(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 566 933**

(51) Int. CI.:

H04L 12/24 (2006.01)
G06F 15/16 (2006.01)
H04L 29/06 (2006.01)
G06F 11/20 (2006.01)
G06F 11/14 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **06.12.2011 E 11846483 (3)**

(97) Fecha y número de publicación de la concesión europea: **02.03.2016 EP 2649750**

(54) Título: **Proporcionar recuperación frente a fallos transparente en un sistema de ficheros**

(30) Prioridad:

10.12.2010 US 964749

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.04.2016

(73) Titular/es:

MICROSOFT TECHNOLOGY LICENSING, LLC (100.0%)
One Microsoft Way
Redmond, WA 98052, US

(72) Inventor/es:

SWAN, PAUL R.;
GEORGE, MATHEW;
KRUSE, DAVID M.;
BATTEPATI, ROOPESH C. y
JOHNSON, MICHAEL C.

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Proporcionar recuperación frente a fallos transparente en un sistema de ficheros

Antecedentes

Existe una diversidad de técnicas para compartir ficheros, impresoras y otros recursos entre dos ordenadores en una red. Por ejemplo, dos protocolos de red de la capa de aplicación para compartir recursos son el Bloque de Mensajes del Servidor (SMB) y el Sistema de Ficheros en Red (NFS). SMB se usa mediante MICROSOFT TM WINDOWS TM y otros sistemas operativos para permitir a dos ordenadores u otros recursos comunicar, solicitar acceso a recursos, especificar acceso pretendido de recursos (por ejemplo, lectura, escritura, etc.), bloquear recursos y así sucesivamente. MICROSOFT TM WINDOWS TM Vista introdujo SMB 2.0, que simplifica el conjunto de comandos de SMB 1.0 y añade muchas otras mejoras. MICROSOFT TM WINDOWS TM 7 y Server 2008 R2 introdujeron SMB 2.1, que añade bloqueo oportunista (oplocks) y otras mejoras.

La mayoría de los protocolos para compartición remota de recursos suponen una relación de uno a uno entre conexiones y sesiones. Una sesión representa el tiempo de vida de cualquier solicitud única para acceder a un recurso y el posterior acceso de ese recurso hasta que la conexión se termina. Una sesión puede asociarse también con unos credenciales principales de seguridad particulares y de seguridad validados que determinan las acciones que se autorizan durante la sesión. Una conexión puede incluir un Protocolo de Control de Transmisión (TCP), Protocolo de Datagramas de Usuario (UDP) u otro tipo de conexión a través de la cual los protocolos de nivel superior como SMB y NFS pueden comunicarse para llevar a cabo comandos. Una sesión de SMB o de NFS típicamente implica abrir una conexión de TCP o de UDP entre un origen de una solicitud y un objetivo de la solicitud, enviar uno o más comandos de SMB o de NFS para acceder al recurso objetivo y a continuación cerrar la sesión. En ocasiones las conexiones se pierden durante una sesión (por ejemplo, debido a un fallo de red), se elimina cualquier estado de cliente y de servidor establecido durante la conexión. Para reestablecer una conexión el cliente y el servidor típicamente tienen que repetir todas las etapas usadas para establecer inicialmente la conexión de nuevo.

El protocolo SMB2 proporciona una clave de reanudación que permite a los clientes reestablecer rápidamente un manejador de fichero a un servidor si un cliente se desconecta del servidor, posibilitando a los clientes reducir los recorridos de ida y vuelta de red al servidor y reducir la carga en el servidor cuando un cliente se reconecta. Sin embargo, hoy en día la clave de reanudación no proporciona restauración del estado en el caso de recuperación frente a fallos de servidor en el que el servidor de SMB2 pierde estado volátil durante un reinicio de servidor o recuperación frente a fallos de una agrupación. La información de estado asociada con las aperturas existentes se pierde y debe reestablecerse. Además, la clave de reanudación es un concepto de nivel de aplicación que puede crearse únicamente y usarse en el límite de una aplicación pero no compartirse.

El documento US 2005/091212 se refiere a un procedimiento y sistema para proporcionar acceso de estado completo a ficheros y reanudar acceso si se cortara una conexión. Una clave de reanudación se devuelve al cliente que permite al cliente solicitar un manejador duplicado a un fichero abierto. El manejador duplicado puede usarse para acceder al fichero de la misma manera que el manejador usado para abrir el fichero. Cuando se corta una conexión, el fichero permanece abierto en el servidor durante un periodo de tiempo y la información de estado asociada con el fichero se mantiene. Incluso si una conexión no se cortara, un cliente puede solicitar uno o más manejadores duplicados y establecer otros canales (también conocidos como conexiones) con los que acceder al fichero.

El documento US 2007/192326 se refiere a un mecanismo de recuperación frente a fallos de sesión distribuida para facilitar la replicación y recuperación de información de sesión. Un primer servidor, en una red confiable, que proporciona una solución de inicio de sesión unificado (SSO), almacena información de sesión que pertenece a un cliente particular que solicita servicios asociados con el servidor. Para proporcionar recuperación frente a fallos de sesión, el primer servidor envía una copia de la información de sesión a un mecanismo de bus, que está conectado a uno o más repositorios persistentes. Cuando un segundo servidor intenta validar el cliente, el segundo servidor puede descubrir que el primer servidor falló. El segundo servidor a continuación solicita una copia de la información de sesión que pertenece al cliente desde el mecanismo de bus. El mecanismo de bus recupera la copia desde un repositorio persistente y proporciona la copia al segundo servidor.

El documento US 2005/223014 se refiere a un sistema de ficheros de NAS escalable y protocolos para implementar CIFS en el mismo. Los protocolos implementan el protocolo de CIFS en una arquitectura de servidor de ficheros escalable que tiene uno o más nodos de terminación de protocolo, uno o más nodos de servidor de fichero y uno o más nodos de controlador de disco. Entre las características que pueden implementarse específicamente están acceso al árbol, acceso a fichero, autenticación de usuario, bloqueo, mantenimiento de estado y recuperación frente a fallos de nodos de terminación de protocolo y nodos de servidor de fichero.

Sumario

Es el objeto de la presente invención proporcionar un procedimiento y sistema para capturar información de sistema de ficheros para facilitar reanudar conexiones.

Este objeto se resuelve mediante la invención como se define mediante la materia objeto de las reivindicaciones independientes adjuntas 1 y 9.

Se definen realizaciones preferidas en las reivindicaciones dependientes.

Se describe en el presente documento un sistema de estado de conexión que permite a un cliente reanudar una conexión con un servidor o un servidor de reemplazo diferente almacenando de manera remota información de estado de cliente en asociación con una clave de reanudación. El sistema proporciona un filtro de clave de reanudación que opera en el servidor que facilita el almacenamiento de información de estado de servidor volátil. La información de estado puede incluir información tal como bloqueos oportunistas, arrendamientos concedidos a un cliente y operaciones en vuelo en un manejador de fichero. El controlador de filtro de clave de reanudación se encuentra por encima del sistema de ficheros, que permite que múltiples protocolos de acceso a ficheros usen el filtro, así como permitir que el filtro proporcione esta funcionalidad a través de múltiples sistemas de ficheros. El sistema proporciona información de estado al protocolo, independiente del protocolo real. Tras un evento de recuperación frente a fallos, tal como un servidor que deja de funcionar o pierde conectividad con un cliente, el sistema puede poner otro servidor o el mismo servidor y reestablecer el estado para los manejadores de ficheros mantenidos por diversos clientes usando el filtro de clave de reanudación. El filtro aplica una ventana de prohibición en los ficheros activos después de la recuperación frente a fallos que garantiza que el estado del fichero activo puede restaurarse de manera coherente y que los otros clientes no intervienen en acceder al fichero mientras tanto. En la fase de reanudación, la clave de reanudación se usa para mapear manejadores de ficheros pre-recuperación frente a fallos existentes al estado de fichero conservado post-recuperación frente a fallos almacenado mediante el filtro de clave de reanudación. Por lo tanto, el sistema de estado de conexión permite que el mismo u otro servidor reanuden el estado de una sesión anterior con un cliente después de un evento de recuperación frente a fallos con tan poca interrupción como sea posible para los clientes.

Este Sumario se proporciona para introducir una selección de conceptos de una forma simplificada que se describen adicionalmente a continuación en la Descripción Detallada. Este Sumario no se pretende para identificar características clave o características esenciales de la materia objeto reivindicada, ni pretende usarse para limitar el alcance de la materia objeto reivindicada.

Breve descripción de los dibujos

La Figura 1 es un diagrama de bloques que ilustra componentes del sistema de estado de conexión, en una realización.

La Figura 2 es un diagrama de flujo que ilustra el procesamiento del sistema de estado de conexión para capturar información de estado de sistema de ficheros, en una realización.

La Figura 3 es un diagrama de flujo que ilustra el procesamiento del sistema de estado de conexión para reanudar una conexión después de recuperación frente a fallos, en una realización.

La Figura 4 es un diagrama de bloques que ilustra el entorno de operación del sistema de estado de conexión, en una realización.

Descripción detallada

Se describe en el presente documento un sistema de estado de conexión que permite a un cliente reanudar una conexión con un servidor o un servidor de reemplazo diferente almacenando de manera remota información de estado de cliente en asociación con una clave de reanudación. El sistema proporciona un filtro de clave de reanudación que opera en el servidor que facilita el almacenamiento de información de estado de servidor volátil. La información de estado puede incluir información tal como bloqueos oportunistas, arrendamientos concedidos a un cliente y operaciones en vuelo en un manejador de fichero. El controlador de filtro de clave de reanudación se encuentra por encima del sistema de ficheros, que permite que múltiples protocolos de acceso de fichero usen el filtro, así como permitir al filtro proporcionar esta funcionalidad a través de múltiples sistemas de ficheros. El sistema proporciona información de estado al protocolo, independiente del protocolo real. Tras un evento de recuperación frente a fallos, tal como un servidor que deja de funcionar o pierde conectividad con un cliente el sistema puede poner otro servidor o el mismo servidor (por ejemplo, mediante conexión diferente, tal como una conexión de Ethernet redundante) y reestablecer el estado para los manejadores de ficheros mantenidos por diversos clientes usando el filtro de clave de reanudación.

El sistema proporciona un filtro de clave de reanudación que puede usarse para recuperación frente a fallos transparente después de que un servidor pierde su conexión con un cliente. El filtro de clave de reanudación se encuentra por encima del sistema de ficheros y es por lo tanto independiente del protocolo usado para acceder al sistema de ficheros. El filtro de clave de reanudación registra el estado de fichero activo y a continuación restaura el estado de fichero activo después de una recuperación frente a fallos. El filtro de clave de reanudación puede capturar una diversidad de información de estado. Por ejemplo, el filtro registra el estado de sistema de ficheros activo que comprende manejadores abiertos (referenciados estáticamente mediante una clave de reanudación), estado de fichero no comprometido (tal como borrar al salir, borrar pendiente y estado de bloqueo), y ciertas operaciones de fichero en vuelo/interrumpidas. El filtro restaura el estado de sistema de ficheros activo después de recuperación frente a fallos de manera que los manejadores abiertos se reanudan para coincidir con aquellas

operaciones anteriores a la recuperación frente a fallos y en vuelo que pueden reproducirse de manera coherente. El filtro proporciona un medio para que múltiples Sistemas de Ficheros Remotos (RFS) almacenen y recuperen datos opacos privados que están asociados con un manejador de fichero abierto referenciado a través de una clave de reanudación. El filtro aplica una ventana de prohibición en ficheros activos después de la recuperación frente a fallos que garantiza que el estado de fichero activo puede restaurarse de manera coherente y que los otros clientes no intervienen en acceder al fichero mientras tanto. El filtro también permite que un fichero actualmente activo se "suspenda" y a continuación se reanude sin una recuperación frente a fallos para soportar SMB en el escenario de agrupación donde los nodos se recuperan frente a fallos.

Un sistema de fichero remoto (RFS) suministra una clave de reanudación con cada operación de creación de fichero como un parámetro extra durante la creación. La clave es única para el RFS. El filtro de clave de reanudación usa una clave de reanudación y una clave de identificación de RFS juntas como un identificador globalmente único (GUID) para un manejador de fichero. En la fase de reanudación, la clave de reanudación se usa para mapear los manejadores de ficheros pre-recuperación frente a fallos existentes al estado de fichero conservado post-recuperación frente a fallos mediante el filtro de clave de reanudación. Por lo tanto, el sistema de estado de conexión permite que el mismo u otro servidor reanuden el estado de una sesión anterior con un cliente después de un evento de recuperación frente a fallos con tan poca interrupción como sea posible para los clientes.

La Figura 1 es un diagrama de bloques que ilustra componentes del sistema de estado de conexión, en una realización. El sistema 100 incluye un componente 110 de recopilación de estado, un componente 120 de almacenamiento de estado, un almacenamiento 130 de datos de estado, un componente 140 de detección de reanudación, un componente 150 de recuperación de estado, un componente 160 de restauración de estado, un componente 170 de aplicación de prohibición y un componente 180 de suspensión de recursos. Cada uno de estos componentes se describe en mayor detalle en el presente documento.

El componente 110 de recopilación de estado crea un registro de estado para cada manejador de fichero y recopila información de estado a medida que un cliente solicita operaciones que usan el manejador de fichero. El componente 110 puede operar en un servidor y almacenar información de estado externamente desde el servidor de modo que puede accederse a la información de estado si el servidor no estuviera disponible. Por ejemplo, el componente 110 puede almacenar la información de estado en el almacenamiento 130 de datos de estado descrito adicionalmente en el presente documento. El componente 110 de recopilación de estado puede recibir una clave de reanudación desde el cliente cuando el cliente se conecta al servidor, y el componente 110 asocia información de estado recopilada con la clave de reanudación en el almacenamiento 130 de datos de estado. Si un cliente se está reconectando después de un evento de recuperación frente a fallos, el cliente proporcionará la misma clave de reanudación usada para abrir la conexión inicial y el servidor actual puede encontrar la información de estado almacenada mediante el servidor anterior y recrear el estado de servidor desde la información de estado.

El componente 120 de almacenamiento de estado almacena información de estado recopilada en asociación con una clave de reanudación proporcionada mediante el cliente. El componente 120 almacena la información de estado en el almacenamiento 130 de datos de estado y mantiene un registro de operaciones relacionadas con la clave de reanudación que se restaurarían en el caso de un evento de recuperación frente a fallos. La información de estado puede incluir manejadores de ficheros abiertos, bloqueos oportunistas concedidos, arrendamientos e información de arrendamiento, operaciones de fichero en progreso, bloqueos de intervalos de bytes y cualquier otra información que otro servidor usaría para llevar a cabo las solicitudes del cliente sin que el cliente restablezca todo el estado anterior.

El almacenamiento 130 de datos de estado almacena de manera persistente información de estado de sistema de ficheros que un servidor de reanudación usa para recrear información de estado almacenada mediante un servidor que falla. En algunos casos, el servidor de reanudación y el servidor que falla pueden ser el mismo servidor usando una conexión diferente al cliente o que vuelve después de un breve apagón. En otros casos, el servidor de reanudación y el servidor que falla son servidores diferentes, y el almacenamiento 130 de datos de estado se proporciona en una localización accesible para que ambos servidores compartan la información de estado. El almacenamiento 130 de datos de estado puede incluir uno o más ficheros, sistemas de ficheros, discos duros, bases de datos, redes de área de almacenamiento (SAN), servicios de almacenamiento basados en la nube u otra instalación de almacenamiento para almacenar datos de manera persistente y accesible para que tanto el servidor que falla como el de reanudación intercambien información. Ya que el servidor que falla está realizando operaciones, está almacenando información de estado acerca del progreso de las operaciones en el almacenamiento 130 de datos de estado. Tras un fallo, el servidor que falla se interrumpirá, y un servidor de reanudación accede a la información de estado para reanudar el estado y sigue llevando a cabo cualquier operación que no se completó.

El componente 140 de detección de reanudación detecta una condición que hace al servidor que falla no disponible e informa a un servidor de reanudación para actuar en lugar del servidor que falla. La detección puede accionarse por el cliente, de manera que el sistema no realiza ninguna etapa de reanudación hasta que el cliente se reconecta al sistema y proporciona una clave de reanudación usada previamente. El sistema identifica la clave y cualquier información de estado almacenada en asociación con la clave y restaura esa información de estado como parte de establecimiento de la conexión. El servidor de reanudación puede ser el mismo o un servidor diferente del servidor que falla, y el componente 140 de detección de reanudación asegura que el servidor de reanudación se vuelve activo para manejar las solicitudes de los clientes. En otras realizaciones, la detección puede accionarse por el

servidor y el sistema puede poner de manera proactiva un servidor de reanudación tras detectar que un servidor que falla ha dejado de funcionar. El sistema puede pre-rellenar también el servidor de reanudación con información de estado almacenada incluso antes de que un cliente solicite una conexión al servidor.

El componente 150 de recuperación de estado recupera la información de estado almacenada desde una localización accesible al servidor de reanudación, en el que la información de estado permite el servidor de reanudación reanudar cualquier operación de sistema de ficheros previamente solicitada que se interrumpiera por la condición de fallo detectada. El componente 150 de recuperación de estado recupera información de estado desde el almacenamiento 130 de datos de estado e invoca el componente 160 de restauración de estado para cargar la información en el servidor de reanudación de modo que el servidor de reanudación puede continuar las operaciones solicitadas mediante el cliente.

El componente 160 de restauración de estado carga la información de estado recuperada en el servidor de reanudación de modo que el servidor de reanudación puede continuar las operaciones previamente solicitadas mediante el cliente. La restauración puede incluir también refrescar cualquier bloqueo oportunista y/o arrendamientos mantenidos por el cliente para asegurar que los otros clientes respeten los niveles de acceso previamente solicitados y/o exclusivamente concedidos al cliente. El componente 160 de restauración de estado permite a un nuevo servidor o nodo tomar el lugar de un servidor o nodo que falla sin poner una carga pesada en el cliente para restaurar información de estado repitiendo operaciones pasadas. Los clientes que usan protocolos como SMB 2.0 ya conocen cómo usar una clave de reanudación para restaurar una conexión al mismo servidor, y el sistema de estado de conexión permite que un servidor sustituto tome el lugar de un servidor que falla de manera transparente para el cliente. Las claves de reanudación pueden usarse también con NFS. En el caso de NFS, el concepto de una clave de reanudación es completamente opaco para el cliente. El cliente no hace referencia explícitamente o participa en la generación, gestión y asociación de la clave de reanudación. En su lugar, la clave de reanudación es un concepto del lado del servidor.

El componente 170 de aplicación de prohibición aplica un periodo de prohibición en acceso a uno o más ficheros u otros recursos que evita que un segundo cliente interfiera con recursos de tal manera que pudiera entrar en conflicto con un primer cliente que reanuda una conexión con el servidor de reanudación. El componente 170 puede seleccionar automáticamente un periodo que se considera que es suficientemente largo para evitar la mayoría de las operaciones en conflicto (por ejemplo, 15 o 30 segundos), pero no tan largo como para evitar que otros clientes accedan a los recursos si el primer cliente no reanuda la conexión. El periodo permite al primer cliente reanudar la conexión si el primer cliente lo elige. En algunas realizaciones, el sistema permite a un administrador u otro usuario configurar la duración del periodo de prohibición para ajustar el sistema para fines específicos de la aplicación. El sistema puede permitir también a clientes individuales solicitar un periodo de prohibición como un parámetro para una solicitud de creación/apertura u otra interfaz de programación de aplicación (API). En respuesta a intentos para acceder a un recurso prohibido, el componente 170 puede proporcionar una indicación para intentar de nuevo después de un periodo particular o simplemente fallar la solicitud. Después del periodo de prohibición si ningún cliente ha reanudado la conexión, entonces se termina la prohibición y las solicitudes para acceder al recurso sucederán de manera normal.

El componente 180 de suspensión de recurso permite a un recurso actualmente activo que se suspenda y se reanude sin un evento de recuperación frente a fallos para permitir a una agrupación recuperarse frente a fallos a otro nodo de una manera planeada. Un ejemplo es el equilibrio de carga. La suspensión permite escenarios donde un subconjunto del estado se está pasando a un nuevo nodo. Por ejemplo, si un nodo en la agrupación está sobrecargado, un administrador puede desear migrar la mitad de los clientes del nodo a un nuevo nodo. La suspensión permite capturar el estado de las aperturas que se están migrando y permite al cliente conectarse al nuevo nodo como una continuación de la misma apertura (por ejemplo, sin reestablecer el estado del servidor). Como otro ejemplo, SMB soporta escenarios de agrupación en los que nodos genéricos se ponen en una agrupación y pueden usarse de manera intercambiable para servir solicitudes de cliente. En ocasiones hay una razón para apagar un nodo particular, tal como para mantenimiento, y es deseable suspender de manera limpia el nodo actual, activar el nuevo nodo, desactivar el nodo antiguo y a continuación realizar cualquier operación de mantenimiento en el nodo desactivado. Esto puede tener un impacto indeseable en los clientes, pero usando las técnicas descritas en el presente documento, el sistema 100 puede suspender el nodo de una manera organizada, y permitir a los clientes reanudar operaciones con el nuevo nodo de manera eficaz.

El dispositivo informático en el que se implementa el sistema de estado de conexión puede incluir una unidad de procesamiento central, memoria, dispositivos de entrada (por ejemplo, teclado y dispositivos apuntadores), dispositivos de salida (por ejemplo, dispositivos de pantalla) y dispositivos de almacenamiento (por ejemplo, unidades de disco u otro medio de almacenamiento no volátil). La memoria y los dispositivos de almacenamiento son medios de almacenamiento legibles por ordenador que pueden codificarse con instrucciones ejecutables por ordenador (por ejemplo, software) que implementan o posibilitan el sistema. Además, las estructuras de datos y estructuras de mensaje pueden almacenarse o transmitirse mediante un medio de transmisión de datos, tal como una señal en un enlace de comunicación. Pueden usarse diversos enlaces de comunicación, tales como internet, una red de área local, una red de área extensa, una conexión de marcación de punto a punto, una red de telefonía celular y así sucesivamente.

Las realizaciones del sistema pueden implementarse en diversos entornos operativos que incluyen ordenadores personales, ordenadores servidores, dispositivos de mano o portátiles, sistemas multiprocesador, sistemas basados en microprocesador, electrónica de consumo programable, cámaras digitales, PC de red, miniordenadores, ordenadores centrales, entornos informáticos distribuidos que incluyen cualquiera de los sistemas o dispositivos anteriores, decodificadores de salón, sistemas en un chip (SOC) y así sucesivamente. Los sistemas informáticos pueden ser teléfonos celulares, asistentes digitales personales, teléfonos inteligentes, ordenadores personales, electrónica de consumo programable, cámaras digitales y así sucesivamente.

El sistema puede describirse en el contexto general de instrucciones ejecutables por ordenador, tales como módulos de programa, ejecutados mediante uno o más ordenadores u otros dispositivos. En general, los módulos de programa incluyen rutinas, programas, objetos, componentes, estructuras de datos y así sucesivamente que realizan tareas particulares o implementan tipos de datos abstractos particulares. Típicamente, la funcionalidad de los módulos de programa puede combinarse o distribuirse según se desee en diversas realizaciones.

La Figura 2 es un diagrama de flujo que ilustra el procesamiento del sistema de estado de conexión para capturar información de estado de sistema de fichero, en una realización. Comenzando en el bloque 210, el sistema recibe desde un cliente una solicitud para acceder a un recurso remoto almacenado en un servidor. La solicitud de acceso puede incluir uno o más parámetros, incluyendo una clave de reanudación usada para identificar la sesión a través de múltiples conexiones potenciales si una conexión falla. La solicitud de acceso de recursos puede ser la primera en una serie de solicitudes de acceso enviadas desde el cliente, y si el cliente se desconectara alguna vez del servidor el cliente puede proporcionar la misma clave de reanudación en una solicitud de apertura posterior al mismo o a un nuevo servidor para reanudar la conexión. La clave de reanudación ayuda al servidor a responder al cliente más rápido correlacionando información de estado mantenida por el servidor (o a través de servidores) entre lo que de otra manera parecería que son conexiones de cliente independientes.

Continuando en el bloque 220, el sistema determina un identificador que identifica una sesión de cliente relacionada con la solicitud. El identificador en algunos casos es una clave de reanudación que el cliente proporciona para manejadores duraderos que permiten reanudar sesiones que se desconectan por diversas razones. La solicitud de acceso puede incluir uno o más parámetros en localizaciones bien definidas en el protocolo de modo que el sistema puede extraer la clave leyendo la localización apropiada en la solicitud. Como alternativa o adicionalmente, el servidor puede incluir un procedimiento automatizado para determinar el identificador que no implica información explícitamente proporcionada mediante el cliente. Por ejemplo, el servidor puede identificar el cliente mediante la dirección del Protocolo de Internet (IP) u otros datos deducidos que indican al servidor que la conexión del cliente está correlacionada con una sesión anterior.

Continuando en el bloque 230, el sistema crea un registro de reanudación que puede buscarse mediante el identificador extraído que asocia información de estado creada mediante operaciones solicitadas mediante el cliente con el identificador extraído. El registro de reanudación puede almacenarse en una localización externa al servidor que maneja la solicitud de acceso actual de modo que si el servidor falla otro servidor podrá leer el registro para reanudar las operaciones y actuar en lugar del servidor original. El registro de reanudación puede incluir un fichero, un registro de base de datos u otra forma de almacenamiento. El registro puede contener una lista de manejadores de ficheros abiertos, bloqueos oportunistas obtenidos mediante el cliente, arrendamientos u otra información de estado del sistema de ficheros.

Continuando en el bloque 240, el sistema recibe una operación de fichero desde el cliente que solicita acceso a un fichero accesible a través del servidor. La operación de fichero puede ser una solicitud para abrir un fichero, cerrar un fichero, leer un fichero, escribir un fichero, imprimir en una impresora compartida u otras operaciones de sistema de ficheros. La operación recibida implica una cierta cantidad de información de estado que se crea en el servidor. Por ejemplo, si el cliente abre un manejador al fichero, a continuación el servidor rastrea ese manejador para gestionar otras solicitudes relacionadas con el fichero y para gestionar el tiempo de vida y/o procesamiento de limpieza para el manejador.

Continuando en el bloque 250, el sistema almacena información de estado de reanudación en el registro de reanudación creado que proporciona información para reanudar la operación de fichero recibida si el cliente pierde su conexión con el servidor. Si la conexión del cliente falla, el cliente intentará reanudar la conexión abriendo de nuevo un recurso remoto y especificando la misma clave de reanudación u otro identificador de sesión. Esto permitirá al servidor o a otro servidor acceder al registro de reanudación almacenado y reestablecer la información de estado anterior.

Continuando en el bloque 260, el sistema realiza la operación de fichero solicitada. La operación puede abrir un fichero, leer los contenidos del fichero, escribir datos en el fichero, cambiar derechos de acceso al fichero o cualquier otra operación de sistema de ficheros. El resultado de la operación puede cambiar el estado almacenado mediante el servidor. Por ejemplo, si el cliente intenta elegir un manejador y el servidor cierra satisfactoriamente el manejador, entonces el estado de servidor se actualizará para eliminar el manejador de una lista de manejadores rastreados mediante el servidor.

Continuando en el bloque 270, el sistema actualiza la información de estado de reanudación almacenada en el registro de reanudación creado basándose en un resultado de la operación de fichero realizada. El sistema no puede conocer con antelación cuándo tendrá lugar un fallo que produzca recuperación frente a fallos, por lo que el sistema mantiene una vista actualizada del estado del servidor en el registro de reanudación que permite a un servidor reestablecer el estado tan próximo al estado del servidor anterior como sea posible. Las operaciones que no se completaron pueden reproducirse para completar las operaciones mientras que las operaciones que se completaron no necesitan repetirse (pero el servidor puede reenviar el resultado al cliente). Por lo tanto, el sistema actualiza el estado según sea necesario durante y después de diversas operaciones de sistema de ficheros que cambian la información de estado de servidor.

Continuando en el bloque 280, el sistema envía una respuesta al cliente que indica el resultado de la operación de fichero solicitada. Si el cliente y el servidor están aún conectados, entonces las operaciones continúan como si solicitaran mediante el cliente y el servidor sigue rastreando información de estado actualizada. Si en cualquier momento se pierde la conexión, puede ponerse otro servidor o repararse el servidor existente y la información de estado puede cargarse desde el almacenamiento de estado para reestablecer el estado del servidor anterior. Tras recibir una nueva solicitud desde el cliente para reanudar la sesión, el cliente no necesita conocer que ha tenido lugar la recuperación frente a fallos y que el cliente está interactuando potencialmente con un servidor diferente al original. Después del bloque 280, estas etapas concluyen.

La Figura 3 es un diagrama de flujo que ilustra el procesamiento del sistema de estado de conexión para reanudar una conexión después de recuperación frente a fallos, en una realización. Comenzando en el bloque 310, el sistema recibe desde un cliente una solicitud para abrir un recurso remoto almacenado en un servidor. La solicitud de acceso puede incluir uno o más parámetros, incluyendo una clave de reanudación usada para identificar la sesión a través de múltiples conexiones potenciales si una conexión falla. A diferencia de la solicitud de acceso de recurso analizada con referencia a la Figura 2, esta solicitud es una solicitud para reconectar a una sesión previamente conectada. El cliente proporciona la misma clave de reanudación como se proporcionó originalmente, de modo que el servidor puede correlacionar la solicitud de sesión actual con la sesión anterior.

Continuando en el bloque 320, el sistema determina un identificador de sesión que identifica una sesión de cliente relacionada con la solicitud. El identificador en algunos casos es una clave de reanudación de SMB 2 que el cliente proporciona para manejadores duraderos que permiten reanudar sesiones que se desconectan por diversas razones. La solicitud de acceso puede incluir uno o más parámetros en localizaciones bien definidas en el protocolo de modo que el sistema puede extraer la clave leyendo la localización apropiada en la solicitud. En otros casos, el servidor puede determinar el identificador automáticamente basándose en información acerca del cliente.

Continuando en el bloque 330, el sistema busca el identificador de sesión recibido en un almacenamiento de estado para identificar un registro de reanudación asociado con el identificador de sesión. Cualquier interacción de servidor anterior con el cliente usando una sesión que puede reanudarse almacena información de estado en una base en curso a través de la interacción con el cliente. Cuando el cliente intenta reestablecer la conexión, la información de estado está disponible para un servidor de recuperación frente a fallos que se pone en marcha en el servidor original. La información de estado puede almacenarse externamente al servidor original de modo que la información es accesible después de un fallo del servidor original.

Continuando en el bloque 340, el sistema recibe desde el almacenamiento de estado información de estado anterior asociada con el registro de reanudación. La información de estado identifica el estado estático, tal como manejadores de ficheros abiertos, arrendamientos obtenidos, bloqueos oportunistas obtenidos y así sucesivamente, así como el estado dinámico, tal como operaciones en vuelo que pueden no haberse completado. La información de estado almacenada permite al servidor de recuperación frente a fallos tomar el lugar del servidor original sin procesamiento específico mediante el cliente. El cliente entiende los manejadores que pueden reanudarse y realiza etapas para hacer una conexión que puede reanudarse, pero puede no conocer cuál servidor termina manejando la conexión en algún momento particular. El cliente puede acceder al servidor mediante un nombre de dominio o compartición de fichero de red que puede resolver a una dirección de uno cualquiera de varios servidores, incluyendo el servidor de recuperación frente a fallos.

Continuando en el bloque 350, el sistema restaura la información de estado anterior recibida cargando la información en los componentes del sistema de ficheros que rastrean el estado del sistema de ficheros. Después de cargar el estado, el estado local del servidor de recuperación frente a fallos es similar a cómo parecería el estado si todas las operaciones anteriores hubieran ocurrido en el servidor de recuperación frente a fallos. Por lo tanto, el servidor de recuperación frente a fallos es tan útil para que el cliente continúe la serie de operaciones como si el servidor original no hubiera tenido la conexión fallida.

Continuando en el bloque 360, el sistema responde a la solicitud de acceso del cliente indicando que el servidor encontró el registro de reanudación y está listo para recibir operaciones de cliente relacionadas con la sesión anterior. Basándose en la respuesta del servidor, el cliente puede determinar si la sesión se reanuda o si el cliente necesita tomar etapas para repetir operaciones anteriores. Si la sesión se reanudó satisfactoriamente, entonces el cliente puede seguir conociendo las operaciones anteriores completadas o se reproducen para completar después de que el servidor se reanudó. En algunos casos, el sistema puede dar al cliente un nuevo manejador de fichero que

tiene el mismo estado que el manejador de fichero pre-recuperación frente a fallos. Después del bloque 360, estas etapas concluyen.

La Figura 4 es un diagrama de bloques que ilustra el entorno de operación del sistema de estado de conexión, en una realización. El entorno incluye uno o más servicios de sistema operativo o aplicaciones que interactúan con sistemas de ficheros. Por ejemplo, MICROSOFT TM WINDOWS TM incluye un servicio 420 de servidor conocido como SRV, y un servicio 410 de sistema de ficheros de red conocido como NFS. El servicio 410 de sistema de ficheros de red y el servicio 420 de servidor proporcionan acceso a recursos compartidos, tales como ficheros e impresoras, entre sistemas informáticos. El servicio 420 de servidor usa el protocolo de SMB común a redes de WINDOWS TM, mientras el servicio 410 de sistema de ficheros de red proporciona acceso a sistemas basados en Unix que usan más comúnmente NFS. Independientemente del protocolo, el filtro 430 de clave de reanudación captura operaciones de fichero y almacena información de estado para reanudar las operaciones en un almacenamiento de datos remoto. Las operaciones pasan a través del nivel 440 de sistema de ficheros (por ejemplo, NTFS u otro sistema de ficheros), y afectan a uno o más ficheros 450 de datos de usuario. Mientras tanto, el filtro 430 de clave de reanudación escribe información de estado en un fichero 460 de registro u otro almacenamiento de datos, que otro servidor puede acceder para recuperar información de estado y reanudar una conexión con un cliente. El sistema puede operar independiente del protocolo particular o del sistema de ficheros implicado, y pueden actualizarse diversos componentes para grabar su propia información de estado particular en el almacenamiento de datos de estado.

En algunas realizaciones, el sistema de estado de conexión almacena objetos binarios grandes opacos de datos en beneficio de los componentes del sistema de ficheros para permitir al sistema reanudar las conexiones sin conocimiento específico del componente. Por ejemplo, el filtro de clave de reanudación descrito en el presente documento puede pedir al servicio de servidor algún dato que el servicio de servidor necesitaría recrear en su estado actual. El filtro puede a continuación almacenar cualquier dato recibido como un objeto binario grande opaco (es decir, el filtro no necesita conocer qué hay en el objeto binario grande o su significado semántico) en el almacenamiento de estado. Tras una condición de recuperación frente a fallos, un filtro de clave de reanudación que opera en el nuevo servidor puede acceder a la información de estado almacenada, recuperar el objeto binario grande almacenado, y proporcionar el objeto binario grande al servicio de servidor de modo que el servicio de servidor puede restaurar su propio estado. De esta manera, el sistema puede hacerse funcionar con muchos tipos de protocolos sin conocimiento específico de las operaciones internas de los componentes que implementan cada protocolo para un servidor.

En algunas realizaciones, el sistema de estado de conexión bloquea que otros clientes accedan a ficheros u otros recursos relacionados con un manejador que puede reanudarse durante alguna cantidad de tiempo (es decir, periodo de prohibición). Si el cliente original se reconecta durante el periodo de prohibición, entonces el cliente original obtiene su propia conexión de vuelta con todo el estado anterior, y puede reanudar operaciones. Si otro cliente intenta conectar, el servidor puede proporcionar un mensaje que indica esperar una cantidad de tiempo y reintentar. Los clientes conocedores de la reanudación pueden usar esta información para retardar el reintento hasta después del periodo de prohibición, mientras los clientes más antiguos pueden simplemente fallar la conexión y reintentar manualmente en la solicitud del usuario. Si el cliente original no vuelve en el periodo de prohibición, el servidor limpia la información de estado de reanudación y permite que accedan nuevos clientes a los recursos como es habitual.

En algunas realizaciones, el sistema de estado de conexión puede usar una diversidad de dispositivos de almacenamiento o estrategias para acelerar las reanudaciones. Por ejemplo, el sistema puede usar un dispositivo de almacenamiento no volátil rápido (por ejemplo, un disco de estado sólido (SSD)) para almacenar información de estado de reanudación de modo que las reanudaciones acceden más rápido a los datos para evitar retardar aún más las operaciones ya interrumpidas por un fallo. Como otro ejemplo, el sistema puede difundir todos los cambios realizados mediante cada servidor a un grupo de servidores, de modo que cada servidor puede mantener su propia copia de la información de estado y puede ser el servidor de recuperación frente a fallos elegido en el caso de un fallo del servidor original.

A partir de lo anterior, se apreciará que se han descrito en el presente documento realizaciones específicas del sistema de estado de conexión para fines de ilustración, pero que pueden realizarse diversas modificaciones sin desviarse del alcance de la invención.

REIVINDICACIONES

1. Un procedimiento implementado por ordenador para capturar información de estado del sistema de ficheros para facilitar la reanudación de las conexiones, comprendiendo el procedimiento:

recibir (210) desde un cliente una solicitud para acceder a un recurso remoto almacenado en un servidor;
determinar (220) un identificador que identifica una sesión de cliente relacionada con la solicitud;
crear (230), en un almacenamiento (130) de datos de estado externo al servidor y accesible mediante un servidor de reanudación distinto del servidor, un registro de estado para cada manejador de fichero, pudiéndose buscar el registro de estado mediante el identificador que asocia información de estado, creada mediante las operaciones solicitadas por el cliente usando el manejador de fichero, con el identificador;
recibir (240) una operación de fichero desde el cliente que solicita acceso a un fichero accesible a través del servidor;
almacenar (250), en el almacenamiento de datos de estado, información de estado de reanudación en el registro de estado creado que proporciona información para reanudar la operación de fichero recibida si el cliente pierde su conexión con el servidor;
detectar una condición que hace al servidor no disponible e informar al servidor de reanudación para actuar en lugar del servidor;
recuperar (340) información de estado almacenada desde el almacenamiento de datos de estado, en el que la información de estado permite al servidor de reanudación reanudar cualquier operación de sistema de ficheros previamente solicitada que se interrumpiera por la condición de fallo detectada; y
cargar (350) la información de estado recuperada en el servidor de reanudación para permitir al servidor de reanudación continuar (360) operaciones previamente solicitadas por el cliente,
en el que se aplica un periodo de prohibición en el acceso a uno o más recursos, evitando el periodo de prohibición que un segundo cliente interfiera con los recursos de tal manera que pudiera entrar en conflicto con la reanudación de la conexión por el cliente al servidor de reanudación.

2. El procedimiento de la reivindicación 1, en el que la solicitud de acceso incluye uno o más parámetros, incluyendo una clave de reanudación que identifica la sesión del cliente a través de múltiples conexiones potenciales si una conexión falla, y en el que la clave de reanudación es al menos parte del identificador determinado.

3. El procedimiento de la reivindicación 1, en el que un servidor de Sistema de Ficheros de Red, NFS, determina el identificador automáticamente sin recibir una clave de reanudación desde el cliente.

4. El procedimiento de la reivindicación 1, en el que el identificador es una clave de reanudación de Bloque de Mensajes del Servidor, SMB, que proporciona el cliente para manejos duraderos que permiten reanudar sesiones que se desconectaron.

5. El procedimiento de la reivindicación 1, donde recibir la operación de fichero comprende una solicitud para realizar una operación seleccionada del grupo que consiste en abrir un fichero, cerrar un fichero, leer un fichero, escribir un fichero, obtener un arrendamiento de un fichero y obtener un bloqueo en un fichero.

6. El procedimiento de la reivindicación 1, que comprende adicionalmente, tras haberse desconectado el cliente del servidor, cargar en el servidor de reanudación el registro de estado almacenado de modo que el cliente pueda conectarse al servidor de reanudación y continuar cualquier operación anterior.

7. El procedimiento de la reivindicación 1, en el que realizar la operación de fichero solicitada modifica el estado almacenado mediante el servidor, y en el que actualizar la información de estado de reanudación almacenada captura el estado modificado.

8. El procedimiento de la reivindicación 1, en el que actualizar la información de estado de reanudación almacenada comprende mantener una vista actualizada del estado del servidor en el registro de estado que permite al servidor de reanudación reestablecer el estado y manejar solicitudes de cliente en lugar del servidor original sin requerir que el cliente reestablezca al menos alguna de la información de estado.

9. Un sistema informático para capturar información de estado de sistema de ficheros para facilitar la reanudación de las conexiones, comprendiendo el sistema:

un procesador y memoria configurados para ejecutar instrucciones de software incorporadas en los siguientes componentes;
un componente (110) de recopilación de estado configurado para operar en un servidor, para crear, en un almacenamiento (130) de datos de estado externo al servidor y accesible mediante un servidor de reanudación distinto del servidor, un registro de estado para cada manejador de fichero, y para recopilar información de estado a medida que un cliente solicita operaciones usando el manejador de fichero;
un componente (120) de almacenamiento de estado configurado para almacenar información de estado recopilada en asociación con un identificador de sesión proporcionado por el cliente;
el almacenamiento (130) de datos de estado configurado para almacenar de manera persistente información de estado del sistema de ficheros que un servidor de reanudación usa para recrear información de estado

almacenada mediante el servidor si el servidor falla;
un componente (140) de detección de reanudación configurado para detectar una condición que hace al servidor no disponible y para informar al servidor de reanudación para actuar en lugar del servidor;
un componente (150) de recuperación de estado configurado para recuperar información de estado almacenada desde el almacenamiento de datos de estado, en el que la información de estado permite al servidor de reanudación reanudar cualquier operación de sistema de ficheros previamente solicitada que se interrumpiera mediante la condición de fallo detectada;
un componente (160) de restauración de estado configurado para cargar la información de estado recuperada en el servidor de reanudación para permitir al servidor de reanudación continuar operaciones previamente solicitadas por el cliente; y
un componente (170) de aplicación de prohibición configurado para aplicar un periodo de prohibición en el acceso a uno o más recursos que evita que un segundo cliente interfiera con los recursos de tal manera que pudiera entrar en conflicto con la reanudación de la conexión por el cliente al servidor de reanudación.

10. El sistema de la reivindicación 9, en el que el componente de recopilación de estado está configurado adicionalmente para recibir el identificador de sesión proporcionado por el cliente, siendo el identificador de sesión una clave de reanudación proporcionada por el cliente cuando el cliente se conecta al servidor, y para asociar información de estado recopilada con la clave de reanudación en el almacenamiento de datos de estado.

11. El sistema de la reivindicación 9, en el que el almacenamiento de datos de estado está configurado adicionalmente para recibir información de estado a medida que el servidor está realizando operaciones y, tras un fallo, proporcionar acceso a la información de estado previamente recibida al servidor de reanudación para reanudar el estado y seguir llevando a cabo cualquier operación que no se completó.

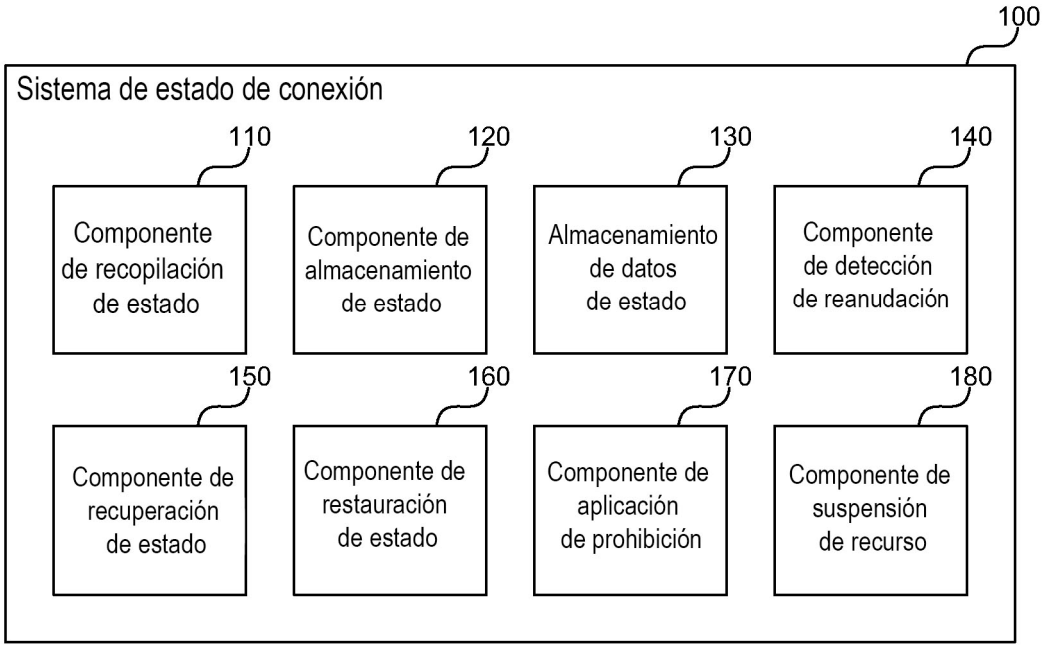
100
Sistema de estado de conexión
110
Componente de recopilación de estado
120
Componente de almacenamiento de estado
130
Almacenamiento de datos de estado
140
Componente de detección de reanudación
150
Componente de recuperación de estado
160
Componente de restauración de estado
170
Componente de aplicación de prohibición
180
Componente de suspensión de recurso

FIG. 1

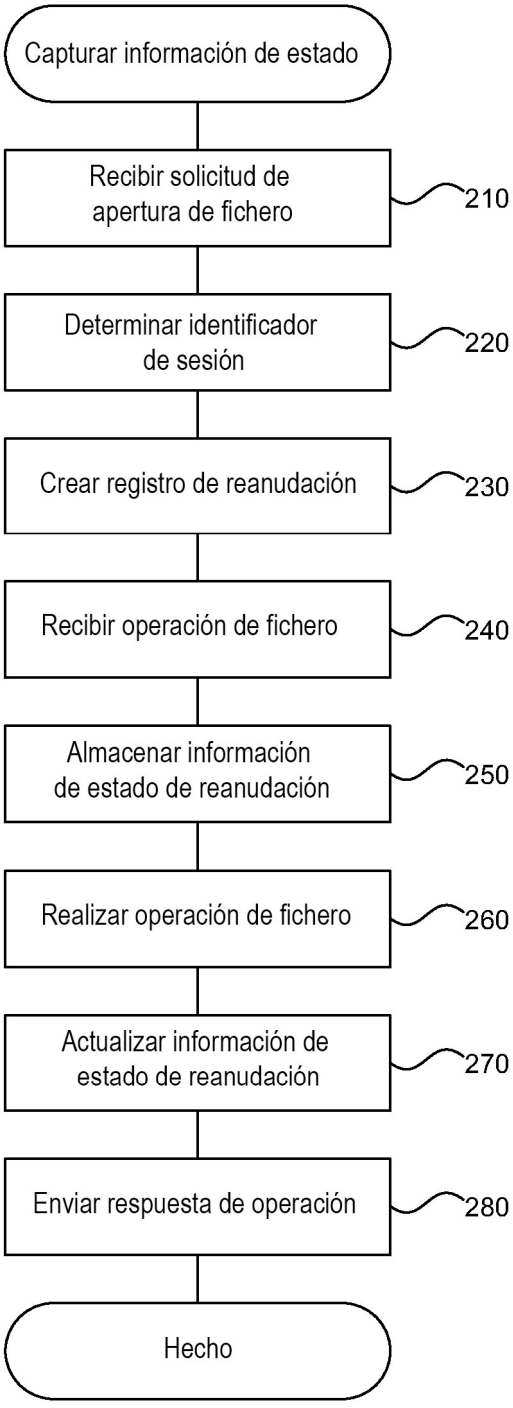
Capturar información de estado
Recibir solicitud de apertura de fichero
210
Determinar identificador de sesión
220
Crear registro de reanudación
230
Recibir operación de fichero
240
Almacenar información de estado de reanudación
250
Realizar operación de fichero
260
Actualizar información de estado de reanudación
270
Enviar respuesta de operación
280
Hecho

FIG. 2

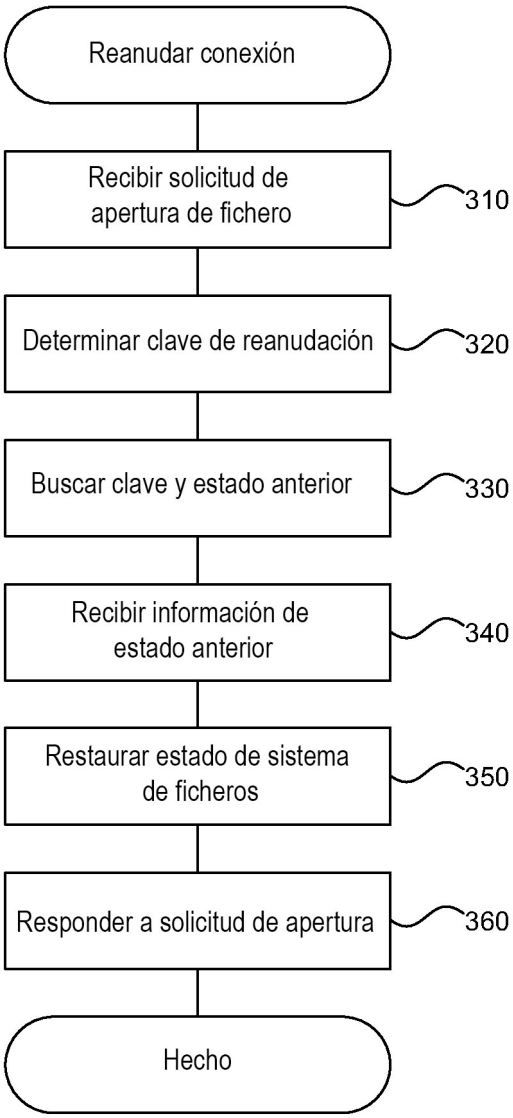
Reanudar conexión
Recibir solicitud de apertura de fichero
310
Determinar clave de reanudación
320
Buscar clave y estado anterior
330
Recibir información de estado anterior
340
Restaurar estado de sistema de ficheros
350
Responder a solicitud de apertura
360
Hecho

FIG. 3

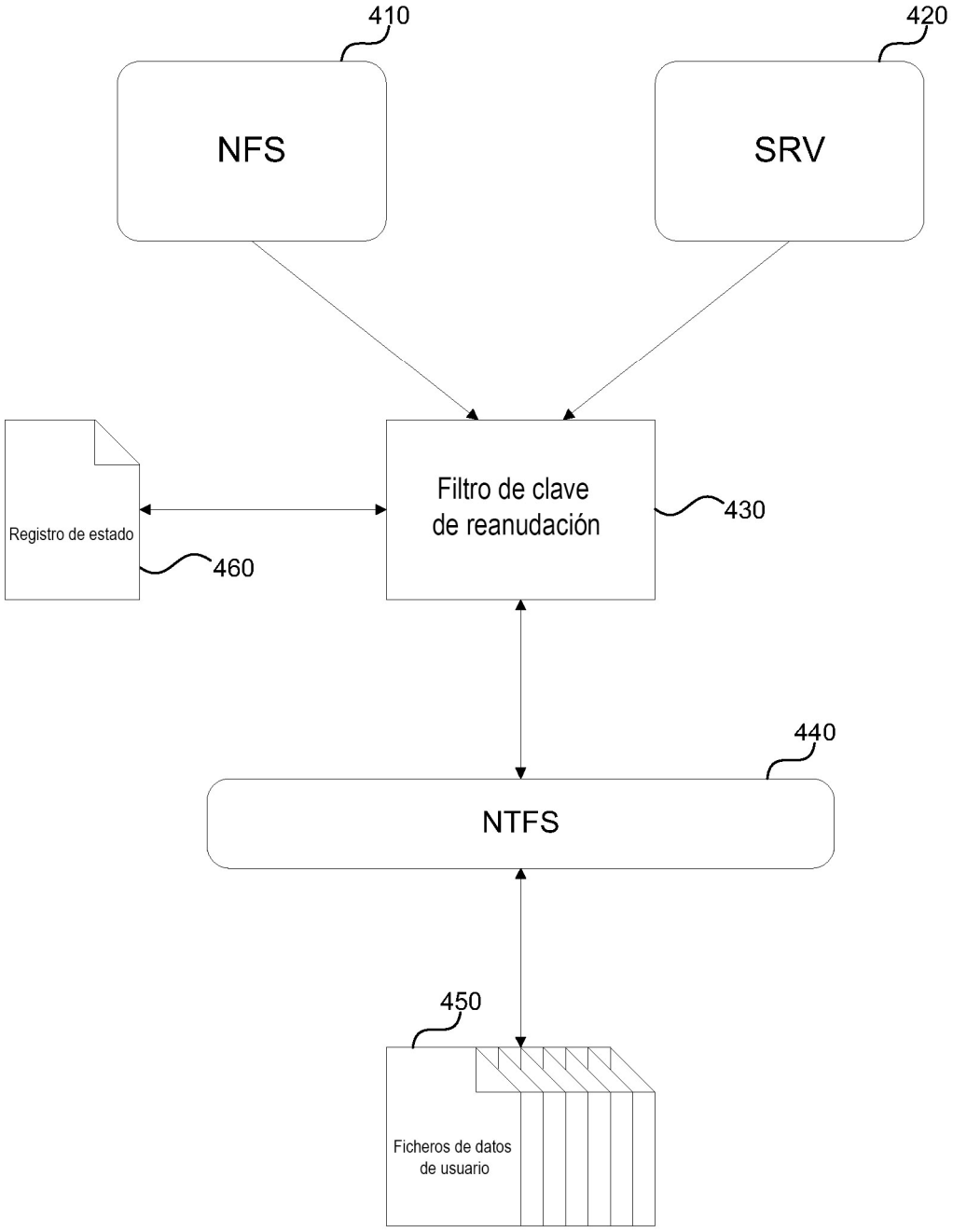
410
420
NFS
SRV
Registro de estado
460
Filtro de clave
de reanudación
430
440
NTFS
450
Ficheros de datos
de usuario

FIG. 4