(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 643 489**

(51) Int. CI.:

H04L 12/24 (2006.01)
H04L 29/14 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.10.2001 E 11190558 (4)**

(97) Fecha y número de publicación de la concesión europea: **19.07.2017 EP 2424165**

(54) Título: **Sistema y procedimiento para la gestión distribuida de ordenadores compartidos**

(30) Prioridad:

24.10.2000 US 695812

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.11.2017

(73) Titular/es:

ZHIGU HOLDINGS LIMITED (100.0%)
Harneys Services (Cayman) Limited 4th Floor, Harbour Place 103 South Church Street George Town P.O. Box 10240
Grand Cayman KY1-1002, KY

(72) Inventor/es:

HUNT, GALEN C.;
HYDRIE, AAMER;
LEVI, STEVEN P.;
STUTZ, DAVID S.;
TABBARA, BASSAM y
WELLAND, ROBERT V.

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Sistema y procedimiento para la gestión distribuida de ordenadores compartidos

Campo técnico

Esta invención se refiere a la gestión de sistemas informáticos. Más específicamente, la invención se refiere a la gestión distribuida de ordenadores compartidos.

Antecedentes de la invención

La Internet y su uso se han ampliado considerablemente en los últimos años, y se espera que esta expansión continúe. Una forma significativa en la que se usa la Internet es la World Wide Web ((telaraña mundial) también conocida como la "web"), que es una colección de documentos (que se denomina como "páginas web") que los usuarios pueden ver o de otro modo ejecutar y que, por lo general, incluyen enlaces a una o más páginas a las que el usuario puede tener acceso. Muchas empresas e individuos han creado una presencia en la web, por lo general consiste en una o más páginas web describiéndose a sí mismos, la descripción de sus productos o servicios, la identificación de otras informaciones de interés, permitiendo que los bienes o servicios se compren, etc.

Las páginas web suelen estar disponibles en la web a través de uno o más servidores web, un procedimiento denominado como "alojamiento" de las páginas web. A veces, estas páginas web están disponibles para cualquiera que las solicite (por ejemplo, los anuncios de una empresa) y otras veces el acceso a las páginas web está restringido (por ejemplo, puede ser necesaria una contraseña para acceder a las páginas web). Dado el gran número de personas que pueden estar solicitando ver las páginas web (especialmente a la luz de la accesibilidad global a la web), puede ser necesario un gran número de servidores para alojar adecuadamente las páginas web (por ejemplo, la misma página web puede alojarse en múltiples servidores para aumentar el número de personas que pueden acceder a la página web de manera concurrente). Además, debido a que la web está distribuida geográficamente y tiene una no uniformidad de acceso, a menudo puede desearse distribuir los servidores en diversos lugares remotos con el fin de minimizar los tiempos de acceso para las personas en diversos lugares del mundo. Además, las personas tienden a ver las páginas web todo el día (de nuevo, especialmente a la luz de la accesibilidad global a la web), por lo que los servidores que alojan páginas web deberían mantenerse funcionales las 24 horas del día.

Sin embargo, puede ser difícil gestionar un gran número de servidores. Un suministro de energía fiable es necesario para garantizar que los servidores puedan funcionar. La seguridad física es necesaria para garantizar que un ladrón u otra persona maliciosa no intenten dañar o robar los servidores. Se requiere una conexión a Internet fiable para garantizar que las solicitudes de acceso lleguen a los servidores. Se requiere un entorno operativo adecuado (por ejemplo, temperatura, humedad, etc.) para garantizar que los servidores funcionen correctamente. Por lo tanto, se han desarrollado "instalaciones de co-localización" que ayudan a las empresas a manejar estas dificultades.

Una instalación de co-localización se refiere a un complejo que puede alojar diversos servidores. La instalación de co-localización suele proporcionar una conexión a Internet fiable, un suministro de energía fiable y un entorno operativo adecuado. La instalación de co-localización también incluye normalmente múltiples áreas seguras (por ejemplo, jaulas) en las que diferentes empresas pueden ubicar sus servidores. La recopilación de servidores que una empresa específica ubica en la instalación de co-localización se denomina como un "grupo de servidores", aunque de hecho puede haber solo un único servidor en cualquier instalación de co-localización individual. La empresa específica es la responsable de gestionar el funcionamiento de los servidores en su grupo de servidores.

Sin embargo, tales instalaciones de co-localización también presentan problemas. Un problema es la seguridad de los datos. Diferentes empresas (incluso competidoras) pueden tener los grupos de servidores en la misma instalación de co-localización. En tales circunstancias, se requiere mucho cuidado para garantizar que los datos recibidos a través de Internet (o enviados por un servidor en el grupo de servidores) que están destinados a una empresa no se encaminan a un servidor de otra empresa ubicada en la instalación de co-localización.

Un problema adicional es la gestión de los servidores una vez que se colocan en la instalación de co-localización. Actualmente, un administrador de sistema de una empresa puede ponerse en contacto con un administrador de la instalación de co-localización (normalmente por teléfono) y pedirle que restablezca un servidor determinado (normalmente pulsando un botón de reinicio del hardware en el servidor o apagando y a continuación encendiendo el servidor) en el caso de un fallo de (u otro problema con) el servidor. Esta capacidad limitada de solo restablecimiento proporciona muy poca funcionalidad de gestión a la empresa. Como alternativa, el administrador del sistema de la compañía puede desplazarse él mismo físicamente a la instalación de co-localización y atender al servidor defectuoso. Desafortunadamente, una cantidad significativa de tiempo puede desperdiciarse por el administrador del sistema en desplazarse a la instalación de co-localización para atender a un servidor. Por lo tanto, sería beneficioso tener una forma mejorada de gestionar ordenadores servidores remotos en una instalación de co-localización.

Otro problema se refiere a la aplicación de los derechos tanto de los operadores de los servidores en la instalación de co-localización como de los operadores del servicio web alojado en los servidores. Los operadores de los

servidores deben ser capaces de mantener sus derechos (por ejemplo, volver a controlar las zonas de la instalación donde se almacenan los servidores), aunque los servidores sean propiedad de los operadores del servicio web. Además, los operadores del servicio web deben tener la seguridad de que sus datos permanecen seguros.

La invención descrita a continuación aborda estas desventajas, mejorando la gestión distribuida de los ordenadores compartidos en instalaciones de co-localización.

El documento EP 1 024 428 A2 desvela un sistema informático agrupado que proporciona ventajas tanto de velocidad como de fiabilidad. Sin embargo, cuando las comunicaciones entre los ordenadores agrupados se ven comprometidas, los mismos ordenadores pueden convertirse en archivos de base de datos confusos y corruptos. El presente procedimiento y aparato se usan para mejorar la gestión de los sistemas informáticos agrupados. Específicamente, el sistema amplía el número de nodos disponibles para condiciones de tolerancia frente a fallos. Además, se prevé el retorno del sistema a un estado inicial después de un evento de tolerancia frente a fallos.

El documento de Estados Unidos 5 287 453 A desvela un sistema informático de grupo que incluye una pluralidad de sistemas informáticos operados independientemente, localizados en estrecha proximidad entre sí. Cada sistema incluye un bus del sistema, una memoria y un conjunto de dispositivos periféricos locales que se conectan en común al bus del sistema. Los sistemas informáticos están interconectados para transferir mensajes entre sí a través de los canales de un controlador de grupo de alta velocidad que se conecta a los buses del sistema. Cada sistema incluye además un controlador de grupo que transfiere los mensajes entre la memoria del sistema informático y el canal de controlador de grupo correspondiente cuando el sistema está configurado para funcionar en un modo de funcionamiento de grupo. Los programas de aplicación de usuario emiten llamadas de monitor para acceder a los archivos contenidos en un dispositivo(s) periférico. La instalación de acceso rápido a archivos remotos (FRFA) incluida en cada sistema tras detectar que el dispositivo periférico no está conectado localmente, empaqueta la llamada de monitor y la información que identifica la aplicación de usuario en un mensaje. El mensaje se transfiere a través del controlador de grupo y del controlador de grupo al FRFA del sistema informático al que se conecta el dispositivo periférico. La llamada de monitor se ejecuta y la respuesta se envía de vuelta a través del controlador de grupo y se entrega a la aplicación de usuario de una manera tal que el dispositivo periférico de los otros sistemas informáticos parece estar conectado localmente y la llamada de monitor parece estar ejecutada localmente.

Sumario de la invención

La presente invención proporciona un procedimiento de acuerdo con la reivindicación 1.

En el presente documento se describe la gestión distribuida de ordenadores compartidos. De acuerdo con un aspecto, se emplea una arquitectura de gestión de múltiples niveles que incluye un nivel de desarrollo de aplicación, un nivel de operaciones de aplicación, y un nivel de operaciones de grupo. En el nivel de desarrollo de aplicaciones, las aplicaciones se desarrollan para su ejecución en uno o más ordenadores servidores. En el nivel de las operaciones de aplicación, se gestiona la ejecución de las aplicaciones y pueden establecerse sub-límites dentro de un grupo de servidores en una instalación de co-localización. En el nivel de operaciones de grupo, se gestiona el funcionamiento de los ordenadores servidores sin preocuparse de qué aplicaciones se están ejecutando en uno o más ordenadores servidores y pueden establecerse límites de grupo de servidores en la instalación de co-localización.

De acuerdo con otro aspecto, una instalación de co-localización incluye múltiples grupos de servidores, cada uno correspondiente a un cliente diferente. Para cada grupo de servidores, se implementa una consola de gestión de operaciones de grupo a nivel local en la instalación de co-localización para gestionar las operaciones de hardware del grupo, y se implementa una consola de gestión de operaciones de aplicación en una localización remota de la instalación de co-localización para gestionar las operaciones del software del grupo. En el caso de un fallo de hardware, la consola de gestión de operaciones de grupo toma acciones correctivas (por ejemplo, notificar a un administrador de la instalación de co-localización o intentar corregir el fallo en sí). En el caso de fallo del software, la consola de gestión de operaciones de aplicación toma acciones correctivas (por ejemplo, notificar a uno de los gestores del cliente o intentar corregir el fallo en sí).

De acuerdo con otro aspecto, los límites de un grupo de servidores se establecen mediante una consola de gestión de operaciones de grupo. El establecimiento de los límites garantiza que los datos se encaminan solo a los nodos dentro del grupo de servidores y no a otros nodos en la instalación de co-localización que no forman parte del grupo de servidores. Pueden establecerse otros sub-límites dentro de un grupo de servidores mediante una consola de gestión de operaciones de aplicación para garantizar que los datos se encaminan solo a los nodos específicos dentro del grupo de servidores.

De acuerdo con otro aspecto, se venden a un cliente los derechos de múltiples ordenadores servidores que se localizan en una instalación de co-localización y se aplica un esquema de gestión de múltiples niveles en los ordenadores servidores. De acuerdo con el esquema de gestión de múltiples niveles, el funcionamiento del hardware de los ordenadores servidores se gestiona localmente en la instalación de co-localización, mientras que el funcionamiento del software de los ordenadores servidores se gestiona desde una localización remota de la instalación de co-localización. Los ordenadores servidores pueden venderse directamente al cliente o alquilarse al

cliente.

De acuerdo con otro aspecto, se crea una relación de arrendador/inquilino usando uno o más ordenadores servidores en una instalación de co-localización. El operador de la instalación de co-localización suministra la instalación, así como los servidores (y por lo tanto puede verse como un “arrendador”), mientras que los clientes de la instalación alquilan el uso de la instalación, así como los servidores en esa instalación (y por lo tanto pueden verse como “inquilinos”). Esta relación entre arrendador/inquilino permite al arrendador establecer grupos de ordenadores para diferentes inquilinos y establecer límites entre los grupos de tal manera que los datos de un inquilino no pasan más allá de su grupo (y a otro grupo del inquilino). Además, se emplea el cifrado de diversas maneras para garantizar al inquilino que la información almacenada en los servidores que arrenda no puede verse por nadie más, incluso si el inquilino termina su arrendamiento o devuelve al arrendador uno de los servidores que está arrendando.

De acuerdo con otro aspecto, se emplea una arquitectura de gestión de múltiples niveles en la gestión de ordenadores que no son parte de una instalación de co-localización. Esta arquitectura de múltiples niveles se usa para gestionar ordenadores (tanto si se trata de ordenadores servidores como de otro tipo) con una variedad de configuraciones, como empresas, hogares, etc.

Breve descripción de los dibujos

La presente invención se ilustra a modo de ejemplo y no de limitación en las figuras de los dibujos adjuntos. Los mismos números se usan en todas las figuras para hacer referencia a componentes y/o características similares.

La figura 1 muestra un sistema de red cliente/servidor y un entorno tal como el que puede usarse con ciertas realizaciones de la invención.
La figura 2 muestra un ejemplo general de un ordenador que puede usarse de acuerdo con ciertas realizaciones de la invención.
La figura 3 es un diagrama de bloques que ilustra una instalación de co-localización a modo de ejemplo con más detalle.
La figura 4 es un diagrama de bloques que ilustra una arquitectura de gestión de múltiples niveles a modo de ejemplo.
La figura 5 es un diagrama de bloques que ilustra un nodo a modo de ejemplo con más detalle de acuerdo con ciertas realizaciones de la invención.
La figura 6 es un diagrama de flujo que ilustra un proceso a modo de ejemplo para la generación y distribución de una clave de cifrado de acuerdo con ciertas realizaciones de la invención.
La figura 7 es un diagrama de flujo que ilustra un proceso a modo de ejemplo para la operación de una consola de gestión de operaciones de grupo de acuerdo con ciertas realizaciones de la invención.
La figura 8 es un diagrama de flujo que ilustra un proceso a modo de ejemplo para la operación de una consola de gestión de operaciones de aplicación de acuerdo con ciertas realizaciones de la invención.

Descripción detallada

La figura 1 muestra un sistema de red cliente/servidor y un entorno tal como el que puede usarse con ciertas realizaciones de la invención. En general, el sistema incluye múltiples (n) ordenadores 102 cliente y múltiples (m) instalaciones 104 de co-localización incluyendo cada una, múltiples grupos de ordenadores 106 servidores (grupos de servidores). Los ordenadores servidores y cliente se comunican entre sí a través de una red 108 de comunicaciones de datos. La red de comunicaciones de la figura 1 comprende una red 108 pública tal como Internet. También pueden usarse otros tipos de redes de comunicaciones, además de o en lugar de Internet, incluidas las redes de área local (LAN), las redes de área extensa (WAN), etc. La red 108 de comunicaciones de datos puede implementarse en cualquiera de una variedad de diferentes maneras, incluyendo los medios de comunicaciones cableados y/o inalámbricos.

La comunicación a través de la red 108 puede realizarse usando cualquiera de una amplia variedad de protocolos de comunicaciones. En una implementación, los ordenadores 102 cliente y los ordenadores 106 servidores agrupados pueden comunicarse entre sí usando el protocolo de transferencia de hipertexto (HTTP), en el que las páginas web se alojan por los ordenadores servidores y se escriben en un lenguaje de marcado, como el lenguaje de marcado de hipertexto (HTML) o el lenguaje de marcado extensible (XML).

En las exposiciones en el presente documento, las realizaciones de la invención se describen principalmente haciendo referencia a la implementación en una instalación de co-localización (tal como la instalación 104). La invención, sin embargo, no se limita a tales implementaciones y puede usarse para la gestión distribuida en cualquiera de una amplia variedad de situaciones. Por ejemplo, en situaciones donde todos los servidores de una instalación son propiedad o están alquilados a un mismo cliente, en situaciones donde se gestiona un único dispositivo informático (por ejemplo, un servidor o un cliente), en situaciones donde se gestionan ordenadores (ya sean servidores u otros) en un entorno de negocio o doméstico, etc.

En la exposición en el presente documento, las realizaciones de la invención se describen en el contexto general de instrucciones ejecutables por ordenador, tales como módulos de programa, que se ejecutan mediante uno o más

ordenadores personales convencionales. En general, los módulos de programa incluyen rutinas, programas, objetos, componentes, estructuras de datos, etc., que realizan tareas específicas o implementan tipos de datos abstractos específicos. Por otra parte, los expertos en la materia apreciarán que diversas realizaciones de la invención pueden ponerse en práctica con otras configuraciones de sistemas informáticos, incluyendo dispositivos de mano, consolas de juegos, aparatos de Internet, sistemas de multiprocesador, electrónica de consumo programable o basada en microprocesadores, unos PC de red, miniordenadores, ordenadores de sistema central, y similares. En un entorno de ordenadores distribuidos, los módulos de programa pueden estar localizados tanto en dispositivos de almacenamiento de memoria local como remota.

Como alternativa, las realizaciones de la invención pueden implementarse en hardware o una combinación de hardware, software, y/o firmware. Por ejemplo, la totalidad o parte de la invención puede implementarse en uno o más circuitos integrados de aplicación específica (ASIC) o en dispositivos lógicos programables (PLD).

La figura 2 muestra un ejemplo general de un ordenador 142 que puede usarse de acuerdo con ciertas realizaciones de la invención. El ordenador 142 se muestra como un ejemplo de un ordenador que puede realizar las funciones de un ordenador 102 cliente de la figura 1, un ordenador o nodo en una instalación 104 de co-localización de la figura 1 u otra localización (por ejemplo, el nodo 248 de la figura 5 abajo), o una consola de gestión local o remota como se trata en más detalle a continuación.

El ordenador 142 incluye uno o más procesadores o unidades 144 de procesamiento, una memoria 146 de sistema, y un bus 148 que acopla diversos componentes del sistema incluyendo la memoria 146 de sistema a los procesadores 144. El bus 148 representa uno o más de cualquiera de diversos tipos de estructuras de bus, incluyendo un bus de memoria o un controlador de memoria, un bus periférico, un puerto de gráficos acelerado y un procesador o bus local que usa cualquiera de una variedad de arquitecturas de bus. La memoria de sistema incluye una memoria 150 de solo lectura (ROM) y una memoria 152 de acceso aleatorio (RAM). Un sistema 154 básico de entrada/salida (BIOS), que contiene las rutinas básicas que ayudan a transferir información entre elementos dentro del ordenador 142, tal como durante el arranque, se almacena en la ROM 150.

El ordenador 142 incluye además una unidad 156 de disco duro para leer de y escribir en un disco duro, no mostrado, conectada al bus 148 a través de una interfaz 157 de controlador de disco duro (por ejemplo, un SCSI, ATA u otro tipo de interfaz); una unidad 158 de disco magnético para leer de y escribir en un disco 160 magnético extraíble, conectado al bus 148 mediante una interfaz de unidad de disco magnético 161; y una unidad de disco óptico 162 para leer o escribir en un disco 164 óptico extraíble tal como un CD ROM, DVD u otro medio óptico, conectado al bus 148 a través de una interfaz 165 de unidad óptica. Las unidades y sus medios legibles por ordenador asociados proporcionan un almacenamiento no volátil de instrucciones legibles por ordenador, estructuras de datos, módulos de programa y otros datos al ordenador 142. Aunque el entorno a modo de ejemplo descrito en el presente documento emplea un disco duro, un disco 160 magnético extraíble y un disco 164 óptico extraíble, debería apreciarse por los expertos en la materia que otros tipos de medios legibles por ordenador que pueden almacenar datos y que pueden accederse por un ordenador, tales como casetes magnéticos, tarjetas de memoria flash, discos de vídeo digitales, memorias de acceso aleatorio (RAM), memorias de solo lectura (ROM), y similares, también pueden usarse en el entorno operativo a modo de ejemplo.

Un número de módulos de programa puede almacenarse en el disco duro, el disco 160 magnético, el disco 164 óptico, la ROM 150 o la RAM 152, incluyendo un sistema 170 operativo, uno o más programas 172 de aplicación, otros módulos 174 de programa y unos datos 176 de programa. Un usuario puede introducir comandos e información en el ordenador 142 a través de dispositivos de entrada tales como el teclado 178 y un dispositivo 180 de señalización. Otros dispositivos de entrada (no mostrados) pueden incluir un micrófono, una palanca de mando, una almohadilla de juegos, una antena parabólica, un escáner o similares. Estos y otros dispositivos de entrada están conectados a la unidad 144 de procesamiento a través de una interfaz 168 que está acoplada al bus de sistema. Un monitor 184 u otro tipo de dispositivo de visualización también están conectados al bus 148 de sistema a través de una interfaz, tal como un adaptador 186 de vídeo. Además del monitor, los ordenadores personales incluyen normalmente otros dispositivos periféricos de salida (no mostrados) tales como altavoces e impresoras.

El ordenador 142 funciona opcionalmente en un entorno de red usando conexiones lógicas a uno o más ordenadores remotos, tal como un ordenador 188 remoto. El ordenador 188 remoto puede ser otro ordenador personal, un servidor, un encaminador, un PC de red, un dispositivo par u otro nodo de red común, y normalmente incluye muchos o todos los elementos descritos anteriormente en relación con el ordenador 142, aunque solo se ha ilustrado un dispositivo 190 de almacenamiento de memoria en la figura 2. Las conexiones lógicas representadas en la figura 2 incluyen una red 192 de área local (LAN) y una red 194 de área extensa (WAN). Tales entornos de red son comunes en oficinas, redes informáticas de toda la empresa, intranets e Internet. En la realización descrita de la invención, el ordenador 188 remoto ejecuta un programa de navegador Web de Internet (que puede estar opcionalmente integrado en el sistema 170 operativo), tal como el navegador Web “Internet Explorer” fabricado y distribuido por Microsoft Corporation de Redmond, Washington.

Cuando se usa en un entorno de red LAN, el ordenador 142 está conectado a la red 192 local a través de una interfaz o adaptador 196 de red. Cuando se usa en un entorno de red WAN, el ordenador 142 incluye normalmente un módem 198 u otro componente para establecer comunicaciones a través de la red 194 de área extensa, tal como

Internet. El módem 198, que puede ser interno o externo, está conectado al bus de sistema 148 a través de una interfaz (por ejemplo, una interfaz 168 de puerto serie). En un entorno de red, los módulos de programa representados en relación con el ordenador 142 personal, o partes de los mismos, pueden almacenarse en el dispositivo de almacenamiento de memoria remota. Debe apreciarse que las conexiones de red mostradas son a modo de ejemplo y pueden usarse otros medios para establecer un enlace de comunicaciones entre los ordenadores.

En general, los procesadores de datos del ordenador 142 se programan por medio de instrucciones almacenadas en momentos diferentes en los diversos medios de almacenamiento legibles por ordenador del ordenador. Los programas y sistemas operativos se distribuyen normalmente, por ejemplo, en disquetes o CD-ROM. A partir de ahí, se instalan o se cargan en la memoria secundaria de un ordenador. En la ejecución, se cargan al menos parcialmente en la memoria electrónica primaria del ordenador. La invención descrita en el presente documento incluye estos y otros diversos tipos de medios de almacenamiento legibles por ordenador cuando tales medios contienen instrucciones o programas para implementar las etapas descritas a continuación junto con un microprocesador u otro procesador de datos. La invención también incluye el propio ordenador cuando está programado de acuerdo con los procedimientos y técnicas descritas a continuación. Además, pueden programarse ciertos subcomponentes del ordenador para realizar las funciones y etapas descritas a continuación. La invención incluye tales subcomponentes cuando están programados como se ha descrito. Además, la invención descrita en el presente documento incluye unas estructuras de datos, descritas a continuación, cuando se realizan en diversos tipos de medios de memoria.

Para fines de ilustración, los programas y otros componentes de programa ejecutables, tales como el sistema operativo, se ilustran en el presente documento como bloques discretos, aunque se reconoce que tales programas y componentes residen en diversos momentos en diferentes componentes de almacenamiento del ordenador, y se ejecutan por el procesador(es) de datos del ordenador.

La figura 3 es un diagrama de bloques que ilustra una instalación de co-localización a modo de ejemplo con más detalle. La instalación 104 de co-localización se ilustra incluyendo múltiples nodos 210 (también denominados como ordenadores servidores). La instalación 104 de co-localización puede incluir cualquier número de nodos 210 y puede incluir fácilmente una cantidad de nodos numerados en miles.

Los nodos 210 se agrupan en grupos, denominados como grupos de servidores (o grupos de nodos). Para facilitar la explicación y evitar el desorden de los dibujos, solo se ilustra un único grupo 212 en la figura 3. Cada grupo de servidores incluye unos nodos 210 que corresponden a un cliente específico de la instalación 104 de co-localización. Los nodos 210 de un grupo de servidores están físicamente aislados de los nodos 210 de otros grupos de servidores. Este aislamiento físico puede adoptar diferentes formas, tal como jaulas bloqueadas separadas o habitaciones separadas en la instalación 104 de co-localización. El aislamiento físico de los grupos de servidores garantiza a los clientes de la instalación 104 de co-localización que solo ellos pueden acceder físicamente a sus nodos (otros clientes no pueden). Como alternativa, los grupos de servidores pueden aislarse lógicamente, pero no físicamente, unos de otros (por ejemplo, usando límites de grupo como se trata en más detalle a continuación).

Una relación de arrendador/inquilino (también denominada como una relación de arrendatario/arrendador) puede establecerse también basándose en los nodos 210. El propietario (y/o el operador) de la instalación 104 de co-localización posee (o de otro modo tiene derechos) los nodos 210 individuales y, por lo tanto, puede verse como un “arrendador”. Los clientes de la instalación 104 de co-localización alquilan los nodos 210 del arrendador, y por lo tanto pueden verse como un “inquilino”. El arrendador normalmente no se ocupa de qué tipos de datos o programas están almacenándose en los nodos 210 por el inquilino, pero impone límites sobre los grupos que evitan que los nodos 210 de diferentes grupos se comuniquen entre sí, como se trata en más detalle a continuación.

La relación de arrendador/inquilino se trata en el presente documento principalmente haciendo referencia a solo dos niveles: el arrendador y el inquilino. Sin embargo, en realizaciones alternativas esta relación puede expandirse a cualquier número de niveles. Por ejemplo, el arrendador puede compartir sus responsabilidades de gestión con uno o más sub-arrendadores (cada uno de los cuales tendría cierto control gerencial sobre uno o más nodos 210) y el inquilino puede compartir de manera similar sus responsabilidades de gestión con uno o más sub-inquilinos (cada uno de los cuales tendría cierto control gerencial sobre uno o más nodos 210).

Aunque aislados físicamente, los nodos 210 de diferentes grupos están a menudo acoplados físicamente al mismo medio 211 de transporte (o medios) lo que permite el acceso a la conexión(es) 216 de red, y posiblemente a la consola 242 de gestión de operaciones de aplicación, tratada con más detalle a continuación. Este medio de transporte puede ser por cable o inalámbrico.

Como cada nodo 210 puede estar acoplado a un medio 211 de transporte compartido, cada nodo 210 puede configurarse para restringir a qué otros nodos 210 pueden enviarse o recibirse datos. Dado que pueden incluirse un número de diferentes nodos 210 en el grupo de servidores de un inquilino, el inquilino puede querer poder pasar datos entre los diferentes nodos 210 dentro del grupo para su procesamiento, almacenamiento, etc. Sin embargo, el inquilino normalmente no quiere pasar datos a otros nodos 210 que no están en el grupo de servidores. Configurar cada nodo 210 en el grupo para restringir que otros nodos 210 puedan enviarse a o recibir datos permite que se

establezca y se aplique un límite al grupo de servidores. El establecimiento y la aplicación de estos límites de grupo de servidores evitan que los datos de los inquilinos se reenvíen erróneamente o incorrectamente a un nodo que no forma parte del grupo.

Estos límites iniciales establecidos por el arrendador evitan la comunicación entre los nodos 210 de los diferentes inquilinos, garantizando de este modo que los datos de cada inquilino puedan pasarse a otros nodos 210 de ese inquilino. El propio inquilino puede definir también más sub-límites dentro de su grupo, estableciendo sub-grupos de nodos 210 que no pueden comunicar datos fuera de (o dentro de), ya sea hacia o desde otros nodos en el grupo. El inquilino es capaz de añadir, modificar, eliminar, etc. tales límites de sub-grupo a voluntad, pero solo dentro de los límites definidos por el arrendador (es decir, los límites de grupo). Por lo tanto, el inquilino no es capaz de alterar los límites en un navegador lo que permitiría la comunicación hacia o desde un nodo 210 para extenderse a otro nodo 210 que no está dentro del mismo grupo.

La instalación 104 de co-localización suministra energía 214 fiable y conexión(es) 216 de red fiable a cada uno de los nodos 210. La energía 214 y la conexión(es) 216 de red se comparten por todos los nodos 210, aunque como alternativa pueden suministrarse energía 214 y conexión(es) 216 de red independientes a los nodos 210 o a las agrupaciones (por ejemplo, grupos) de nodos. Puede usarse cualquiera de una amplia variedad de mecanismos convencionales para suministrar energía fiable para suministrar la energía fiable 214, tal como la energía recibida desde una compañía de servicios públicos junto con generadores de respaldo en caso de fallos de energía, generadores redundantes, baterías, pilas de combustible u otros mecanismos de almacenamiento de energía, etc. De manera similar, puede usarse cualquiera de una amplia variedad de mecanismos convencionales para suministrar una conexión de red fiable para suministrar la conexión(es) 216 de red, tal como medios de transporte de conexión redundantes, diferentes tipos de medios de conexión, diferentes puntos de acceso (por ejemplo, diferentes puntos de acceso a Internet, diferentes proveedores de servicios de Internet (ISP), etc.).

En ciertas realizaciones, los nodos 210 se alquilan o se venden a los clientes por el operador o propietario de la instalación 104 de co-localización junto con el espacio (por ejemplo, jaulas bloqueadas) y el servicio (por ejemplo, el acceso a energía fiable 214 y a una conexión(es) 216 de red) en la instalación 104. En otras realizaciones, el espacio y el servicio en la instalación 104 pueden alquilarse a los clientes mientras que uno o más nodos se suministran por el cliente.

La gestión de cada nodo 210 se realiza de una manera de múltiples niveles. La figura 4 es un diagrama de bloques que ilustra una arquitectura de gestión de múltiples niveles a modo de ejemplo. La arquitectura de múltiples niveles incluye tres niveles: un nivel 230 de gestión de operaciones de grupo, un nivel 232 de gestión de operaciones de aplicación y un nivel 234 de desarrollo de aplicación. El nivel 230 de gestión de operaciones de grupo se implementa localmente en la misma localización que el servidor(es) que se está gestionando (por ejemplo, en una instalación de co-localización) e implica gestionar las operaciones de hardware del servidor(es). En el ejemplo ilustrado, el nivel 230 de gestión de operaciones de grupo no tiene que ver con los componentes de software que se están ejecutando en los nodos 210, solo con la continuación de la operación de hardware de los nodos 210 y el establecimiento de límites entre los grupos de nodos.

El nivel 232 de gestión de operaciones de aplicación, por el contrario, se implementa en una localización remota distinta de la que se encuentra el servidor(es) que se está manejando (por ejemplo, otra distinta de la instalación de co-localización), pero desde un ordenador cliente que está acoplándose de manera comunicativa al servidor(es). El nivel 232 de gestión de operaciones de aplicación implica la gestión de las operaciones del software del servidor(es) y la definición de sub-límites dentro de los grupos de servidores. El cliente puede acoplarse a los servidores de cualquiera de una variedad de formas, tales como a través de Internet o a través de una conexión dedicada (por ejemplo, una conexión telefónica). El cliente puede estar acoplado continuamente con el servidor(es), o como alternativa de manera esporádica (por ejemplo, solo cuando sea necesario para fines de gestión).

El nivel 234 de desarrollo de aplicación se implementa en otro ordenador cliente en una localización distinta a la del servidor(es) (es decir, otra distinta de la instalación de co-localización) e implica el desarrollo de componentes o motores de software para su ejecución en el servidor(es). Como alternativa, el software actual en un nodo 210 en la instalación 104 de co-localización podría accederse por un cliente remoto para desarrollar componentes o motores de software adicionales para el nodo. Aunque el cliente en el que se implementa el nivel 234 de desarrollo de aplicación es normalmente un cliente diferente al que se implementa el nivel 232 de gestión de operaciones de aplicación, los niveles 232 y 234 podrían implementarse (al menos en parte) en el mismo cliente.

Aunque solo se ilustran tres niveles en la figura 4, como alternativa la arquitectura de múltiples niveles podría incluir diferentes números de niveles. Por ejemplo, el nivel de gestión de operaciones de aplicación puede separarse en dos niveles, teniendo cada uno diferentes (o solapadas) responsabilidades, dando como resultado una arquitectura de 4 niveles. La gestión en estos niveles puede producirse desde el mismo lugar (por ejemplo, puede compartirse una única consola de gestión de operaciones de aplicación), o como alternativa desde diferentes lugares (por ejemplo, dos consolas de gestión de operaciones diferentes).

Volviendo a la figura 3, la instalación 104 de co-localización incluye una consola de gestión de operaciones de grupo para cada grupo de servidores. En el ejemplo de la figura 3, la consola 240 de gestión de operaciones de grupo

corresponde al grupo 212. La consola 240 de gestión de operaciones de grupo implementa el nivel 230 de gestión de operaciones de grupo (figura 4) para el grupo 212 y es responsable de la gestión de las operaciones de hardware de los nodos 210 agrupados 212. La consola 240 de gestión de operaciones de grupo monitoriza el hardware en el grupo 212 e intenta identificar los fallos de hardware. Cualquiera de una amplia variedad de fallos de hardware puede monitorizarse tales como los fallos de procesadores, los fallos del bus, los fallos de memoria, etc. Las operaciones de hardware pueden monitorizarse de cualquiera de una variedad de maneras, tales como enviando la consola 240 de gestión de operaciones de grupo mensajes de prueba o señales de control a los nodos 210 que requieren el uso de hardware específico con el fin de responder (sin respuesta o una respuesta incorrecta indica un fallo), que tienen mensajes o señales de control que requieren el uso de hardware específico para generar periódicamente el envío por los nodos 210 a la consola 240 de gestión de operaciones de grupo (no recibir un mensaje o una señal de control dentro de un período de tiempo especificado indica un fallo), etc. Como alternativa, la consola 240 de gestión de operaciones de grupo puede no hacer ningún intento de identificar qué tipo de fallo de hardware se ha producido, sino simplemente que se ha producido un fallo.

Una vez que se detecta un fallo de hardware, la consola 240 de gestión de operaciones de grupo actúa para corregir el fallo. La acción tomada por la consola 240 de gestión de operaciones de grupo puede variar en función del hardware, así como del tipo de fallo, y puede variar para los diferentes grupos de servidores. La acción correctiva puede ser la notificación a un administrador (por ejemplo, una luz intermitente, una alarma de audio, un mensaje de correo, llamar a un teléfono móvil o a un buscapersonas, etc.), o un intento de corregir físicamente el problema físico (por ejemplo, reiniciar el nodo, activar otro nodo de respaldo para tomar su lugar, etc.).

La consola 240 de gestión de operaciones de grupo también establece límites de grupo dentro de la instalación 104 de co-localización. Los límites de grupo establecidos por la consola 240 evitan que los nodos 210 en un grupo (por ejemplo, el grupo 212) se comuniquen con los nodos en otro grupo (por ejemplo, cualquier nodo no en el grupo 212), mientras que al mismo tiempo no se interfiere con la capacidad de los nodos 210 dentro de un grupo para comunicarse con otros nodos dentro de ese grupo. Estos límites proporcionan seguridad a los datos de los inquilinos, lo que les permite saber que sus datos no pueden comunicarse con otros nodos 210 de los inquilinos en la instalación 104 a pesar de que la conexión 216 de red puede compartirse por los inquilinos.

En el ejemplo ilustrado, cada grupo o instalación 104 de co-localización incluye una consola de gestión de operaciones de grupo dedicada. Como alternativa, una sola consola de gestión de operaciones de grupo puede corresponder a, y gestionar las operaciones de hardware de servidor de, diversos grupos. De acuerdo con otra alternativa, múltiples consolas de gestión de operaciones de grupo pueden corresponder a, y gestionar las operaciones de hardware de, un único grupo de servidores. Tales múltiples consolas pueden gestionar un único grupo de servidores de una manera compartida, o una consola pueden funcionar como respaldo para otra consola (por ejemplo, proporcionando una mayor fiabilidad a través de la redundancia, para permitir el mantenimiento, etc.).

Una consola 242 de gestión de operaciones de aplicación también está acoplada comunicativamente a la instalación 104 de co-localización. Una consola 242 de gestión de operaciones de aplicación se localiza en una localización remota de la instalación 104 de co-localización (es decir, no está dentro de la instalación 104 de co-localización), normalmente se localiza en las oficinas del cliente. Una consola 242 de gestión de operaciones de aplicación diferente corresponde a cada grupo de servidores de instalación 104 de co-localización, aunque como alternativa varias consolas 242 pueden corresponder a un único grupo de servidores, o una única consola 242 puede corresponder a múltiples grupos de servidores. La consola 242 de gestión de operaciones de aplicación implementa un nivel 232 de gestión de operaciones de aplicación (figura 4) para el grupo 212 y es responsable de la gestión de las operaciones del software de los nodos 210 en el grupo 212, así como de garantizar los sub-límites dentro de grupo 212.

La consola 242 de gestión de operaciones de aplicación monitoriza el software en el grupo 212 e intenta identificar fallos de software. Cualquiera de una amplia variedad de fallos de software puede monitorizarse para, tal como los procesos o subprocesos de aplicación que se “cuelgan” o de otra manera no responden, un error en la ejecución de procesos o subprocesos de aplicación, etc. Las operaciones del software puede monitorizarse de cualquiera de una variedad de maneras (similar a la monitorización de las operaciones de hardware tratadas anteriormente), tal como la consola 242 de gestión de operaciones de aplicación que envía mensajes de prueba o señales de control a procesos o subprocesos específicos que se ejecutan en los nodos 210 que requieren el uso de rutinas específicas con el fin de responder (sin respuesta o una respuesta incorrecta indica un fallo), teniendo mensajes o señales de control que requieren el uso de rutinas de software específicas para generar periódicamente el envío mediante procesos o subprocesos que se ejecutan en los nodos 210 a la consola 242 de gestión de operaciones de aplicación (no recibir un mensaje de este tipo o una señal de control dentro de un período de tiempo especificado indica un fallo), etc. Como alternativa, la consola 242 de gestión de operaciones de aplicación puede no hacer ningún intento de identificar qué tipo de fallo de software se ha producido, sino simplemente que se ha producido un fallo.

Una vez que se detecta un fallo de software, la consola 242 de gestión de operaciones de aplicación actúa para corregir el fallo. La acción tomada por la consola 242 de gestión de operaciones de aplicación puede variar en función del hardware, así como del tipo de fallo, y puede variar para los diferentes grupos de servidores. La acción correctiva puede ser una notificación de un administrador (por ejemplo, una luz intermitente, una alarma de audio, un mensaje de correo electrónico, llamar a un teléfono móvil o a un buscapersonas, etc.), o un intento de corregir el

problema (por ejemplo, reiniciar el nodo, volver a cargar el componente de software o una imagen del motor, interrumpir y volver a ejecutar el proceso, etc.).

Por lo tanto, la gestión de un nodo 210 se distribuye a través de múltiples gestores, sin importar el número de otros nodos (si los hay) localizados en la misma localización que el nodo 210. La gestión de múltiples niveles permite que la gestión de operaciones de hardware se separe de la gestión de operaciones de aplicación, lo que permite dos consolas diferentes (cada una bajo el control de una entidad diferente) para compartir la responsabilidad de gestión para el nodo.

La arquitectura de gestión de múltiples niveles puede usarse también en otras situaciones para gestionar uno o más ordenadores desde una o más localizaciones remotas, incluso si los ordenadores no son parte de una instalación de co-localización. A modo de ejemplo, una pequeña empresa puede comprar sus propios ordenadores, sin embargo, contratar a otra empresa para gestionar las operaciones de hardware de los ordenadores, y posiblemente a otra empresa para gestionar las operaciones del software de los ordenadores.

En este ejemplo, la pequeña empresa (el propietario de los ordenadores) es un primer nivel de gestión. A continuación, el propietario arrienda los ordenadores al operador de hardware subcontratado, que es el segundo nivel de gestión. El operador de hardware puede gestionar la operación de hardware desde una consola de control, o localizada a nivel local en la pequeña empresa, junto con los ordenadores que se gestionan, o como alternativa en algún lugar remoto, de manera análoga a la consola 240 de gestión de operaciones de grupo. A continuación, el operador de hardware arrienda los ordenadores a un operador de hardware subcontratado, que es el tercer nivel de gestión. El operador de software puede gestionar la operación del software desde una consola de control, o localizada a nivel local en la pequeña empresa, junto con los ordenadores que se gestionan, o como alternativa en algún lugar remoto, de manera análoga a la consola 242 de gestión de operaciones de aplicación. A continuación, el operador de software arrienda los ordenadores de nuevo a su propietario, por lo que el propietario se convierte en el "usuario" de los ordenadores, que es el cuarto nivel de gestión. Durante el funcionamiento normal, el propietario del ordenador ocupa este cuarto nivel de gestión. Sin embargo, el propietario del ordenador puede ejercer sus derechos de primer nivel de gestión para romper uno o ambos de los arrendamientos al operador de software y al operador de hardware, tal como cuando el propietario del ordenador desea cambiar los operadores de software o hardware.

La figura 5 es un diagrama de bloques que ilustra un nodo a modo de ejemplo en más detalle de acuerdo con ciertas realizaciones de la invención. El nodo 248 es un nodo a modo de ejemplo gestionado por otros dispositivos (por ejemplo, las consolas 240 y 242 de la figura 3) externos al nodo. El nodo 248 puede ser un nodo 210 de la figura 3, o, como alternativa, un nodo en otro lugar (por ejemplo, un ordenador en un entorno empresarial o doméstico). El nodo 248 incluye un monitor 250, denominado como el "BMonitor", y una pluralidad de componentes o motores 252 de software, y está acoplado a (o como alternativa incorpora) un dispositivo 262 de almacenamiento masivo. En el ejemplo ilustrado, el nodo 248 es un ordenador servidor que tiene un procesador(es) que soporta múltiples niveles de privilegio (por ejemplo, unos anillos en un procesador de arquitectura x86). En el ejemplo ilustrado, estos niveles de privilegios se conocen como anillos, aunque las implementaciones alternativas que usan diferentes arquitecturas de procesador pueden usar una nomenclatura diferente. Los múltiples anillos proporcionan un conjunto de niveles de prioridad que el software puede ejecutar, a menudo incluyendo 4 niveles (anillos 0, 1, 2, y 3). El anillo 0 se denomina normalmente como el anillo más privilegiado. Los procesos de software que se ejecutan en el anillo 0 normalmente puede acceder a más funciones (por ejemplo, instrucciones) que los procedimientos que se ejecutan en los anillos menos privilegiados. Además, un procesador que ejecuta en un anillo específico no puede alterar el código o los datos en un anillo de prioridad más alta. En el ejemplo ilustrado, BMonitor 250 se ejecuta en el anillo 0, mientras que los motores 252 se ejecutan en el anillo 1 (o como alternativa en los anillos 2 y/o 3). Por lo tanto, el código o los datos de BMonitor 250 (que se ejecutan en anillo 0) no pueden alterarse directamente por los motores 252 (que se ejecutan en el anillo 1). Más bien, cualquiera de tales alteraciones tendría que hacerse por un motor 252 que solicita al BMonitor 250 hacer la alteración (por ejemplo, enviando un mensaje a BMonitor 250, invocando una función de BMonitor 250, etc.). La implementación de BMonitor 250 en el anillo 0 protege a BMonitor 250 de un motor 252 no autorizado o malicioso que trata de eludir las restricciones impuestas por BMonitor 250.

BMonitor 250 es el módulo de control fundamental del nodo 248, controla (y opcionalmente incluye) tanto la tarjeta de interfaz de red como el gestor de memoria. Controlando la tarjeta de interfaz de red (que puede separarse de BMonitor 250, o como alternativa BMonitor 250 puede incorporarse en la tarjeta de interfaz de red), BMonitor 250 puede controlar los datos recibidos por y enviados por el nodo 248. Controlando el gestor de memoria, BMonitor 250 controla la asignación de memoria a los motores 252 que se ejecutan en el nodo 248 y por lo tanto puede ayudar a evitar la interferencia de motores no autorizados o maliciosos con el funcionamiento de BMonitor 250.

Aunque diversos aspectos del nodo 248 pueden estar bajo el control de BMonitor 250 (por ejemplo, la tarjeta de interfaz de red), BMonitor 250 todavía hace que al menos parte de dicha funcionalidad esté disponible para los motores 252 que se ejecutan en el nodo 248. BMonitor 250 proporciona una interfaz (por ejemplo, a través del controlador 254 tratado en más detalle a continuación) a través de la cual los motores 252 pueden solicitar acceso a una funcionalidad, tal como enviar datos a otro nodo 248 o a Internet. Estas solicitudes pueden tomar cualquiera de una variedad de formas, tal como enviar mensajes, llamar a una función, etc.

BMonitor 250 incluye un controlador 254, una interfaz 256 de red, uno o más filtros 258, y un módulo 260 de

protocolo de configuración dinámica de host (DHCP). La interfaz 256 de red proporciona la interfaz entre el nodo 248 y la red (por ejemplo, las conexiones 126 de red de la figura 3) a través del medio 211 de transporte interno de la instalación 104 de co-localización. Los filtros 258 identifican otros nodos 248 (y/u otras fuentes u destinos (por ejemplo, acoplados a la Internet 108 de la figura 1) cuyos datos pueden (o, como alternativa, no pueden) enviarse a y/o recibirse. Los nodos u otras fuentes/destinos pueden identificarse de cualquiera de una amplia variedad de formas, tales como por una dirección de red (por ejemplo, una dirección del protocolo de Internet (IP)), algún otro identificador único global, un identificador único local (por ejemplo, un esquema de numeración propietario o local para la instalación 104 de co-localización), etc.

Los filtros 258 pueden restringir totalmente el acceso a un nodo (por ejemplo, no pueden recibirse datos desde o enviarse al nodo), o restringir parcialmente el acceso a un nodo. La restricción de acceso parcial puede tomar diferentes formas. Por ejemplo, un nodo puede estar restringido de tal manera que los datos pueden recibirse desde el nodo, pero no enviarse al nodo (o viceversa). A modo de otro ejemplo, un nodo puede estar restringido de tal manera que solo ciertos tipos de datos (por ejemplo, las comunicaciones de acuerdo con ciertos protocolos, tal como HTTP) puedan recibirse desde y/o enviarse al nodo. El filtrado basándose en unos tipos específicos de datos puede implementarse de diferentes maneras, tal como mediante la comunicación de datos en paquetes con una información de cabecera que indica el tipo de datos incluidos en el paquete.

Unos filtros 258 pueden añadirse por la consola 242 de gestión de operaciones de aplicación o por la consola 240 de gestión de operaciones de grupo. En el ejemplo ilustrado, los filtros añadidos por la consola 240 de gestión de operaciones de grupo (para establecer límites de grupo) restringen el acceso completo a los nodos (por ejemplo, cualquier acceso a otro nodo puede evitarse) mientras que los filtros añadidos por la consola 242 de gestión de operaciones de aplicación (para establecer unos sub-límites dentro de un grupo) pueden restringir o el acceso completo o el acceso parcial a los nodos.

El controlador 254 también impone algunas restricciones en lo que los filtros pueden añadirse a los filtros 258. En el ejemplo ilustrado, el controlador 254 permite que la consola 240 de gestión de operaciones de grupo añada cualquier filtro que se desee (que definirán los límites del grupo). Sin embargo, el controlador 254 restringe a la consola 242 de gestión de operaciones de aplicación para añadir solo filtros que son al menos tan restrictivos como los añadidos por la consola 240. Si la consola 242 intenta añadir un filtro que sea menos restrictivo que los añadidos por la consola 240 (en cuyo caso el sub-límite puede extenderse más allá de los límites de grupo), el controlador 254 se niega a agregar el filtro (o como alternativa puede modificar el filtro de tal manera que no sea menos restrictivo). Al imponer una restricción de este tipo, el controlador 254 puede garantizar que los sub-límites establecidos en el nivel de gestión de operaciones de aplicación no se extienden más allá de los límites de grupo establecidos en el nivel de gestión de operaciones de grupo.

El controlador 254, que usa uno o más filtros 258, funciona para restringir los paquetes de datos enviados desde el nodo 248 y/o recibidos por el nodo 248. Todos los datos destinados a un motor 252, o enviados por un motor 252, a otro nodo, se pasan a través de la interfaz 256 de red y los filtros 258. El controlador 254 aplica los filtros 258 a los datos, comparando el destino de los datos (por ejemplo, normalmente identificados en una parte de la cabecera de un paquete que incluye los datos) a los nodos aceptables (y/o restringidos) (y/o las direcciones de red) identificados en los filtros 258. Si los filtros 258 indican que puede aceptarse el destino de los datos, entonces el controlador 254 permite que los datos pasen a su través hacia el destino (o hacia el nodo 248 o fuera del nodo 248). Sin embargo, si los filtros 258 indican que no puede aceptarse el destino de los datos, entonces el controlador 254 evita que los datos pasen a su través hacia el destino. El controlador 254 puede devolver una indicación a la fuente de los datos de que los datos no pueden pasar hacia el destino o puede simplemente ignorar o descartar los datos.

La aplicación de los filtros 258 a los datos por el controlador 254 permite que se impongan las restricciones de límite de un grupo de servidores. Los filtros 258 pueden programarse (por ejemplo, la consola 242 de gestión de operaciones de aplicación de la figura 3) con las direcciones de nodo de todos los nodos dentro del grupo de servidores (por ejemplo, el grupo 212). A continuación, el controlador 254 evita que los datos recibidos desde cualquier nodo no dentro del grupo de servidores pasen a través de un motor 252, y de manera similar evita que los datos se envíen a un nodo distinto de uno dentro del grupo de servidores desde el que se envía. Del mismo modo, los datos recibidos desde Internet 108 (figura 1) pueden identificar un nodo 210 de destino (por ejemplo, mediante una dirección IP), de tal manera que el controlador 254 de cualquier nodo distinto del nodo de destino evitará que los datos pasen a través de un motor 252.

El módulo 260 de DHCP implementa el protocolo de control de host distribuido, permitiendo que BMonitor 250 (y por tanto el nodo 210) obtenga una dirección IP de un servidor DHCP (por ejemplo, la consola 240 de gestión de operaciones de grupo de la figura 3). Durante un proceso de inicialización para el nodo 210, el módulo 260 de DHCP solicita una dirección IP del servidor DHCP, que a su vez proporciona la dirección IP al módulo 260. Una información adicional acerca de DHCP está disponible en Microsoft Corporation de Redmond, Washington.

Los motores 252 de software incluyen cualquiera de una amplia variedad de componentes de software convencionales. Ejemplos de motores 252 incluyen un sistema operativo (por ejemplo, Windows NT®), un componente de servidor de balanceo de carga (por ejemplo, para balancear la carga de procesamiento de múltiples nodos 248), un componente de servidor de almacenamiento en caché (por ejemplo, para datos y/o instrucciones de

caché de otro nodo 248 o recibidos a través de Internet), un componente gestor de almacenamiento (por ejemplo, para gestionar el almacenamiento de los datos de otro nodo 248 o recibidos a través de Internet), etc. En una implementación, cada uno de los motores 252 es un motor basado en un protocolo, que comunica con BMonitor 250 y otros motores de 252 a través de mensajes y/o llamadas de función sin necesidad de que los motores 252 y BMonitor 250 se escriban usando el mismo lenguaje de programación.

El controlador 254 es responsable además de controlar la ejecución de los motores 252. Este control puede tomar diferentes formas, incluso comenzando la ejecución de un motor 252, terminando la ejecución de un motor 252, recargando una imagen de un motor 252 desde un dispositivo de almacenamiento, depurando la ejecución de un motor 252, etc. El controlador 254 recibe instrucciones desde la consola 242 de gestión de operaciones de aplicación de la figura 3 con respecto a cuál de estas acciones de control tomar y cuándo tomar las mismas. Por lo tanto, el control de los motores 252 se gestiona realmente por la consola 242 de gestión de operaciones de aplicación, no localmente en la instalación 104 de co-localización. El controlador 254 también proporciona una interfaz a través de la que la consola 242 de gestión de operaciones de aplicación puede identificar filtros a añadir (y/o a quitar) del conjunto 258 de filtros.

El controlador 254 incluye también una interfaz a través de la que la consola 240 de gestión de operaciones de grupo de la figura 3 puede comunicar comandos al controlador 254. Diferentes tipos de comandos orientados a la operación de hardware pueden comunicarse al controlador 254 por la consola 240 de gestión de operaciones de grupo, tal como reiniciar el nodo, apagar el nodo, colocar el nodo en un estado de baja energía (por ejemplo, en un estado de suspenso o de espera), cambiar los límites de grupo, cambiar las claves de cifrado, etc.

El controlador 254 proporciona soporte adicional de cifrado para BMonitor 250, permitiendo que los datos se almacenen de manera segura en el dispositivo 262 de almacenamiento masivo (por ejemplo, un disco magnético, un disco óptico, etc.) y se produzcan comunicaciones seguras entre el nodo 248 y una consola de gestión de operaciones (por ejemplo, la consola 240 o 242 de la figura 3). El controlador 254 mantiene múltiples claves de cifrado, incluyendo: una para el arrendador (denominada como la “clave de arrendador”) que accede al nodo 248 desde la consola 240 de gestión de operaciones de grupo, una para el inquilino del nodo 248 (denominada como la “clave de inquilino”) que accede al nodo 248 desde la consola 242 de gestión de operaciones de aplicación y unas claves que BMonitor 250 usa para almacenar datos de manera segura en el dispositivo 262 de almacenamiento masivo (denominadas como las “clave de disco”).

BMonitor 250 hace uso de la criptografía de clave pública para proporcionar comunicaciones seguras entre el nodo 248 y las consolas de gestión (por ejemplo, las consolas 240 y 242), la criptografía de clave pública se basa en un par de claves, incluyendo una clave pública y una clave privada, y un algoritmo de cifrado. El algoritmo de cifrado puede cifrar los datos basándose en la clave pública de tal manera que no puede descifrarse eficazmente sin la clave privada. De este modo, las comunicaciones del titular de la clave pública pueden cifrarse usando la clave pública, permitiendo que solo el titular de clave privada descifre las comunicaciones. Cualquiera de una variedad de técnicas de criptografía de clave pública puede usarse, tal como la técnica de cifrado RSA (Rivest, Shamir y Adelman) bien conocida. Para una introducción básica de la criptografía, se remite al lector a un texto escrito por Bruce Schneier y titulado “Applied Cryptography: Protocols, Algorithms and Source Code in C”, publicado por John Wiley & Sons con copyright de 1994 (o la segunda edición con copyright de 1996).

BMonitor 250 se inicializa para incluir un par de claves pública/privada tanto para el arrendador como para el inquilino. Estos pares de claves pueden generarse por BMonitor 250, o como alternativa por algún otro componente y almacenarse dentro de BMonitor 250 (con ese otro componente que se confía para destruir su conocimiento del par de claves). Tal como se usa en el presente documento, U se refiere a una clave pública y R se refiere a una clave privada. El par 264 de claves pública/privada para el arrendador se denomina como (U_L, R_L), y el par 266 de claves pública/privada para el inquilino se denomina como (U_T, R_T). BMonitor 250 hace que las claves públicas U_L y U_T estén disponibles para el arrendador, pero mantiene las claves privadas R_L y R_T secretas. En el ejemplo ilustrado, BMonitor 250 no divulga nunca las claves privadas R_L y R_T, de manera que tanto el arrendador como el inquilino pueden estar seguros de que no hay ninguna entidad, que no sea el BMonitor 250, que pueda descifrar la información que cifran usando sus claves públicas (por ejemplo, a través de la consola 240 de gestión de operaciones de grupo y la consola 242 de gestión de operaciones de aplicación de la figura 3, respectivamente).

Una vez que el arrendador tiene las claves públicas U_L y U_T, el arrendador puede asignar el nodo 210 a un inquilino específico, dando a ese inquilino la clave pública U_T. El uso de la clave pública U_T permite al inquilino cifrar las comunicaciones para BMonitor 250 que solo BMonitor 250 puede descifrar (usando la clave privada R_T). Aunque no es necesario, una primera etapa prudente para el inquilino es requerir que BMonitor 250 genere un nuevo par de claves pública/privada (U_T, R_T). En respuesta a una solicitud de este tipo, un generador 268 de claves de BMonitor 250 genera un nuevo par de claves pública/privada de cualquiera de una variedad de maneras bien conocidas, almacena el nuevo par de claves como el par 266 de claves, y devuelve la nueva clave pública U_T al inquilino. Generando un nuevo par de claves, el inquilino se asegura de que ninguna otra entidad, incluyendo el arrendador, es consciente de la clave pública de inquilino U_T. Además, el inquilino puede tener también nuevos pares de claves generados en momentos posteriores.

BMonitor 250 impone restricciones a aquellas entidades que pueden solicitar nuevos pares de claves

públicas/privadas. El inquilino es capaz de solicitar nuevos pares de claves públicas/privadas, pero no es capaz de solicitar nuevos pares de claves públicas/privadas de arrendador. El arrendador, sin embargo, puede solicitar nuevos pares de claves públicas/privadas de arrendador, así como nuevos pares de claves públicas/privadas de inquilino. Cada vez que se recibe una solicitud de un nuevo par de claves pública/privada, el controlador 254 verifica la identidad del solicitante como el inquilino o el arrendador (por ejemplo, basándose en un procedimiento remoto de inicio de sesión, verificación de contraseña, manera en la que el solicitante está comunicando con o está acoplado al nodo 248, etc.) antes de generar el nuevo par de claves.

Con el fin de garantizar la seguridad de la comunicación bidireccional entre el BMonitor 250 y los dispositivos de control de arrendador y de inquilino (por ejemplo, las consolas 240 y 242 de gestión de operaciones, respectivamente), los dispositivos de control de arrendador y de inquilino también pueden generar (o de otra manera asignar pares de claves públicas/privadas. En esta situación, las consolas 240 y 242 pueden comunicar sus respectivas claves públicas a los BMonitor 250 de los nodos 248 que deseen (o se espera desear) para comunicarse con seguridad. Una vez que la clave pública de una consola se conoce por un BMonitor 250, el BMonitor 250 puede cifrar las comunicaciones a esa consola usando su clave pública, evitando de este modo que cualquier otro dispositivo, excepto la consola que tiene la clave privada, lea la comunicación.

BMonitor 250 también mantiene una clave 270 de disco, que se genera basándose en una o más claves 272 y 274 simétricas (las claves simétricas se refieren a claves secretas utilizadas en la criptografía de clave secreta). La clave 270 de disco, también una clave simétrica, se usa por BMonitor 250 para almacenar información en los dispositivos 262 de almacenamiento masivo. BMonitor 250 mantiene la clave 270 de disco segura, usándola solamente para cifrar los datos que el nodo 248 almacena en el dispositivo 262 de almacenamiento masivo y descifrar los datos que el nodo 248 recupera desde el dispositivo 262 de almacenamiento masivo (por lo tanto, no hay necesidad de que otras entidades, incluyendo el arrendador y el inquilino, tengan conocimiento de la clave 270 de disco). Como alternativa, el arrendador o el inquilino pueden ser informados de la clave 270 de disco, u otra clave en la que se basa una clave 270 de disco.

El uso de una clave 270 de disco garantiza que los datos almacenados en el dispositivo 262 de almacenamiento masivo solo pueden descifrarse por el nodo 248 que los cifró, y no por cualquier otro nodo o dispositivo. De este modo, por ejemplo, si el dispositivo 262 de almacenamiento masivo se eliminase y se intenta hacer una lectura de los datos en el dispositivo 262, tales intentos no tendrían éxito. BMonitor 250 usa una clave 270 de disco para cifrar los datos que se almacenan en el dispositivo 262 de almacenamiento masivo, independientemente del origen de los datos. Por ejemplo, los datos pueden provenir de un dispositivo cliente (por ejemplo, el cliente 102 de la figura 1) usado por un cliente del inquilino, desde una consola de gestión de operaciones (por ejemplo, la consola 242 de la figura 3), etc.

La clave 270 de disco se genera basándose en las claves 272 y 274 simétricas. Tal como se usa en el presente documento, K se refiere a una clave simétrica, por lo que K_L se refiere a una clave simétrica de arrendador (la clave 272) y K_T se refiere a una clave simétrica de inquilino (la clave 274). Las claves 272 y 274 individuales pueden generarse en cualquiera de una amplia variedad de maneras convencionales (por ejemplo, basándose en un generador de números aleatorios). La clave 270 de disco es o la clave K_L sola, o como alternativa es una combinación de las claves K_L y K_T. En situaciones donde el nodo 210 no está arrendado actualmente a un inquilino, o en las que el inquilino no ha establecido una clave K_T, entonces el controlador 254 mantiene la clave K_L como una clave 270 de disco. Sin embargo, en situaciones donde se alquila el nodo 248 a un inquilino que establece una clave K_T entonces la clave 270 de disco es una combinación de las claves K_L y K_T. Las claves K_L y K_T pueden combinarse de una variedad de diferentes maneras, y en una implementación se combinan usando una de las claves para cifrar la otra clave, siendo la clave cifrada resultante la clave 270 de disco. Por lo tanto, los datos almacenados en el dispositivo 262 de almacenamiento masivo siempre están cifrados, incluso si el inquilino no establece una clave K_T simétrica. Además, en situaciones donde el arrendador y el inquilino son conscientes de sus respectivas claves K_L y K_T, entonces la combinación de las claves resulta en una clave que puede usarse para cifrar los datos de tal manera que ni el arrendador ni el inquilino puedan descifrarla individualmente.

En el ejemplo ilustrado, un nodo 248 no tiene inicialmente las claves K_L y K_T simétricas. Cuando el arrendador inicializa el nodo 248, solicita una nueva clave K_L (por ejemplo, a través de la consola 240 de gestión de operaciones de grupo de la figura 3), en respuesta a lo cual el generador 268 de claves genera una nueva clave y el controlador 254 mantiene la clave recién generada como la clave 272. Del mismo modo, cuando un inquilino arrienda inicialmente un nodo 248 todavía no existe una clave K_T simétrica de inquilino para el nodo 248. El inquilino puede comunicar una solicitud de una nueva clave K_T (por ejemplo, a través de la consola 242 de gestión de operaciones de aplicación de la figura 3), en respuesta a lo cual el generador 268 de claves genera una nueva clave y el controlador 254 mantiene la clave recién generada como la clave 274. Además, cada vez que se genera una nueva clave K_L o K_T, entonces el controlador 254 genera una nueva clave 270 de disco.

Aunque solo se ilustra una clave de arrendador y de inquilino (K_L y K_T) en la figura 5, como alternativa pueden combinarse unas claves simétricas adicionales (por ejemplo, a partir de un sub-inquilino, un sub-arrendador, etc.) para generar la clave 270 de disco. Por ejemplo, si hay tres claves simétricas, entonces pueden combinarse cifrando una primera de las claves con una segunda de las claves, y a continuación cifrar el resultado con la tercera de las claves para generar la clave 270 de disco. Las claves simétricas adicionales pueden usarse, por ejemplo, para un

sub-inquilino(s).

El arrendador también puede solicitar nuevos pares de claves públicas/privadas de BMonitor 250, o pares de claves de inquilino o pares de claves de arrendador. Solicitar nuevos pares de claves puede permitir, por ejemplo, que el arrendador vuelva a asignar un nodo 248 de un inquilino a otro. A modo de ejemplo, si un inquilino ya no desea el nodo 248 (o no hace los pagos de arrendamiento requeridos para el nodo), entonces el arrendador puede comunicarse con BMonitor 250 (por ejemplo, a través de la consola 240 de la figura 3) para cambiar los pares de claves públicas/privadas de inquilino (prohibiendo de este modo que se descifre cualquier comunicación desde el inquilino por el BMonitor 250 debido a que el inquilino no tiene la nueva clave). Además, el arrendador también puede solicitar un nuevo par de claves pública/privada para el arrendador, esto puede hacerse a intervalos específicos o simplemente cada vez que el arrendador desee una nueva clave (por ejemplo, por razones de seguridad).

En una implementación, BMonitor 250 descarta tanto la clave 270 de disco como la clave simétrica K_L de arrendador, y genera una nueva clave K_L (y una nueva clave 270 de disco) cada vez que se genera una nueva clave privada R_L de arrendador. Sustituyendo la clave K_L y la clave 270 de disco (y no manteniendo un registro de las claves antiguas), el arrendador puede garantizar que una vez que cambia su clave, no puede accederse a cualquier dato de inquilino anteriormente almacenado en el nodo 210. Por lo tanto, el arrendador debería tener cuidado de generar un nuevo par de claves pública/privada solo cuando el arrendador quiera evitar que el inquilino acceda a los datos almacenados anteriormente en el nodo 248.

Además, BMonitor 250 también puede sustituir tanto la clave 270 de disco como la clave K_T simétrica de inquilino, con una recién generada clave K_T (y una nueva clave 270 de disco) cada vez que se genera una nueva clave R_T privada de inquilino. Esto permite que el inquilino aumente la seguridad de los datos que se almacenan en el nodo 248 debido a que puede cambiarse la forma en que esos datos se cifran, como se desee. Sin embargo, como BMonitor 250 descarta la clave K_T anterior y la clave 270 de disco, el inquilino debería tener cuidado al solicitar una nueva clave R_T privada de inquilino solo cuando ya no se necesitan los datos anteriormente almacenados en el nodo 210 (por ejemplo, se ha hecho una copia de seguridad en otra parte).

Debería tenerse en cuenta que los diferentes nodos 248 tendrán normalmente diferentes claves (las claves 264, 266, y 270). Como alternativa, pueden hacerse intentos para tener múltiples nodos usando la misma clave (por ejemplo, la clave 270). Sin embargo, en tales situaciones, debería tenerse cuidado para garantizar que cualquier comunicación de las claves (por ejemplo, entre los nodos 248) se hace de una manera segura con el fin de que la seguridad no se vea comprometida. Por ejemplo, pueden usarse unos pares de claves públicas/privadas adicionales por los BMonitor 250 de dos nodos 248 para comunicarse información de manera segura entre sí.

Por lo tanto, puede establecerse un entorno de hardware arrendado que tiene derechos garantizados y forzados. Los arrendadores pueden arrendar nodos a múltiples inquilinos diferentes y establecer límites que eviten que los nodos alquilados por diferentes inquilinos se comuniquen entre sí. Los inquilinos pueden estar seguros de que los nodos que alquilan pueden accederse para su gestión solamente por ellos mismos, no por otros, y que los datos se almacenan en los nodos de manera segura para que nadie más pueda acceder a los mismos (incluso si el inquilino abandona o reduce sus usos de hardware). Además, los arrendadores y los inquilinos están seguros de que el arrendador puede mover el equipo, cambiar qué nodos están asignados a individuos, eliminar hardware (por ejemplo, los dispositivos de almacenamiento masivo), etc., sin comprometer el almacenamiento seguro de los datos de cualquiera de los inquilinos.

La figura 6 es un diagrama de flujo que ilustra un procedimiento a modo de ejemplo para generar y distribuir claves de cifrado de acuerdo con ciertas realizaciones de la invención. Inicialmente, el ordenador (por ejemplo, un nodo 248 de la figura 5) identifica los pares de claves públicas/privadas, tanto para el arrendador como para el inquilino (acción 280). Esta identificación puede acceder a los pares de claves generadas anteriormente, o como alternativa, generar un nuevo par de claves para el propio ordenador. El ordenador mantiene tanto la clave privada de arrendador del par de claves de arrendador como la clave privada de inquilino del par secreto de claves de inquilino, pero reenvía la clave pública de arrendador del par de claves de arrendador y la clave pública de inquilino del par de claves de inquilino al arrendador (acción 282). En el ejemplo ilustrado, el arrendador está representado por la consola 240 de gestión de operaciones de grupo de la figura 3, aunque como alternativa otros dispositivos o entidades podrían representar el arrendador.

A continuación, el arrendador reenvía la clave pública de inquilino al inquilino (acción 284). En el ejemplo ilustrado, el inquilino está representado por la consola 242 de gestión de operaciones de aplicación de la figura 3, aunque como alternativa otros dispositivos o entidades podrían representar al inquilino. A continuación, el inquilino se comunica con el ordenador para generar un nuevo par de claves de inquilino (acción 286). El ordenador mantiene la clave privada de inquilino del nuevo par de claves secretas y reenvía la clave pública de inquilino del nuevo par de claves al inquilino (acción 288). A continuación, el inquilino es capaz de comunicar mensajes seguros (por ejemplo, datos, instrucciones, solicitudes, etc.) al ordenador usando la nueva clave pública de inquilino (acción 290), mientras que el arrendador es capaz de comunicar mensajes seguros al ordenador usando la clave pública de arrendador (acción 292).

La figura 7 es un diagrama de flujo que ilustra un procedimiento a modo de ejemplo para la operación de una consola de gestión de operaciones de grupo de acuerdo con ciertas realizaciones de la invención. El procedimiento de la figura 7 se implementa por una consola de gestión de operaciones de grupo en una instalación de co-localización, y puede realizarse en software.

Inicialmente, la consola de gestión de operaciones de grupo configura los nodos en el grupo de servidores con los límites (si existen) del grupo de servidores (acción 300). Esta configuración se logra mediante la consola de gestión de operaciones de grupo que comunica los filtros a los nodos en el grupo(s) de servidores.

A continuación, se monitorizan continuamente las operaciones de hardware dentro de un grupo de servidores para un fallo de hardware (acciones 302 y 304). Una vez que se detecta un fallo de hardware, se toma una acción correctiva (acción 306) y la monitorización de la operación de hardware continúa. Cualquiera de una amplia variedad de acciones correctivas puede tomarse, como se ha tratado anteriormente. Téngase en cuenta que, basándose en la acción correctiva (o en otros momentos), los nodos pueden reconfigurarse con nuevos límites de grupo (acción 300).

La figura 8 es un diagrama de flujo que ilustra un procedimiento a modo de ejemplo para la operación de una consola de gestión de operaciones de aplicación de acuerdo con ciertas realizaciones de la invención. El procedimiento de la figura 8 se implementa por una consola de gestión de operaciones de aplicación localizada remotamente de la instalación de co-localización, y puede realizarse en software.

Inicialmente, la consola de gestión de operaciones de aplicación configura los nodos en el grupo de servidores con sub-límites (si existen) del grupo de servidores (acción 320). Esta configuración se logra mediante la consola de gestión de operaciones de aplicación comunicando los filtros a los nodos en el grupo de servidores.

A continuación, se monitorizan continuamente las operaciones del software dentro del grupo de servidores hasta que se detecta un fallo de software (acciones 322 y 324). Este fallo de software podría ser un fallo de un motor de software específico (por ejemplo, un motor falla, pero los otros motores están todavía funcionando), o como alternativa, el fallo de todo el nodo (por ejemplo, todo el nodo se cuelga). Una vez que se detecta un fallo de software, se toma una acción correctiva (acción 326) y la monitorización de la operación del software continúa. Cualquiera de una amplia variedad de acciones correctivas puede tomarse, como se ha tratado anteriormente. Téngase en cuenta que, basándose en la acción correctiva (o en cualquier otro momento durante la operación), el ordenador servidor puede reconfigurarse con los nuevos sub-límites (acción 320).

Conclusión

Aunque la descripción anterior usa un lenguaje que es específico para las características estructurales y/o las acciones metodológicas, debe entenderse que la invención definida en las reivindicaciones adjuntas no se limita a las características o acciones específicas descritas. Más bien, las características y las acciones específicas se desvelan como formas a modo de ejemplo de implementar la invención.

REIVINDICACIONES

1. Un procedimiento que comprende:

establecer, en una instalación (104) de co-localización, siendo la instalación (104) de co-localización un complejo que puede alojar múltiples ordenadores servidores, unos límites de grupo entre una pluralidad de grupos de ordenadores localizados en la instalación (104) de co-localización, evitando los límites de grupo que los ordenadores de un grupo de la pluralidad de grupos se comuniquen con ordenadores de otro grupo de la pluralidad de grupos;
monitorizar, en la instalación (104) de co-localización, las operaciones de hardware de la pluralidad de grupos de ordenadores localizados en la instalación (104) de co-localización;
detectar un fallo de hardware en uno de los ordenadores de uno de la pluralidad de grupos; y
realizar una acción, en respuesta a la detección del fallo de hardware, para corregir el fallo de hardware;
estando además el procedimiento **caracterizado por**
monitorizar las operaciones del software de cada grupo de la pluralidad de grupos de ordenadores localizados en la instalación de co-localización desde una localización remota de la instalación (104) de co-localización,
detectar un fallo de software en uno de los ordenadores de uno de la pluralidad de grupos; y
realizar una acción, en respuesta a la detección del fallo de software, para corregir el fallo de software.

2. Un procedimiento de acuerdo con la reivindicación 1, en el que la acción en respuesta a la detección del fallo de hardware comprende notificar el fallo a un administrador de la instalación de co-localización.

3. Un procedimiento de acuerdo con la reivindicación 1, en el que la acción en respuesta a la detección del fallo de hardware comprende restablecer el ordenador que incluye el hardware que ha fallado.

4. Un procedimiento de acuerdo con la reivindicación 1, en el que la operación de hardware incluye una o más de: una operación de dispositivo de almacenamiento masivo, una operación de dispositivo de memoria, una operación de interfaz de red y una operación de procesador.

5. Un procedimiento de acuerdo con la reivindicación 1, que comprende además configurar cada ordenador en el grupo (212) para imponer unos límites que eviten que una pluralidad de otros ordenadores que no son parte del grupo accedan a los uno o más ordenadores del grupo (212).

6. Un procedimiento de acuerdo con la reivindicación 1, en el que la acción en respuesta a la detección del fallo de software comprende notificar el fallo a un administrador y/o restablecer el ordenador que ejecuta el software que ha fallado.

7. Un procedimiento de acuerdo con la reivindicación 1, que comprende, además, configurar uno o más ordenadores del grupo (212) para imponer unos sub-límites que eviten que un primero o más ordenadores dentro del grupo accedan a un segundo o más ordenadores dentro del grupo.

8. Un procedimiento de acuerdo con la reivindicación 1, que comprende, además, gestionar la carga de un componente de software en uno de los ordenadores en el grupo (212).

9. Un procedimiento de acuerdo con la reivindicación 1, en el que el fallo de software comprende uno o más de:

un proceso de aplicación colgado, un subproceso colgado, y un error en la ejecución de un proceso de aplicación.

10. Un procedimiento de acuerdo con la reivindicación 1, en el que monitorizar la operación del software, detectar el fallo de software, y realizar una acción en respuesta a la detección del fallo de software se implementan en un ordenador remoto, y que comprende además usar la criptografía de clave pública para comunicarse de manera segura entre el ordenador remoto y cada ordenador en el grupo de ordenadores.

11. Uno o más medios legibles por ordenador que tienen almacenado en los mismos un programa informático que, cuando lo ejecutan uno o más procesadores, hace que los uno o más procesadores realicen un procedimiento de una de las reivindicaciones 1 a 10.

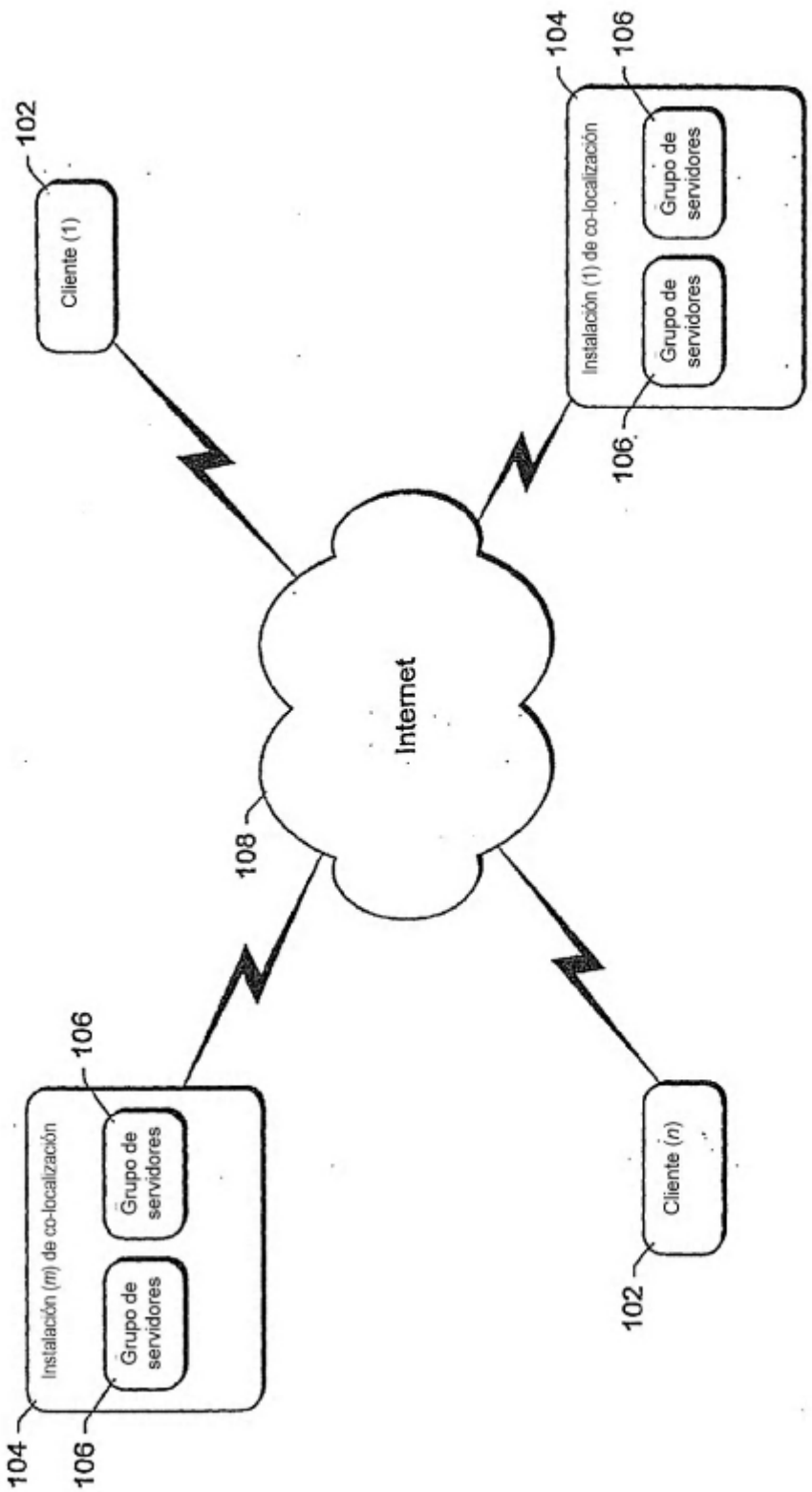
102
Cliente (1)
104
106
Instalación (1) de co-localización
Grupo de servidores
Grupo de servidores
106
104
106
Instalación (m) de co-localización
Grupo de servidores
Grupo de servidores
106
108
Internet
102
Cliente (n)

Fig. 1

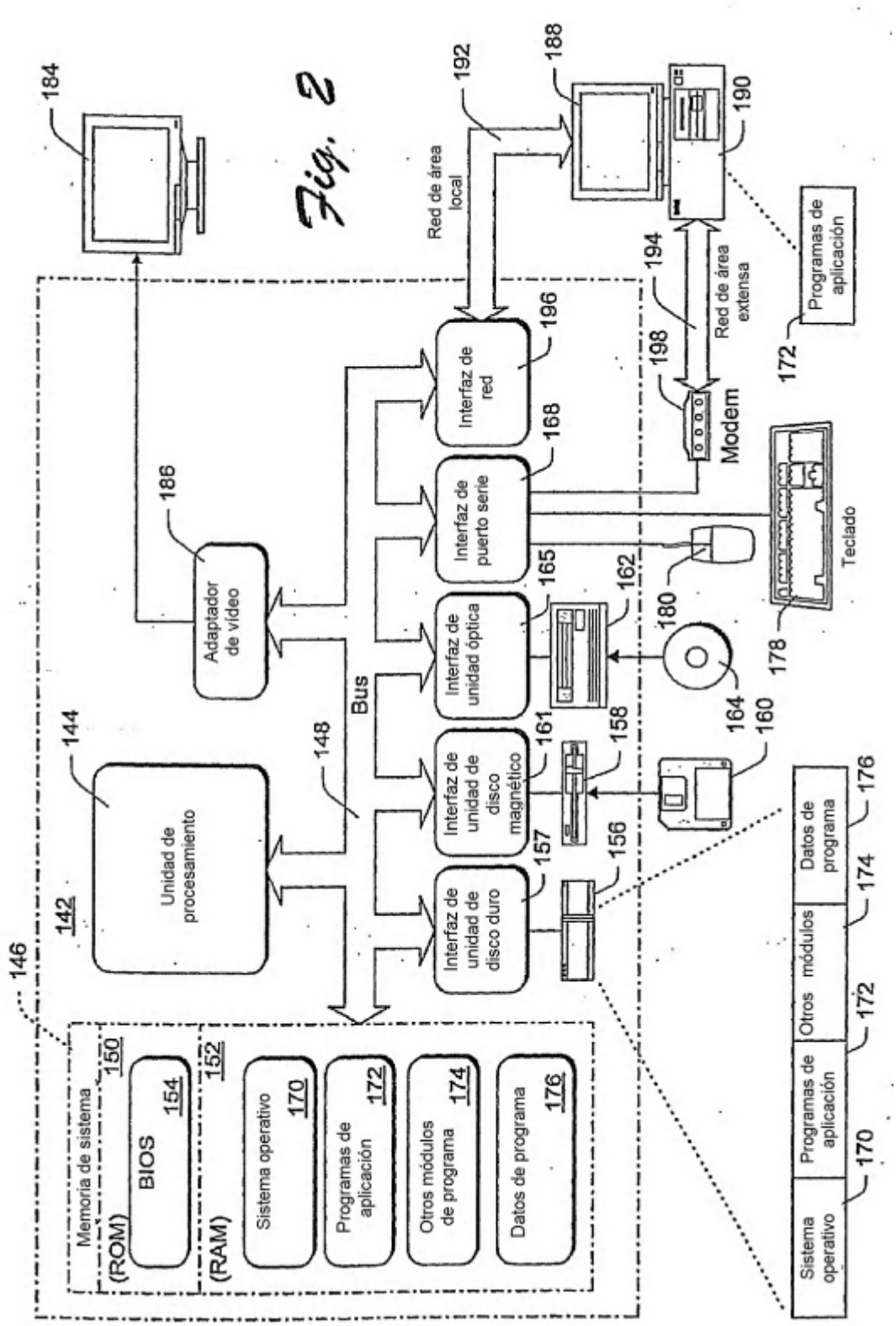
Fig. 2
184
192
188
190
Red de área local
Programas de aplicación
194
Red de área extensa
172
198
Modem
196
Interfaz de red
168
Interfaz de puerto serie
186
Adaptador de vídeo
Teclado
165
162
180
Interfaz de unidad óptica
178
Bus
144
148
Unidad de procesamiento
161
158
164
160
Interfaz de unidad de disco magnético
157
156
Interfaz de unidad de disco duro
176
Datos de programa
174
Otros módulos
172
Programas de aplicación
170
Sistema operativo
146
142
Memoria de sistema
150
(ROM)
BIOS
154
152
(RAM)
Sistema operativo
170
Programas de aplicación
172
Otros módulos de programa
174
Datos de programa
176

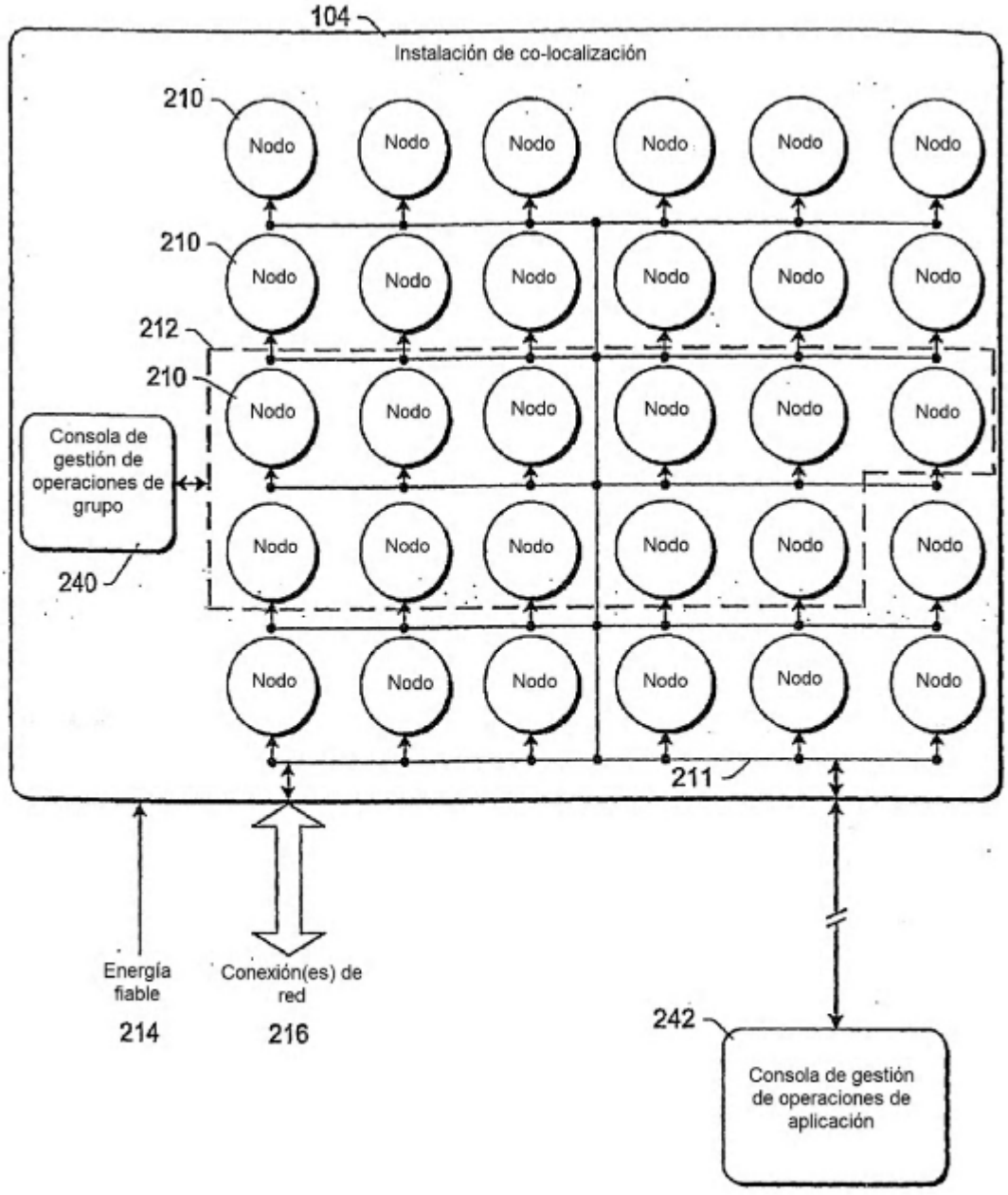
104
Instalación de co-localización
210
Nodo
212
Consola de gestión de operaciones de grupo
240
211
Energía fiable
214
Conexión(es) de red
216
242
Consola de gestión de operaciones de aplicación

Fig. 3

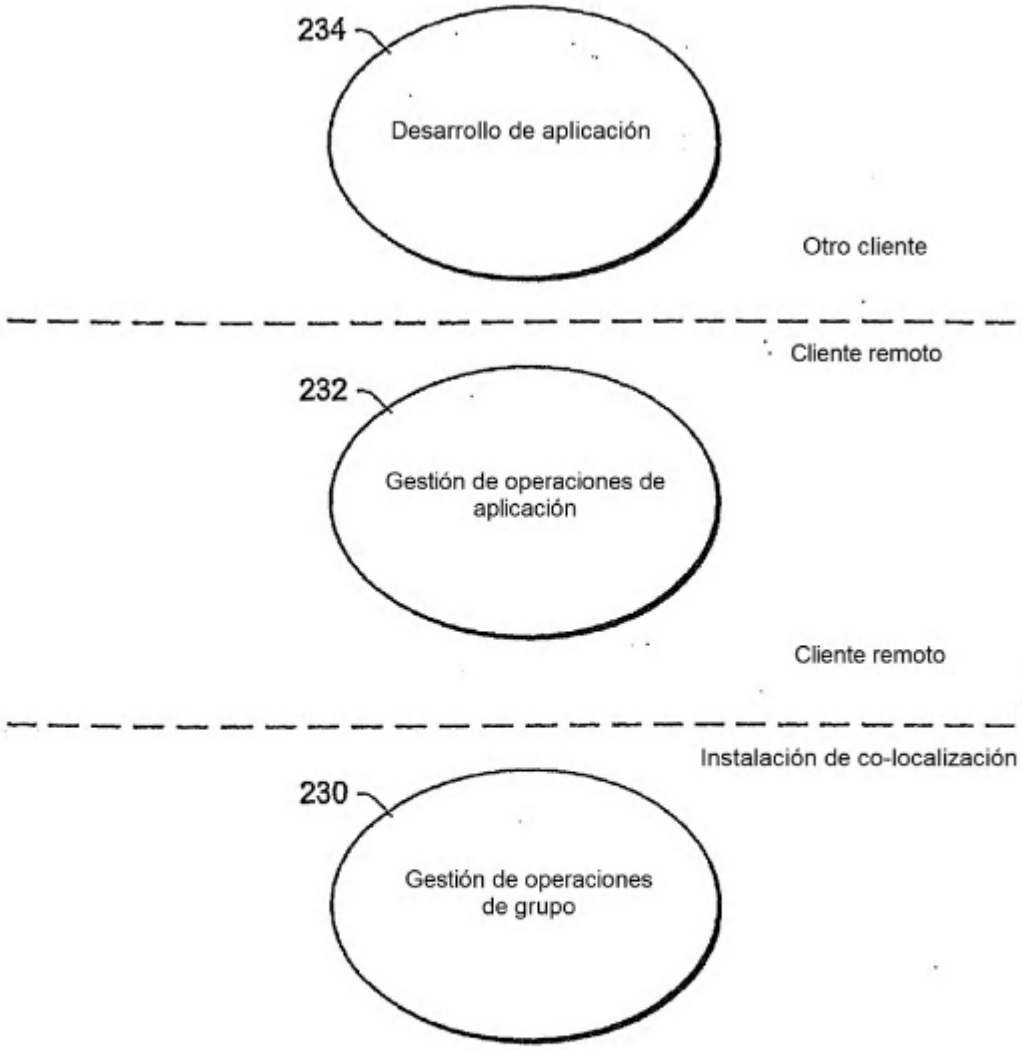
234
Desarrollo de aplicación
Otro cliente
Cliente remoto
232
Gestión de operaciones de aplicación
Cliente remoto
Instalación de co-localización
230
Gestión de operaciones de grupo

Fig. 4

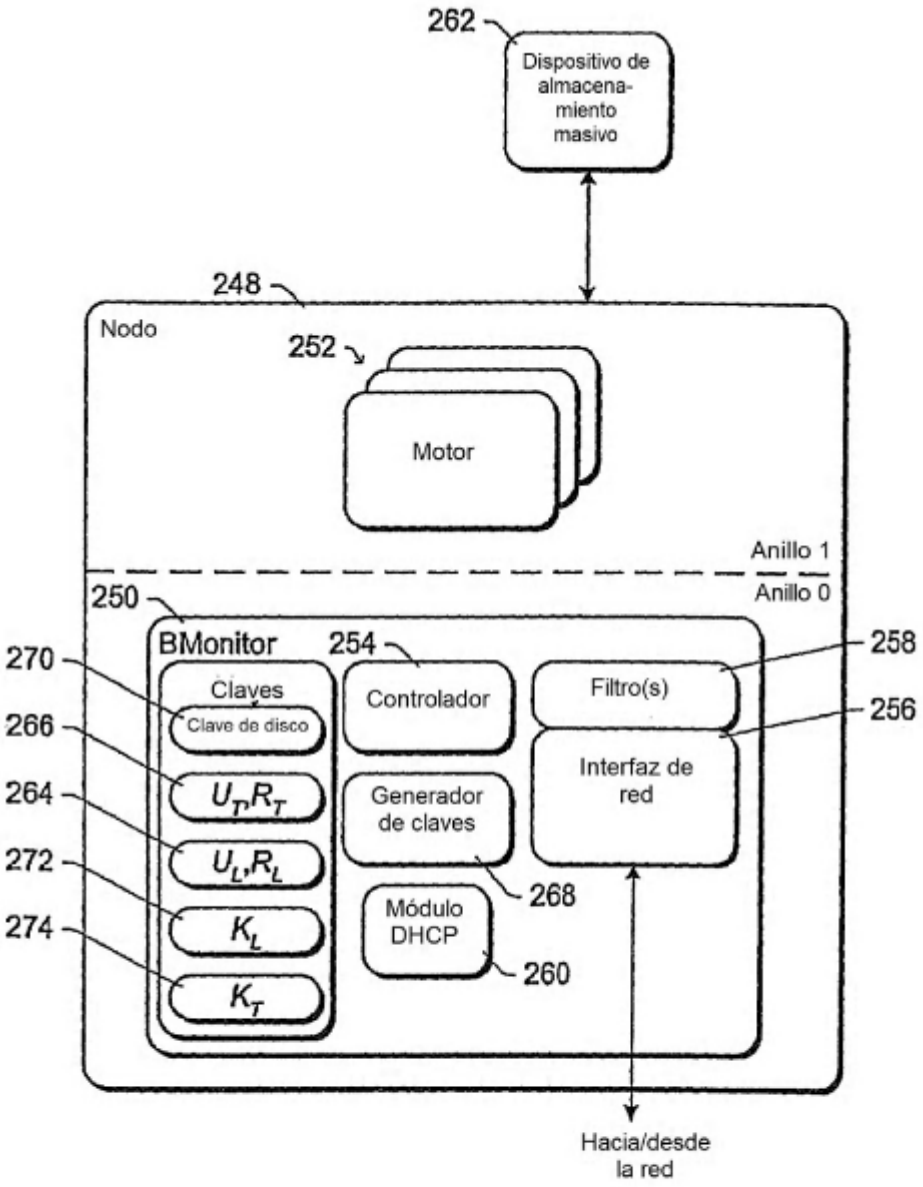
262
Dispositivo de almacena-miento masivo
248
Nodo
252
Motor
Anillo 1
Anillo 0
250
BMonitor
254
Claves
Clave de disco
U_T,R_T
U_L,R_L
K_L
K_T
Controlador
Generador de claves
Módulo DHCP
260
268
Filtro(s)
Interfaz de red
258
256
270
266
264
272
274
Hacia/desde la red

Fig. 5

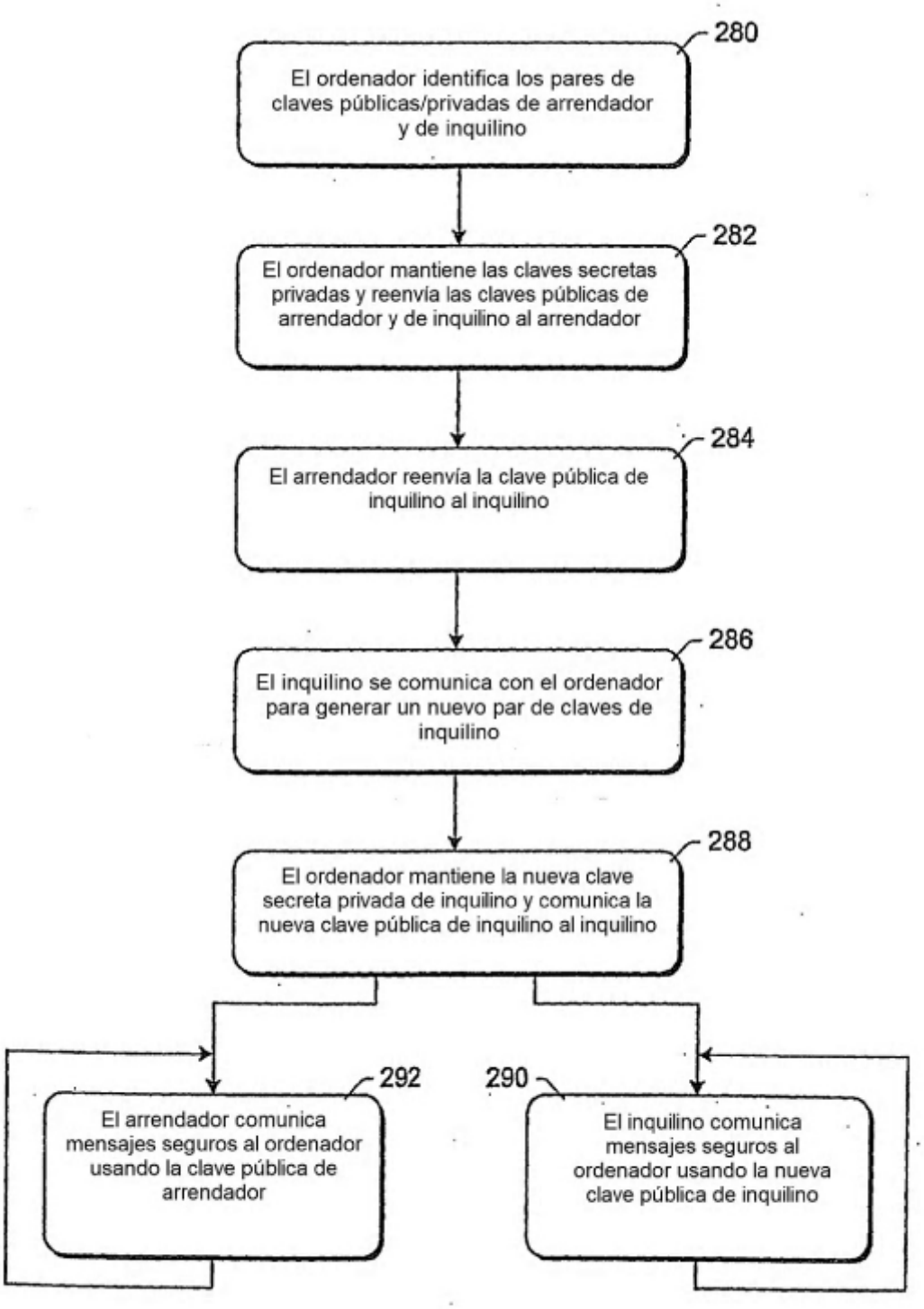
280
El ordenador identifica los pares de claves públicas/privadas de arrendador y de inquilino
282
El ordenador mantiene las claves secretas privadas y reenvía las claves públicas de arrendador y de inquilino al arrendador
284
El arrendador reenvía la clave pública de inquilino al inquilino
286
El inquilino se comunica con el ordenador para generar un nuevo par de claves de inquilino
288
El ordenador mantiene la nueva clave secreta privada de inquilino y comunica la nueva clave pública de inquilino al inquilino
292
El arrendador comunica mensajes seguros al ordenador usando la clave pública de arrendador
290
El inquilino comunica mensajes seguros al ordenador usando la nueva clave pública de inquilino

Fig. 6

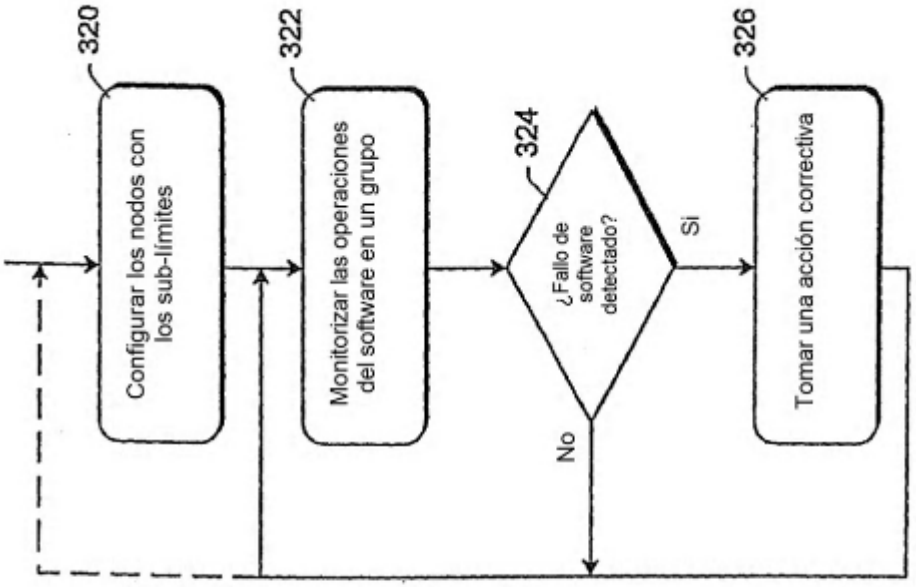
320
Configurar los nodos con los sub-límites
322
Monitorizar las operaciones del software en un grupo
324
¿Fallo de software detectado?
Si
No
326
Tomar una acción correctiva

Fig. 8

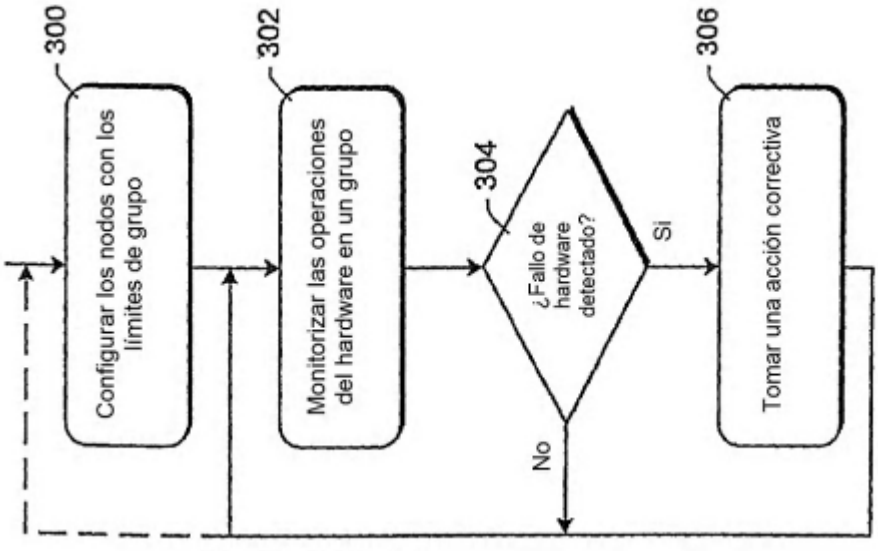
300
Configurar los nodos con los límites de grupo
302
Monitorizar las operaciones del hardware en un grupo
304
¿Fallo de hardware detectado?
Si
No
306
Tomar una acción correctiva

Fig. 7