

2023

CHECKMK



asirMP - García Velo, Laura

Ies San Clemente

14/04/2023

ÍNDICE

1.	INTRODUCCIÓN	2
a.	Ventajas:	2
2.	CARACTERÍSTICAS	3
3.	COMPONENTES	4
4.	REQUISITOS	4
5.	INSTALACIÓN	4
6.	FUNCIONAMIENTO	6
6.1.	AÑADIR UNA REGLA PARA LAS NOTIFICACIONES DE ALGÚN CAMBIO/ERROR	10
7.	WINDOWS	13
8.	BIBLIOGRAFÍA	15

1. INTRODUCCIÓN

El software de monitoreo se utiliza en las empresas que tienen una red de equipos medianamente grande para así facilitar el trabajo a la hora de saber si tenemos problemas y solucionarlos en el menor tiempo posible.

a. Ventajas:

- Aprovechar al máximo los recursos HW de una empresa.
- Prevención de incidencias y detección de problemas.
- Notificación de posibles problemas.
- Ahorro de costes.
- Ahorro de tiempo.
- Mejorar la satisfacción en atención al cliente.

Checkmk es un software para el monitoreo de infraestructuras de TI (*tecnología de la información*). Se utiliza para el monitoreo de:

- Servidores
- Aplicaciones de software
- Redes
- Infraestructuras en la nube
 - Públicas
 - Privadas
 - Híbridas
- Contenedores
- Almacenamiento de datos
- Bases de datos
- Sensores

Este programa nos sirve tanto para instalar un servidor en linux como en Windows al igual que para añadir a el un cliente.

El checkmk se creó en 2008 como un agente que sustituye al shell script para Inetd (demonio presente en la mayoría de sistemas de tipo Unix, conocido como el Super

Servidor de Internet) y se publicó en abril de 2009 bajo la GPL (Licencia Pública General).

Mientras que en el pasado checkmk fue diseñado para monitorear entornos locales grandes y heterogéneos, desde la versión 1.5+ también admite el monitoreo de los servicios de AWS, Azure, Docker y Kubernetes.

Está siendo desarrollado por tribe29 en Munich Alemania que operaba bajo el nombre de Mathias Kettner GmbH hasta el 16 de abril de 2019. Al hacer el cambio de nombre de la compañía, el nombre del producto ha pasado de ser "Check_MK" a ser "Checkmk"

2. CARACTERÍSTICAS

- Checkmk se divide en tres ediciones:
 - Edición de código abierto (Checkmk Raw Edition - CRE)
 - Edición comercial empresarial (Checkmk Enterprise Edition - CEE)
 - Edición comercial para proveedores de servicios administrados (Edición Checkmk Manager Services - CME)
- Todas las ediciones están disponibles en una variedad de plataformas, para varias versiones de Debian, Ubuntu, SLES, RedHat / CentOS y también como una imagen Docker.
- Se ofrecen dispositivos físicos de varios tamaños, así como un dispositivo virtual para simplificar la administración del sistema operativo subyacente usando una interfaz gráfica de usuario, para obtener soluciones de alta disponibilidad.
- Los agentes utilizados por checkmk para recopilar datos están disponibles para once plataformas, incluido windows.
- Combina tres tipos de monitoreo de TI:
 - Monitoreo basado en el estado: registra la salud de un dispositivo o aplicación.
 - Monitoreo basado en métricas: permite el registro y análisis gráfico de series temporales.
 - Monitoreo basado en registros y eventos.

3. COMPONENTES

- Núcleo de supervisión (Ckeckmk Microcore -CMC).
- Configuración y motor de verificación.
- Interfaz de datos (Livestatus).
- Web-GUI (Multisite).
- Administración web (WATO).
- Sistema de alerta.
- Inteligencia de negocios (BI).
- Consola de eventos.
- Gráficos de métricas.
- Reportes.
- Inventario de hardware / software.

4. REQUISITOS

Para utilizar un servidor ubuntu debe estar al menos en la versión 16.04 o superior.

Se necesita a mayores de un servidor, un cliente. Este lo necesitamos para descargar el paquete checkmk y enviarlo a nuestro servidor ya que este será sin interfaz gráfica.

5. INSTALACIÓN

Configuramos tanto el servidor como el cliente en la misma red NAT.

Empezamos con la descarga en el servidor debian sin interfaz gráfica:

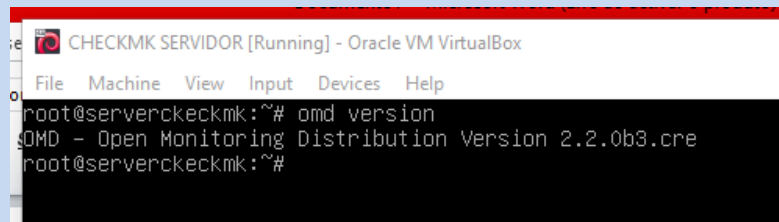
- Nos logueamos como root y ejecutamos los siguientes comandos:
 - Descargar el paquete:

```
wget https://download.checkmk.com/checkmk/2.2.0b3/check-mk-raw-2.2.0b3_0.bullseye_amd64.deb
```
 - Instalar el paquete:

```
apt install ./check-mk-raw-2.2.0b3_0.bullseye_amd64.deb
```

- Comprobar si la instalación se completó:

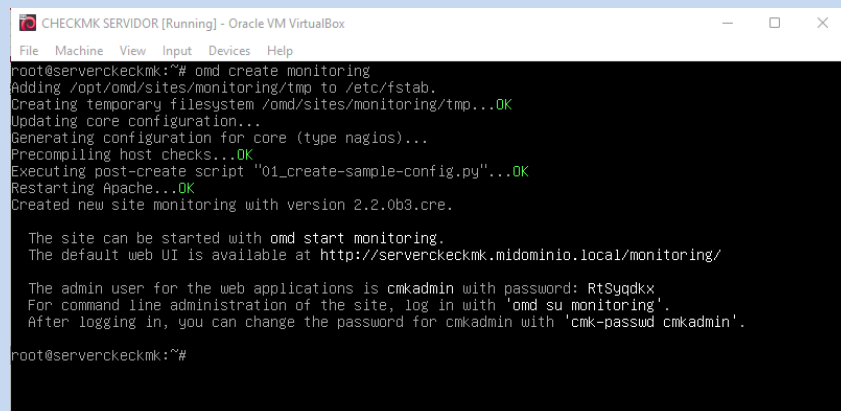
omd version



```
CHECKMK SERVIDOR [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@serverckeckmk:~# omd version
OMD - Open Monitoring Distribution Version 2.2.0b3.cre
root@serverckeckmk:~#
```

- Crear un sitio de monitoreo, en nuestro caso se llamará monitoring pero pueden ponerle el nombre que quieran. Este comando nos va a proporcionar la ruta de acceso a nuestro sitio así como el usuario y contraseña de acceso:

omd create monitoring



```
CHECKMK SERVIDOR [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@serverckeckmk:~# omd create monitoring
Adding /opt/omd/sites/monitoring/tmp to /etc/fstab.
Creating temporary filesystem /omd/sites/monitoring/tmp...OK
Updating core configuration...
Generating configuration for core (type nagios)...
Precompiling host checks...OK
Executing post-create script "01_create-sample-config.py"...OK
Restarting Apache...OK
Created new site monitoring with version 2.2.0b3.cre.

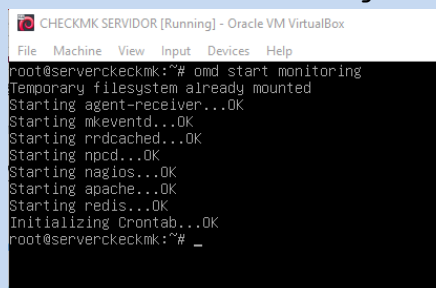
The site can be started with omd start monitoring.
The default web UI is available at http://serverckeckmk.midominio.local/monitoring/

The admin user for the web applications is cmkadmin with password: RtSygdKx.
For command line administration of the site, log in with 'omd su monitoring'.
After logging in, you can change the password for cmkadmin with 'cmk-passwd cmkadmin'.

root@serverckeckmk:~#
```

- Iniciar el sitio

omd start monitoring

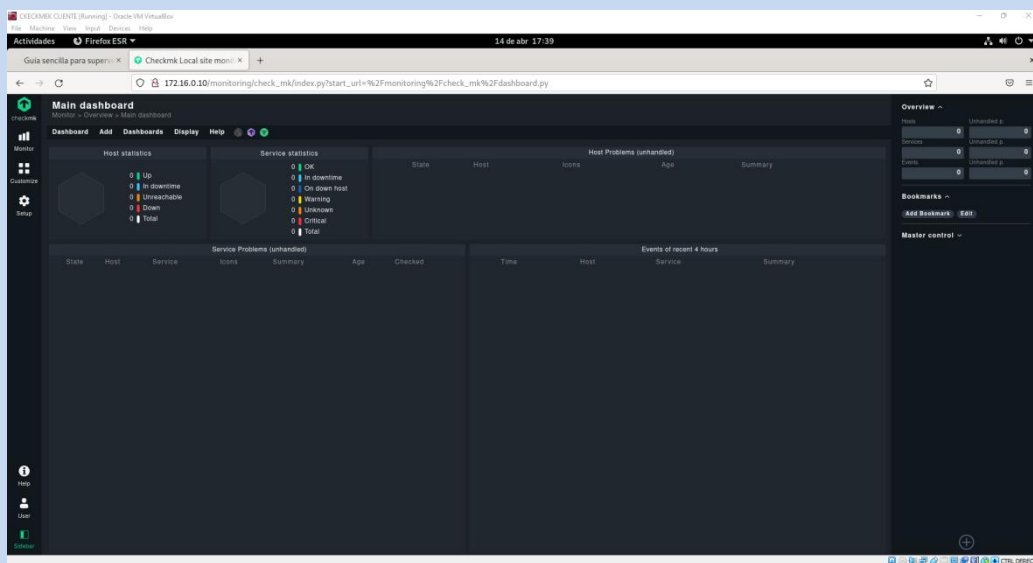


```
CHECKMK SERVIDOR [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@serverckeckmk:~# omd start monitoring
Temporary filesystem already mounted
Starting agent-receiver...OK
Starting mkeventd...OK
Starting rrdcached...OK
Starting npcd...OK
Starting nagios...OK
Starting apache...OK
Starting redis...OK
Initializing Crontab...OK
root@serverckeckmk:~# _
```

Una vez terminada la instalación y configuración podemos acceder a nuestro sitio a través del cliente, para ello tenemos que poner la siguiente ruta en el navegador:

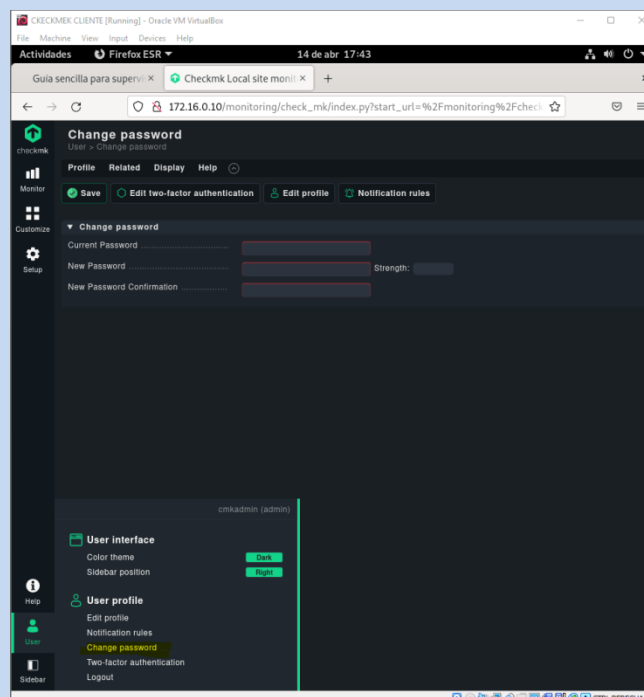
<http://nuestroservidor/monitoring>

Esta viene siendo la ruta proporcionada anteriormente por el comando de creación del sitio.



6. FUNCIONAMIENTO

Lo primero que deberíamos hacer al iniciar sesión sería cambiar la contraseña y poner una contraseña fácil de recordar y segura.



Para volver a inicio pulsamos en el icono de Checkmk (arriba a la izquierda).

La primera vez que iniciamos sesión vemos que el panel está bastante vacío, esto se debe a que no estamos monitorizando nada.

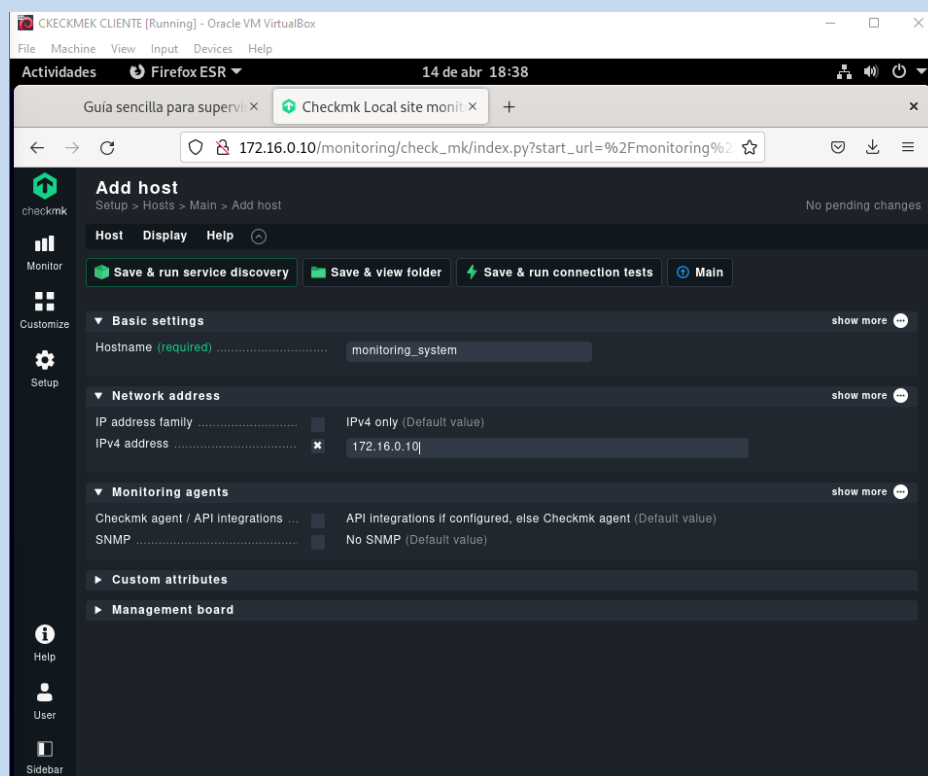
Nos vamos a *setup-agentes-linux* para descargar el paquete que nos permitirá monitorizar nuestro servidor. En *packaged agents* seleccionamos el *.deb*, lo descargamos y luego lo copiamos al servidor a través de ssh y con los siguientes comandos:

```
scp /home/usuario/Descargas/check-mk-agent_2.2.0b3-1_all.deb
usuario@172.16.0.10:/checkmk/
```

Una vez copiado en el servidor, accedemos a él y lo instalamos con:

```
apt install /checkmk/check-mk-agent_2.2.0b3-1_all.deb
```

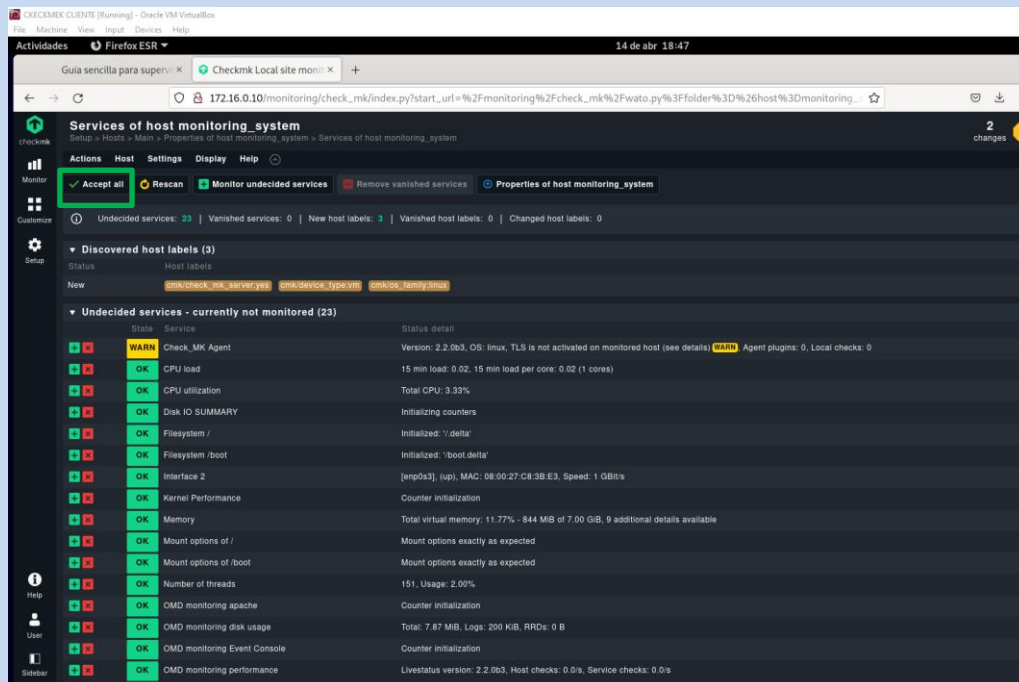
A continuación nos vamos a *setup -> hosts -> add host*



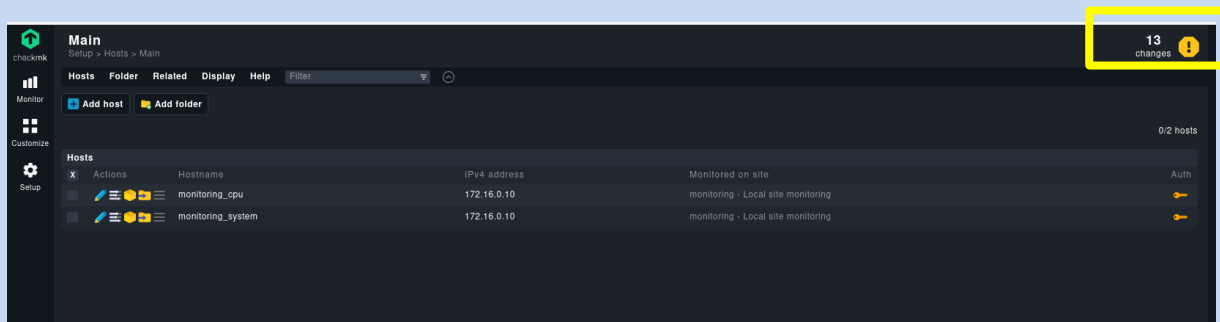
Save & run service discovery, luego de esto, nos muestra los servicios que podemos monitorizar, si le damos a la x los descartamos de la lista y si le damos al + es que lo queremos monitorizar.

Si no seleccionamos ninguno ni descartamos ninguno y le damos a accept all nos monitoriza todos los servicios de la lista.

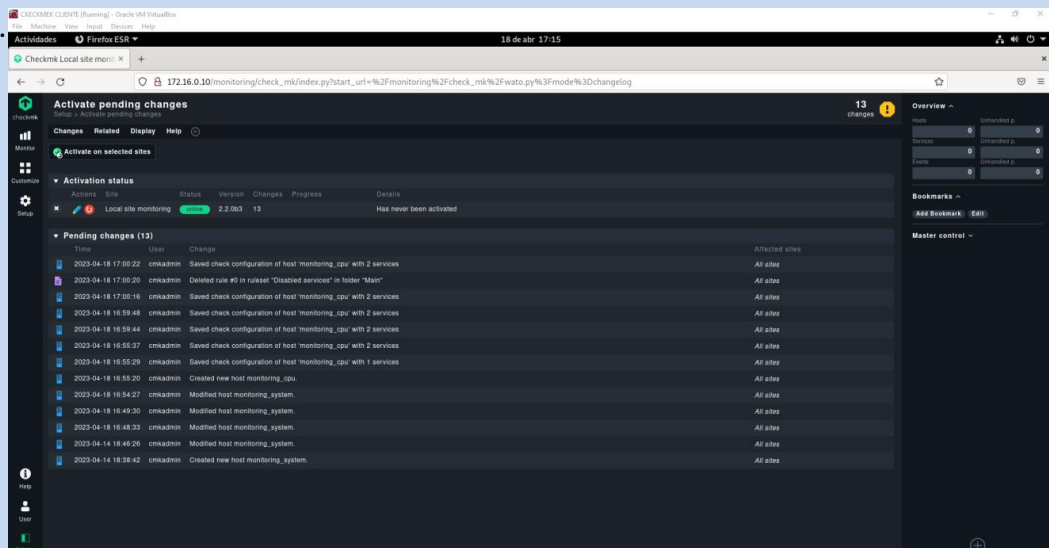
Una vez decidido lo que queremos monitorizar clicaremos sobre accept all si no seleccionamos ningún servicio, sino basta con seleccionar los que queremos y aplicar los cambios.

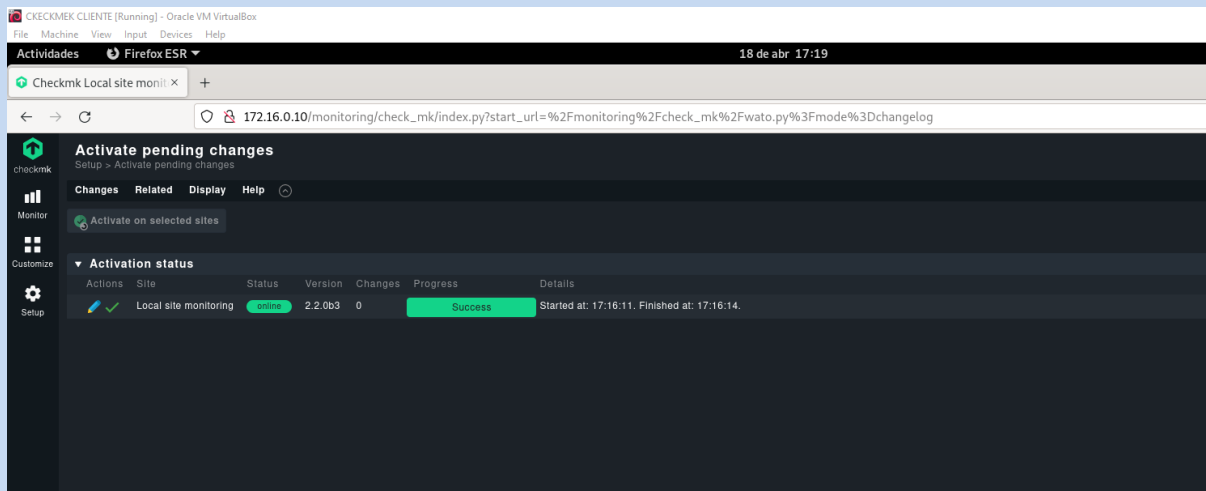


En el icono amarillo que nos aparece arriba a la derecha y que pone 13 cambios es en el que tenemos que pulsar si queremos aplicar los cambios hechos hasta el momento.

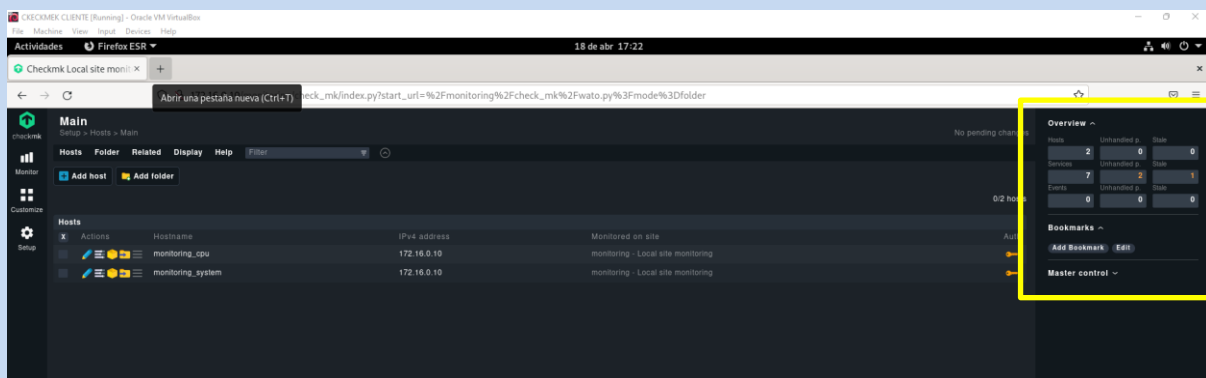


Al clicar en él nos sale está otra ventana en la cual nos aparecen todos los cambios por aplicar. Si clicamos sobre activar en sitios seleccionados se nos aplicaran todos los cambios realizados.

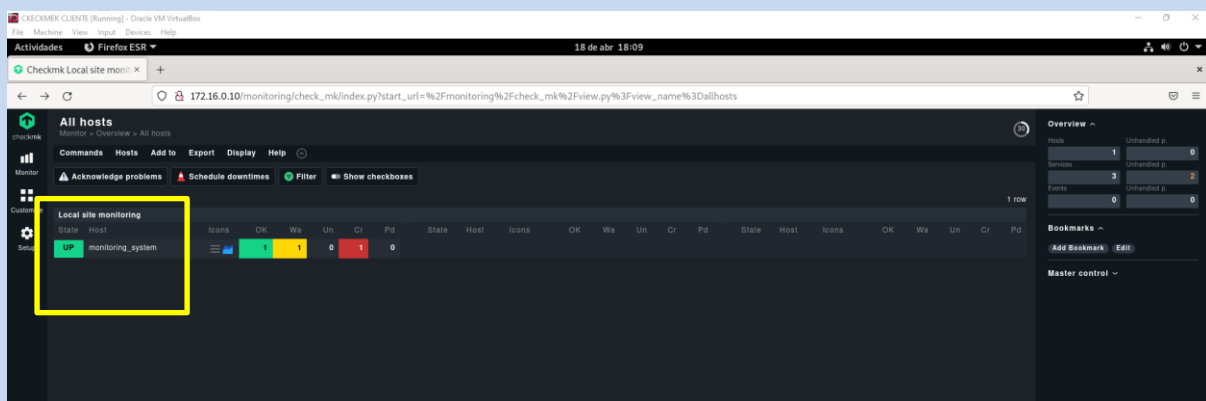


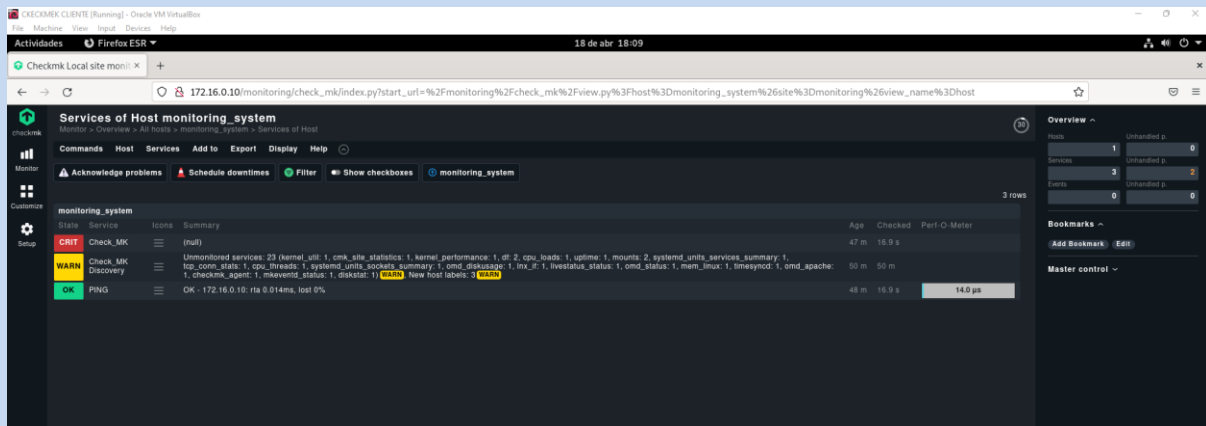


En la parte superior derecha podemos ver todo lo que tenemos activo, como por ejemplo que estamos monitorizando 7 servicios.

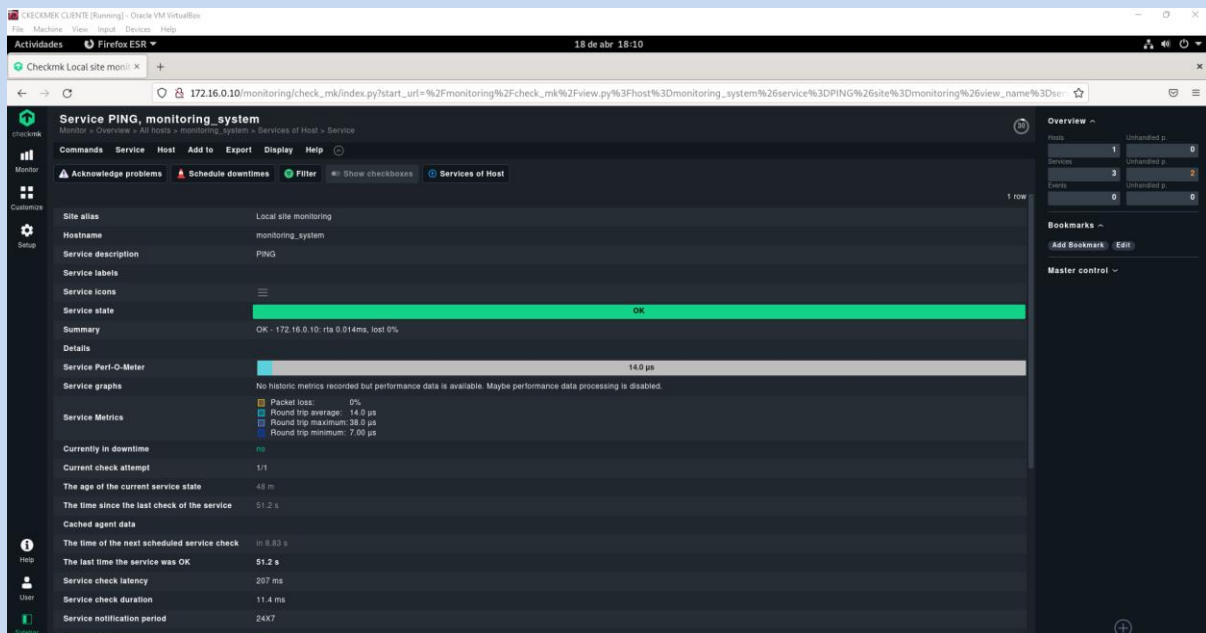


Se puede pulsar sobre cada número de lo que estamos monitorizando y al hacer esto accederemos a una descripción general donde veremos todos los hosts, servicios... en nuestro sistema. Actualmente tenemos un host y si pinchamos sobre el nombre podemos ver los todos los servicios que lo componen.





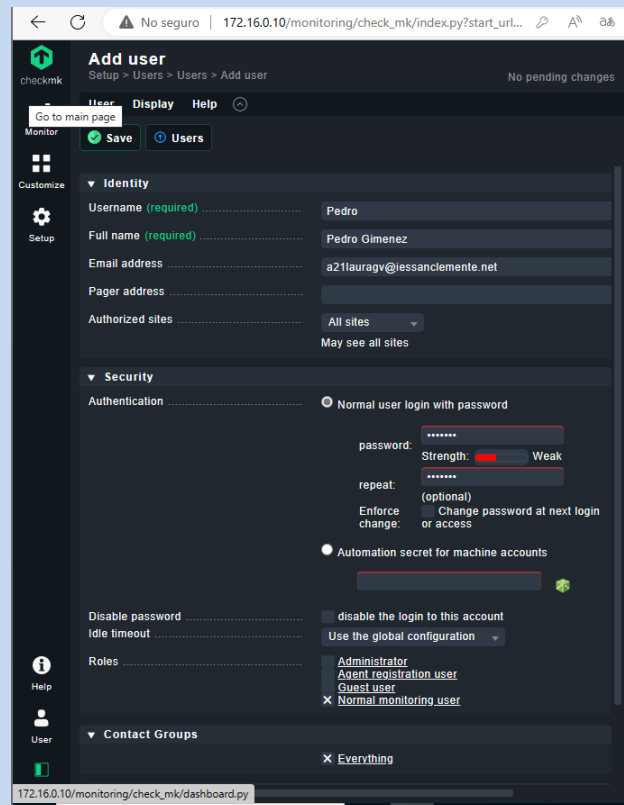
Si clicamos en uno de los servicios podemos ver más datos sobre él pero como de momento llevamos poco tiempo monitorizando no hay muchos datos que mostrar, con el paso del tiempo irán apareciendo más.



6.1. AÑADIR UNA REGLA PARA LAS NOTIFICACIONES DE ALGÚN CAMBIO/ERROR

a. Añadir un usuario

Setup -> users -> users -> add user



b. Instalar exim4 en el servidor:

```
apt install exim4
```

c. Reconfigurar exim4:

```
dpkg-reconfigure exim4-config
```

i. Opciones:

- (1) El correo se envía mediante un «smarthost»; **se recibe a través de SMTP**
- (2) Nombre del sistema de correo: **tudominio.xxx**
- (3) Direcciones IP en las que recibir conexiones SMTP entrantes: **127.0.0.1**
- (4) Otros dominios para los que se acepta el correo: **en blanco**
- (5) Máquinas para las cuales reenviar correo: **en blanco**
- (6) Direccion IP o nombre del equipo (smarthost) saliente: **smtp.gmail.com::587**
- (7) Desea ocultar el nombre de correo local en los mensajes salientes? **NO**
- (8) Limitar el numero de consultas DNS (Marcación bajo demanda)? **NO**
- (9) Dividir la configuración en pequeños ficheros? **Sí**

d. Editar el siguiente fichero:

```
nano /etc/exim4/passwd.client
```

i. En él añadiremos el siguiente contenido:

```
gmailsmtp.1.google.com:yourAccountName@gmail.com:y0uRpaSsw0RD
*.google.com:yourAccountName@gmail.com:y0uRpaSsw0RD
smtp.gmail.com:yourAccountName@gmail.com:y0uRpaSsw0RD
```

- e. Cambiar los permisos del archivo anterior:

```
chown root:Debian-exim /etc/exim4/passwd.client
```

- f. Reiniciar el servicio:

```
/etc/init.d/exim4 restart
```

- g. Cambiar en la cuenta de correo-e que vamos a utilizar para enviar los correos:

Gestionar tu cuenta de google -> seguridad -> aplicaciones menos seguras:
activado

- h. Probar que funciona:

```
echo "content" | mail -s test-subject harry.hirsch@example.com
```

- i. Añadir la regla:

```
setup -> events -> notifications -> add rule
```

Edit notification rule 0
Setup > Events > Notification configuration > Edit notification rule 0 No pending changes

Notification rule Display Help

Save Notification configuration

Rule properties

Description Notify all contacts of a host/service via HTML email

Comment

Documentation URL

Rule activation do not apply this rule

Overriding by users ☒ allow users to deactivate this notification

Notification method

Notification Method HTML Email

Create notification with the following parameters:

- From
- Reply to
- Subject for host notifications
- Subject for service notifications
- Display additional information
- Add HTML section above table (e.g. title, description)
- URL prefix for links to Checkmk
- Display graphs among each other
- Notification sort order for bulk notifications
- Send separate notifications to every recipient
- Graphs per notification (default: 5)
- Bulk notifications with graphs (default: 5)

Notification Bulking ☐

Contact selection

All contacts of the notified object ☒ Notify all contacts of the notified host or service.

All users ☐ Notify all users

All users with an email address ☐ Notify all users that have configured an email address in their profile

The following users

- j. Probar que funciona dicha regla, para ello vamos a tirar un host que está levantado:

Monitor -> overview -> all hosts -> comandos -> fake check results (le damos a los tres puntitos para que aparezca)

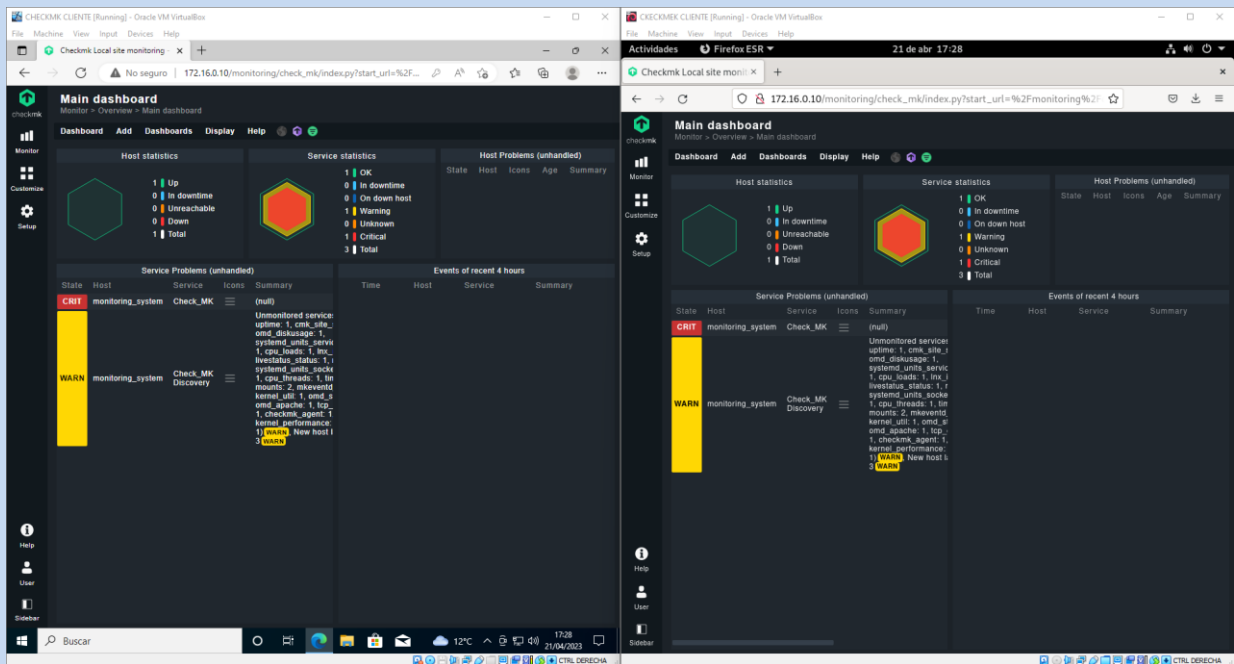
Clicamos sobre *down* y nos debería llegar una notificación a nuestro correo-e seleccionado.

7. WINDOWS

Si queremos monitorizar desde un cliente Windows simplemente basta con ponerlo en la misma red y poner en el buscador del navegador la siguiente url:

`http://nuestroservidor/monitoring`

Una vez iniciado vamos a visualizarlo de la misma forma que en nuestro cliente linux.



Para monitorizar a un cliente windows nos vamos a *setup-agentes-windows* para descargar el paquete que nos permitirá monitorizarlo. En *packaged agents* seleccionamos el *.msi* y una vez descargado lo ejecutamos.

Dejamos todas las opciones por defecto en la instalación.

Una vez instalado debemos acceder a nuestro programa de monitoreo, lo podemos hacer desde nuestro cliente linux o desde nuestro cliente windows, como prefiramos.

A continuación nos vamos a *setup -> hosts -> add host*.

Al añadir un nuevo host nos va a pedir que le digamos cuales son los servicios que queremos monitorizar.

A partir de este punto es todo exactamente igual que para el monitoreo de Linux.

En este caso como le he dado a monitorizar todos los servicios de la lista nos aparecerá de la siguiente forma:

checkmk

Monitor

Customize

Setup

Help

User

Support

Checkmk Local site monitor

172.16.0.10/monitoring/check_mk/index.py?start_url=%2Fmonitoring%2Fcheck_mk%2Fview.py%3Fhost%3Dmonitoring_cliente_windows%26site%3Dmonitoring%26view_name%3Dhost

Services of Host monitoring_cliente_windows

Monitor > Overview > All hosts > monitoring_cliente_windows > Services of Host

Commands Host Services Add to Export Display Help

Acknowledge problems Schedule downtimes Filter Show checkboxes monitoring_cliente_windows

19 rows

State	Service	Icons	Summary	Age	Checked	Perf-O-Meter
OK	Check_MK		[agent] Success, [piggyback] Success (but no data found), execution time 1.4 sec	6 m	37.4 s	1.45 s
WARN	Check_MK Agent		Version: 2.2.0b3, OS: windows, TLS is not activated on monitored host (see details) WARN Agent plugins: 0, Local checks: 0	6 m	35.4 s	
WARN	Check_MK Discovery		Unmonitored services: 1 (dotnet_clrmemory: 1) WARN All host labels up to date	4 m	4 m	
OK	CPU utilization		Total CPU: 1.81%	5 m	35.4 s	1.81%
OK	Disk IO SUMMARY		Read: 120 KiB/s, Write: 572 KiB/s, Latency: 1 millisecond	5 m	35.5 s	116.99 KiB/s / 559.03 KiB/s
OK	Filesystem C:/		Used: 44.56% - 22.1 GiB of 49.5 GiB, trend per 1 day 0 hours: +22.2 GiB, trend per 1 day 0 hours: +44.80%, Time left until disk full: 1 day 5 hours	5 m	35.5 s	44.56%
OK	Interface 1		[Intel(R) PRO 1000 MT Desktop Adapter], (Connected), Speed: 1 GB/s, In: 114 B/s (<0.01%), Out: 533 B/s (<0.01%)	6 m	35.5 s	914 bits / 4.26 kbit/s
CRIT	Log Application		1 CRIT messages (Last worst: "Apr 25 16:43:32 32768 264 Microsoft-Windows-Defrag El optimizador de almacenamiento no pudo completar volver a optimizar en Windows (C:) debido a El hardware del volumen no admite la operación solicitada. (0x8900002A)")	6 m	35.5 s	
OK	Log HardwareEvents		No error messages	6 m	35.5 s	
OK	Log Internet Explorer		No error messages	6 m	35.5 s	
OK	Log Key Management Service		No error messages	6 m	35.5 s	
OK	Log Security		No error messages	6 m	35.5 s	
WARN	Log System		1 WARN messages (Last worst: "Apr 25 16:46:13 0.10016 DCOM establecido de forma predeterminada en el equipo Local Activación (C2F03A33-21F5-47FA-B4B8-156362A3F239) (316CDE05-E4AE-4B15-9113-7055084DC097) CLIENTE2 Juan S-1-5-21-520473904-1238116915-3872693859-1000 LocalHost (con LRPC) Microsoft Windows ShellExperienceHost 10.0.15041.1023 neutral neutral cs5n1h23tyray S-1-15-2-155514346-2573954481-755741238-1654018636-123331829-3075935687-2861478708")	215 s	35.5 s	
OK	Log Windows PowerShell		No error messages	6 m	35.5 s	
OK	Memory		RAM: 65.47% - 1.31 GiB of 2.00 GiB, Commit charge: 55.50% - 1.73 GiB of 3.12 GiB	6 m	35.5 s	65.47%
OK	Processor Queue		15 min load: 12.49, 15 min load per core: 6.24 (2 logical cores)	6 m	35.5 s	0
OK	Service Summary		Autostart services: 59, Stopped services: 4	6 m	35.5 s	
OK	System Time		Offset: -956 milliseconds	6 m	35.5 s	-956 ms
OK	Uptime		Up since Apr 25 2023 16:25:58, Uptime: 23 minutes 42 seconds	6 m	35.5 s	23 m

Overview

Hosts: 2 Unhandled p: 1

Services: 22 Unhandled p: 2

Events: 0 Unhandled p: 0

Bookmarks

Add Bookmark Edit

Master control

8. BIBLIOGRAFÍA

https://es.wikipedia.org/wiki/Check_MK

<https://checkmk.com/download?method=cmk&edition=cre&version=2.2.0b3&platform=debian&os=bullseye&type=cmk>

<https://pandorafms.com/blog/es/monitorizacion-de-sistemas/>

<https://cwflores.wordpress.com/2010/11/04/utilizando-exim4-en-debian-para-enviar-mensajes-a-traves-de-gmail/>

<https://docs.checkmk.com/latest/en/notifications.html>

<https://docs.checkmk.com/latest/en/commands.html>