TELECO 3:

Proyecto Final: Monitoreo de infraestructura con Nagios.

# I.INTRODUCCIÓN.

El monitoreo de infraestructura es importante en la gestión de sistemas de TI. Básicamente, se trata de asegurarse de que todos los componentes clave de la tecnología, como los servidores, aplicaciones, servicios, bases de datos y redes, estén funcionando bien y sin problemas. Una de las herramientas más conocidas y usadas para hacer esto se llama Nagios.

Nagios ayuda a los administradores de TI a detectar y solucionar problemas en la infraestructura antes de que los usuarios se den cuenta o se vean afectados. Es como tener un sistema de alerta temprana que te avisa cuando algo no está funcionando correctamente, permitiéndote arreglarlo rápido.

Además, Nagios no solo te avisa cuando hay un problema, sino que también te permite ver cómo han estado funcionando los sistemas a lo largo del tiempo, gracias a sus informes y gráficos.

# II.CONTEXTO (PROBLEMA)

Algunas problemáticas que se pueden abordar y solucionar mediante el uso de Nagios incluyen las siguientes:

Tiempo de Inactividad No Planificado:

Problemática: La infraestructura de TI puede experimentar fallos inesperados que resultan en la caída de servicios críticos.

Rendimiento Degradado:

Problemática: Las aplicaciones y servicios pueden volverse lentos, afectando la experiencia del usuario y la eficiencia operativa.

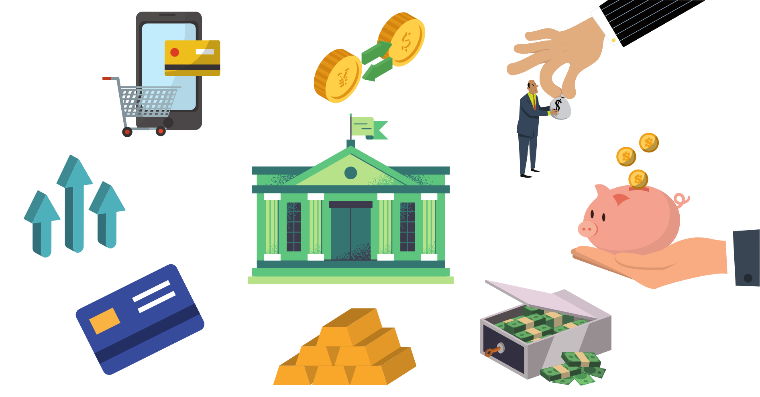
Fallas en Servicios Críticos:

Problemática: Servicios esenciales como bases de datos, servidores web o aplicaciones de negocio pueden fallar, interrumpiendo las operaciones.

Problemas de Conectividad en la Red:

problemática: La pérdida de conectividad en la red puede interrumpir la comunicación entre sistemas y servicios, afectando la operatividad general.

Para el caso del desarrollo de este proyecto se toma una problemática que se pueda evidenciar en un caso real de la vida, una empresa de servicios financieros con sede en Colombia que ofrece una variedad de productos financieros, como cuentas de ahorro, préstamos, tarjetas de crédito y servicios de inversión. Esta empresa depende en gran medida de su infraestructura de TI para gestionar transacciones, almacenar datos confidenciales de los clientes y proporcionar servicios en línea a través de su plataforma digital.



La problemática específica de la empresa es que la empresa experimenta problemas de tiempo de inactividad y rendimiento en su infraestructura de TI de forma periódica. Estos problemas afectan la experiencia del cliente, ralentizan las transacciones.

IV. ALTERNATIVAS DE SOLUCIÓN

Las alternativas de solución son diferentes opciones o estrategias que se pueden emplear para resolver un problema o enfrentar una situación. En el contexto de la toma de decisiones, ingeniería, negocios, tecnología, y prácticamente cualquier disciplina, es fundamental evaluar varias alternativas antes de decidir un curso de acción. Esto permite optimizar los resultados y minimizar los riesgos asociados con cualquier decisión.

algunos ejemplos de alternativas de solución que podrías considerar en distintos contextos usando Nagios, un sistema de monitoreo de red y servidores. Estas alternativas pueden aplicarse cuando enfrentas problemas específicos o deseas optimizar el rendimiento y la funcionalidad de tu infraestructura de monitoreo.

1. Mejora del rendimiento de Nagios en entornos grandes

Problema: Nagios se vuelve lento y menos eficiente a medida que la escala de la red o el número de nodos monitorizados aumenta.

Alternativas de solución:

Distribución de la carga: Utilizar Nagios XI o emplear addons como Mod-Gearman para distribuir las tareas de monitoreo entre múltiples instancias de Nagios.

Optimización de la configuración: Revisar y optimizar la configuración de los checks, intervalos de tiempo y uso de recursos para mejorar el rendimiento sin comprometer la cobertura de monitoreo.

Escalado vertical: Aumentar los recursos del servidor donde se ejecuta Nagios, como CPU y memoria, para manejar cargas más grandes.

2. Reducción de falsos positivos en alertas

Problema: Recibir demasiadas alertas que no corresponden a problemas reales puede llevar a ignorar alertas importantes.

Alternativas de solución:

Ajuste de umbrales: Revisar y ajustar los umbrales de alerta para ser más representativos de problemas reales.

Depuración de scripts: Mejorar la precisión de los scripts y plugins de chequeo para asegurar que detectan adecuadamente las condiciones de error.

3. Integración de Nagios con nuevas tecnologías

Problema: Integrar Nagios con plataformas modernas de IT y nuevas tecnologías puede ser desafiante.

Alternativas de solución:

Plugins modernos: Desarrollar o implementar plugins actualizados que soporten nuevas tecnologías y plataformas como contenedores, microservicios y la nube.

APIs de terceros: Utilizar APIs para integrar Nagios con otras herramientas de gestión y orquestación para una visión más unificada de la infraestructura y operaciones.

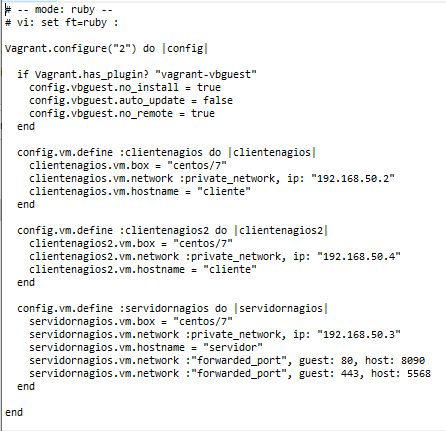
Adopción de herramientas complementarias: Complementar Nagios con otras herramientas de monitoreo que se especialicen en áreas donde Nagios podría ser menos eficiente.

V. DISEÑO DE LA SOLUCIÓN

El diseño propuesto para abordar los desafíos de Coomeva implicó la implementación de Nagios para el monitoreo, utilizando tres máquinas virtuales: un servidor principal y dos clientes Linux, también actuando como servidores. Uno de los clientes aloja Apache y el otro FTP. Las pruebas de rendimiento se realizaron en el cliente con Apache, donde se simuló una carga de 10,000 solicitudes a la página utilizando JMeter. Este enfoque permitió identificar niveles críticos de rendimiento, desde advertencias hasta la eventual falla o ralentización del sistema, lo que refleja situaciones similares a las que enfrenta Coomeva. Para una mejora adicional, podría considerarse la inclusión de pruebas de estrés graduales y medidas de mitigación para analizar la resistencia del sistema y su capacidad de recuperación.

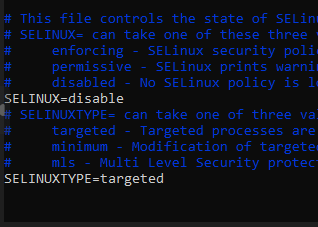
VI. IMPLEMENTACIÓN DE LA SOLUCIÓN

Primero se va a realizar una carpeta donde estará la realización del proyecto, se va al cmd se busca la ruta de la carpeta y se ejecuta el vagrant init, después en esa carpeta se creará un vagrant file ,en este Vagrantfile se configura un entorno con tres máquinas virtuales, dos clientes y un servidor, todas corriendo CentOS 7. Las VMs están en una red privada con IP estáticas asignadas, y el servidor tiene puertos específicos mapeados para acceder a servicios web externamente. Es una configuración útil para simular un entorno de red con un servidor de monitoreo (como Nagios) y clientes en la misma red.

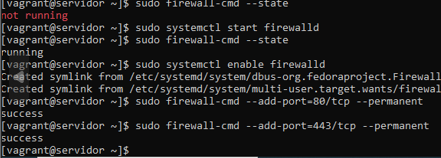


Una vez dado el vagrant up y entrado en vagrant ssh servidornagios se debe Instalar vim y net-tools para poder colocar los comandos de instalación de las dependencias de nagios pero antes de esto se deben realizar dos pasos sumamente importantes los cuales son:

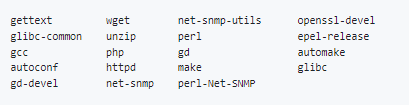
* Deshabilitar SELinux en el directorio: /etc/selinux/config



* Habilitar los puertos 80 y 443, en caso de que el Firewall esté corriendo.



Tras estos pasos, se realizan las configuraciones iniciales del servidor en concreto la instalación de las dependencias necesarias para instalar Nagios.



Despues se obtienen los binarios para compilar Nagios desde un repositorio de github, se descomprimen y una vez descomprimido con CD se entra al directorio de los archivos descomprimidos y se ingresan los siguientes comandos:

./configure

Compilar Nagios con el comando:

make all

Hacer la instalación con:

make install

Continuar con:

make install-commandmode

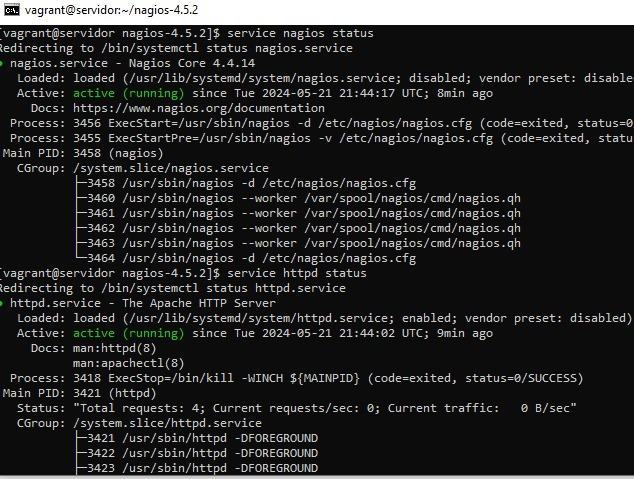
make install-config

make install webconf

Se deben habilitar tanto los servicios de nagios tanto como los de httpd

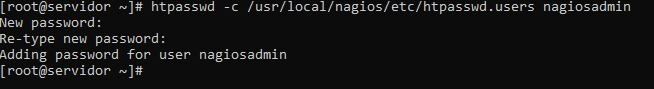


Tambien se activan los servicios nagios y httpd y se puede visualizar su estado para saber si se activaron de la forma correcta.

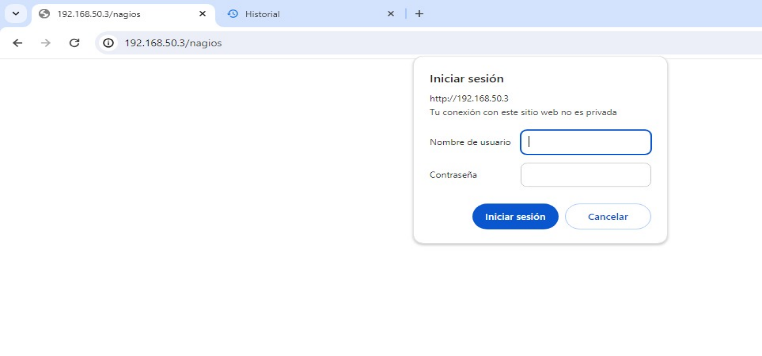


Se crea un usuario nagios con los que se brindara protección para que no cualquiera entre a la pagina, si ya se creo un usuario no es necesario usar el –c debido a que si se usa se sobre escribirá el anteriormente creado por el nuevo, entonces para agregar nuevos simplemente es no usar el comando sin el –c

htpasswd -c/usr/local/nagios/etc/htpasswd.users



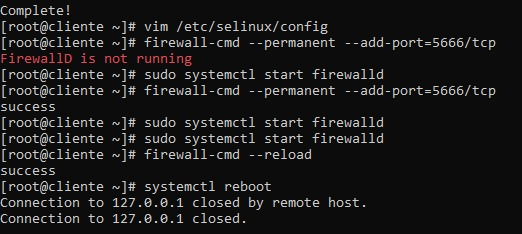
Una vez realizados los pasos anteriormente entramos a nuestro navegador y colocamos 192.168.50.3/nagios para entrar a la página web donde podremos realizar el monitoreo.





Despues se obtiene plugings por medio de github se descomprimen y se instalan y se procede con la instalación de una herramienta fundamental que es el nrpe.

Para instalar NRPE, primero se descarga la versión deseada desde el repositorio oficial de GitHub de Nagios Enterprises. Una vez descargado, descomprime el archivo tar.gz y ejecuta el comando './configure' dentro del directorio descomprimido. Asegúrate de habilitar el puerto 5666 en los clientes donde instalarás NRPE con plugins. Luego, compila el comando 'make check\_nrpe' y el plugin con 'make install-plugin'. Finalmente, dirígete al directorio /usr/local/nagios/etc/objects/ y edita el archivo commands.cfg para definir el comando 'check\_nrpe', que permitirá a Nagios utilizar NRPE con la configuración recién realizada.



En el primer cliente se instalaron los plugins de Nagios y NRPE, además de otras dependencias para la instalación de Nagios. Para el monitoreo del hardware del cliente se creó el archivo check\_mem para el monitoreo de la memoria RAM de este cliente. Este archivo se encuentra dentro del cliente 1 con el nombre de check\_mem.pl. También en el archivo nrpe.cfg del cliente 1 (con path /usr/local/nagios/etc/nrpe.cfg) se tuvo que agregar los siguientes comandos para que se pudiera realizar la revisión de los recursos.

Para configurar el monitoreo básico de los clientes en Nagios, primero definimos los servidores en el archivo 'linux.cfg' ubicado en '/usr/local/nagios/etc/objects/'. Aquí asignamos nombres, alias, direcciones IP y frecuencias de verificación a los hosts, así como la agrupación de los mismos en 'hostgroups'. Luego, definimos los servicios que queremos monitorear, como el espacio en disco, el tiempo de actividad, la carga actual, el intercambio de memoria, la cantidad de usuarios y el ping, utilizando el comando 'check\_nrpe'.

Después, en el archivo de configuración principal de Nagios, 'nagios.cfg', incluimos nuestro archivo recién creado 'linux.cfg' como parte de la configuración. Luego, verificamos la sintaxis de los archivos de configuración de Nagios con el comando '/usr/local/nagios/bin/nagios -v'. También podemos ajustar la tasa de actualización en el archivo 'cgi.cfg'. Finalmente, reiniciamos el servicio de Nagios para aplicar los cambios.

En el lado del cliente, primero ejecutamos 'df -h' para identificar el nombre del disco o la partición que queremos monitorear. Luego, editamos el archivo 'nrpe.cfg' para agregar los comandos específicos de NRPE que se encargan de monitorear el espacio de intercambio y el tiempo de actividad. Si surgen errores con algún comando, podemos depurar ejecutando los comandos desde '/usr/local/nagios/libexec' y observando los mensajes de error. Una vez realizadas estas configuraciones, reiniciamos el servicio NRPE en el cliente para aplicar los cambios.

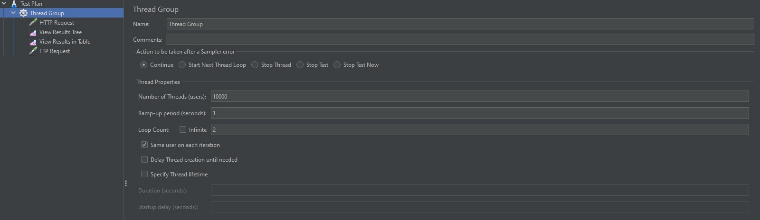
Realizamos una configuración de los clientes linux, solucionamos problemas con el servidor de nagios y se procede a realizar la instalación de la herramienta con la que se obtendran grafico.

Para configurar gráficos con PNP4Nagios en el servidor, primero instala los paquetes necesarios como rrdtool, perl-Time-HiRes, php-gd y php-xml mediante 'yum install'. Luego, descarga PNP4Nagios desde el sitio web oficial y descomprímelo. Accede al directorio descomprimido y ejecuta './configure', 'make all' y 'make fullinstall'. Habilita el servicio de inicio con 'chkconfig npcd on' y reinicia el servicio de Apache. Haz una copia de seguridad del archivo 'install.php' y edita 'nagios.cfg' para habilitar el almacenamiento de datos de rendimiento y su procesamiento. Define comandos en 'commands.cfg' para manejar los archivos de datos de servicios y hosts. Agrega en 'templates.cfg' las definiciones de botones para acceder a PNP4Nagios. Copia el archivo 'status-header.ssi' en el directorio de Nagios para agregar un efecto de hover a los botones. Reinicia los servicios de npcd y Nagios. Por último, en los archivos de configuración de los hosts y servicios, agrega referencias a los botones recién definidos y realiza ajustes en archivos PHP para corregir errores relacionados con JSON. Finalmente, reinicia el servicio de Nagios para aplicar todos los cambios.

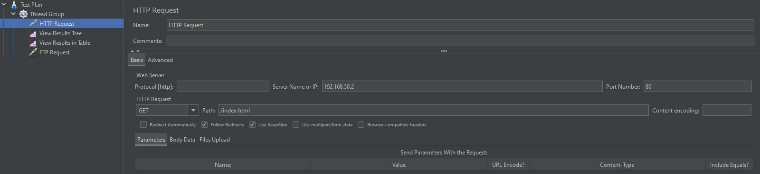
Se utilizo la aplicación jmeter para poder mandar una carga al cliente linux que posee apache para visualizar como afecta esa carga en el rendimiento de la pagina.

VII. IMPLEMENTACIÓN DE LA SOLUCIÓN

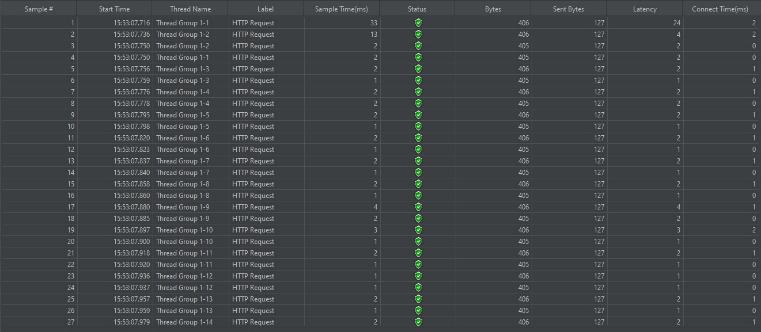
Se define el grupo por el cual se va hacer los envios de peticiones aca se configura el número de peticiones que se quieren realizar, el tiempo de rampa de subida que va a ser de un segundo y las veces que se va repetir la acción la cual serán dos veces con el fin de saturar la carga en el servidor de apache



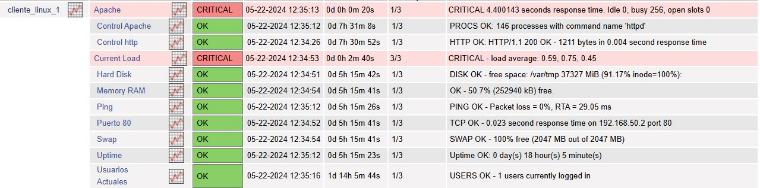
Se configura el http rsqst que es por donde se realizan las peticiones al servidor que tiene el apache, el puerto 80 es el dedicado apache y se le coloca la dirección de ip



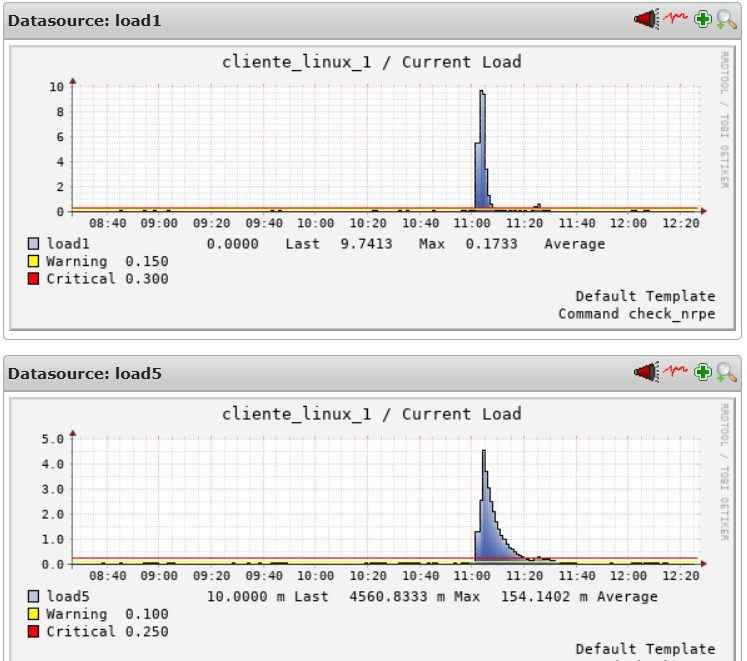
Se hicieron todas la peticiones http rqst y se verifica que la prueba de las 10 mil personas se hizo y esta bien.



Como se puede observar al realizarse las 10.000 peticiones se genera una señal critica debido a que ya se supero el porcentaje que se habia definido para critico y warning.



En esta grafica se puede ver como se supera el número de peticiones los niveles críticos y de warning previamente establecido para las alarmas



IX. DISCUSION DE LAS PRUEBAS

El sistema de monitoreo de infraestructura de Nagios, es una herramienta potente para observar como se comporta una red de equipos que presentan diferentes servicios, o incluso para monitorear un solo equipo, sin embargo no es su uso apropiado, por lo que Nagios resalta su importancia cuando se implementa en redes locales amplias, para este proyecto Nagios sirvió como un referente para poder entender como se comportan los diferentes servicios instalados en servidores, que hemos visto a lo largo del semestre, en nuestro caso particular Apache y VSFTPD, se pudo evidenciar como afecta el trafico de usuarios a una pagina Web y como puede colapsar para no permitir mas el ingreso de usuarios, esto ligado a nuestra problemática planteada nos permite conocer que aspectos se deben y se tienen que fortalecer, para corregir estos errores se puede aplicar el ancho de banda de la carga y descarga de datos por segundo de la pagina, para permitir mas ingreso de usuarios sin colapsar esta misma.

Para el servicio de FTP también se podría aplicar los mismo sobre ampliar el ancho de banda, y en este servicio es mas importante ya que en muchas ocasiones es necesario subir archivos como documentos de identificación, por lo tanto es importante monitoria el Ping y la cantidad de usuarios que pueden montar información, para no perder ningún tipo de información y evitar retrasos, ya que estos servicios se ejecutan mediante tiempos específicos.

VIII. CONCLUSION

* La implementación del proyecto nos ayudó a aplicar los conocimientos adquiridos durante el curso, en donde monitoreamos los servicios de HTTP y FTP para los clientes que se definieron en la configuración de Nagios. También nos brinda la posibilidad de escalar el proyecto a empresas que cuenten con redes medianas o más complejas, el reto puede ser mayor, pero ya vimos que Nagios cuenta con un amplio soporte y una comunidad grande que ofrece soluciones a problemas que se puedan llegar a presentar.
* La generación de reportes y gráficas mediante Nagios brinda una amplia gama de opciones para los administradores de una infraestructura tanto de máquinas como también de redes y servicios en la nube que resultan de gran ayuda en el momento de conocer el estado de una infraestructura sin la necesidad de ejecutar largas líneas de comandos dentro del servidor.
* Nagios, al ser un programa de código abierto, le brinda a las personas y a las empresas una mayor agilidad en la gestión de la tecnología, y una mayor practicidad en la seguridad ya que corre sobre SSL.

X. CONCLUSION

[1]https://www.e-dea.co/blog/que-debe-tener-una-solucionde-monitoreo-de-infraestructura-tecnologica

[2]https://en.wikipedia.org/wiki/Nagios

[3]https://www.edureka.co/blog/nagios-tutorial/#:~:text=Na gios%20runs%20on%20a%20server,SMS%20notifications %20if%20something%20happens.

[4] https://en.wikipedia.org/wiki/VirtualBox

[5] https://www.bujarra.com/nagios-monitorizando-nrpe/

[6]https://www.ochobitshacenunbyte.com/2017/03/28/anadi r-graficas-a-icinga2-con-pnp4nagios/

[7https://www.youtube.com/watch?v=bqFKJzj9UQo&list=PLf0g2cV4iCkE9vRbsSoe5f428zMNlasKd&pp=iAQB

[8] https://www.paessler.com/prtg