(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 782 207**

(51) Int. CI.:

H04L 12/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.04.2016 PCT/US2016/028576**

(87) Fecha y número de publicación internacional: **27.10.2016 WO16172300**

(96) Fecha de presentación y número de la solicitud europea: **21.04.2016 E 16783827 (5)**

(97) Fecha y número de publicación de la concesión europea: **04.03.2020 EP 3286656**

(54) Título: **Sistema y método para gestionar eventos que implican sistemas informáticos y redes usando sistema de monitorización de tejido**

(30) Prioridad:

24.04.2015 US 201562152211 P
20.04.2016 US 201615134277

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.09.2020

(73) Titular/es:

GOLDMAN SACHS & CO. LLC (100.0%)
200 West Street
New York, NY 10282, US

(72) Inventor/es:

ANDERSON, ROBERT;
BERMAN, ILIA;
BILLIS, KEITH y
JOSHI, AMOL

(74) Agente/Representante:

ARIAS SANZ, Juan

DESCRIPCIÓN

Sistema y método para gestionar eventos que implican sistemas informáticos y redes usando sistema de monitorización de tejido

Campo técnico

Esta divulgación se refiere generalmente a sistemas informáticos. Más específicamente, esta divulgación se refiere a un sistema y método para gestionar eventos que implican sistemas informáticos y redes usando un sistema de monitorización de tejido.

Antecedentes

Las empresas, gobiernos y otras organizaciones a menudo tienen un número extremadamente grande de dispositivos de red e informáticos distribuidos a lo largo de un amplio rango de áreas geográficas. Por ejemplo, una gran corporación multinacional podría tener múltiples centros de datos, cada uno con decenas de miles de dispositivos de red e informáticos, así como diversas oficinas alrededor del mundo que oscilan desde unos pocos dispositivos de red o informáticos hasta muchos miles de dispositivos de red o informáticos. Cada dispositivo de red o informático denota una fuente de posibles anomalías u otros eventos que necesitan rastrearse, investigarse y resolverse si es necesario. Sin embargo, a medida que el tamaño de una organización crece junto con sus sistemas informáticos y redes, gestionar estos eventos puede consumir cada vez más tiempo y recursos de la organización.

El documento US 2014/223555 (A1) da a conocer un método y un sistema para mejorar la detección de amenazas de seguridad en una red de comunicación, incluyendo dispositivos de seguridad que generan eventos de seguridad. Una etiqueta dinámica se asigna a cada evento según la descripción del evento, y las etiquetas relacionadas con la misma amenaza de seguridad se agrupan formando un patrón de modelo de datos. Un algoritmo de inteligencia artificial, que aprende de la información real conocida, analiza los patrones y decide si debe generarse o no una alarma.

Sumario

Según la presente divulgación, se proporciona un método según la reivindicación 1, un sistema según la reivindicación 2, y un medio legible por ordenador no transitorio según la reivindicación 13. Características opcionales del método, sistema y medio legible por ordenador no transitorio se exponen en las reivindicaciones dependientes.

Esta divulgación proporciona un sistema y método para gestionar eventos que implican sistemas informáticos y redes usando un sistema de monitorización de tejido.

En una primera realización, un método incluye recibir, en un sistema de monitorización de tejido, información que identifica ocurrencias de eventos en un sistema de empresa que tiene múltiples sistemas de red o informáticos. Los eventos ocurren en o implican dispositivos de red o informáticos en los sistemas de red o informáticos, y los eventos se identifican usando reglas accesibles por el sistema de monitorización de tejido. El método también incluye procesar, usando el sistema de monitorización de tejido, la información en tiempo real para identificar las ocurrencias de los eventos y para asignar los eventos a múltiples situaciones. Los eventos se asignan a las situaciones usando uno o más modelos de procesamiento accesibles por el sistema de monitorización de tejido. El método incluye además enviar información que identifica las situaciones.

En una segunda realización, un sistema incluye un sistema de monitorización de tejido que tiene múltiples nodos informáticos y múltiples enlaces de comunicación que acoplan los nodos informáticos. El sistema de monitorización de tejido está configurado para recibir información que identifica ocurrencias de eventos en un sistema de empresa que tiene múltiples sistemas de red o informáticos. Los eventos ocurren en o implican dispositivos de red o informáticos en los sistemas de red o informáticos, y los eventos se identifican usando reglas accesibles por el sistema de monitorización de tejido. El sistema de monitorización de tejido también está configurado para procesar la información en tiempo real para identificar las ocurrencias de los eventos y asignar los eventos a múltiples situaciones. Los eventos se asignan a las situaciones usando uno o más modelos de procesamiento accesibles por el sistema de monitorización de tejido. El sistema de monitorización de tejido se configura además para enviar información que identifica las situaciones.

En una tercera realización, un medio legible por ordenador no transitorio contiene código de programa legible por ordenador que, cuando se ejecuta por nodos informáticos de un sistema de monitorización de tejido, provoca que los nodos informáticos reciban información que identifica ocurrencias de eventos en una sistema de empresa que tiene múltiples sistemas de red o informáticos. Los eventos ocurren en o implican dispositivos de red o informáticos en los sistemas de red o informáticos, y los eventos se identifican usando reglas accesibles por el sistema de monitorización de tejido. El código de programa legible por ordenador, cuando se ejecuta por los nodos informáticos del sistema de monitorización de tejido, también provoca que los nodos informáticos para procesar la información en tiempo real para identificar las ocurrencias de los eventos y asignar los eventos a múltiples situaciones. Los eventos se asignan a las situaciones usando uno o más modelos de procesamiento accesibles por el sistema de monitorización de tejido. El

código de programa legible por ordenador, cuando se ejecuta por los nodos informáticos del sistema de monitorización de tejido, provoca además que los nodos informáticos envíen información que identifica las situaciones.

Otras características técnicas pueden hacerse evidentes fácilmente para un experto en la técnica a partir de las siguientes figuras, descripciones y reivindicaciones.

Breve descripción de los dibujos

Para una comprensión más completa de esta divulgación y sus características, se hace referencia ahora a la siguiente descripción, tomada junto con los dibujos adjuntos, en los que:

la figura 1 ilustra un sistema de ejemplo para gestionar eventos que implican sistemas informáticos y redes usando un sistema de monitorización de tejido según esta divulgación;

la figura 2 ilustra un dispositivo informático de ejemplo asociado con un sistema para gestionar eventos que implican sistemas informáticos y redes usando un sistema de monitorización de tejido según esta divulgación;

las figuras 3 a 6 ilustran un sistema de monitorización de tejido de ejemplo para gestionar eventos que implican sistemas informáticos y redes y detalles relacionados según esta divulgación; y

las figuras 7 y 8 ilustran flujos de proceso de ejemplo en un sistema para gestionar eventos que implican sistemas informáticos y redes usando un sistema de monitorización de tejido según esta divulgación.

Descripción detallada

Las figuras 1 a 8, comentadas a continuación, y las diversas realizaciones utilizadas para describir los principios de la presente invención en este documento de patente son solo a modo de ilustración y no deben interpretarse en modo alguno para limitar el alcance de la invención. Aquellos expertos en la técnica comprenderán que los principios de la invención pueden implementarse en cualquier tipo de dispositivo o sistema dispuesto de manera adecuada.

La figura 1 ilustra un sistema de ejemplo 100 para gestionar eventos que implican sistemas informáticos y redes usando un sistema de monitorización de tejido según esta divulgación. Como se muestra en la figura 1, el sistema 100 incluye o está asociado con uno o más sistemas informáticos o redes 102a-102n. Cada sistema informático o red 102a-102n denota una colección de dispositivos informáticos 104 y/o dispositivos de red 106. Cada sistema informático o red 102a- 102n puede incluir cualquier número de dispositivos 104 y/o 106. Como se señaló anteriormente, un sistema informático o red 102a-102n puede variar desde sistemas o redes con solo unos cuantos dispositivos 104 y/o 106 hasta sistemas o redes con decenas de miles de dispositivos 104 y/o 106 (o incluso más). Pueden utilizarse múltiples sistemas informáticos o redes 102a-102n dentro de una sola área geográfica común o a través de múltiples áreas geográficas, incluyendo áreas separadas por distancias muy largas.

Uno o más dispositivos en cada uno de los sistemas informáticos o redes 102a-102n pueden comunicarse a través de al menos una red 108. La red 108 denota cualquier red o combinación de redes adecuada en una o más ubicaciones. La red 108 puede, por ejemplo, incluir una o más redes de área local (LAN), redes de área amplia (WAN), redes de área metropolitana (MAN) o una red regional o mundial. Una colección de sistemas informáticos o redes 102a-102n y red(es) relacionadas 108 puede denominarse “sistema de empresa” en este documento de patente.

Un sistema de monitorización de tejido 110 se implementa dentro del sistema de empresa, tal como usando diversos de los dispositivos informáticos 104 y dispositivos de red 106 en los sistemas informáticos o redes 102a-102n. La informática de tejido (también conocida como informática unificada, tejido unificado, tejido de centro de datos y tejido de centro de datos unificada) implica la creación de un tejido informático formado por nodos informáticos 112 que están interconectados usando enlaces de comunicación 114. La disposición exacta de los nodos informáticos 112 y la topología de conectividad de red definida por los enlaces de comunicación 114 pueden variar de la mostrada en este caso según se necesite o se desee. Un sistema de monitorización de tejido 110 incluye de manera rutinaria un sistema informático de alto rendimiento consolidado que incluye de manera general funciones de almacenamiento acoplado, red y procesamiento paralelo enlazadas por interconexiones de ancho de banda alto (como conexiones Ethernet de 10 gigabits e InfiniBand). En algunas realizaciones, los nodos interconectados parecen funcionar como una única unidad lógica.

Los componentes fundamentales del sistema de monitorización de tejido 110 son sus nodos 112 y sus enlaces 114. Los nodos 112 incluyen generalmente componentes de hardware como procesadores, memorias y dispositivos periféricos. Los enlaces 114 son conexiones funcionales entre los nodos 112. Un sistema de monitorización de tejido 110 puede distinguirse de otras arquitecturas por diversas razones. Por ejemplo, un sistema de monitorización de tejido 110 puede desplegarse en múltiples “tramas” y proporcionar soporte para comunicaciones y señalización de a través de tramas. Esto proporciona una mejorada escalabilidad y resiliencia del sistema de monitorización de tejido 110. Además, un sistema de monitorización de tejido 110 puede soportar múltiples tipos de modelos de procesamiento (como modelos definidos por el usuario y analíticos), lo que soporta múltiples mecanismos para identificar y clasificar

eventos asociados con los sistemas informáticos o redes 102a-102n.

Tal como se describe con más detalle a continuación, el sistema de monitorización de tejido 110 puede utilizarse ventajosamente en la monitorización, diagnóstico y mantenimiento de aplicaciones de empresa desplegadas en los sistemas informáticos o redes 102a-102n, así como otros aspectos de los sistemas informáticos o redes 102a-102n. Las aplicaciones de empresa denotan aplicaciones desplegadas en múltiples dispositivos 104 y/o 106 en una o más ubicaciones y que proporcionan información relacionada con eventos al sistema de monitorización de tejido 110. Mientras que los sistemas de monitorización convencionales a menudo proporcionan alertas para anomalías individuales o fallos del sistema, estos sistemas de monitorización normalmente fallan al proporcionar un enfoque integrado para categorizar adecuadamente y procesar eventos de sistema y aplicación a través de un gran sistema de empresa. El sistema de monitorización de tejido 110 puede proporcionar un enfoque integrado de este tipo para categorizar y procesar adecuadamente eventos de sistema y aplicación para su uso en diversos entornos, incluyendo grandes sistemas de empresa.

Entre otras cosas, esto permite que el sistema de monitorización de tejido 110 proporcione diagnóstico y mantenimiento a nivel de organización. Por ejemplo, el sistema de monitorización de tejido 110 puede utilizarse como se describe a continuación para proporcionar un ciclo de vida de gestión de situaciones completo para eventos, desde la ocurrencia o inicio de los eventos hasta su (posiblemente automatizada) resolución. El sistema de monitorización de tejido 110 también puede proporcionar el procesamiento de eventos basándose en analítica y aprendizaje automático de máquina en lugar de, o además de, reglas estáticas. Además, el sistema de monitorización de tejido 110 puede proporcionar una plataforma altamente escalable para la colección de métricas de infraestructura y aplicación, con una rápida resolución de incidentes basándose en analítica predictiva. Esto puede permitir que el sistema de monitorización de tejido 110 se utilice para funciones más predictivas relacionadas con el procesamiento de eventos, en lugar de simplemente reaccionar a eventos que han ocurrido.

Eventos que se identifican y procesan por el sistema de monitorización de tejido 110 denotan bits de información y pueden originarse a partir de cualquier fuente adecuada dentro de los sistemas informáticos o redes 102a-102n. Por ejemplo, los eventos pueden denotar un estado actual o un cambio en el estado actual de un dispositivo, sistema o red (o, por lo tanto, una parte). También pueden utilizarse eventos para identificar anomalías u ocurrencias de condiciones definidas dentro de los sistemas informáticos o redes 102a-102n. Ejemplos de tipos específicos de eventos pueden incluir la utilización de la unidad central de procesamiento (CPU) actual de un ordenador que ejecuta una aplicación, una identificación de un fallo en un ordenador que ejecuta una aplicación, o una conexión defectuosa identificada por una aplicación. Como se describe a continuación, las reglas utilizadas por el sistema de monitorización de tejido 110 ayudan a identificar eventos de interés en tiempo real, y los eventos se utilizan luego para identificar situaciones a investigar o resolver (o bien de forma manual o bien automatizada).

Se derivan situaciones de flujos de eventos y pueden identificarse usando diversos modelos de procesamiento, que definen cómo el sistema de monitorización de tejido 110 procesa los eventos para identificar las situaciones. Por ejemplo, un modelo de procesamiento puede indicar que se va a crear una situación para cada evento. Como otro ejemplo, un modelo de procesamiento puede indicar que se va a crear una situación cuando se produce(n) un número o tipo(s) específico(s) de eventos relacionados con un solo ítem o un grupo de ítems en un período de tiempo definido. Un ítem generalmente denota algún hardware, software, firmware o, por tanto, una combinación. Ejemplos de ítems pueden incluir hardware específico (como conmutadores u ordenadores centrales), aplicaciones específicas u otras plataformas informáticas virtuales/físicas. Pueden crearse y almacenarse bibliotecas de modelos de procesamiento y políticas de base dentro del sistema de monitorización de tejido 110, y estos modelos y políticas pueden aplicarse directamente al dominio de la infraestructura o a la monitorización de eventos de aplicación.

Cada situación identificada puede traducirse y comunicarse a través de un sistema para acción adicional. Por ejemplo, puede darse un número de ticket para una situación dado y dirigirse a la plataforma de inteligencia de operación o mantenimiento de sistema para una acción correctiva, o puede identificarse una situación en relación con una función correctiva y generación de informes automatizada y dentro de una aplicación de empresa.

De esta manera, los sistemas de empresa completos pueden monitorizarse y mantenerse usando el sistema de monitorización de tejido 110, con generación de informes y registro a un nivel de caso específico. El procesamiento de eventos, que incluye categorización, generación de informes y acción predictiva y/o correctiva, puede basarse en técnicas de aprendizaje automático de máquina y analítica en lugar de, o además de, filtros y reglas estáticas. Como tal, la monitorización de eventos que utiliza el sistema de monitorización de tejido 110 en sistemas de empresa presenta una plataforma unificada altamente escalable para la colección de métricas de infraestructura y aplicación y proporciona una rápida resolución de incidentes basándose en analítica predictiva.

El sistema de monitorización de tejido 110 también puede hacerse funcionar para ayudar a garantizar que se mitiga la inanición de eventos. La inanición de eventos puede producirse cuando se genera un número excesivo de eventos, tal como debido a una aplicación o dispositivo defectuosos o debido a un ataque intencional de denegación de servicio (DOS), un ataque de DOS distribuido (DDOS) u otro ataque. Un número excesivo de eventos puede sobrecargar un sistema convencional, provocando que el sistema deje de proporcionar eventos a los componentes aguas abajo (que por lo tanto están “con inanición” de eventos). En algunas realizaciones, el sistema de monitorización de tejido 110

aborda cuestiones relacionadas con la inanición de eventos permitiendo la abstracción de componentes.

El sistema de monitorización de tejido 110 puede además proporcionar transmisión de mensajes y persistencia, así como el uso de datos de referencia durante enrutamiento de eventos, detección de situaciones y enriquecimiento de eventos. Por ejemplo, en algunas realizaciones, un historial detallado de procesamiento para cada evento puede almacenarse en un almacenamiento persistente ya que cada evento se procesa a través del sistema de monitorización de tejido 110. Los historiales de eventos pueden consultarse y buscarse, como por ejemplo usando una función de consulta o búsqueda.

Además, los protocolos y la funcionalidad relacionados con las suscripciones de eventos permiten que el sistema de monitorización de tejido 110 soporte el conocimiento preventivo de eventos y situaciones dentro de un sistema de empresa y aplicaciones de empresa dentro del sistema de empresa, que a menudo dependen de un nivel bajo subyacente de componentes de infraestructura. Por ejemplo, el sistema de monitorización de tejido 110 puede soportar la suscripción de eventos para crear así una situación derivada a partir de los eventos que se producen en áreas separadas o diferentes de la infraestructura de una organización.

En algunas realizaciones, los usuarios pueden configurar las políticas y reglas que se utilizan para especificar cómo se clasifican y escalan los eventos. Dos mecanismos de ejemplo para configurar políticas de gestión de eventos incluyen (i) selecciones predefinidas para especificaciones estandarizadas y (ii) un lenguaje específico de dominio (DSL) para describir especificaciones especializadas. El DSL puede permitir, por ejemplo, que se dé a eventos el mismo nombre u otro identificador o que se envíe a un modelo de agrupación, que puede seleccionarse basándose en analítica de planificación o comportamiento.

El sistema de monitorización de tejido 110 también soporta diversos modelos de procesamiento para la agrupación de eventos y la identificación de situaciones. Dos tipos de modelos de ejemplo incluyen modelos de agrupación definidos por el usuario y modelos de agrupación descubiertos o analíticos. Pueden utilizarse o soportarse diversos modelos de procesamiento, y pueden crearse modelos de procesamiento adicionales según se necesite o desee para definir diferentes patrones de agrupación. Los modelos de agrupación definidos por el usuario se definen por uno o más usuarios, y ejemplos de modelos de agrupación definidos por el usuario pueden incluir “uno por uno”, “X por encima de Y” y “fallo de batería”. Se definen modelos analíticos como modelos que soportan una o más funciones analíticas, y ejemplos de modelos analíticos pueden incluir agrupación por similitud de eventos o agrupación por anomalías de eventos (tales como eventos no categorizados, eventos nuevos o nunca antes vistos, irregularidades de volumen de eventos, ausencia de eventos anticipados, eventos no registrados, y otros).

En algunas realizaciones, la categorización de eventos puede ser sin indicación de estado y puede distribuirse, sin embargo, muchos nodos 112 se requieren o están disponibles para procesar la carga. Un sistema de mensajería dentro del sistema de monitorización de tejido 110 puede utilizarse para distribuir eventos a nodos de procesamiento disponibles 112. El sistema de mensajería puede implementar o utilizar una “clave de grupo” u otro indicador para garantizar que cualquier evento que forme parte del mismo grupo se entregará al mismo nodo de procesamiento 112. Pueden definirse grupos de cualquier manera adecuada, como agrupando eventos asociados a un solo ítem o colección de ítems. El sistema de mensajería y determinados mecanismos de persistencia también pueden ser “conectables”, lo que facilita las implementaciones menos costosas de diversos mecanismos para la garantía de calidad y desarrollo de funcionalidades adicionales dentro del sistema de tejido. El estado necesario para la evaluación de modelo puede almacenarse en caché en instancias de procesos, el sistema de mensajería puede entregar eventos a los nodos 112 o ubicaciones en las que la información se almacena en caché, y la continuidad puede lograrse, por ejemplo, mediante una copia de los cambios con respecto al estado en un almacén de persistencia fuera de la máquina.

Como se señaló anteriormente, el sistema de monitorización de tejido 110 puede incluir soporte incorporado para el flujo de procesamiento de tramas, que puede ayudar a permitir el aislamiento de la plataforma y mitigar riesgos relacionados con la inanición de eventos. Con el tramado, diferentes nodos 112 o incluso diferentes instancias del propio sistema de monitorización de tejido 110 pueden utilizarse para procesar eventos de diferentes fuentes, como eventos de diferentes ítems, diferentes regiones, o diferentes despliegues de hardware/software/firmware. También pueden utilizarse otras particiones para soportar el tramado, tal como dividiendo un sistema de empresa por unidad de negocio o por tipo de negocio que se gestiona usando los sistemas informáticos o redes 102a-102n. Un desafío con el tramado implica cómo comunicar un evento o una situación en una trama a otras tramas que necesitan saber de tal evento o situación. En algunas realizaciones, esto puede realizarse creando eventos sintéticos tras la creación de situaciones en una trama. Estos eventos sintéticos pueden distribuirse entonces a otras tramas para permitir las correlaciones de a través de tramas de los eventos o situaciones.

Dependiendo de la implementación, el sistema de monitorización de tejido 110 proporciona notificación y monitorización inteligente de situaciones que requieren acción, incluyendo notificación a administradores de sistema, grupos de usuarios o suscriptores. Además, una situación puede ser un solo evento en un sistema de empresa o múltiples eventos correlacionados para proporcionar un profundo conocimiento de una anomalía dentro del sistema de empresa. Además, el sistema de monitorización de tejido 110 puede reducir los riesgos funcionales y reglamentarios aportando transparencia y gestión inteligente de eventos de entorno tecnológico empresarial a gran

escala. El sistema de monitorización de tejido 110 también aporta un flujo de trabajo para que los usuarios especifiquen cómo se categorizan eventos (como por prioridad, grupo, situación o categoría definida por el usuario), se reportan y registran y cómo se asignan y ejecutan las acciones subsecuentes. El sistema de monitorización de tejido 110 permite además que las políticas de agrupación de eventos se sometan a ciclos de vida de promoción y se sometan a pruebas controladas y, reduciendo así la exposición relacionada con cambios no deseados o procesamiento innecesario en entornos de producción. Además, el sistema de monitorización de tejido 110 puede soportar la aplicación forzosa de ciclos de vida controlados para políticas y reglas debido a la separación de usuarios que pueden crear reglas y usuarios que pueden promover aquellas reglas para su producción o uso.

Se proporcionan a continuación detalles adicionales sobre el sistema de monitorización de tejido 110. Cabe señalar que el sistema de monitorización de tejido 110 puede incluir cualquier número de nodos 112 y enlaces de comunicación 114 en cualquier disposición adecuada. Si bien se muestra como que se encuentra fuera de los sistemas informáticos o redes 102a-102n, el sistema de monitorización de tejido 110 puede formarse o encontrarse dentro de uno o más de los sistemas informáticos o redes 102a-102n.

Aunque la figura 1 ilustra un ejemplo de un sistema 100 para gestionar eventos que implica sistemas informáticos y redes usando un sistema de monitorización de tejido 110, pueden hacerse diversos cambios a la figura 1. Por ejemplo, el sistema 100 puede incluir cualquier número de sistemas informáticos o redes (cada uno con cualquier número de dispositivos de red o informáticos), redes y sistemas de monitorización de tejido. Además, los sistemas y redes que implican ordenadores son altamente configurables, y la figura 1 no limita esta divulgación a ninguna configuración específica de sistema o red.

La figura 2 ilustra un dispositivo informático de ejemplo 200 asociado con un sistema para gestionar eventos que implican sistemas informáticos y redes usando un sistema de monitorización de tejido según esta divulgación. En particular, la figura 2 ilustra una implementación de ejemplo de los nodos informáticos 112 en el sistema de monitorización de tejido 110 de la figura 1.

Como se muestra en la figura 2, el dispositivo informático 200 incluye un sistema de bus 202, que soporta la comunicación entre al menos un dispositivo de procesamiento 204, al menos un dispositivo de almacenamiento 206, al menos una unidad de comunicaciones 208 y al menos una unidad de entrada/salida (E/S) 210. El dispositivo de procesamiento 204 ejecuta instrucciones que pueden cargarse en una memoria 212. El dispositivo de procesamiento 204 puede incluir cualquier número(s) y tipo(s) adecuado(s) de procesadores u otros dispositivos en cualquier disposición adecuada. Tipos de ejemplo de dispositivos de procesamiento 204 incluyen microprocesadores, microcontroladores, procesadores de señal digital, matrices de puertas de campo programable, circuitos integrados específicos de aplicación y circuitos discretos.

La memoria 212 y un almacenamiento persistente 214 son ejemplos de dispositivos de almacenamiento 206, que representan cualquier estructura capaz de almacenar y facilitar la recuperación de información (como datos, código de programa, y/u otra información adecuada de forma temporal o permanente). La memoria 212 puede representar una memoria de acceso aleatorio o cualquier otro dispositivo de almacenamiento volátil o no volátil adecuado. El almacenamiento persistente 214 puede contener uno o más componentes o dispositivos que soportan almacenamiento de datos a largo plazo, como una memoria de solo lectura, un disco duro, una memoria flash o un disco óptico.

La unidad de comunicaciones 208 soporta comunicaciones con otros sistemas o dispositivos. Por ejemplo, la unidad de comunicaciones 208 puede incluir una tarjeta de interfaz de red o un transceptor inalámbrico que facilita las comunicaciones con otros nodos 112 a través de uno o más enlaces de comunicación 114. La unidad de comunicaciones 208 puede soportar comunicaciones a través de cualquier enlace de comunicación físico o inalámbrico adecuado.

La unidad de E/S 210 permite la entrada y salida de datos. Por ejemplo, la unidad de E/S 210 puede proporcionar una conexión para la entrada y salida de datos a una memoria externa local, una base de datos o un dispositivo periférico.

Aunque la figura 2 ilustra un ejemplo de un dispositivo informático 200 asociado con un sistema para gestionar eventos que implican sistemas informáticos y redes usando un sistema de monitorización de tejido, pueden hacerse diversos cambios a la figura 2. Por ejemplo, los dispositivos informáticos son altamente configurables, y la figura 2 no limita esta divulgación a ninguna configuración específica de dispositivo informático.

Las figuras 3 a 6 ilustran un sistema de monitorización de tejido de ejemplo 110 para gestionar eventos que implican sistemas informáticos y redes y detalles relacionados según esta divulgación. Como se muestra en la figura 3, el sistema de monitorización de tejido 110 se hace funcionar junto con un anfitrión 302, lo que podría denotar cualquiera de los dispositivos informáticos 104 o dispositivos de red 106 en la figura 1. El anfitrión 302 en este caso incluye diversos componentes de hardware, como uno o más procesadores 304, uno o más discos duros 306 y una o más memorias 308. Los procesadores 304 pueden (entre otras cosas) utilizarse para ejecutar una o más aplicaciones de empresa u otras aplicaciones. Por supuesto, dispositivos anfitriones pueden venir en una amplia variedad de configuraciones, que pueden incluir componentes de hardware adicionales u otros. Cabe señalar que mientras un

anfitrión 302 se muestra en la figura 3, el sistema de monitorización de tejido 110 puede utilizarse con cualquier número de anfitriones u otras fuentes de eventos.

El anfitrión 302 incluye un agente de eventos 310 y una interfaz de programación de aplicaciones de eventos (API) 312. El agente de eventos 310 recoge los eventos que se generan por el anfitrión 302 y proporciona los eventos al sistema de monitorización de tejido 110 a través de la API de eventos 312. El agente de eventos 310 incluye cualquier lógica adecuada para recopilar eventos, y la API de eventos 312 incluye cualquier interfaz adecuada para interactuar con el agente de eventos 310. El agente de eventos 310 puede, por ejemplo, denotar una o más aplicaciones ejecutadas por el procesador 304.

El sistema de monitorización de tejido 110 incluye una plataforma de monitorización 314, que se hace funcionar para recopilar eventos del anfitrión 302 y otras fuentes de eventos. Entre otras cosas, los eventos detectados pueden identificar aspectos de un entorno de red o informático que no funcionan como se espera o que satisfacen reglas definidas por el usuario u otras de monitorización. En este ejemplo, la plataforma de monitorización 314 incluye un servidor de eventos 314 y un módulo de telemetría 316. El servidor de eventos 314 recopila eventos del agente de eventos 310 en el anfitrión 302 y de otros agentes de eventos en otros anfitriones o fuentes de eventos. El módulo de telemetría 316 analiza los eventos detectados u otra información con el fin de proporcionar métricas para la resolución de problemas, la planificación de capacidad u otras funciones. La información del módulo de telemetría 316 puede, por ejemplo, contribuir al menos parcialmente a la prevención de la inanición de eventos. El servidor de eventos 314 incluye cualquier lógica adecuada para recopilar eventos de agentes de eventos. En algunas realizaciones, el agente de eventos 310 y el servidor de eventos 314 pueden denotar herramientas de monitorización de tecnología de la información (IT), como aquellas disponibles de NAGIOS ENTERPRISES. El módulo de telemetría 316 incluye cualquier lógica adecuada para identificar una o más métricas asociadas a eventos entrantes.

El sistema de monitorización de tejido 110 también incluye una plataforma central 320, que analiza los eventos obtenidos por la plataforma de monitorización 314 con el fin de identificar situaciones que están surgiendo, han surgido o pueden surgir en uno o más de los sistemas informáticos o redes 102a-102n. En este ejemplo, la plataforma central 320 soporta una función de correlación 322, que puede utilizarse para identificar eventos que están relacionados y que, por lo tanto, pueden formar parte de una o más situaciones. La plataforma central 320 también soporta una función de agregación 324, que puede utilizarse para agrupar eventos relacionados para procesamiento adicional. La plataforma central 320 además soporta una función de enriquecimiento 326, que puede utilizarse para proporcionar información adicional sobre eventos o grupos de eventos. La información proporcionada por la función de enriquecimiento 326 puede, en algunos casos, utilizarse por la función de agregación 324 para agrupar eventos relacionados. La plataforma central 320 también soporta una función de supresión 328, que puede utilizarse para suprimir ciertos eventos de modo que esos eventos no se utilicen para crear situaciones (como para eventos que se conoce que no son de interés). Además, la plataforma central 320 soporta uno o más servicios autónomos 330, lo que puede denotar servicios que se producen automáticamente en respuesta a condiciones cambiantes. Por ejemplo, los servicios autónomos 330 pueden soportar funciones de autorreparación, autoconfiguración, autooptimización o autoprotección que modifican el sistema de monitorización de tejido 110 o los sistemas informáticos o redes 102a-102n en respuesta a situaciones detectadas.

Aunque no se muestra, el sistema de monitorización de tejido 110 o la plataforma central 320 pueden soportar otras funciones. Por ejemplo, pueden utilizarse una o más funciones analíticas para analizar eventos con el fin de estimar la salud de las aplicaciones y sus dependencias dentro de los sistemas informáticos o redes 102a-102n. Como otro ejemplo, pueden utilizarse una o más funciones de generación de informes para proporcionar una visión histórica de eventos, salud de agente y datos recogidos por el sistema. En este ejemplo, los informes u otra información pueden proporcionarse a diversos destinos 332a-332c. En este ejemplo, los destinos incluyen una consola de alertas 332a que denota un dispositivo configurado para presentar alertas u otra información a usuarios, un gráfico de dependencia 332b que denota un elemento de visualización gráfico que representa las dependencias de dispositivos en un sistema informático o red, y un indicador de pulso 332c que presenta una indicación del número de eventos o situaciones detectadas. Por supuesto, la información del sistema de monitorización de tejido 110 puede presentarse a cualquier otro destino o adicional o utilizarse de cualquier otra manera adecuada.

En este ejemplo, un gestor de políticas 334 permite que los usuarios autogestionen las reglas de monitorización que se utilizan por la plataforma de monitorización 314 y la plataforma central 320. Como ejemplos, estas reglas pueden utilizarse para identificar eventos de interés, agrupar eventos relacionados, suprimir eventos e identificar situaciones relacionadas con los eventos. Las reglas definidas usando el gestor de políticas 334 pueden almacenarse en un repositorio 336, como una base de datos u otro dispositivo o sistema de almacenamiento y recuperación.

El sistema de monitorización de tejido 110 también es capaz de recuperar datos de al menos un servicio de datos de referencia 338. El servicio de datos de referencia 338 puede utilizarse para proporcionar cualquier dato de referencia adecuado utilizado por el sistema de monitorización de tejido 110. Por ejemplo, el servicio de datos de referencia 338 puede utilizarse para obtener información que ayude con la clasificación y agrupación de eventos y con la identificación de situaciones. Cada servicio de datos 338 incluye cualquier estructura adecuada para almacenar y facilitar la recuperación de información.

Detalles adicionales del sistema de monitorización de tejido 110 se muestran en la figura 4. Como se muestra en la figura 4, un usuario (como un propietario técnico de aplicación) puede configurar una o más políticas, como usando un portal de autoservicio soportado por el gestor de políticas 334. Las directivas pueden almacenarse en el repositorio 336. Las políticas se ponen a disposición de la plataforma de monitorización 314, que utiliza las políticas para (entre otras cosas) obtener eventos del anfitrión 302 y otras fuentes de eventos. Múltiples anfitriones pueden estar ejecutando una o más aplicaciones de empresa comunes desplegadas en un sistema de empresa.

En este ejemplo, la plataforma de monitorización 314 soporta una función de distribución de configuración 402, que se utiliza para proporcionar información de umbral y reglas de las políticas recibidas a agentes de eventos distribuidos en los anfitriones y otras fuentes de eventos. La plataforma de monitorización 314 también soporta una función de gestión de estados 404, que es un componente de preprocesamiento que se encuentra entre los agentes de eventos distribuidos y la plataforma central 320 y que rastrea las transiciones de estado y envía eventos basándose en las transiciones de estado a la plataforma central 320. La plataforma de monitorización 314 además soporta una función de supresión 406, que puede utilizarse para suprimir ciertos eventos de modo que los eventos no se utilizan para crear situaciones. Además, la plataforma de monitorización 314 soporta una función de “enviar trampa”, que puede representar una API sin agente utilizada para enviar eventos directamente a la plataforma central 320 desde una aplicación u otra fuente.

La plataforma de monitorización 314 envía criterios de evento e información de monitorización, como políticas de monitorización de referencia y políticas de monitorización de aplicación, al agente de eventos 310 y recibe eventos del agente de eventos 310. Los eventos recibidos se identifican por el agente de eventos 310 usando los criterios de eventos y la información de monitorización. La plataforma de monitorización 314 también puede ser capaz de comunicarse con y recibir eventos desde módulos de monitorización externos 410 y funciones de escaneo de empresa 412. Los módulos de monitorización externos 410 pueden recibir los criterios de eventos y la información de monitorización de la plataforma de monitorización 314 y utilizar esa información para identificar eventos, mientras que las funciones de escaneo de empresa 412 pueden funcionar sin dicha información. Como puede verse en este caso, la plataforma de monitorización 314 es capaz de recibir eventos desde diversas fuentes como entradas. Dado que los agentes de eventos 310, funciones y módulos de monitorización externos 410 y funciones de escaneo de empresa 412 pueden distribuirse a través de un sistema de empresa, la plataforma de monitorización 314 puede recibir eventos que se producen en múltiples ubicaciones e informar de los eventos a través del sistema para proporcionar visibilidad al desempeño real de la empresa.

Una vez se reciben los eventos en la plataforma de monitorización 314, los eventos (o al menos los eventos no suprimidos) se envían a la plataforma central 320, donde los eventos se evalúan según las reglas cargadas de las políticas. Por ejemplo, las reglas pueden utilizarse para clasificar los eventos y determinar qué tipo de modelos de procesamiento se utilizarán para monitorear los flujos de eventos que llegan a la plataforma central 320. Por lo tanto, se selecciona al menos un modelo de procesamiento y se utiliza para determinar cuándo se debe crear una situación. Pueden marcarse eventos como que están suprimidos después de la clasificación, y el/los modelo(s) que evalúan los eventos pueden o bien ignorar la indicación de supresión y procesar los eventos suprimidos o bien usar la indicación de supresión para ignorar los eventos suprimidos. Las funciones de correlación y agregación 322 y 324 pueden impulsarse por las reglas y los modelos que las reglas especifican durante la clasificación de eventos.

Se utilizan una o más funciones de creación de tickets 414 en la plataforma central 320 en este caso. Las situaciones identificadas pueden distribuirse a las funciones de creación de tickets 414 basándose en las reglas cargadas de las políticas, que indican qué funciones de creación de tickets 414 son apropiadas para qué situaciones. Una vez que los eventos se procesan dentro de la plataforma central 320, los eventos o situaciones se ponen a disposición para escalar a cualquier número de destinos adicionales 416, tales como terminales, procesadores o usuarios, para registrar, analizar, acciones correctivas/preventivas u otras funciones.

En algunas realizaciones, la plataforma central 320 proporciona la aglomeración de eventos relacionados en situaciones de impacto de servicio. Tal aglomeración permite, en algunos ejemplos, una reducción del 65% o más del ruido de monitorización aglomerando o agrupando eventos analíticamente similares, excluyendo eventos duplicados, e identificando eventos analíticamente únicos.

Pueden además procesarse situaciones, como ocurre con eventos, en múltiples modelos de situaciones, como modelos definidos por el usuario y/o descubiertos. Debido a las funciones de registro de evento/situación y tickets del sistema de monitorización de tejido 110, puede proporcionarse una pista de auditoría transparente y completa de todos los eventos y situaciones. Además, el registro, la categorización y la auditoría de eventos y situaciones proporciona la capacidad de analizar e identificar tendencias, valores atípicos, situaciones falsas y otros datos asociados a los eventos y situaciones.

La figura 5 ilustra detalles adicionales de cómo los eventos pueden procesarse dentro de realizaciones específicas de la plataforma central 320. Como se muestra en la figura 5, diversas fuentes de eventos 502 proporcionan eventos al sistema de monitorización de tejido 110. Las fuentes de eventos 502 incluyen aplicaciones, servidores anfitriones y dispositivos de usuario que pueden proporcionar eventos al sistema de monitorización de tejido 110, tal como mediante el uso de agentes de eventos 310. Los eventos se informan a través de un bus de eventos 504, que puede denotar

una cola u otra estructura configurada para recibir eventos. El bus de eventos 504 puede utilizarse, por ejemplo, en la plataforma de monitorización 314 o en la plataforma central 320.

Un sistema de procesamiento de eventos 504 incluye un módulo de registro de eventos 508, un módulo de evaluación de modelos 510 y un módulo de enriquecimiento de situaciones 512. El módulo de registro de eventos 508 puede identificar eventos entrantes, asignar identificadores únicos a los eventos y realizar otras operaciones relacionadas con los eventos entrantes. El módulo de evaluación de modelos 510 procesa los eventos para identificar diversas situaciones asociadas a los eventos. El módulo de enriquecimiento de situaciones 512 procesa las situaciones identificadas y proporciona información adicional sobre las situaciones identificadas.

Estos módulos 508-512 extraen datos e información de un almacén de políticas de eventos 514, un almacén de eventos/situaciones 516 y un almacén de indicador de proceso clave (KPI) 518. También se proporciona una pista de auditoría y un módulo de rastreo 520 y un visualizador de eventos/situaciones 522 u otra interfaz de usuario. El almacén de políticas de eventos 514 indica un almacenamiento en el que se almacenan diversas políticas definidas por el usuario u otras, como cuando se reciben políticas del repositorio 336. El almacén de eventos/situaciones 516 almacena información sobre eventos recibidos y situaciones identificadas. El almacén KPI b proporciona información sobre mediciones capturadas por el sistema de monitorización de tejido 110 y cómo se utilizan las mediciones. La pista de auditoría y el módulo de rastreo 520 rastrea información sobre eventos y situaciones y almacena la información, incluyendo información sobre los eventos y situaciones en sí mismos y cómo se resuelven las situaciones. El visualizador de eventos/situaciones 522 proporciona una interfaz de usuario para interactuar con el sistema de monitorización de tejido 110 y ver resultados obtenidos por el sistema de monitorización de tejido 110.

El sistema de procesamiento de eventos 504 proporciona eventos agrupados y categorizados definiendo situaciones en un bus de situaciones 524, lo que podría denotar una cola u otra estructura configurada para enviar las situaciones. Las situaciones en este caso se envían a los destinos 526, así como a consolas, dispositivos y servicios de mensajería para el conocimiento de usuario y a servidores y procesadores para el procesamiento automatizado.

El uso de una arquitectura de monitorización basada en tejido en el sistema 110 para soportar procesamiento de eventos complejo como se muestran en este caso las transiciones fuera de las alertas de fallo del sistema de empresa, como se encontró con las capacidades anteriores de monitorización de empresa. En cambio, el sistema de monitorización de tejido 110 permite el conocimiento de eventos/situacional a través de un sistema de empresa. En las realizaciones de ejemplo mostradas en este caso, la clasificación de eventos incluye definiciones de autoservicio de procesamiento de eventos a través del uso de un lenguaje de definición de monitorización (como un DSL) y la separación u otra categorización de flujos de eventos en dominios para el aislamiento. Modelos de procesamiento dentro del sistema de monitorización de tejido 110 definen cómo procesar eventos en situaciones y cómo gestionar eventos individuales. Pueden definirse modelos de cualquier manera para categorizar mejor eventos anticipados en el sistema de empresa. Por ejemplo, los modelos pueden procesar eventos en situaciones por frecuencia de evento, tipo de evento, ubicación o impacto local de evento, o fuente de evento (como influencia externa en el sistema de empresa, como *hacking*, uso no registrado, uso no autorizado o uso múltiple por el mismo usuario). También pueden utilizarse modelos analíticos para aglomerar eventos en situaciones con la misma causa de origen, la misma ubicación geográfica o la misma ocurrencia de fecha/hora.

En realizaciones de ejemplo, las señales que representan eventos sintéticos pueden generarse por el sistema de monitorización de tejido 110 para un ítem dependiente basándose en una fuente de datos de referencia conectable. Por ejemplo, un evento asociado con la caída de un anfitrión puede conducir a la generación de un evento sintético para el despliegue de aplicaciones. Además, en realizaciones de ejemplo, el sistema de monitorización de tejido 110 proporciona transparencia total del procesamiento, mostrando cómo y por qué los eventos se agrupan o procesan en una situación o situaciones.

El uso del sistema de monitorización de tejido 110 es totalmente resistente, y el sistema de monitorización de tejido 110 puede escalarse en múltiples dimensiones. Por ejemplo, el número de nodos informáticos 112 utilizado en el sistema de monitorización de tejido 110 puede ajustarse basándose en la carga, y el número de instancias del sistema de monitorización de tejido 110 (el número de tramas) también puede ajustarse basándose en la carga. En algunos casos, el sistema de monitorización de tejido 110 puede manejar hasta mil eventos por minuto o más. Como un ejemplo particular, el sistema de monitorización de tejido 110 puede (de media) recibir alrededor de 2,8 millones de eventos, procesar alrededor de 1,7 millones de eventos (estando el resto suprimidos) e identificar aproximadamente 130.000 situaciones diarias para una instalación específica.

En algunas realizaciones, el sistema de monitorización de tejido 110 puede soportar una arquitectura de mensajería conectable, por ejemplo mediante el uso de cualquier mensajería compatible con SERVICIO DE MENSAJES JAVA (JMS). El sistema de monitorización de tejido 110 también puede soportar el enriquecimiento de servicios y eventos a través de una o más fuentes de datos de referencia, y correlaciones de eventos integradas pueden hacerse a través de métodos analíticos descubiertos y modelados. El sistema de monitorización de tejido 110 puede conectarse fácilmente a marcos de trabajo de automatización externos, soportar API de sumisión y supresión de eventos y soportar definiciones de políticas de eventos a través de un DSL autodefinido. El sistema de monitorización de tejido 110 puede proporcionar la capacidad de construir modelos de situación personalizados, la capacidad de rastrear

eventos y situaciones, y proporcionar un marco de trabajo que es independiente de agente.

En la figura 6 se muestra un uso de ejemplo de un lenguaje de definición de monitorización. Un lenguaje específico de dominio permite a los usuarios describir por sí mismos eventos y cómo procesar los eventos. Esta información puede proporcionarse al gestor de políticas 334 y almacenarse como políticas en el repositorio 336. Como se muestra en la figura 6, un usuario puede definir múltiples archivos de eventos 602, cada uno de los cuales define uno o más tipos de eventos. El usuario también puede combinar múltiples archivos de eventos 602 en un único archivo de modelo de procesamiento 604, que puede utilizarse para identificar la ocurrencia de una situación. Este tipo de funcionalidad puede utilizarse por cualquier número de usuarios para definir eventos de interés y definir cómo esos eventos se agrupan en situaciones.

El uso de un lenguaje de definición de monitorización permite a equipos de personal gestionar más fácilmente la monitorización realizada por el sistema de monitorización de tejido 110. También proporciona una mejor transparencia en cuanto a cómo se están procesando los eventos, así como la cobertura y el uso del sistema de monitorización de tejido 110. Además, el uso de un lenguaje de definición de monitorización puede proporcionar controles entorno a la publicación de cambios y la liberación de cambios para reglas.

En algunas realizaciones, el lenguaje de definición de monitorización puede utilizarse para definir paquetes que contienen definiciones de eventos, cómo se produce la monitorización para esos eventos y cómo se identifican situaciones como resultado de la monitorización. Lo siguiente representa un ejemplo de un paquete que puede definirse usando un lenguaje de definición de monitorización.

```
package {
  //alcance - dar valores a las entidades de appdir para los eventos de interés
      “did” : [],
      “app”: [“15075”],
      “fam” : [],
      “subbu” : [],
      “bu” : [],
```

```
    //enrutar - escalamientos por defecto
        "rota" : ["gs-my-app-support"]
}
event_set "CapacityMgmt" {
        rule "HighCPU" = "CPU.Busy(threshold:95,operator:>,frequency:60)"
        rule "HighMemory" = "Memory.Used(threshold:95,operator:>,frequency:60)"
        rule "HighDisk" =
"Filesystem.Used(target:All,threshold:95,operator:>,frequency:60)"
}
event_set "AppAvailable" {
        rule "ProcessUp" = Process.Count(threshold:1,operator:=,frequency:60)
        rule "UIResponse" =
URL.ResponseStatus(threshold:200,URL="home.web.gs.com",frequency:60)
        subscribe = ["host_unreachable","db_temp_full","DB_MAX_CONN",
"DB_HOME_FS"]
}
monitor "MyCapacityMgmt" {
        processing = [ type = "OneForOne" , count = "1" , aggregated = "true" ]
//processing = [ type = "XOverTimeY" , count = "5", time = "200" ]
        event_set_ref = [ "CapacityMgmt" ]
        situation_ref = ["MC_Rota"]
        filter = [ "environment" == "prod" ]
        enrichment = [ "myTag" = "myvalue" ]
}
situation "MC_Rota" {
        Rota = [ "inform_rota" ]
        iconclude = [ flowId = "1234567" ]
}
```

Diversas funciones dentro del sistema de monitorización de tejido 110 permiten que se obtengan diversos beneficios. Por ejemplo, es posible integrar el sistema de monitorización de tejido 110 con plataformas de gestión de incidentes y automatización y proporcionar controles y soporte de ciclo de vida de desarrollo de sistemas (SDLC) para políticas de monitorización. También es posible utilizar el sistema de monitorización de tejido 110 para proporcionar visibilidad en situaciones de producción y funcionales en todas las unidades de negocio y aislar flujos de eventos mediante múltiples tramas. Una trama puede definirse como un conjunto de eventos asociados a una región o unidad de negocio que se procesa por una instancia separada del sistema de monitorización de tejido 110. Una trama puede tener sus propias instancias de mensajería, persistencia y procesamiento con instancias de servicio independientes. El funcionamiento de una trama puede ser independiente de otras tramas, y la comunicación entre tramas para correlaciones de a través de tramas puede producirse a través de eventos sintéticos.

Cabe señalar que cada una de las plataformas, funciones y módulos descritos anteriormente puede implementarse usando cualquier hardware adecuado o una combinación de hardware e instrucciones de software/firmware. En

realizaciones particulares, cada una de las plataformas, funciones y módulos incluye instrucciones de software ejecutadas por uno o más dispositivos de procesamiento. Múltiples dispositivos de procesamiento pueden ejecutar múltiples instancias de las plataformas, funciones y módulos, y los dispositivos de procesamiento pueden distribuirse a través de cualquier número de nodos de un sistema informático de tejido.

Aunque las figuras 3 a 6 ilustran un ejemplo de un sistema de monitorización de tejido 110 para gestionar eventos que implican sistemas informáticos y redes y detalles relacionados, pueden hacerse varios cambios a las figuras 3 a 6. Por ejemplo, las divisiones funcionales mostradas en las figuras 3 a 6 son solo para ilustración. Diversos componentes de las figuras 3 a 6 pueden combinarse, además de subdividirse, reorganizarse u omitirse y pueden añadirse componentes adicionales según necesidades particulares.

Las figuras 7 y 8 ilustran flujos de proceso de ejemplo en un sistema para gestionar eventos que implican sistemas informáticos y redes usando un sistema de monitorización de tejido y detalles relacionados según esta divulgación. En particular, la figura 7 ilustra un ejemplo de flujo de proceso 700 para gestionar eventos para identificar situaciones, mientras que la figura 8 ilustra un flujo de proceso de ejemplo 800 para gestionar situaciones identificadas. Cabe señalar que mientras que las figuras 7 y 8 se describen con respecto al sistema de monitorización de tejido 110 de la figura 1 que tiene la implementación como se muestra en las figuras 3 a 6, los flujos de proceso 700 y 800 pueden utilizarse con cualquier sistema de monitorización de tejido adecuado y en cualquier sistema adecuado.

Como se muestra en la figura 7, un evento ocurre dentro de un sistema de empresa y se proporciona a un sistema de monitorización de tejido en la etapa 702. Esto puede incluir, por ejemplo, un agente de eventos 310 que identifica un evento en un anfitrión 302 u otra fuente de eventos 502 y que proporciona el evento a la plataforma de monitorización 314 o al bus de eventos 504.

El evento se registra en la etapa 704. Esto puede incluir, por ejemplo, la plataforma de monitorización 314 o el módulo de registro de eventos 508 del sistema de procesamiento de eventos 504 que identifica el evento entrante y que realiza diversas acciones usando el evento. El registro de eventos ocurre en este caso usando diversos datos. Por ejemplo, el registro de eventos puede basarse en reglas obtenidas a partir de una o más políticas de monitorización de tejido, como reglas de autoservicio para hacer coincidir eventos con dominios de interés y para hacer coincidir eventos individuales con tipos de eventos específicos (como tipos predefinidos o tipos derivados). Datos de referencia también pueden proporcionar consultas sobre reglas u otra categorización de eventos para facilitar el registro de eventos. Durante el registro de eventos, los eventos pueden coincidir con patrones y valores especificados en las políticas. Después de que un evento ha coincidido con una regla, el evento puede comprobarse para ver si el evento coincide con cualquier criterio de supresión cargado desde el sistema de políticas. Si lo hace, el evento puede anotarse como que está dentro de un intervalo de supresión de modo que puedan tenerse en cuenta uno o más modelos de procesamiento. Durante el registro de eventos, puede asignarse al evento un nombre de ítem, un nombre de evento, un tipo de modelo de procesamiento y (si no se ha asignado previamente) un identificador único (UID) de evento.

El evento se envía en la etapa 706 para su evaluación en la etapa 708. Esto puede incluir, por ejemplo, la plataforma central 320 o el módulo de evaluación de modelos 510 del sistema de procesamiento de eventos 504 que evalúa el evento para identificar si alguna situación está indicada por el evento. La plataforma central 320 o el módulo de evaluación de modelos 510 pueden recibir diversas entradas para procesar un flujo de eventos, como múltiples entradas para cada nombre de ítem, en situaciones. Las entradas a la plataforma central 320 o al módulo de evaluación de modelos 510 pueden incluir reglas de políticas de tejido y otra información de modelo, información de estado de situación y modelo, y datos de referencia de empresa. La plataforma central 320 o módulo de evaluación de modelos 510 procesa el evento como el último en un flujo de eventos que forman potencialmente una situación. En algunas realizaciones, la creación de una situación puede definir por sí misma un evento.

Cualquier situación identificada se envía en la etapa 710. Esto puede incluir, por ejemplo, la plataforma central 320 o el módulo de evaluación de modelos 510 del sistema de procesamiento de eventos 504 que envía la situación identificada y cualquier información relacionada.

Como se muestra en la figura 8, una vez que se identifica una situación a partir de un flujo de eventos y según políticas de tejido aplicables, la situación se envía e introduce en un servicio de distribución de bus de situación en la etapa 802. Desde el bus de servicio 524, la situación puede enviarse a diversos dispositivos o sistemas, como diversos sistemas de tickets de evento/situación, dependiendo de la situación. Por ejemplo, si se permite o es posible la resolución automatizada de una situación, la situación puede enviarse a un agente de automatización en la etapa 804. El agente de automatización puede denotar una aplicación u otra lógica que realice alguna función o funciones para resolver automáticamente una situación dada. Si no es posible o no se permite la resolución automatizada de una situación y se identifica o asocia un sistema específico de tickets con la situación, la situación puede enviarse a un agente de incidentes y de tickets en la etapa 806. El agente de incidentes y de tickets puede entonces generar tickets u otras notificaciones de acuerdo con los detalles de ese sistema de tickets e incidentes. El agente de tickets e incidentes puede devolver un identificador de referencia para la situación y una indicación de que la situación debe cerrarse.

Si no se identifica ningún agente de incidentes y tickets, puede proporcionarse una situación a un agente de tickets

ligero en la etapa 808. El agente de tickets ligero incluye una base de datos de persistencia de tickets que soporta el almacenamiento de situaciones en la etapa 810 y recibe entrada de uno o más servicios de ejecución. El agente de tickets ligero transforma el ticket en una alerta, sirve como puente para la intervención en vivo de la situación y genera correos electrónicos, notificaciones de mensajes u otras notificaciones a usuarios o partes interesadas relevantes. En este ejemplo, el agente de tickets ligero puede proporcionar uno o más temas de mensajería (como alertas) a un servicio de almacenamiento en caché de alertas en la etapa 812, que puede notificar a uno o más usuarios de las alertas a través de al menos una consola en la etapa 814. Usando la(s) consola(s), el/los usuario(s) pueden identificar diversas acciones de alerta que van a realizarse para cada alerta, como asignar o cerrar la alerta. Las acciones de alerta se proporcionan a uno o más servicios de ejecución en la etapa 816, que pueden tomar medidas para implementar las acciones de alerta seleccionadas. Por ejemplo, los servicios de ejecución pueden emitir acciones de "tejido de procesamiento de eventos" (EPF) para implementarse por el agente de tickets ligero en la etapa 818 y/o por otro núcleo informático de tejido en la etapa 820.

Aunque las figuras 7 y 8 ilustran ejemplos de flujos de proceso 700 y 800 en un sistema para gestionar eventos que implica sistemas informáticos y redes usando un sistema de monitorización de tejido y detalles relacionados, pueden hacerse diversos cambios a las figuras 7 y 8. Por ejemplo, pueden superponerse diversas etapas en cada figura, ocurrir en paralelo, ocurrir en un orden diferente u ocurrir cualquier número de veces. Además, los flujos de proceso mostrados en este caso pueden variar dependiendo de cómo se identifican y se convierten eventos en situaciones y cómo se gestionan situaciones en sistemas de monitorización de tejido particulares.

El uso del sistema de monitorización de tejido 110 como se describe anteriormente para monitorización, diagnóstico y mantenimiento de sistemas informáticos o redes 102a-102n proporciona soluciones técnicas a problemas técnicos en el campo de la gestión informática y de redes. Como se ha señalado anteriormente, los eventos gestionados por el sistema de monitorización de tejido 110 pueden relacionarse con estados actuales o cambios en los estados actuales de dispositivos, sistemas o redes, así como anomalías u ocurrencias de condiciones definidas, dentro de los sistemas informáticos o redes 102a-102n. Para sistemas de empresas grandes, el número de eventos puede ser masivo, a veces ascendiendo a miles por minuto. Esto hace que sea extremadamente difícil o imposible para el personal revisar y resolver manualmente los eventos e identificar eventos relacionados que puedan ser indicativos de infracciones de seguridad más graves u otros problemas en los sistemas informáticos o redes 102a-102n.

El sistema de monitorización de tejido 110 soporta la identificación automatizada de eventos, así como la clasificación automatizada de eventos y la identificación de situaciones de eventos relacionados. Esto hace mucho más fácil gestionar los eventos, identificar situaciones a resolver y posiblemente incluso resolver las situaciones automáticamente. Entre otras cosas, esto puede ayudar a mantener los sistemas informáticos o redes 102a-102n funcionando de manera más satisfactoria y resolver las cuestiones que surjan. Además, como se señaló anteriormente, esto puede hacerse de manera personalizable, tal como definiendo eventos, cómo se produce la monitorización para los eventos y cómo se usan los eventos para identificar situaciones. Esto proporciona una gran flexibilidad en el uso del sistema de monitorización de tejido 110. También se han proporcionado anteriormente otras características técnicas.

En algunas realizaciones, se implementan diversas funciones descritas en este documento de patente se implementan o se soportan por un programa informático que se forma a partir de un código de programa legible por ordenador y que se incorpora en un medio legible por ordenador. La frase "código de programa legible por ordenador" incluye cualquier tipo de código informático, incluyendo código fuente, código objeto y código ejecutable. La frase "medio legible por ordenador" incluye cualquier tipo de medio al que se puede acceder mediante un ordenador, tal como memoria de solo lectura (ROM), memoria de acceso aleatorio (RAM), una unidad de disco duro, un disco compacto (CD), un disco de vídeo digital (DVD) o cualquier otro tipo de memoria. Un medio legible por ordenador "no transitorio" excluye enlaces de comunicación por cable, inalámbricos, ópticos o de otro tipo que transporten señales eléctricas transitorias u otras señales. Un medio legible por ordenador no transitorio incluye medios en los que los datos pueden almacenarse permanentemente y medios en los que los datos pueden almacenarse y sobreescribirse posteriormente, como un disco óptico reescribible o un dispositivo de memoria borrable.

Puede resultar ventajoso establecer definiciones de determinadas palabras y frases utilizadas a lo largo de este documento de patente. Los términos "aplicación" y "programa" se refieren a uno o más programas informáticos, componentes de software, conjuntos de instrucciones, procedimientos, funciones, objetos, clases, instancias, datos relacionados o una parte de los mismos adaptada para su implementación en un código informático adecuado (incluyendo código fuente, código objeto, o código ejecutable). El término "comunicar", así como derivados del mismo, abarca tanto la comunicación directa como la indirecta. Los términos "incluir" y "comprender", así como derivados de los mismos, significan inclusión sin limitación. El término "o" es inclusivo, significando y/o. La frase "asociado con", así como sus derivados, puede significar incluir, estar incluido dentro de, interconectar con, contener, estar contenido dentro de, conectar a o con, acoplar a o con, poder comunicarse con, cooperar con, intercalar, yuxtaponer, estar próximo a, estar vinculado a o con, tener, tener una propiedad de, tener una relación a o con, o similares. La frase "al menos uno de", cuando se utiliza con una lista de elementos, significa que pueden utilizarse diferentes combinaciones de uno o más de los elementos enumerados, y puede que solo se necesite un elemento de la lista. Por ejemplo, "al menos uno de: A, B y C" incluye cualquiera de las siguientes combinaciones: A, B, C, A y B, A y C, B y C, y A y B y C.

Aunque esta divulgación ha descrito determinadas realizaciones y métodos asociados generalmente, alteraciones y permutaciones de estas realizaciones y métodos serán evidentes para los expertos en la técnica. Por consiguiente, la descripción anterior de realizaciones de ejemplo no define o limita esta divulgación. También son posibles otros cambios, sustituciones y alteraciones sin apartarse del alcance de esta divulgación, tal como se define en las siguientes reivindicaciones.

REIVINDICACIONES

1. Método que comprende:

recibir, en un sistema de monitorización de tejido (110), información que identifica ocurrencias de eventos en un sistema de empresa que comprende múltiples sistemas de red o informáticos (102a, 102b, ..., 102n), ocurriendo en o implicando los eventos dispositivos de red o informáticos (104, 106) en los sistemas de red o informáticos (102a, 102b, ..., 102n), los eventos identificados usando reglas accesibles por el sistema de monitorización de tejido (110);

procesar, usando múltiples tramas, la información en tiempo real para identificar las ocurrencias de los eventos y asignar los eventos a múltiples situaciones, los eventos asignados a las situaciones usando uno o más modelos de procesamiento accesibles por el sistema de monitorización de tejido (110), comprendiendo cada trama una instancia separada del sistema de monitorización de tejido (110);

transmitir eventos sintéticos entre las tramas para soportar correlaciones de a través de tramas de los eventos o situaciones; y

enviar información que identifica las situaciones.

2. Sistema que comprende:

múltiples tramas, comprendiendo cada trama una instancia separada de un sistema de monitorización de tejido (110), comprendiendo el sistema de monitorización de tejido (110) múltiples nodos informáticos (112) y múltiples enlaces de comunicación (114) que acoplan los nodos informáticos (112), en el que:

el sistema de monitorización de tejido está configurado para recibir información que identifica ocurrencias de eventos en un sistema de empresa que comprende múltiples sistemas de red o informáticos (102a, 102b, ..., 102n), ocurriendo en o implicando los eventos dispositivos de red o informáticos (104, 106) en los sistemas de red o informáticos (102a, 102b, ..., 102n), los eventos identificados usando reglas accesibles por el sistema de monitorización de tejido (110);

cada una de las múltiples tramas está configurada para procesar al menos una parte de la información en tiempo real para identificar las ocurrencias de los eventos y asignar los eventos a múltiples situaciones, los eventos asignados a las situaciones usando uno o más modelos de procesamiento accesibles por el sistema de monitorización de tejido (110);

cada una de las múltiples tramas está configurada para generar y transmitir eventos sintéticos a otras tramas con el fin de soportar correlaciones de a través de tramas de los eventos o situaciones; y

el sistema de monitorización de tejido está configurado para enviar información que identifica las situaciones.

3. Método según la reivindicación 1 o el sistema según la reivindicación 2, en el que el sistema de monitorización de tejido (110) es escalable en múltiples dimensiones, una dimensión asociada a un número de nodos informáticos (112) que funcionan en el sistema de monitorización de tejido (110), otra dimensión asociada con un número de tramas.

4. Método según la reivindicación 1, que comprende además:

almacenar información asociada con los eventos y situaciones, incluyendo información sobre los eventos y situaciones e información sobre cómo se resuelven las situaciones, para proporcionar una pista de auditoría para los eventos y situaciones; o

sistema según la reivindicación 2, en el que el sistema de monitorización de tejido (110) está configurado además para almacenar información asociada a los eventos y situaciones, incluyendo información sobre los eventos y situaciones e información sobre cómo se resuelven las situaciones, para proporcionar una pista de auditoría para los eventos y situaciones.

5. Método según la reivindicación 1, que comprende además:

obtener las reglas de una o más políticas, al menos una parte de las una o más políticas definidas por al menos un usuario usando un lenguaje de definición de monitorización; o

sistema según la reivindicación 2, que comprende además:

un repositorio (336) configurado para almacenar una o más políticas que comprenden las reglas, al menos

una parte de las una o más políticas definidas por al menos un usuario usando un lenguaje de definición de monitorización.

6. Método según la reivindicación 1 o sistema según la reivindicación 2, en el que los uno o más modelos de procesamiento definen cómo categorizar los eventos e identificar las situaciones, incluyendo los uno o más modelos de procesamiento:

al menos un modelo definido por el usuario definido por al menos un usuario; y

al menos un modelo analítico que define una o más funciones analíticas que funcionan usando la información que identifica las ocurrencias de los eventos.

7. Método según la reivindicación 1, que comprende además:

ser sensible a la identificación de las situaciones por cada una de las múltiples tramas, creando los eventos sintéticos, en el que cada trama de las múltiples tramas funciona de manera independiente; o

sistema según la reivindicación 2, en el que cada trama está configurada además para:

ser sensible a la identificación de las situaciones por cada una de las múltiples tramas, crear los eventos sintéticos, en el que cada trama de las múltiples tramas funciona de manera independiente.

8. Método según la reivindicación 7, en el que diferentes tramas procesan eventos que se asocian con al menos uno de:

diferentes ítems en los sistemas de red o informáticos (102a, 102b, ..., 102n);

diferentes ubicaciones en las que se despliegan los sistemas de red o informáticos (102a, 102b, ..., 102n);

diferentes despliegues de hardware, software o firmware en los sistemas de red o informáticos (102a, 102b, ..., 102n);

diferentes unidades de negocio que usan los sistemas de red o informáticos (102a, 102b, ..., 102n); y

diferentes tipos de negocio que se gestionan usando los sistemas de red o informáticos (102a, 102b, ..., 102n); o

sistema según la reivindicación 2, en el que diferentes tramas están configuradas para procesar eventos que se asocian con al menos uno de:

diferentes ítems en los sistemas de red o informáticos (102a, 102b, ..., 102n);

diferentes ubicaciones en las que se despliegan los sistemas de red o informáticos (102a, 102b, ..., 102n);

diferentes despliegues de hardware, software o firmware en los sistemas de red o informáticos (102a, 102b, ..., 102n);

diferentes unidades de negocio que usan los sistemas de red o informáticos (102a, 102b, ..., 102n); y

diferentes tipos de negocio que se gestionan usando los sistemas de red o informáticos (102a, 102b, ..., 102n).

9. Método según la reivindicación 1 o sistema según la reivindicación 2, en el que los eventos comprenden al menos uno de:

estados actuales de los dispositivos de red o informáticos (104, 106) en los sistemas de red o informáticos (102a, 102b, ..., 102n);

cambios en los estados actuales de los dispositivos de red o informáticos (104, 106) en los sistemas de red o informáticos (102a, 102b, ..., 102n);

anomalías en los dispositivos de red o informáticos (104, 106) en los sistemas de red o informáticos (102a, 102b, ..., 102n); y

ocurrencias de condiciones definidas dentro de los sistemas de red o informáticos (102a, 102b, ..., 102n).

10. Método según la reivindicación 1, en el que enviar la información que identifica las situaciones comprende:

proporcionar información que identifica al menos una de las situaciones a un agente automatizado que resuelve automáticamente la al menos una situación; o

sistema según la reivindicación 2, en el que el sistema de monitorización de tejido (110) está configurado para enviar la información que identifica las situaciones proporcionando información que identifica al menos una de las situaciones a un agente automatizado que resuelve automáticamente la al menos una situación.

11. Método según la reivindicación 1, en el que enviar la información que identifica las situaciones comprende:

proporcionar información que identifica al menos una de las situaciones a un agente de tickets que genere al menos una notificación para el personal, la al menos identificando una notificación la al menos una situación; o

sistema según la reivindicación 2, en el que el sistema de monitorización de tejido (110) está configurado para enviar la información que identifica las situaciones proporcionando información que identifica al menos una de las situaciones a un agente de tickets que genera al menos una notificación para personal, la al menos identificando una notificación la al menos una situación.

12. Sistema según la reivindicación 7, en el que cada trama está configurada para generar al menos algunos de los eventos sintéticos tras la identificación de situaciones por esa trama.

13. Medio legible por ordenador no transitorio que contiene código de programa legible por ordenador que, cuando se ejecuta por nodos informáticos (112) de un sistema de monitorización de tejido (110), provoca que los nodos informáticos (112) realicen el método según la reivindicación 1.

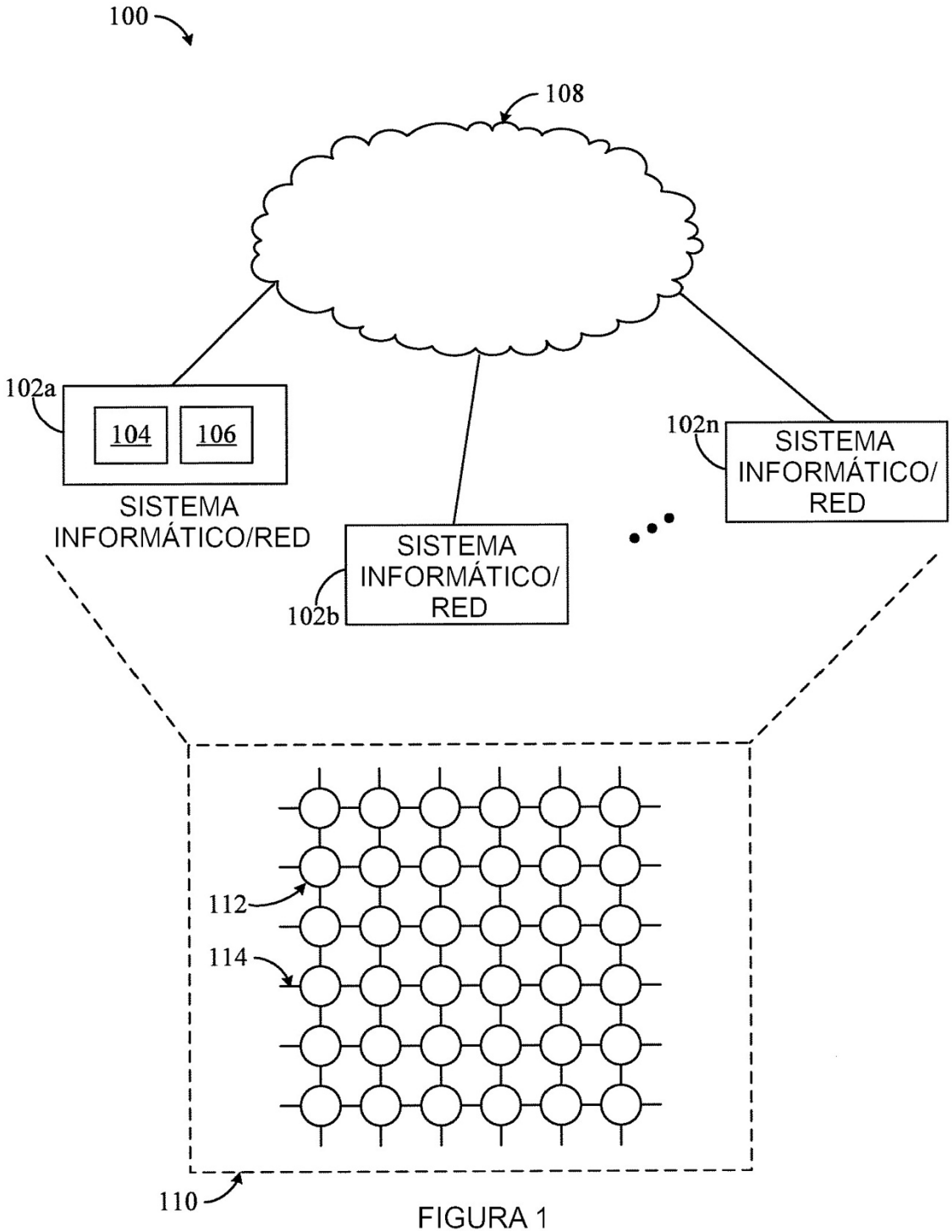
100
108
102a
104
106
SISTEMA INFORMÁTICO/RED
102b
SISTEMA INFORMÁTICO/ RED
102n
SISTEMA INFORMÁTICO/ RED
112
114
110

FIGURA 1

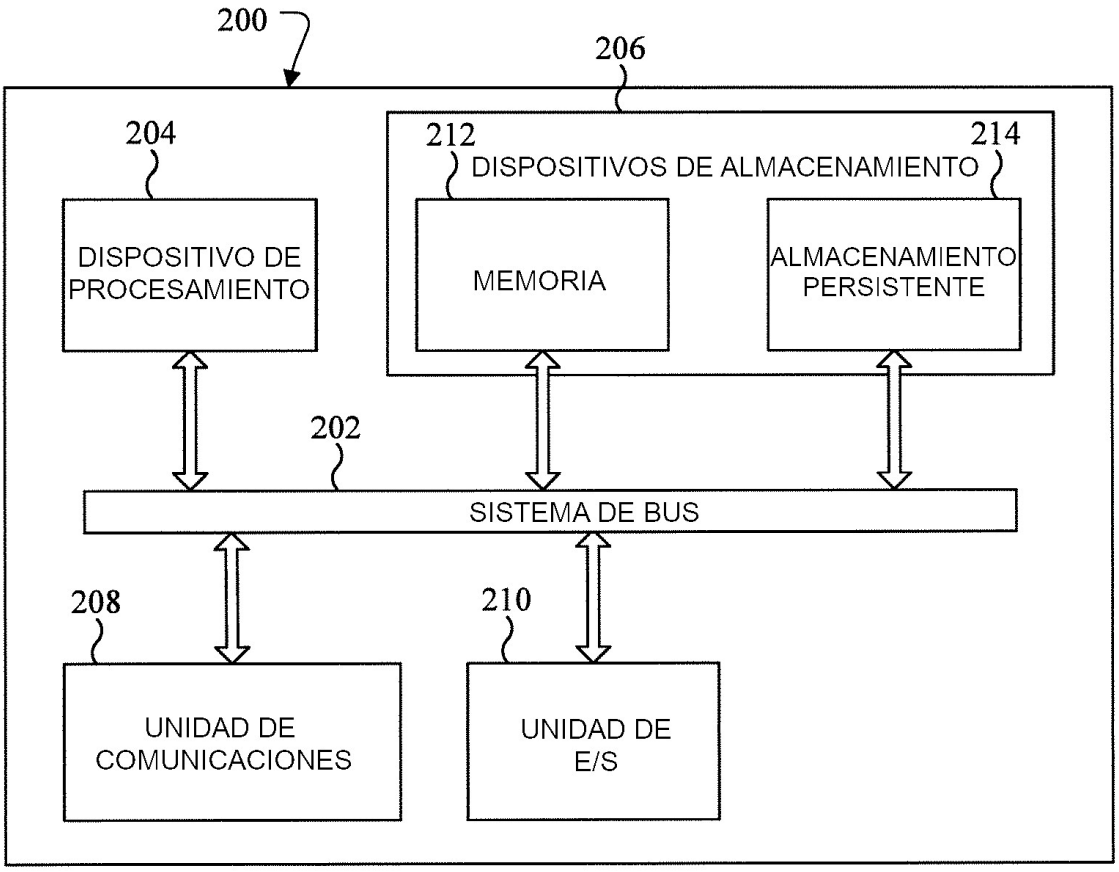
200
206
204
212
DISPOSITIVOS DE ALMACENAMIENTO
214
DISPOSITIVO DE PROCESAMIENTO
MEMORIA
ALMACENAMIENTO PERSISTENTE
202
SISTEMA DE BUS
208
210
UNIDAD DE COMUNICACIONES
UNIDAD DE E/S

FIGURA 2

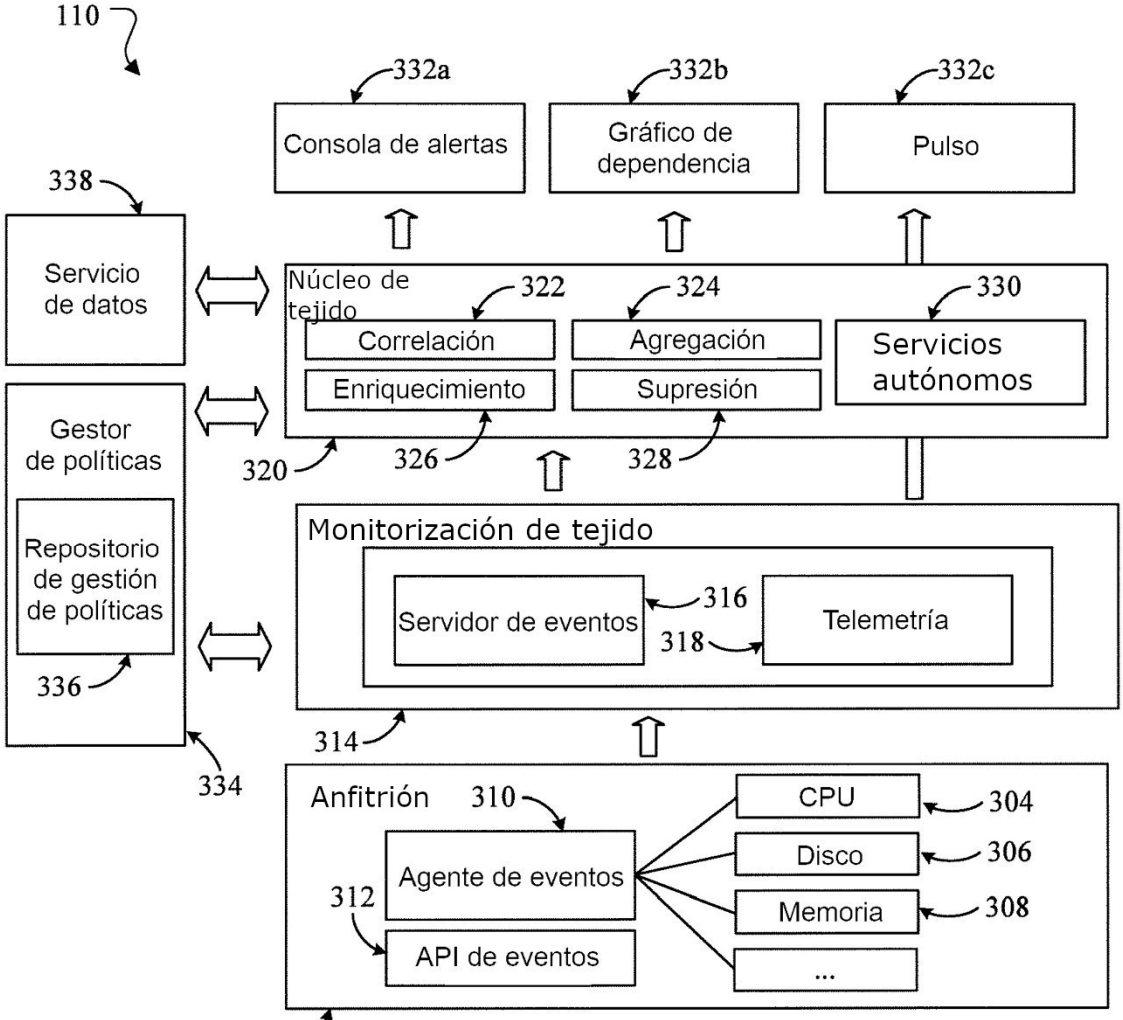
110
332a
332b
332c
Consola de alertas
Gráfico de dependencia
Pulso
338
Servicio de datos
Núcleo de tejido
322
324
330
Correlación
Agregación
Servicios autónomos
Enriquecimiento
Supresión
Gestor de políticas
Repositorio de gestión de políticas
320
326
328
Monitorización de tejido
Servidor de eventos
316
318
Telemetría
336
314
334
Anfitrión
310
CPU
304
Agente de eventos
Disco
306
312
Memoria
308
API de eventos
...
302

FIGURA 3

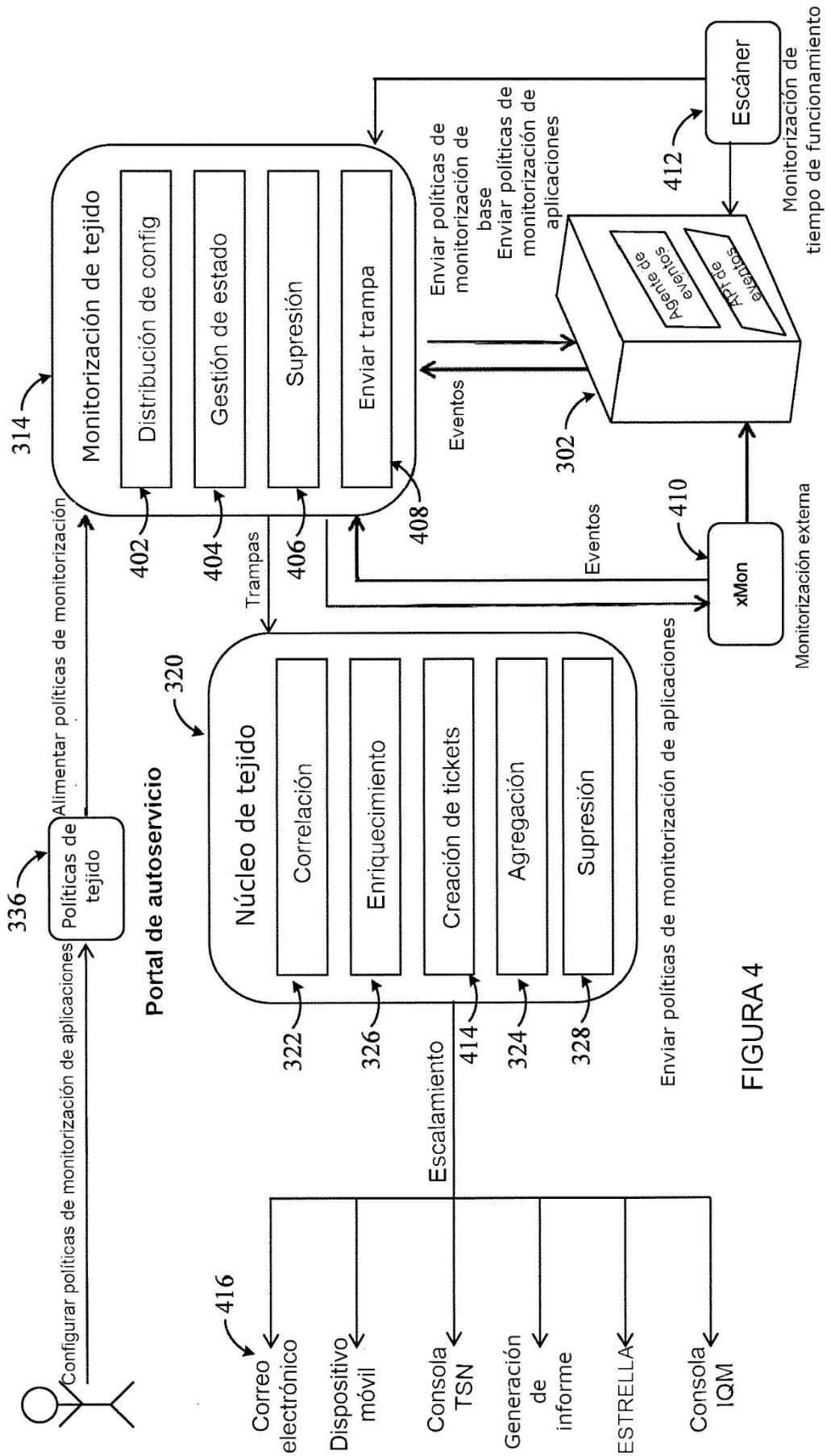
Monitorización de tejido
Distribución de config
Gestión de estado
Supresión
Enviar trampa
314
402
404
406
408
Trampas
Eventos
Enviar políticas de monitorización de base
Enviar políticas de monitorización de aplicaciones
Escáner
412
Monitorización de tiempo de funcionamiento
Agente de eventos
API de eventos
302
xMon
410
Monitorización externa
Alimentar políticas de monitorización
Políticas de tejido
336
Portal de autoservicio
Núcleo de tejido
320
Correlación
Enriquecimiento
Creación de tickets
Agregación
Supresión
322
326
414
324
328
Escalamiento
Enviar políticas de monitorización de aplicaciones
Configurar políticas de monitorización de aplicaciones
416
Correo electrónico
Dispositivo móvil
Consola TSN
Generación de informe
ESTRELLA
Consola IQM

FIGURA 4

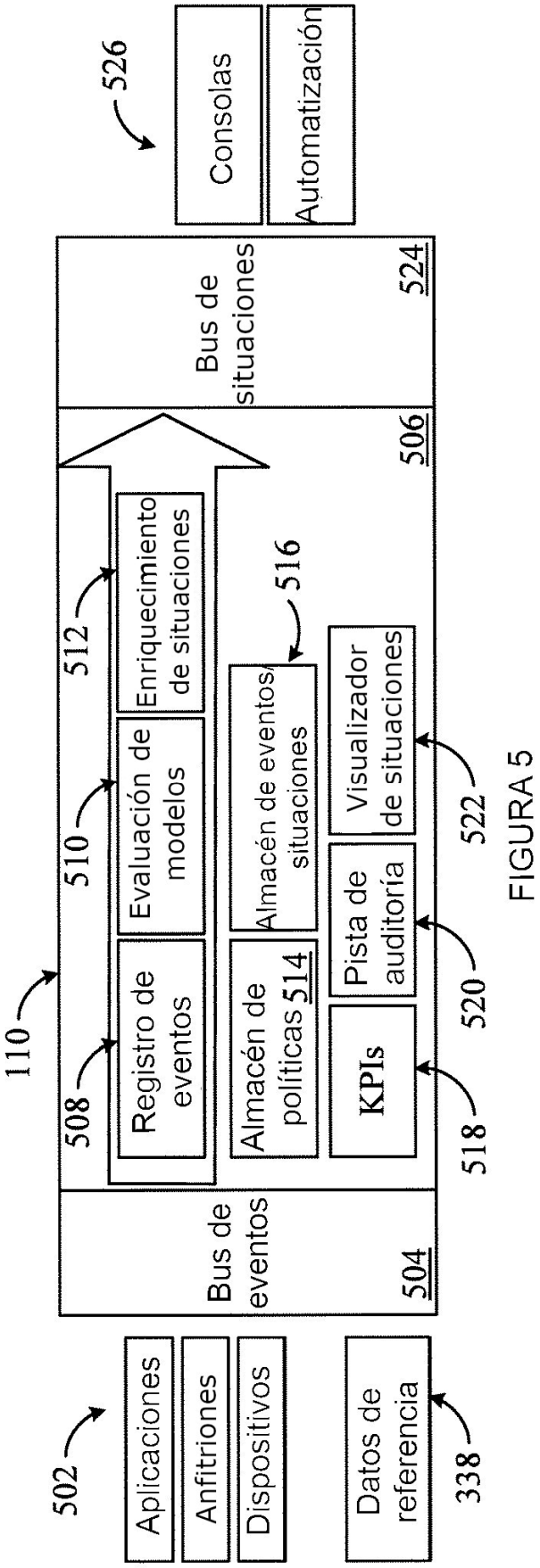
526
Consolas
Automatización
Bus de situaciones
524
506
512
Enriquecimiento de situaciones
510
Evaluación de modelos
516
Almacén de eventos situaciones
Visualizador de situaciones
522
110
508
Registro de eventos
Almacén de políticas 514
Pista de auditoría
520
KPIs
518
Bus de eventos
504
502
Aplicaciones
Anfitriones
Dispositivos
Datos de referencia
338

FIGURA 5

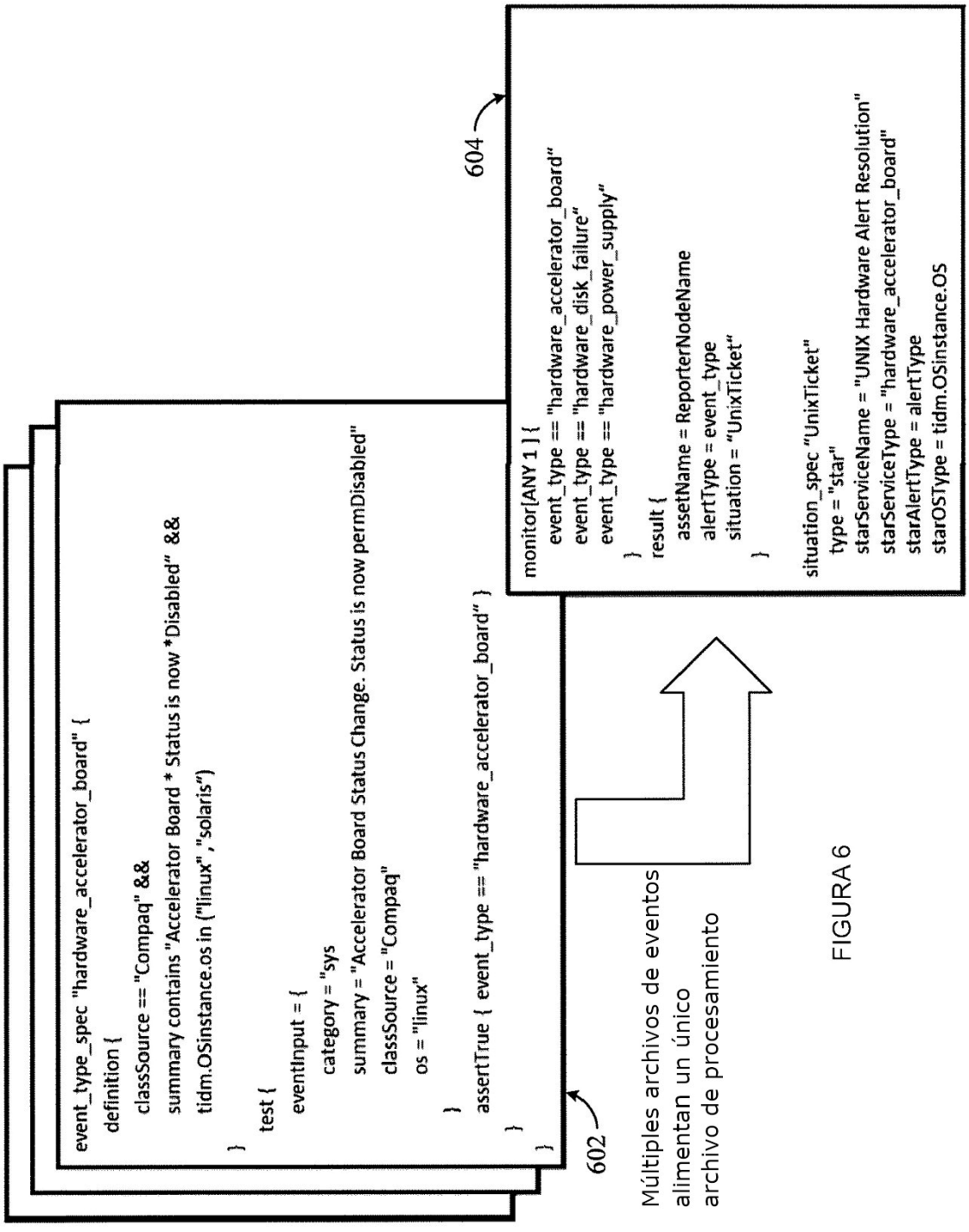
event_type_spec "hardware_accelerator_board" {
definition {
className == "Compaq" &&
summary contains "Accelerator Board * Status is now *Disabled" &&
tidm.OSinstance.os in ("linux", "solaris")
}
test {
eventInput = {
category = "sys
summary = "Accelerator Board Status Change. Status is now permDisabled"
className = "Compaq"
os = "linux"
}
assertTrue { event_type == "hardware_accelerator_board" }
}
}
602
Múltiples archivos de eventos alimentan un único archivo de procesamiento
604
monitor[ANY 1] {
event_type == "hardware_accelerator_board"
event_type == "hardware_disk_failure"
event_type == "hardware_power_supply"
}
result {
assetName = ReporterNodeName
alertType = event_type
situation = "UnixTicket"
}
situation_spec "UnixTicket"
type = "star"
starServiceName = "UNIX Hardware Alert Resolution"
starServiceType = "hardware_accelerator_board"
starAlertType = alertType
starOSType = tidm.OSinstance.OS

FIGURA 6

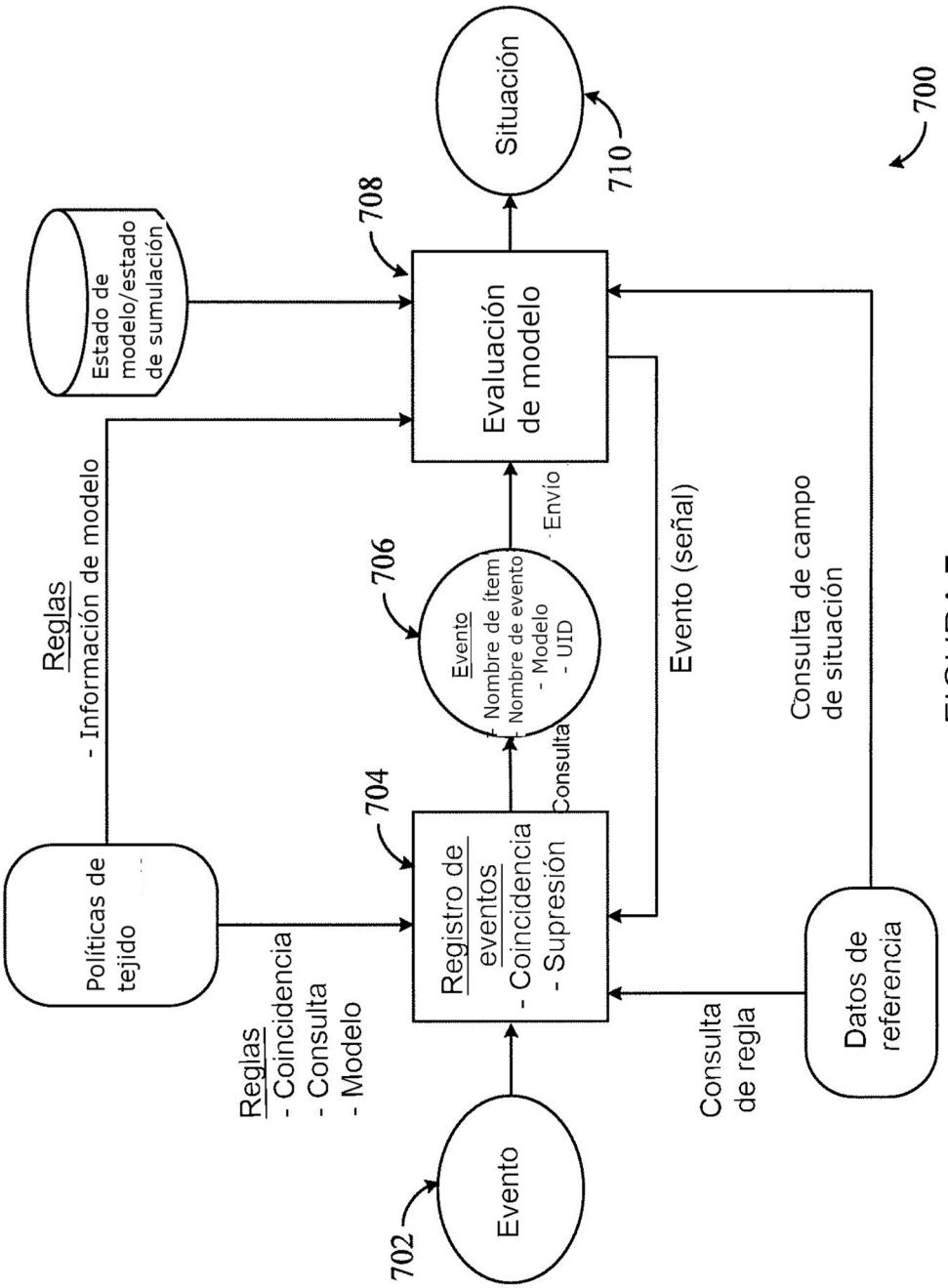
Situación
710
700
708
Estado de modelo/estado de sumulación
Evaluación de modelo
Reglas
- Información de modelo
706
Evento
Nombre de ítem
Nombre de evento
- Modelo
- UID
Envío
Evento (señal)
Consulta de campo de situación
Políticas de tejido
704
Registro de eventos
- Coincidencia
- Supresión
Consulta
Reglas
- Coincidencia
- Consulta
- Modelo
Consulta de regla
Datos de referencia
Evento
702

FIGURA 7

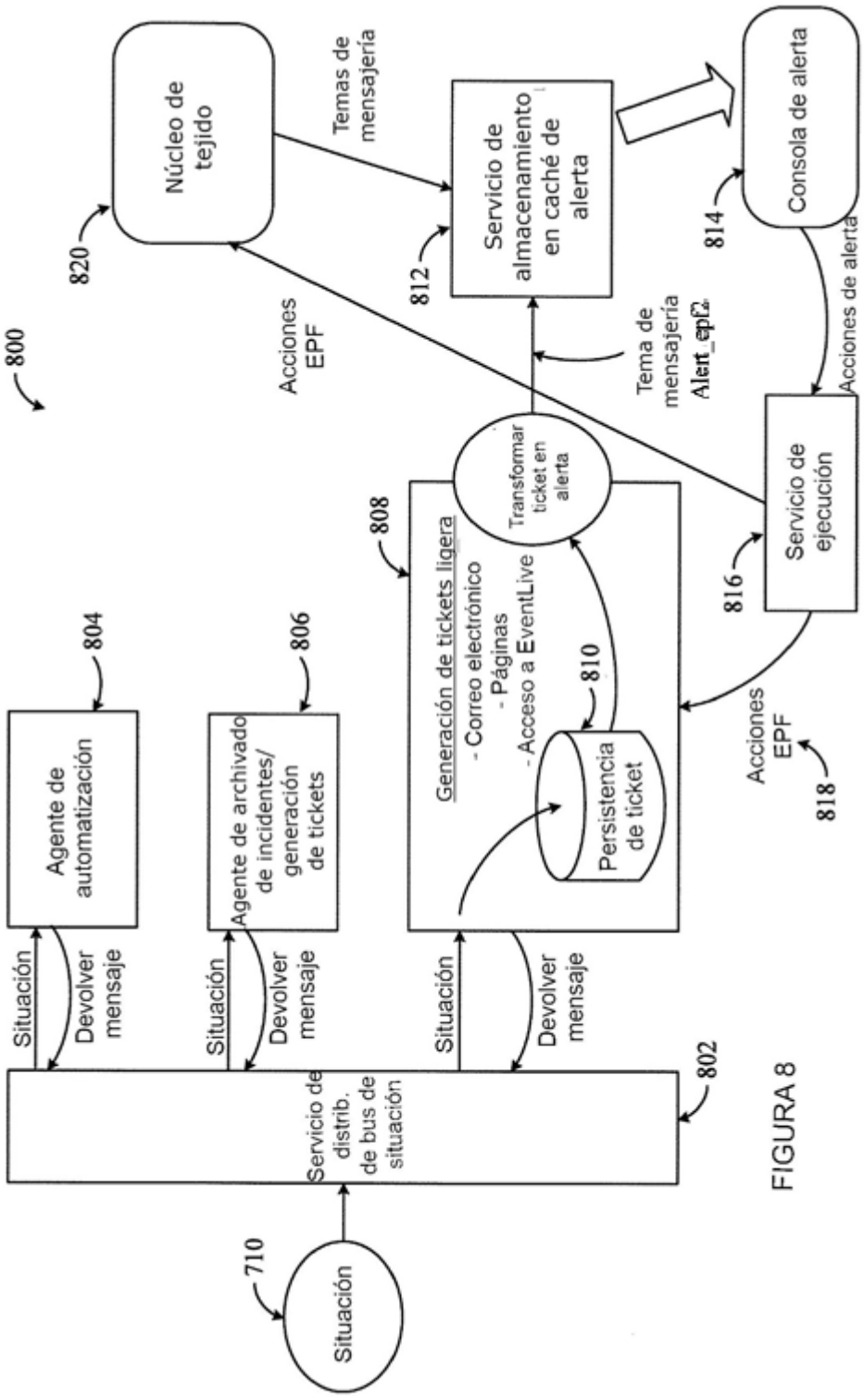
800
820
Núcleo de tejido
Temas de mensajería
812
Servicio de almacenamiento en caché de alerta
814
Consola de alerta
Acciones EPF
Tema de mensajería Alert_epf2
Acciones de alerta
808
Transformar ticket en alerta
Generación de tickets ligera
- Correo electrónico
- Páginas
- Acceso a EventLive
810
Persistencia de ticket
816
Servicio de ejecución
Acciones EPF
818
804
Agente de automatización
806
Agente de archivado de incidentes/ generación de tickets
Situación
Devolver mensaje
Situación
Devolver mensaje
Situación
Devolver mensaje
802
Servicio de distrib. de bus de situación
710
Situación

FIGURA 8