UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN

Sistema de Control de redes Computacionales para la detección de fallas en la infraestructura

TESIS Y EXAMEN PROFESIONAL

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN INFORMÁTICA

PRESENTA:

ALAN YAIR JIMENEZ VAZQUEZ

ASESOR: MTRO. ROGELIO SÁNCHEZ ARRASTIO

CUAUTITLÁN IZCALLI, ESTADO DE MÉXICO, 2020

Resumen

En este trabajo se implementa un sistema de monitoreo de redes de comunicaciones (Icinga Web 2) para analizar las características de supervisión que proporciona en la gestión de la infraestructura.

En el primer capítulo de este trabajo se da una introducción de cómo ha ido evolucionado la red a lo largo del tiempo y mencionamos algunos conceptos básicos que creemos indispensables para el óptimo entendiendo.

El segundo capítulo menciona lo que es un sistema de monitoreo describiendo algunas de sus características principales y se analizan algunos de los sistemas de monitorización que se encuentran en el mercado para poder ver algunas de sus características y cuál es que el que ofrece mayor rendimiento.

En el tercer capítulo hablamos de lo que es Icinga Web 2, se muestran algunas de sus principales características, los requerimientos básicos que se ocupan para su instalación correcta en diferentes sistemas operativos, de esta forma elegimos nuestro sistema operativo base donde se lleva a cabo la puesta en marcha.

En el cuarto capítulo hacemos la creación de 3 casos prácticos donde vamos a ocupar la herramienta, para monitorizar un servidor, un proxy y un switch, usando diferentes tipos de comandos de chequeo (http, load, procs, etc.) y vemos su comportamiento desde un ambiente gráfico.

El quinto y último capítulo analizamos los resultados de los casos prácticos y observamos si el sistema de monitoreo nos facilita la supervisión de la infraestructura de red dando un rendimiento óptimo.

DEDICATORIAS Y AGRADECIMIENTOS.

Gracias.

A mi papá Salvador Jimenez Sánchez y a mi mamá Elvia Vázquez Duran por darme el apoyo necesario para estudiar una carrera, por los valores que me inculcan día con día, ellos han sido el impulso para querer salir adelante y lograr mis sueños. Hoy que concluyo mis estudios les dedico a ustedes este logro, como una meta más.

Gracias por ser quienes son y por creer en mí.

A el Mtro. Rogelio Moisés Sánchez Arrastio quien me apoyo en mi proceso de titulación por ser una gran persona y tenerme mucha paciencia.

A M. en C. José Luis Garza Rivera y Lic. Carlos Pineda Muñoz por sus sabias palabras, sus conocimientos rigurosos y precisos, que fueron fundamentales en mi proceso de titulación.

Gracias por su paciencia, por compartir sus conocimientos de manera profesional e invaluable, por su dedicación perseverancia y tolerancia.

En memoria de mi abuelo José Isabel Vazquez Hernández, que fue como un segundo padre para mí.

Índice

Índice de figuras

Capítulo 1. Evolución del Internet y conceptos generales

Evolución del Internet

Internet es la tecnología más decisiva de la era de la información del mismo modo que el motor eléctrico fue el vector de la transformación tecnológica durante la era industrial. Esta red global de redes informáticas, que actualmente operan sobre todo a través de plataformas de comunicaciones inalámbricas, nos proporciona la ubicación de una comunicación multimodal e interactiva en cualquier momento y libre de limites espaciales. (Castells, M, 2013)

La tecnología de internet en realidad no es algo nuevo a finales de los años 50 e inicio de los años 60, se cruzaban dos caminos investigación independientes, uno era el que eventualmente condujo a las redes de conmutación de paquetes de la internet actual, el otro fue la creación y crecimiento de la Agencia de Proyectos de investigación Avanzada de los EE. UU.(ARPA), la institución que fundo e implemento estas tecnologías.

Eventualmente se unieron a mediados de los años 60, creando una nueva red de ordenadores llamada ARPANET.

Primeramente, surge la necesidad de la comunicación entre una gran cantidad de computadoras. No obstante, la tecnología existente de conmutación de circuitos era inadecuada para soportar la comunicación entre varias fuentes de datos. Surgió entonces, el concepto de reparto o admisión de recursos en el contexto de tiempo compartido de la capacidad de computación. Este tiempo compartido se basó en reconocer que los usuarios generan demandas en ráfagas y, por lo tanto, gran parte del valioso recurso computacional se desperdicia cuando la computadora está dedicada a un solo usuario. Esta ineficiencia se puede superar compartiendo los recursos durante los intervalos en que un usuario está inactivo. Los principios y ventajas del tiempo compartido de los recursos fue clave para la

realización de enlaces de comunicación eficientes en redes de datos, desarrollándose el concepto y la tecnología de la conmutación de paquetes. *(A. Medina, s.f.)*

Surge la necesidad de una red para conectar a los investigadores de ARPA a las pocas computadoras grandes y costosas para investigación diseminadas en los EE. UU. Esto les permitiría compartir, unos con otros, hardware, software y aplicaciones en una forma eficiente y efectiva.

Después de un período corto de evaluación que siguió a la implementación inicial de los cuatro primeros nodos, siguió la adición a la ARPANET de una sucesión continua de redes y procesadores de mensajes (IMP- *Interface Message Processor*). A inicios de 1970 la red contenía 10 IMPs, y para marzo de 1971 ya habla crecido a 15 IMPs. Para finales de 1971 se anunció la nueva capacidad de la red: el correo electrónico (e-mail), y en julio de 1972 se adicionó una utilidad de administración al correo que permitía crear listas, seleccionar los correos, archivar, reenviar, y responder los mensajes de correo directamente a los remitentes. El e-mail resultó "*the killer application*", es decir, la aplicación que cambió para siempre la Internet e hizo que su crecimiento fuera exponencial y su uso se propagara rápidamente. En menos de un año, el correo correspondía a la mayoría del tráfico, lo que hacía evidente la capacidad de la red para extender la comunicación entre personas.

Durante los años 1970 ARPANET había crecido hasta 15 nodos con 23 ordenadores *hosts* (centrales). Un año más tarde Ray Tomlinson, escribe el software básico de envío-recepción de mensajes de correo electrónico, impulsado por la necesidad que tenían los desarrolladores de ARPANET de un mecanismo sencillo de coordinación. Poco más tarde amplía su valor añadido con un primer programa de correo electrónico para relacionar, leer selectivamente, almacenar, reenviar y responder a mensajes. *(E.C.O. UMBERTO, 2015)*

La reacción de los fabricantes de computadoras a este fenómeno del ARPANET fue la creación de arquitecturas de redes propietarias basadas en sus propias marcas de computadoras, como la SNA de IBM y le DECnet de DEC. Mientras tanto, las compañías

telefónicas continuaban ignorando el fenómeno, pero la red abierta que era ARPANET seguía creciendo con fuerza.

Para los años 1980 se da un acuerdo sin precedentes entre CSNET (Computer Science Network, Red de Ciencias de la Computación) y NSF (National Science Foundation, Fundación Nacional de Ciencia), y DARPA (*Defense Advanced Research Projects Agency*, Agencia de Proyectos de Investigación Avanzados de Defensa), que permite que el tráfico de CSNET compartiera la infraestructura de ARPANET, en consecuencia, y de forma similar, la NFS (Network File System, Sistema de archivos de red), promociona sus redes regionales de NSFNET(National Science Foundation's Network, Red de la Fundación Nacional de Ciencias), inicialmente académicas, para buscar clientes comerciales, expandiendo sus servicios y explotando las economías de escala resultantes para reducir los costos de suscripción para todos.

En diciembre de 1989 se implementaron los primeros cuatro nodos de ARPANET que usaban la pila de protocolos NCP (*Network Control Program*- Programa de Control de Redes), un protocolo de máquina a máquina.

ARPANET fue creada en un principio conectando cuatro minicomputadoras localizadas cada una en universidades separadas, las universidades de California en Santa Bárbara California, en los Ángeles, el SRI en Stanford y la Universidad de Utah. La red original se suponía que tendría una velocidad de solamente 2400 bits por segundo (bis), aunque ya se disponía de tecnología para aumentar la velocidad de la línea a 50 kb/s (miles de bits por segundo).

Durante los años 1990, la Internet continuó su crecimiento y avance gracias a la gran cantidad de innovaciones, incluyendo aquellas de carácter social y comercial que permitieron la inyección de dinero e investigación en esta increíble tecnología.

La Internet había pasado de ser una herramienta usada principalmente por investigadores y conocedores de tecnología a ser un utensilio de casa que se puede encontrar en casi en cualquier hogar y que resultó una explosión económica.

A principios de los 1990, ya existían unos 300,000 computadoras en la red, y para finales de la década, el número estaría en el orden de los cientos de millones. Esta red de redes ha transformado el mundo para siempre. Además de los cambios tecnológicos, también ha cambiado la sociedad y tiene un impacto en cada uno de los aspectos de nuestras vidas.

Las aplicaciones e innovaciones que han alimentado el crecimiento de la red a través de los años. Entre las más significativas están:

La *World Wide Web* (WWW), creada en 1989 por Sir Tim Bemers-Lee, Sir Sam Walker y Robert Caillau, es un sistema de documentos de hipertexto vinculados entre sí en Internet accesibles a través de navegadores. Esta usa enlaces de hipertexto, los cuales son códigos que enlazan un sitio con otro, y que permiten acceder a información con un simple clic del ratón, moviéndonos entre computadoras que estén conectadas a la red. *(Hugo, D. 2015)*

El correo electrónico, que ha hecho de la Internet algo irresistible como tecnología de comunicación para empresas e individuos, ya que no solo es rápido, fácil y muy efectivo, sino que es gratis, permitiendo la comunicación en cualquier lugar y en cualquier momento.

Así que, cada día la Internet se expande por las actividades sociales, políticas y económicas de las personas alrededor del mundo, y su impacto crece exponencialmente. En este nuevo mundo no hay separación geográfica y no hay fronteras, y todas las personas están animadas a participar y contribuir aprovechando sus experiencias y recursos. En el ciberespacio las acciones y reacciones son esencialmente instantáneas, por esto la Internet es tan gratificante y atractiva, y ha impactado nuestra sociedad en casi todas las áreas del quehacer humano. Sin embargo, es necesario considerar los aspectos negativos que puede tener la Internet. Por ejemplo, los niños y jóvenes pueden tener acceso a áreas o información que no es adecuada y puede resultar peligrosa. En el área de negocios, la seguridad es una gran preocupación y es de suma importancia; hay menos oportunidad de reunirse con personas e intercambiar ideas presencialmente por lo que el trabajo en grupo se hace más difícil.

Basado en el crecimiento de las redes y los problemas que traen estas se decide crear herramientas de monitoreo tomando como clave la proactividad, es decir, anticiparse a una degradación final sobre los recursos de información.

Entre los retos que por años han tenido que enfrentar los administradores de TI, está el presentar la información de su operación de manera tal que los ejecutivos de la organización dispongan de elementos suficientes para reconocer y fomentar la importancia de la tecnología como un componente habilitador del negocio.

Han sido muchos los esfuerzos para hacer que la industria acuerde un estándar universal, primeramente, a través de protocolos como la propuesta del ITU: CMIP (*Common Management Information Protocol*), o las del IETF SNMP (*Simple Network Management Protocol*) y RMON, o bien a través de plataformas donde converge la información de todos los recursos de TI, como HP Openview, IBM Tivoli, Sun Solstice o CA Infrastructure Management, por mencionar algunos.

La evolución de las herramientas de monitoreo también se ha ido alimentando mediante la llegada de protocolos más avanzados de visualización de tráfico como NetFlow, Jflow, Cflow, sflow, IPFIX o Netstream; el propósito hoy es tener una perspectiva global del "todo" para categorizar adecuadamente los eventos que afectan el desempeño de un servicio o del proceso de negocio involucrado.

El siguiente esquema demuestra cómo se ha venido dando la evolución de las herramientas de monitoreo:

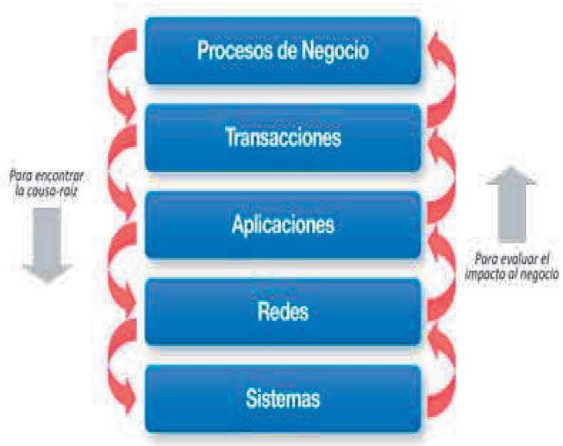


Figura 1 Evolución De Herramientas de Monitoreo

La clave siempre ha estado en la proactividad, es decir, anticiparse a una degradación en la experiencia del usuario final sobre los recursos de información; independientemente de que los indicadores sean técnicos o enfocados a procesos de negocio. Para tener la posibilidad de "afinar" en vez de "arreglar" es fundamental que las herramientas de monitoreo se acoplen adecuadamente a la infraestructura que estarán supervisando. *(Ciss, C.R.S, 2019)*

Una red de computadoras es conocida como una red de ordenadores, se refiere a un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos electrónicos, ondas electromagnéticas o cualquier otro medio para el transporte de datos con la finalidad de compartir información y recursos. *(Tacoa, K. 2018).*

Las redes se clasifican según de la siguiente manera:

- Red de área personal o *PAN (Personal Area Network)* es una red de computadoras usadas para la comunicación entre los dispositivos de la computadora cerca de una persona.
- Red de área local o LAN (*Local Area Network*) es una red que se limita a un área especial relativamente pequeña tal como un cuarto, un solo edificio, una nave, o un avión. Las redes de área local a veces se llaman una sola red de localización.
- Una red de área de campus o CAN (*Campus Area Network*) es una red de computadoras que conecta redes de área local a través de un área geográfica limitada, como un campus universitario, o una base militar.
- Una red de área metropolitana (*Metropolitan Area Network* o MAN, en inglés) es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa.
- Las redes de área amplia (*Wide Area Network*, WAN) son redes informáticas que se extienden sobre un área geográfica extensa.

Una red de computadoras consta tanto de hardware como de software. En el hardware se incluyen: estaciones de trabajo, servidores, tarjeta de interfaz de red, cableado y equipo de conectividad. En el software se encuentra el sistema operativo de red (*Network Operating System*, NOS).

- Estaciones de trabajo

Cada computadora conectada a la red conserva la capacidad de funcionar de manera independiente, realizando sus propios procesos. Asimismo, las computadoras se convierten en estaciones de trabajo en red con acceso a la información y recursos contenidos en el servidor de archivos de la misma. Una estación de trabajo no comparte sus propios recursos con otras computadoras.

- Servidores

Son aquellas computadoras capaces de compartir sus recursos con otras. Los recursos compartidos pueden incluir impresoras, unidades de disco, CD-ROM, directorios en disco duro e incluso archivos individuales.

- Tarjeta de Interfaz de Red

Para comunicarse con el resto de la red, cada computadora debe tener instalada una tarjeta de interfaz de red (*Network Interface Card*, NIC). Se les llama también adaptadores de red o sólo tarjetas de red. En la mayoría de los casos, la tarjeta se adapta en la ranura de expansión de la computadora, aunque algunas son unidades externas que se conectan a ésta a través de un puerto serial o paralelo. *(Calameo, C. 2013)*

Por la tanto, para una red se ocupan herramientas de monitoreo, pero como base se tiene que conocer a que se refiere el término, este describe el uso de un sistema que

constantemente monitoriza (supervisa) una red de computadoras en busca de algún componente defectuoso, para después informar a los administradores de redes mediante un correo electrónico, mensajes de texto u otras alarmas. Un sistema de monitorización de red es el encargado de buscar problemas causados por la sobrecarga y/o fallas en los servidores, como también problemas de la infraestructura de red (u otros dispositivos).

Por ejemplo, para determinar el estatus de un servidor web un software de monitorización puede enviar, periódicamente, peticiones HTTP (Protocolo de Transferencia de Hipertexto) para obtener páginas; para un servidor de correo electrónico, enviar mensajes mediante SMTP (Protocolo de Transferencia de Correo Simple) para luego ser recuperados mediante IMAP (Protocolo de Acceso a Mensajes de Internet) o POP3 (Protocolo Post Office). Comúnmente, los datos evaluados son tiempo de respuesta y estadísticas tales como consistencia y fiabilidad han ganado popularidad. Las fallas de peticiones de estado, tales como que la conexión no pudo ser establecida, el tiempo de espera agotado, entre otros, usualmente produce una acción desde del sistema de monitorización. *(Colaboradores de Wikipedia, 2019)*

Para el uso de una herramienta de monitoreo se tendrán que conocer algunos conceptos generales, para el buen uso de algún sistema de monitoreo. A continuación, mencionamos algunos conceptos generales que creemos son los más relevantes.

Conceptos generales

Red de computadoras

En cualquier operación de redes con computadoras, hay tres presunciones subyacentes. Primero, una red debe tener miembros; segundo, los miembros deben estar conectados entre sí de alguna manera y tercero, todos los miembros de la red deben establecer claramente una comunicación con cada uno de los paquetes para obtener una comunicación efectiva. En el mundo de las redes de computadoras, las entidades conectadas de una red son llamadas computadoras u otros dispositivos (aunque muchas veces son llamados genéricamente nodos);
el enlace mediante el cual tiene lugar la comunicación se llama medio de la red.
Las reglas que gobiernan la manera en que los datos son intercambiados entre dispositivos se logran a través de un protocolo común de red.

Colectivamente, estos tres conceptos conducen a la siguiente definición formal de una red de computadoras:
“Una red de computadoras es una colección de computadoras y otros dispositivos (nodos) que usan un protocolo común de red para compartir recursos entre si a través de un medio de red”. (*Michael A. Gallo & William M. Hancock, 2003)*

Redes TCP/IP

Las redes IP fueron desarrolladas inicialmente por el Departamento de Defensa de los Estados Unidos como topología de red para sus comunicaciones. El protocolo IP es la base de una estructura de protocolos en formas de capas, en el que cada capa proporciona una serie de funcionalidades a la capa superior. Cuando se transmite información cada uno de los protocolos de la pila interpreta todas las cabeceras y datos del protocolo superior como si fueran datos y los envuelve con sus propias cabeceras e información de control.

El concepto original de esta estructura sigue proporcionando hoy día una infraestructura muy sólida para las comunicaciones en Internet. En el conjunto de protocolo IP existen cuatro componentes básicos, componentes a lo que se les denomina comúnmente conjunto de protocolos TCP/IP. *(Andrew Hopper, Steven Temple, Robin Williamson, 1989).*

Protocolo de Internet (IP)

El protocolo de Internet aparece descrito en el documento RFC-791. Se trata de un protocolo no orientado a conexión, lo que significa que cada paquete se coloca en la red y se envía a su destino de forma independiente. No hay ninguna garantía de que los paquetes lleguen a su destino, y en el caso de que así sea, tampoco es seguro que lleguen en el orden correcto. Los paquetes IP pueden fragmentarse cuando atraviesan redes con un tamaño de trama pequeño. Esta función es necesaria para asegurar el funcionamiento de la red, sin embargo, esta fragmentación también puede utilizarse para realizar un ataque. Los fragmentos pueden utilizarse para intentar traspasar el firewall. Esto se haría enviando un primer fragmento que contuviera algo con la apariencia de una cabecera TCP inocente. El segundo fragmento se genera de tal forma que superponga con el primer fragmento y con la cabecera TCP. De esta forma se podría generar un ataque que estaría permitido por el firewall. *(Andrew Hopper, Steven Temple, Robin Williamson, 1989).*

Protocolo de control de transmisión (TCP)

TCP garantiza el envío de los paquetes, así como su correcto orden de llegada. Esto se consigue mediante unos números de secuencia junto con un sistema de acuses de recibo. Igual que el protocolo IP, utilizara las direcciones IP para enviar los paquetes a su correcto destino, TCP utiliza los números de puertos para garantizar la transmisión completa en el orden correcto y para identificar al proceso emisor del sistema origen de ese paquete.

La cabecera TCP proporciona un mecanismo que identifica el tipo de paquete TCP que está siendo enviado. Estos tipos se definen con los Bits de control. *(Andrew Hopper, Steven Temple, Robin Williamson, 1989).*

Comunicación entre computadoras.

Se refiere a la transmisión electrónica de datos de un sistema a otro; ella describe la manera en que las computadoras intercambian información entre sí. Una denominación común que da a entender un significado similar es; comunicación de datos. Aunque se usa de manera intercambiable, algunas personas restringen el termino datos para incluir solo hechos básicos y no realizados, y usan el termino información para dar a entender la organización de esos hechos en forma significativa para los humanos. (*Michael A. Gallo & William M. Hancock, 2003)*

Ruta

Es la forma de referenciar un archivo informático o directorio en un sistema de archivos de un sistema operativo determinado.

Una ruta señala la localización exacta de un archivo o directorio mediante una cadena de caracteres concreta. Esta puede ser de diversas formas dependiendo del sistema operativo y del sistema de archivos en cuestión. En líneas generales se compondrá de los nombres de los directorios que conforman el camino hasta el archivo o directorio a lo largo del árbol de directorios, y finalmente estará el nombre del archivo o directorio que se quiere referenciar. *(Andrew Hopper, Steven Temple, Robin Williamson, 1989).*

Infraestructura

Una infraestructura de red se refiere a todos aquellos elementos básicos e imprescindibles para cualquier institución u organización pública o privada que precisa todos o algunos de los servicios de telecomunicación. *(Andrew Hopper, Steven Temple, Robin Williamson, 1989).*

Monitoreo

Es un proceso que recolecta, analiza y utiliza la información para realizar un seguimiento al proceso de transmitir un paquete en pos de la consecuencia de sus objetivos, y para guiar las decisiones de gestión. El monitoreo generalmente se dirige a los procesos en los que respecta a cómo, cuándo y donde tienen lugar las actividades, quien las ejecuta y a cuantas personas o entidades beneficia. *(Richard Bejtlich, José Rafael García-Bermejo Giner, 2005).*

Análisis de riesgo

Para entender la amenaza a una compañía, tenemos que estimar cuando costaría la perdida de bienes. Este concepto se llama análisis de riesgos y puede ser muy complejo en grandes compañías que controlan muchos bienes. En la mayoría de los casos, al efectuar algunos cálculos simples sobre el costo de reemplazar, actualizar, reparar o administrar una situación de amenaza, se obtendrán algunos números sorprendentes. Se debería de comparar el costo de administrar una situación de amenaza con el precio de defender la situación si se dispone de un software sobre análisis de riesgo especialmente diseñado como ayuda en esta tarea. *(David Terán, 2014).*

Seguridad de una red.

La seguridad de una red se define como el resguardo apropiado de todos los componentes asociados a la red, incluidos datos, medios e infraestructura. Un enfoque pleno sobre la seguridad de una red implica tres elementos esenciales: una estimación precisa de las amenazas, el uso de las mejores herramientas de codificación disponibles y despliegue de productos efectivos de control de acceso a la red (por ejemplo, firewalls). Tal vez, lo más importante es que la seguridad en una red solo puede lograrse garantizando que todos los recursos de la red se usen de acuerdo con una política corporativa prescrita y únicamente por personal autorizado.

En vista de los ataques en la actividad por hackers y la proliferación de virus, la mayoría de la gente piensa que la seguridad de las redes es uno de los asuntos más importantes en el actual comercio electrónico. Toda organización requiere, pero pocas tienen una buena idea de cómo lograrlo. Hay muchas maneras de lograr niveles variables de seguridad, pero esos métodos pueden ser extremadamente caros o pueden no proteger completamente a los usuarios de muchos azares que emergen diariamente.

Una implementación apropiada de la seguridad en redes no es virtual ni barata, y requiere experiencia que abarque la mayoría de las áreas de la ciencia de redes.

Los entusiastas del movimiento *open source* presumen que sus programas son más seguros. Los críticos de este movimiento afirman que produce software más inseguro. *(Hatch, B. - Lee, J. - Kurtz, G. - Montaño, G.C, 2001).*

Conmutación

La conmutación implica el proceso de enlazar una fuente transmisora a un destino apropiado. Dos estrategias básicas de conmutación usadas en tecnología de redes son las conmutaciones de circuitos y conmutación de paquetes. Las redes basadas en la primera se

llaman redes de circuitos conmutados y aquellas basadas en la última se llama redes de paquetes conmutados. *(Michael A. Gallo & William M. Hancock, 2003).*

Conmutación de circuitos

En una red con conmutación de circuitos, un circuito físico dedicado debe establecerse entre los nodos fuentes y de destino antes que ocurra cualquier transmisión de datos. Además, este circuito debe permanecer en su lugar durante la transmisión. El sistema telefónico público, conocido formalmente como red telefónica publica conmutada (PSTN, por sus iniciales en inglés), es un buen ejemplo de una red con conmutación de circuitos. Cuando marcamos un número telefónico, un conmutador que reside en la oficina central de la compañía telefónica establece una conexión lógica a un conjunto de alambres con base en el número que marcamos. Este conjunto de alambres se conectará a una central que contiene otro conmutador. Finalmente se establece un circuito que conecte los teléfonos de quien llama con el receptor. *(Michael A. Gallo & William M. Hancock, 2003).*

Conmutación de paquetes

Es una red con paquetes conmutados, en vez de usarse un circuito físico dedicado para cada comunicación nodo a nodo, los nodos comparten un canal de comunicación por medio de un circuito virtual. Un circuito virtual es una conexión no dedicada, directa del nodo fuente al nodo destino. Un circuito virtual es creado multiplexando un enlace físico de manera que el enlace físico pueda ser compartido por programas múltiples de red o transmisión de datos. Este concepto es sumamente valioso para proporcionar comunicaciones de bajo costo ya que resulta muy caro proporcionar enlaces dedicados para cada transmisión de datos, como ocurre en las redes con circuitos conmutados.

En una red conmutada de paquetes, los mensajes son subdivididos en mensajes más pequeños, llamados paquetes, que pueden contener solo unos cuantos cientos de bytes de

datos, acompañados por información direccional y números de secuencia. Un paquete representa la unidad de datos más pequeña que puede ser transferida a través de una red dada.

Los paquetes son enviados al nodo de destino uno a la vez, en cualquier tiempo, y no necesariamente es un orden especifico. El *hardware* de la red entrega los paquetes a través del circuito virtual al nodo destino especificando, que es responsable reensamblarlos en el orden correcto. A diferencia de las redes de circuitos conmutados, donde los enlaces dedicados se establecen *a priori*, cada paquete en una red de paquetes conmutados debe llevar la dirección del nodo de destino. En una red de circuito conmutado solo el primer mensaje de datos lleva la dirección destino, que es necesaria para establecer inicialmente el enlace. La mayoría de las redes de comunicaciones de datos son de paquetes conmutados. *(Michael A. Gallo & William M. Hancock, 2003).*

MAC

Las LAN emplean una topología de difusión, esto es que los nodos de una LAN comparten un solo canal de comunicaciones y todos deben contender por el mismo medio para transmitir datos. Esto es semejante a un grupo grande de personal militar compartiendo el único teléfono en funcionamiento en la base durante su primera semana de entrenamiento básico; puede resultar en una larga espera cuando todos quieren usar el aparato. Debido al caos potencial asociado con tal contenido, las LAN deben emplear protocolos que definen la manera en que los nodos comparten el único medio físico de transmisión. El nombre lo dice todo Medios, Acceso, Control. Dos amplias categorías de métodos de acceso son las más adecuadas para las LAN: acceso aleatorio (llamado a veces estocástico o estadístico) y de paso token (o determinístico). *(Andrew Hopper, Steven Temple, Robin Williamson, 1989).*

Documentación

Un aspecto por considerar acerca de la estimación de amenazas en la segunda de redes es la documentación y las actualizaciones. Todos los asuntos previos no sirven de nada si la documentación no sigue el trabajo. El legado debe ser registrado para otros y actualizado conforme las amenazas cambian. Este proceso puede tomar una gran cantidad de tiempo y esfuerzo, pero es una parte esencial de cualquier plan bien pensado respecto a la administración de amenazas. *(Andrew Hopper, Steven Temple, Robin Williamson, 1989).*

Objetivo del trabajo

- Implementar un sistema de monitoreo de redes de comunicaciones para analizar las características de supervisión que proporciona en la gestión de la infraestructura.

Hipótesis

- Implementar un sistema de monitoreo de redes de comunicación facilita la supervisión de la infraestructura de red.

Capítulo 2. Sistemas de monitoreo

La detección oportuna de fallas y el monitoreo de los elementos que conforman una red de computadoras son actividades de gran relevancia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de contar con un esquema capaz de notificarnos las fallas en la red y de mostrarnos su comportamiento mediante el análisis y recolección de tráfico. *(David Terán, 2014).*

El monitoreo de red es una actividad que comúnmente desarrollan los administradores de redes, debido a que permite observar el comportamiento de la red en tiempo real. Específicamente:

- Prevención de incidencias y detección de problemas.
- Notificación de posibles problemas.
- Ahorro de costos y tiempo.
- Mejorar la satisfacción en atención al cliente.

Para conseguir los puntos ya mencionados, lo primero es contar con un sistema de monitorización que esté centrado en los procesos, la memoria, el almacenamiento y las conexiones red.

A continuación, analizaremos algunos sistemas de monitorización:

Nagios

Es un sistema de código abierto para la monitorización de redes que vigila los equipos (*hardware*) y servicios (*software*) que se especifiquen, alertando cuando su comportamiento no sea el esperado. Ente sus características principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP), la monitorización de los recursos de sistemas de hardware, la independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugin.

Se trata de un software que proporciona versatilidad para consultar parámetros de interés en un sistema, genera alertas que pueden ser recibidas por los responsables correspondientes, mediante (entre otros medios) correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador de red.

Llamado originalmente Netsaint, nombre que se debió cambiar por coincidencia con otra marca comercial, fue creado y es actualmente mantenido por Ethan Galstad, junto con un grupo de desarrolladores de software que mantienen también varios complementos.

Nagios fue originalmente diseñado para ser ejecutado en GNU/Linux, pero también se ejecuta bien en variantes de Unix.

Nagios esta licenciada bajo GNU General *Public License Version 2,* publicada por la *Free Software Foundation*.

Visualiza el estado de la reda través de una interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización de listado de notificaciones enviadas, historial de problemas y archivos de registros.

Nagios tiene una nomenclatura que explicaremos a continuación.

Host: Son los equipos a monitorear, normalmente para probar conectividad entre ambos puntos, se monitorea el estado por medio de ping ICMP, aunque pueden utilizarse otras formas como pulling SNMP, como un servicio de consulta remota como NRPE a un agente *dummy* que siempre responda OK y su estado siempre sea up si logra comunicación o un monitoreo pasivo que entregue un mensaje de OK en forma regular y si se supera dicho tiempo se alerte, entre otros. En los hosts las alarmas tienen sólo dos estados *UP* y *DOWN*.

Servicio: Asociado a cada Host existen los denominados servicios, aunque estos son básicamente consultas de distinto tipo para diferentes variables dentro del host, por ejemplo, si es un Switch, habrá servicios que monitorean mediante ping ICMP al equipo, existirá otro que haga consultas SNMP para saber el estado especifico de algun puerto o cuanto tráfico posee en ese instante o si es un servidor, cuanta capacidad disponible tiene los *filesystem*, si determinado puerto se encuentra abierto, si el servicio del servidor se encuentra en ejecución, etc... Estos pueden tener diversos estados que son CRITICAL, WARNING, OK y UNKNOWN.

Nomenclatura	
CRITICAL	Representa un estado de riesgo
WARNING	Representa un estado de alerta
OK	Representa un estado de éxito
UNKNOWN	Representa un estado desconocido

Figura 2 Estados de pruebas

Cada servicio o *Host* se suele monitorear cada 5 minutos, esto es determinado por configuración, si algún estado de monitoreo da un resultado que no es *UP* en el caso de un Host u *OK* en el caso de Servicio, el equipo volverá a consultar al minuto siguiente cambiando de estado al nuevo estado pero con el apodo de *SOFT*, hace consultas cada minuto y si el servicio o host no obtiene un resultado positivo cambia el estado a *HARD*,

pero si por el contrario encuentra que el estado varía mucho de estado este tomará un estado de *FLAPPING*.

Existen dos tipos fundamentales de monitoreo en Nagios:

Monitoreo Activo: Es la consulta desde el servidor de monitoreo a equipo remoto y esperar la respuesta de este con el resultado esperado, este es el tipo de monitoreo más común en Nagios y los ejemplos más clásicos son el ping ICMP, las consultas SNMP, consulta de puertos TCP abiertos, consultas WMI mientras que otrosson más propio de Nagios como el uso de los agentes NRPE, NSClient, etc.

Monitoreo Pasivo: Obtiene la información desde el equipo remoto sin una consulta previa de parte del servidor de monitoreo, los ejemplos en este sentido son los *traps SNMP*, el protocolo syslog, el protocolo Netflow (no soportado nativamente por Nagios XI) y el agente remoto NSCA. *(NORTH, A. 2017).*

Pandora FMS

Pandora proporciona herramientas para monitorizar rendimiento y disponibilidad, monitorizando los recursos claves a través de la infraestructura, para asegurarse de que todos los dispositivos están funcionando bajo los criterios de operación establecidos. Es posible ejecutar las pruebas de monitorización de forma remota, o hacerlos mediante un agente que recoge información local de la máquina donde está instalado.

SLA e informes.

Pandora FMS puede crear informes HTML, PDF y XML para cualquier elemento monitorizado. A estos informes se pueden añadir datos como: gráficas, SLAs, métricas, sumatorios, tablas, eventos, etc. Los informes se crean para un marco de tiempo configurable, que va desde una hora hasta seis meses. Los informes SLA de Pandora FMS, permiten definir qué grado de cumplimiento en porcentaje existe por cada parámetro, definiendo unos umbrales de operación válidos. Esto, permite definir métricas combinadas de varios valores para determinar el grado de cumplimiento de una serie de parámetros a lo largo de un rango de tiempo.

Control remoto de equipos

Mediante la integración con eHorus es posible controlar equipos remotamente, tanto por escritorio remoto, como por terminal (Linux, Mac y Windows). También permite copia de archivos bidireccional, gestión de procesos y de servicios. Y todo ello, integrado en la consola de Pandora FMS.

Monitorización descentralizada.

- Se puede implementar mediante agentes proxy o Satélite server. Le permite realizar monitorización descentralizada de forma remota para pruebas WMI, ICMP, SNMP v1 y 2 así como ejecución de chequeos personalizados.
- Integra un mecanismo de descubrimiento si detecta un dispositivo SNMP/WMI en el barrido de la red.
- Miles de chequeos por segundo. Funciona en Windows y Linux.

- Envía la información de vuelta al Dataserver y no requiere una Base de Datos ni conexión permanente con Pandora FMS.

Consola visual personalizable.

Pandora FMS permite a cada usuario definir su vista de monitorización personalizada. Esta es una vista gráfica personalizada, basada en una representación en el espacio, con items seleccionados, estatus representado, datos, gráficas u otros estatus de la consola visual, escalando siempre el evento crítico.

Gestión de errores y eventos.

El sistema de eventos de Pandora FMS mantiene un *log* de todo lo que ha sucedido: cuando un servicio o un host se cae o cuando se recupera, cuando se dispara una alerta, cuando se descubren nuevos hosts en la red, etc.

Es posible buscar eventos, filtrándolos por grupo, tipo, severidad o estatus del evento. Todo esto se hace desde la consola Web. Los eventos se pueden exportar a un fichero CSV o estar asociados a lectores de alimentación gracias a su RSS.

La operativa de eventos permite validarlo o marcarlo como “en proceso” por un operador concreto, de forma que quede patente que se está trabajando en él dejando un rastro de comentarios. Además, los eventos llevan asociado un conjunto de tags o categorías que permiten búsquedas y agrupaciones semánticas.

Alta disponibilidad.

Pandora FMS tiene una estructura basada en servidores múltiples (Data Server, Plugin Server, Network Server, …), una consola Web y una Base de Datos. Tiene redundancia sobre todos sus sistemas. Se puede crear cualquier cantidad de servidores o consolas, así como un cluster MySQL para la Base de Datos. Esto, está incluido en las características de la versión OpenSource. Los agentes también disponen de mecanismos para poder enviar a varios servidores, por si falla uno de ellos.

Detección de topología de red y autodescubrimiento.

Pandora FMS es capaz de reconocer y detectar periódicamente nuevos sistemas no monitorizados, detectando su sistema operativo y su relación con otros nodos de la red, bien a nivel de red o a nivel de enlace (mediante exploración de tablas ARP vía SNMP). Esto significa que Pandora FMS puede explorar una red de 1,000 nodos y dibujar su red conectando las interfaces de sus *routers* con las de sus *switches*, en menos de una hora. *(Team, P.F. 2019).*

Op5 Monitor

Op5 Monitor es un producto de software para monitorizacion de redes basado en el producto de código abierto Nagios, promovido y desarrollado por op5 AB.

Op5 Monitor muestra el estado, situación y rendimiento de la red y las TI que se están monitorizando y tiene integrado el registro de los logs del sistema, op5 Logger. La empresa comercializa el software descargable que controla, visualiza y soluciona los problemas de TI recogiendo la información tanto del Hardware como del software, sea virtual y/o en los servicios basados en la nube.

Características

- Monitoriza y gestiona la red.
- Fácil solución de problemas de sus redes.
- Seguimiento distribuido.
- Soporte para balanceo de carga y redundancia.
- Monitoreo extensible.
- Seguimiento de SLA y reportes.
- Configuración basada en web.
- Gráficos de rendimiento.
- Mapea tu red.
- Mapa geográfico y mapas de red.
- Trampa de trampas y motor de reglas.
- Monitorización SNMP y Syslog.
- Soporte de servicios Easy Cloud.
- API está disponible.
- GUI fácil de usar.
- Resumen táctico con widgets.

- Autenticación LDAP.

Con solo una mirada rápida, los usuarios pueden obtener perspectivas más profundas y de gran acción a través de los gráficos y mapas fáciles de comprender del Monitor OP5. Los filtros avanzados se pueden activar según las reglas del usuario. El monitor OP5 es fácil de escalar en entornos distribuidos y las posibilidades de automatización son infinitas. Además de todo eso, el software tiene una API muy amigable, que permite a los desarrolladores realizar cambios en la plataforma para satisfacer sus necesidades.

OP5 Monitor es un software de monitoreo de TI que le brinda control sobre su infraestructura de TI. Con un entorno unificado, puede supervisar fácilmente aplicaciones, redes, servidores y almacenamiento. Funciona completamente bien, independientemente de la ubicación y funciona sin problemas si su infraestructura de TI se implementa en las instalaciones, híbrida o en una nube privada / pública.

Sus capacidades de gestión de servicios empresariales mejoran su visibilidad en sus infraestructuras de TI y ofrecen información altamente procesable sobre su red y su relación con sus servicios comerciales, permitiéndole tomar decisiones mejores e informadas.

Los informes potentes y personalizados hacen que sea fácil obtener y comunicar información precisa y relevante a las personas adecuadas. OP5 Monitor puede generar una gran cantidad de informes que se ajustan a sus necesidades: informes de SLA, informes de disponibilidad e informes de alertas, por mencionar algunos. Y puede acceder a estos y otros informes útiles directamente desde el panel de control.

Se elimina la necesidad de solicitar información de cada dispositivo. OP5 Monitor puede leer, procesar y crear alertas desde las trampas SNMP. Con OP5 Monitor, el dispositivo envía automáticamente alertas al administrador de eventos que afectan o afectan la salud de su hardware y software.

Al ser una plataforma de código abierto, OP5 Monitor se desarrolla y mejora continuamente por. Esto es posible a través de una comunicación abierta dentro y entre la comunidad OP5

y los usuarios. Se recomienda la transparencia, especialmente en áreas como informes de errores, solicitudes de funciones y asesoramiento dedicado de productos. *(Colaboradores de Wikipedia, 2019).*

Network Miner

Es una herramienta de análisis forense de red (NFAT) de código abierto para Windows (pero también funciona en Linux / Mac OS X / FreeBSD). NetworkMiner se puede utilizar como herramienta de captura de paquetes / olfateador de red pasiva para detectar sistemas operativos, sesiones, nombres de host, puertos abiertos, etc. sin poner tráfico en la red. NetworkMiner también puede analizar archivos PCAP para análisis fuera de línea y regenerar / volver a ensamblar archivos transmitidos y certificados de archivos PCAP.

NetworkMiner facilita el análisis de tráfico de red (NTA) avanzado al proporcionar artefactos extraídos en una interfaz de usuario intuitiva. La forma en que se presentan los datos no solo simplifica el análisis, sino que también ahorra tiempo para el analista o el investigador forense.

Desde el primer lanzamiento en 2007, se ha convertido en una herramienta popular entre los equipos de respuesta a incidentes, así como en la aplicación de la ley y es utilizado hoy por empresas y organizaciones de todo el mundo.

NetworkMiner puede extraer archivos, correos electrónicos y certificados transferidos a través de la red al analizar un archivo PCAP o al rastrear el tráfico directamente desde la red, muestra los archivos extraídos del tráfico de red husmeando en el disco.

Otra característica muy útil es que el usuario puede buscar datos olfateados o almacenados para palabras clave, permite al usuario insertar cadenas arbitrarias o patrones de bytes que se deben buscar con la funcionalidad de búsqueda de palabras clave.

NetworkMiner Professional viene instalado en una unidad flash USB especialmente diseñada. Puede ejecutar NetworkMiner directamente desde la unidad flash USB ya que NetworkMiner es una aplicación portátil que no requiere ninguna instalación.

Es un software forense de red escrito en C # utilizando Microsoft .NET Framework. El corazón del software NetworkMiner es el código para analizar varios protocolos de red, que está escrito en código C # 100 por cien. Los protocolos implementados en NetworkMiner incluyen:

- DHCP
- DNS
- FTP
- HTTP
- IRC
- IEC 60870-5-104
- IMAP
- Modbus ICP
- Servicio de nombres de NetBios
- Servicio de datagrama de NetBios
- Servicio de sesión NetBios
- OpenFlow
- Oscar
- Transferencia de archivos Oscar
- POP3
- RTP

- SMTP
- SNMP
- Calcetines
- SSH
- SSL
- Syslog
- Flujo de datos tabulares
- TFTP
- TPKT
- UPnP
- sorbo
- Protocolo del servidor Spotify
- VXLAN [11].

(Sied, G. 2014).

Capítulo 3 Icinga web 2

Una curiosidad de la aplicación es su nombre, “Icinga” proviene del zulú y significa “el que busca” o “el que examina”.

Icinga es un sistema de monitoreo para redes, servidores y aplicaciones, de forma segura y confiable, lo que nos permite mantenernos al tanto de los problemas de nuestra infraestructura.

Es un sistema *Open source* impulsado por la Fundación Icinga, derivado de Nagios (uno de los sistemas de monitoreo más usado) del cual utiliza el *Nagios Remote Plugin Executor* (NRPE).

Icinga Web 2 es un marco de PHP para aplicaciones web que viene en un diseño limpio y reducido. Es rápido, sensible, accesible y fácilmente extensible con módulos.

Notifica al usuario los errores, el restablecimiento y recopila la información para la creación de los informes. Escalable y extensible, Icinga puede monitorear grandes entornos complejos a través de su interfaz gráfica.

Permite tener un control detallado de la infraestructura de nuestra red. Nos permite obtener información sobre los servicios que se estén ejecutando en un servidor específico, así también como el estado de las particiones de los servidores.

Uno de los fuertes de esta aplicación es su alto grado de configuración, tanto de las evaluaciones que efectúa sobre los equipos como las acciones consecuentes de las respuestas de los mismos. Icinga permite la interacción con aplicaciones instaladas en el equipo. Esto significa a nivel funcional que no se limita a las funcionalidades provistas por defecto ni la dependencia de actualizaciones o *plugins* para ampliarlas.

Básicamente, supervisa el estado de los protocolos de red, como HTTP, FTP, SMTP, IMAP u otros servicios de red, recursos de host, sensores físicos, instalaciones de software, carga de CPU, memoria, espacio en disco y casi todos los dispositivos de red interconectados a través de ICMP o solicitudes de ping. Además, se puede configurar fácilmente para notificar a los administradores del sistema o de la red por correo, SMS, chat u otros tipos de alertas sobre la red, los sistemas, los servicios u otros cortes de red relacionados, y también puede generar gráficos sobre el tiempo de inactividad o el rendimiento de la red.

Características

- Monitorización de servicios de red (Ej: SMTP, POP3, HTTP, NTP, ping, …).
- Monitorización de componentes de red (*hosts, servers, switches, routers*, etcétera).
- Notificación visual del estado de los servicios.
- Alertas configurables (EMail, SMS, llamada telefónica, …).
- Dos interfaces web (Icinga Clasic UI e Icinga Web).
- Soporta características y plugins de Nagios, facilitando la migracióndesde Nagios.
- Soporta extensiones, desarrollos e integraciones gracias a una API.
- Cuenta con una nueva interfaz web basada en PHP.
- Tendrá como addons: PNP, NagVis, Grapher V2 y NagTrap.
- Nueva interfaz NDO con soporte para ser almacenado en ficheros o en base de datos permitiendo el acceso a esos datos desde la API con PHP o desde WebServices.
- ReportDesigner para realizar informes personalizados y se podrán configurar envíos automáticos de informes cada cierto tiempo.
- También se contemplan mejoras para grandes instalaciones. *(Blyx, T. 2009.)*

La instalación preferida para Icinga web 2 es usar repositorios de paquetes oficiales según sea el sistema operativo y la distribución de este ejecutando.

Requerimientos Icinga web 2

Instalación de requisitos

- Icinga 2 con la base de datos IDO (MySQL o PostgreSQL.
- Un servidor web, por ejemplo. Apache o Nginx.
- PHP versión > = 5.6.0.
- Se deben instalar los siguientes módulos PHP: cURL, gettext, intl, mbstring, OpenSSL y xml.
- Zona horaria predeterminada configurada para PHP en el archivo php.ini.
- Biblioteca PHP LDAP cuando se utiliza Active Directory o LDAP para la autenticación.
- MySQL o bibliotecas PHP PostgreSQL. *(Luna, D. 2017)*

Instalando Icinga Web 2 del paquete.

Lista de los repositorios de paquetes oficiales para instalar Icinga Web 2 para varios sistemas operativos.

Distribución

Debian

Ubuntu

RHEL/Centos

OpenSUSE

SLES

Gentoo

FreeBSD

ArchLinux

Alpine Linux

Configuración de repositorios de paquetes.

- Se debe agregar el repositorio Icinga a la configuración de administración de paquetes para instalar Icinga Web 2.

- Si ya configuró su sistema operativo para usar el repositorio Icinga para instalar Icinga 2, puede omitir este paso.

A continuación, hay una lista con ejemplos de varias distribuciones.

- Debian Stretch:

```
wget -O - http://packages.icinga.com/icinga.key | apt-key add -
echo 'deb http://packages.icinga.com/debian icinga-stretch main'
>/etc/apt/sources.list.d/icinga.list
apt-get update.
```

- Ubuntu Xenial:

```
wget -O - http://packages.icinga.com/icinga.key | apt-key add -
add-apt-repository 'deb http://packages.icinga.com/ubuntu icingab-
xenial main'
apt-get update.
```

- RHEL and CentOS 7:

```
yum install https://packages.icinga.com/epel/icinga-rpm-release-7-
latest.noarch.rpm
```

- Fedora 26:

```
dnf install https://packages.icinga.com/fedora/icinga-rpm-release-26-latest.noarch.rpm
```

- SLES 12:

```
zypper ar http://packages.icinga.com/SUSE/ICINGA-release.repo
zypper ref
```

- openSUSE:

```
zypper ar http://packages.icinga.com/openSUSE/ICINGA-release.repo
zypper ref
```

- Alpine Linux:

```
echo "http://dl-cdn.alpinelinux.org/alpine/edge/community" >> /etc/apk/repos
apk update
```

La última versión de Icinga Web 2 está en el repositorio /, que es la rama /dev.

- CentOS 7/6:

```
yum instalar epel-release
```

- RedHat 7:

```
yum instala https://dl.fedoraproject.org/pub/epel/epel-release-latest- 7.noarch.rpm
```

Si está utilizando RHEL, necesita habilitar el repositorio opcional para usar algunos contenidos de EPEL.

- RedHat:

```
subscription-manager repos --enable rhel-7-server-optional-rpms
# o
subscription-manager repos --enable rhel-6-server-optional-rpms
```

- CentOS:

```
yum install centos-release-scl
```

- RedHat:

```
subscription-manager repos --enable rhel-server-rhscl-7-rpms
# o
subscription-manager repos --enable rhel-server-rhscl-6-rpms
```

Instalación de Icinga Web 2

Puede instalar Icinga Web 2 utilizando el administrador de paquetes de su distribución para instalar el paquete icingaweb2. *(Daniel Luna and, 2018)*

A continuación, hay una lista con ejemplos de varias distribuciones. El paquete adicional icingacli es necesario para seguir los pasos en esta guía. El paquete adicional libapache2-mod-php es necesario en Ubuntu para que Icinga Web 2 funcione de manera inmediata.

- Debian:

```
apt-get install icingaweb2 icingacli
```

- Ubuntu:

```
apt-get install icingaweb2 libapache2-mod-php icingacli
```

- RHEL, CentOS and Fedora:

```
yum install icingaweb2 icingacli
```

Si tiene SELinux habilitado, también se requiere el paquete icingaweb2- selinux.
Para RHEL / CentOS

- SLES and openSUSE:

```
zypper install icingaweb2 icingacli
```

- Alpine Linux:

```
apk add icingaweb2
```

Instalando el servidor web

Dependiendo de su sistema operativo, es posible que tenga que instalar o configurar el servidor web. Usualmente solo requerimos PHP como dependencia fuerte.

Por lo general, construimos en Apache httpd como el servidor web predeterminado, pero también puede usar nginx.

- RedHat / CentOS / Fedora

  Asegúrese de instalar httpd, iniciarlo y habilitarlo en el arranque.

  ```
  yum instalar httpd


  systemctl start httpd. service
  systemctl habilitar httpd. service
  ```

Nota para EPEL 6 y 7: Consulte “Configuración de FPM”

Nota para Fedora> = 27:

¡Se tiene que elegir qué modo httpd PHP quieres usar!

Habilite `mod_php: \ Edit /etc/httpd/conf.modules.d/00-mpm.conf y habilite prefork en lugar de evento o inicie php-fpm: \ systemctl inicie php-fpm. service \ systemctl habilite`

SUSE SLE / openSUSE

Asegúrese de que el servidor web esté instalado y de que se carguen los módulos necesarios.

```
zypper install apache2

rewrite a2enmod
a2enmod php7

systemctl start apache2.service
systemctl habilitar apache2.service
```

- Debian / Ubuntu

  Su servidor web debe estar en funcionamiento después de la instalación de Icinga Web 2

Configurando FPM

Si está en CentOS / RedHat 6 o 7, o simplemente desea ejecutar Icinga Web2 con PHP-FPM en lugar del módulo Apache.

Operating System	**FPM configuration path**
RedHat 7 (with SCL)	/etc/opt/rh/rh-php71/php-fpm.d/
RedHat 6 (with SCL)	/etc/opt/rh/rh-php70/php-fpm.d/
Fedora	/etc/php-fpm.d/
Debian/Ubuntu	/etc/php*/*/fpm/pool.d/

El grupo predeterminado www debería ser suficiente para Icinga Web 2.

En RedHat necesita iniciar y habilitar el servicio FPM.

- RedHat / CentOS 7 (paquete SCL):

```
systemctl start rh-php71-php-fpm. service
systemctl habilita rh-php71-php-fpm. service
```

- RedHat / CentOS 6 (SCL package):

```
service rh-php70-php-fpm start
chkconfig rh-php70-php-fpm on
```

- Fedora:

```
systemctl start php-fpm. service
systemctl enable php-fpm. service
```

Todos los paquetes de módulos para PHP tienen este prefijo SCL, por lo que puede instalar un módulo de base de datos como este:

```
yum install rh-php71-php-mysqlnd
# o
yum install rh-php71-php-pgsql

# en el6
yum install rh-php70-php-mysqlnd
# o
yum install rh-php70-php-pgsql
```

En RedHat / CentOS 6 también necesita instalar mod_proxy_fcgi para httpd:

```
yum install mod_proxy_fcgi
```

Dependiendo de la instalación de su servidor web, podríamos haber instalado o actualizado el archivo de configuración para icingaweb2 con los valores predeterminados para FPM.

```
Comprobar: /etc/httpd/conf.d/icingaweb2.conf or
/etc/apache2/conf.d/icingaweb2.conf. And *.rpm* *.dpkg*
```

Archivos con actualizaciones.

Asegúrese de que la parte FilesMatch esté incluida para Apache> = 2.4. Para Apache <2.4 tiene que incluir el bloque LocationMatch.

Vea también el ejemplo de icingacli:

```
icingacli config servidor web apache
```

Actualización a FPM

Válido para:

RedHat / CentOS 6
RedHat / CentOS 7

También son posibles otras distribuciones si se prefiere, pero no se incluyen aquí.

Algunos trabajos de actualización deben realizarse manualmente, mientras que instalamos PHP FPM como dependencia, necesita iniciar el servicio y configurar algunas cosas.

La configuración de php.ini que ha sintonizado en el pasado debe migrarse a una instalación SCL de PHP.

Compruebe estos directorios:

```
/etc/php.ini
/etc/php.d/*.ini
```

Lo más importante para icingaweb2 es date. timezone.

La configuración de PHP se debe almacenar en:

```
RedHat / CentOS 7: /etc/opt/rh/rh-php71/php.d/
RedHat / CentOS 6: /etc/opt/rh/rh-php70/php.d/
```

Asegúrese de instalar los módulos de base de datos requeridos

- RedHat / CentOS 7:

```
yum instalar rh-php71-php-mysqlnd
# o
yum instalar rh-php71-php-pgsql
```

- RedHat / CentOS 6:

```
yum instalar rh-php70-php-mysqlnd
# o
yum instalar rh-php70-php-pgsql
```

Después de cualquier cambio relacionado con PHP, ahora necesita reiniciar FPM:

- RedHat / CentOS 7:

```
 ystemctl restart rh-php71-php-fpm.service
```

- RedHat / CentOS 6:

```
service rh-php70-php-fpm restart
```

Si no necesita mod_php para otras aplicaciones en el servidor, debe deshabilitarlo en Apache.

Desactivar PHP en Apache httpd:

```
cd /etc/httpd
cp conf.d/php.conf{,.bak}
: >conf.d/php.conf

# ONLY on el7!
cp conf.modules.d/10-php.conf{,.bak}
: >conf.modules.d/10-php.conf
```

```
systemctl restart httpd. service
# or on el6
service httpd restart
```

También puede desinstalar el paquete mod_php, o todos los paquetes relacionados con PHP que no sean SCL.

```
yum remove php
# or
yum remove php-common
```

Preparando la configuración web.

Puede configurar Icinga Web 2 rápida y fácilmente con el asistente de configuración de Icinga Web 2 que está disponible la primera vez que visita Icinga Web 2 en su navegador. Cuando utilice la configuración web, deberá autenticarse utilizando un token. *(Daniel Luna and, 2018)*

Para generar un token usa el icingacli: icingacli setup token créate

En caso de no recordar el token puede mostrarlo usando el: icingacli:

icingacli setup token show

Preparando la configuración web en Debian

En Debian, debe crear manualmente una base de datos y un usuario de base de datos antes de iniciar el asistente web. Esto se debe a las restricciones de seguridad local,

mientras que el asistente web no puede crear una base de datos / usuario a través de un socket de dominio unix local.

```
MariaDB [mysql]> CREATE DATABASE icingaweb2;

MariaDB [mysql]> GRANT ALL ON icingaweb2. * TO icingaweb2@localhost
IDENTIFIED BY '********';
```

También puede crear una cuenta administrativa separada con todos los privilegios en su lugar.

Nota: Esto solo es necesario si está utilizando una base de datos local como tipo de autenticación.

Iniciando la configuración web

Finalmente, visite Icinga Web 2 en su navegador ingresando url: `localhost/icingaweb2/setup` para acceder al asistente de configuración y completar la instalación.

Nota para Debian

Utilice la misma base de datos, usuario y detalles de contraseña creados anteriormente cuando se le solicite. El asistente de configuración detecta automáticamente los paquetes requeridos. En caso de que falte uno de ellos, por ej. un módulo PHP, instale el paquete, reinicie su servidor web y vuelva a cargar la página de configuración. Si tiene SELinux habilitado, asegúrese de tener instalado el paquete selinux para Icinga Web 2 o deshabilite SELinux.

Configuración

Visión general

Además de sus capacidades de configuración web, la configuración local se almacena en /etc/icingaweb2 de forma predeterminada (dependiendo de la configuración de su configuración). *(Daniel Luna and, 2018)*

Directoriode archivos	**Descripción**
config.ini	Configuración general (global, logging, temas, etc.)
resources.ini	Recursos globales (base de datos Icinga Web 2 para preferencias y autenticación, base de datos Icinga 2 IDO)
roles.ini	Funciones específicas del usuario (por ejemplo, administrators) y permisos
authentication.ini	Backends de autenticación (por ejemplo, base de datos)
enabledModules	Enlaces simbólicos a módulos habilitados
modules	Directorio para la configuración específica del módulo

Configuración general

Navegue en Configuración> Aplicación> General.

Esta configuración se almacena en el archivo config.ini en /etc/icingaweb2.

Configuración global

Opción	Descripción
show_stacktraces	Opcional. Ya sea para mostrar debtrac stacktraces. El valor predeterminado es 0.
Module_path	Opcional. Especifica los directorios donde se pueden instalar los módulos. Los directorios múltiples deben estar separados con dos puntos.
config_backend	Opcional. Seleccione el almacenamiento de preferencias del usuario. Se puede establecer en ini (predeterminado), db o none. Si se selecciona db, esto requiere el atributo config_resource.
config_resource	Opcional. Especifique un nombre de recurso definido. Solo se puede utilizar si config_backend se establece en db.

Ejemplo para almacenar las preferencias de usuario en el recurso de base de datos icingaweb_db:

```
[global]
 show_stacktraces = "0"
 config_backend = "db"
 config_resource = "icingaweb_db"
 module_path = "/ usr / share / icingaweb2 / modules"
```

Configuración de registro

Opción	Descripción
log	Opcional. Especifica el tipo de registro. Se puede establecer en syslog, file o none.
level	Opcional. Especifica el nivel de registro. Se puede configurar en ERROR, WARNING, INFORMATION o DEBUG.
file	Opcional. Especifica la ruta del archivo de registro si el log se establece en file.
application	Opcional. Especifica el nombre de la aplicación si el log se establece en syslog.
facility	Opcional. Especifica la función de syslog si log se establece en syslog. Se puede configurar para user, local0 para local7. Por defecto al user.

Ejemplo para un registro de depuración más detallado en un archivo:

```
[explotación florestal]
 log = "archivo"
 level = "DEBUG"
 file = "/usr/share/icingaweb2/log/icingaweb2.log"
```

Configuración del tema

Opción	Descripción
Default	Opcional. Elige el tema. Puede configurarse en Icinga, high-contrast, Winter o su propio tema instalado. Por defecto a Icinga. Tenga en cuenta que esta configuración distingue entre mayúsculas y minúsculas porque se refiere al nombre de archivo del tema.
Disabled	Opcional. Establecerlo en 1 si los usuarios no deberían poder cambiar su tema. El valor predeterminado es 0. *(Daniel Luna and, 2018)*

Ejemplo:

```
[temas]
disabled = "1"
tema = "Icinga"
```

Puesta en marcha de Icinga web 2

Antes de comenzar con la instalación, debemos asegurar que nuestro sistema operativo cumpla con los requerimientos del software para poder realizar la compilación e instalación de la aplicación.

Para la puesta en marcha vamos a ocupar el S.O Debian GNU/Linux, ya que posee un mayor rendimiento, es altamente personalizable y por lo general es más seguro. Debian sobrepasa a todas las otras distribuciones en lo bien integrados que están sus paquetes. Como todo el software lo empaqueta un grupo coherente, no solo puede encontrar todos los paquetes en un mismo sitio, sino que puede estar seguro de que se han eliminado todos los problemas al respecto de complejas dependencias; Debian Soporta un mayor número de arquitecturas CPU: Alpha, amd64, armel, hppa, i386, ia64, mips, mipsel, powerpc, s390, y sparc. También corre con los kernels GNU Hurd y FreeBSD, además de Linux, y con la utilidad debootstrap es difícil que encuentre un dispositivo que no pueda correr Debian.

El primer paso sería actualizar los repositorios del sistema (Debian) y los paquetes del software emitiendo el siguiente comando.

```
 # apt update
# apt install bash-completed
```

El segundo paso es configurar el nombre del host para el servidor. Esta operación se llevaba a cabo con el siguiente comando.

```
  # hostnamectl set-hostname
# hostnamectl
 Nombre de host estático: icinga2
 Nombre del icono: computer-vm
 Chasis: vm
 ID de máquina: 7f2b1120403449a3b27d2f40de770be2
 ID de inicio: 321481f419e94e6cb377ae804d9bab42
```

```
Virtualización: kvm
Sistema operativo: Debian GNU / Linux 9 (estiramiento)
Kernel: Linux 4.9.0-4-amd64
Arquitectura: x86-64
# cat / etc / hostname
icinga2
```

Finalmente, se necesita reiniciar el servidor para poder aplicar las actualizaciones del kernel y los cambios de nombre de host correctamente.

Instalar LAMP

- Servidor web Apache.
- MySQL.
- PHP y sus módulos.

Este procedimiento se lleva acabo utilizando los siguientes comandos.

```
# apt install apache2 libapache2-mod-php7.0 php7.0-xml php7.0-opcache php7.0- xml php7.0- mbstring php7.0-json php7.0-curl php7.0-ldap php7.0- cli php7.0-gd php7.0-intl php7.0- readline php7.0-pgsql

#apt install mariadb-server mariadb-client php7.0-mysql
```

Habilitar e iniciar el Servicio Apache – MySQL.

```
# systemctl enable apache2 mariadb
# systemctl start apache2 mariadb
# systemctl status apache2 mariadb
```

Crear una base de datos Mysql para icinga2

Inician sesion en la cosola de MySQL y se va a ejecura el siguiente comando para proteger la base de datos MariaDB y establecer una contraseña como root:

```
# mysql_secure_installation
```

Despues de realizar la configuracion se puede crear la base de datos que puede ser utilizada por la aplicación y un usuario y contraseña el cual pueda administrar esta base de datos.

```
# mysql -u root -p
```

Introducir la contraseña:

```
MariaDB [(none)]> create icingaweb2 database;

Query OK, 1 row affected (0.00 sec)

 MariaDB [(none)]> grants all privileges on icingaweb2. * An
'icinga_user' @ 'localhost' identified by 'password';

Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> creates the icinga_users database;

Query OK, 1 row affected (0.00 sec)


MariaDB [(none)]> grants all privileges on icinga_users. * An
'icinga_user' @ 'localhost' identified by 'password';

Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> download privileges;

Query OK, 0 rows affected (0.01 sec) [14]
```

La base de datos icingaweb2 se crea para la aplicación web icinga2.

Después de terminar la instalación de los requerimientos de la aplicación se puede continuar con la instalación de icingaweb2 utilizando el módulo IDO de mysql.

Se puede realizar a través de su administrador de paquetes apt usando la terminal.

 # apt install icinga2 icinga2-ido-mysql

En primer lugar, se le pregunta si desea configurar y habilitar icinga 2 para usar el módulo MySQL. Seleccione YES en el indicador y presione la tecla [enter] para continuar.

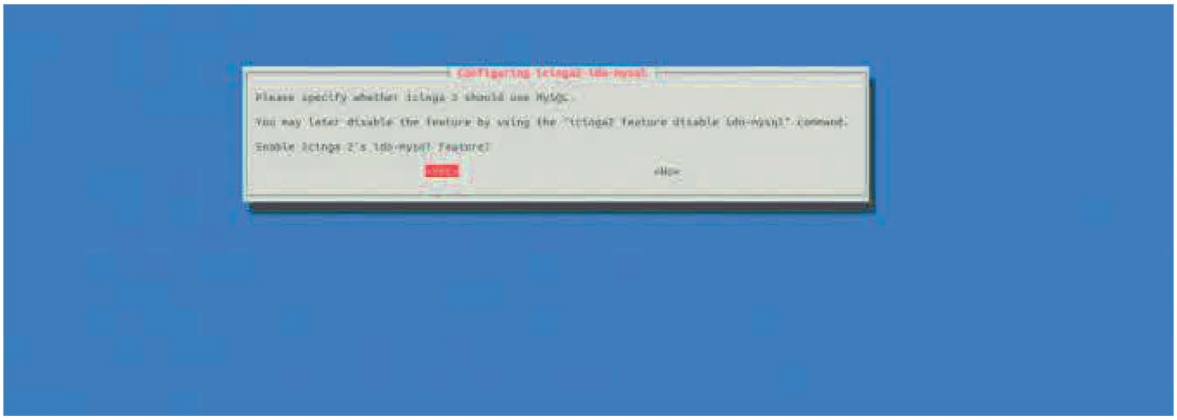


Figura 3 Configurar y Habilitar Icinga 2

En la siguiente solicitud se le pregunta si desea configurar la base de datos para icinga2-ido-mysql. Con la opción dbconfig-common. Se elige NO en el indicador y presione la tecla [enter] para finalizar la instalación de Icinga 2.

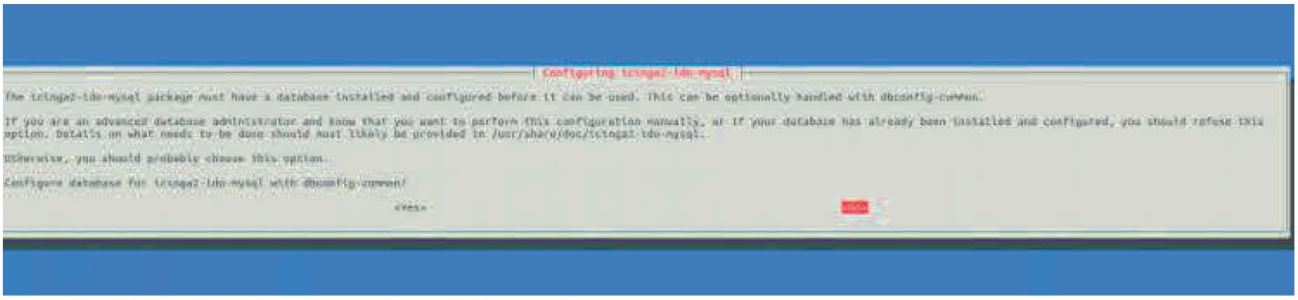


Figura 4 Configurar Base de Datos para Icinga2-ido-mysql

Después de terminar esta configuración, se habilita el módulo y crea nuestra base de datos, es necesario reiniciar el servicio Icinga2.

```
# systemctl start icinga2.service
```

```
# systemctl status icinga2.service
```

Asegurarse de que el archivo de configuración IDO MySQL este configurado correctamente con las credenciales de la base de datos.

```
# cat /etc/icinga2/features-enabled/ido-mysql.conf
```

```
/ **

 * La biblioteca db_ido_mysql implementa la funcionalidad IDO
 * para MySQL.
 * /

 biblioteca "db_ido_mysql"
 objeto IdoMysqlConnection "ido-mysql" {
 usuario = "icingaweb2
 contraseña = "contraseña",
```

```
host = "localhost",
base de datos = "icingaweb2”
}
```

Habilitar las características

Icinga2 por defectos habilita las siguientes características, podemos habilitar cualquier función a la lista ejecutando

```
# icinga2 feature enable <feature name>

# icinga2 feature list
```

Funciones desactivadas: comando api compatlog debuglog gelf grafito influxdb livestatus opentsdb perfdata statusdata syslog
Características habilitadas: checker ido-mysql mainlog notification

Las siguientes funciones están habilitadas por defecto:

- Verificador: esta característica permite la ejecución de chequeos.
- Mainlog: esta característica permite el registro.
- Notificación: esta característica habilita el mecanismo de notificación.
- IDO-mysql: proporciona un módulo IDO para la base de datos.

Instalar Icinga Web2

El siguiente paso es el instalar la interfaz web de icinga 2 y los paquetes de utilidad de línea de comandos desde el repositorio de Debian 9 utilizando su administrador de paquetes, esto se lleva acabo con el siguiente comando:

```
# apt install icingaweb2 icingacli
```

Después de la instalación puede reiniciar el *daemon* Icinga 2 para recoger todos los cambios y verificar el estado de la aplicación.

```
# systemctl restart icinga2.service
```

```
# systemctl status icinga2.service
```

```
# systemctl restart apache2
```

El siguiente paso es la instalación del esquema MySQL para la base de datos Icinga ejecutando el siguiente comando. El esquema de la base de datos MySQL se encuentra en el directorio /usr/share/icinga2-ido-mysql/Schema/.

```
mysql -u raíz icingaweb2 -p </usr/share/icinga2-ido-mysql/schema/mysql.sql
```

Como último paso se genera el Token de instalación para complementar la instalación del complemento Icinga web 2 a través de una interfaz web.

```
# icingacli setup token create
```

El token de configuración recién generado es: c25b22acfc9f9094

Configurando el plugin de Icinga Web 2

Ya que se generó el token, se puede comenzar la configuración de icingaweb2.

Abrir el navegador URL: hostname/icingaweb2/setup

Paso 1: Configuración del token

Le pide que proporcione el token generado antes para iniciar la fase de instalación.

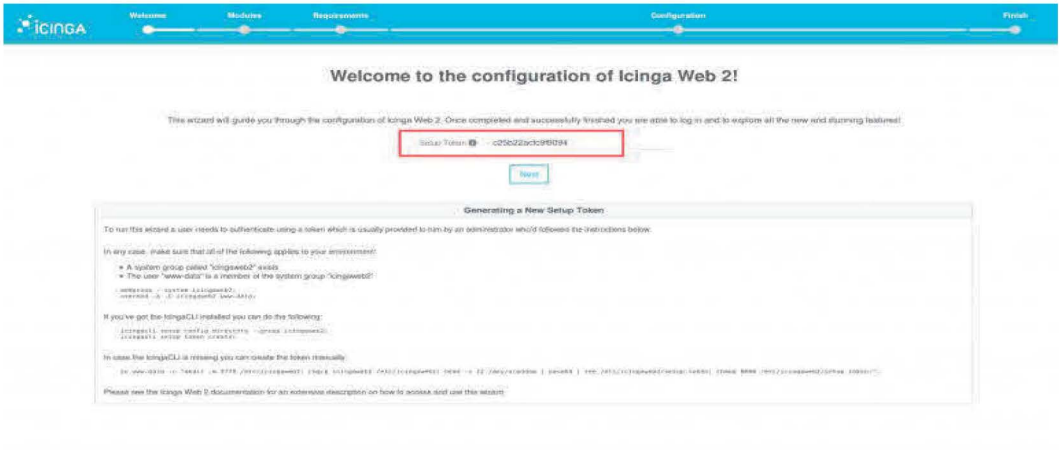


Figura 5 Configuración Token

Paso 2: Selección de los módulos Icinga Web2

Ya que ingreso el token, pasara a la siguiente sección para seleccionar los módulos que requiera.

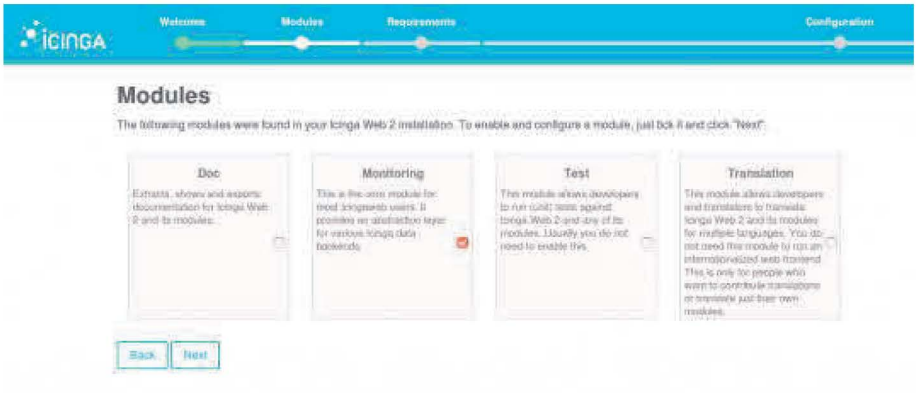


Figura 6 Módulos de Icinga Web2

Paso 3: Verificando la configuración de PHP

Para continuar, necesitamos instalar los módulos de PHP que faltan y establecer la zona horaria adecuada, después de cumplir con la configuración requerida, puede pasar a la siguiente etapa.

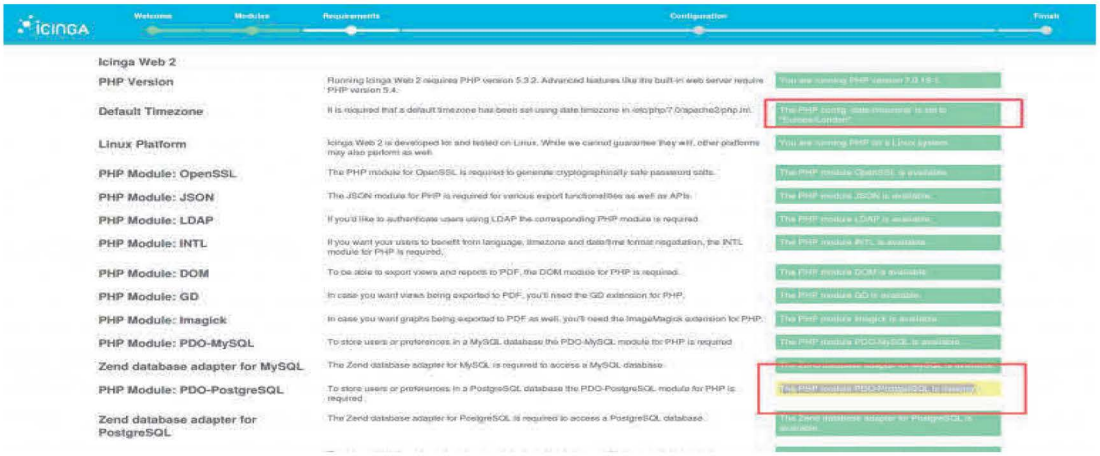


Figura 7 Verificación de la configuración de PHP

Paso 4: Métodos de autenticación

Necesita elegir los medios de autenticación preferidos para continuar con la instalación.

Figura 8 Método de autenticación

Paso 5: Ingrese los detalles de la base de datos

Agrege el nombre de la base de datos Icinga 2 web MySQL y las credenciales de acceso para esta base de datos. Esta base de datos se utilizará para almacenar usuarios y grupos de la interfaz web de Icinga 2.

Agregue icingaweb_db como nombre para este recurso y deje las variables de conjunto de Host, Puerto y Carácter como predeterminadas. No marque la opción Persistente y SSL. Presione el botón Validar configuración para validar la conexión de la base de datos, como se muestra en la imagen de abajo. Cuando termine, pulse el botón Siguiente para pasar a la siguiente sección del instalador.

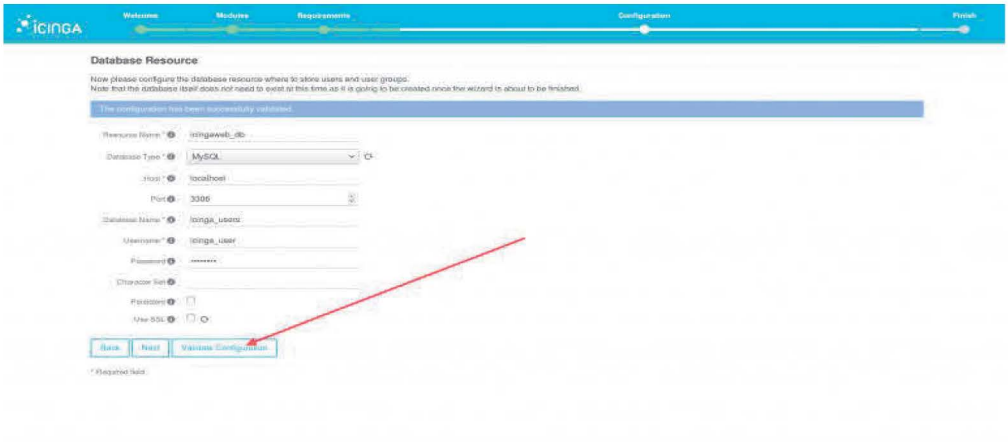


Figura 9 Detalles de la base de datos

Figura 10 Backend de autenticación

Paso 6: Crear inicios de sesión de administración web de Icinga

Después de autentificar con éxito los recursos de la base de datos, debe crear la cuenta de administrador para administrar la interfaz web.

Figura 11 Creacion de inicios de sesión de Icinga

Paso 7: Elegir las opciones de configuración de la aplicación

A continuación, debemos configurar la aplicación icinga y los registro con los siguientes parámetros.

Comprobar Show Stacktraces

- Tipo de almacenamiento = Base de datos
- Tipo de registro = Archivo
- Nivel de registro = Error
- Ruta del archivo = /var/log/icingaweb2/icingaweb2.log

Se necesita crear este archivo de registro desde el servidor backend y establece el permiso / propiedad adecuados para asegurarnos de que funcione correctamente los registros de icinga Web 2.

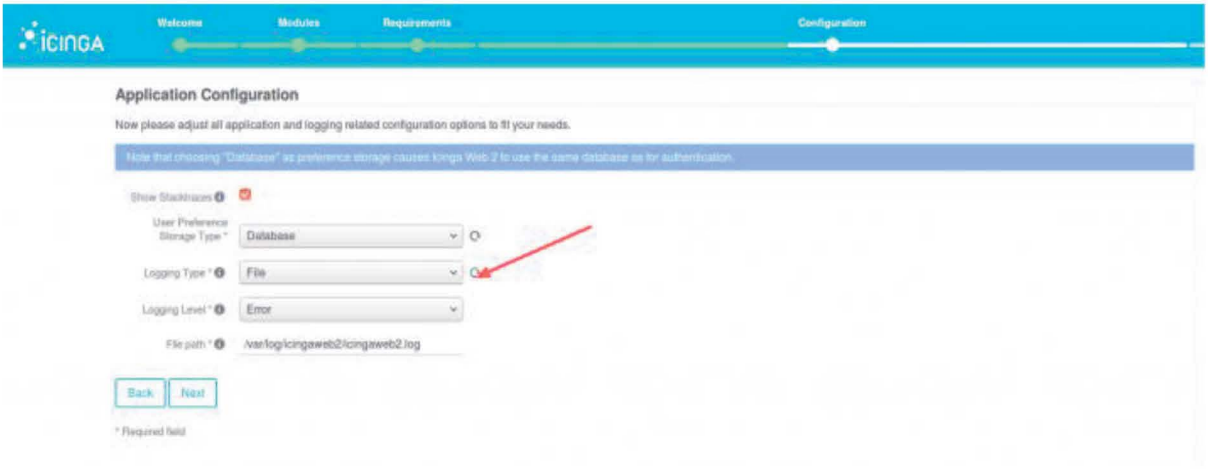


Figura 12 Enlace con archivo backend

Paso 8: Revisar todas las configuraciones elegidas.

Esta pantalla le informa que icinga web 2 se ha configurado correctamente y un informe detallado mostrara todas las configuraciones realizadas hasta el momento. Revise el informe y presione el botón Siguiente para continuar con la siguiente sección de instalación.

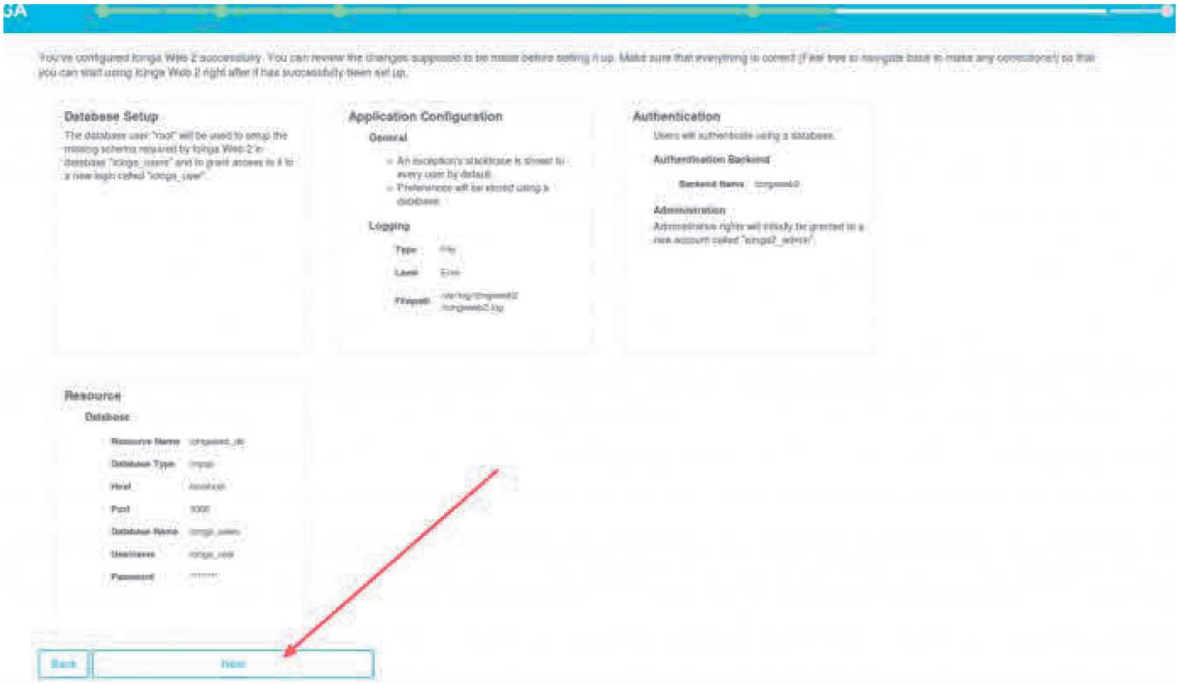


Figura 13 Revision de la configuracion

Paso 9: Configurando el Módulo de Monitoreo

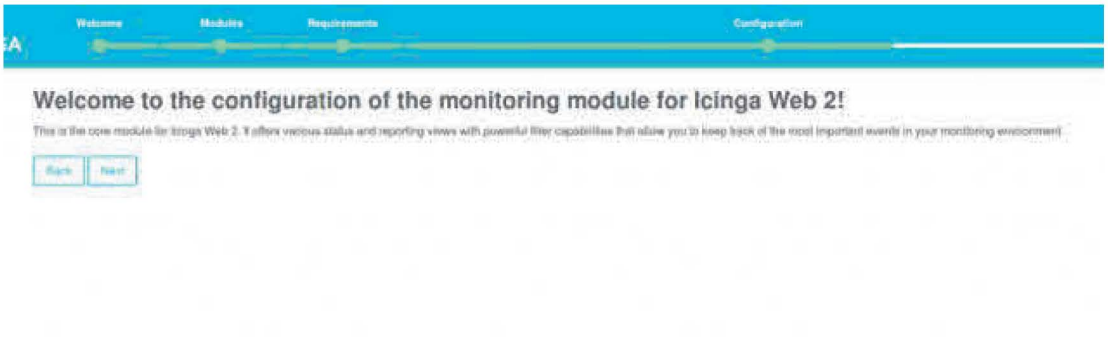


Figura 14 Configuración del módulo de monitoreo

Ya tenemos completado la parte de autenticación y sigue con la configuración del módulo de monitoreo.

Como se menciona, el módulo IDO de icinga exporta toda la información de estado y las partes de configuración a la base de datos principal de Icinga. Por lo que se debe seleccionar el módulo y configurarlo correctamente para actualizar la base de datos con la información.

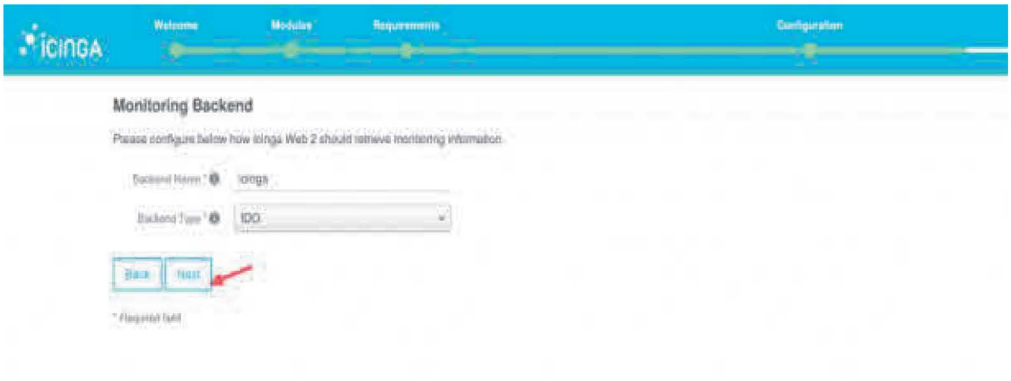


Figura 15 Detalles de configuración del módulo de monitoreo

Aquí se necesita proporcionar la información de la base de datos principal para continuar.

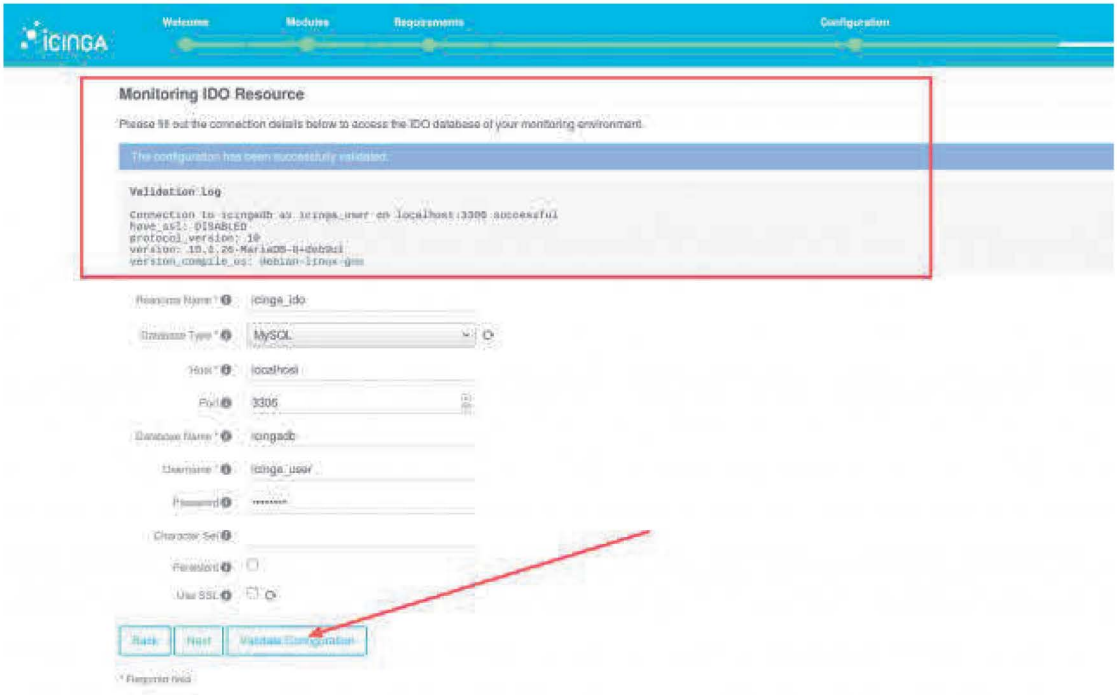


Figura 16 Información de la base de datos para el módulo de monitoreo

Configure *Icinga Command Transport* con las siguientes configuraciones y presione el botón Siguiente para continuar.

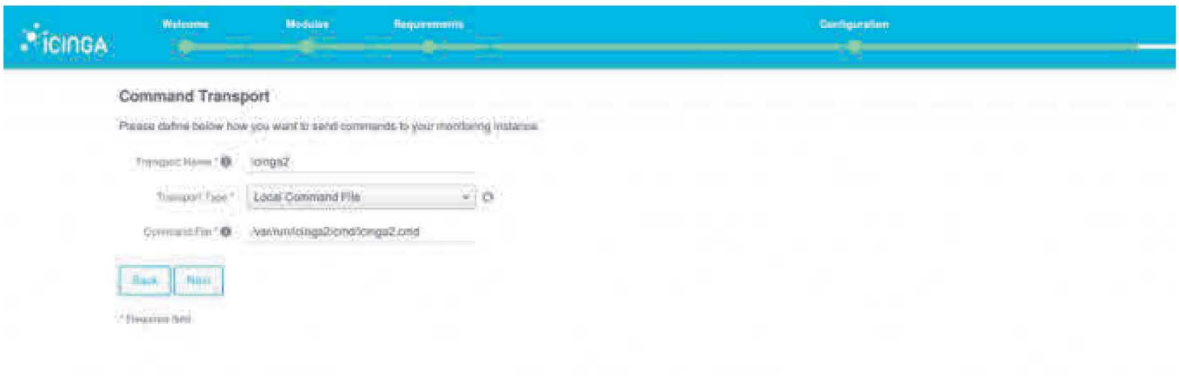


Figura 17 Configuración de Command Transport

No necesitamos realizar ninguna modificación en esta etapa de seguridad. Podemos continuar con la configuración predeterminada haciendo clic en Next.

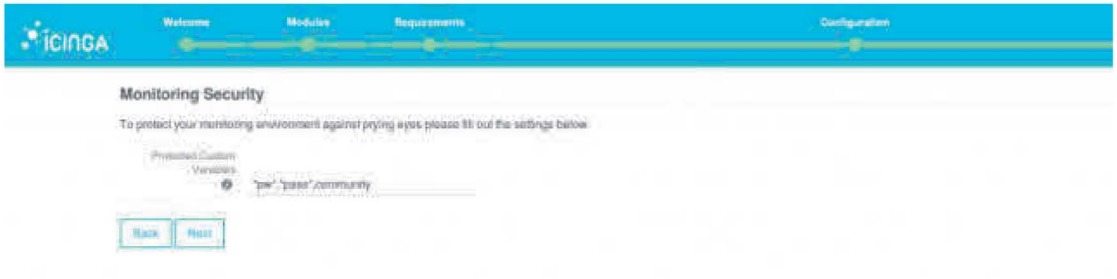


Figura 18 Supervisión de la seguridad

Paso 10: Revisión de las opciones de configuración del módulo de monitoreo

En esta etapa muestra todos los parámetros del módulo de monitoreo que ha seleccionado. Solo puede confirmar la configuración y continuar para completar la configuración.

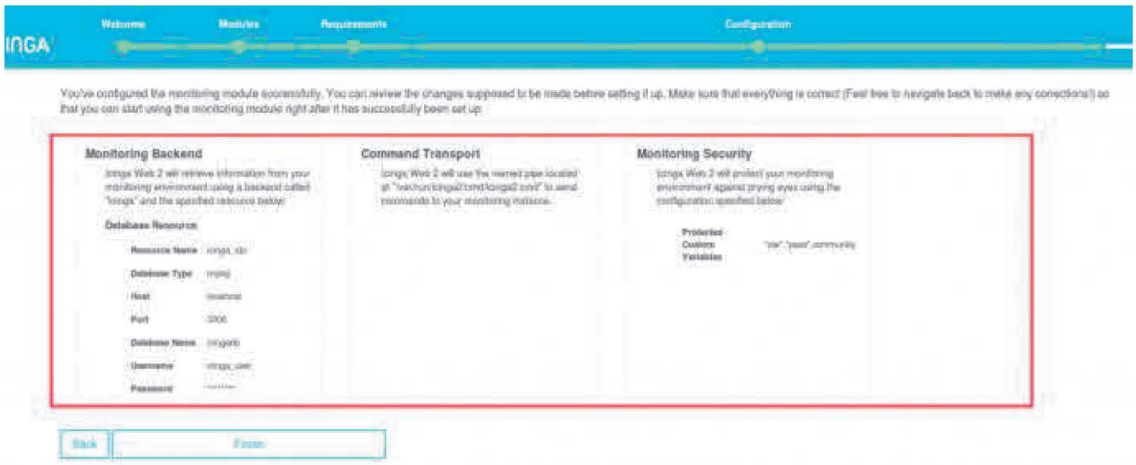


Figura 19 Revisión de la configuración del módulo de monitoreo

Paso final: iniciar sesión en la interfaz web.

Después de que el proceso de instalación termino con éxito.

Presione el Login link para redirigir a la página de inicio de sesión de Icinga2.

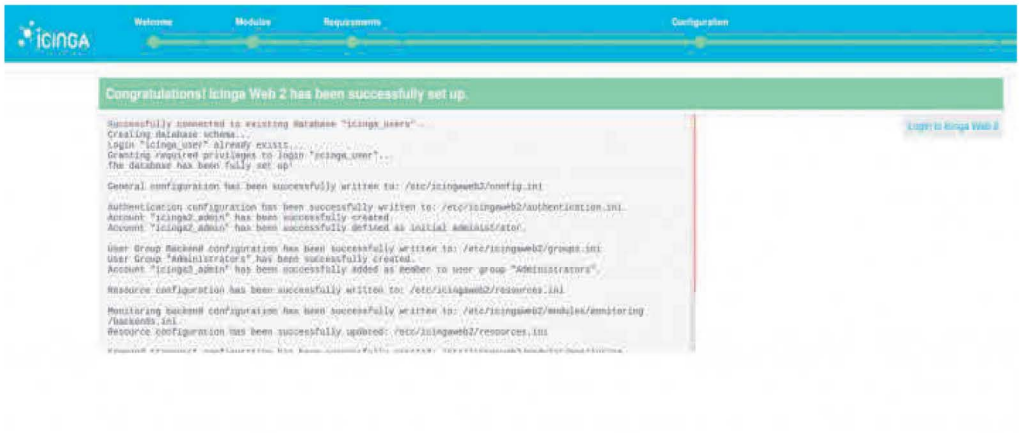


Figura 20 Finalización de instalación

Inicie sesión en Icinga Web 2 con las credenciales configuradas durante el proceso de instalación.

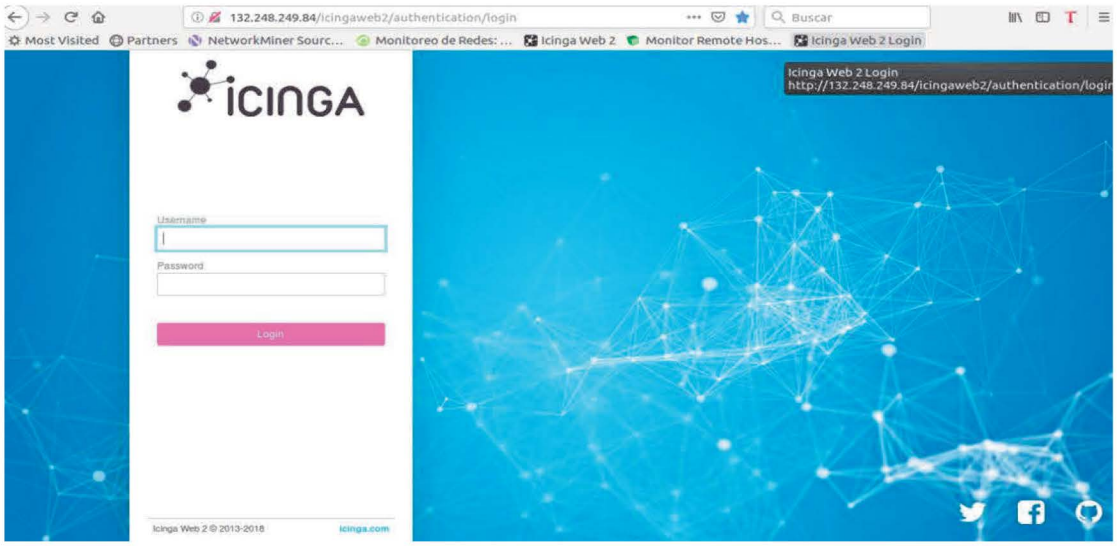


Figura 21 Inicio de Sesión en Icinga Web 2

El nodo maestro se agrega de forma predeterminada a este sistema.

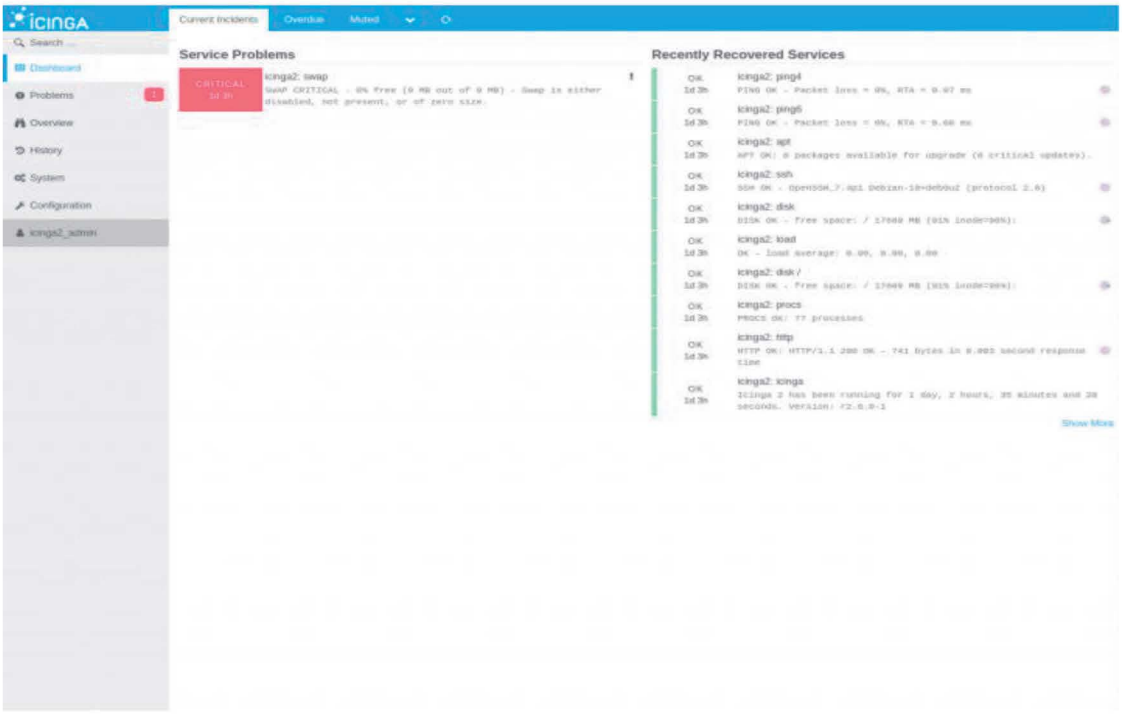


Figura 22 Presentación de la plataforma

Instalación y configurar módulo Icinga director en Icingaweb2

Se trata de un módulo que está diseñado para facilitar el uso de icinga. Ya que ayuda a editar ficheros de configuración, desde la consola de comandos, añadiendo nuevos hosts, servicios, comandos, etcétera, puede ser algo realmente tedioso. Todo esto nos lo podemos evitar, gracias a este módulo. Ya que todas estas gestiones se podrán hacer vía web, con una amigable interfaz. Similar al producto de pago Nagios XI

En la documentación oficial indica que este producto "ha sido diseñado para facilitar el manejo de la configuración de icinga. Intenta enfocarse tanto en los usuarios con el deseo de automatizar su centro de datos, como en los administradores que están dispuestos a otorgar a sus usuarios una experiencia de apuntar y hacer click".

1. Base de datos

El módulo utilize su propia base de datos, por lo que se inicia sesión el servidor y se crea la db.

```
mysql -u root -p

CREATE DATABASE director CHARACTER SET 'utf8';

GRANT ALL ON director. * TO director@localhost IDENTIFIED BY 'password';
```

Una vez hecho esto. Nos vamos a la web y a la ubicación "Configuración > Aplicación > Recursos"

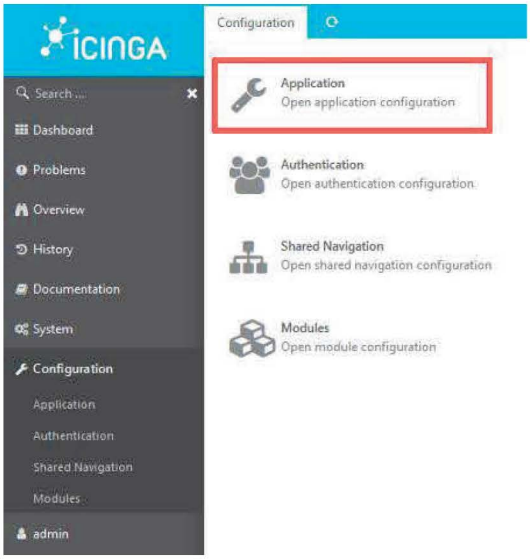


Figura 23 Configuración del módulo director

De esta manera añadiremos la base de datos como un recurso disponible para icinga, tal y como se observa en la imagen.

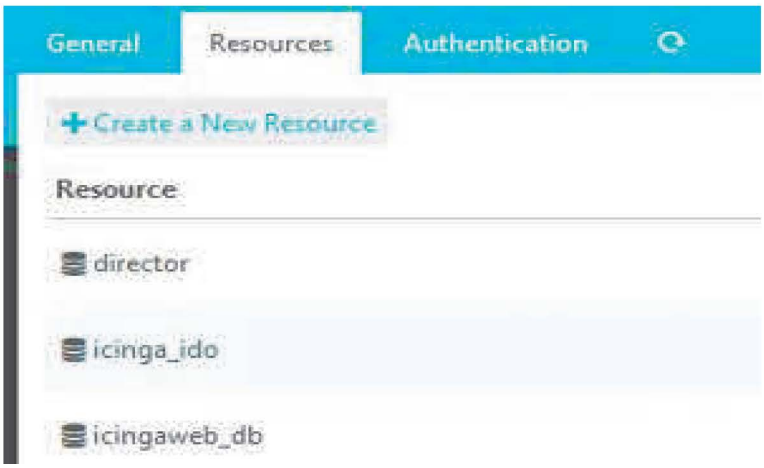


Figura 24 Base de datos para el módulo director

2. Añadir el Módulo.

Se debe añadir el módulo. Para ello creamos la siguiente ruta.

```
/usr/share/icingaweb2/modules
```

Dentro de esta ruta se descarga el proyecto.

```
wget https://github.com/Icinga/icingaweb2-module-director/archive/master.zip
```

Una vez descargado el fichero “master.zip” lo descomprimimos.

```
unzip master.zip
```

 # Si no tenemos instalado el paquete unzip, sólo debemos realizar esto:

```
# apt-get update
# apt-get  install unzip
```

Cambiamos el nombre del directorio recién creado.

```
mv icingaweb2-module-director-master director
```

Y habilitamos el módulo en la web.

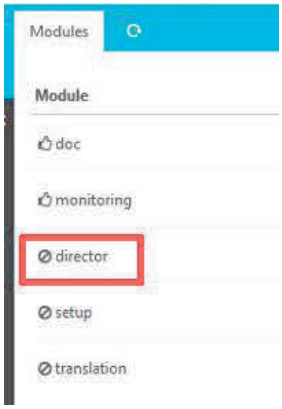


Figura 25 Habilitar modulo director

3. Añadir usuario.

Una vez habilitado, volvemos a la consola de comandos y añadimos otro usuario para la API.

```
/etc/icinga2/conf.d/api-users.conf
```

Añadimos el nuevo usuario:

```
object ApiUser "director" {
        password = "*******"
        permissions = [ "*”]
}
```

Se define la configuración de la zona en la que actuara el sistema de monitorización. Para ellos editamos el fichero */etc/icinga2/zones.conf,* lo modificamos, añadimos la información de nuestro servidor.

Figura 26 Configuración de la zona para el módulo director

Una vez hecho esto, reiniciamos Icinga2

```
# systemctl restart icinga2
```

Ahora desde la interfaz de icinga, realizamos la conexión entre el módulo e icinga2, utilizando los datos de la API que hemos creado.

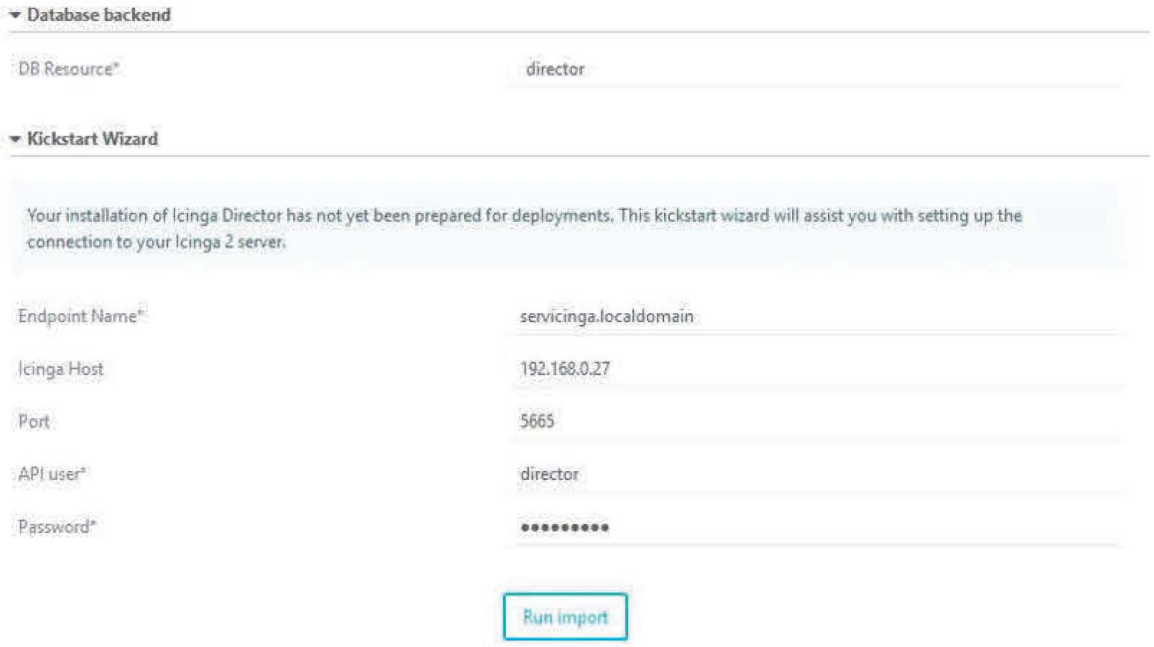


Figura 27 Conexión del módulo director a icinga

Una vez hecho esto, podemos comenzar a utilizarlo.

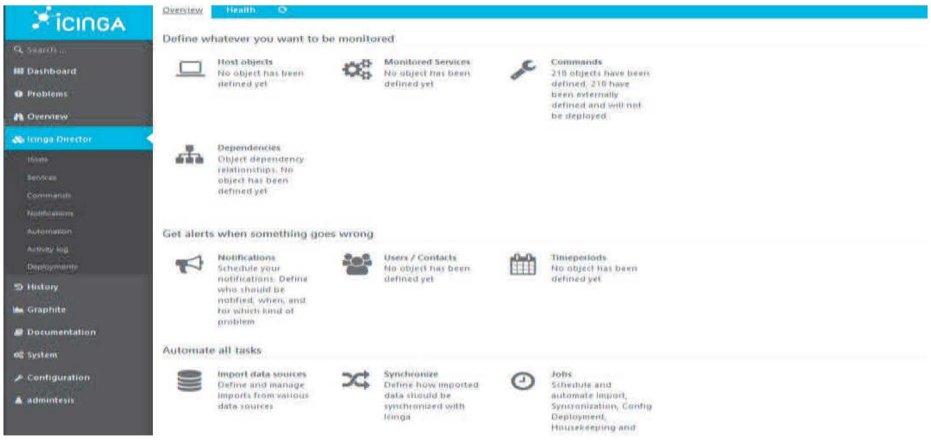


Figura 28 Modulo Director

Instalación y configurar módulo Graphite en Icingaweb2

1. Graphite

Se trata de un producto del área open source -código abierto- , englobado dentro de FOSS. Es una herramienta para la monitorización y las gráficas de rendimiento de los sistemas de computación. Ha sido desarrollada por la empresa Orbitz, lanzándose al mercado como producto open source en el año 2008. Utiliza una licencia Apache 2.0. 21

Uno de sus componentes esenciales es Carbon, responsable de recibir las métricas a través de la red y escribirlas en el disco, utilizando un backend de almacenamiento

Prerrequisitos

```
# apt-get update.
# apt-get install python2.7 python-pip python-dev python-cairo \
   python-django python-django-tagging apache2 libapache2-mod-wsgi \
   python-twisted python-memcache python-pysqlite2 python-simplejson.
```

Instalación.

Si desea conectarse a una base de datos MySQL en lugar del SQLite3 local

```
# apt-get install libmysqlclient-dev
# pip install mysql-python
```

Si desea instalar la red de graphite, carbon y whisper con pip.

```
# pip install https://github.com/graphite-project/whisper/tarball/master
# pip install https://github.com/graphite-project/carbon/tarball/master
# pip install https://github.com/graphite-project/graphite-web/tarball/master.
```

La ubicación de instalación predeterminada es `/opt/graphite`.

Configuración.

Copiamos las configuraciones de ejemplo

```
# cd /opt/graphite/conf/
# cp graphite. wsgi.example graphite. wsgi
# cp carbon.conf.example carbon.conf
# cp storage-schemas.conf.example storage-schemas.conf
# cp storage-aggregation.conf.example storage-aggregation.conf
# cd /opt/graphite/webapp/graphite
# cp local_settings.py.example local_settings.py
```

Edite el archivo local_settings.py, agregue la hora de su zona.

```
nano local_settings.py
TIME_ZONE = 'YourTimeZone'
```

Por ejemplo

```
TIME_ZONE = 'America/Mexico_city'
```

Eso es bastante importante; de lo contrario, los puntos de medición tendrán la marca de tiempo incorrecta.

Para encontrar el nombre correcto de su zona horaria, puede ingresar esto: `ls /usr/share/zoneinfo/`

Vamos a la siguiente ruta: `/opt/graphite/conf/storage-schemas.conf`

Agregue esas líneas a la parte superior de su archivo de configuración.

```
[icinga2_internals]
pattern                                                    =
^icinga2\.*\.(max_check_attempts|reachable|current_att
empt|execution_time|latency|state|state_type)
retentions = 5m:7d

[icinga2_default]
pattern = ^icinga2\.
retentions = 5m:10d,30m:90d,360m:4y
```

Inicio automático de carbon.

La última pieza para completar la configuración de graphite. Queremos que el servicio de carbon se inicie automáticamente.

```
# cd /etc/init. d
#wget https://gist.githubusercontent.com/martinseener/
5ddb8c47209bb9569c9e/raw/
82eab3547db8569c05ea0e7a310bcaec48ad7db7/carbon-cache.sh
   chmod +x carbon-cache.sh.
```

y registre el script de inicio

```
# update-rc. d carbon-cache default
```

2. Apache.

Copiamos un ejemplo de configuración a la carpeta de sitios disponibles de apache. La nueva configuración se llamará graphite.conf

```
# wgethttps://raw.githubusercontent.com/graphite-project/graphite-web/master/examples/example-graphite-vhost.conf -O /etc/apache2/sites-available/graphite.conf
```

Editar

```
/etc/apache2/sites-available/graphite.conf
```

Busque WSGISocketPrefix, cambie la línea a:

```
WSGISocketPrefix /var/run/apache2/wsgi
```

Si ejecuta Icingaweb2 y Graphite en el mismo sistema, cambie el puerto del host virtual. El puerto 80 ya está ocupado principalmente por Icingaweb2. Por ejemplo 8000.

```
<VirtualHost *:8000>
```

Siguiente asunto. El acceso a la ruta de contenido estático no está permitido. Si abre la página web, el navegador no puede encontrar el img, js ...

Permitir el acceso a la carpeta estática.

```
<Directory /opt/graphite/static/>
      Require all granted
</Directory>
```

Guarde el archivo y ciérrelo.

Habilita el modo wsgi

- `a2enmod wsgi`

Deshabilita la página apache predeterminada

- `a2dissite 000-default.conf`

Habilita el sitio de grafito.

- `a2ensite graphite`

Necesitamos dar acceso al usuario de www-data a la carpeta de almacenamiento:

- `chown -R www-data: www-data /opt/graphite/storage/`

Reiniciar apache.

- `/etc/init. d/apache2 restart`

3. Base de datos.

Inicie sesión en su servidor mysql. Crea el db y el usuario

```
# mysql -u root -p
  CREATE DATABASE graphite;
  CREATE USER graphite@localhost IDENTIFIED BY 'Password';
  GRANT ALL PRIVILEGES ON graphite.* TO graphite@SERVER;
exit
```

Edite la configuración de conexión

`/opt/graphite/webapp/graphite/local_settings.py`

```
DATABASES = {
        'default': {
                'NAME': 'graphite',
                'ENGINE': 'django.db.backends.mysql',
                'USER': 'graphite',
                'PASSWORD': 'PASSWORD',
                'HOST': 'SERVER',
                'PORT': ''
         }
}
```

Actualizar y crear tablas de bases de datos.

```
export GRAPHITE_ROOT=/opt/graphite
PYTHONPATH=$GRAPHITE_ROOT/webapp      django-admin.py      migrate
settings=graphite.settings --run-syncdb
```

4. Icinga

Cambie al servidor Icinga2

Configuración

```
icinga2 feature enable graphite
```

Edite la configuración de grafito

```
nano /etc/icinga2/features-enabled/graphite.conf

library "perfdata"

object GraphiteWriter "graphite" {
```

```
 host = "GraphiteHostIPAdress"
 port = 2003
 enable_send_thresholds = true
enable_send_metadata = true
}
```

A continuación, debe instalar el módulo Icingaweb2

```
/usr/share/icingaweb2/modules
git clone https://github.com/findmypast/icingaweb2-module-graphite
mv icingaweb2-module-graphite graphite
```

Crear archivo de configuración en / etc / icingaweb2 / modules / graphite

```
/etc/icingaweb2/modules/graphite
nano config.ini
```

copia la configuración. Agregue su nombre de host de grafito. Si configura un puerto diferente para el grafito, agregue también el puerto (Opcional).

```
[graphite]
metric_prefix = icinga
base_url = http://HOSTNAME:PORT/render?
```

Activación

Para activar Graphite, vaya a su panel de control IcingaWeb2.

Configuración -> Módulos -> grafito, haga clic en Habilitar

(Ocho, D. 2017)

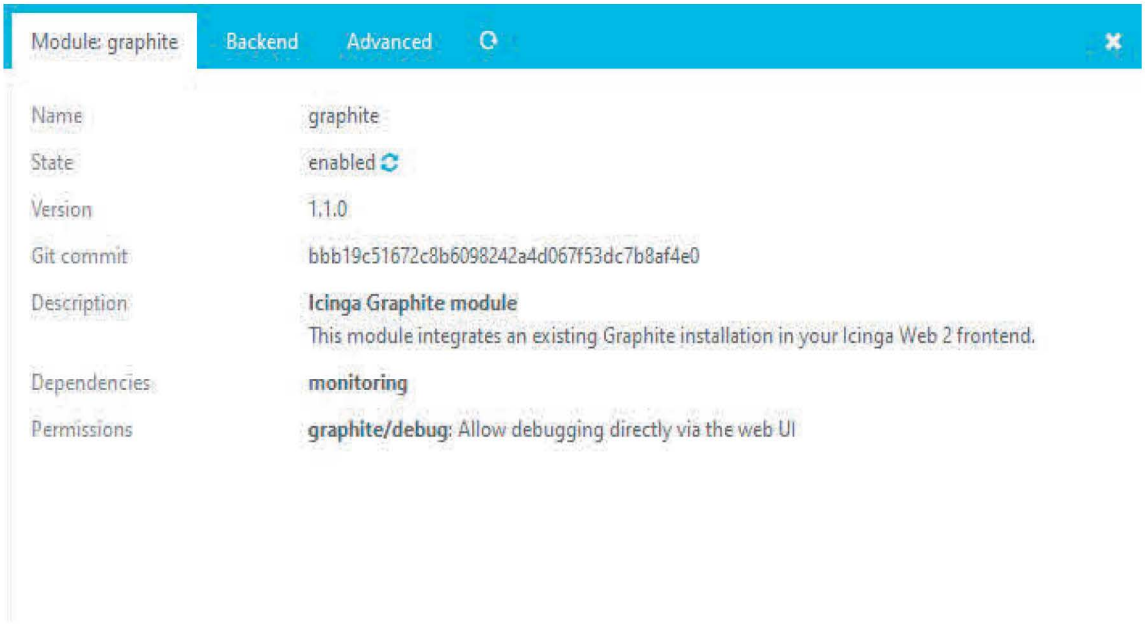


Figura 29 Configuración del módulo grafito

Hemos terminado con la instalación.

Figura 30 Modulo Graphit

Capítulo 4 Casos prácticos

Caso práctico 1 Servidor

Añadiendo host y servicios.

Servicios de red (HTTP, HTTPS, SMTP, SNMP, SSH, etcétera), Impresoras, Switches y Proxys, entre otros.

Cuenta con una moderna interfaz web, más adaptada la Web 2.0. También incorpora conectores adicionales para bases de datos (MySQL/MariaDB, Oracle y PostgreSQL). Otra importante mejora una RESTAPI para que los desarrolladores puedan crear nuevas extensiones.

Tenemos en cuenta que los ficheros de configuración que debemos modificar están ubicados en la carpeta `/etc/icinga2/conf.d`, y son:

- hosts.conf, contiene los datos de nuestro "NodeName", esto es, el servidor donde tenemos ubicado Icinga2, con los parámetros generales.
- services.conf, en el fichero definimos los servicios a utilizar. Por defecto tiene configurados los del servidor.
- users.conf, contiene los datos de los usuarios y sus direcciones de correo electrónico.
- notificacions.conf, incluye las definiciones de las alertas.
- command.conf, contiene la definición de los comandos.
- groups.conf, definición de los grupos a utilizar, por defecto contiene dos, unos para los servidores Linux y otro para los Windows.
- templates.conf, ejemplos de configuración de objetos.

- downtimes.conf, definición de los tiempos con los que tienen que trabajar los servicios.
- timeperiods.conf, aquí están definidos los tiempos de servicio, por ejemplo, por defecto trabajan con 24×7.
- satellite.conf, incluye las plantillas por defecto para los clientes remotos.

Para añadir nuestro servidor, añadiremos las siguientes líneas al fichero ubicado en `/etc/icinga2/conf.d/hosts.cfg`

```
nano /etc/icinga2/conf.d/hosts.conf
```

Y añadimos:

```
object Host "nombre del Servidor” {
  address = “ip.del.servidor"
  address6 = "::1"
  vars.os = "Linux"
  check_command = "hostalive"
}
```

Reiniciamos el servicio:

```
service icinga2 restart
o bien:
/etc/init.d/icinga2 restart
```

Ejemplos:

Host y Services

Un **host** es un equipo que alberga servicios que pueden ser monitorizados. Entre otros atributos se definen comúnmente su nombre y dirección o hostname. (Javier, F.P. 2019)

Un **service** es el elemento fundamental a monitorizar, y que por lo general corresponde con algún servicio en ejecución. (Javier, F.P. 2019)

Veamos algún ejemplo:

```
object Host "my-server1" {
  address = "10.0.0.1"
  check_command = "hostalive"
}
object Service "ping4" {
  host_name = "my-server1"
  check_command = "ping4"
}
object Service "http" {
  host_name = "my-server1"
  check_command = "http"
}
```

Vemos en los ejemplos anteriores:

- Un elemento **Host,** dentro del cual se definen los atributos:
  - **address**: la dirección IP o hostname del host
  - **check_command**: identifica el comando de chequeo a efectuar en relación al host, en este caso un hostalive corresponde con un ping
- Dos elementos **Service**, en los que se definen
  - **host_name**: el nombre del host asociado al service, es decir, el nombre del host que "corre" el service, en este caso el definido anteriormente
  - **check_command**: comando de chequeo para monitorizar el servicio

Los comandos de chequeo forman parte de los plugins de Icinga, y constituyen el elemento funcional más importante del sistema de monitorización. En el ejemplo anterior encontramos dos ejemplos:

- **http**: comando del plugin check_http
- **ping4**: comando perteneciente al plugin check_ping que efectúa un ping IPv4

NOTA

Para determinar las ubicaciones de los plugins podemos visualizar el contenido del archivo **/etc/icinga2/constants.conf** donde se definen, entre otras, variables de localización de los directorios de plugins, por defecto estos se ubican en /usr/lib/nagios/plugins

Host Groups y Service Groups.

Es posible agrupar conjuntos de hosts mediante la definición de un elemento HostGroup. Del mismo modo pueden agruparse servicios utilizando elementos de tipo ServiceGroup. Veamos algún ejemplo:

extracto del archivo `/etc/icinga2/conf.d/groups.conf`

```
object HostGroup "linux-servers" {

display_name = "Servidor Linux"

assign where host.vars.os == "Linux"

}
```

La sintaxis es clara, se define un HostGroup y se agruparán los hosts utilizando como criterio lo establecido por la directiva assign, que en este caso agrupa todos los Host que tengan establecida la variable vars.os al valor “Linux”.

De modo análogo podríamos establecer un HostGroup para los windows-servers.

```
object HostGroup "windows-servers" {

display_name = "Servidor Windows"

assign where host.vars.os == "Windows"

}
```

A continuación, vemos la definición de un objeto ServiceGroup.

```
object ServiceGroup "ping" {

display_name = "Ping Checks"

assign where match ("ping*", service.name)

}
```

Este ejemplo es similar, con la diferencia de que se está definiendo un elemento de tipo ServiceGroup, cuya finalidad es agrupar Services que tengan algo en común, en este caso según la directiva assign, se establece que todos los Services que tengan en el valor del atributo service.name el texto “ping” serán agrupados bajo el ServiceGroup “Ping Checks”.

Monitorización de Servidor

1.- Añadimos un servidor en la siguiente ruta en nuestro servidor

nano /etc/icinga2/conf.d/hosts.conf

```
/*Virtual.cuautitlan.unam.mx*/
object Host "Virtual"{
  address = "132.248.102.20"
  address6 = "::1"
  vars.os = "Linux"
  check_command = "hostalive"
}
```

Añadimos el Servidor llamado Virtual, que su dirección ip es: 132.248.102.20.

```
object Service "http" {
 host_name = "Virtual"
  check_command = "http"
}
```

Agregamos el comando de chequeo para monitorizar el servicio" http".

```
}

object Service "Disk" {
 host_name = "Virtual"
  check_command = "disk"
}
```

Agregamos el comando de chequeo para monitorizar el servicio" Disk".

```
object Service "load" {
 host_name = "Virtual"
  check_command = "load"
}
```

Agregamos el comando de chequeo para monitorizar el servicio" load".

```
object Service "procs" {
 host_name = "Virtual"
  check_command = "procs"
}
```

Agregamos el comando de chequeo para monitorizar el servicio" procs".

```
root@debian9:/etc/icinga2# cd conf.d/
root@debian9:/etc/icinga2/conf.d# nano hosts.conf
root@debian9:/etc/icinga2/conf.d# cd /
root@debian9:/# systemctl restart icinga2
root@debian9:/#
```

Reiniciamos el Servicio Icinga2 desde la terminal de nuestro servidor.

Vamos a nuestra dirección 132.248.102.84/icingaweb2.

Ingresamos nuestro usuario y contraseña.

Podemos observar que en nuestra interfaz web de icinga ya se encuentra el servidor llamado virtual que declaramos previamente en nuestro archivo de configuración, como aprecios en la siguiente imagen de igual forma nuestra muestra nos servicios de chequeo que le añadimos al host.

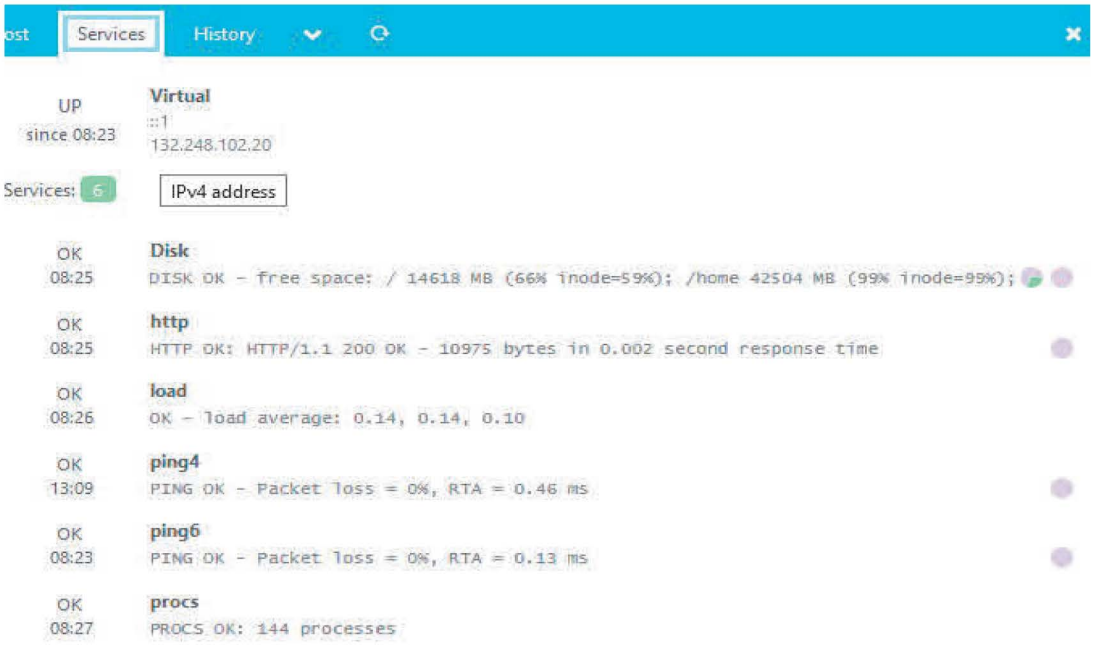


Figura 31 Servicios de chequeo

Como se ve en la imagen muestra el nombre del servidor con su dirección IP que le corresponde, desplegando los servicios de que añadimos a este con algunas de sus características de esto que inmediatamente formal una vitacora para poder realizar las gráficas que se muestran a continuación.

Vamos al módulo de **Graphite** y como lo mencionamos ya podemos observar cómo se comportan los comandos de chequeo sobre nuestro servidor de una forma más visual.

En la siguiente imagen podemos observar el espacio de almacenamiento que tiene el disco duro en uso y cuanto tiene libre.

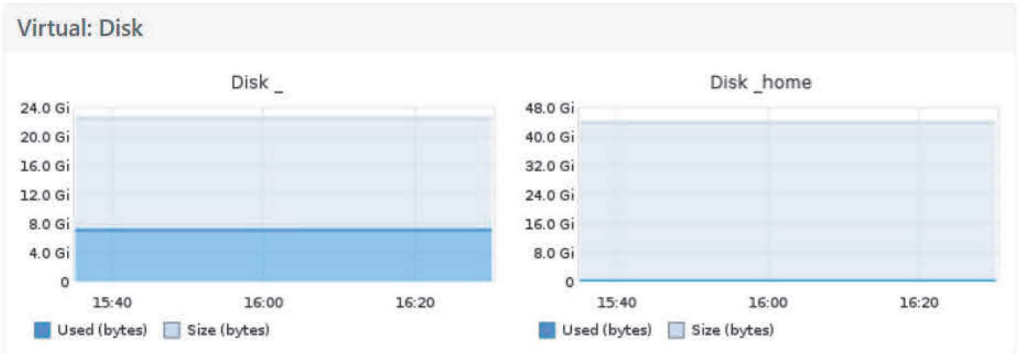


Figura 32 Graficas de espacio de almacenamiento

En la siguiente grafica podemos observar el tiempo que tiene activo el servicio desde que se declaro y se mostrara si en este lapso tuvo alguna falla el servicio se tiene la opción de seleccionar si lo queremos ver desde unos cuantos minutos o ver desde algunos años, en la parte lateral tenemos el parametro de tamaño de respuesta (bytes).

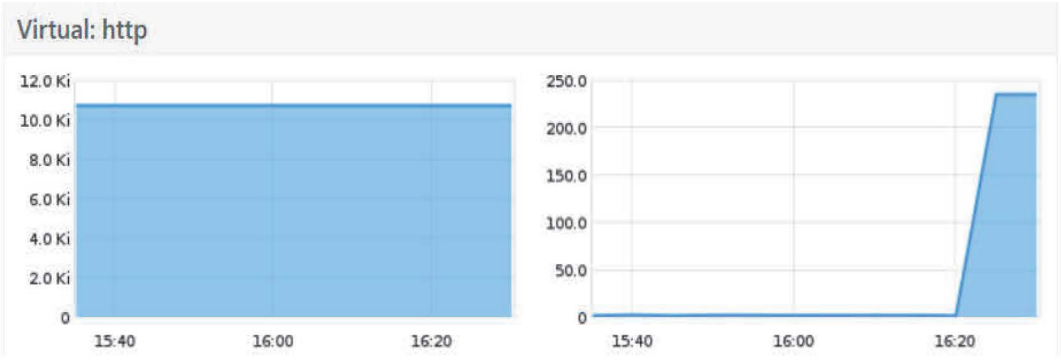


Figura 33 Graficas de teimpo activo del server

En la siguiente grafica se pude observar la carga de datos de nuestro servidor.

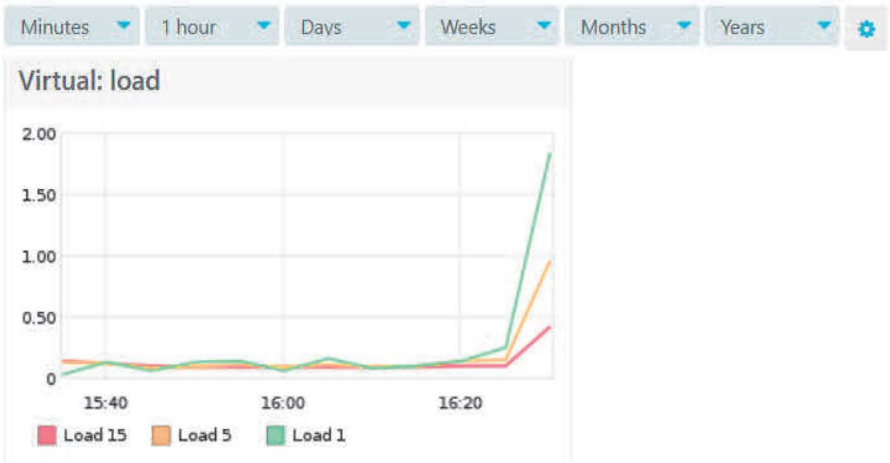


Figura 34 Grafica de carga de datos al server

En la siguiente grafica ayuda para probar la conectividad, el funcionamiento, la disponibilidad del servidor para saber el tiempo de respuesta de la conexión, entre otras tareas posibles.

Figura 35 Grafica de conectividad, funcionamiento, disponibilidad del server

En la siguiente grafica observarnos los procesos que están activos y se están ejecutando en nuestro sistema

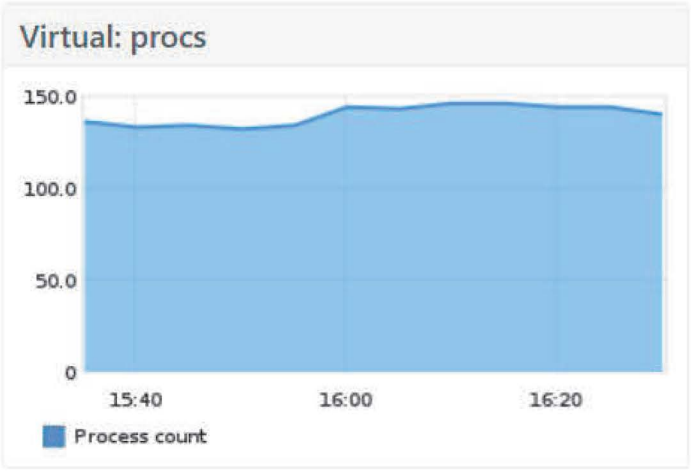


Figura 36 Grafica de procesos activos en el server

Caso Práctico 2 Monitorización de un proxy.

¿Qué es un Proxy?

Un proxy es un equipo informático que hace de intermediario entre las conexiones de un cliente y un servidor de destino, filtrando todos los paquetes entre ambos. Siendo usted el cliente, esto quiere decir que el proxy recibe peticiones de acceder a una u otra página, y se encarga de transmitírselas al servidor de la web que esta no sepa que lo estás haciendo.

De esta manera, cuando vayas a visitar una página web, en vez de establecer una conexión directa entre tu navegador y ella puedes dar un rodeo y enviar y recibir los datos a través de este proxy. La página que visites no sabrá tu IP sino la del proxy.

Diagrama de un proxy.

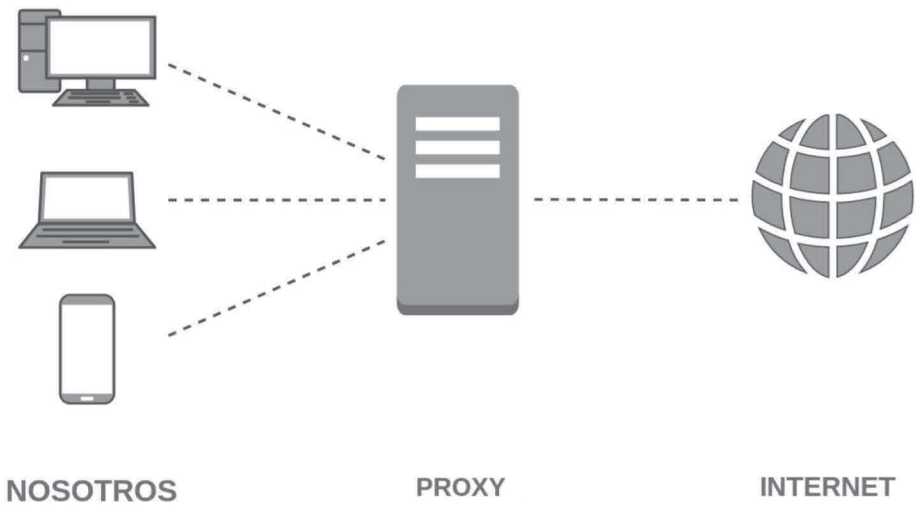


Figura 37 Diagrama de un proxy

Importancia de un proxy

Ahora que conocemos lo que es un proxy, sabemos la importancia que tiene ya que si en nuestro entorno necesitamos tener un control sobre el uso que se hace de internet desde su red se debería implementar, para monitorizar el funcionamiento del proxy resulta fundamental garantizar el funcionamiento óptimo, ahora vamos a ver el comportamiento de un proxy con Icinga web2.

1.- Añadimos un Proxy en la siguiente ruta en nuestro servidor.

/etc/icinga2/conf.d/hosts.conf

```
/*PROXY FESC UNAM*/

object Host "PROXY" {
  address = "132.248.102.231"
  address6 = "::1"
  vars.os = "Linux"
  check_command = "hostalive"
}
```

Añadimos el Proxy, que su dirección ip es: 132.248.102.231. y Agregamos el comando de chequeo "hostalive".

```
object Service "Disk" {
  host_name = "PROXY"
  check_command = "disk"
}
```

Agregamos el comando de chequeo para monitorizar el servicio" Disk".

```
object Service "procs" {
 host_name = "PROXY"
  check_command = "procs"
}
```

Agregamos el comando de chequeo para monitorizar el servicio" Procs".

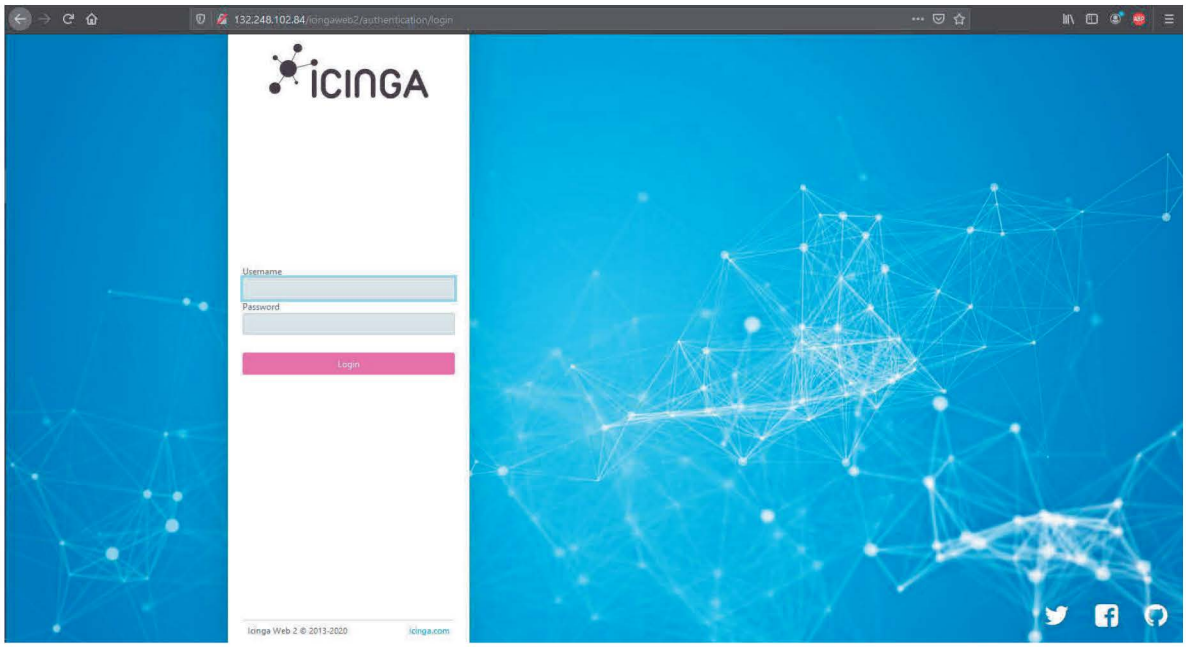
```
object Service "load" {
 host_name = "PROXY"
  check_command = "load"
}
```

Agregamos el comando de chequeo para monitorizar el servicio" load".

```
object Service "load" {
 host_name = "PROXY"
  check_command = "load"
}
```

Reiniciamos el Servicio Icinga2 desde la terminal de nuestro servidor.

Vamos a nuestra dirección 132.248.102.84/icingaweb2.



Ingresamos nuestro usuario y contraseña.

Podemos observar nuestro Proxy con la dirección ip que declaramos en el archivo, listando los comandos de chequeo que declaramos.

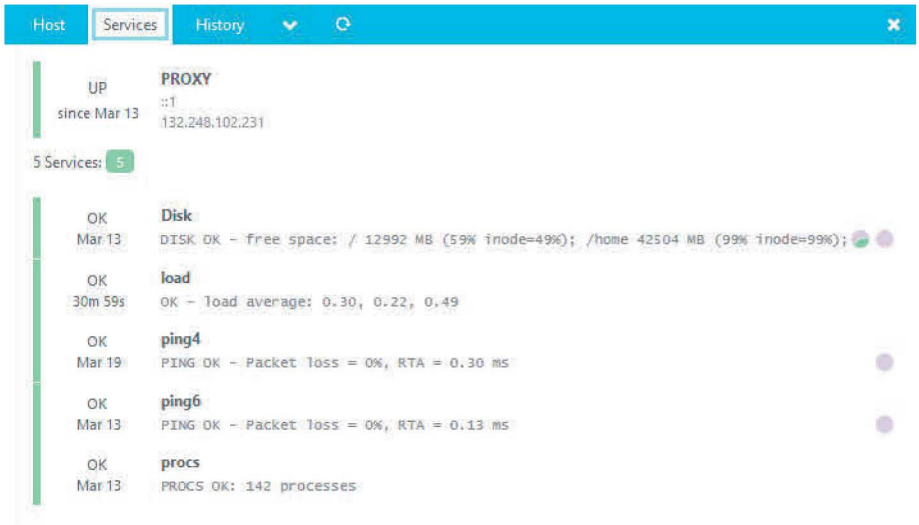


Figura 38 Servicios de chequeo en proxy

*Ahora vamos a observar cada uno de los comandos de chequeo por separado comenzaremos por el "**hostalive**".*

Observamos que al agregar este comando ya podemos visualizar el comportamiento en nuestro entorno gráfico.

Con este comando se monitorea el tiempo de respuesta de nuestro Proxy y muestra características de nuestro proxy donde informa que tenemos un 0% de pérdidas de paquetes, con un tiempo de respuesta de 0.32 ms en promedio.

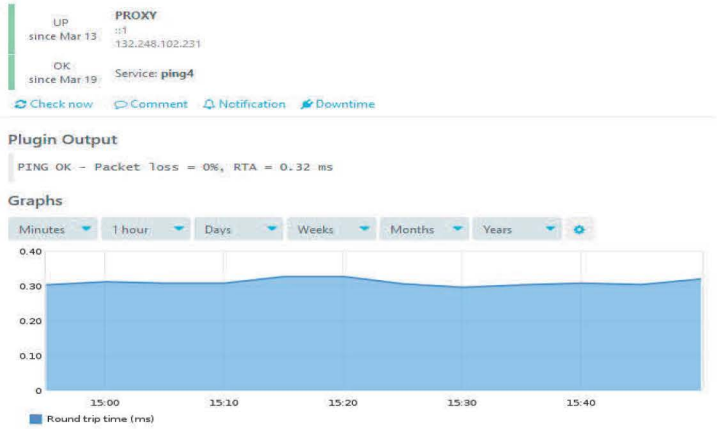


Figura 39 Prueba Hostalive en proxy

Observamos que al agregar el comando de chequeo ***"Disk"*** podemos visualizar el comportamiento en nuestro entorno gráfico, mostrándonos algunas de características de almacenamiento de nuestro equipo.

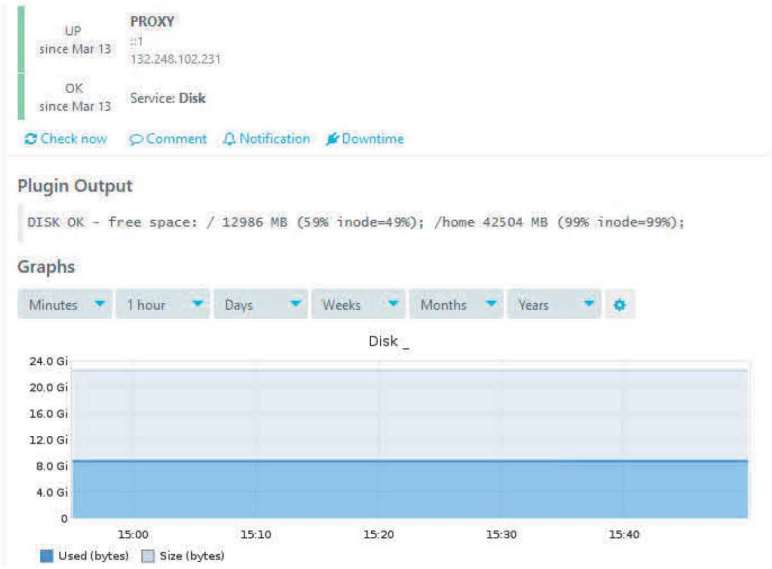


Figura 40 Prueba Disk en proxy

Observamos que al agregar el comando de chequeo ***"Procs"*** podemos visualizar el comportamiento en nuestro entorno gráfico, mostrando que tenemos 144 procesos activos en nuestro sistema, de igual forma en la parte superior de la gráfica muestra un menú de tiempos donde podemos elegir que nos muestre desde minuto a minuto o desde años.

Figura 41 Prueba Procs en proxy

Observamos que al agregar el comando de chequeo ***"load"*** podemos visualizar la carga de datos en nuestro Proxy y después que dejamos pasar algunos minutos nos muestra un promedio de carga y donde las líneas verde, amarilla y roja reflejan el rendimiento.

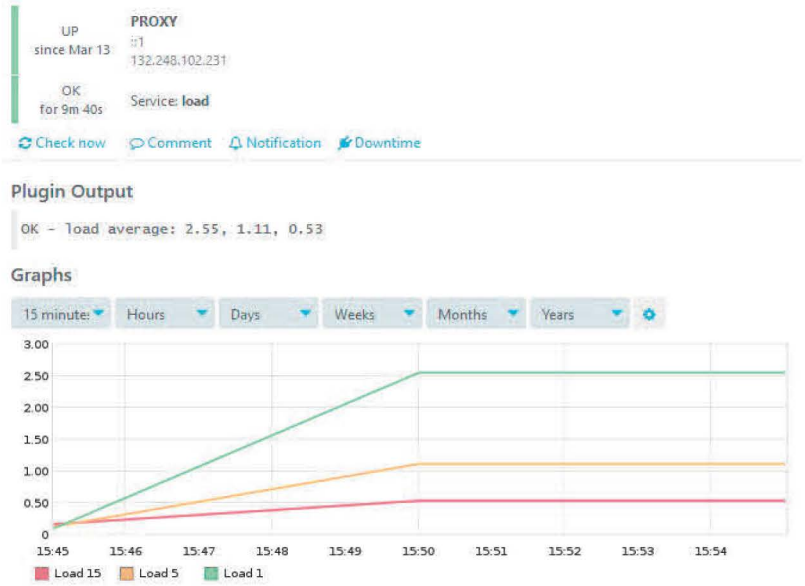


Figura 42 Prueba load en proxy

Caso Practico 3 Monitorización de un Switch

¿Qué es un Switch?

Es un dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local (LAN) y cuyas especificaciones técnicas siguen el estándar conocido como Ethernet.

El switch es posiblemente uno de los dispositivos con un nivel de escalabilidad más alto. Existen switches de cuatro puertos con funciones básicas para cubrir pequeñas necesidades de interconexión. Pero también podemos encontrar switches con cientos de puertos y con unas prestaciones y características muy avanzadas.

Son dispositivos fundamentales en muchas redes, especialmente en las redes locales, permiten la comunicación de datos utilizando eficientemente técnicas de conmutación por hardware, gracias a las cuales se han conseguido velocidades de hasta 10 Gbps. La gran flexibilidad de Ethernet como tecnología subyacente a los switches, ha propiciado una enorme flexibilidad a la hora de establecer las configuraciones y topologías de las redes basadas en Ethernet (prácticamente el 100 % de las redes LAN cableadas del mundo), que van desde pequeñas redes domésticas de unos pocos equipos, hasta grandes redes corporativas con miles de equipos conectados.

Funcionamiento de un switch.

La función básica de un switch es la de unir o conectar dispositivos en red. Es importante tener claro que un switch **no** proporciona por si solo conectividad con otras redes, y obviamente, tampoco proporciona conectividad con Internet. Para ello es necesario un router.

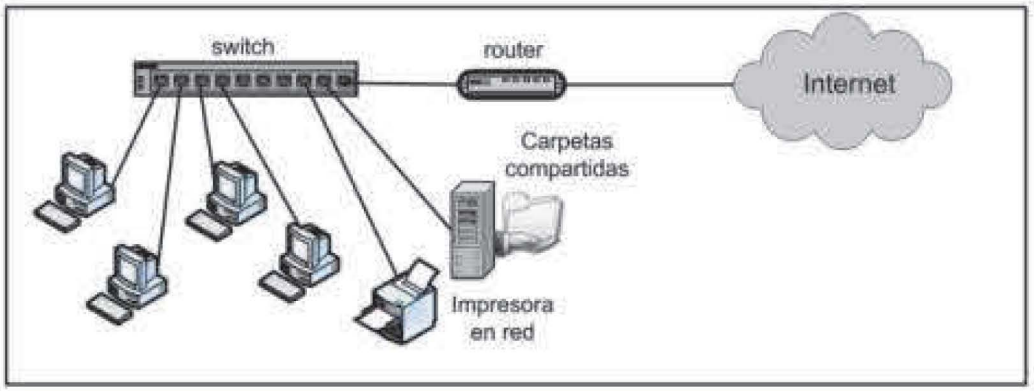


Figura 43 Funcionamiento de un switch

La conmutación consiste en trasferir datos entre los diferentes dispositivos de la red. Para ello, los **switches** procesan la información contenida en las cabeceras de la trama ethernet, los switches guardan en una tabla las direcciones MAC de todos los dispositivos conectados junto con el puerto en el que están conectados, de forma que cuando llega una trama al switch, dicha trama se envía al puerto correspondiente.

Importancia de un switch

Ahora que conocemos lo que es un switch, sabemos que es un dispositivo con propósitos especiales, diseñado para resolver problemas de rendimiento en la red, debido a anchos de banda pequeños y embotellamientos. El switch segmenta la red dentro de pequeños dominios de colisiones, obteniendo un alto porcentaje de ancho de banda para cada estación final, para monitorizar el funcionamiento de un switch resulta fundamental garantizar el funcionamiento óptimo, ahora vamos a ver el comportamiento de un switch con Icinga web2, para esto usaremos el protocolo simple de administración de redes (**SNMP**).

1.- Instalamos el plugin check_snmp

apt-get install monitoring-plugins

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
root@alan:/# apt-get install monitoring-plugins
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Paquetes sugeridos:
  icinga | icinga2 nagios-plugins-contrib
Se instalarán los siguientes paquetes NUEVOS:
  monitoring-plugins
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 43 no actualizados.
Se necesita descargar 0 B/8 608 B de archivos.
Se utilizarán 55.3 kB de espacio de disco adicional después de esta operación.
Seleccionando el paquete monitoring-plugins previamente no seleccionado.
(Leyendo la base de datos ... 228954 ficheros o directorios instalados actualme
nte.)
Preparando para desempaquetar .../monitoring-plugins_2.2-3ubuntu3_all.deb ...
Desempaquetando monitoring-plugins (2.2-3ubuntu3) ...
Configurando monitoring-plugins (2.2-3ubuntu3) ...
```

Figura 44 Monitoring plugins.

2.- Configuramos nuestro switch

Utilizamos la versión 2c de SNMP.

Agregamos la comunidad REDES_FESC21.

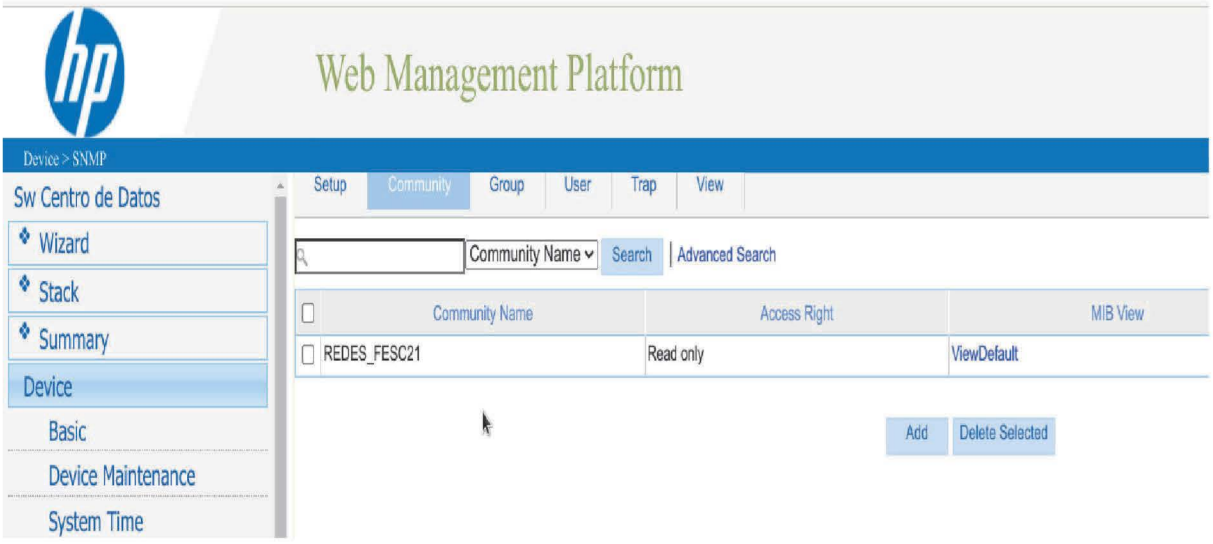


Figura 45 Switch Community

Con esta configuración podemos realizar algunas pruebas en nuestra terminal usando el comando **snmpwalk** para verificar que están funcionando.

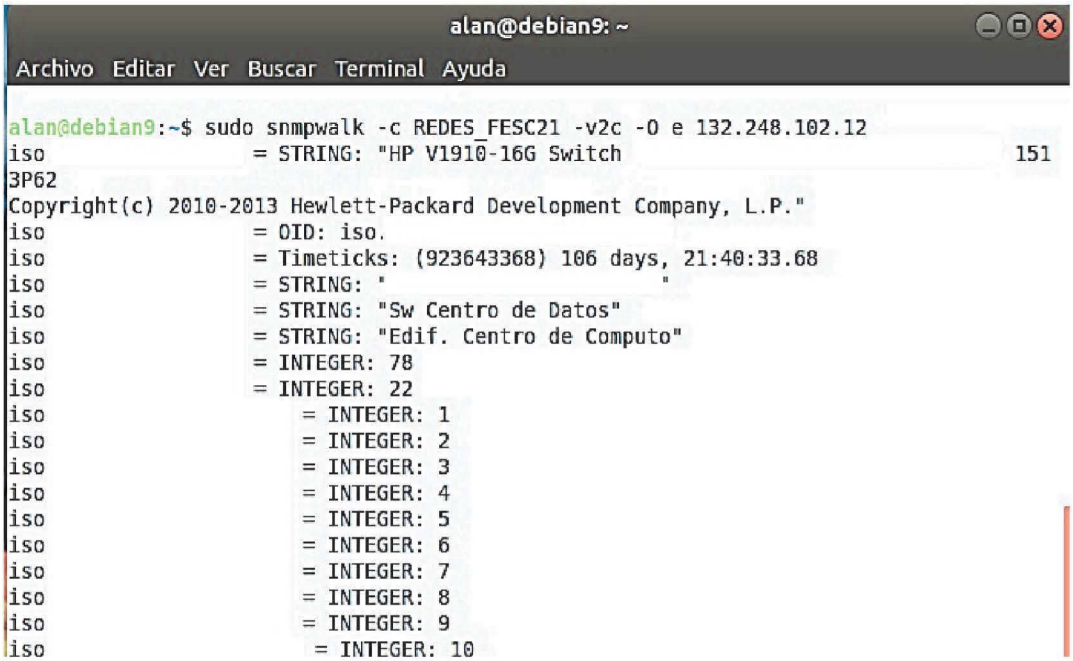


Figura 46 Snmpwalk

Una vez realizado estas pruebas verificamos que usando el plugin nos muestre datos usando una cadena en específico.

Figura 47 Check_snmp

Ahora lo vamos a implementar en icinga, para esto ingresamos a nuestro directorio:

/etc/icinga2/conf.d/

y editamos el archivo **host.conf**

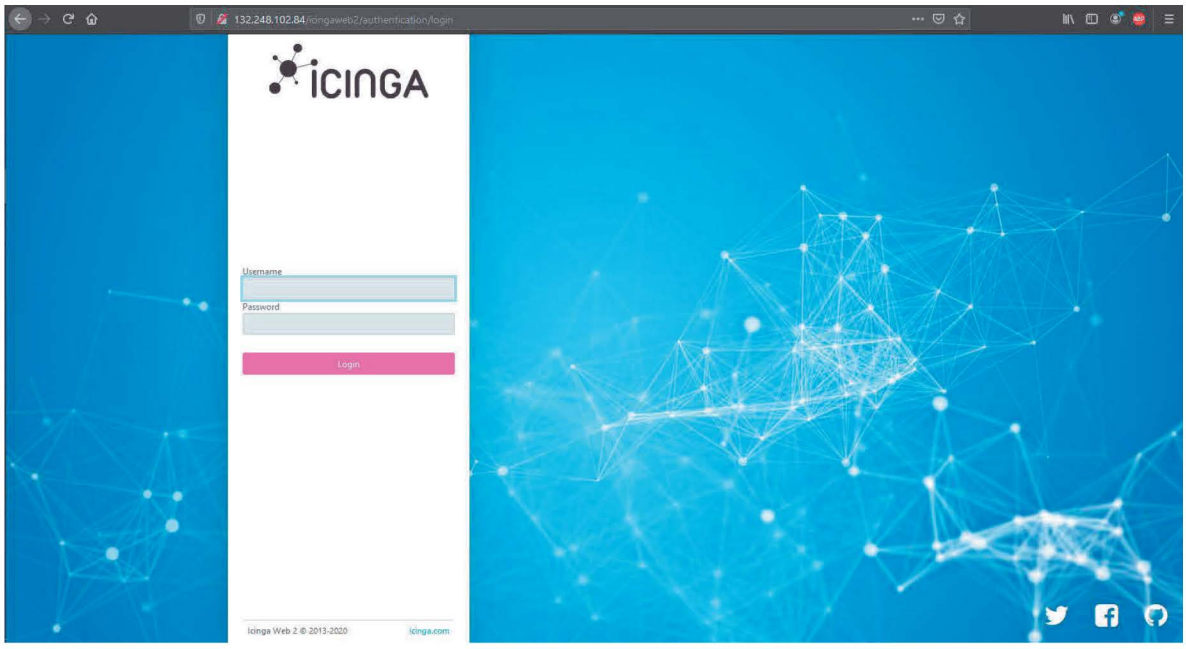
```
object Host "Switch-SNMP"{
        address = "132.248.102.12"
        check_command = "snmp"
        vars.snmp_oid = "1.3.6.1.2.1.1.3.0"
        vars.snmp_community = "REDES_FESC21"
        vars.snmp_version = "2c"
}
```

Añadimos el switch, que su dirección ip es: 132.248.102.12 y Agregamos los parámetros vistos anteriormente.

```
object Service "snmp" {
        host_name = "Switch-SNMP"
        check_command = "snmp"
}
```

Añadimos el comando de chequeo 'snmp', con el cual nos va a mostrar el tiempo activo debido a la cadena oid que elegimos.

Vamos a nuestra dirección 132.248.102.84/icingaweb2.



Ingresamos nuestro usuario y contraseña.

Podemos observar nuestro Switch con la dirección ip que declaramos en el archivo, listando el comando de chequeo que declaramos.

Figura 48 Switch-SNMP

Figura 49 Snmp-Ping

Observamos que al agregar el comando de chequeo ***"Snmp"*** podemos visualizar el tiempo activo que tiene nuestro switch, esto se debe a la cadena que elegimos, se puede varear agregando una diferente cadena dependiendo nuestras necesidades de supervisión.

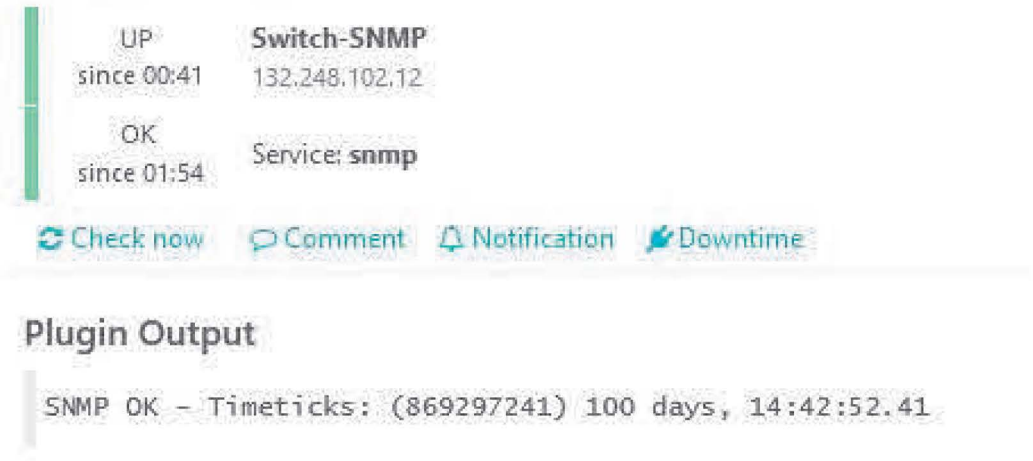


Figura 50 Timeticks Switch

Resultados y Análisis

Una vez realizado los casos prácticos de monitoreo en Icinga web2, se procedió a realizar el análisis de la información que arrojo, esta será la que indique las conclusiones a las cuales llega la implementación del sistema Icinga, por cuanto mostrará las características de supervisión de redes de comunicación.

A lo largo del desarrollo de este proyecto de tesis, se analizó la facilidad de implementar el sistema de monitoreo Icinga web2, además se implementaron sobre la plataforma algunos casos prácticos para la supervisión de la infraestructura de redes de comunicación. La supervisión de estos casos se realizó usando algunos comandos de chequeo capaces de generar detalles realistas para gestionar la infraestructura.

A través de los resultados derivados de la construcción de los casos prácticos podremos analizar la información que nos muestra, como primer punto analizaremos la presentación de los datos como podemos observar en la siguiente imagen el sistema nos traza de una forma gráfica los datos que lleva recabando desde el momento en el que nosotros dimos de alta el comando de chequeo, dando diferentes tiempos para mostrar los datos(minutos, horas, días, semanas, meses y años), este modo nos permite realizar un análisis y poder sacar en promedio de la variación de los datos.

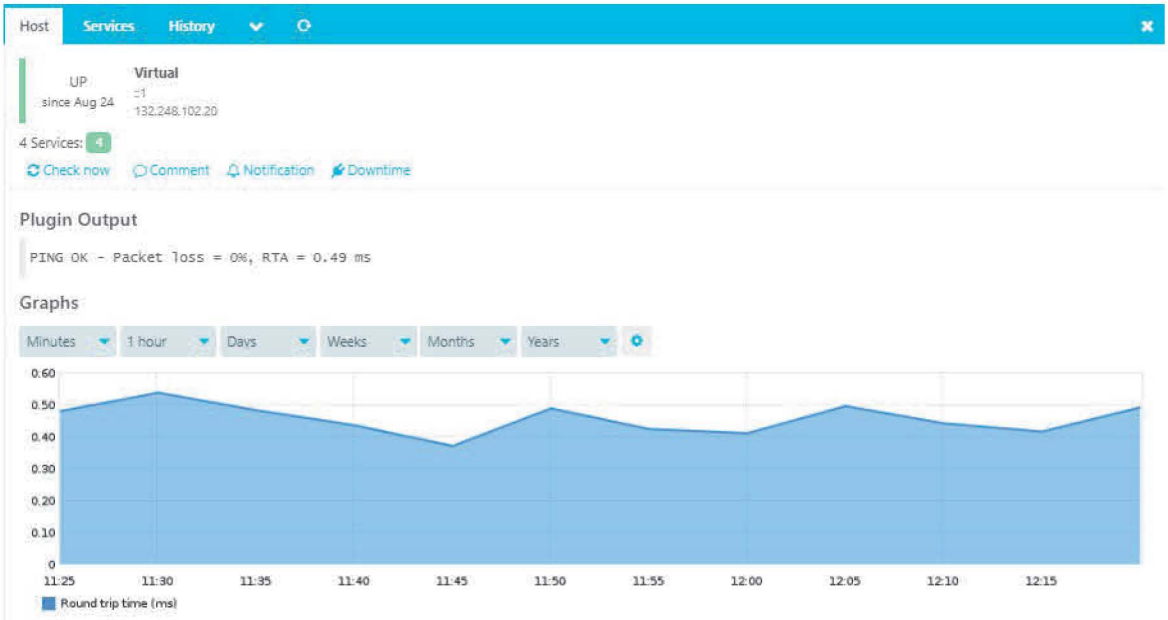


Figura 51 Presentación de los datos

El sistema nos muestra una plataforma donde tenemos diferentes opciones para checar nuestros servicios dados de alta, facilitándonos observar toda la información que nos arroja, estas opciones nos facilitaran el análisis de la información y tener una mejor toma de decisiones. En la siguiente imagen les mostramos el menú que nos presenta icinga para su navegación del sistema.

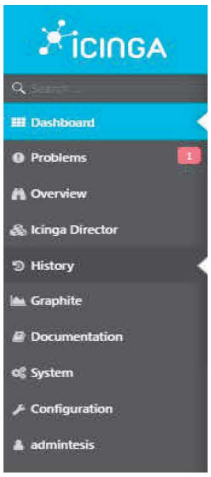


Figura 52 Panel de control

Estos paneles nos harán más fácil la supervisión de los servicios, teniendo un mejor análisis y poder prever algún problema ya que podremos analizar gráficamente el movimiento que están tendiendo los servicios, por ejemplo, el crecimiento de la información y el espacio disponible y ocupado que tiene el host, en este caso podremos analizar la información de que tan rápido esta aumentado el volumen de datos, en la siguiente imagen les mostramos un ejemplo de lo ya mencionado.

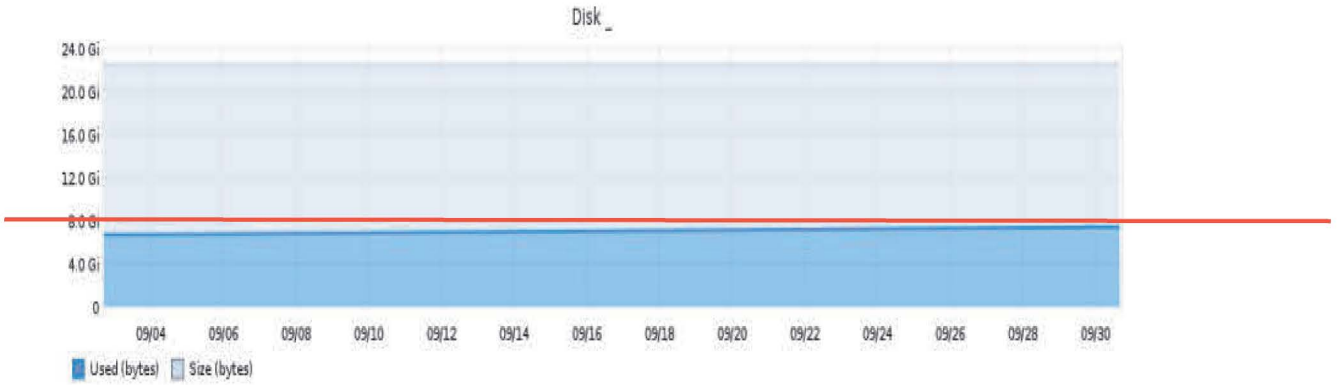


Figura 53 Grafica de espacio en Disk

En la imagen anterior podemos observar un pequeño crecimiento del día 04 a 30 y vemos que el crecimiento de datos es algo mínimo así que podemos tomar una mejor decisión en cuanto el espacio otorgado a diferentes actividades o servicios en el host.

La carga de servicio es la carga que una estructura vería a diario cuando se usa según su diseño, las cargas de servicio reflejan la carga diaria de una estructura y están directamente relacionadas con la comodidad del usuario de la estructura, ahora un pequeño ejemplo, si un edificio está diseñado únicamente sobre la base de la carga máxima o de diseño puede ser aceptable que resistirá la falla hasta un punto aceptable, pero sería un edificio inhabitable. La carga de servicio dirige a uno a criterios de deflexión entre otras cosas. Un piso elástico puede estar bien en un sentido general de capacidad, pero si los usuarios de la estructura se sienten incómodos con un piso laminado, la estructura ha "fallado" desde el punto de vista de la capacidad de servicio.

Ahora nosotros como podemos observar la carga de servicios en nuestro host, para esto existe un comando de chequeo “Load” este comando nos permitirá observar la carga que tenemos en nuestro host, para de esta forma supervisar la carga de servicios y evaluar cuándo podremos estar en riesgo, en la siguiente imagen les mostramos la carga de servicios en nuestro host.

Figura 54 Grafica de servicio Load

Como podemos observar en la imagen anterior vemos de las 16:10 a 16:25 tuvimos un aumento de carga, pero nada grave ya que el pico más alto tuvo una carga aproximada de 0.70, esto nos permite evaluar y checar que servicio esta ocasionado esta carga y poder tomar una mejor decisión en la repartición de recursos.

Los procesos involucran procedimientos, tareas, mecanismos, actividades y rutinas mediante las cuales se entrega un servicio a un usuario o cliente, un proceso es una parte fundamental en un servicio, pero como podemos observar si tenemos una sobre carga de procesos en nuestro host, en la siguiente imagen observamos la carga de procesos que tiene nuestro host en ejecución.

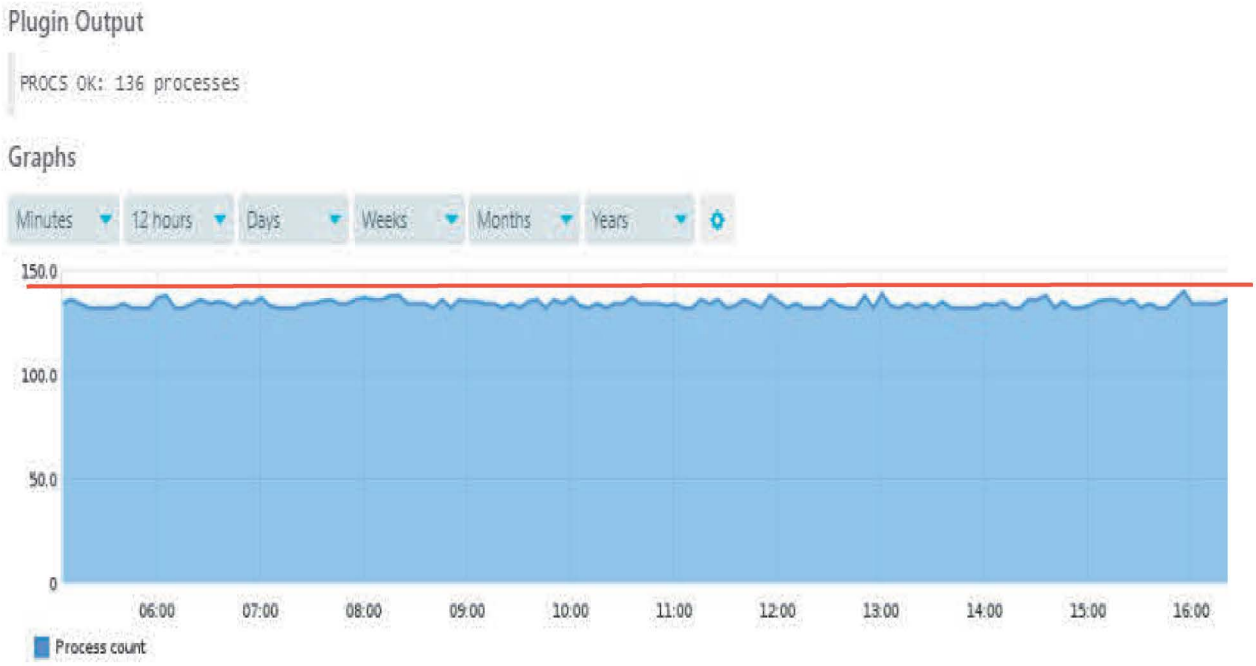


Figura 55 Grafica de Carga de procesos

En la imagen anterior podremos observar que tenemos una variación de procesos, pero analizando la gráfica vemos que el rango este entre 125 – 147 teniendo como promedio 136 procesos en ejecución, para nuestro host en un promedio intermedio ya que los valores máximos rondan en los 4000 procesos así que estamos por debajo de la mitad.

El ping está diseñado para hacer una prueba automáticamente al host y detectar sus interrupciones y problemas de calidad de conexión. Utilizar pings ICMP para detectar estados de los hosts monitoreados y estima la calidad de la conexión en tiempo real en función de la perdida de paquetes, la latencia y las métricas de Jitter. En la siguiente imagen podemos observar las pruebas del ping.

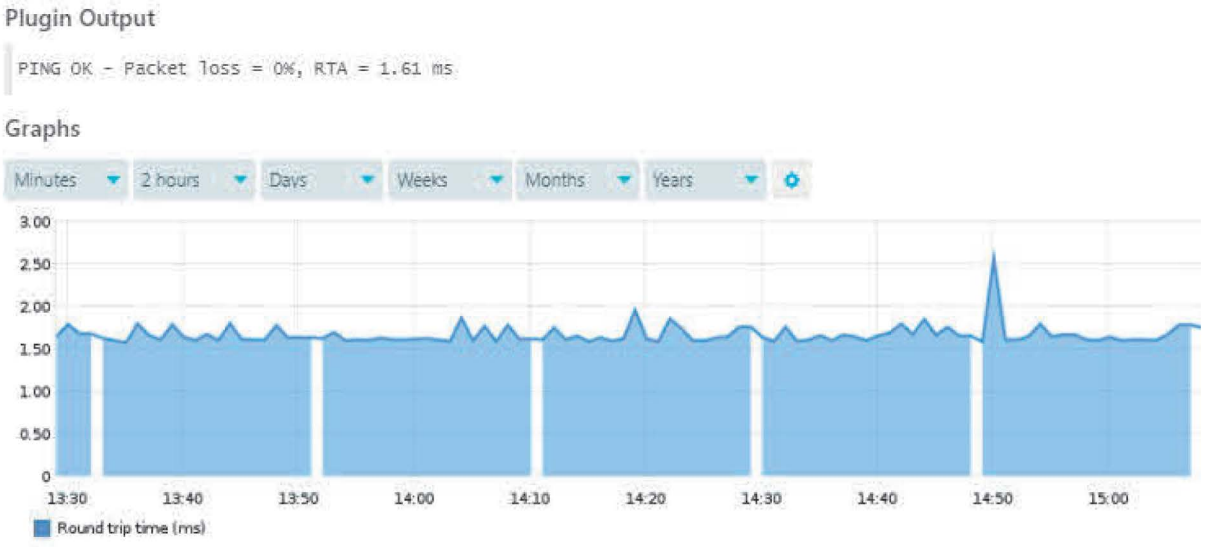


Figura 56 Grafica de pruebas de ping

El sistema almacena información sobre cada ping y permite obtener estadísticas detalladas de cualquier host durante cualquier periodo histórico, como el porcentaje de paquetes perdidos, el promedio de viaje de ida y vuelta, etc.

SWAP (Espacio de intercambio), es una parte del almacenamiento secundario que se utiliza como memoria virtual. Cuando la memoria principal (almacenamiento primario) está llena, las paginas inactivas se mueven a la memoria virtual y luego se regresan cuando es necesario. El uso de almacenamiento secundario como memoria virtual puede aumentar el rendimiento de los sistemas que tienen poca memoria principal disponible.

El uso de intercambio se refiere al porcentaje de memoria virtual que se está utilizando actualmente para almacenar temporalmente paginas inactivas de la memoria física principal. Es crucial monitorear el uso de SWAP, porque el espacio de SWAP es su "red de seguridad" para cuando se quede sin RAM, en la siguiente imagen les mostramos el monitoreo de SWAP para obtener información que nos pueda ayudar en el uso y manejo del espacio disponible.

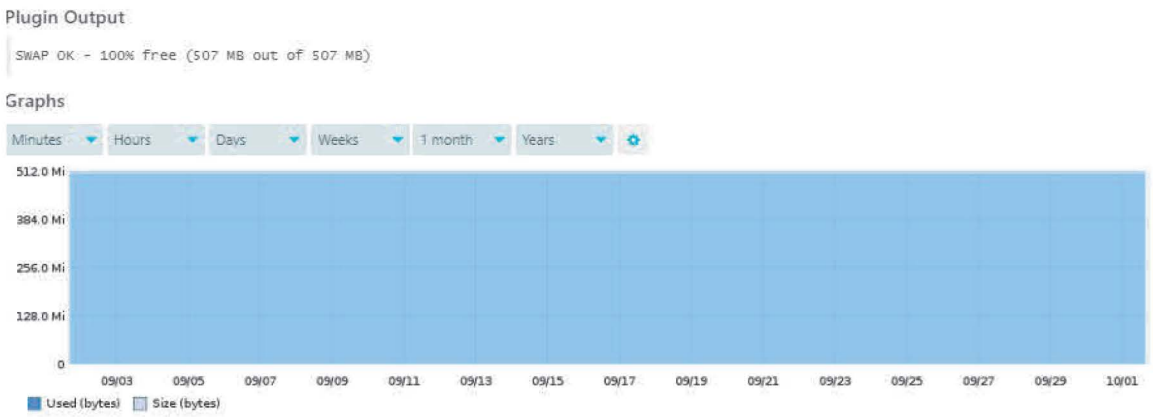


Figura 57 Grafica SWAP

Durante el intercambio, los procesos pueden volverse más lentos, pero los datos aún se procesan. Sin embargo, cuando se queda sin memoria virtual, los procesos se ponen en cola y se detienen hasta que se libera algo de memoria.

En la imagen anterior podemos observar que de 507 MB tenemos disponibles 507 MB, así que tenemos el 100% de espacio de intercambio disponible debido a esta información podemos definir que nuestro host no tiene algún riesgo memoria de intercambio, los valores en riego estarían debajo de los 250 MB.

Monitorear el uso y la tasa de intercambio puede ayudar a analizar las cargas de trabajo en su servidor. Por ejemplo, si determina que la mayoría de los procesos requieren un procesamiento rápido, debe tener suficiente memoria principal, mientras que la memoria virtual no ayudará mucho. Por otro lado, si una gran cantidad de procesamiento es bastante lento con grandes cantidades de datos almacenados en la memoria entre cálculos, puede usar el intercambio para liberar la memoria principal para un procesamiento más rápido de las solicitudes del cliente. Equilibrar las cargas de trabajo entre los servidores y en cada servidor por separado es la clave para brindar servicios eficientes.

HTTP el protocolo de transferencia de hipertexto es un protocolo de aplicación para sistemas de información distribuidos, colaborativos e hipermedia. HTTP es la base de la comunicación de datos para la World Wide Web. Monitorear HTTP se puede utilizar como una manera de recopilar información para comprobar la disponibilidad del servicio, de obtener información sobre un servidor web, en la siguiente imagen podemos observar algunos de los datos ya mencionados.

Figura 58 Grafica del protocolo http

Como podemos observar en la imagen anterior nos muestra el tamaño de respuesta en bytes y el tiempo que está tardando en responder en segundos.

Monitorear el servicio http nos puede ayudar para mejorar la accesibilidad a los archivos alojados en nuestro servidor, para que las páginas puedan ser visitadas por los usuarios con mayor facilidad, básicamente si nuestro servicio http se encuentra en óptimas condiciones podrán guardar y transmitir datos vía el sistema de redes llamado Internet. Ejemplo cuando un usuario entra en una página de internet, su navegador se comunica con el servidor, enviado y recibiendo datos que determinan que es lo que vera en su pantalla.

Mantener el sistema operativo bien actualizado, es de vital importancia para el buen funcionamiento de nuestro ordenador, aunque existen otros puntos relevantes para mantener nuestro sistema completamente actualizado.

Las actualizaciones del sistema son mejoras que se realizan al núcleo del sistema operativo y a diversas aplicaciones que se ejecutan en este sistema, con la finalidad de mantener su funcionamiento óptimo y reparar fallas, errores y vulnerabilidades que se pueden presentar en nuestro sistema. Este proceso de actualizaciones se puede realizar manual o automáticamente, dependiendo de la personalización del sistema.

En la siguiente imagen podemos observar cómo nuestro sistema icinga web2 nos presenta información detallada sobre nuestras actualizaciones.

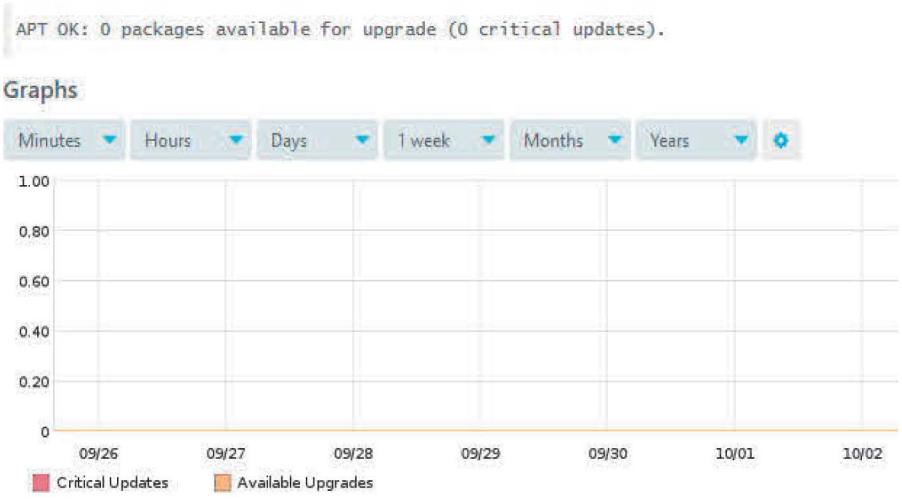


Figura 59 Grafica de actualizaciones

En la imagen anterior nos muestra información sobre las actualizaciones que tenemos disponibles y si tenemos alguna actualización de carácter crítico. Como observamos tenemos 0 actualizaciones disponibles y 0 actualizaciones criticas así que podemos decir que nuestro servidor se encuentra en óptimas condiciones para su funcionamiento.

Conclusión.

La presente tesis tuvo como objetivo la implementación de un sistema de monitoreo de redes de comunicación para analizar las características de supervisión que proporciona en la gestión de la infraestructura, se analizó teóricamente algunos conceptos básicos que se consideraron de importancia para poder implementar el sistema, se realizó una comparativa de diferentes sistemas de monitoreo, se implementó el sistema de monitoreo Icinga y se desarrollaron diferentes casos prácticos para la supervisión de la infraestructura de red para poner aprueba el sistema de monitoreo.

Observamos que implementar un sistema de monitoreo de redes es de suma importancia en nuestra infraestructura, ya que nos permite analizar las características de la infraestructura de red y facilita la supervisión de esta.

El sistema icinga web2 se caracteriza por ser rico en funcionalidades y es capaz de monitorear la mayoría de los recursos, tanto los que tiene en la actualidad como los que puede tener en el futuro, Icinga web2 es un monitor de host y servicios diseñado para sistemas operativos Linux tomando como base a Nagios.

Se llevo a cabo la construcción de algunos casos prácticos donde se puso a prueba a Icinga web2, para analizar la información que nos arrojaba y si facilitaba la interpretación de esta, debido al módulo de graficación que se le integro al sistema tuvimos una mejor interpretación de resultados debido a que nos fue fácil de supervisar el comportamiento de la red e interpretar la información.

Se considera que una de las mayores virtudes que puede tener este proyecto es poner a prueba de forma real en la infraestructura de red de la Facultad Estudios Superiores Cuautitlán, para poder realizar casos prácticos con equipos activos y poder tener un mejor reflejo de la información.

De esta manera, se concluye que Icinga web2 es la mejor opción para monitorear la infraestructura de red de comunicaciones, debido a su amigable plataforma, la forma de presentar la información, la realización de informes personalizados y se pueden configurar envios automáticos de informes cada cierto tiempo.

Referencias Bibliográficas

1. *Michael A. Gallo & William M. Hancock. (2003).6. Comunicación entre computadoras y tecnologías de redes Thomson.*
2. *Andrew Hopper, Steven Temple, Robin Williamson. (1989).5. Diseño de redes locales. Paz Montes de oca: Addison-Wesley Iberoamericana.*
3. *David Terán. (2014). 1. Administración Estratégica de la función informática. México: Alfaomega Grupo Editor.*
4. *Richard Bejtlich, José Rafael García-Bermejo Giner. (2005). 3. El Tao de la monitorización de seguridad en redes: más allá de la detección de intrusiones. España: Pearson Educación.*
5. *Hatch, B. - Lee, J. - Kurtz, G. - Montaño, G.C. (2001). 4. Hackers en Linux: secretos y soluciones para la seguridad de Linux. Madrid: S.A. Mccgraw-Hill / Interamericana de España.*
6. *Gerardo Sánchez Ambriz, Marcela Angeles Dauahare. (17/02/2017). Tesis y otras modalidades de titulacion Estrategias metodologicas. Fesc: fesc*
7. *A. Medina., D. I. C. (s. f.). Vista de Internet: Evolución e Impacto de la Red de Redes | Revista Prisma Tecnológico. Recuperado 20 de octubre de 2019, de https://revistas.utp.ac.pa/index.php/prisma/article/view/537/html*
8. *UMBERTO, E. C. O. (2015). Historia Internet - ARPANET en sus inicios. Recuperado 20 de octubre de 2019, de http://www.paralibros.com/passim/p20-tec/pg2050ci.htm*
9. *Castells, M. (2013). El impacto de internet en la sociedad: una perspectiva global. Recuperado 22 de octubre de 2019, de https://www.bbvaopenmind.com/articulos/el-impacto-de-internet-en-la-sociedad-una-perspectiva-global/*
10. *HUGO, D. (2015, 23 noviembre). WWW World Wide Web ¿Qué es? historia y origen. Recuperado 22 de octubre de 2019, de https://disenowebakus.net/world-wide-web-www.php*
11. *Cissp, C. R. S. C. E. Y. (2019). Evolución y tendencias de las herramientas de monitoreo de redes. Recuperado 24 de octubre de 2019, de https://www.magazcitum.com.mx/?p=1157#.Xp4vUiNR2Ch*
12. *Tacoa, K. (2018, 27 abril). RED DE COMPUTADORAS - Katherine Tacoa. Recuperado 28 de octubre de 2019, de https://medium.com/@KVTacoa/red-de-computadoras-e3941854e4d3*
13. *Calameo, C. (2013). Elementos de una red. Recuperado 28 de octubre de 2019, de https://es.calameo.com/read/00057374306306dcd3e53*
14. *Colaboradores de Wikipedia. (2019, 27 mayo). Monitoreo de red. Recuperado 30 de octubre de 2019, de https://es.wikipedia.org/wiki/Monitoreo_de_red*
15. *NORTH, A. (2017, 23 octubre). ¿Que es Nagios? Recuperado 8 de noviembre de 2019, de https://www.north-networks.com/fabricante/que-es-nagios/*
16. *Team, P. F. (2019, 11 enero). Monitoreo de Red. Qué debemos saber. Recuperado 8 de noviembre de 2019, de https://pandorafms.com/blog/es/monitoreo-de-red-que-debemos-saber/*
17. *colaboradores de Wikipedia. (2019b, octubre 24). Op5 Monitor. Recuperado 10 de noviembre de 2019, de https://es.wikipedia.org/wiki/Op5_Monitor*
18. *Sied, G. (2014, 6 febrero). NetworkMiner (Análisis Forense de Red) :: Herramientas. Recuperado 12 de noviembre de 2019, de https://blog.sied.com.ar/2014/02/networkminer-analisis-forense-de-red-herramientas.html*
19. *Blyx, T. (2009, 9 mayo). Adios Nagios, hola Icinga. Recuperado 14 de noviembre de 2019, de https://blyx.com/2009/05/09/adios-nagios-hola-icinga/.*

20. *Luna, D. (2018). Icinga Web 2. Recuperado 18 de noviembre de 2019, de https://icinga.com/docs/icinga-web-2/latest/*
21. *Ocho, D. (2017, 24 abril). Instalar y configurar módulo Graphite en Icingaweb2. Recuperado 26 de noviembre de 2019, de https://www.ochobitshacenunbyte.com/2017/04/24/instalar-y-configurar-modulo-graphite-en-icingaweb2/*
22. Javier, F. P. (2019). Icinga - Manuais Informática - IES San Clemente. Recuperado 18 de diciembre de 2019, de https://manuais.iessanclemente.net/index.php/Icinga