(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 672 938**

(51) Int. CI.:

***H04L 29/06*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.04.2013 PCT/US2013/038555**

(87) Fecha y número de publicación internacional: **07.11.2013 WO13165859**

(96) Fecha de presentación y número de la solicitud europea: **29.04.2013 E 13722908 (4)**

(97) Fecha y número de publicación de la concesión europea: **18.04.2018 EP 2845364**

(54) Título: **Conexión basada en certificado a una máquina virtual en la nube**

(30) Prioridad:

**02.05.2012 US 201213462223**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**18.06.2018**

(73) Titular/es:

**MICROSOFT TECHNOLOGY LICENSING, LLC (100.0%)**
**One Microsoft Way**
**Redmond, Washington 98052-6399, US**

(72) Inventor/es:

**WRIGHT, ERON D.;**
**AZAD, MUHAMMAD UMER;**
**REWASKAR, SUSHANT P .;**
**SANDERS, COREY M. y**
**SYED, SAAD**

(74) Agente/Representante:

**CARPINTERO LÓPEZ, Mario**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

## DESCRIPCIÓN

Conexión basada en certificado a una máquina virtual en la nube

### Antecedentes

La virtualización de los sistemas de computación ha permitido la configuración y el mantenimiento flexibles y convenientes de los sistemas de computación. Un sistema de computación se virtualiza al hacer que una máquina virtual opere de forma remota desde el sistema de computación cliente al que sirve la máquina virtual. La máquina virtual emula la lógica de un sistema de computación totalmente operativo que incluye el sistema operativo, sus diversas aplicaciones y configuraciones correspondientes, y se comunica con el usuario a través de un sistema de computación de cliente ubicado remotamente. Por ejemplo, la máquina virtual recibe una entrada de cliente remoto y proporciona de retorno la información resultante de la imagen del escritorio al cliente. El cliente no opera el sistema operativo correspondiente, sino que simplemente recibe la entrada de usuario, retransmite dicha entrada de usuario a la máquina virtual y representa el escritorio utilizando la imagen de escritorio resultante proporcionada por la máquina virtual.

Las máquinas virtuales se han implementado más recientemente en entornos de computación en la nube . La "computación en la nube " es un modelo que permite el acceso a la red ubicuo, conveniente y bajo demanda a una agrupación compartida de recursos de computación configurables (por ejemplo, redes, host, almacenamiento, aplicaciones y servicios). La agrupación compartida de recursos de computación configurables puede ser proporcionada rápidamente a través de la virtualización y ser liberada con un bajo esfuerzo de gestión o interacción del proveedor de servicios, y a continuación, ser escalada consecuentemente . Un modelo de computación en la nube puede estar compuesto de varias características (por ejemplo, autoservicio bajo demanda, amplio acceso a la red, agrupación de recursos, elasticidad rápida, servicio medido, etc.), modelos de servicio (por ejemplo, Software como Servicio ("SaaS") , Plataforma como Servicio ("PaaS"), Infraestructura como Servicio ("IaaS") y modelos de implementación (por ejemplo, nube privada, nube comunitaria, nube pública, nube híbrida, etc.).

El documento US 2011/0246765 A1 se refiere a proporcionar servicios de identidad criptográfica, distribuidos y seguros en apoyo de transacciones electrónicas de datos que requieren autenticación de individuos. Una Nube de Ecosistema de Identidad (IEC) proporciona servicios de identidad criptográfica global, escalable y basado en la nube como mecanismo de aseguramiento de la identidad para otros servicios, tales como almacenamiento de datos, servicios web y motores de comercio electrónico. La IEC complementa estos otros servicios al proporcionar protección y autenticación de identidad mejorada. Una IEC realiza servicios de identidad usando certificados digitales subrogados que tienen claves de cifrado que nunca están expuestas al público. Un individuo que solicita otros servicios debe cumplir con un desafío de identidad antes de que se le otorgue acceso a estos otros servicios. Las solicitudes de servicio a la IEC y las respuestas de la IEC están cifradas de forma segura. Una IEC se integra suavemente en los servicios existentes al superponerse o utilizarse junto con las medidas de seguridad existentes.

El documento EP 2 278 514 A1 se refiere a el campo de las máquinas virtuales seguras. La técnica descrita para configurar máquinas virtuales seguras comprende arrancar un procesador con una imagen de administrador de zona, obtener en el procesador un primer par de claves pública / privada asociadas con la sesión de administrador de zona, certificar la clave pública del primer par de claves pública / privada en el procesador con una clave privada asociada al procesador, recibir en el administrador de zona un comando de instanciación de máquina virtual segura, crear entre el administrador de zona y el usuario un canal de comunicación seguro, producir un segundo par de claves pública / privada asociadas con la máquina virtual segura y certificar la clave pública del segundo par de claves pública / privada con la clave privada del primer par de claves pública / privada.

### Breve sumario

El objeto de la presente invención es simplificar la autenticación para clientes. Este objeto se resuelve por el asunto sujeto de las reivindicaciones independientes. Las realizaciones preferidas están definidas por las reivindicaciones dependientes.

Al menos una realización que se describe en la presente memoria descriptiva se refiere a un sistema en el que un sistema de computación host ejecuta máquinas virtuales, y un canal de computación en la nube que acopla comunicativamente el ordenador host a un sistema de computación cliente que está asignado a una de las máquinas virtuales. En algunas realizaciones, el canal de computación en la nube existe para proporcionar seguridad de extremo a extremo entre el sistema de computación cliente y el sistema de computación del ordenador host. Usando los principios que se describen en la presente memoria descriptiva, dicha seguridad de extremo a extremo puede extenderse desde el sistema de computación cliente hasta la máquina virtual correspondiente que se ejecuta en nombre del cliente.

La máquina virtual está configurada para generar un certificado, instalar el certificado en la máquina virtual y devolver una representación de certificado al cliente. Por ejemplo, esto puede ocurrir cuando se aprovisiona la máquina

virtual. Durante una solicitud de conexión posterior del cliente a la máquina virtual, la máquina virtual devuelve el certificado al cliente. El cliente compara la representación de certificado que se ha devuelto durante el aprovisionamiento con el certificado que se ha devuelto durante la conexión posterior, y si hay una coincidencia, la máquina virtual es autenticada para el cliente. Por lo tanto, en este caso, la máquina virtual se autentica sin que el cliente tenga que generar e instalar un certificado, simplificando el proceso para el cliente.

Este sumario no pretende identificar las características clave o las características esenciales de la materia reivindicada, ni está destinado a ser utilizado como una ayuda para determinar el alcance de la materia objeto reivindicada.

**Breve descripción de los dibujos**

Con el fin de describir la manera con la que se pueden obtener las ventajas y características que se han mencionado más arriba y otras, se hará una descripción más particular de varias realizaciones por medio de referencia a los dibujos adjuntos. Con el entendimiento de que estos dibujos representan solo realizaciones de muestra y, por lo tanto, no se deben considerar limitantes del alcance de la invención, las realizaciones se describirán y explicarán con especificidad y detalle adicionales mediante el uso de los dibujos adjuntos en los que:

la figura 1 ilustra un sistema de computación en el que se pueden emplear algunas realizaciones que se describen en la presente memoria descriptiva;

la figura 2 ilustra un sistema que es un entorno operativo en el que un sistema de computación cliente provisiona y se conecta a una máquina virtual que está alojada por un sistema de computación host en un entorno de computación en la nube , de manera que el cliente pueda operar posteriormente la máquina virtual;

la figura 3 ilustra un ejemplo de un entorno de computación en la nube 200 y representa un ejemplo del entorno de computación en la nube de la figura 2;

la figura 4 ilustra un diagrama de flujo de un procedimiento para que un sistema de computación cliente se conecte a una máquina virtual;

la figura 5 ilustra un entorno en el que una máquina virtual puede ser instanciada, aprovisionada y operada; y

la figura 6 ilustra un diagrama de flujo de un procedimiento 600 que aprovisiona una máquina virtual cuando se arranca la máquina virtual desde una imagen de máquina virtual generalizada.

**Descripción detallada**

De acuerdo con las realizaciones que se describen en la presente memoria descriptiva, un sistema de computación cliente autentica una máquina virtual a la que está asignado sin tener que generar e instalar un certificado. En primer lugar, se describirá una explicación introductoria sobre los sistemas de computación con respecto a la figura 1. A continuación, se describirán las realizaciones de la autenticación con respecto a las figuras 2 a 6.

Los sistemas de computación ahora están tomando cada vez más una gran variedad de formas. Los sistemas de computación pueden ser, por ejemplo, dispositivos portátiles, dispositivos eléctricos, ordenadores portátiles, ordenadores de escritorio, ordenadores centrales, sistemas de computación distribuidos o incluso dispositivos que tradicionalmente no se han considerado un sistema de computación. En esta descripción y en las reivindicaciones, el término "sistema de computación" se define ampliamente de manera que incluya cualquier dispositivo o sistema (o una combinación de los mismos) que incluye al menos un procesador físico y tangible, y una memoria física y tangible capaz de tener en la misma instrucciones ejecutables por ordenador que pueden ser ejecutadas por el procesador. La memoria puede tomar cualquier forma y puede depender de la naturaleza y la forma del sistema de computación. Un sistema de computación puede estar distribuido en un entorno de red y puede incluir múltiples sistemas de computación constituyentes.

Como se ilustra en la figura 1, en su configuración más básica, un sistema de computación 100 incluye típicamente al menos una unidad de procesamiento 102 y una memoria 104. La memoria 104 puede ser una memoria física del sistema, que puede ser volátil, no volátil o alguna combinación de los dos. El término "memoria" también se puede usar en la presente memoria descriptiva para referirse al almacenamiento masivo no volátil tal como medios físicos de almacenamiento. Si el sistema de computación está distribuido, el procesamiento, la memoria y / o la capacidad de almacenamiento también pueden estar distribuidos . Tal como se usa en la presente memoria descriptiva, el término "módulo" o "componente" puede referirse a objetos o rutinas de software que se ejecutan en el sistema de computación. Los diferentes componentes, módulos, motores y servicios que se describen en la presente memoria descriptiva pueden ser implementados como objetos o procesos que se ejecutan en el sistema de computación (por ejemplo, como hilos de ejecución separados).

En la descripción que sigue, las realizaciones se describen con referencia a acciones que son ejecutados por uno o más sistemas de computación. Si tales acciones son implementados en software, uno o más procesadores del sistema de computación asociado que realiza la acción dirigen la operación del sistema de computación en respuesta a la ejecución de instrucciones ejecutables por ordenador. Un ejemplo de una operación de este tipo implica la manipulación de datos. Las instrucciones ejecutables por ordenador (y los datos manipulados) pueden ser almacenados en la memoria 104 del sistema de computación 100. El sistema de computación 100 también puede contener canales de comunicación 108 que permiten que el sistema de computación 100 se comunique con otros procesadores de mensaje , por ejemplo, sobre la red 110.

Las realizaciones que se describen en la presente memoria descriptiva pueden comprender o utilizar un ordenador de propósito especial o de propósito general que incluye hardware de ordenador, tal como, por ejemplo, uno o más procesadores y memoria del sistema, como se explicará con mayor detalle a continuación. Las realizaciones que se describen en la presente memoria descriptiva también incluyen medios físicos y otros medios legibles por ordenador para transportar o almacenar instrucciones ejecutables por ordenador y / o estructuras de datos. Tales medios legibles por ordenador pueden ser cualesquiera medios disponibles a los que se pueda acceder mediante un sistema de computación de propósito general o de propósito especial. Los medios legibles por ordenador que almacenan las instrucciones ejecutables por ordenador son medios físicos de almacenamiento. Los medios legibles por ordenador que tienen instrucciones ejecutables por ordenador son medios de transmisión. Por lo tanto, a modo de ejemplo y no de limitación, las realizaciones de la invención pueden comprender al menos dos tipos distintos de medios legibles por ordenador: medios de almacenamiento de ordenador y medios de transmisión.

Los medios de almacenamiento de ordenador incluyen RAM, ROM, EEPROM, CD-ROM u otro almacenamiento en disco óptico, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético o cualesquiera otros medios que puedan ser utilizados para almacenar los códigos de programa deseados en forma de instrucciones ejecutables por ordenador o estructuras de datos a las que se puede acceder mediante un ordenador de propósito general o especial.

Una "red" se define como uno o más enlaces de datos que permiten el transporte de datos electrónicos entre sistemas de ordenadores y / o módulos y / u otros dispositivos electrónicos. Cuando la información se transfiere o se proporciona a través de una red u otra conexión de comunicaciones (ya sea cableada, inalámbrica o una combinación de cableada o inalámbrica) a un ordenador, el ordenador visualiza apropiadamente la conexión como un medios de transmisión. Los medios de transmisión pueden incluir una red y / o enlaces de datos que pueden ser usados para transportar medios de código de programa deseados en forma de instrucciones ejecutables por ordenador o estructuras de datos y a los que se puede acceder por medio de un ordenador de propósito general o de propósito especial. Las combinaciones de lo anterior también deben estar incluidas dentro del alcance de los medios legibles por ordenador.

Además, cuando se alcanzan diversos componentes del sistema de ordenador, los medios de código de programa en forma de instrucciones ejecutables por ordenador o estructuras de datos pueden transferirse automáticamente desde los medios de transmisión a los medios de almacenamiento de ordenador (o viceversa). Por ejemplo, las instrucciones ejecutables por ordenador o estructuras de datos recibidas a través de una red o enlace de datos pueden ser almacenadas en memoria RAM dentro de un módulo de interfaz de red (por ejemplo, una "NIC") y a continuación ser transferidas eventualmente a la RAM del sistema de ordenador y / o a medios de almacenamiento de ordenador menos volátiles en un sistema de ordenador. Por lo tanto, se debe entender que los medios de almacenamiento de ordenador se pueden incluir en los componentes del sistema de ordenador que también (o incluso principalmente) utilizan medios de transmisión.

Las instrucciones ejecutables por ordenador comprenden, por ejemplo, instrucciones y datos que, cuando se ejecutan en un procesador, provocan que un ordenador de propósito general, un ordenador de propósito especial o un dispositivo de procesamiento de propósito especial realice una determinada función o grupo de funciones. Las instrucciones ejecutables por el ordenador pueden ser, por ejemplo, instrucciones binarias, de formato intermedio como el lenguaje ensamblador o incluso el código fuente. Aunque el tema se ha descrito en un lenguaje específico para las características estructurales y / o las acciones metodológicos, se debe entender que el tema definido en las reivindicaciones adjuntas no está limitado necesariamente a las características o acciones que se han descrito más arriba. Más bien, las características y acciones se describen como formas ejemplares de implementación de las reivindicaciones.

Los expertos en la materia apreciarán que la invención puede ser practicada en entornos de computación en red con muchos tipos de configuraciones de sistemas de ordenadores, que incluyen ordenadores personales, ordenadores de escritorio, ordenadores portátiles, procesadores de mensajes, dispositivos portátiles, sistemas multiprocesadores, productos electrónicos de consumo programables o basados en microprocesador , PC en red, miniordenadores, ordenadores centrales, teléfonos móviles, PDA, buscapersonas, enrutadores, conmutadores y otros similares. La invención también puede ser practicada en entornos de sistemas distribuidos en los que los sistemas de ordenadores locales y remotos, que están enlazados (ya sea mediante enlaces de datos cableados, enlaces de datos inalámbricos o mediante una combinación de enlaces de datos cableados e inalámbricos) a través de una red, realizan

ambas tareas. En un entorno de sistema distribuido, los módulos de programa pueden ubicarse en dispositivos de almacenamiento de memoria tanto locales como remotos.

La figura 2 ilustra un sistema 200 que es un entorno operativo en el que un sistema de computación cliente 201 aprovisiona y se conecta a una máquina virtual (por ejemplo, la máquina virtual 211A) que está alojada en un sistema de ordenador host 210 dentro de un entorno de computación en la nube 203, de manera que el cliente 201 puede operar posteriormente la máquina virtual 211A. El sistema de computación cliente 201 puede estar estructurado como se ha descrito más arriba para el sistema de computación 100 de la figura 1, y también en lo sucesivo se denominará simplemente "cliente 201". El sistema de computación host 210 también puede ser estructurado como se ha descrito más arriba para el sistema de computación 100 de la figura 1, y también en lo sucesivo se denominará simplemente "host 210". Si bien los principios que se describen en la presente memoria descriptiva se refieren principalmente a los procedimientos previos a la operación de aprovisionamiento y conexión inicial, a continuación se describirá una breve nota sobre el funcionamiento de la máquina virtual.

Durante la operación, la máquina virtual 211A emula un sistema de computación totalmente operativo que incluye al menos un sistema operativo, y quizás también una o más aplicaciones adicionales. La máquina virtual genera una imagen de escritorio u otras instrucciones de representación que representan un estado actual del escritorio, y a continuación transmite la imagen o las instrucciones al cliente para la representación del escritorio. A medida que el usuario interactúa con el escritorio, las entradas del usuario son transmitidas a la máquina virtual. La máquina virtual procesa las entradas del usuario y, si corresponde, cambia el estado del escritorio. Si un cambio de este tipo en el estado del escritorio produce un cambio en el escritorio representado, entonces la máquina virtual altera las instrucciones de imagen o representación, si corresponde, y transmite la imagen modificada o las instrucciones procesadas al sistema de computación cliente para una representación adecuada. Desde la perspectiva del usuario, es como si el sistema de computación cliente estuviera realizando el procesamiento en el escritorio.

Como se ha mencionado previamente, el ordenador host 210 opera en un entorno de computación en la nube . En esta descripción y en las afirmaciones que siguen , la "computación en la nube " se define como un modelo para permitir un acceso a la red ubicuo, conveniente bajo demanda a un conjunto compartido de recursos de computación configurables (por ejemplo, redes, host, almacenamiento, aplicaciones y servicios) . El conjunto compartido de recursos de computación configurables se puede aprovisionar rápidamente a través de la virtualización y liberarse con un bajo esfuerzo de gestión o interacción del proveedor de servicios, y a continuación ser escalado en consecuencia. Un modelo de computación en la nube puede estar compuesto de varias características (por ejemplo, autoservicio bajo demanda, amplio acceso a la red, agrupación de recursos, elasticidad rápida, servicio medido, etc.), modelos de servicio (por ejemplo, Software como Servicio ("SaaS") , Plataforma como Servicio ("PaaS"), Infraestructura como Servicio ("IaaS") y modelos de implementación (por ejemplo, nube privada, nube comunitaria, nube pública, nube híbrida, etc.). En esta descripción y en las reivindicaciones , un "entorno de computación en la nube " es un entorno en el que se emplea la computación en la nube .

El ordenador host 210 es capaz de alojar varias máquinas virtuales 211, y es típicamente una única máquina física con recursos de procesamiento, memoria, almacenamiento y redes. En el ejemplo que se ilustra, el ordenador host 210 ejecuta las máquinas virtuales 211A y 211B, aunque las elipses 211C representan que los principios que se describen en la presente memoria descriptiva no están limitados al número de máquinas virtuales ejecutadas en el ordenador host.

El sistema 200 también incluye un canal de computación en la nube 202 que acopla comunicativamente el ordenador host 210 al cliente 201. El canal de computación en la nube 202 tiene las características de: 1) puede conectarse a una entidad tal como el cliente 201 fuera del entorno de computación en la nube 203; 2) es accesible para el ordenador host 210; y 3) proporciona cierto nivel de seguridad de identidad con respecto a las identidades de las partes conectadas directamente a cada extremo del canal de computación en la nube 202. Por lo tanto, por la simple actuación de poder comunicarse directamente a través del canal de computación en la nube 202, el cliente 201 puede autenticar el ordenador host 210, y el ordenador host 210 puede autenticar el cliente 201. Sin embargo, sin procesamiento adicional, el cliente 201 aún no ha autenticado la máquina virtual 211A, y la máquina virtual 211A todavía no ha autenticado al cliente 201.

La figura 3 ilustra un ejemplo del entorno de computación en la nube 300. En este ejemplo, el sistema de computación host 302A es un ejemplo del ordenador host central 210 de la figura 2, y es solo uno entre varios host 302 dentro del entorno de computación en la nube 300. Por ejemplo, aunque se ilustran tres host 302A, 302B y 302C, las elipses 302D representan que puede haber cualquier número de host dentro del entorno de computación en la nube 300.

Las máquinas virtuales 311 son ejemplos de las máquinas virtuales 211 de la figura 2. Las máquinas virtuales son creadas en este entorno de computación en la nube a partir de imágenes de máquina virtual 312 que están contenidas dentro de un servicio de almacenamiento 301. Un servicio de control 303 coordina los diversos servicios dentro del entorno de computación en la nube 300 que incluye proporcionar un canal de computación en la nube seguro

entre los host (tales como el ordenador host 302A) y los clientes (tales como el cliente 201) que están asignados a las diversas máquinas virtuales (tales como la máquina virtual 311A) dentro de los host.

La figura 4 ilustra un diagrama de flujo de un procedimiento 400 para que un sistema de computación cliente se conecte a una máquina virtual. En una realización, ese sistema de computación cliente es el cliente 201 de la figura 1, y la máquina virtual es la máquina virtual 211A de la figura 2. En consecuencia, puesto que el procedimiento 400 puede realizarse en el contexto del sistema 200 de la figura 2, el procedimiento 400 de la figura 4 se describirá a continuación con referencia frecuente al sistema 200 de la figura 2.

En la figura 4, algunos de las acciones ilustrados son realizados por el cliente (por ejemplo, el cliente 201) como se representa en la columna izquierda de la figura 4 bajo el encabezado "CLIENTE". Otros de las acciones ilustradas son realizadas por la máquina virtual (por ejemplo, la máquina virtual 211A) como se representa en la columna derecha de la figura 4 bajo el encabezado "VM". Otras de las acciones ilustradas son realizadas por el ordenador host (por ejemplo, el ordenador host 210) tal como se representa en la columna central de la figura 4 bajo el título "HOST". El procedimiento 400 incluye una primera fase de comunicación de ida y retorno 401 en la que se aprovisiona la máquina virtual, asignada al cliente y el cliente recibe una primera representación de certificado. El procedimiento 400 también incluye una segunda fase de comunicación de ida y retorno 402 en la que el cliente realiza una solicitud de conexión inicial a la máquina virtual, y la máquina virtual responde con una segunda representación de certificado. El procedimiento 400 incluye una fase de decisión de autenticación 403 en la que el cliente decide si autentica la máquina virtual dependiendo de las representaciones del certificado.

El procedimiento 400 comienza con una solicitud para aprovisionar una máquina virtual para un cliente (actuación 411). Por ejemplo, en la figura 2, la máquina virtual 211A puede ejemplificarse y aprovisionarse para ser asignada al cliente 201. Aunque esta acción se ilustra en la columna izquierda de la figura 4, esta solicitud de aprovisionamiento inicial no necesita ser realizada por el cliente 201, sino que puede ser realizada por un tercero, como, por ejemplo, un administrador que tiene la responsabilidad de aprovisionar máquinas virtuales para una organización a la que pertenece el usuario cliente 201. Sin embargo, la solicitud de aprovisionamiento puede ser realizada alternativamente por el cliente 201.

Se hace notar que en esta etapa, la máquina virtual 211A aún no existe, e incluso la identidad del sistema de computación host en el que se creará la máquina virtual puede no estar predeterminada (si hay múltiples candidatos potenciales de host dentro del entorno de computación para la máquina virtual). Por ejemplo, en el entorno de computación en la nube 300 de la figura 3, la solicitud de aprovisionamiento de la máquina virtual puede ser realizada al servicio de control 303, que decide qué host 302 ejemplificará la máquina virtual. En este caso, se supone que el servicio de control 303 ha seleccionado el ordenador host 302A como el más adecuado para ejecutar la máquina virtual. La solicitud de aprovisionamiento puede transmitirse entonces (quizás directamente, o quizás con alguna alteración) al host 302A. En el contexto de la figura 2, el ordenador host 210 recibe la solicitud de aprovisionamiento.

El ordenador host hace entonces que la máquina virtual sea instanciada desde una imagen de máquina virtual (actuación 421) y proporciona provisiones adicionales a la máquina virtual. Por ejemplo, en la figura 2, se supone que el ordenador host 210 instancia la máquina virtual 211A para el cliente 201. En la figura 3, se supone que el ordenador host 302A instancia la máquina virtual 311A para el cliente usando una de las imágenes de la máquina virtual 312 dentro del servicio de almacenamiento 301 .

A medida que la máquina virtual se arranca, como parte del proceso de arranque, la máquina virtual genera un certificado (actuación 431) (en la presente memoria descriptiva y en lo que sigue también denominada "certificado de máquina virtual"), instala el certificado en la máquina virtual (actuación 432), y proporciona una primera representación de certificado del certificado de máquina virtual al cliente (actuación 433). Si bien esta representación de certificado podría ser una copia del certificado de la máquina virtual, también podría ser un hash del certificado de máquina virtual. Sin embargo, un hash podría facilitar la transferencia y la comparación del certificado de la máquina virtual. En una realización, el hash es una "huella digital", que es el propio hash, utilizado como una forma abreviada de la clave pública de un certificado.

En una realización, la generación del certificado de máquina virtual (actuación 431), la instalación del certificado de máquina virtual (actuación 432) y la provisión de una primera representación de certificado del certificado de la máquina virtual hacia el cliente (actuación 433) pueden ser realizados ejecutando un agente de aprovisionamiento en la máquina virtual. Aunque no es obligatorio, este agente de aprovisionamiento puede no estar presente en la imagen de la máquina virtual desde la cual se instancia la máquina virtual, y tal vez puede haber sido adquirida por la máquina virtual durante el arranque de la máquina virtual. Este caso se describirá más adelante con respecto a la figura 5.

Una vez que el ordenador host recibe la primera representación de certificado, el ordenador host proporciona la primera representación de certificado al cliente (actuación 422). Por ejemplo, en la figura 2, el ordenador host 210 puede recibir la primera representación de certificado del certificado instalado en la máquina virtual 211A, y proporcionar la primera representación de certificado al cliente 201 a través del canal de computación en la nube 202. En la

figura 3, el ordenador host 302A puede recibir la primera representación de certificado del certificado instalado en la máquina virtual 311a, y proporcionar la primera representación de certificado al cliente a través del servicio de control 303. Esto completa la primera fase de comunicación de ida y retorno 401.

El cliente recibe la primera representación de certificado de la máquina virtual a través del ordenador host (actuación 412). A continuación, el cliente realiza una solicitud de conexión de máquina virtual inicial y envía la solicitud a la máquina virtual (actuación 413). En una realización, esta solicitud de conexión inicial se realiza usando un protocolo que hace que la máquina virtual devuelva automáticamente una segunda representación de certificado del certificado de máquina virtual hacia el cliente. La segunda representación de certificado podría ser, por ejemplo, un hash o una copia del certificado de máquina virtual. Un ejemplo de un protocolo convencional de este tipo es el protocolo de Protocolo de Escritorio Remoto (RDP). Sin embargo, los principios que se describen en la presente memoria descriptiva no están limitados a este protocolo de RDP, o incluso a ningún protocolo existente, ya que en el futuro se pueden desarrollar nuevos protocolos que tengan esta característica. El ordenador host a continuación proporciona la solicitud de conexión inicial a la máquina virtual (actuación 423).

La máquina virtual a continuación recibe la solicitud de conexión inicial (actuación 434). En la presente solicitud inicial se pueden incluir credenciales de cliente y / o usuario que permiten al usuario y / o cliente autenticarse en la máquina virtual. No obstante, se debe tener en cuenta en este punto que la máquina virtual todavía no se ha autenticado al cliente en respuesta a esta solicitud de conexión inicial. Para facilitar que el cliente autentique la máquina virtual, la máquina virtual responde a la solicitud de conexión inicial enviando una segunda representación de certificado del certificado de la máquina virtual al cliente (actuación 435). Esta segunda representación podría ser nuevamente una representación de certificado como, por ejemplo, un hash o una copia del certificado de máquina virtual. Si se usa el protocolo RDP, la máquina virtual normalmente devolverá una copia del certificado de la máquina virtual.

El ordenador host envía (o retransmite) entonces la segunda representación de certificado al cliente (actuación 424). El cliente recibe entonces la segunda representación de certificado del certificado de máquina virtual (actuación 414), completando así la segunda fase de comunicación de ida y retorno 402. Como un ejemplo, en la figura 2, esta segunda fase de comunicación de ida y retorno 402 se produce entre el cliente 201 y la máquina virtual 211A. En la figura 3, esta segunda fase 402 de comunicación de ida y retorno se produce entre el cliente (no mostrado) y la máquina virtual 311A. Esto permite que el cliente realice la fase de decisión de autenticación 403.

Con el fin de que el cliente decida si autentica la máquina virtual, el cliente compara la primera representación de certificado (devuelta al cliente como resultado de la primera fase de comunicación de ida y retorno 401) con la segunda representación de certificado (devuelta al cliente como un resultado de la segunda fase de comunicación de ida y retorno 402). Por ejemplo, si la primera representación de certificado era un hash del certificado de la máquina virtual, y la segunda representación de certificado era una copia del certificado de la máquina virtual, el cliente verificaría la segunda representación de certificado y comprobaría si se había llegado al mismo valor hash.

Si no hay una coincidencia de las representaciones de certificado primero y segundo ("No" en el bloque de decisión 416), entonces el cliente no autentica la máquina virtual (actuación 417), y por lo tanto no puede confiar en que la parte con la que el cliente se está comunicando sea realmente la máquina virtual asignada al cliente. Si, por otro lado, hay una coincidencia de las representaciones de certificado primero y segundo ("Sí" en el bloque de decisión 416), entonces el cliente autentica la máquina virtual (actuación 418), y por lo tanto puede confiar en que la parte con la que el cliente se está comunicando es realmente la máquina virtual asignada al cliente y, por lo tanto, puede operar con confianza con la máquina virtual.

Como se ha mencionado más arriba, la máquina virtual puede realizar la generación e instalación del certificado de la máquina virtual, y proporcionar la primera representación de certificado al cliente utilizando un agente de aprovisionamiento. Este agente de aprovisionamiento también puede ayudar en otras funciones, tales como informar al usuario sobre el estado del proceso de aprovisionamiento. Más acerca de esto se describirá a continuación con respecto a las figuras 5 y 6.

La figura 5 ilustra un entorno 500 en el que una máquina virtual 501 puede ser instanciada, aprovisionada y operada. El entorno 500 representa un ejemplo del sistema de computación central 302A de la figura 3, y la máquina virtual 501 es un ejemplo de la máquina virtual 211A de la figura 2, y la máquina virtual 311A de la figura 3. El entorno 500 también incluye unos medios de almacenamiento virtual 502 a los cuales puede estar conectada la máquina virtual 501 para acceder a los datos en los medios de almacenamiento virtual 502. Los medios de almacenamiento virtual incluyen instrucciones de arranque 511 ejecutables por ordenador que se ejecutan en el momento del arranque de la máquina virtual 511.

Los medios de almacenamiento virtual 502 incluyen el contenido 512 que se hace accesible a la máquina virtual 501 en respuesta a la ejecución de las instrucciones de arranque 511 ejecutables por ordenador. La ejecución de las instrucciones de arranque 511 ejecutables por ordenador también permite que la máquina virtual 501 acceda al contenido 512 de los medios de almacenamiento virtual 502 tal como los datos de aprovisionamiento 521 y un agente de aprovisionamiento 522.

Los datos de aprovisionamiento 521 incluyen datos que pueden ser utilizados por la máquina virtual para establecer información específica del usuario y específica de la máquina dentro de la máquina virtual 501 con el fin de especializar la máquina virtual 501 hacia un usuario o máquina particular. Por lo tanto, aunque la máquina virtual 501 es arrancada desde una imagen de máquina virtual generalizada, la máquina virtual 501 termina siendo especializada para un usuario y una máquina en particular. Por lo tanto, los datos de aprovisionamiento 521 ayudan a aprovisionar la máquina virtual 501. En una realización, los datos de aprovisionamiento pueden ser un archivo de respuesta, que es utilizado por la máquina virtual durante la fase de especialización de la instalación.

El agente de aprovisionamiento 522 representa un código ejecutable por ordenador al que se puede acceder (en respuesta a la ejecución de las instrucciones de arranque 511ejecutables por el ordenador ) y se ejecuta para realizar tareas relacionadas con el aprovisionamiento de la máquina virtual 501. Por ejemplo, el agente de aprovisionamiento puede supervisar el progreso del proceso de aprovisionamiento y / o informar sobre el mismo, y puede generar el certificado de máquina virtual (actuación 431), instalar el certificado de máquina virtual en sí mismo (actuación 432) y despachar la primera representación de certificado del certificado de máquina virtual hacia el cliente (actuación 433).

La figura 6 ilustra un diagrama de flujo de un procedimiento 600 para aprovisionar una máquina virtual cuando se arranca la máquina virtual desde una imagen de máquina virtual generalizada. El procedimiento 600 es iniciado con el arranque de inicio de la máquina virtual (actuación 601). Esto implica crear una instancia de máquina virtual basada en una imagen de máquina virtual generalizada. Además, la instancia de la máquina virtual se completará parcialmente con parámetros que no son específicos del usuario y / o de la máquina que se debe asignar a la máquina virtual.

En este estado, la máquina virtual contiene instrucciones de arranque ejecutables . Por ejemplo, en la figura 5, la máquina virtual 501 incluye las instrucciones de arranque 511 ejecutables por ordenador. Estas instrucciones de arranque ejecutables por ordenador se ejecutan a continuación (actuación 602).

La ejecución de las instrucciones de arranque ejecutables por ordenador hace que la máquina virtual detecte los medios de almacenamiento virtual a los que puede acceder la máquina virtual (actuación 603). Por ejemplo, con referencia a la figura 5, la máquina virtual 501 ejecuta las instrucciones de arranque 511 ejecutables por ordenador , haciendo que la máquina virtual 501 detecte y pueda acceder a los medios de almacenamiento virtual 502, como se representa por la línea 531. Los medios de almacenamiento virtual son presentados por un hipervisor que abstrae los medios físicos de almacenamiento subyacentes. Cuando se arranca un sistema de computación, uno de los procesos que realizan algunos sistemas operativos es descubrir los dispositivos conectados. Puede ser este proceso el que descubra el dispositivo de almacenamiento virtual. En algunas realizaciones, estos medios de almacenamiento virtual pueden ser, por ejemplo, una unidad de DVD virtual.

Una vez que la máquina virtual detecta el dispositivo de almacenamiento virtual, la máquina virtual tiene acceso al menos a parte del contenido del dispositivo de almacenamiento virtual. Por ejemplo, en la figura 5, la máquina virtual 501 es capaz de acceder al contenido 512 de los medios de almacenamiento virtual 502 por la ejecución de las instrucciones de arranque 511 ejecutables por ordenador representadas por la línea 532. En este punto, la máquina virtual puede adquirir tanto los datos de aprovisionamiento (actuación 611) como el agente de aprovisionamiento (actuación 621) desde los medios de almacenamiento virtual. Por ejemplo, en la figura 5, la máquina virtual 501 adquiere los datos de aprovisionamiento 521 y el agente de aprovisionamiento 522 de los medios de almacenamiento virtual 502.

Como ejemplo, los datos de aprovisionamiento pueden ser un archivo de respuesta. Los archivos de respuesta se utilizan convencionalmente para realizar la fase de especialización de la instalación del sistema operativo en un sistema de computación físico. Durante la instalación de un sistema operativo en un sistema de computación físico, hay dos fases; es decir, una fase de copia y una fase de especialización. Durante la fase de copia, los archivos se copian en el sistema de computación físico. Durante la fase de especialización, normalmente se consulta al usuario información específica del usuario o específica de la máquina que adaptará el sistema operativo al sistema de computación físico en el que se está instalando el sistema operativo y para el usuario del sistema de computación físico. Sin embargo, se sabe convencionalmente que en lugar de consultar al usuario, la información específica del usuario y de la máquina puede ser proporcionada por otra parte en un archivo de respuesta que sigue un esquema particular. En su lugar, el proceso de instalación puede revisar el archivo de respuesta para obtener respuestas a las preguntas relevantes que normalmente se plantearían al usuario durante la instalación. Los datos de aprovisionamiento pueden incluir, por ejemplo, parámetros tales como, entre otros, nombre de la máquina, cuentas de usuario, configuración de cuentas de usuario, políticas de grupo, contraseña de acceso, zona horaria.

Los datos de aprovisionamiento se utilizan a continuación para aprovisionar la máquina virtual (actuación 612). Por ejemplo, haciendo referencia a la figura 5, la ejecución de las instrucciones de arranque ejecutables por ordenador puede hacer que la máquina virtual 501 consulte los datos de aprovisionamiento 521 (por ejemplo, un archivo de respuesta) para configuraciones específicas del usuario o de la máquina, y configure sus propias configuraciones

con lo mismo, creando así una máquina virtual que está aprovisionada a la máquina y / o usuario específico que está asignado para usar la máquina virtual.

La máquina virtual también puede adquirir el agente de aprovisionamiento de los medios de almacenamiento detectados (actuación 621). Por ejemplo, en la figura 5, la máquina virtual 501 adquiere el agente de aprovisionamiento 522 desde los medios de almacenamiento virtual 502. Esto puede ser realizado por la máquina virtual 501 que ejecuta las instrucciones de arranque 511 ejecutables por ordenador .

El agente de aprovisionamiento representa una colección de instrucciones ejecutables por ordenador que pueden ser ejecutadas por la máquina virtual. La máquina virtual a continuación ejecuta el agente de aprovisionamiento (actuación 622). La máquina virtual también puede monitorizar el progreso de la máquina virtual (actuación 623) e informar el estado del proceso de provisión al cliente (actuación 624). Por ejemplo, en la figura 5, la máquina virtual 501 puede ejecutar el agente de aprovisionamiento 522 en respuesta a la ejecución de las instrucciones de arranque 511 ejecutables por ordenador . Las instrucciones de arranque 511 ejecutables por ordenador y el agente de aprovisionamiento 522 se pueden incorporar individual o colectivamente en unos medios legibles por ordenador, tales como unos medios de almacenamiento del ordenador , como componente de un producto de programa de ordenador.

Por ejemplo, se supone que la máquina virtual que se está aprovisionando es la máquina virtual 311A de la figura 3. El estado del aprovisionamiento de la máquina virtual 311 se puede informar al sistema de computación host 302A, y a continuación al servicio de control 303, y a continuación al usuario. Algunos ejemplos del estado del informe incluyen el éxito o el fracaso del proceso de aprovisionamiento, o quizás un estado de tiempo de espera del proceso de aprovisionamiento (por ejemplo, si el aprovisionamiento se ha demorado, o no, más de un período de tiempo de espera especificado). Los ejemplos de servicios de control 303 incluyen servicios que soportan sistemas de computación en la nube , tales como, por ejemplo, MICROSOFT AZURE.

El agente de aprovisionamiento 522 también podría realizar la generación del certificado de máquina virtual (actuación 431), la instalación del certificado de máquina virtual en la máquina virtual (actuación 432) y la provisión de una primera representación de certificado para el cliente (actuación 433) .

Una vez que se ha completado el aprovisionamiento, o al menos después de que los datos de aprovisionamiento y el agente de aprovisionamiento sean adquiridos del dispositivo de almacenamiento virtual, el dispositivo de almacenamiento virtual puede desconectarse de la máquina virtual (actuación 631), si el dispositivo de almacenamiento virtual no va a ser utilizado para la operación normal por la máquina virtual.

En una realización, el sistema operativo (en lo sucesivo denominado "sistema operativo habilitado para el arranque") de la máquina virtual puede ser de un tipo que tenga instrucciones en tiempo de arranque 511 ejecutables por ordenador que se ejecutan automáticamente durante el arranque para hacer que la máquina virtual adquiera y utilice los datos de aprovisionamiento para aprovisionar la máquina virtual y para adquirir y ejecutar el agente de aprovisionamiento. Un ejemplo de un sistema de computación de este tipo es MICROSOFT WINDOWS.

En una realización, el sistema operativo (en lo sucesivo denominado "sistema operativo no habilitado para el arranque") de la máquina virtual puede ser de un tipo que no tenga tales instrucciones en tiempo de arranque 511 ejecutables por ordenador. Un ejemplo de un sistema operativo de este tipo es LINUX. En este caso, cuando se genera la imagen de máquina virtual generalizada que incluye dicho sistema operativo, las instrucciones en tiempo de arranque 511 ejecutables por ordenador se agregan a la imagen de la máquina virtual generalizada, de manera que estén presentes en la ejecución de la máquina virtual en tiempo de arranque

Por lo tanto, los principios que se describen en la presente memoria descriptiva describen un mecanismo para que un cliente proporcione e inicialmente se conecte a una máquina virtual de manera que el cliente pueda autenticar la máquina virtual cuando se conecta inicialmente. Las realizaciones que se describen deben ser consideradas en todos los aspectos solo como ilustrativas y no restrictivas. El alcance de la invención, por lo tanto, está indicado por las reivindicaciones adjuntas más que por la descripción que antecede.

**REIVINDICACIONES**

1. Un sistema que comprende:

un sistema de computación host configurado para ejecutar una pluralidad de máquinas virtuales (211, 311) en un entorno de computación en la nube ;

un canal de computación en la nube que acopla comunicativamente el sistema de computación host a un sistema de computación cliente asignado a una máquina virtual particular de la pluralidad de máquinas virtuales, en el que el canal de computación en la nube incluye seguridad de identidad con respecto a las identidades de las partes que se comunican a través del canal de computación en la nube ;

en el que la máquina virtual particular está configurada para realizar lo que sigue:

una actuación de generar un certificado;

una actuación de instalar el certificado en la máquina virtual; y

una actuación de proporcionar una primera representación de certificado correspondiente al certificado al sistema de computación host, de manera que el sistema de computación host proporcione la representación de certificado al sistema de computación cliente a través del canal de computación en la nube ; y

en el que la máquina virtual en el entorno de computación en la nube está configurada para responder a una solicitud de conexión inicial desde el sistema de computación cliente con una segunda representación de certificado correspondiente al certificado de manera que el sistema de computación cliente pueda comparar la primera representación de certificado con la segunda representación de certificado.

2. El sistema de la reivindicación 1, en el que la segunda representación de certificado es una copia del certificado.

3. El sistema de la reivindicación 2, en el que la máquina virtual en el entorno de computación en la nube está configurada para recibir también credenciales de autenticación del sistema de computación cliente y autenticar el sistema de computación cliente o el usuario que usa las credenciales de autenticación.

4. El sistema de la reivindicación 2, en el que el sistema de computación cliente está configurado para realizar la solicitud de conexión inicial utilizando un protocolo en el que la máquina virtual está configurada para devolver automáticamente el certificado.

5. El sistema de la reivindicación 1, en el que la máquina virtual en el entorno de computación en la nube contiene instrucciones ejecutables por ordenador que cuando se ejecutan hacen que la máquina virtual realice las acciones de generación del certificado, instale el certificado y proporcione la primera representación de certificado , en el que la máquina virtual está configurada para obtener las instrucciones ejecutables por ordenador durante el tiempo de arranque, aunque no estén implícitas en un sistema operativo de la máquina virtual.

6. El sistema de la reivindicación 5, en el que la máquina virtual en el entorno de computación en la nube está configurada para obtener las instrucciones ejecutables por ordenador durante el arranque de la máquina virtual al estar configurada para realizar lo siguiente:

una actuación de detección de medios de almacenamiento virtual a los que puede acceder la máquina virtual;

una actuación de adquisición de las instrucciones ejecutables por ordenador desde los medios de almacenamiento detectados después de detectar los medios de almacenamiento virtual.

7. El sistema de la reivindicación 1, en el que la primera representación de certificado es un hash del certificado.

8. El sistema de la reivindicación 1, en el que la primera representación de certificado es una copia del certificado.

9. Un procedimiento para que un sistema de computación cliente se conecte a una máquina virtual, comprendiendo el procedimiento :

recibir (412) una primera representación de certificado de una máquina virtual, correspondiendo la primera representación de certificado a un certificado instalado en la máquina virtual;

presentar (413) una solicitud de conexión a la máquina virtual utilizando un protocolo que hace que la máquina virtual devuelva una segunda representación de certificado instalado en la máquina virtual;

recibir (414) la segunda representación de certificado de la máquina virtual;

comparar (415) la primera y la segunda representaciones de certificado; y

autenticar (418) la máquina virtual dependiendo de si coinciden la primera y la segunda representación de certificado .

10. El sistema de acuerdo con la reivindicación 6, en el que los medios de almacenamiento virtual son una unidad virtual de DVD .

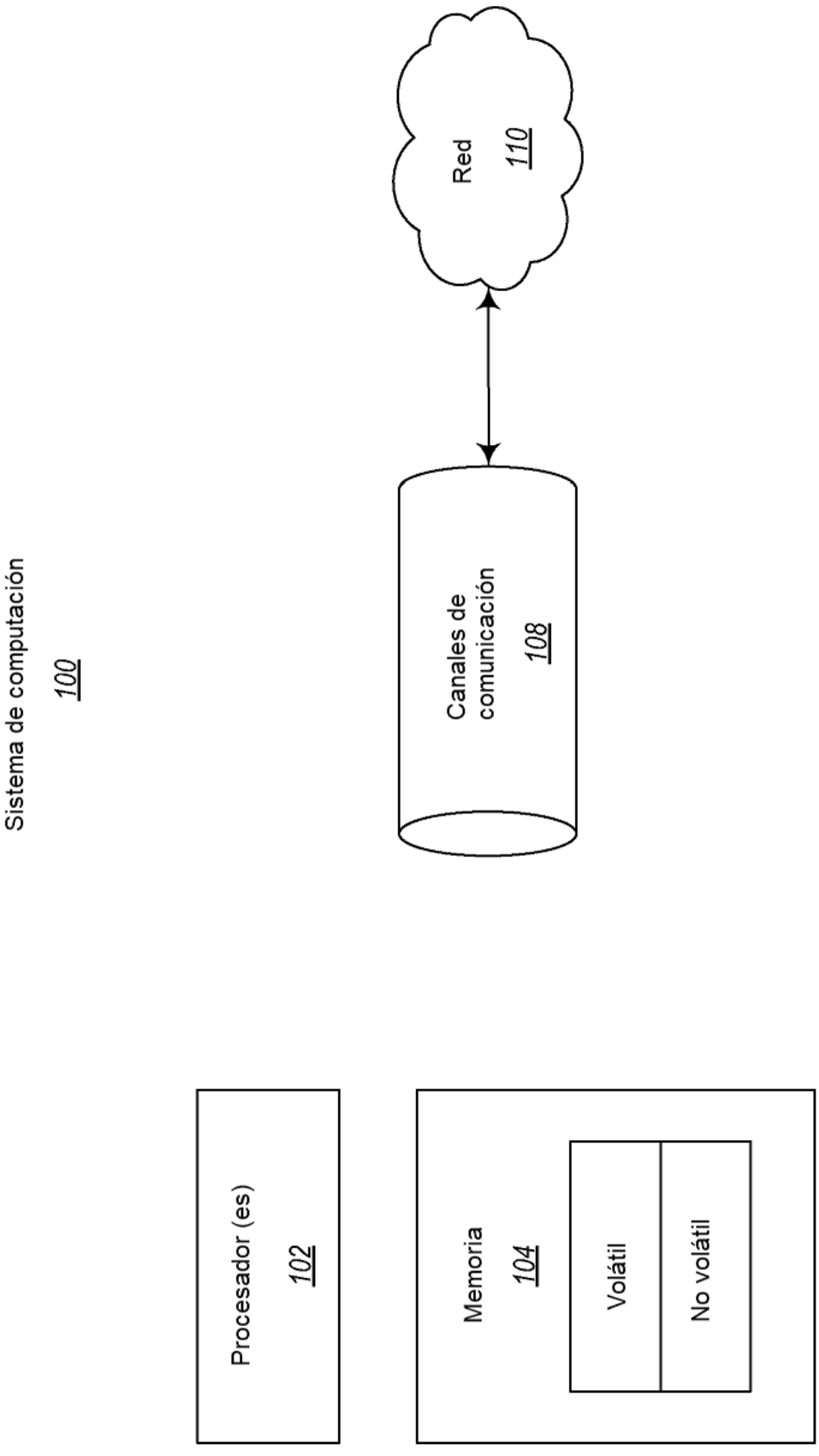
Sistema de computación
100
Red
110
Canales de comunicación
108
Procesador (es)
102
Memoria
104
Volátil
No volátil

Figura 1

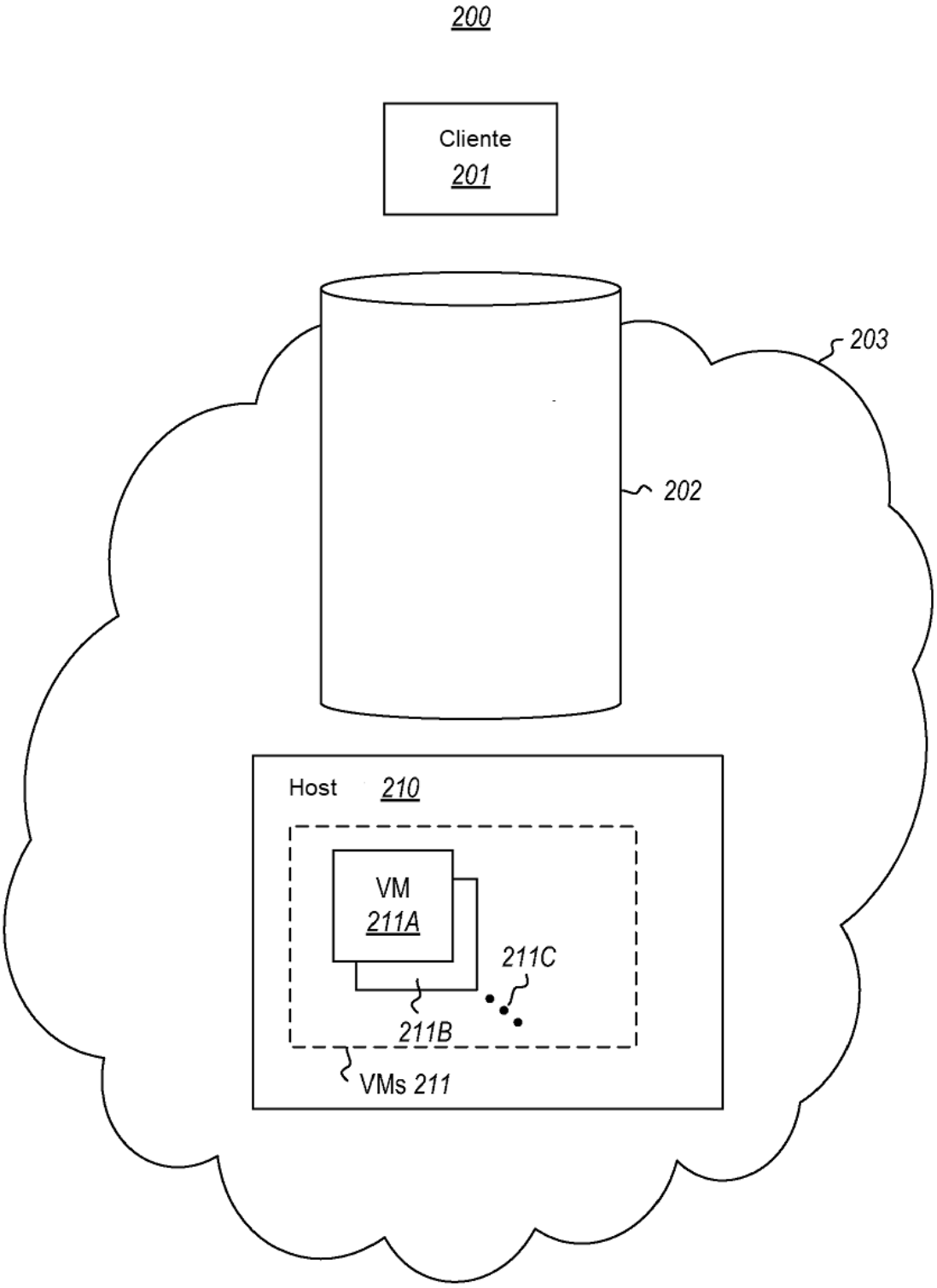


**Figura 2**

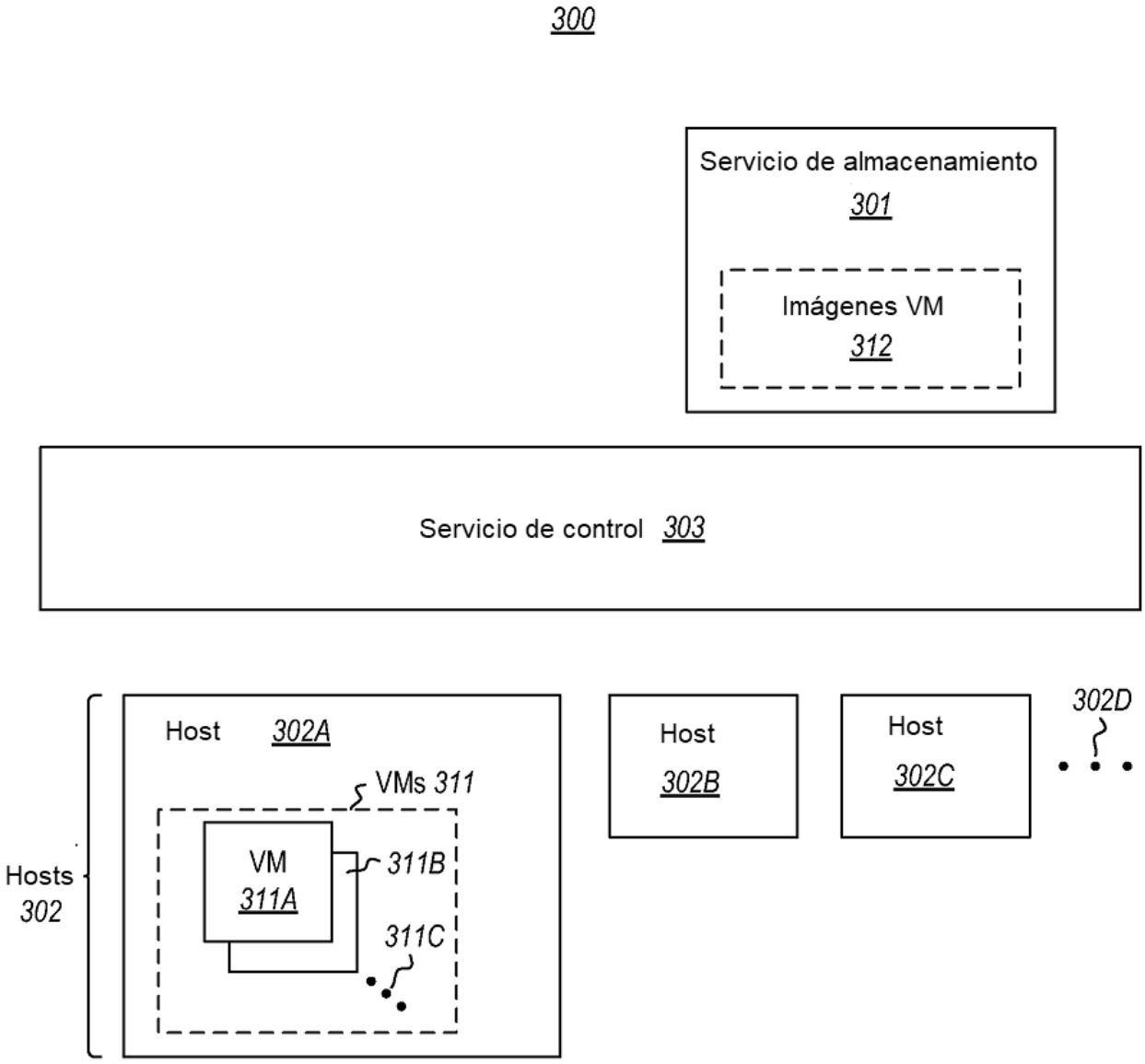
300
Servicio de almacenamiento
301
Imágenes VM
312
Servicio de control 303
Hosts
302
Host 302A
VMs 311
VM
311A
311B
311C
Host
302B
Host
302C
302D

**Figura 3**

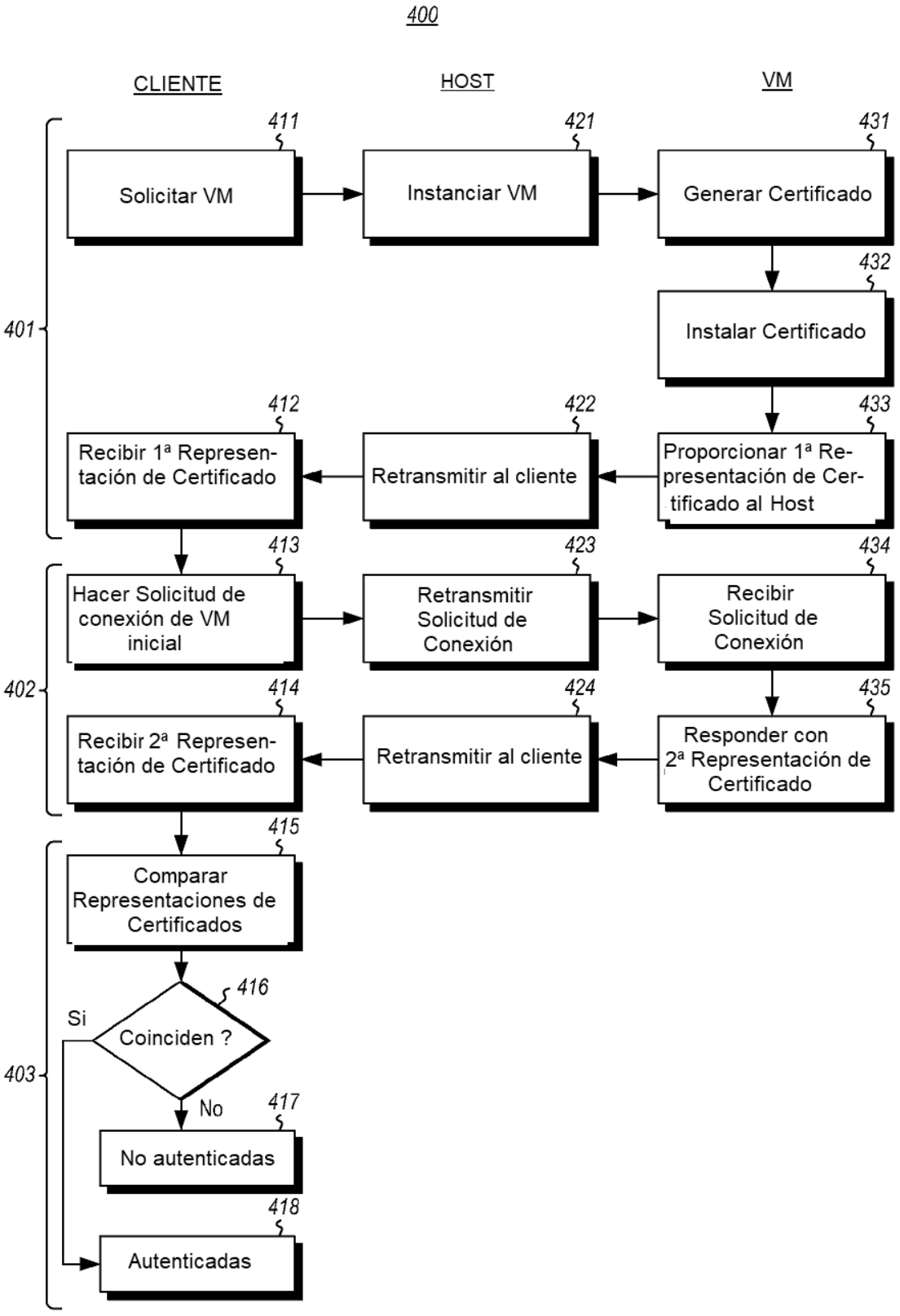
400
CLIENTE
HOST
VM
411
Solicitar VM
421
Instanciar VM
431
Generar Certificado
432
Instalar Certificado
401
412
Recibir 1ª Representación de Certificado
422
Retransmitir al cliente
433
Proporcionar 1ª Representación de Certificado al Host
413
Hacer Solicitud de conexión de VM inicial
423
Retransmitir Solicitud de Conexión
434
Recibir Solicitud de Conexión
402
414
Recibir 2ª Representación de Certificado
424
Retransmitir al cliente
435
Responder con 2ª Representación de Certificado
415
Comparar Representaciones de Certificados
416
Si
Coinciden ?
403
No
417
No autenticadas
418
Autenticadas

**Figura 4**

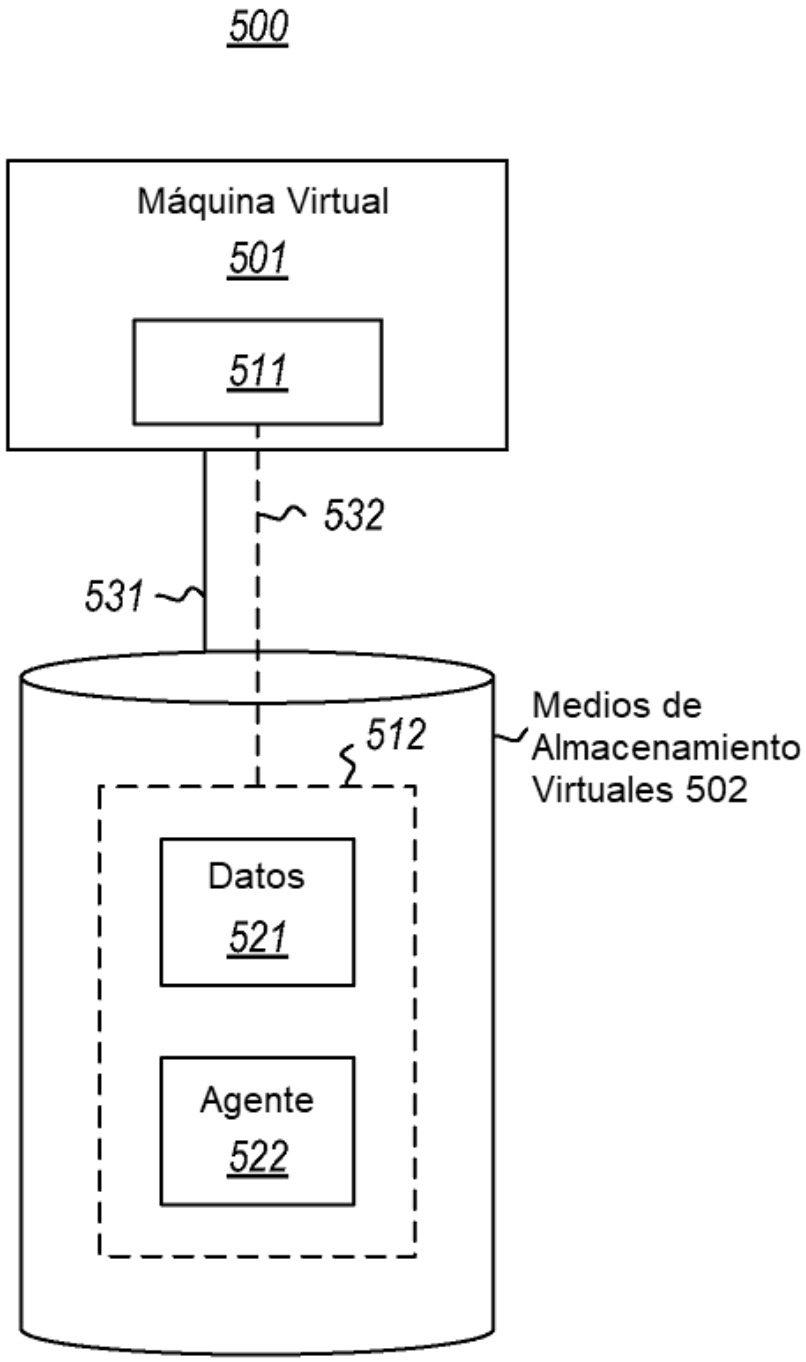
500
Máquina Virtual
501
511
532
531
512
Medios de Almacenamiento Virtuales 502
Datos
521
Agente
522

**Figura 5**

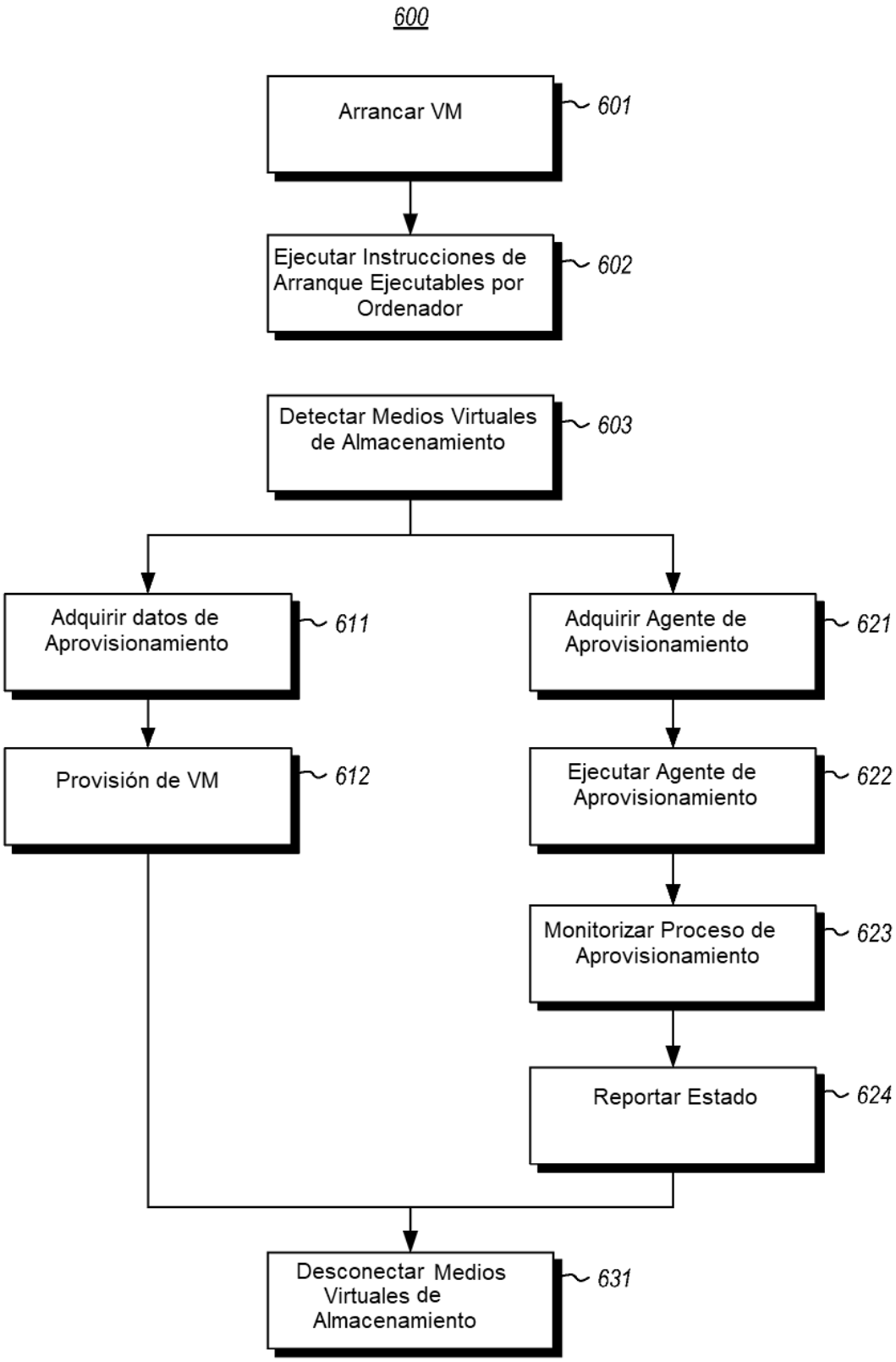
600
Arrancar VM
601
Ejecutar Instrucciones de Arranque Ejecutables por Ordenador
602
Detectar Medios Virtuales de Almacenamiento
603
Adquirir datos de Aprovisionamiento
611
Provisión de VM
612
Adquirir Agente de Aprovisionamiento
621
Ejecutar Agente de Aprovisionamiento
622
Monitorizar Proceso de Aprovisionamiento
623
Reportar Estado
624
Desconectar Medios Virtuales de Almacenamiento
631

**Figura 6**