



Monitoreo de infraestructura con Nagios

Proyecto Final
Telecomunicaciones III

- Iván C. Holguín
- Miguel S. Rondón
- Kevin A. Trujillo
- Julián A. Vega



INFORMACIÓN LEGAL

Dando cumplimiento a la Ley estatutaria 1581 de 2012, la Universidad Autónoma de Occidente se permite informar que esta sesión académica será transmitida en vivo, se podrán tomar imágenes de los asistentes y ser grabada en video para usos y fines estrictamente académicos.

Los derechos de autor sobre el contenido de la sesión académica se encuentran protegidos conforme a lo dispuesto por el artículo 20 de la Ley 23 de 1982, modificado por el artículo 28 de la Ley 1450 de 2011. Queda prohibida su difusión, distribución o divulgación en redes sociales o cualquier otro medio no institucional.

CONTEXTO



Prestador Servicios WEB



Realtek S.A

Servicios: Usos y aplicaciones

Empresa Solicitante



ElectroVTRH S.A

Encargados de estudiar el caso y brindar una solución

Problemática



Disponibilidad

Servidores Web y FTP, así como sus servicios

Consecuencias



Economía

Pérdidas para la Realtek S.A y sus clientes

Solución



Plataforma

Implementar una plataforma de monitoreo de infraestructura

Objetivos



Identificar

Posibles fallas usando alertas tempranas que permitan realizar acciones preventivas.

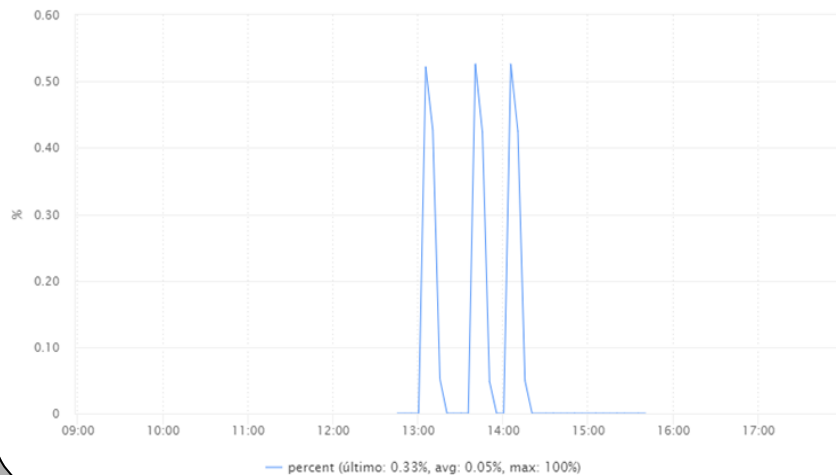
REQUERIMIENTOS



192.168.1.101 CPU Usage Grafica de Rendimiento

192.168.1.101 : CPU Usage

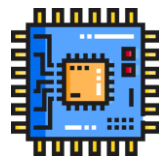
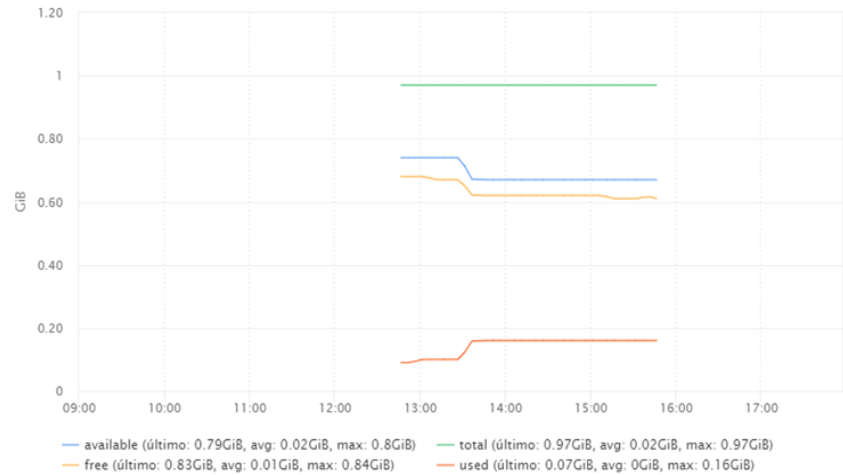
Reset zoom



192.168.1.101 Memory Usage Grafica de Rendimiento

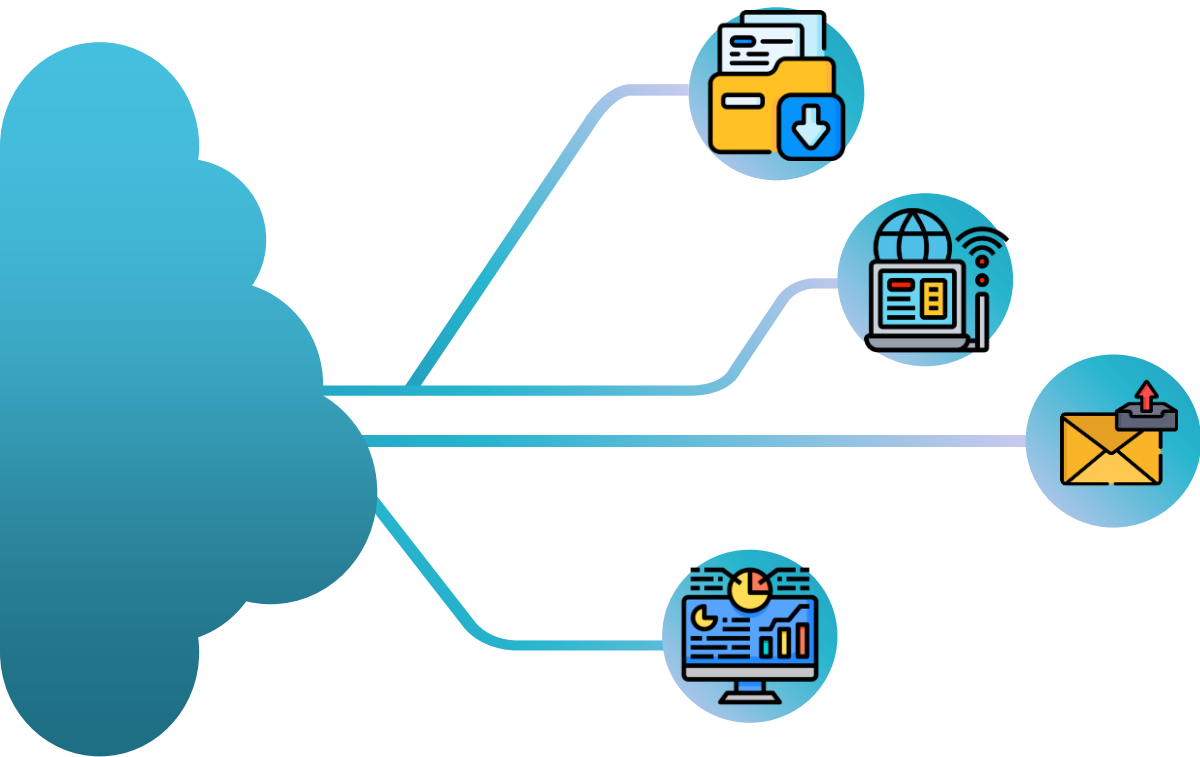
192.168.1.101 : Memory Usage

Reset zoom



MARCO TEÓRICO





| | |
|----------------|---|
| FTP | 1 |
| HTTP | 2 |
| SMTP | 3 |
| MONITOR DE RED | 4 |

ALTERNATIVAS





Ventajas

- Modificaciones totalmente en línea.
- Gran gama de gráficos.
- Interfaz web moderna.
- Mayor cantidad de protocolos con respecto a Nagios.
- Sistema de escalamiento en las notificaciones

Desventajas

- No cuenta con detección automática de forma predeterminada.
- No permite la integración de complementos personalizados. [9]



Ventajas

- Escalamiento.
- Integrable con otros servicios.
- Poderoso para redes de aplicaciones y seguridad [8].
- Detección automática.
- Variedad de complementos. [9]

Desventajas

- No tiene soporte en Windows ni MAC.
- No ofrece gráficos por defecto.
- Interfaz de configuración web desactualizada. [9]



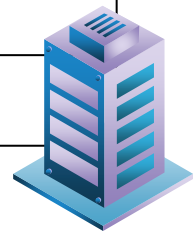
Ventajas

- Integrable con casi todos los sistemas de la industria.
- Amigable visualmente.
- Facilidad de uso.
- Monitorea la funcionalidad de la aplicación [8]

Desventajas

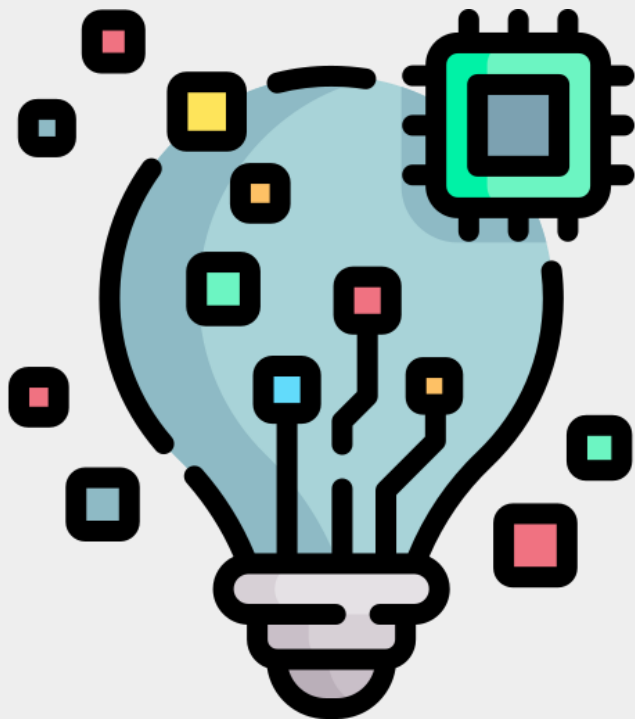
- El escalado de aplicaciones afecta los datos en tiempo real.
- Aumento en los esfuerzos de mantenimiento e incremento en los costos del servicio. [8]

| Servicios | Nagios | Zabbix | Prometheus |
|---|--|--|---|
| Panel de control e interfaz de usuario | Proporciona información básica, como el estado de los dispositivos, pero no ofrece tanto nivel de claridad y calidad de visualización. | Tiene la ventaja en función de su valor de producción. Su tablero se puede personalizar y ofrece una experiencia más limpia. | Activo para el escaneo de servicios por etiquetas y protocolos. Totalmente editable |
| Configuración | Obliga al usuario a ingresar configuraciones como archivos de texto. | Le permite cambiar sus configuraciones a través de una interfaz basada en web. | Necesita que todas sus configuraciones se establezcan por red |
| Protocolos | HTTP, FTP, SMTP, SNMP, POP3, SSH y MySQL. | HTTP, FTP, SMTP, SNMP, POP3, SSH y MySQL. | HTTP, HTTPS, Graphite, StatsD, SNMP, JMXy CollectD. |
| Plantillas de monitoreo | NO | FTP, HTTP, HTTPS, IMAP, LDAP, MySQL, NNTP, SMTP, SSH, POP y Telnet. | NO |
| Complementos | SI | NO | SI |
| Comunidad | 67,000 | 80,000 | 47,000 |
| Precio | Gratis con ventajas de pago | Gratis | Gratis |

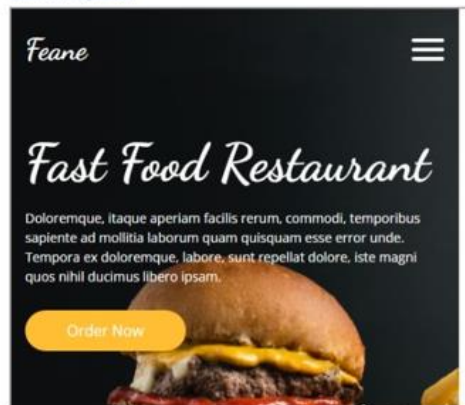


IMPLEMENTACIÓN





Vista Previa Página Web



Vista Previa Página Web Segura



Tamaño de Paquetes HTTP



Tiempo de Respuesta solicitud HTTP



Tamaño de Paquetes HTTPS



Tiempo de Respuesta solicitud HTTPS



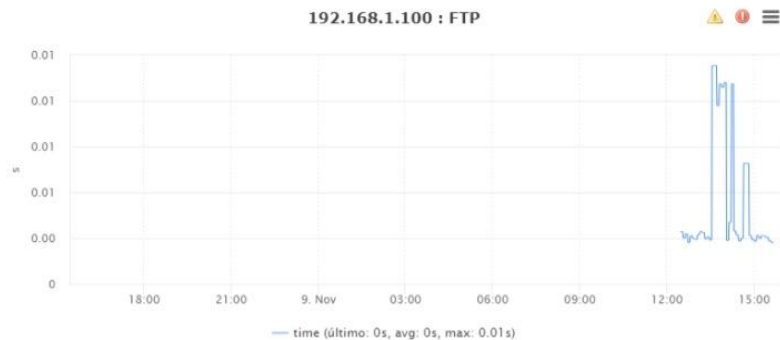
192.168.1.101 HTTP Gráfica de Rendimiento



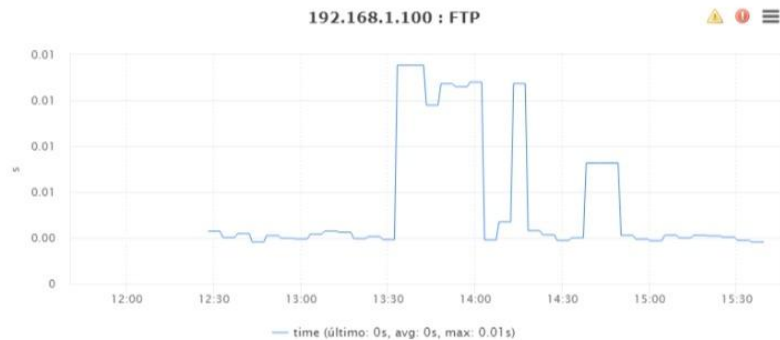
192.168.1.101 HTTPS Gráfica de Rendimiento



192.168.1.100 FTP Grafica de Rendimiento



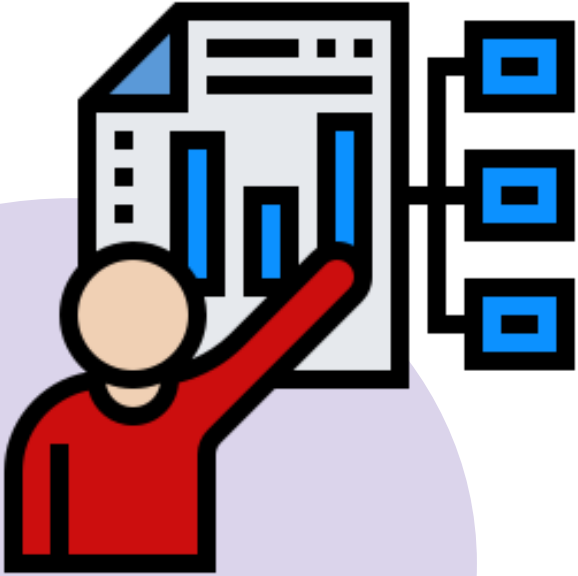
192.168.1.100 FTP Grafica de Rendimiento 4 horas

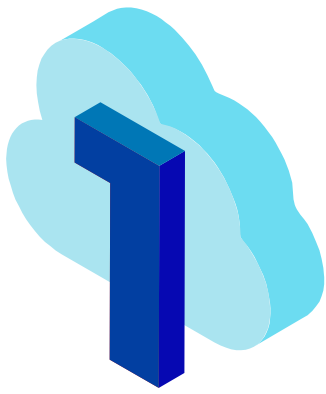


Tiempo de Respuesta FTP



CONCLUSIONES





Nagios

A pesar de que existen diferentes plataformas que permiten el monitoreo de redes todas tienen un énfasis que las hace significativas para las diferentes aplicaciones. En el caso de nagios, se encontró que es una herramienta que permite la detección de equipos y servicios en tiempo real de manera simple ya que es muy intuitiva para el usuario. Para el caso de este proyecto, fue muy eficiente.



Monitoreo

Al no contar con una herramienta en Nagios que nos permitiera conocer de manera explícita el número de transferencias (FTP) o de solicitudes get (HTTP), se consideró el monitoreo de otro tipo de parámetros como el uso de memoria y CPU.





Prevención

Es importante contar con una herramienta de monitoreo cuando se tienen redes grandes, debido a que permite identificar y alertar de forma oportuna sobre posibles fallas en la disponibilidad y calidad de los servicios que se prestan de acuerdo a parámetros configurables por el administrador de la red, brindando la posibilidad de solucionar los problemas detectados antes de que se presenten de forma crítica.



Benchmark

Para el monitoreo de la CPU y memoria de las máquinas asociadas a Nagios, fue indispensable tener un indicador que nos permitiera visualizar el estado de estas dos variables. Sin embargo fue necesario descargar un paquete en los dispositivos monitoreados que brinda la posibilidad de modificar el comportamientos de estos parámetros sin la necesidad de generar procesos manualmente.



REFERENCIAS



[1] FTP: qué es y cómo funciona (xataka.com) . Tomado de <https://www.xataka.com/basics/ftp-que-como-funciona>

[2] Generalidades del protocolo HTTP - HTTP | MDN (mozilla.org). Tomado de <https://developer.mozilla.org/es/docs/Web/HTTP/Overview>

[3] IBM Docs. Tomado de <https://www.ibm.com/docs/es/i/7.3?topic=information-smtp>

[4] ¿Qué es el monitoreo de red? - Cisco . Tomado de https://www.cisco.com/c/es_mx/solutions/automation/what-is-network-monitoring.html

[5] Monitorización en tiempo real con Nagios - LIDER IT Consulting. Tomado de <https://www.liderit.es/monitorizacion-en-tiempo-real-con-nagios/> [Artículo web]

[6] ¿QUE ES ZABBIX? herramienta de monitoreo de redes (quasarbi.com). Tomado de <https://quasarbi.com/ZABBIX.html> [Artículo web]

[7] Grafana y Prometheus para monitoreo de contenedores | Aplyca. Tomado de <https://www.aplyca.com/es/blog/grafana-y-prometheus-para-monitoreo-de-contenedores>

[8] Prometeo vs. Nagios | MetricFire Blog. Tomado de <https://www.metricfire.com/blog/prometheus-vs-nagios/#strongWhen-to-use-Hosted-Prometheus-by-MetricFirestrong>

[9] Comparación de Nagios y Zabbix: ¿cuál es mejor para la supervisión de la red? (dementium2.com). Tomado de <https://dementium2.com/administrador-neto/comparacion-de-nagios-y-zabbix-cual-es-mejor-para/>

[10] Nagios XI Resources. Tomado de <https://www.nagios.com/resources/nagios-xi/>

[11] Telecomunicaciones 3 Proyecto Final Tomado de <https://github.com/miguel-rondon/Telecomunicaciones-3-Proyecto-Final/blob/master/Guia.md>