comunica con el servidor de nombre para encontrar a qué nodo le está permitido conectarse, el servidor de nombre responderá sólo con los nodos que están dentro de esa zona de puertos.

Como los controladores del dispositivo de Canal de Fibra estándar comunican con el servidor de nombre de esta manera, este tipo de zonificación es adecuado para la mayor parte de las situaciones. Sin embargo, es posible que un controlador de dispositivo pudiera estar diseñado de modo que intentara acceder a nodos que no están en su lista de conexiones permitidas. Si esto ocurriera, el conmutador ni impediría ni detectaría la violación.

Con el fin de impedir este caso, los conmutadores también emplean opcionalmente un mecanismo denominado “zonificación fuerte” además de zonificación suave, dónde la red de conmutación decide basándose solamente en la dirección de fuente y de destino de cada trama si esta trama se permite que sea transportada.

Las Redes de Área de Almacenamiento de Canal de Fibra (SAN) son redes que conectan dispositivos de almacenamiento a servidores anfitriones. Están construidas sobre la tecnología de Canal de Fibra como una infraestructura de red. Lo que diferencia las SAN de los esquemas de interconexión previos en el concepto básico de que todo (o casi todo) el almacenamiento pueden estar consolidados en un gran “área de almacenamiento” que permite la gestión (simplificada) centralizada además de la conectividad de cualquiera a cualquiera entre servidores anfitriones y el almacenamiento.

Las SAN de canal de Fibra tiene el potencial para permitir la interconexión de sistemas abiertos y almacenamiento (es decir, no Series z) en la misma red que sistemas de Series z y almacenamiento. Esto es posible porque los protocolos tanto para la unión abierta como para la unión de Series z están siendo hechos corresponder a la capa FC-4 de la arquitectura de Canal de Fibra.

En uniones de Canal de Fibra, las LUN tienen una afinidad al adaptador de Canal de Fibra de anfitrión (a través del Identificador Único de Ámbito Mundial del adaptador, a.k.a el Nombre del Puerto de Ámbito Mundial), independientemente de a qué puerto de canal de Fibra (Servidor de Almacenamiento de Empresa de IBM) ESS está unido el anfitrión. Por ello, en una configuración de tejido conmutado en la que un solo anfitrión de Canal de Fibra puede tener acceso a múltiples puertos

de Canal de Fibra en el ESS, los conjuntos de LUN, que pueden ser accedidos por el anfitrión de Canal de Fibra, son los mismos en cada uno de los puertos ESS.

Un resultado de esta puesta en práctica es que con el Canal de Fibra, a diferencia de en SCSI, los anfitriones que están unidos a ESS a través de un tejido al mismo puerto de Canal de Fibra no sean capaces de "ver" las mismas LUN, ya que el enmascaramiento de LUN puede ser diferente para cada anfitrión de Canal de Fibra. En otras palabras, cada ESS puede definir qué anfitrión tiene acceso a qué LUN.

Otro método es crear zonas en el conmutador de tal modo que cada puerto de Canal de Fibra desde cada anfitrión está restringido a unirse a un puerto de Canal de Fibra en el ESS, permitiendo por ello que el anfitrión vea las LUN a través de un solo trayecto.

Los detalles de la especificación de Canal de Fibra están mostrados en las normas siguientes: Interfaz Física y de Señalización de Canal de Fibra (FC-PH), AINSI X3.230-1994; Interfaz Física de Segunda Generación de Canal de Fibra (FC-PH-2), AINSI X3.297-1997; Interfaz Física de Tercera Generación de Canal de Fibra (FC-PH-3), AINSI X3.303-199X, Revisión 9.4 y Bucle Arbitrado de Canal de Fibra (FC-AL), AINSI X3.272-1996. Otras normas importantes son FC-FS, FC-GS-3.

Otra información que se refiere al Canal de Fibra está descrita en el Consultor de Canal de Fibra – Una Introducción Comprensiva (Robert W. Kembel, 1998) y El Consultor de Canal de Fibra – Bucle Arbitrado (Robert W. Kembel, 1996).

El documento EP-1.115.225 A2, de Barry Stanley Barnett y col., asignado a Internacional Business Machines Corporation, Armonk, NY, Estados Unidos de Norteamérica, presentado el 22 de Diciembre de 2000, publicado el 11 de Julio de 2001, "Método y sistema para determinación del problema de extremo a extremo y aislamiento de fallo para redes de área de almacenamiento" describe un método y sistema para la determinación del problema y el aislamiento del fallo en una red de área de almacenamiento (SAN). Una configuración compleja de sistemas anfitriones de múltiples vendedores, conmutadores de FC, y periféricos de almacenamiento están conectados en una SAN a través de una arquitectura de comunicaciones (CA). Un elemento de arquitectura de comunicaciones (CAE) es un dispositivo conectado a una red que ha sido registrado satisfactoriamente con un gestor de arquitectura de comunicaciones (CAM) en un ordenador anfitrión a través de un protocolo de servicio de red, y el CAM contiene la funcionalidad de determinación del problema (PD) para la SAN y mantiene una tabla de información de SAN PD (SPDIT). La CA comprende todos los elementos conectados a una red capaces de comunicar información almacenada en la SPDIT. El CAM usa una correspondencia de topología SAN y la SPDIT es usada para crear una tabla de diagnóstico SAN (SDT). Un componente que falla en un dispositivo particular puede generar errores que hacen que los dispositivos a lo largo del mismo trayecto de conexión de red generen errores. Cuando el CAM recibe paquetes de error o mensajes de error, los errores son almacenados en la SDT, y cada error es analizado temporal y espacialmente comprando el error con otros errores en la SDT. Si un CAE es determinado como un candidato para generar el error, entonces el CAE es informado para su reemplazamiento si es posible.

El documento US 2001/0054093 A1, de Sawao Iwatani, Kawasaki, Japón, presentado el 9 de Febrero de 2001, publicado el 20 de Diciembre de 2001, "Sistema de gestión de la red de área de almacenamiento, método, y medio legible por ordenador" describe un mecanismo de gestión integrado de una red de área de almacenamiento (SAN) que integra y gestiona un sistema de seguridad dispersado tradicionalmente desde una sola fuente y automatiza la gestión de seguridad en la SAN. El mecanismo de gestión integrado integra y gestiona la SAN, y está configurado de modo que las relaciones de acceso de los ordenadores anfitriones y los dispositivos de almacenamiento de la SAN son gestionados usando el mecanismo de gestión integrado. Un trayecto de acceso en el mecanismo de gestión integrado, que incluye una región de los dispositivos de almacenamiento a los que se ha intentado acceder desde el ordenador anfitrión, los adaptadores de canal de fibra usados cuando se accede a ese almacenamiento, y los adaptadores de bus o línea de transmisión de anfitrión (HBA) están configurados. Basándose en la información de trayecto de acceso configurada, el mecanismo de gestión integrado establece ajustes de almacenamiento respectivo, ajustes de almacenamiento respectivos, ajustes de zonificación, y permisos de región accesible para un mecanismo de gestión de SAN del ordenador anfitrión, un mecanismo de ajustes de zonificación del conmutador, y un mecanismo de gestión de almacenamiento del dispositivo de almacenamiento.

El documento US 2002/0174211A1 describe técnicas para gestionar dispositivos de almacenamiento basados en red. Los servidores de aplicación tienen capacidades de partición lógica en los que cada partición puede contener diferentes sistemas operativos. Varias particiones pueden compartir un único HBA para acceder a la SAN. La seguridad de acceso en la SAN es gestionada por un subsistema de gestión sobre la base de HBA.

Objeto del Invento

Empezando a partir de esto, el objeto del presente invento es proporcionar un método y un sistema para hacer funcionar una red de área de almacenamiento en un entorno de servidor, en el que un servidor múltiple comparte un adaptador de Canal de Fibra, que tiene un mecanismo de seguridad mejorado.

Breve Sumario del Invento

El objeto anterior es conseguido por un método y un sistema como se ha presentado en las reivindicaciones independientes. Se han descrito otras realizaciones ventajosas del presente invento en las sub-reivindicaciones y se han

relacionado en la descripción siguiente.

De acuerdo con el presente invento se han proporcionado un método y un sistema para hacer funcionar una red de área de almacenamiento (SAN) en un entorno de servidor en el que múltiples servidores comparten un adaptador de Canal de Fibra. Un Servidor de Gestión de SAN gestiona las regiones en sistemas de almacenamiento y errores de seguridad y/o de detección y configuración del SAN, una Red de Canal de Fibra proporciona una conexión a dispositivos de almacenamiento, y una pluralidad de Imágenes de Sistemas de Operativo se ejecutan en dicho entorno de servidor. Además, una Unidad de Cliente de Gestión de SAN segura está conectada a dicho Servidor de Gestión de SAN y un adaptador de Canal de Fibra, por lo que la Unidad de Cliente de Gestión de SAN segura está configurada para emitir órdenes en dicha Red de Canal de Fibra en lugar de cada una de dichas Imágenes de Sistema Operativo.

En una realización preferida del presente invento, el entorno de servidor incluye servidores virtuales y/o servidores divididos.

Preferiblemente, el Servidor de Gestión de SAN está configurado para distinguir un primer conjunto de órdenes y un segundo conjunto de órdenes, por lo que el primer conjunto de órdenes es procesado por el Cliente SM junto con dicho SAN, y por lo que dicho segundo conjunto de órdenes es procesado por dichas Imágenes OS sin acceso a dicho SAN. Favorablemente, el adaptador de Canal de Fibra (adaptador de FC) está configurado para autenticar dicha Unidad de Cliente de Gestión de SAN.

Ventajosamente, el adaptador FC y dicho SAN pueden ser adaptados para restringir el acceso de las Imágenes OS no seguras al conjunto mínimo necesario de órdenes. Alternativamente, el adaptador de FC y una capa de virtualización del servidor virtual pueden estar adaptados para restringir el acceso de las Imágenes OS no seguras al conjunto mínimo necesario de órdenes.

En otra realización del presente invento, sólo se ha previsto un Cliente de SM con el fin de mantener la pequeña carga del servidor. Opcionalmente, uno o más Clientes de SM reserva están previstos para proporcionar redundancia.

Ventajosamente, sólo se ha registrado el Cliente de SM para recibir mensajes desde el SAN y el Cliente de SM está configurado para enviar dichos mensajes sólo a dicho Servidor de SM. Opcionalmente, el adaptador de FC está configurado para enviar todos los mensajes para los que no es necesario un registro solamente al Cliente de SM y no a las Imágenes de OS no seguras.

En una realización diferente del presente invento el servidor está equipado con dos clases de agentes, en particular, el Cliente de SM y un Servidor de Acceso Remoto (Servidor de RA). Preferiblemente, el servidor está equipado con un repertorio para conservar los datos de autorización para acceder al Servidor de RA.

Preferiblemente, sólo el Cliente de SM y el adaptador de FC están configurados para reunir la información usada para facturar el uso de recursos por cada Imagen de OS no segura. Ventajosamente, el Marco de SM está adaptado para comunicar con una aplicación de control de Cortafuegos, con el fin de ajustar los derechos de acceso.

En otra realización del presente invento el Cliente de SM está adaptado para funcionar como un encaminador para las solicitudes procedentes del servidor de SM al servidor de RA. Preferiblemente, un servidor telnet/sshd existente forma el servidor de RA.

Además, el presente invento puede ser puesto en práctica como un método para hacer funcionar una red de área de almacenamiento (SA) en un entorno de servidor en el que múltiples imágenes de sistema operativo comparten un adaptador de Canal de Fibra, en el que la SAN es gestionada por un software de Gestión de SAN con al menos un servidor de Gestión de SAN y al menos un cliente de Gestión de SAN con un trayecto de comunicación a dicho Adaptador de Canal de Fibra. Las solicitudes emitidas por el servidor de Gestión de SAN están separadas en al menos dos grupos, en particular, un primer grupo es procesado por el adaptador de Canal de Fibra y la SAN en interés del cliente de SM en lugar de otros sistemas operativos que comparten el mismo adaptador, correspondiente a un trayecto seguro, y un segundo grupo es procesado por los otros sistemas operativos sin necesidad de enviar solicitudes al adaptador de FC y la SAN o recibirlas de los mismos.

En una realización preferida del método toda la información contenida en mensajes no solicitados generados en la SAN y el adaptador de FC son encaminados al Gestor de SAN por el cliente de gestión de SAN. Preferiblemente, las solicitudes de vinculación HBA_API son usadas para modificar el cortafuegos.

Opcionalmente, el trayecto de comunicación desde el cliente de Gestión de SAN al adaptador es operado de modo que no pueda ser modificado o escuchado secretamente por otra imagen de sistema operativo. En otra realización preferida toda la información relevante para facturar imágenes individuales del sistema operativo es generada en el adaptador y es encaminada a través del SAN al Gestor de SAN por el cliente de SAN en el trayecto seguro.

Ventajosamente, el servidor de SM proporciona datos de autorización al cliente de SM para ejecutar solicitudes desde dicho primer grupo. Opcionalmente, el servidor de SM y el cliente de SM proporcionan datos de autorización a las otras imágenes de OS para ejecutar solicitudes desde dicho segundo grupo. Preferiblemente, las imágenes de OS son operadas de

modo que sólo se les deja ejecutar un conjunto limitado de órdenes en el SAN.

Un gran número de sistemas operativos (>256, 4000 servidores virtuales son probablemente en 2004) tiene que participar en una SAN con adaptadores de FC compartidos. Los adaptadores son compartidos en este tipo de escenario debido a razones de coste y razones de capacidad de gestión. Un servidor con 256 adaptadores de FC necesita por ejemplo 256 cables desde los adaptadores al conmutador y 256 puertos en la red de conmutación.

En un entorno de anfitrión de servidor cada imagen de OS necesita datos privados, a los que no se puede acceder por otras imágenes de OS (por ejemplo la configuración del servidor) y datos de lectura-escritura compartidos, por ejemplo una base de datos compartida que sólo lee datos, por ejemplo, una imagen de sistema operativo preinstalada (/usr en un sistema unix) para LUN compartidas por imágenes de OS por el mismo adaptador no es posible garantizar un comportamiento compliant completamente scsi (por ejemplo (reserva/liberación, manejo de NACA, reglas de puesta en cola como se ha definido por SAM-2).

Cada “imagen de sistema operativo no segura” es propiedad de una entidad potencialmente peligrosa, por ejemplo dos compañías que compiten entre sí o un pirata informático (“hacker”). Propiedad significa la entidad que realmente tiene acceso a la raíz y puede alterar cada pieza de la imagen del sistema operativo incluyendo todos los clientes de SM u otro software. El propietario de la imagen de OS no tiene acceso y no puede modificar el hardware por su propio interés sino que necesita al propietario de la máquina para hacer esto. El propietario de la máquina (departamento de IT/ASP/ISP) tiene control total sobre todo el hardware, correspondencias y políticas en la SAN.El propietario de la máquina asigna recursos en la SAN (más probablemente LUN en un controlador de disco) a las imágenes del sistema operativo. El propietario de la máquina necesita una herramienta para realizar la Detección de Error y el Aislamiento de Fallo en la SAN para impedir el tiempo de inactividad de las imágenes del sistema operativo. El propietario de la máquina podría querer dividir su hardware en múltiples entidades y subredes, que pueden ser gestionadas independientemente desde otras subredes (servidores múltiples de grupo o LPAR). Un adaptador compartido no franquear subredes, pero puede franquear LPAR.

Cada imagen de OS es o bien ejecutada en un servidor individual (servidor de lámina) o bien como un servidor virtual. Pueden crearse entornos de Servidor Virtual por ejemplo mediante un soporte lógico inalterable LPAR-Serie z, el sistema operativo VM de Serie z o servidores basados en VMware o Intel).

La presentación de recursos de SAN en la interfaz de usuario de Gestor de SAN debería hacerse de tal modo que el propietario de la máquina pueda mover una imagen de OS desde un servidor virtual a un servidor físico sin tener un tipo de vista completamente diferente presentado por la interfaz de usuario de servidor de SM.

Puede restringirse el acceso de cada imagen de OS por un cortafuegos en el adaptador de FC u otra entidad, que no pertenece a la imagen de OS (de otra manera un usuario con derechos de acceso a la raíz que tiene el control total sobre la imagen de OS tiene la capacidad de sortearlo).

La correspondencia de FC a SCSI en cada imagen de OS no segura puede ser configurada por una interfaz MAP_IF de correspondencia y configuración del controlador del dispositivo de FC. Por ejemplo el MAP_IF en varias versiones de Canal de Fibra en Series z es puesto en práctica por un método de configuración específico Linux denominado sistema-archivo-proc para ajustar y preguntar dicha correspondencia. El servidor de SM no debería basarse en datos correctos informados por una MAP_IF (el cumplimiento de acceso es realizado por cortafuegos, de modo que cualquiera de los OS coopera o no quieren ver ningún dato en absoluto). Las mediciones para facturar no pueden ser hechas en las imágenes de OS no seguras (debido a que el usuario de raíz es libre de modificar los datos). Por ello el adaptador u otras entidades han de proporcionar los datos de medición requeridos.

Otras realizaciones pueden proporcionar múltiples WWPN aunque el número de WWPN podría ser inferior que el número de imágenes de OS soportado por el adaptador.

Breve Descripción de las Distintas Vistas de los Dibujos

Lo anterior, así como otros objetivos adicionales, características y ventajas del presente invento, resultarán evidentes en la siguiente descripción detallada.

Las nuevas características del invento están descritas en las reivindicaciones adjuntas. El invento en sí mismo, sin embargo, así como un modo preferido de uso, otros objetivos, y ventajas del mismo, serán mejor comprendidos con referencia a la descripción detallada siguiente de una realización ilustrativa cuando es leída junto con los dibujos adjuntos, en los que:

La fig. 1 muestra un diagrama de bloques que ilustra una primera realización de un sistema de acuerdo con el presente invento;

La fig. 2 muestra un diagrama de bloques que ilustra una segunda realización del sistema de acuerdo con el presente invento;

La fig. 3 muestra un diagrama de flujo que ilustra el método para hacer funcionar una red de área de almacenamiento

en un entorno de servidor en el que múltiples servidores comparten un adaptador de Canal de Fibra de acuerdo con el presente invento;

La fig. 4 muestra un diagrama de flujo que ilustra señales simplificadas y el flujo para el tipo antes mencionado de órdenes de HBA_API relacionadas con el tejido;

La fig. 5 muestra un diagrama de flujo que ilustra señales simplificadas y un flujo para el tipo antes mencionado de órdenes de HBA-API de correspondencia de FCP a SCSI; y

La fig. 6 muestra un diagrama de flujo que ilustra señales simplificadas y un flujo para el tipo antes mencionado de órdenes de HBA_API para manejar solicitudes de manejo de ELS iniciadas por la SAN.

Descripción Detallada del Invento

Con referencia a la fig. 1, se ha representado un diagrama de bloques que ilustra una primera realización de un sistema 100 de acuerdo con el presente invento. El sistema 100 comprende múltiples sistemas de ordenador 104, 105 y 106, estando todos adaptados para acceder a una SAN 110 a través de un adaptador 112 de Canal de Fibra Común que tiene un WWPN 1 (Nombre de Puerto de Ámbito Mundial). Con el propósito de claridad solo se han representado tres sistemas de ordenador. Se reconoce que el número de sistemas de ordenador puede ser de centenares o incluso de millares. Teniendo tal número elevado de sistemas de ordenador, más de un adaptador de Canal de Fibra puede estar presente en el sistema, sin embargo, incluso en este caso una pluralidad de sistemas de ordenador compartiría uno y el mismo adaptador de Canal de Fibra.

Como una pasarela entre cada uno de los sistemas de ordenador 104, 105 y 106 y el adaptador de Canal de Fibra, hay previsto un cortafuegos 114, 115 y 116, respectivamente, para asegurar que cada uno de los sistemas de ordenador está solo habilitado para acceder a partes permitidas de la SAN 110. Los cortafuegos 114, 115 y 116 pueden estar integrados en el adaptador de Canal de Fibra o unidos a él. Por otro lado, todos los sistemas de ordenador 104, 105 y 106 están conectados a una red 120, tal como una red Ethernet.

Además, el sistema 100 comprende dos o más sistemas de ordenador 122 y 123 que están conectados a la red 120, que acogen un Servidor 130 de Gestión de SAN (Servidor SM) que se ejecuta sobre un sistema operativo (OS) 131 y un Cliente 132 de Gestión de SAN (Cliente SM), respectivamente. El Servidor 130 de SM ejecuta la parte de servidor de un Sistema de Gestión de SAN, por ejemplo, Gestor de Red de Almacenamiento Tivoli

(http://www.tivoli.com/products/index/storage_net_mgr/), donde el Cliente 132 de SM ejecuta la parte de cliente respectiva de tal sistema.

El Servidor 130 de SM está conectado además a una aplicación 134 de control de cortafuegos a través de una línea de comunicación, mientras que el Cliente 132 de SM tiene un enlace de comunicación al adaptador 112 de Canal de Fibra. La aplicación 134 de control de cortafuegos está provista con enlaces de comunicación a cada uno de los cortafuegos 114, 115 y 116, bien a través del adaptador de Canal de Fibra (como se ha representado) o bien directamente a cada uno de ellos.

El Servidor 130 de SM accede a cada uno de los sistemas de ordenador 104, 105 y 106 a través de una Interfaz de Envolvente Segura respectiva 144, 145 y 146, es decir, un programa para registrarse, y ejecutar órdenes en, un ordenador remoto. Una interfaz de correspondencia MAP_IF 154, 155, 156 prevista en cada sistema de ordenador 104, 105 y 106 tiene cuidado de la correspondencia del Canal de Fibra a la SCSI (Interfaz de Sistema de Ordenador Pequeño). Esto puede por ejemplo ser puesto en práctica como una interfaz de línea de orden o un archivo de configuración.

Cada sistema de ordenador 104, 105 y 106 ejecuta un sistema operativo 164, 165 y 166, que puede ser “no seguro”. “No seguro” en este contexto significa que el sistema operativo puede ser controlado o manipulado por una entidad potencialmente peligrosa, por ejemplo, una pieza de código malicioso, tal como un virus de ordenador o una persona que intenta manipular indebidamente el sistema operativo con el fin de acceder o alterar información en la SAN, lo que sería inalcanzable para dicha entidad. El propio sistema operativo puede estar formado por cualquiera de una amplia variedad de sistemas operativos, tales como AIX o z/OS de Internacional Business Machines Corporation, UNIX y Linux.

Como el mecanismo de seguridad de acuerdo con el presente invento tiene en consideración que una solicitud de acceso a SAN no autorizada puede ser emitida por cualquiera de los sistemas de ordenador 104, 105 y 106, el cortafuegos respectivo 114, 115 y 116 filtra todas las solicitudes de acceso a SAN y sólo acepta aquellas autorizadas por la aplicación de control de cortafuegos. Solo la aplicación 134 de control de cortafuegos, que no es accesible por ninguno de los sistemas de ordenador 104, 105 y 106, está habilitada para que modifique ajustes de cortafuegos que especifican solicitudes autorizadas de acceso a SAN. De acuerdo con la primera realización del presente invento, el Servidor 130 de SM controla la aplicación 134 de control de cortafuegos.

El Cliente 132 de SM ejecuta por encima de la HBA_API 168 (Interfaz de Programa de Aplicación de Adaptador de Bus Anfitrión) por encima de un sistema operativo 170, que ha a ser “seguro”, es decir, el sistema operativo es gestionado por una entidad que no pretende manipular indebidamente los derechos de acceso a SAN o similares. El adaptador 112 de Canal

de Fibra está adaptado para distinguir sistemas operativos no seguros y seguros. Esta autorización puede ser cumplida identificando el sistema operativo 170 o el Cliente 132 de SM por algunos medios de esquemas de autorización bien conocidos como direcciones de fuente fijas (por ejemplos ID de hardware), claves y algoritmos criptográficos, o contraseñas, que no son parte de este invento. Las solicitudes relacionadas con la Información crucial, tal como la configuración de SAN, componentes de SAN, derechos de acceso a SAN, mensajes de error, estadísticas o información de facturación solo pueden ser aceptadas cuando provienen del sistema operativo seguro 170 que ejecuta el cliente 132 de SM. De forma correspondiente, los resultados de tales solicitudes son solo devueltos al sistema operativo seguro 170. En otras palabras, el Cliente 132 de SM controlado por el Servidor de SM y que actúa en lugar de los sistemas operativos no seguros solamente realiza la gestión de SAN.

El Servidor 130 de SM comprende un motor principal SM (no mostrado), que emite solicitudes con el fin de preguntar y ajustar información en la SAN y en los sistemas operativos gestionados y un módulo de comunicación (no mostrado), que encamina las solicitudes y respuestas desde el motor principal a los clientes. El módulo de comunicación puede o bien ser puesto en práctica como parte del Servidor de SM, o bien ser distribuido sobre sobre el Servidor de SM y los componentes de cliente de SM, que residen en los entornos “seguros”.

La sshd daemon de envolvente segura y las interfaces de configuración de FC específicas de OS son resumidos como servidor de RA (Acceso Remoto). El servidor de acceso remoto está adaptado para responder a solicitudes autorizadas enviadas por un servidor de SM o un cliente de SM. En una puesta en práctica preferida el cliente de SM y el servidor de RA usan datos de autorización tales como contraseñas, id de usuario y claves criptográficas para identificar al que origina las solicitudes. Por ello, el módulo de comunicación está equipado con un almacén (no mostrado) para dicha información de autorización. El módulo de comunicación separa solicitudes relacionadas con el tejido, es decir, solicitudes para gestionar el SAN, y solicitudes relacionadas con el adaptador, es decir, solicitudes para gestionar el adaptador de Canal de Fibra, de las solicitudes específicas de OS de acuerdo con la lista de órdenes siguiente. Como se ha mencionado antes, la conexión entre el servidor de SM, el cliente de SM y el servidor de RA es una red basada en el IP, que se ejecuta, por ejemplo, en Ethernet. En una realización diferente algunas comunicaciones entre el cliente de SM, el servidor de SM y el Servidor de RA podrían utilizar las capacidades de los adaptadores de FC para transportar otros protocolos en lugar de una red separada. Un ejemplo sería TCP/IP sobre Canal de Fibra.

Con referencia ahora a la fig. 2, se ha representado un diagrama de bloques que ilustra una segunda realización del sistema de acuerdo con el presente invento.

De acuerdo con el sistema de la primera realización (fig. 1), el presente sistema comprende múltiples sistemas de ordenador 204, 205 y 206, estando todos adaptados para acceder a una SAN 210 a través de un adaptador 212 de Canal de Fibra común que tiene un WWPN 1 (Nombre de Puerto de Ámbito Mundial). Con propósito de claridad sólo se han representado tres sistemas de ordenador. Se reconoce que el número de sistemas de ordenador puede ser de centenares o incluso de millares. Teniendo tal número elevado de sistemas de ordenador, más de un adaptador de Canal de Fibra puede estar presente en el sistema, sin embargo, incluso en este caso una pluralidad de sistemas de ordenador compartiría el mismo adaptador de Canal de Fibra.

Como una pasarela entre cada uno de los sistemas de ordenador 204, 205 y 206 y el adaptador de Canal de Fibra se ha previsto un cortafuegos 214, 215 y 216, respectivamente, para asegurar que cada uno de los sistemas de ordenador está solo habilitado para acceder a partes permitidas de la SAN 210. Los cortafuegos 214, 215 y 216 pueden estar integrados en el adaptador de Canal de Fibra o unidos a él.

Contrariamente a la primera realización, los servidores virtuales se ejecutan en un entorno de servidor virtual, tal como LPAR (modo dividido lógicamente) más VM (máquina Virtual), forman los sistemas de ordenador 204, 205 y 206. Además, se ha previsto otro servidor virtual 223 para alojar un Cliente 232 de Gestión de SAN (Cliente de SM). Los sistemas de ordenador 204, 205 y 206 comunican con el Cliente 232 de SM a través de una conexión de Envolvente Segura en la parte superior de los Hipersockets (o enlaces de muy alta velocidad de IBM).

Se ha previsto un sistema de ordenador separado 222 para alojar un Servidor de Gestión de SAN (Servidor de SM). El Servidor 230 de SM ejecuta la parte de servidor de un Sistema de Gestión de SAN, por ejemplo, Gestor de Red de Almacenamiento Tivoli, mientras que el Cliente 232 de SM ejecuta la parte de cliente respectiva de tal sistema. El Servidor 230 de SM accede al Cliente de SM a través de una red de Ethernet 220.

Cada sistema de ordenador 204, 205 y 206 ejecuta un sistema operativo 264, 265 y 266, que puede ser “no seguro” (véase lo anterior). El propio sistema operativo puede estar formado por cualquiera de una amplia variedad de sistemas operativos, tales como AIX o z/OS de Internacional Business Machine Corporation, UNIX y Linux.

El Cliente 232 de SM ejecuta por encima de la HBA_API 268 (Interfaz de Programa de Aplicación de Adaptador de Bus Anfitrión) por encima de un sistema operativo 270, que ha de ser “seguro”, (véase lo anterior). De nuevo, el adaptador 212 de Canal de Fibra está adaptado para distinguir sistemas operativos no seguros y seguros. Las solicitudes relacionadas con Información crucial sólo pueden ser aceptadas cuando provienen del sistema operativo seguro 270 que ejecuta el cliente 232 de SM. Una aplicación 234 de control de cortafuegos también se ejecuta por encima del sistema operativo “seguro” 270.

La aplicación de control de cortafuegos es usada para instruir a los cortafuegos 214, 215 y 216, de si realmente emiten o no solicitudes de acceso particular desde los sistemas operativos “no seguros” 264, 265 y 266 hasta la SAN 210. En otras palabras, sólo la aplicación 234 de control de cortafuegos, que no es accesible por ninguno de los sistemas de ordenador 204, 205 y 206, está habilitadapara modificar ajustes de cortafuegos que especifican solicitudes de acceso de SAN autorizadas.

Con referencia ahora a la fig. 3, se ha representado un diagrama de flujo que ilustra el método para hacer funcionar una red de área de almacenamiento en un entorno de servidor en el que múltiples servidores comparten un adaptador de Canal de Fibra de acuerdo con el presente invento (bloque 300). En primer lugar, el motor principal de SM crea una solicitud (bloque 302), y a continuación el módulo de comunicación determina el objetivo de la solicitud (bloque 306). En caso de que sea una solicitud para el SAN o el adaptador de Canal de Fibra, entonces el módulo de comunicación establece un trayecto de comunicación al Cliente de SM con datos de autorización respectivos (bloque 308), que pueden ser contraseñas, id de usuario y claves criptográficas.

Subsiguientemente, el Cliente de SM comprueba si la autorización es válida o no (bloque 312). Si lo es, el Cliente de SM crea una respuesta preguntando a entidades en la SAN tales como conmutadores (por ejemplo para recuperar una lista de dispositivos de FC en la SAN) o controladores de disco (por ejemplo para recuperar una lista de discos lógicos en el controlador) y ajustar el adaptador de Canal de Fibra y los atributos de SAN tales como RNID-ELS que es usado para registrar ciertos tipos de mensajes de notificación de error (bloque 314).

Si no lo es, el Cliente de SM crea una respuesta de rechazo que informa a dicho núcleo de SM de que la solicitud ha sido rechazada (bloque 316). Ambos trayectos alternativos continúan enviando la respuesta al sistema de comunicación (bloque 318).

Volviendo de nuevo al bloque 306, en caso de que el módulo de comunicación determine que el motor principal de SM ha creado una solicitud para los datos de configuración del sistema operativo (OS), tal como la correspondencia del canal de fibra al scsi definida por la función HBAGetFcpTargetMappingFunc, el módulo de comunicación establece un trayecto de comunicación al servidor de RA con los datos de autorización respectiva (bloque 320).

A continuación, el componente de autorización en el Servidor de RA, por ejemplo un sshd, determina si la autorización es válida o no (bloque 321) comparando los id de usuario, contraseñas y claves presentados a los id de usuario, contraseñas y claves, que son conocidos por el Servidor de RA que ha de ser autorizado.

Si lo es, el Servidor de RA crea una respuesta por operaciones de configuración de OS (bloque 324) tal como acceder a la información de configuración del canal de fibra almacenada por el controlador del dispositivo de canal de fibra del sistema operativo.

Si no lo es, el Servidor de RA crea una respuesta de rechazo (bloque 326). De nuevo, ambas alternativas continúan enviando la respuesta al sistema de comunicación (318). Subsiguientemente, el sistema de comunicaciones envía la respuesta al motor principal de SM (bloque 320) y el motor principal de SM en el servidor de SM procesa la respuesta (bloque 322) como se ha definido en las dos patentes mencionadas.

A continuación, se han mostrado el flujo y los tipos de solicitudes para una puesta en práctica preferida. Puede encontrarse la sintaxis de las órdenes HBA_API en “Proyecto de Trabajo de HBA API de Canal de Fibra” (ftp://ftp.t11.org/t11/pub/fc/hba/02-268v2.pdf)

1. En primer lugar, son recogidos las órdenes o comandos CT, ELS, SCSI de solicitudes relacionadas con el tejido y el adaptador. El cliente de SM que usa adaptador y los recursos SAN maneja estas órdenes:

typedef HBA_STATUS(* HBASendCTPassThruFunc) (HBA_HANDLE, void *, HBA_UINT32, void *, HBA_UINT32);

typedef HBA_STATUS (* HBASendRNIDFunc) (HBA_HANDLE, HBA-WWN, HBA_WWNTYPE, void *,HBA_UINT 32 *);

typedef HBA_STATUS (*HBASendScsiInquiryFunc) (HBA_HANDLE, HBA_WWN,HBA_UINT64, HBA_UINTB, HBA_UINT32,void *, HBA_UINT32, void *, HBA_UINT32);

typedef HBA_STATUS (* HBASendReportLUNsFunc) (HBA_HANDLE, HBA_WWN, void *, HBA_UINT32, void *,HBA_UINT32);

typedef HBA_STATUS (* HBASendReadCapacityFunc) (HBA_HANDLE, HBA-WWN, HBA_UINT64, void *, HBA_UINT32,void *, HBA_UINT32);

typedef HB~STATUS (* HBASendCTPassThruV2Func) (HBA_HANDLE, HBA_WWN, void *, HBA_UINT32, void *,HBA_UINT32 *);

typedef HBA-STATUS (* HBASendRNIDV2Func) (HBA_HANDLE, HBA_WWN, HBA-WWN, HBA_UINT32, HBA_UINT32, void *,HB~UINT32*);

typedef HBA_STATUS (* HBAScsiInquiryV2Func)

(HBA_HANDLE,HBA_WWN,HBA_WWN, HBA_UINT64, HBA_UINT8, HBA_UINT8, void *, HBA_UINT32 *, HBA_UINT8 *,void *, HBA_UINT32 *);

typedef HBA_STATUS (* HBAScsiReportLUNsV2Func) (HBA_HANDLE, HBA_WWN, HBA_WWN, void *, HBA_UINT32 *,HBA_UINT8 *, void *, HBA-UINT32 *);

typedef HBA_STATUS (* HBAScsiReadCapacityV2Func) (HBA_HANDLE, HBA-WWN, HBA_WWN, HBA-UINT64, void *,HBA-UINT32 *, HBA_UINTB *, void *, HBA_UINT32 *);

typedef HBA_STATUS (* HBASendRPLFunc) (HBA_HANDLE, HBA_WWN, HBA_WWN, HBA_UINT32,HBA_UINT32, void *, HBA_UINT32 *);

typedef HB~STATUS (* HBASendRPSFunc) (HBA_HANDLE, HBA_WWN, HBA_WWN, HBA_UINT32, HBA_WWN,HBA_UINT32, void *, HBA_UINT32 *); typedef HBA_STATUS (* HBASendSRLFUnc) (HBA_HANDLE, HBA_WWN, HBA_WWN, HBA-UINT32, void*,HBA_UINT32 *);

typedef HBA_STATUS (* HBASendLIRRFunc) (HBA_HANDLE, HBA_WWN, HBA_WWN, HBA_UINT8, HBA_UINT8,void *, HBA_UINT32 *);

typedef HBA_HANDLE (* HBAOpenAdapterFunc) (char *);

typedef void (* HBACloseAdapterFunc) (HBA-HANDLE);

typedef HBA_STATUS (* HBAGetAdapterAttributesFunc) (HBA_HANDLE, HBA_ADAPTERATTRIBUTES *);

typedef HBA_STATUS (* HBAGetAdapterPortAttributesFunc) (HBA_HANDLE, HBA_UINT32, HBA_POR TATTRIBUTES *);

typedef HBA_STATUS (* HBAGetPortStatisticsFunc) (HBA_HANDLE, HBA_UINT32, HBA_PORTSTATISTICS *);

typedef HBA_STATUS (* HBAGetDiscoveredPortAttributesFunc) (HBA_HANDLE, HBA_UINT32, HBA_UINT32, HBA_PORTATTRIBUTES *);

typedef HBA_STATUS (* RBAGetPortAttributesByWWNFunc) (HBA_HANDLE, HBA_WWN, HBA_PORTA TTRIBUTES *);

typedef void (* HBARefreshInformationFunc) (HBA_HANDLE);

typedef void (* HBAResetStatisticsFunc) (HBA_HANDLE, HBA_UINT32);

typedef HBA_STATUS (* RBAGetEventBufferFunc) (HBA_HANDLE, HBA_EVENTINFO *, HBA_UINT32 *);

typedef HBA_STATUS (* HBASetRNIDMgmtInfoFunc) (HBA_HANDLE, HBA_MGMTINFO *);

typedef HBA_STATUS (* HBAGetRNIDMgmtInfoFunc) (HBA_HANDLE, HBA_MGMTINFO *);

typedef HBA_STATUS (* HBAOpenAdapterByWWNFunc) (HBA_HANDLE *, HBA_WWN);

typedef void (* HBARefreshAdapterConfigurationFunc) ();

typedef HBA_UINT32 (*HBAGetVendorLibraryAttributesFunc)(HBA_LIBRARYATTRIBUTES *);

typedef HBA_STATUS (*HBAGetFC4StatisticsFunc) (HBA_HANDLE, HBA_WWN, HBA_UINT8, HBA_F C4STATISTICS *);

typedef HBA_STATUS (* HBAGetFCPStatisticsFunc) (HBA_HANDLE, const HBA_SCSIID *,HBA_FC4STATIS

typedef HBA_UINT32 (* HBAGetNumberOfAdaptersFunc) ();

typedef HBA_STATUS (* HBAGetAdapterNameFunc) (HBA_UINT32, char *);

La fig. 4 muestra un diagrama de flujo que ilustra señales simplificadas y el flujo para el tipo antes mencionado de órdenes de HBA_API. Como es evidente de la fig. 4, un Servidor de SM comunica con un Cliente de SM, que comunica con un Conmutador de FC. El Servidor de SM, el Cliente de SM y el Conmutador de FC han comenzado y se ejecutan independientemente entre sí como se ha ilustrado por los bloques 402, 404 y 406. Se reconoce que los siguientes pasos sólo constituyen un segmento de la operación, y más solicitudes son enviadas o recibidas antes o después del método como se ha descrito en lo que sigue.

Inicialmente el servidor de SM envía la solicitud al cliente de SM (bloque 408, 410). En este ejemplo es un

HBASendLIRRFunc. En detalle el cliente de SM usa el HBA API a fin de enviar secuencias de CT_IU, ELS o FC_CMD según se ha definido por los estándares de Canal de Fibra FC-FS y FC-GS3 al tejido (412, 414).

La respuesta generada en el tejido según se ha definido por los estándares de FC es enviada al cliente de SM por la parte de completado de la llamada de HBA_API (418, 420). El cliente de SM envía dicha respuesta al servidor de SM (422, 424).

2. Órdenes de correspondencia de FCP<->SCSI

Estas órdenes son manejadas mediante un servidor de RA que usa órdenes de recursos de OS y de un controlador de dispositivo de OS. La sintaxis puede ser encontrada en “Proyecto de Trabajo de HBA API de Canal de Fibras”.

(ftp://ftp.tll.org/tll/pub/fc/hba/02-268v2.pdf)

typedef HBA_STATUS (* HBAGetFcpTargetMappingFunc) (HBA_HANDLE, HBA_FCPTARGETMAPPING *);

typedef HBA_STATUS (* RBAGetFcpPersistentBindingFunc) (HBA_HANDLE, HBA_FCPBINDING *);

typedef HBA_STATUS (* HBAGetBindingCapabilityFunc) (HBA_HANDLE, HBA_WWN, RBA_BIND_CAPABILITY *);

typedef HBA_STATUS (* HBAGetBindingSupportFunc) (HBA_HANDLE, HBA-WWN, HBA_BIND_CAPABILITY *);

typedef HB~STATUS (* HBASetBindingSupportFunc) (HBA_HANDLE, HBA_WWN, HBA_BlND_CAPABILITY);

typedef HBA_STATUS (*HBASetPersistentBindingV2Func) (HBA-HANDLE, HBA_WWN, const HBA_FCPBIN DING2 *);

typedef HBA_STATUS (* HBAGetPersistentBindingV2Func) (HBA_HANDLE, HBA_WWN, HBA_FCPBINDING2 *);

typedef HBA_STATUS (* HBARemovePersistentBindingFunc) (HBA_HANDLE, HBA_WWN, const HBA_FCPBIN DING2 *);

typedef HBA_STATUS (* HBARemoveAllPersistentBindingsFunc) (HBA_HANDLE, HBA_WWN);

typedef HBA_STATUS (* HBAGetFcpTargetMappingV2Func) (HBA_HANDLE, HBA~WWN, HBA_FCPTARGE TMAPPING *);

Con referencia ahora a la fig. 5, se ha representado un diagrama de flujo que ilustra señales simplificadas y el flujo para el tipo antes mencionado de órdenes de HBA API. Como es evidente de la fig. 5, un servidor de SM comunica de nuevo con un cliente de SM. El cliente de SM, en retorno, comunica con un Cortafuegos y una imagen de OS, respectivamente. El servidor de SM, el cliente de SM, el Cortafuegos y la imagen de OS han comenzado y se ejecutan independientemente entre sí como se ha ilustrado por los bloques 502, 504, 506 y 508. Se reconoce que los siguientes pasos sólo constituyen un segmento de la operación, y más solicitudes son enviadas o recibidas antes o después del método como se ha descrito en lo que sigue.

En primer lugar el servidor de SM envía una solicitud al cliente de SM (bloques 510, 512) por ejemplo una solicitud que corresponde a la solicitud HBASetPersistentBindingV2 de HBA_API. Si el cliente de SM tiene control directo sobre el cortafuegos puede modificar opcionalmente el cortafuegos (514, 516, 518, 520) si ésto se requiere por la política de seguridad del cortafuegos. El cliente de SM modifica entonces el cortafuegos disparando la operación de envío de un mensaje de cortafuegos de actualización del propietario (514, 516).

El cortafuegos señala la terminación de la operación al cliente de SM (518, 520). A continuación el cliente de SM dispara un conjunto o solicitud de pregunta en imagen de OS no segura (526) por el servidor de RA (522, 524). El cliente de SM espera a la terminación del mensaje de dicha solicitud (528, 530) El cliente de SM devuelve la respuesta de dichas solicitudes al servidor de SM (532, 534).

3. ELSses entrantes (RNID)

Estos son mensajes, que inician en el tejido y necesitan ser enviados al servidor de SM. Estos mensajes son usados para identificar la fuente de problemas, que ocurren en la SAN.

Órdenes definidas en HBA_API para manejar ELSses entrantes:

typedef HBA_STATUS (* HBARegisterForAdapterAddEventsFunc) (void (*) (void *, HBA_WWN, HBA_UINT32), void *,HBA_CALLBACKHANDLE *);

typedef HBA_STATUS (* HBARegisterForAdapterEventsFunc) (void (*) (void *, HBA_WWN, HBA_UINT32),void *,HBA_HANDLE, HBA_CALLBACKHANDLE *);

typedef HBA_STATUS (* HBARegisterForAdapterPortEventsFunc) (void (*) (void *, HBA_WWN, HBA_UINT32,

HBA_UINT32),void *, HBA_HANDLE, HBA-WWN, HBA_CALLBACKHANDLE *);

typedef HBA_STATUS (* HBARegisterForLinkEventsFunc) (void (*) (void *, HBA_WWN, HBA_UINT32, void *,HBA_UINT32),void *, void *, HBA_UINT32, HBA_HANDLE,HBA_CALLBACKHANDLE *);

typedef HBA_STATUS (* HBARegisterForAdapterPortStatEventsFunc) (void (*) (void *, HBA_WWN, HBA_UINT32), void *,HBA_HANDLE, HBA_WWN, HBA_PORTSTATISTICS, HBA_UINT32, HBA_CALL BACK HANDLE *);

typedef HBA_STATUS (* HBARegisterForTargetEventsFunc) (void (*) (void *, HBA_WWN, HBA_WWN, HBA_UINT32),void *, HBA_HANDLE, HBA-WWN, HBA_WWN,HBA_CALLBACKHANDLE *, HBA_UINT32);

typedef HBA_STATUS (* HBARemoveCallbackFunc) (HBA_CALLBACKHANDLE);

Ahora, con referencia a la fig. 6, que represente un diagrama de flujo que ilustra las señales simplificadas y el flujo para el tipo antes mencionado de órdenes de HBA_API. Como resulta evidente a partir de la fig. 6, un Servidor de SM comunica con un Cliente SM, que comunica con un conmutador de FC. El Servidor de SM, el Cliente de SM y el Conmutador de FC han comenzado y son ejecutados independientemente entre sí como se ha ilustrado por los bloques 602, 604 y 606. Se reconoce que los siguientes pasos solo constituyen un segmento de la operación, y son enviadas más solicitudes antes o después del método como se ha descrito en lo que sigue.

El servidor de SM (602) instruye al cliente de SM (604) para registrar una vez eventos por HBA_API (608, 610) y espera la confirmación de la terminación (612, 614), no se permiten registrar imágenes de OS no seguras. Después de que esto haya sido realizado cada mensaje (616) creado por la SAN dispara el procedimiento siguiente:

1. El cliente de SM recibe el evento desde el adaptador de FC (616, 618)

2. El cliente de SM envía el evento al servidor de SM (620, 622).

En una puesta en práctica alternativa el cliente de SM puede filtrar y condensar los mensajes (616, 618) para reducir el número de mensajes enviados al servidor de SM.

Funciones HBA_API que no son relevantes para este invento:

typedef HBA_UINT32 (* HBAGet VersionFunc) ();

typedef HBA_STATUS (* HBALoadLibraryFunc) ();

typedef HBA_STATUS (* HBAFreeLibraryFunc) ();

El presente invento puede ser realizado en hardware, software o en una combinación de hardware y software. Cualquier tipo de sistema de ordenador – o aparato adaptado para llevar a la práctica los métodos descritos aquí – es adecuado. Una combinación típica de hardware y software podría ser un sistema de ordenador de propósito general con un programa de ordenador que, cuando es cargado y ejecutado, controla el sistema de ordenador de tal modo que lleva a cabo los métodos descritos aquí. El presente invento puede también estar embebido en un producto de programa de ordenador, que comprende todas las características que permiten la puesta en práctica de los métodos descritos aquí, y que – cuando es cargado en un sistema de ordenador – es capaz de llevar a la práctica estos métodos.

Los medios del programa de ordenador o el programa de ordenador en el presente contexto significan cualquier expresión, en cualquier lenguaje, código o notación, de un conjunto de instrucciones destinadas a hacer que un sistema que tiene una capacidad de tratamiento de información realice una función particular bien directamente o bien después de cualquiera o ambas de las siguientes a) conversión a otro lenguaje, código o notación; b) reproducción en una forma material diferente.

REIVINDICACIONES

1. Un sistema (100) para hacer funcionar una red de área de almacenamiento, SAN, en un entorno de servidor en el que múltiples servidores comparten un adaptador (112) de Canal de Fibra, comprendiendo el sistema: un Servidor (130) de Gestión de SAN, una Red de Canal de Fibra que proporciona una conexión a dispositivos de almacenamiento, y una pluralidad de Imágenes (164, 165, 166) de Sistema Operativo que se ejecuta en dicho entorno de servidor, caracterizado porque un Cliente (132) de Gestión de SAN que está conectado a dicho Servidor (130) de Gestión de SAN, un adaptador (112) de Canal de Fibra, un adaptador de FC, con al menos un cortafuegos (114, 115, 116) unido a él, por lo que el Cliente de Gestión de SAN seguro está configurado para emitir órdenes en dicha Red de Canal de Fibra en lugar de cada una de dichas Imágenes del Sistema Operativo, Imágenes de OS; por lo que solo una aplicación (134) de control de cortafuegos, no accesible por ninguno de los múltiples servidores, está habilitada para modificar ajustes de cortafuegos que especifican órdenes autorizados de dichos servidores múltiples.

2. El sistema según la reivindicación precedente, en el que dicho Servidor de Gestión de SAN está configurado para distinguir un primer conjunto de órdenes y un segundo conjunto de órdenes, por lo que el primer conjunto de órdenes es procesado por el Cliente de Gestión de SAN junto con dicha SAN, y por lo que dicho segundo conjunto de órdenes es procesado por dichas Imágenes de OS sin acceso a dicho SAN.

3. El sistema según una de las reivindicaciones precedentes, en el que dicho Cliente de Gestión de SAN está configurado para distinguir un primer conjunto de órdenes y un segundo conjunto de órdenes, por lo que el primer conjunto de órdenes es procesado por el Cliente de Gestión de SAN junto con dicha SAN, y por lo que dicho segundo conjunto de órdenes es procesado por dichas Imágenes de OS sin acceso a dicho SAN.

4. El sistema según una de las reivindicaciones precedentes, en el que el entorno de servidor incluye servidores virtuales.

5. El sistema según una de las reivindicaciones precedentes, en el que el entorno de servidor incluye servidores divididos.

6. El sistema según una de las reivindicaciones precedentes, en el que dicho adaptador de Canal de Fibra (adaptador de FC) está configurado para autenticar dicho Cliente de Gestión de SAN seguro.

7. El sistema según una de las reivindicaciones precedentes, en el que dicho adaptador de FC y dicha SAN están adaptados para restringir el acceso de las Imágenes de OS no seguras al conjunto mínimo necesario de órdenes.

8. El sistema según la reivindicación 4 en el que dicho adaptador de FC y una capa de virtualización del servidor virtual están adaptados para restringir el acceso de las Imágenes de OS no seguras al conjunto mínimo necesario de órdenes.

9. El sistema según la reivindicación 8, en el que uno o más Clientes de Gestión de SAN de reserva están previstos para proporcionar redundancia.

10. El sistema según una de las reivindicaciones precedentes, en el que solo el Cliente de Gestión de SAN está registrado para recibir mensajes desde la SAN y el Cliente de Gestión de SAN está configurado para enviar dichos mensajes solo a dicho Servidor de Gestión de SAN.

11. El sistema según una de las reivindicaciones precedentes, en el que el Adaptador de FC está configurado para enviar todos los mensajes generados por la SAN para los que no es necesario un registro únicamente al Cliente de Gestión de SAN y no a las imágenes de OS no seguro.

12. El sistema según una de las reivindicaciones precedentes, en el que el Adaptador de FC está configurado para enviar una copia de todos los mensajes generados por el SAN para los que no es necesario un registro al Cliente de Gestión de SAN además de enviar el mensaje original a las Imágenes de OS no seguras.

13. El sistema según una de las reivindicaciones precedentes, en el que el entorno de servidor está equipado con dos clases de agentes, en particular, el Cliente de Gestión de SAN y un Servidor de Acceso Remoto, Servidor de RA.

14. El sistema según la reivindicación 13, en el que el Servidor de Gestión de SAN está equipado con un almacén para conservar los datos de autorización para acceder al Servidor de RA.

15. El sistema según la reivindicación 13, en el que el Cliente de Gestión de SAN está equipado con un almacén para conservar datos de autorización para acceder al Servidor de RA.

16. El sistema según una de las reivindicaciones precedentes, en el que el Cliente de Gestión de SAN y el adaptador de FC están configurados para reunir información fiable usada para facturar el uso de recursos por cada imagen de OS no seguro.

17. El sistema según una de las reivindicaciones precedentes, en el que el Servidor de Gestión de SAN está adaptado para comunicar con la aplicación de control de cortafuegos, con el fin de ajustar los derechos de acceso.

18. El sistema según una de las reivindicaciones 13 a 15, en el que el Cliente de Gestión de SAN está adaptado para funcionar como un encaminador para las solicitudes desde el Servidor de Gestión de SAN al servidor de RA.

19. El sistema según una de las reivindicaciones 13 a 15, en el que el Servidor de RA está formado por un servidor telnet/sshd existente.

20. Un método para hacer funcionar una red de área de almacenamiento, SAN, en un entorno de servidor en el que múltiples imágenes del sistema operativo comparten un adaptador de Canal de Fibra con al menos un cortafuegos (114, 115, 116) unido a él, comprendiendo el método las operaciones de: gestionar el SAN por un software de Gestión de SAN con al menos un Servidor (130) de Gestión de SAN y al menos un Cliente (132) de Gestión de SAN con un trayecto de comunicación a dicho adaptador (112) de Canal de Fibra, separar las solicitudes emitidas por el Servidor de Gestión de SAN en al menos dos grupos, procesar un primer grupo por el adaptador (112) de Canal de Fibra y la SAN en interés del Cliente (130) de Gestión de SAN en lugar de otros sistemas operativos que comparten el mismo adaptador, correspondiente a un trayecto seguro, y procesar un segundo grupo por los otros sistemas operativos sin la necesidad de enviar o recibir solicitudes al adaptador de FC y la SAN o recibirlas de los mismos; y controlar dicho cortafuegos (114, 115, 116) modificando ajustes de cortafuegos que especifican solicitudes de SAN autorizadas de dichas múltiples imágenes del sistema operativo solo por una aplicación (134) de control de cortafuegos, no accesible por cualquiera de las múltiples imágenes del sistema operativo.

21. El método según la reivindicación 20, que comprende además la operación de: encaminar toda la información contenida en mensajes no solicitados generados en la SAN y en el adaptador de FC al Gestor de SAN por el Cliente de gestión de SAN.

22. El método según la reivindicación 20 o 21, que comprende además la operación de: usar las solicitudes de vinculación de HBA_API para modificar los cortafuegos.

23. El método según una de las reivindicaciones 20 a 22, que comprende además la operación de: acceder a toda la información relevante para facturar imágenes individuales del sistema operativo generadas en el adaptador y la SAN solo a través del Cliente de Gestión de SAN en el trayecto seguro.

24. El método según una de las reivindicaciones 20 a 23, que comprende además la operación de: dicho Servidor de Gestión de SAN que proporciona datos de autorización al Cliente de Gestión de SAN para ejecutar solicitudes desde dicho primer grupo.

25. El método según una de las reivindicaciones 20 a 24, que comprende además la operación de: dicho Servidor de Gestión de SAN y dicho Cliente de Gestión de SAN que proporcionan datos de autorización a las otras imágenes de OS para ejecutar solicitudes desde dicho segundo grupo.

26. Un producto de programa de ordenador almacenado en un medio utilizable por ordenador, que comprende medios de programa legibles por ordenador para hacer que un ordenador realice un método según cualquiera de las reivindicaciones precedentes 20 a 25.

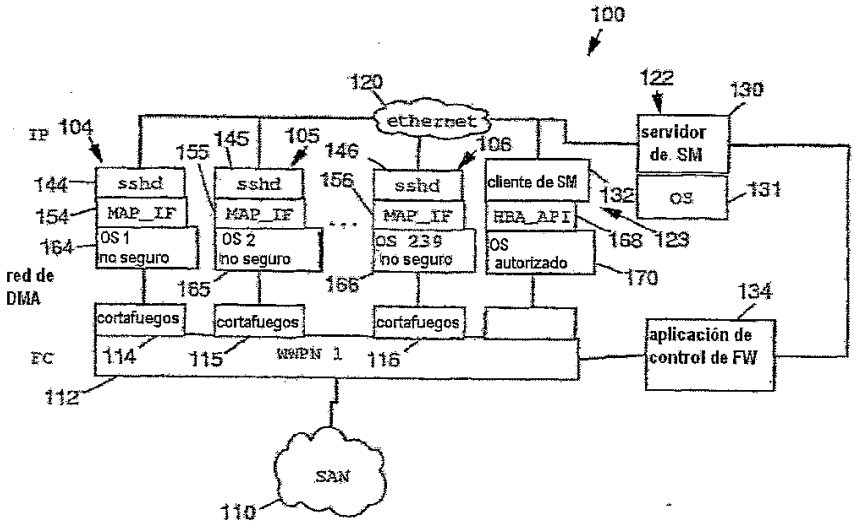
100
120
ethernet
122
130
servidor de SM
IP
104
155
145
105
146
106
144
sshd
sshd
sshd
cliente de SM
132
OS
131
154
MAP_IF
MAP_IF
MAP_IF
HBA_API
168
123
164
OS 1 no seguro
OS 2 no seguro
OS 239 no seguro
OS autorizado
170
red de DMA
165
166
134
cortafuegos
cortafuegos
cortafuegos
aplicación de control de FW
FC
114
115
WWPN 1
116
112
SAN
110

Fig. 1

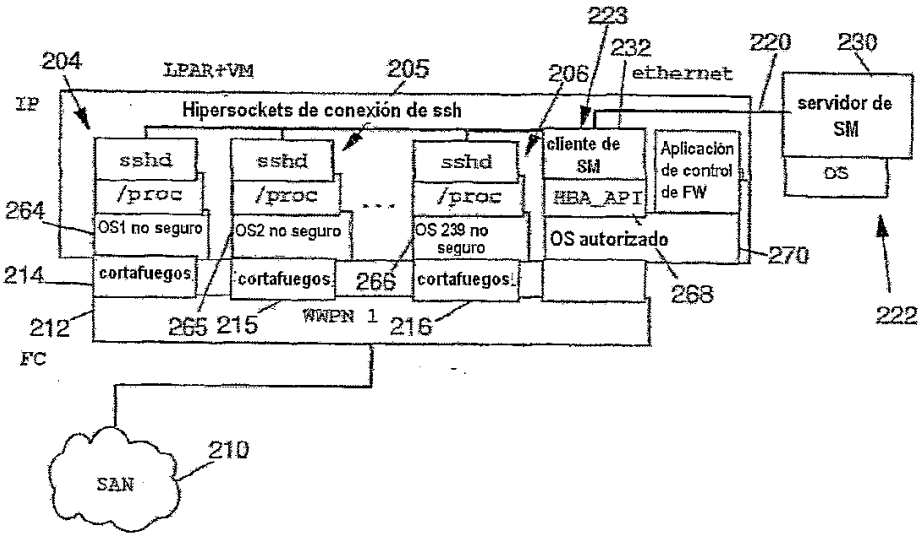
223
232
220
230
204
LPAR+VM
205
206
ethernet
IP
Hipersockets de conexión de ssh
servidor de SM
sshd
sshd
sshd
cliente de SM
Aplicación de control de FW
/proc
/proc
/proc
HBA_API
OS
264
OS1 no seguro
OS2 no seguro
OS 239 no seguro
OS autorizado
270
214
cortafuegos
cortafuegos
266
cortafuegos
268
212
265
215
WWPN 1
216
222
FC
210
SAN

Fig. 2

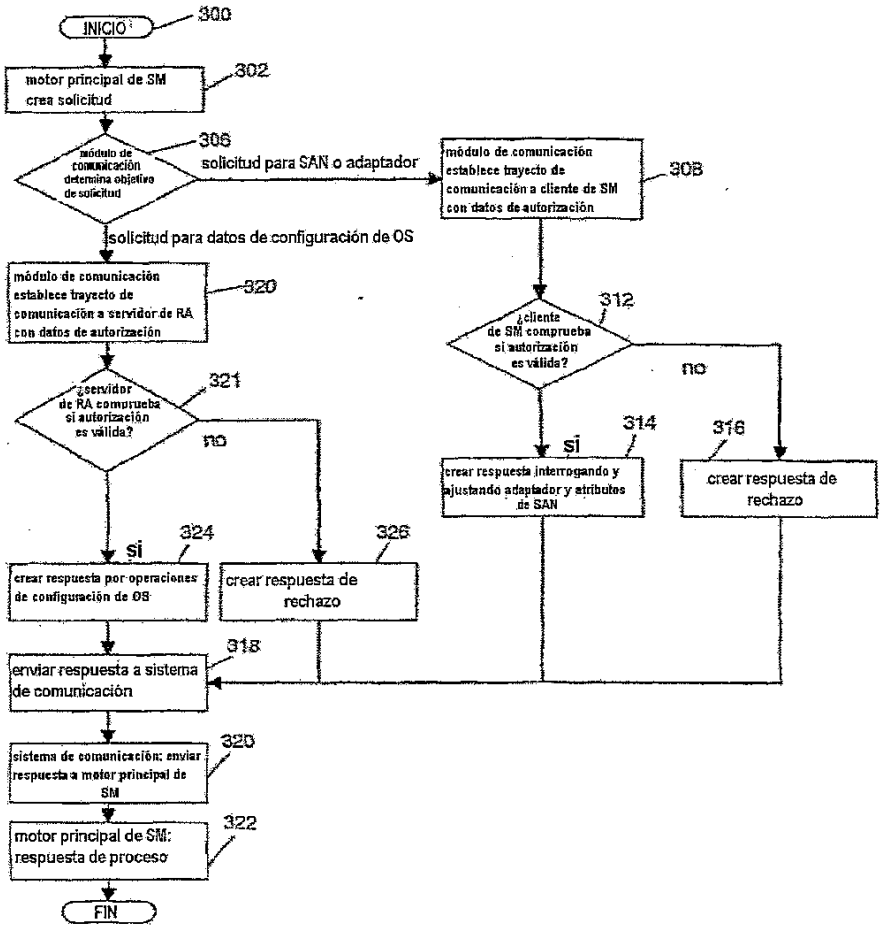
INICIO
300
motor principal de SM crea solicitud
302
módulo de comunicación determina objetivo de solicitud
306
solicitud para SAN o adaptador
módulo de comunicación establece trayecto de comunicación a cliente de SM con datos de autorización
308
solicitud para datos de configuración de OS
módulo de comunicación establece trayecto de comunicación a servidor de RA con datos de autorización
320
¿cliente de SM comprueba si autorización es válida?
312
no
si
314
crear respuesta interrogando y ajustando adaptador y atributos de SAN
316
crear respuesta de rechazo
¿servidor de RA comprueba si autorización es válida?
321
no
si
324
crear respuesta por operaciones de configuración de OS
326
crear respuesta de rechazo
enviar respuesta a sistema de comunicación
318
sistema de comunicación: enviar respuesta a motor principal de SM
320
motor principal de SM: respuesta de proceso
322
FIN

Fig. 3

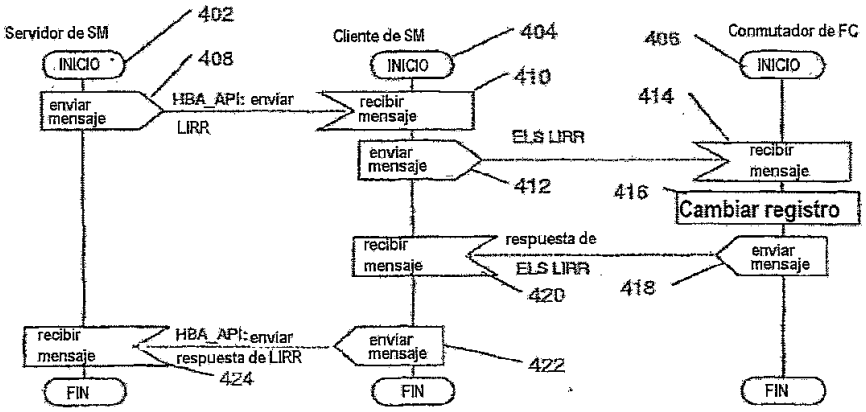
Servidor de SM
Cliente de SM
Conmutador de FC
INICIO
402
404
406
408
410
414
enviar mensaje
HBA_API: enviar LIRR
recibir mensaje
ELS LIRR
412
416
Cambiar registro
respuesta de ELS LIRR
418
420
HBA_API: enviar respuesta de LIRR
422
424
FIN

Fig. 4

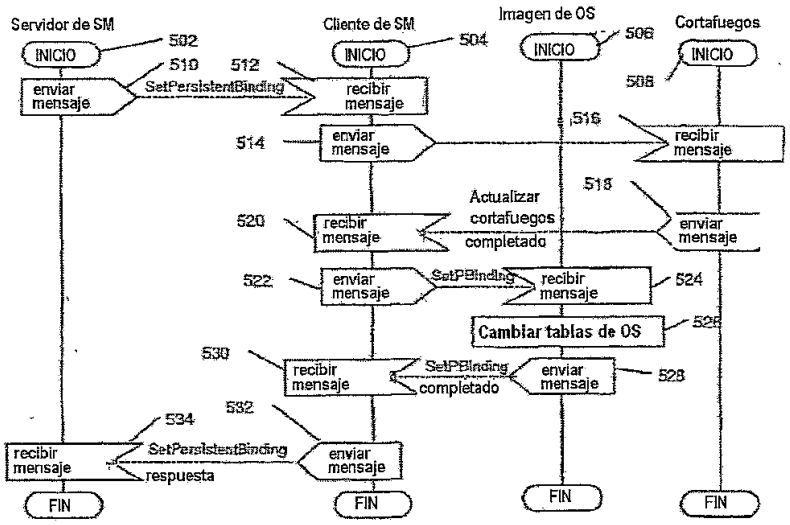
Servidor de SM
Cliente de SM
Imagen de OS
Cortafuegos
INICIO
502
504
506
508
510
512
514
516
518
520
522
524
526
528
530
532
534
SetPersistentBinding
Actualizar cortafuegos completado
SetPBinding
Cambiar tablas de OS
respuesta
FIN

Fig. 5

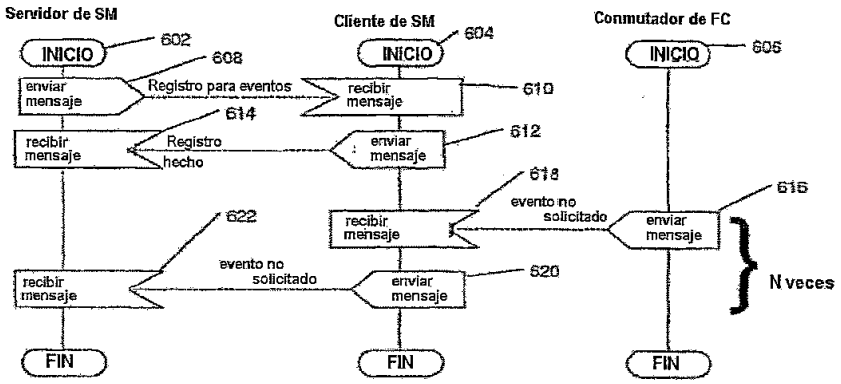
Servidor de SM
Cliente de SM
Conmutador de FC
INICIO
602
604
606
608
Registro para eventos
enviar mensaje
recibir mensaje
610
614
Registro hecho
612
618
evento no solicitado
615
622
evento no solicitado
620
N veces
FIN

Fig. 6