[AESM] Nuevo Paradigma de Monitorización de Servicios usando Dynatrace

Guía



**Índice**

[1. Toma de requisitos y *tagging* 3](#_Toc184903118)

[2. Instrumentalización técnica 3](#_Toc184903119)

[2.1 Sintéticos 3](#_Toc184903120)

[2.2 OneAgent 3](#_Toc184903121)

[2.3 RUM 3](#_Toc184903122)

[2.4 Business Agents 3](#_Toc184903123)

[3. Sistema de información 3](#_Toc184903124)

[3.1 Dashboards dinámicos 3](#_Toc184903125)

[3.2 Reporting periódico de estado de aplicación 3](#_Toc184903126)

[4. Sistema de alarmado 3](#_Toc184903127)

[4.1 Perfiles de alarmado 4](#_Toc184903128)

[4.2 Perfiles de notificación 4](#_Toc184903129)

**Resumen Ejecutivo**

# **Toma de requisitos y tagging**

El primer paso es realizar una captura de requisitos y familiarizarse con todas las dimensiones y actores en juego dentro de la aplicación objetivo.

## ***Stakeholders***

Principales actores con intereses en el aplicativo:

* **Nivel de Servicio**
* **Nivel de Infraestructura**
* **Nivel de Negocio**
* **Nivel de Resolución**
* **Nivel de Gestión de Incidencias**

## **Identificación functional de Key Requests, User Action, Business Events…**

## **Tagging**

# **Instrumentalización técnica**

## **Sintéticos**

## **OneAgent**

### Business Events

### User actions

### Key Requests

## **RUM**

### User properties

### Session variables

# Sistema de información

## Dashboards dinámicos

## Reporting periódico de estado de aplicación

# Sistema de alarmado

## Problemas de Dynatrace

Dynatrace integra capacidades como detección de problemas, análisis de rendimiento y trazabilidad, facilitando la gestión de entornos complejos. Dynatrace es fundamental para identificar cuellos de botella, reducir tiempos de inactividad y garantizar una experiencia de usuario óptima.

### Tipos de Eventos en Dynatrace

Dynatrace categoriza los eventos generados en la plataforma para facilitar el análisis y la resolución de problemas. Los principales tipos de eventos incluyen:

• **Availability events**: Indican problemas de disponibilidad, como servicios que están caídos o inaccesibles. Estos eventos pueden desencadenarse cuando un host o servicio no responde dentro de un periodo esperado o si una prueba sintética falla en varias ubicaciones simultáneamente.

• **Error events**: Relacionados con fallos de aplicación o errores en el código. Ejemplos incluyen aumentos en la tasa de errores HTTP, excepciones no gestionadas en aplicaciones o fallos repetidos en las transacciones de usuario.

• **Performance events**: Detectan degradaciones en el rendimiento, como tiempos de respuesta altos. Estos eventos se disparan cuando se exceden umbrales dinámicos basados en el comportamiento histórico de la aplicación o servicio.

• **Resource events**: Monitorean el uso de recursos como CPU, memoria y disco. Por ejemplo, alertas por uso prolongado de CPU superior al 90%, saturación de memoria o almacenamiento críticamente bajo.

• **Custom events**: Eventos definidos por el usuario para métricas o situaciones específicas. Estos pueden configurarse para supervisar KPIs específicos del negocio, como tasas de conversión o rendimiento en tiempo real.

• **Anomaly detection events**: Identifican patrones o comportamientos fuera de lo esperado en función de líneas base dinámicas. Un ejemplo es detectar un descenso brusco en el volumen de sesiones de usuario en un segmento geográfico específico.

Cada tipo de evento incluye un contexto detallado que facilita el análisis de causa raíz. Estos eventos son analizados automáticamente por Davis AI, el motor de inteligencia artificial de Dynatrace, para proporcionar recomendaciones accionables.

### Tipos de Alertas en Dynatrace

### Alertas de Servicios

Estas alertas están orientadas al rendimiento de los servicios.

Métricas Comunes:

• **Tiempo de respuesta**: Se genera una alerta cuando el tiempo de respuesta excede un umbral definido.

• **Tasa de errores**: Detecta incrementos significativos en errores (500, fallos de conexión, etc.).

• **Tasa de solicitudes**: Identifica anomalías en el volumen de solicitudes, como picos inusuales.

Ejemplo:

Si un servicio presenta un aumento en los tiempos de respuesta superiores al 10% durante más de 5 minutos, Dynatrace generará un problema.

### Alertas de Infraestructura

Enfocadas en el estado de los recursos subyacentes.

Métricas Comunes:

• **CPU**: Alertas por uso constante superior al 90% durante un periodo prolongado.

• **Memoria**: Detecta problemas de fuga de memoria o saturación.

• **Disco**: Envía notificaciones si el espacio libre es inferior al 10%.

Configuración Avanzada:

• Incluye reglas para monitorizar grupos de hosts.

• Uso de etiquetas automáticas para categorizar entidades.

### Alertas Sintéticas

Diseñadas para monitorizar pruebas simuladas de la experiencia del usuario.

Métricas Comunes:

• **Disponibilidad**: Alertas si una prueba falla repetidamente en diferentes ubicaciones.

• **Tiempo de carga**: Detecta incrementos en los tiempos de carga simulados.

### Alertas de RUM (Real User Monitoring)

Enfocadas en la experiencia real de los usuarios.

Métricas Comunes:

• **Apdex**: Alerta cuando el índice Apdex cae por debajo de un valor aceptable.

• **Errores de JavaScript**: Detecta errores críticos en la capa del navegador.

• **Tiempo de carga de página**: Supervisa el tiempo desde que el usuario inicia la solicitud hasta que la página está completamente cargada.

• **Número de sesiones**: Genera alertas si el volumen de sesiones cae por debajo de una línea base dinámica calculada en función del comportamiento histórico.

Ejemplo:

Si el número de sesiones de una aplicación desciende un 20% por debajo de la línea base esperada durante un período de 30 minutos, se dispara una alerta para investigar la causa.

## Perfiles de alarmado

[Incluir perfiles de alarmado comunes a todas las monitorizaciones]

## Perfiles de notificación

# Casos de uso y batería de pruebas