ALDABA

Zabbix a escala:

Observabilidad e integración ITSM

ALDABA

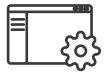
ALDABA

Quiénes somos

ALDABA

Quiénes somos

Desde 2003 especializadas/os en la optimización de procesos de negocio



Área

Ingeniería de Sistemas y Ciberseguridad.



Equipo

Consultoras/es certificadas/os en Zabbix y tecnologías Microsoft, Google Cloud, Vmware, Veeam, FortiNet, Elastic, HPE, CompTIA Pentest+, …



Proyectos de Ingeniería y Operación de Infraestructuras de cliente

Diseñamos soluciones, las operamos y mantenemos.



Proyectos de Ciberseguridad

Servicios de seguridad gestionada. Protegemos información digital, dispositivos y activos frente a incidentes de seguridad.

ALDABA

Índice de contenidos

1 Zabbix a escala

2 Observabilidad

3 Integración ITSM

ALDABA

01

Zabbix a escala

ALDABA

Zabbix a escala

El punto de partida

Hosts

- Imposibilidad de acceso a todas las redes desde Zabbix Server.

[50K]

Hosts monitorizados

Ítems

- Diferentes tipos de ítems

[2 M]

Ítems recogidos

[5K]

VPS

Alertas

- ¿Cuántas requieren acción?

[700K]

Triggers

Monitorizar es recoger datos; observar es poder responder preguntas.

ALDABA

Zabbix a escala

ZABBIX

Mecanismos de monitorización

HTTP

IPMI

JMX

Escenarios web

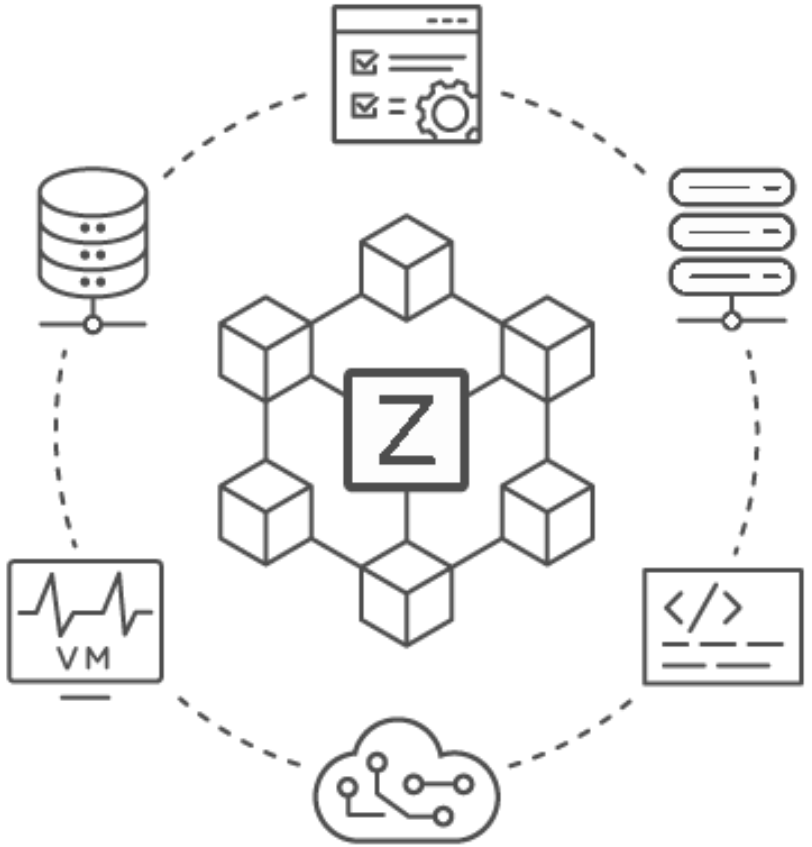
Zabbix *agent*

SNMP

Comprobaciones simples

- SNMP
- TCP / UDP *check*

Syslog



ALDABA

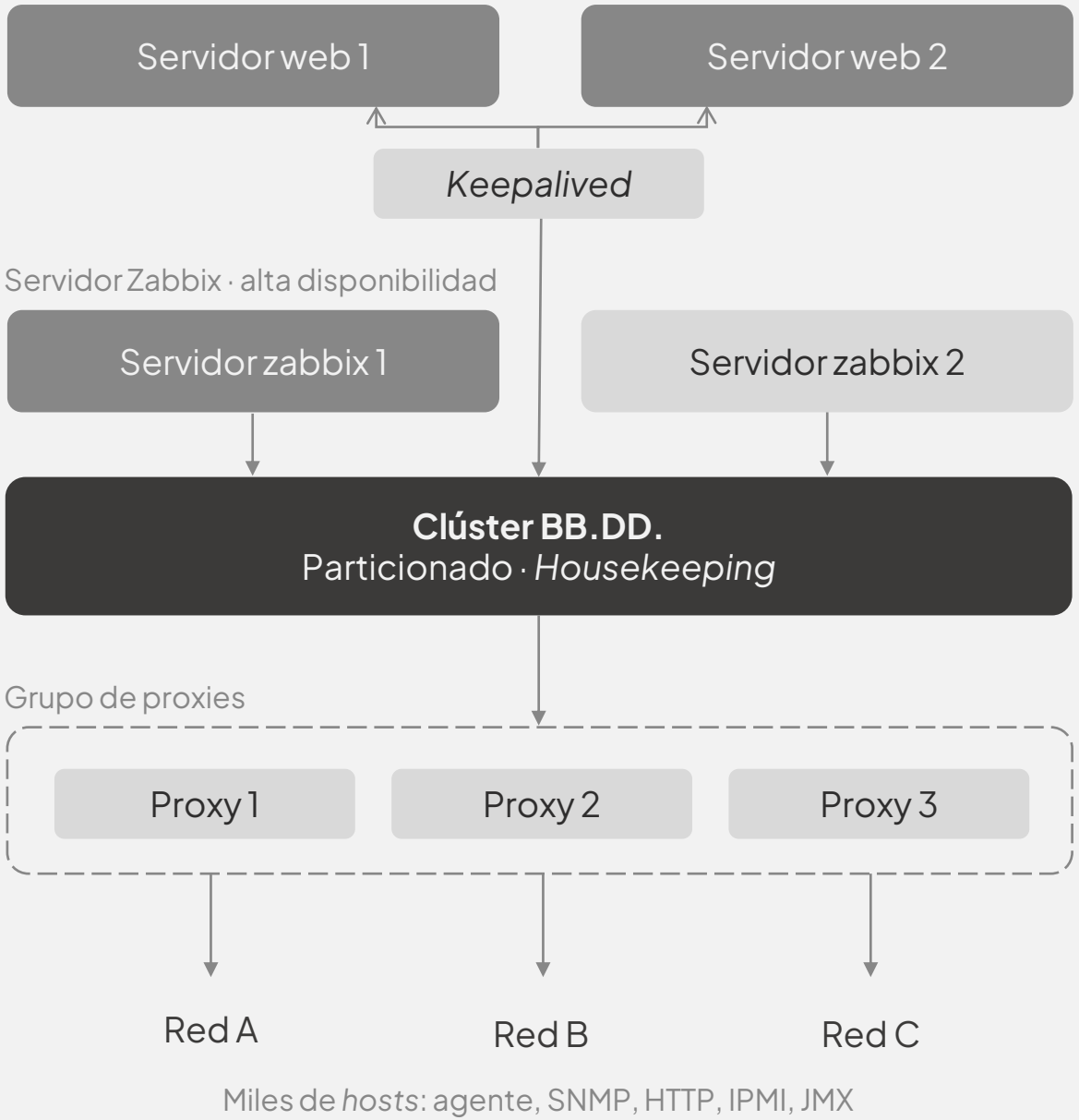
Zabbix a escala

Arquitectura

Distribuir la carga, aislar redes y no perder datos si algo falla.

Claves

- Servidores web configurados en HA.
- Proxies y grupos de proxies, con *failover* automático.
- Alta disponibilidad nativa del servidor.
- Clúster de BB.DD.: particionado y *housekeeping*.
- Zabbix monitorizando Zabbix: colas y *pollers*.



ALDABA

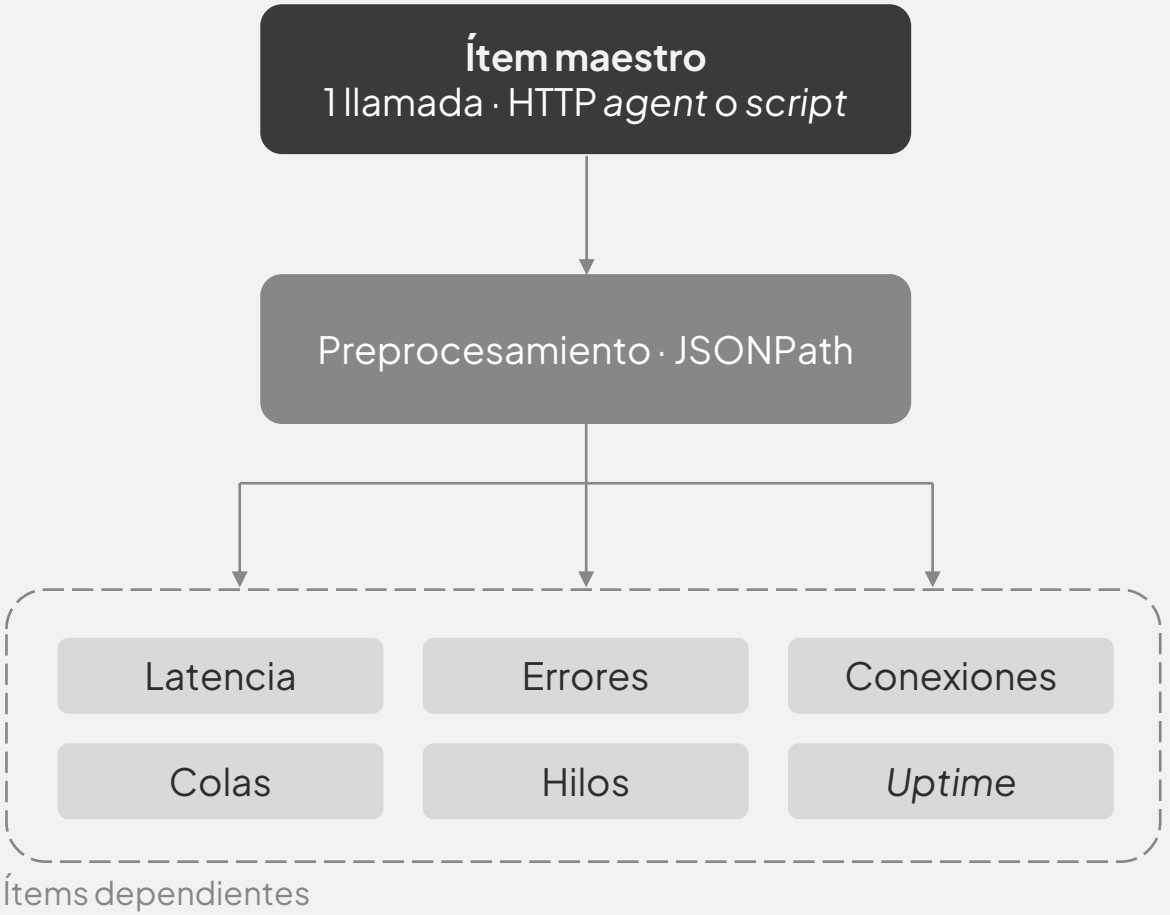
Zabbix a escala

Recolectar con eficiencia

Menos llamadas, más valor en cada interacción y cero altas manuales.

Técnicas

- Ítems dependientes: un ítem maestro, muchos valores.
- LLD, autoregistro y *network discovery*.
- Plantillas modulares e intervalos razonables.



1 → [150]

Llamada → Valores recogidos

ALDABA

Zabbix a escala

Reducir el ruido

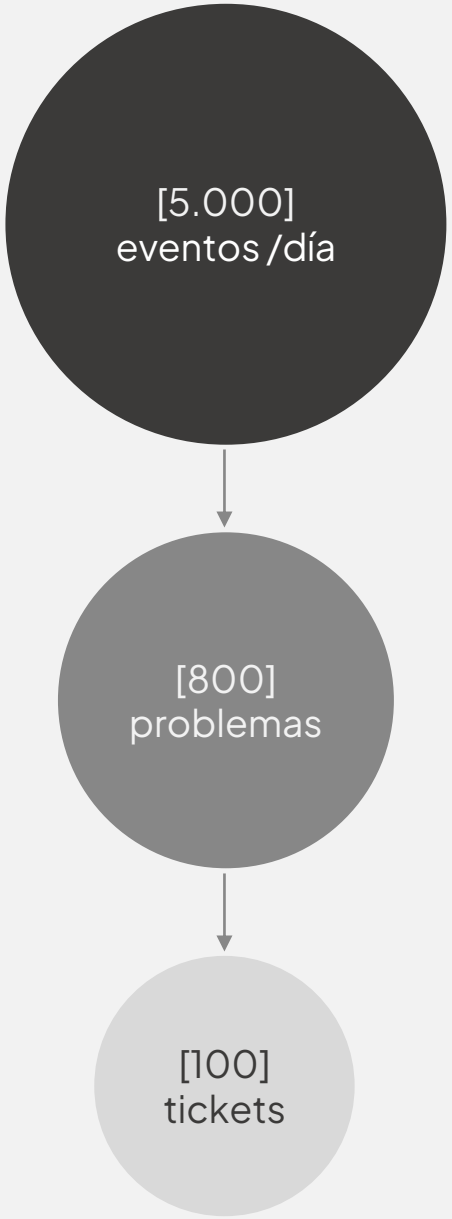
Un ticket solo debería nacer de un problema accionable.

Técnicas

- Dependencias entre *triggers*
- Histéresis
- Mantenimientos
- Nodata afinado

Convención de tags

- *Service*
- *Env*
- *Owner*
- *Criticality*
- CI



ALDABA

02

Observabilidad

ALDABA

Observabilidad

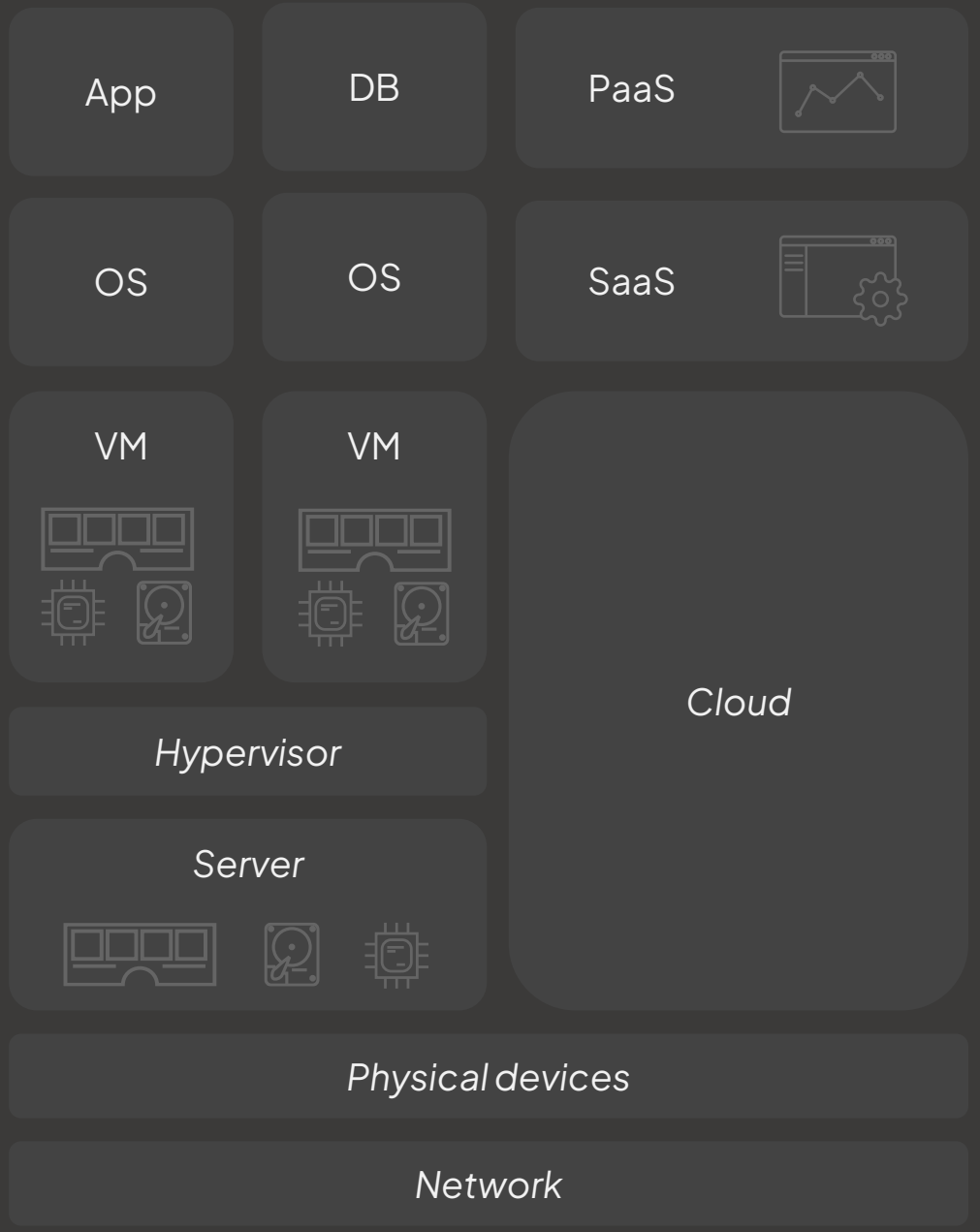
Monitorización

Recopilar y analizar métricas de los sistemas IT.

Objetivo → Verificar el funcionamiento

Tipos

Externas | Internas | RUM (*Real User Monitoring*)



ALDABA

Observabilidad

Reducir el ruido

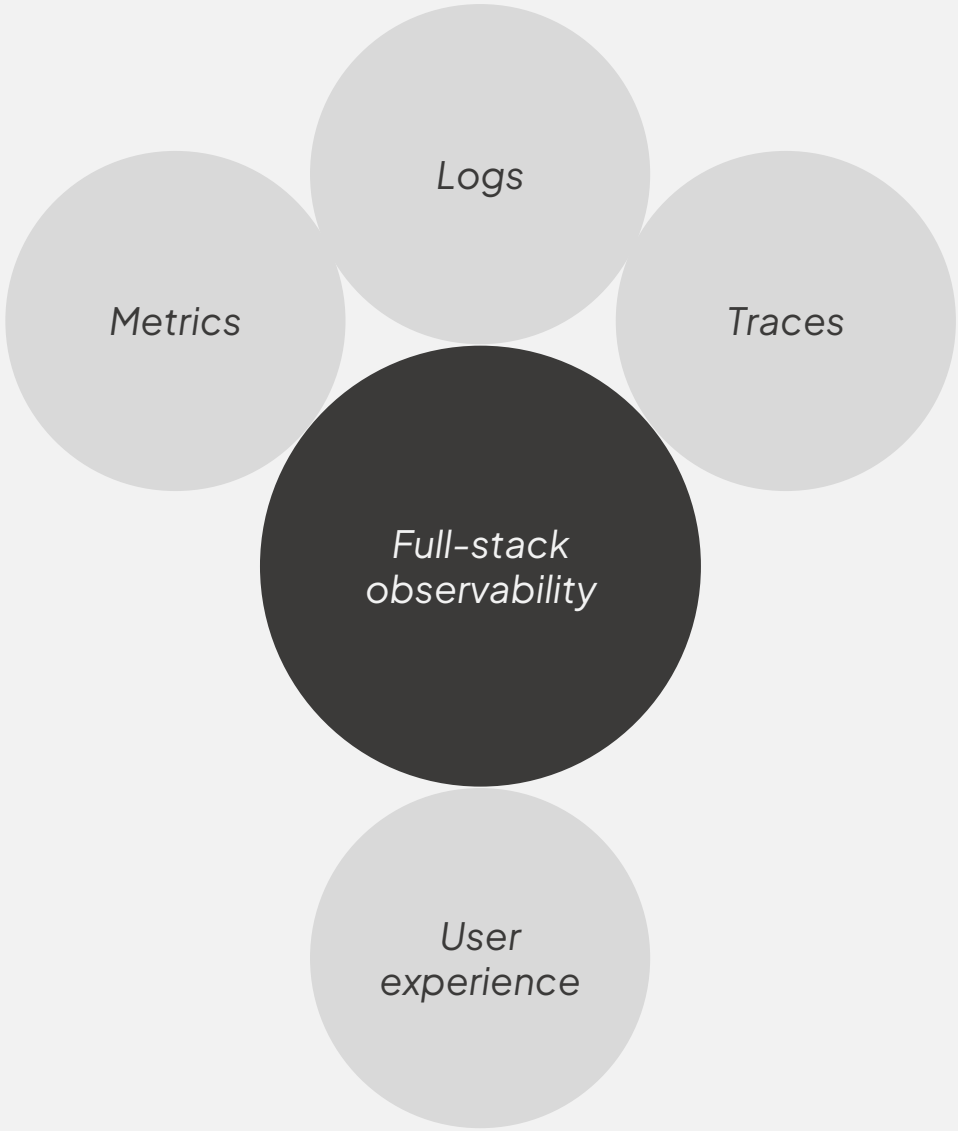
Entender el comportamiento de los sistemas a partir de la correlación de datos.

Objetivos

- Detectar patrones
- Prevenir fallos
- Analizar causas

Complejidad

- Volumen datos
- Diversidad fuentes
- Relacionar datos



ALDABA

Observabilidad

Zabbix, base de la observabilidad

Métricas

- Agente, SNMP, IPMI, JMX, HTTP.
- Plantillas y descubrimiento.

Nativo

Logs

- Lectura con agente y *triggers* por patrón.
- Búsqueda avanzada con Elastic o Loki.

Integrado

Trazas

- Se correlaciona con Tempo o Jaeger en Grafana.

Integrable

Zabbix aporta la base de infraestructura y servicios, y se integra con el resto del *stack*.

ALDABA

Observabilidad

APM con OpenTelemetry

Ver cómo viaja cada petición por aplicaciones y servicios, y dónde se ralentiza o falla.

Por qué nos interesa

- Trazas dentro de Zabbix, junto a métricas y alertas.
- El proxy recibe la telemetría y la guarda en ClickHouse.
- Se usa en *triggers* y gráficos con *telemetry query*.



El servidor no recibe telemetría, solo el proxy

ALDABA

Observabilidad

IA sobre Zabbix

Agentes con MCP

- El servidor MCP conecta asistentes de IA con la API de Zabbix.
- Cada acción respeta los permisos del token.

Servidor MCP oficial

Operación asistida

- Consultar incidencias, cambios y mantenimientos mediante lenguaje natural.
- Objetivo: entender antes el incidente.

Lenguaje natural

Uso de IA

- Plantillas para monitorizar OpenAI, Claude y Copilot.
- Visible junto al resto de servicios.

Previsto en 8.0 LTS

Cada acción del agente pasa por la API: permisos del token y registro de auditoría de Zabbix.

ALDABA

03

Integración ITSM

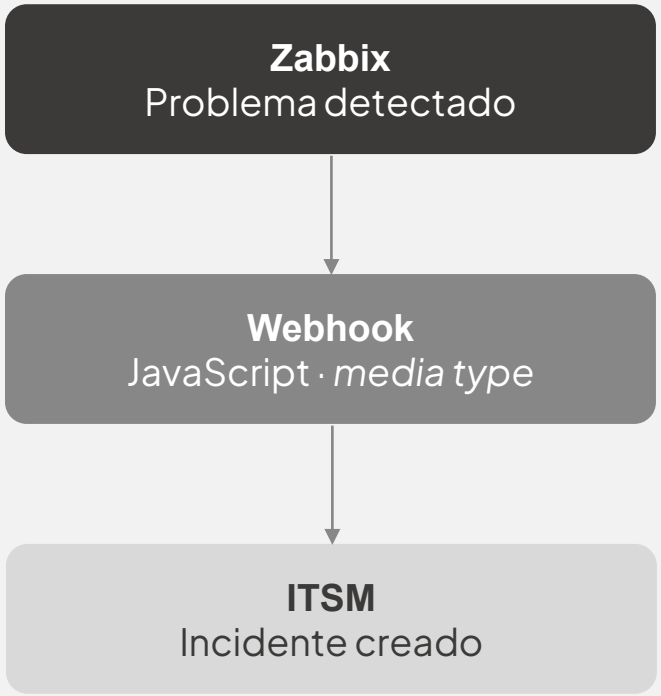
ALDABA

Integración ITSM

Integración vía webhooks

- *Media types* con *webhook* en JavaScript.
- Oficiales: ServiceNow, Jira, JSM, Zendesk, PagerDuty, …
- API para el resto: GLPI o herramientas propias.





ALDABA

Integración ITSM

Ciclo de vida del ticket

01

Problema

- El *trigger* genera el evento y la acción lanza el *webhook*.

Zabbix

02

Incidente

- Se crea en el ITSM con contexto y su ID vuelve a Zabbix.

ITSM

03

Sincronización

- Acuses, cambios de severidad y recuperación llegan al ticket.

Zabbix ⇄ ITSM

04

Cierre

- La resolución en el ITSM devuelve acuse o cierre a Zabbix.

ITSM → Zabbix

Webhook — Zabbix → ITSM: crea, actualiza y resuelve el incidente.

API — ITSM → Zabbix: devuelve el acuse (*event.acknowledge*) y el cierre.

ALDABA

Integración ITSM

Contexto en el ticket

El técnico no tiene por qué abrir Zabbix para entender el ticket.

Desde Zabbix

- *Host*
- Servicio
- Severidad
- *Tags*
- Enlace al evento

Desde la CMDB

- CI
- Propietario
- Criticidad
- Grupo de resolución

Incidente INC-20261014101

Zabbix	Resumen	Disco al 92 % en srv-db-01
Zabbix	Severidad	*High*
Zabbix	Servicio	Pagos (prod)
Zabbix	Tags	env=prod · owner=dba
Zabbix	Evento	Enlace al problema y al gráfico
CMDB	CI	srv-db-01 · criticidad alta
CMDB	Grupo de resolución	DBA N2

ALDABA

Integración ITSM

Buenas prácticas a escala

Deduplicación

- Un incidente por problema, no por evento.
- Alertar por servicio, no por síntoma.

Menos ruido

Resiliencia

- Reintentos y *rate limiting* en el *webhook*.
- El ITSM también se cae.

Más robusto

Enrutado

- Grupos de resolución según *tags*.
- Supresión en mantenimientos y cambios.

Llega a quien resuelve

ALDABA

Integración ITSM

Conclusiones

El ticket es parte del monitor

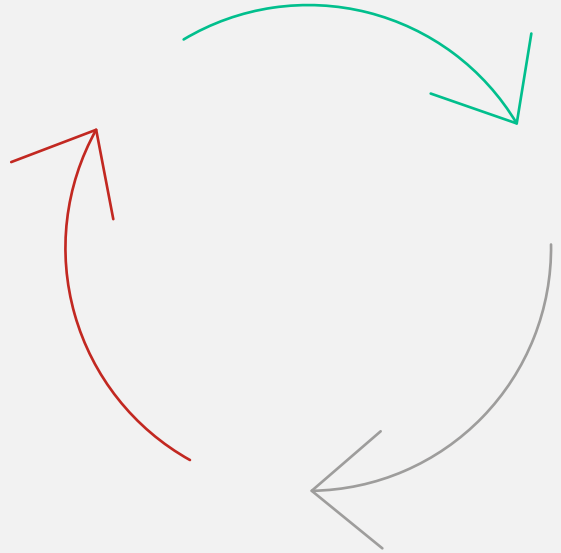
- Integración bidireccional.
- Deduplicada y con contexto.

Escala = diseño

- Proxies, ítems dependientes y BB.DD.

Contexto > volumen

- *Tags* y modelo de servicios.
- Alertar por servicio, no por síntoma.



ALDABA

¡Gracias!

aldaba.es | info@aldaba.es | t. +34 981 90 20 60 | f. +34 981 90 20 05