Laura Mayals

ASO

Sistemas Integrados de monitorización de redes

El término monitoreo de red describe el uso de un sistema que constantemente monitoriza una red de computadoras para buscar componentes lentos o defectuosos. Si encuentra alguno, se notifica vía correo o con otro tipo de alarma a los administradores de redes. Un sistema de monitorización de red busca problemas causados por la sobrecarga y/o fallas en los servidores, como también problemas de la infraestructura de red u otros dispositivos.

A la hora de evaluar un software de monitorización de la red se debe tener en consideración las siguientes características (entre otros):

- Comunicación de las alertas.
- Integraciones con servidores externos.
- Usabilidad y presentación de los datos en el panel.
- API de acceso desde sistemas externos.
- Detección de dispositivos de forma automática.
- Integraciones con Bases de Datos
- Multidispositivo
  -Escalado: Puede monitorizar más que sólo la red (aplicaciones, servidores...)
- Soporte del mayor número de protocolos de adquisición de datos posible
- Seguridad
- Integración con máquinas virtuales
- Integraciones hardware
- Control remoto
- Monitorización de la nube

Lo que nos aporta es una optimización de nuestras instalaciones y componentes. Podremos saber cuándo vamos a necesitar más hardware y cuándo estamos sobredimensionando. Por otro lado, obtendremos una mayor anticipación de problemas y evitar que lleguen a más y detectar tráfico intruso o malintencionado. También nos sirven para detectar cuellos de botella.

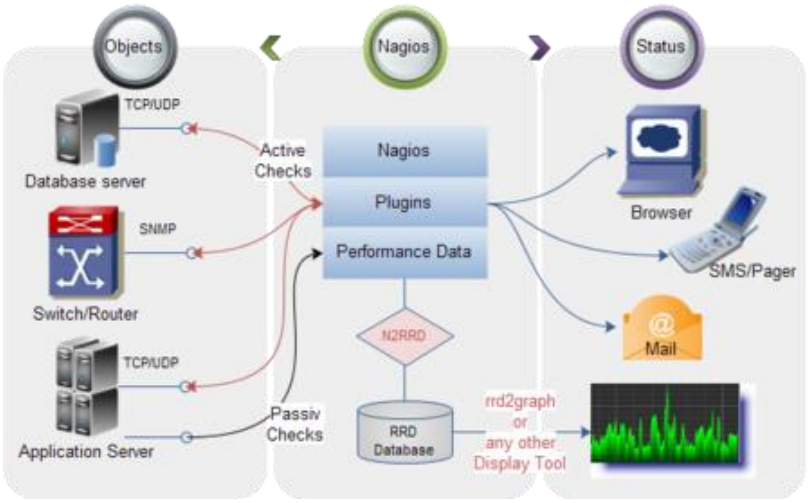
Hay varios programas que permiten el monitoreo de redes entre ellos está Nagios.

Nagios es un sistema de código abierto que vigila los equipos a nivel de hardware y servicios que se especifiquen y alerta cuando el comportamiento no es el deseado. Una de sus características principales es la monitorización de servicios de red (SMTP, POP3, HTTP...) , la monitorización de la carga de los procesadores, el uso de los discos y memoria. También su independencia de sistemas operativos, la posibilidad de programar plugins sobre el core específicos para nuevos sistemas y de poder monitorizar remotamente a través de túneles SSL cifrados o SSH.

Las alertas se pueden recibir a través de correo electrónico y sms (entre otros).

Es un acrónimo recursivo “Nagios Ain't Gonna Insist On Sainthood”. Es una referencia a la encarnación original del software bajo el nombre de Netsaint, que tuvo que ser cambiado por ser supuestamente similar a un nombre comercial. "Agios" significa "santo" en griego.

Su gran uso es debido a que fue el primer jugador que desarrolló una herramienta que cubría características indispensables en una monitorización de red. Pero ha ido disminuyendo a lo largo de esta década



Ventajas:

1. Si se tiene gran conocimiento de la herramienta, la configuración manual puede darle mucha potencia a la hora de monitorizar casos aislados y particulares.
2. Ofrece muchos plugins para adaptar Nagios a las necesidades del usuario.
3. Para la configuración básica es muy fácil.
4. Versión libre
5. Capacidad para reiniciar automáticamente aplicaciones, servicios, servidores y dispositivos cuando se detecten problemas.

Inconvenientes:

1. El interfaz gráfico carece de una buena usabilidad.
2. Coste de aprendizaje elevado.
3. Si el equipo técnico (generalmente una única persona) se va de la compañía, será imposible mantener el proyecto de monitorización
4. El Nagios base está extremadamente limitado en funcionalidades de serie, y eso se suple con plugins, addons y extensiones de terceros, lo que lo convierte en un ecosistema todavía menos estándar. En pocas palabras, un puzzle de piezas hechas por personas que no tienen nada en común, y que carecen de una visión conjunta.
5. Informes sencillos.

En resumen, Nagios fue el origen de la monitorización y, de hecho, muchas nuevas herramientas de monitoreo de redes han heredado el código de Nagios y lo han evolucionado. Aunque tienes muchos perfiles en el mercado, estos deben tener un conocimiento muy técnico y tu instalación dependerá de ellos al 100%. La futura migración podrá ser complicada.

Otro ejemplo sería Zabbix.

Zabbix es un Sistema de Monitorización de Redes creado por Alexei Vladishev. Está diseñado para monitorizar y registrar el estado de varios servicios de red, Servidores y hardware de red.

muchos usuarios de Nagios se están moviendo a Zabbix porque ha recogido el legado de Nagios y empieza a tener la visibilidad que tenía antes Nagios.

Usa MySQL, PostgreSQL, SQLite, Oracle o IBM DB2 como base de datos. Su backend está escrito en C y el frontend web está escrito en PHP.

Fácil configuración y potente interfaz gráfico. Empieza a caer su rendimiento cuando se empiezan a monitorizar muchos nodos. Destaca el servicio de

monitorización sin necesidad de instalar agentes. Se pueden monitorizar hasta 10,000 nodos sin problemas de rendimiento.

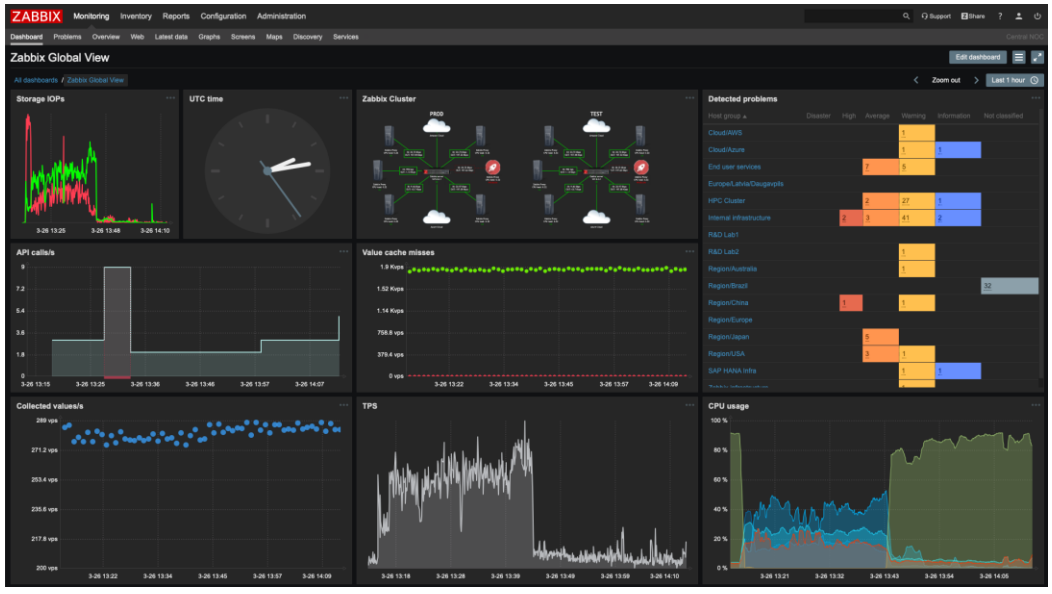
Ventajas:

1. Su comunidad es bastante activa.
2. Es potente a bajo nivel.
3. Auto descubrimiento de servidores y dispositivos de red
4. Posibilidad de monitorización sin agentes

Desventajas:

1. Aunque se ha utilizado en grandes instalaciones, a partir de 1000 nodos puede disminuir su rendimiento.
2. Difícil crear y definir plantillas de informes y alertas. Las configuraciones pueden requerir muchos clics y pasos para completarlas.
3. Es difícil de depurar cuando hay errores.
4. No posee informes en tiempo real.
5. Pobre tratamiento de traps.

Zabbix recoge el testigo de Nagios y empieza a aparecer en muchas instalaciones. La problemática es su escalado para grandes CPDs. Si la instalación tiene varios elementos del mismo tipo (por ejemplo bases de datos) sus configuraciones van a ser complicadas.



Finalmente, también existe **Pandora FMS** que es un software de código abierto que sirve para monitorizar y medir todo tipo de elementos. Monitoriza sistemas, aplicaciones o dispositivos de red. Permite conocer el estado de cada elemento de un sistema a lo largo del tiempo ya que dispone de histórico de datos y eventos.

Está orientado a grandes entornos, y permite gestionar con y sin agentes, varios miles de sistemas, por lo que se puede emplear en grandes clusters, centros de datos y redes de todo tipo.

Puede detectar si una interfaz de red se ha caído, un ataque de "defacement" en una web, una pérdida de memoria en algún servidor de aplicaciones y puede enviar SMS si un sistema falla o cuando cuándo x cosa suceda como el valor de acciones.

Es un framework de monitorización que permite desde monitoreo de infraestructura (redes y servidores), monitorización de rendimiento y aplicaciones (APM) hasta monitorización transaccional de negocio (BAM)

Pandora FMS está formado por tres componentes: servidor, consola y agente

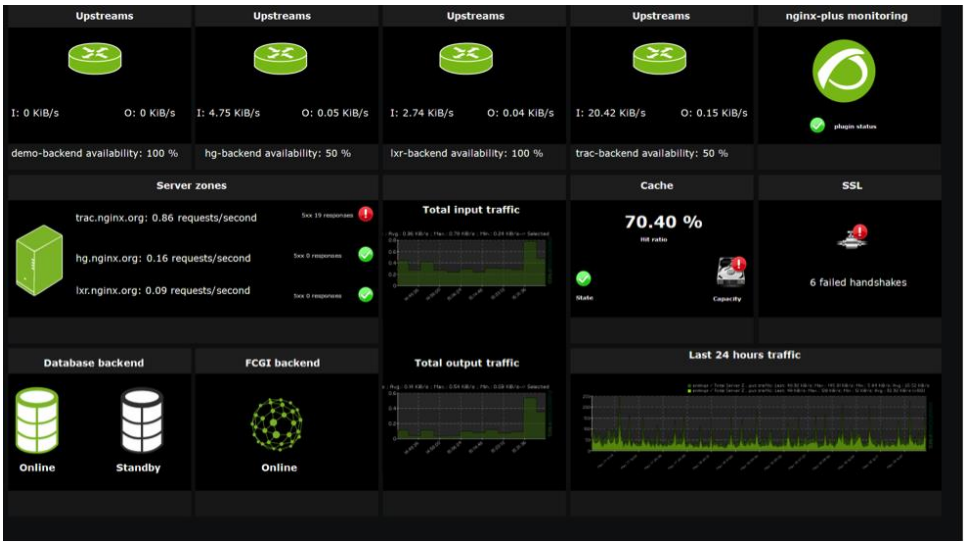
El servidor de Pandora FMS es quien procesa los datos recolectados de diferentes maneras, también son los que ejecutan alertas y guardan la información en la base de datos. Consola: la interfaz web con la interfaz al usuario para administrar los servidores, catalogar la información, crear alertas, crear incidentes, cambiar contraseñas de acceso y en general permiten toda la configuración del sistema de manera horizontal. Aquí se realiza la conversión de lenguaje de bajo nivel al lenguaje de alto nivel. Finalmente los agentes de Pandora FMS son entidades organizativas, generalmente un ordenador. Los agentes tienen la información, y pertenecen a un solo grupo.

Ventajas:

1. Funciona con cualquier sistema operativo.
2. No necesita instalar agentes.
3. Sistema de alerta sms.
4. Versión libre.
5. Misma herramienta para distintos entornos.
6. Interfaz Web.
7. SQL backend.
8. Tiempo de evaluación muy bajo.

Desventajas:

1. La versión no gratuita es muy cara



En mi opinión este último software de monitorización de red es el más completo ya que engloba muchas funcionalidades y apenas le encuentro defectos