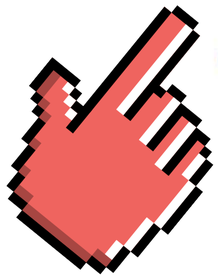
GESTIÓN DE INCIDENTES Y ANÁLISIS DE RIESGO

Home Content Demo

Herramientas de Respuesta a Incidentes

Nagios®

Por: Agustín Sánchez



Start

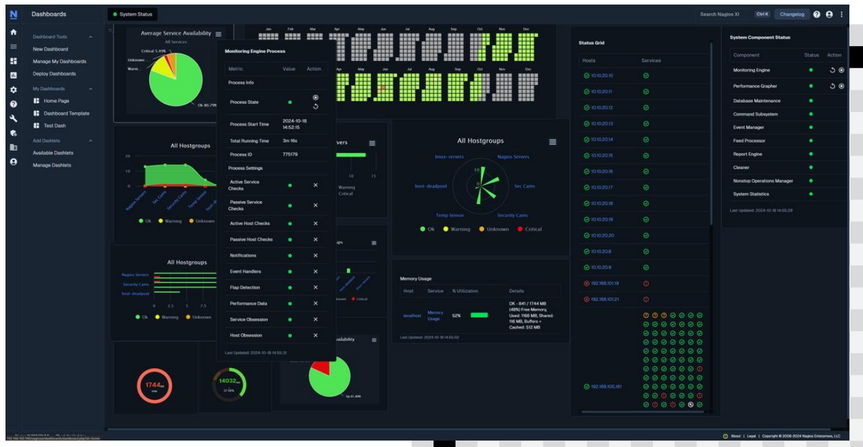
Nagios es una plataforma de **monitoreo y alertamiento de infraestructura IT** (servidores, redes, aplicaciones y servicios) que nace como **NetSaint** y se publica por primera vez en 1999, creada por **Ethan Galstad**; en 2002 adopta el nombre Nagios (acrónimo recursivo “Nagios Ain’t Gonna Insist On Sainthood”) por temas de marca.

Hoy conviven la edición open-source (Nagios Core) y la edición comercial Nagios XI, que añade asistentes, dashboards y reportes empresariales.

PRINCIPALES FUNCIONALIDADES

- **Vigila tus sistemas**: monitorea servidores, apps y dispositivos para saber si están bien o fallan (usa “plugins” para hacer las pruebas).
- **Te avisa cuando algo va mal:** envía alertas cuando un servicio pasa de OK a WARNING o CRITICAL, con reglas y umbrales que tú defines.
- **Intenta arreglar solo lo básico**: puede ejecutar scripts automáticos al detectar un problema (reiniciar un servicio, por ejemplo).
- **Tiene un agente fácil de usar (NCPA):** un solo agente para Windows, Linux y macOS que da métricas en tiempo real y soporta checks activos y pasivos.
- **Funciona bien en redes distribuidas:** acepta “checks pasivos” enviados desde otras sedes o equipos a través de NRDP (sin estar consultando todo el tiempo).
- **Muestra paneles y reportes claros (XI):** en su versión XI tienes dashboards y reportes listos para compartir con el equipo o la gerencia.

¿CÓMO CONTRIBUYE A LA RESPUESTA A INCIDENTES?



Nagios detecta y alerta fallas con checks y umbrales, puede actuar de inmediato ejecutando scripts (event handlers) para contener o remediar, mantiene visibilidad distribuida con su agente NCPA y los checks pasivos vía NRDP, y facilita el análisis posterior con dashboards y reportes en XI.

Áreas donde se usa Nagios

- NOC/SOC de TI para servicios críticos.
- Aplicaciones web y APIs (HTTP/HTTPS, uptime y performance).
- Redes y data centers (switches/routers/UPS/sensores).
- Gestión y monitoreo de logs para seguridad y cumplimiento.
- Entornos distribuidos/air-gapped con checks pasivos (NRDP).

Caso de la vida real

Integración Nagios → ServiceNow (2025, Constellation vía ZigiOps).
Qué pasó: La empresa recibía miles de alertas y la creación manual de tickets retrasaba la respuesta.
Cómo se usó Nagios: Se configuró un flujo bidireccional: cada alerta de Nagios generaba automáticamente un incidente en ServiceNow con severidad/prioridad/servicio mapeados; al actualizar o cerrar el ticket, el estado se sincronizaba de vuelta en Nagios.
Resultado: creación instantánea de incidentes, menos trabajo manual y mejor cumplimiento de SLA.

GESTIÓN DE INCIDENTES Y ANÁLISIS DE RIESGO

Home Content **Demo**

NAGIOS VS OTROS

Propuesta	¿Ventaja de Nagios?	¿Por qué?	¿Quién gana y por qué?
Auto-remediación ante incidentes	Sí	Event handlers ejecutan scripts al fallar (reinicio, aislar, ticket).	
Reportes SLA y paneles ejecutivos	Sí (XI)	XI trae dashboards y reportes de SLA listos para gerencia.	
Arranque “todo en uno” (plantillas + descubrimiento)	No (parcial)	Requiere más configuración para quedar completo.	Zabbix: templates y discovery nativos aceleran el despliegue.
Monitoreo cloud-native / Kubernetes a escala	No	No está orientado al modelo pull y métricas masivas.	Prometheus: pull + exporters + ecosistema K8s.
Consultas avanzadas de métricas (series temporales)	No	Sin lenguaje nativo de series temporales.	Prometheus: PromQL para reglas/correlaciones.
Visualización “lista” sin extras	Parcial	XI mejora bastante, pero no tanto out-of-the-box.	Zabbix: dashboards/mapas nativos; Prometheus suele usar Grafana.
Ecosistema de plugins/extensibilidad	Sí	Amplio catálogo de plugins y add-ons para hosts/servicios.	

CONCLUSIÓN

Nagios es una opción sólida para respuesta a incidentes en entornos IT tradicionales: detecta y alerta con precisión y, gracias a los event handlers, puede actuar automáticamente (reinicios, aislar, abrir ticket) reduciendo el MTTR; en Nagios XI además tienes SLA reports y dashboards listos para presentar.

En comparación, si necesitas arranque “todo en uno” con plantillas y descubrimiento nativos, Zabbix suele llevar ventaja; y para cloud-native/Kubernetes y consultas avanzadas de series temporales, Prometheus domina por su modelo pull, exporters y PromQL.

1. Nagios Enterprises. (n.d.). Event handlers · Nagios Core documentation. https://assets.nagios.com/downloads/nagioscore/docs/nagioscore/4/en/eventhandlers.html
2. Nagios Enterprises, LLC. (2025). Nagios XI application architecture overview [PDF]. https://assets.nagios.com/downloads/nagiosxi/docs/Nagios-XI-Architecture-Overview.pdf
3. Nagios Enterprises, LLC. (2025). Introduction to event handlers in Nagios XI 2024 and 2026 [PDF]. https://assets.nagios.com/downloads/nagiosxi/docs/Introduction-to-Event-Handlers-2024.pdf
4. Nagios Enterprises, LLC. (2025). How to generate SLA reports with Nagios XI 5 [PDF]. https://assets.nagios.com/downloads/nagiosxi/docs/Generating-SLA-Reports-With-Nagios-XI.pdf
5. Nagios Enterprises, LLC. (2025). NCPA v3 agent installation instructions [PDF]. https://assets.nagios.com/downloads/ncpa/docs/Installing-NCPA.pdf
6. Prometheus Authors. (n.d.). Overview. https://prometheus.io/docs/introduction/overview/

GESTIÓN DE INCIDENTES Y ANÁLISIS DE RIESGO

Home **Content** Demo

GRACIAS POR SU ATENCIÓN