“Fault Trace” Sistema Detector de Fallas en Sistemas Distribuidos.

Kevin Cerón
Fidel Perez

1 Objetivo General del Sistema

Desarrollar y desplegar un sistema de monitoreo integral adaptable a diferentes sistemas distribuidos, denominado "Fault Trace", diseñado para optimizar la operación y gestión de infraestructuras tecnológicas complejas dentro de entornos corporativos. Este sistema aspira a proporcionar una solución robusta y fácil de usar que permita a empresas de desarrollo de software, como la del señor Gutiérrez, ofrecer un nuevo producto en el mercado que no solo mejore sus oportunidades comerciales sino que también ayude a sus clientes a supervisar y gestionar eficientemente sus sistemas. "Fault Trace" se enfocará en la detección de fallas, la gestión de recursos (físicos y virtuales), el análisis de tráfico de red, la identificación de cuellos de botella y picos de demanda, todo esto con el fin de facilitar una rápida respuesta a incidentes y una planificación estratégica de la infraestructura tecnológica basada en datos reales y comportamientos históricos de los sistemas. El sistema se distinguirá por su adaptabilidad a distintos tipos de sistemas y situaciones de alta demanda, asegurando una implementación no invasiva y una integración con las infraestructuras existentes de los clientes.

2 Problemas Identificados

- Dificultades en la gestión eficiente de usuarios y asignación de roles. Falta de sistemas que permitan una gestión clara y segura de accesos y permisos, aumentando el riesgo de brechas de seguridad y uso ineficiente de recursos.
- Incapacidad para diferenciar y monitorear adecuadamente servidores físicos de virtuales y sus métricas asociadas. Carencia de herramientas específicas para obtener visibilidad completa sobre ambos tipos de servidores, complicando la gestión de la infraestructura IT.
- Falta de una supervisión detallada del tráfico de red. Limitaciones en el análisis de tráfico de red impiden identificar eficazmente patrones anormales y potenciales amenazas, aumentando la vulnerabilidad frente a ataques cibernéticos.
- Ausencia de un sistema de notificaciones efectivo para eventos críticos y métricas de rendimiento. La falta de alertas proactivas y configurables reduce la capacidad

de respuesta ante incidentes críticos, afectando la continuidad y el rendimiento operacional.

- Ineficiencias en el monitoreo de respuestas y fallos de microservicios. Dificultades para monitorear arquitecturas basadas en microservicios, lo que puede resultar en interrupciones del servicio y degradación del rendimiento.
- Limitaciones en la supervisión de recursos a nivel de arquitectura. Falta de monitoreo adecuado de los recursos impide identificar y resolver eficientemente cuellos de botella.
- Falta de configuración personalizada de umbrales y alertas. La imposibilidad de ajustar umbrales y alertas a necesidades específicas limita la gestión proactiva y la capacidad para anticiparse a problemas.
- Carencia de integración efectiva con otros sistemas. La falta de integración con otros sistemas y herramientas limita la gestión holística de la infraestructura TI.
- Insuficiencia en la generación y visualización de métricas y estadísticas en tiempo real. Limitaciones en la visualización de datos en tiempo real restringen la toma de decisiones informada y ágil.

3 Objetivos Específicos y Problemas Identificados

3.1 Objetivos Específicos:

3.1.1 Gestión Eficiente de Usuarios

- Problema: Gestión ineficiente de roles y permisos de usuarios.

3.1.2 Monitoreo Avanzado de Servidores

- Problema: Dificultad para identificar y monitorear diferencias entre servidores físicos y virtuales.

3.1.3 Supervisión Detallada del Tráfico de Red

- Problema: Limitaciones en la detección de amenazas y análisis de tráfico de red.

3.1.4 Sistema de Notificaciones y Alertas Efectivo

- Problema: Ausencia de alertas proactivas para eventos críticos.

3.1.5 Monitoreo de Microservicios

- Problema: Ineficiencias en la detección de fallos y rendimiento de microservicios.

3.1.6 Optimización del Rendimiento de Recursos

- Problema: Limitaciones en la supervisión de recursos y detección de cuellos de botella.

3.1.7 Configuración Personalizada de Umbrales y Alertas

- Problema: Falta de gestión proactiva mediante umbrales personalizados.

3.1.8 Integración con Otros Sistemas

- Problema: Carencia de una integración efectiva para una gestión TI holística.

3.1.9 Visualización de Datos en Tiempo Real

- Problema: Insuficiencia en la visualización de métricas para la toma de decisiones.

4 Requerimientos Generales

Los requerimientos generales se derivan directamente de los objetivos específicos y problemas identificados, buscando proporcionar una solución integral que abarque:

- Gestión avanzada de usuarios y roles.
- Monitoreo diferenciado y detallado de servidores físicos y virtuales.
- Supervisión exhaustiva del tráfico de red con capacidad de análisis profundo y detección de amenazas.
- Implementación de un sistema de notificaciones y alertas proactivas y configurables.
- Monitoreo efectivo de respuestas y fallos de microservicios.

- Supervisión y optimización de recursos a nivel de arquitectura.
- Configuración de umbrales y generación de alertas personalizadas.
- Integración fluida con otros sistemas.
- Generación y visualización de métricas en tiempo real.

5 Requerimientos Específicos

Los requerimientos específicos se listan a continuación, cada uno asociado a un ID único, nombre del requerimiento, y una descripción detallada, tal como se ha proporcionado:

- **5.1 Gestión de Usuarios**
  - El sistema debe permitir la gestión de usuarios, incluyendo la asignación de roles y permisos diferenciados.
- **5.2 Detección de Tipo de Servidor**
  - Capacidad para distinguir entre servidores físicos y virtuales, recopilando métricas relevantes y adaptándose a cambios dinámicos en el entorno.
- **5.3 Detección del Tráfico de Red**
  - Análisis detallado del tráfico de red, identificación de patrones inusuales, análisis DPI, y capacidad de generación de bloqueos o mitigaciones.
- **5.4 Notificaciones de Eventos Específicos**
  - Generación de notificaciones y alertas basadas en métricas de rendimiento y detección de anomalías.
- **5.5 Respuestas y Fallas de Microservicios**
  - Monitoreo de las respuestas de los microservicios y registro de fallas.
- **5.6 Gestión de Recursos de la Arquitectura**
  - Supervisión de recursos como almacenamiento, CPU, memoria RAM, y recursos a nivel de proceso.
- **5.7 Capacidad de Configuraciones de Umbrales y Alertas**
  - Permitir la configuración de umbrales para recursos monitoreados y la generación de alertas automáticas.
- **5.8 Integración con Otros Sistemas**

    - Facilitar la integración con otros sistemas a través de herramientas y APIs.
- **5.9 Generación de Métricas para Graficación**
    - Generar métricas adecuadas para visualización en gráficos.
- **5.10 Gráficas en Tiempo Real**
    - Presentar métricas generadas en gráficas en tiempo real de fácil interpretación.
- **5.11 Monitoreo de Respuestas de Servicios**
    - El sistema debe monitorear y registrar el tipo de respuestas proporcionadas por los servicios (éxitos, fallos, tipos de error), facilitando la identificación de problemas comunes o recurrentes y la toma de acciones correctivas específicas.
- **5.12 Detección de Actividades Anómalas y Potenciales Amenazas de Seguridad**
    - Capacidad para detectar incrementos inusuales en las solicitudes a los sistemas, posibles intentos de hackeo, y cualquier otra actividad que se desvíe significativamente de los patrones de tráfico normal, permitiendo una respuesta rápida a posibles amenazas de seguridad.
- **5.13 Gestión de la Configuración y Administración de Usuarios**
    - Implementación de un sistema de gestión de usuarios que permita asignar diferentes roles y permisos, asegurando que cada usuario tenga acceso únicamente a las funcionalidades y datos pertinentes a su rol dentro de la organización.
- **5.14 Flexibilidad en la Implementación**
    - El sistema debe ser diseñado para permitir una implementación flexible, ya sea en la nube o in-situ, y ser capaz de integrarse sin problemas en la infraestructura existente del cliente sin requerir cambios significativos o ser invasivo.

6 Requerimientos No Funcionales

6.1 RNF1: Capacidad de Gestión y Escalabilidad de Datos

- Descripción: El sistema debe ser capaz de manejar eficientemente grandes volúmenes de datos generados por el monitoreo continuo de múltiples fuentes. Esto incluye la capacidad para escalar recursos y almacenamiento según sea necesario, sin degradar el rendimiento, para adaptarse al crecimiento de la infraestructura del cliente y al incremento en la generación de datos.

6.2 RNF2: Monitoreo en Tiempo Real

- Descripción: "Fault Trace" debe garantizar el monitoreo y la visualización en tiempo real de métricas y eventos críticos del sistema. Esto es esencial para permitir la detección inmediata de anomalías y fallas, y facilitar una rápida respuesta ante incidentes.

6.3 RNF3: Disponibilidad y Supervisión Continua

- Descripción: El sistema debe estar diseñado para garantizar una alta disponibilidad y una supervisión continua 24/7 de los sistemas monitoreados. Esto incluye mecanismos de redundancia y recuperación ante desastres para minimizar el tiempo de inactividad en caso de fallos en el sistema de monitoreo.

6.4 RNF4: Interoperabilidad

- Descripción: "Fault Trace" debe ser capaz de integrarse sin problemas con una amplia gama de sistemas, plataformas y tecnologías ya existentes en los entornos de los clientes. Esto implica el uso de estándares abiertos, APIs y protocolos de comunicación que faciliten el intercambio de datos y la compatibilidad entre sistemas.

6.5 RNF5: Seguridad

- Descripción: Dadas la sensibilidad y la criticidad de los datos de monitoreo, el sistema debe implementar robustas medidas de seguridad para proteger contra accesos no autorizados, ataques cibernéticos y cualquier forma de compromiso de datos. Esto incluye cifrado de datos, autenticación fuerte, control de acceso y auditoría de seguridad.

6.6 RNF6: Escalabilidad y Flexibilidad

- Descripción: El sistema debe ser diseñado con una arquitectura que permita su escalabilidad horizontal y vertical para manejar incrementos en la carga de trabajo y la complejidad de los sistemas monitoreados. Debe ser flexible para adaptarse a cambios en los requerimientos del negocio o en la infraestructura tecnológica sin requerir una reconfiguración extensiva o rediseño del sistema.

7 Funcionalidades identificadas

De acuerdo con los requerimientos específicos, consideramos que las funcionalidades que debemos implementar en el sistema son las siguientes:

7.1 Gestión de Usuarios

7.1.1 Crear Usuarios

- Registro de Usuario: Permite a los administradores registrar nuevos usuarios, solicitando información esencial como nombre, correo electrónico, y rol.
- Asignación de Roles Inicial: Posibilidad de asignar roles predefinidos durante el proceso de creación del usuario para determinar su nivel de acceso desde el principio.
- Validación de Datos de Usuario: Verificación automática de la unicidad del correo electrónico y cumplimiento de políticas de seguridad para contraseñas.

7.1.2 Leer Usuarios

- Listado de Usuarios: Visualización de todos los usuarios registrados en el sistema con capacidad de filtrado por nombre, rol, o estado (activo/inactivo).
- Detalle de Usuario: Funcionalidad para ver información detallada de cada usuario, incluyendo roles asignados, fecha de creación, y registro de actividad reciente.

- Búsqueda Avanzada: Herramientas de búsqueda para localizar usuarios específicos basándose en múltiples criterios.

7.1.3 Actualizar Usuarios

- Edición de Información de Usuario: Permite modificar la información personal de los usuarios, como nombre, correo electrónico, y otros campos personalizables.
- Reasignación de Roles: Cambio de roles de usuario para ajustar sus permisos y accesos dentro del sistema.
- Gestión de Estado: Habilitar o deshabilitar cuentas de usuario para controlar su acceso al sistema.

7.1.4 Eliminar Usuarios

- Eliminación Segura de Usuarios: Proceso para eliminar usuarios del sistema, con opciones para archivar su información de manera segura antes de la eliminación.
- Confirmación de Eliminación: Requiere confirmación para evitar eliminaciones accidentales de cuentas de usuario.
- Registro de Eliminación: Mantenimiento de un registro auditado de las eliminaciones de cuentas para seguimiento y seguridad.

7.2 Detección de Tipo de Servidor

7.2.1 Identificación Automática

- Reconocimiento de Huellas del Sistema: Implementar un proceso que automáticamente identifique el sistema operativo y la configuración hardware para distinguir entre servidores físicos y virtuales.
- Integración con Hypervisors: Conectar directamente con sistemas de gestión de virtualización (como VMware, Hyper-V) para recopilar datos sobre los servidores virtuales administrados.

7.2.2 Recopilación de Métricas

- Métricas Diferenciadas por Tipo de Servidor: Diseñar un conjunto de métricas específicas que se recopilan en función de si el servidor es físico o virtual, como la utilización de CPU, memoria, almacenamiento, y red.
- Actualizaciones Dinámicas de Métricas: Capacidad para actualizar y adaptar el tipo y la frecuencia de las métricas recopiladas según cambios en la configuración o el entorno del servidor.

7.2.3 Adaptabilidad a Cambios

- Detección de Cambios en Configuración: Monitorear y reconocer automáticamente cambios en la configuración del servidor que puedan afectar su clasificación como físico o virtual.
- Reconfiguración Automática de Monitoreo: Ajustar automáticamente las estrategias y parámetros de monitoreo basados en los cambios detectados para asegurar la continuidad y precisión del monitoreo.

7.3 Detección del Tráfico de Red

7.3.1 Análisis de Patrones

- Monitoreo Continuo del Tráfico: Establecer un monitoreo constante del tráfico de red para capturar datos en tiempo real.
- Identificación de Patrones con IA: Aplicar algoritmos de inteligencia artificial y machine learning para identificar patrones de tráfico normales y anormales.

7.3.2 Inspección Profunda y Mitigación

- Análisis DPI (Deep Packet Inspection): Implementar capacidades de inspección profunda de paquetes para analizar el contenido y el origen/destino del tráfico en detalle.

- Automatización de Respuestas a Amenazas: Desarrollar mecanismos automáticos de respuesta, como la generación de bloqueos o mitigaciones, en caso de detección de tráfico malicioso o anómalo.

7.3.3 Análisis de Seguridad

- Detección de Anomalías y Amenazas: Utilizar el análisis de tráfico para identificar posibles intentos de hackeo, malware, y otras amenazías de seguridad.
- Integración con Sistemas de Seguridad: Asegurar que los datos y alertas generadas se puedan integrar y compartir con soluciones de seguridad existentes, como firewalls y sistemas de prevención de intrusiones (IPS).

7.4 Notificaciones de Eventos Específicos

7.4.1 Configuración de Alertas

- Creación de Alertas Basadas en Umbrales: Permitir a los usuarios configurar alertas personalizadas basadas en umbrales específicos para diferentes métricas.
- Plantillas de Notificaciones Personalizables: Ofrecer plantillas editables para que los administradores personalicen el contenido de las notificaciones según el tipo de alerta.

7.4.2 Métodos de Notificación

- Múltiples Canales de Notificación: Enviar alertas a través de varios canales, incluyendo email, SMS, aplicaciones de mensajería instantánea y dashboards internos.
- Agrupación de Alertas: Consolidar alertas similares en un periodo corto para evitar la sobrecarga de notificaciones.

7.4.3 Gestión de Alertas

- Histórico de Alertas y Eventos: Mantener un registro accesible de todas las alertas y eventos pasados para análisis y auditoría.

- Suscripción a Tipos de Alertas: Permitir a los usuarios suscribirse a tipos específicos de alertas, personalizando la recepción de notificaciones según sus necesidades o roles.

7.5 Respuestas y Fallas de Microservicios

7.5.1 Monitoreo de Microservicios

- Registro de Respuestas de Microservicios: Rastrear y registrar todas las respuestas emitidas por los microservicios, categorizándolas por éxito, error, o tipo de fallo.
- Análisis de Tiempo de Respuesta: Medir y analizar los tiempos de respuesta de los microservicios para identificar posibles degradaciones del rendimiento.

7.5.2 Gestión de Incidencias

- Alertas de Fallo de Microservicio: Generar alertas inmediatas cuando se detecten fallos o comportamientos anómalos en microservicios.
- Integración con Herramientas de Gestión de Incidencias: Asegurar que las alertas y datos de fallos puedan integrarse con sistemas de gestión de incidencias para una resolución eficaz.

7.5.3 Análisis y Optimización

- Reportes de Salud de Microservicios: Proporcionar reportes periódicos sobre la salud y el rendimiento de los microservicios, destacando problemas recurrentes o áreas de mejora.
- Recomendaciones de Optimización: Basado en el análisis de datos históricos, ofrecer recomendaciones para la optimización de microservicios.

7.6 Gestión de Recursos de la Arquitectura

7.6.1 Monitoreo de Recursos

- Visualización en Tiempo Real de Uso de Recursos: Proporcionar dashboards interactivos que muestran el uso actual de CPU, memoria RAM, almacenamiento y otros recursos críticos en tiempo real.
- Alertas de Saturación de Recursos: Configurar alertas automáticas cuando el uso de recursos exceda umbrales predeterminados, indicando potenciales cuellos de botella.

7.6.2 Análisis de Rendimiento

- Análisis de Tendencias y Patrones de Uso: Utilizar herramientas analíticas para identificar tendencias de uso de recursos a lo largo del tiempo, facilitando la planificación de capacidad y la optimización.
- Recomendaciones Automáticas para la Optimización de Recursos: Basado en el análisis histórico y en tiempo real, ofrecer sugerencias para ajustes en la configuración o la infraestructura para mejorar el rendimiento.

7.6.3 Gestión de Configuración

- Configuración y Ajuste de Recursos: Permitir a los administradores ajustar la asignación de recursos directamente desde el sistema, aplicando cambios recomendados para optimizar el rendimiento.

7.7 Capacidad de Configuraciones de Umbrales y Alertas

7.7.1 Definición de Umbrales

- Interfaz de Configuración de Umbrales: Proporcionar una interfaz gráfica donde los usuarios puedan definir y ajustar umbrales para distintas métricas de monitoreo.
- Umbrales Dinámicos Basados en Comportamiento: Implementar la capacidad de ajustar umbrales dinámicamente basado en el aprendizaje de patrones normales de comportamiento, mejorando la precisión de las alertas.

7.7.2 Gestión de Alertas

- Personalización de Alertas: Habilitar la personalización completa de alertas, incluyendo el mensaje, la severidad y los canales de notificación.
- Agrupación Inteligente de Alertas: Desarrollar mecanismos para agrupar alertas relacionadas y reducir la fatiga de alertas, mejorando la gestión de incidentes.

7.8 Integración con Otros Sistemas

7.8.1 API y Conectividad

- APIs Restful para Integración: Ofrecer APIs Restful bien documentadas para facilitar la integración con otros sistemas, aplicaciones y herramientas de terceros.
- Conectores Predefinidos para Plataformas Populares: Proporcionar conectores o plugins predefinidos para facilitar la integración rápida con plataformas de software populares.

7.8.2 Sincronización de Datos y Herramientas

- Herramientas de Mapeo y Transformación de Datos: Incluir herramientas que permitan mapear y transformar datos entre diferentes formatos y esquemas, asegurando la compatibilidad y la integridad de los datos compartidos.
- Gestión Centralizada de Integraciones: Implementar un panel de control centralizado para gestionar todas las integraciones, permitiendo a los usuarios configurar, monitorear y solucionar problemas de las conexiones establecidas.

7.9 Generación de Métricas para Graficación

7.9.1 Recolección de Datos

- Automatización de la Recolección de Datos: Implementar procesos automáticos para recoger datos de rendimiento y operacionales de diferentes fuentes en tiempo real.
- Normalización de Datos: Establecer procedimientos para normalizar datos recopilados de múltiples fuentes, asegurando consistencia y precisión en las métricas.

7.9.2 Creación de Métricas

- Herramientas de Definición de Métricas: Proporcionar interfaces para que los usuarios definen y configuran nuevas métricas basadas en los datos recopilados.
- Métricas Personalizables y Predefinidas: Ofrecer un conjunto de métricas predefinidas relevantes para la operación y el rendimiento del sistema, además de permitir la creación de métricas personalizadas.

7.10 Gráficas en Tiempo Real

7.10.1 Visualización de Datos

- Dashboards Dinámicos: Facilitar la creación de dashboards interactivos y personalizables que presenten las métricas en gráficos actualizados en tiempo real.
- Soporte para Varios Tipos de Gráficos: Incluir soporte para múltiples formatos de visualización, como gráficos de línea, barras, área, dispersión, y pie, entre otros.

7.10.2 Interactividad y Usabilidad

- Funcionalidades Interactivas: Incorporar opciones para manipular vistas de datos, como zoom, filtrado, y análisis de series temporales, para una exploración detallada.
- Anotaciones y Alertas en Gráficos: Permitir que los usuarios añadan anotaciones o configurar alertas directamente desde los gráficos para marcar eventos o tendencias importantes.

7.11 Monitoreo de Respuestas de Servicios

7.11.1 Registro y Análisis

- Detección y Registro de Tipos de Respuesta: Monitorear y clasificar automáticamente las respuestas de servicios y APIs, identificando éxitos, fallos y tipos específicos de error.
- Análisis de Causa Raíz: Implementar herramientas para el análisis de causa raíz de errores frecuentes o críticos, facilitando la identificación y corrección de problemas subyacentes.

7.11.2 Informes y Alertas

- Generación de Informes de Rendimiento de Servicios: Crear informes detallados sobre el rendimiento y la fiabilidad de los servicios monitoreados, destacando áreas de preocupación.

- Alertas Basadas en Patrones de Fallo: Configurar alertas que se activan por patrones de fallo específicos o incrementos en la tasa de errores.

7.12 Detección de Actividades Anómalas y Potenciales Amenazas de Seguridad

7.12.1 Detección de Anomalías

- Sistema de Detección de Anomalías Basado en IA: Utilizar algoritmos de inteligencia artificial para analizar patrones de tráfico y detectar desviaciones que sugieran actividad sospechosa o maliciosa.
- Alertas de Seguridad en Tiempo Real: Generar notificaciones inmediatas cuando se detecten actividades potencialmente peligrosas, permitiendo una respuesta rápida.

7.12.2 Integración de Seguridad

- Coordinación con Sistemas de Seguridad: Asegurar que las alertas y datos relevantes puedan integrarse con sistemas de gestión de seguridad existentes para una respuesta coordinada a las amenazas.
- Análisis Forense y Rastreo de Incidentes: Proporcionar herramientas para el análisis forense que ayuden a investigar y rastrear la fuente de actividades sospechosas o ataques.

7.13 Gestión de la Configuración y Administración de Usuarios

7.13.1 Control y Auditoría

- Panel de Control de Administración: Ofrecer un panel centralizado para la gestión de configuraciones de seguridad, roles, y permisos.
- Auditoría y Registro de Actividades: Mantener un registro detallado de todas las actividades relacionadas con la gestión y configuración de usuarios, incluyendo cambios en roles y permisos.

7.14 Flexibilidad en la Implementación

7.14.1 Soporte de Despliegue

- Arquitectura Modular y Contenedorizada: Desarrollar el sistema con una arquitectura modular que soporte contenedores, facilitando despliegues flexibles y escalables.
- Guías de Implementación y Documentación: Proporcionar documentación completa y guías paso a paso para la implementación en diferentes entornos, incluyendo la nube, on-premise y configuraciones híbridas.

7.14.2 Personalización y Extensión

- Interfaz de Configuración Flexible: Implementar interfaces que permitan a los usuarios personalizar y ajustar la configuración del sistema para adaptarse a sus necesidades específicas sin cambios invasivos en la infraestructura existente.