Checkmk como herramienta de monitoreo de infraestructura

Carmen Daniela Correa, Brian Mlataz, Gonzalo Sudriá, Rodrigo Zalazar[1]

[1] Fac. de Ciencias Exactas Naturales y Agrimensura, Universidad Nacional del Nordeste, Corrientes
correa.danielacc@gmail.com,ivanmlataz@gmail.com,sudria.gonzalo@gmail.com, rodrigo.zalazar@comunidad.unne.edu.ar

Abstract. El monitoreo de redes informáticas siempre ha sido una tarea compleja, y si no contamos con las herramientas adecuadas esta tarea puede complejizarse aún más; para lo cual en este trabajo vamos a presentar una alternativa como posible solución.

Consideramos que es una herramienta muy poderosa de código abierto con una interfaz intuitiva. En el marco del trabajo de investigación en equipo de la asignatura Redes de Datos, cuarto año de la Carrera Licenciatura en Sistemas de Información, vamos a desarrollar la instalación y el desarrollo inicial de esta solución de software, para comprender su efectividad como herramienta de monitoreo de infraestructura informática.

Keywords: Checkmk, Monitoring, Linux Server, Monitoring Agents.

1 Introducción

Hoy en día, las infraestructuras TI son infinitamente mayor a la escalabilidad de las redes de los años 90, por ejemplo. En el 2021, hubo más de 35 billones de dispositivos conectados.[7] Cada día son más los empleados de empresas que trabajan de forma remota,es decir, que acceden a las redes de la empresa desde el exterior aumentando así las amenazas a la seguridad y privacidad de los datos que se manejan dentro de estas grandes estructuras empresariales.

Como solución al problema planteado anteriormente, presentamos la herramienta de software para monitoreo, Checkmk. Es un software desarrollado en Python y C ++ para monitorear la infraestructura y las redes de TI. Se utiliza para el control de servidores, aplicaciones con y sin contenedores, redes, infraestructuras en la nube (públicas, privadas e híbridas), dispositivos de almacenamiento, bases de datos y sensores ambientales.[3]

Ofrecen varias ediciones, por un lado una edición exclusivamente empresarial (Checkmk Enterprise Edition – CEE) que se basa en un núcleo de monitoreo patentado y tiene muchas funciones adicionales relacionadas con la automatización y la generación de informes, que es muy adecuado para monitorear grandes entornos TI, la misma posee su prueba gratuita, que tiene las mismas características, donde se puede

hacer uso del monitoreo distribuido, monitoreo de dispositivos SNMP, entre otros, pero que está limitada a 25 hosts después de 30 días.

Por otro lado, CheckMk Cloud Edition, la cual cubre casos de uso esenciales de la nube, como computación, redes y almacenamiento, así como tecnología avanzada nativa de la nube, como bases de datos administradas, funciones y microservicios.[2]

Por último, la edición de código abierto (Checkmk Raw Edition - CRE) para empresas y usuarios avanzados, que posee extensibilidad, flexibilidad y adaptabilidad.

Definiciones:

Agente

Recopila los datos relevantes para el monitoreo de un host. Este agente puede ser un pequeño programa instalado en el host (el agente Checkmk), un agente SNMP que se ejecuta independientemente de Checkmk en el host, un agente especial que obtiene la información a través de una API proporcionada por el sistema de destino o una verificación activa que consulta servicios basados en red.[2]

Integraciones de API

Cuando la configuración de Checkmk se refiere a las integraciones de la API, significa monitorear datos que utilizan el formato de datos del agente de Checkmk pero que se originan en una fuente diferente. Dichas fuentes pueden ser programas de fuentes de datos, agentes especiales o hosts que aprovechan sus datos. Si los datos recibidos a través de una integración de API se van a usar en el monitoreo, las integraciones de API deben estar habilitadas en las propiedades de un host.[2]

Check

Controlar una verificación en el contexto de Checkmk es la verificación de un host o servicio de acuerdo con reglas predefinidas y, por lo tanto, un complemento de verificación es el proceso que determina el estado de los hosts y servicios. En otras palabras, la ejecución de un complemento de verificación da como resultado que se devuelva un estado de OK, DOWN, UNREACH, WARN, CRIT, PEND o UNKNOWN.[2]

Monitoreo distribuido

Checkmk distingue entre una monitorización distribuida y una configuración distribuida. El monitoreo distribuido significa que todo el sistema de monitoreo consta de más de un sitio de Checkmk y todos los datos se muestran juntos en un solo lugar. O dicho de otro modo: la monitorización consta entonces de un sitio central y al menos un sitio remoto, y los datos del sitio remoto también se muestran en el sitio central. El monitoreo distribuido se puede combinar opcionalmente con una configuración distribuida.[2]

2 Instrumentación

Para el desarrollo de este trabajo utilizaremos la versión Raw Open Source.

Primeros pasos para la instalación del software en una versión Servidor Linux Ubuntu 22.04, lo descargamos: (fig.1)

$ wget https://download.checkmk.com/checkmk/2.1.0p2/check-mk-free-2.1.0p2_0.jammy_amd64.deb

Instalación.

Ahora se instalará Checkmk con todas sus dependencias, es decir, con su propia versión de Apache, PHP y Python. Todas estas versiones están marcadas en el paquete, por lo que una vez ejecutado el comando de instalación, se agregaran automáticamente.

./check-mk-free-2.1.0p2_0.jammy_amd64 .deb (fig.2)

Crear una instancia.

Con Checkmk instalado, necesitamos crear nuestra primera instancia de monitoreo. Vamos a crear la instancia trtest con el comando:

$sudo omd create trtest (fig.3)

Una vez que la instancia es creada, debemos inicializarla:

$sudo omd start trtest (fig.4)

La web a la que debemos acceder es: http://SERVER/trtest, donde SERVER es la dirección IPv4 de nuestro host servidor, “trtest” es el nombre de la instancia. En nuestro caso seria: 192.168.0.43/trtest

Una vez dentro nos aparecerá la interfaz de checkmk. (fig.5)

Las credenciales a utilizar por defecto son User: cmkadmin, Password: dVgoHd4b (generado automaticamente al crear una nueva instancia por Checkmk, y puede ser modificada al ingresar al apartado visual) Una vez que iniciemos sesión, nos aparecerá el main dashboard. (fig.6)

3 El sistema

Componentes. Configuración y control

Checkmk ofrece descubrimiento de servicios y generación automática de parámetros, utiliza su propio método para realizar comprobaciones y solo sondea cada host una vez para recopilar datos. Los resultados de la encuesta se transmiten al núcleo de seguimiento como "controles pasivos". Esto mejora en gran medida el rendimiento del servidor de supervisión y los hosts supervisados.

Checkmk utiliza diferentes métodos para acceder a los datos. Estos incluyen los agentes instalados en el sistema de destino; los "agentes especiales" que se ejecutan en el supervisor y se comunican con la API del sistema de destino, la API SNMP para la gestión de red de dispositivos e impresoras de red; y protocolos HTTP/TCP para comunicarse con servicios web e Internet. Por defecto, Checkmk realiza una consulta explícita (tracción) de datos con el fin de identificar rápidamente los fallos del sistema.

Un host también puede transferir directamente sus datos a Checkmk o a un host intermedio (push).[3]

Inteligencia de Negocio

El módulo de inteligencia empresarial está integrado en la interfaz gráfica. Reúne el estado general de los procesos comerciales y su dependencia de aplicaciones y elementos de infraestructura de diferentes hosts y servicios. Se basa en las reglas definidas por el operador. También se puede usar para controlar aplicaciones compuestas por microservicios que consisten en módulos de Kubernetes e implementaciones de aplicaciones en contenedores.

Además, se pueden simular los peores escenarios en tiempo real y se pueden analizar datos históricos para identificar las causas de la degradación del rendimiento.[3]

Sistema de alarma

Se pueden configurar varios canales de notificación con diferentes reglas para cada usuario. Por ejemplo, los correos electrónicos se pueden enviar en cualquier momento del día, pero los SMS solo se envían para los problemas más importantes y durante las horas de guardia. Las notificaciones se pueden configurar para todos los equipos o para equipos específicos, por ejemplo, notificando solo a los administradores responsables del almacenamiento que un disco duro ha fallado. Los mensajes duplicados se agrupan para que un usuario no sea notificado dos veces a través del mismo canal. Además, los usuarios pueden configurar sus propias notificaciones. En entornos distribuidos, las alertas se pueden gestionar de forma centralizada. Para los problemas detectados, las acciones se pueden activar automáticamente mediante

scripts. Checkmk incluye integración con pasarelas de correo electrónico y SMS, así como soluciones de comunicación como Slack, Jira, PagerDuty, OpsGenie, VictorOps y ServiceNow.[3]

Consola de eventos

La consola de eventos integra el procesamiento de mensajes de registro y capturas SNMP con la aplicación de monitoreo. Está configurado por un conjunto de reglas que clasifican los mensajes según se deben procesar o eliminar. La consola puede contar mensajes, correlacionarse y esperar nuevos, reescribirlos, etc. Las entradas se pueden agrupar (por ejemplo, después de varios errores de inicio de sesión) para realizar un seguimiento de los eventos.

La consola también incluye un demonio syslog que recibe mensajes directamente en el puerto 514 y un administrador SNMP que los recibe en el puerto 162.[3]

Representación de datos métricos

Las ediciones comerciales de Checkmk utilizan su propia representación gráfica de datos métricos (también conocida como series de tiempo). Esto permite que sus datos sean analizados durante largos intervalos utilizando imágenes HTML5 interactivas

con una resolución de hasta un segundo. Los datos pueden importarse de una variedad de fuentes y formatos (JSON, XML, SNMP, etc.) y almacenarse a largo plazo en otro dispositivo.

También es posible exportar los datos a Graphite o InfluxDB. En la versión 1.5p16 de la versión CEE, hay un complemento disponible para exportar datos directamente a

Grafana para su visualización. El Checkmk Raw Edición utiliza pnp4nagios como el sistema de gráficos.[3]

Informes

Los informes permiten producir documentos en formato PDF, de forma automática o ad hoc y a intervalos regulares. Incluyen análisis de tiempo de actividad en el que se puede proporcionar el historial de datos con un clic durante cualquier período de tiempo. Los cálculos de disponibilidad pueden excluir las horas desatendidas, ajustar la resolución o ignorar intervalos cortos. Además de los cálculos de disponibilidad, también pueden incluir información de calidad de servicio (SLA) en la que se pueden monitorear configuraciones complejas. Los informes solo están disponibles en las versiones comerciales de Checkmk.[3]

4 Ejecución del Programa

Agregar un nuevo host.

Para ello vamos a la barra de herramientas, y accedemos a "setup" y a la opción "hosts" (fig.7). En el menú contextual de hosts, damos click en "Add hosts" para añadir un nuevo host . (fig.8)

Agregamos la ip del host que vamos a añadir. Y en hostname, se le asigna un alias para identificarlo de manera más fácil. (fig.9)

Para cada host, será necesario descargar e instalar un agente. Este apartado se encuentra en la barra de herramientas, en el apartado "setup". Debemos seleccionar en qué plataforma vamos a instalar el agente, y permitir el paso de tráfico a través del Firewall, añadiendolo a la white list. (fig.10)

Una vez hecho todo esto, podemos acceder a la interfaz visual y visualizar y monitorear nuestro host recientemente agregado. (fig.11)

Es posible observar que la barra de herramientas nos permite visualizar todos los hosts, o discriminarlos por plataforma de windows o linux. (fig.12)

Es posible seleccionar un determinado host y obtener una lista de los servicios monitoreados. (fig.13)

Una opción adicional es obtener un estado general del host. (fig.14)

5 Competitividad de Checkmk

En el marco de esta investigación, situaremos a Checkmk frente a otros agentes de monitoreo disponibles actualmente.

Zabbix

En el sistema de monitoreo de Zabbix, se pueden configurar múltiples servidores que se dividen en diferentes roles, como servidores proxy, servidores frontend y

servidores de base de datos, según sus funciones específicas, en este caso los servidores proxy actúan como intermediarios entre los agentes de monitoreo y el servidor central, los cuales pueden llegar a ser cuellos de botella , por otro lado CheckMK se destaca por poseer una arquitectura distribuida, donde los hosts y servicios monitoreados se pueden asignar a instancias esclavas específicas para distribuir la carga de trabajo de manera equilibrada y evitar una sobrecarga en una sola instancia lo que a su vez posibilita la configuración de instancias maestras y esclavas para una alta disponibilidad y así garantizar la continuidad del monitoreo incluso en caso de fallas de servidor. Esto mejora la confiabilidad y la disponibilidad del sistema de monitoreo.[10]

En Zabbix, la configuración centralizada se realiza en el servidor central, y los servidores proxy se encargan del monitoreo y la recopilación de datos. En Checkmk, cada sitio de monitoreo se puede administrar y configurar de manera independiente, lo que permite una mayor flexibilidad en la administración de la arquitectura distribuida.[10]

Zabbix puede requerir más recursos de hardware, como servidores proxy dedicados y servidores de base de datos, dependiendo del tamaño y la complejidad del entorno de monitoreo. Checkmk, por otro lado, puede ejecutarse en una infraestructura más liviana y puede aprovechar tecnologías como la virtualización y el aprovisionamiento en la nube. La implementación de la arquitectura distribuida de Zabbix puede requerir una configuración más detallada y compleja, ya que los componentes individuales deben configurarse y comunicarse correctamente entre sí. Checkmk, por otro lado, ofrece una implementación más sencilla y basada en la replicación de sitios de monitoreo.

PRTG (Paessler Router Traffic Grapher)

En PRTG, la configuración se realiza a través de la interfaz de usuario central, aunque ofrece una interfaz de usuario intuitiva y una amplia gama de sensores preconfigurados, pero puede haber limitaciones en términos de personalización y flexibilidad en comparación con Checkmk, que ofrece una configuración más granular y avanzada que se puede realizar en cada sitio de monitoreo de manera independiente con una interfaz de usuario intuitiva y una configuración simplificada que permite a los usuarios implementar y comenzar a monitorear rápidamente además proporciona herramientas y asistentes para facilitar la configuración y la gestión del monitoreo, lo que reduce la complejidad técnica y el tiempo requerido para poner en funcionamiento el sistema.[9]

Por otro lado, PRTG utiliza un modelo de licenciamiento basado en el número de sensores que se utilizan para monitorear los dispositivos, es decir que el precio puede aumentar significativamente a medida que se requieren más sensores para monitorear más dispositivos y la administración y el rendimiento pueden volverse más desafiantes a medida que se agregan más dispositivos y sensores; sin embargo, Checkmk puede adaptarse a entornos de monitoreo pequeños y grandes, puede manejar grandes volúmenes de datos y mantener un rendimiento óptimo incluso en entornos de monitoreo complejos y distribuidos. Además, ofrece la capacidad de crear reglas y configuraciones personalizadas, crear paneles de control personalizados y desarrollar complementos y extensiones personalizadas para integrarse con otros sistemas y herramientas.[9] Checkmk también, cuenta con una comunidad activa de usuarios y desarrolladores que brindan soporte y comparten conocimientos y, como se presentó al

comienzo, la versión de código abierto que permite a los usuarios aprovechar las capacidades de monitoreo sin costo.

Es importante tener en cuenta que las necesidades y requisitos específicos de monitoreo pueden variar, por lo que se recomienda evaluar cuidadosamente las opciones disponibles y considerar cómo se alinean con los requisitos específicos del entorno a monitorear, pero en cuanto a monitoreo distribuido, licencia de código, alta disponibilidad y rendimiento, Checkmk presenta una considerable ventaja competitiva.

6 Conclusión y posibles mejoras

Las redes continúan haciéndose más grandes y complejas, por lo que comprender los beneficios del monitoreo de redes es extremadamente importante. El monitoreo en sí es una actividad compleja, ya que se necesita tener conocimientos avanzados sobre sistemas y programación de servidores. Por estas consideraciones, Checkmk es una solución de software que centraliza todos las herramientas, de forma eficiente y con una interfaz amigable.

Como posible solución, proponemos una instalación más rápida de los agentes de monitoreo, las cuales se podría hacer desde la interfaz web, con botones que muestran el agente a instalar e internamente lo hagan de forma directa en el servidor en donde está ejecutando el software de monitoreo.

Otra posible mejora, a fin de facilitar la instalación del software, es la implementación de las instrucciones necesarias a través de un comando script. Actualmente todo el software corre en el servidor de apache, el cual para la interfaz live status es un poco lento, tanto en la ejecución como en la actualización de los host y servicios monitoreados. Para estos casos es recomendable usar el servidor de nginx, que tiene un mejor rendimiento.

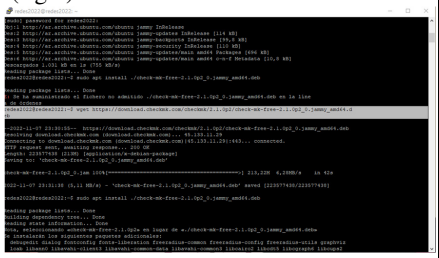
7 Referencias

[1]LINUX Magazine. Easy monitoring with Checkmk.
https://www.linux-magazine.com/Issues/2022/257/Checkmk
[2] Checkmk Documentation. Glossary.
https://docs.checkmk.com/latest/en/glossar.html
[3] Frikiwiki. Chechmk.
https://es.frwiki.wiki/wiki/Checkmk
[4] Tuxfixer. Install and Configure Checkmk on CentOS 8 and Monitor Linux Hosts using Checkmk agent.
https://tuxfixer.com/install-and-configure-checkmk-on-centos-8-and-monitor-linux-hosts-using-checkmk-agent/
[5] Baris Leenders. Checkmk.
https://www.youtube.com/c/checkmk-channel
[6] Aventis Technologies.Upgrade Checkmk Raw to Enterprise Free Edition.
https://aventistech.com/kb/checkmk-raw-to-enterprise -free-edition/
[7] Alexandra Cassandro. The benefits of networking monitoring.
https://www.whatsupgold.com/blog/the-benefits-of-networking-monitoring
[9] ECD. CheckMk: monitorización de IT para su empresa.

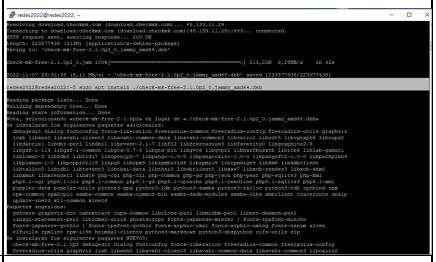
https://www.elconfidencialdigital.com/articulo/innovacion/check-mk-monitorizacion-it-empresa/20220520122406399005.html
[10]Checkmk Documentation. Distributed Monitoring.
https://docs.checkmk.com/latest/en/distributed_monitoring.html
[11] Zabbix Manual
https://www.zabbix.com/documentation/current/en/manual
[12]PGR Networking Monitoring..
https://www.paessler.com/manuals/prtg

Lista de Figuras.

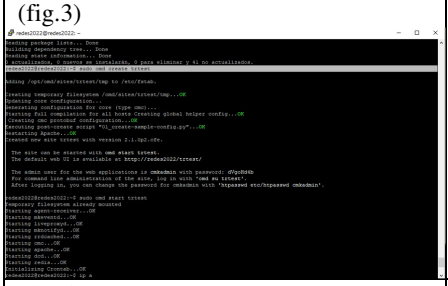
(fig.1)



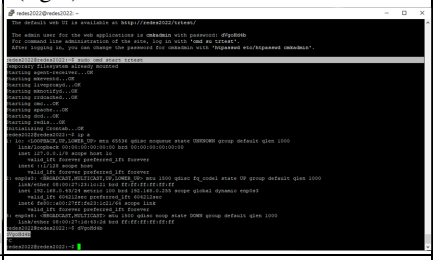
(fig.2)



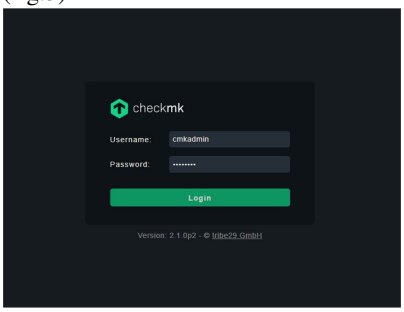
(fig.3)



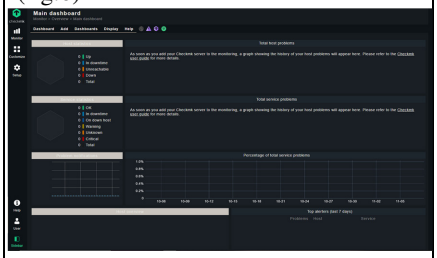
(fig.4)



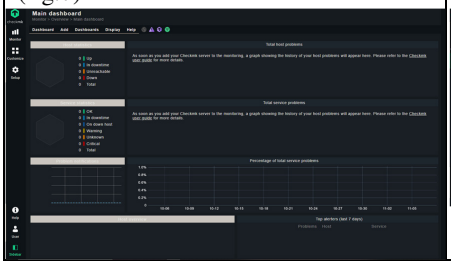
(fig.5)



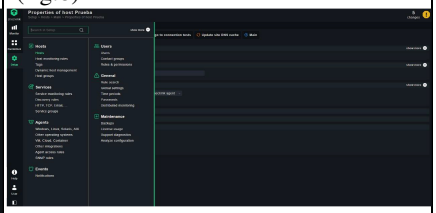
(fig.6)



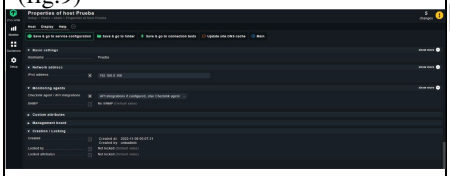
(fig.7)



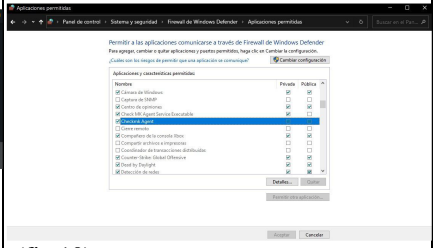
(fig.8)



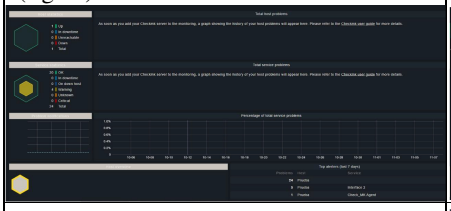
(fig.9)



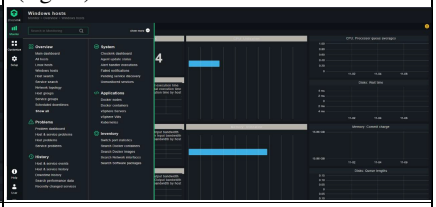
(fig.10)

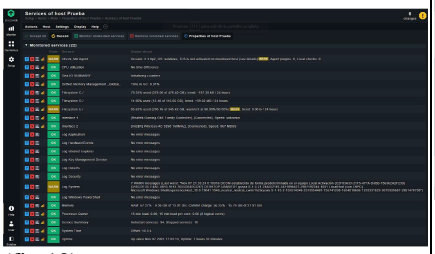


(fig.11)



(fig.12)





(fig.13)

(fig.14)