



Monitoreo de redes **OBSERVIVUM**



Enero 2024

Saioa De la Torre Abad

ÍNDICE

Introducción	03
Instalación de Observium	04
Activar protocolo SNMP	06
• Mikrotik	06
• Windows	08
Entrar a Observium	11
Añadir equipos	12
Crear alertas	12
• Host caído	15
• Almacenamiento	16
• Memoria	17
• CPU	18

¿QUÉ ES OBSERVIVUM?

En el siguiente documento vamos a hablar sobre el monitoreo de redes gracias al software Observium.

Este software (Observium) como otros que monitorizan redes usan el protocolo SNMP que forma parte del nivel de aplicación del modelo TCP/IP.

Vamos a usarlo para tener controlado diferentes dispositivos de la red independientemente del fabricante que sea.

Para ello deberemos de saber que dispositivos tenemos en la red para que en el momento que tengamos el Observium en marcha saber que dispositivos añadir.

¿QUÉ ES EL PROTOCOLO SNMP?

Antes que nada deberemos de saber que es el protocolo SNMP.

El protocolo SNMP es un protocolo usado para la gestión de la red. Es un protocolo de nivel de aplicación. Con este protocolo se puede supervisar, gestionar y controlar el acceso de los dispositivos remotamente.

INSTALACIÓN DE OBSERVIVUM

La instalación de Observium la realizaremos en una máquina virtual con un sistema operativo Ubuntu.

Con el comando “`wget http://www.observium.org/observium_installscript.sh`” descargaremos el script que nos permitirá instalar el Observium.

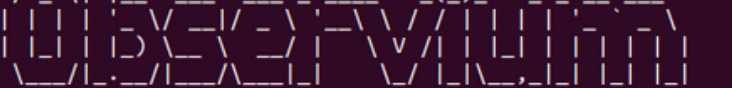
```
inetcom@inetcom:~$ wget http://www.observablehq.com/observablehq_installscript.sh
--2024-01-31 08:41:03-- http://www.observablehq.com/observablehq_installscript.sh
Resolving www.observablehq.com (www.observablehq.com)... 144.76.112.154
Connecting to www.observablehq.com (www.observablehq.com)|144.76.112.154|:80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.observablehq.com/observablehq_installscript.sh [following]
--2024-01-31 08:41:09-- https://www.observablehq.com/observablehq_installscript.sh
Connecting to www.observablehq.com (www.observablehq.com)|144.76.112.154|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 21606 (21K) [text/x-sh]
Saving to: 'observablehq_installscript.sh'

observablehq_installscript.sh      100%[=====>] 21.10K  --.-KB/s  in 0.1s

2024-01-31 08:41:09 (201 KB/s) - 'observablehq_installscript.sh' saved [21606/21606]
```

Ejecutamos el script `./observium_installscrip.sh`

```
root@inetcom:/home/inetcom# ./observium_installscrip.sh
```



```
Welcome to Observium automatic installscrip v0.2.3

Please choose which version of Observium you would like to install

1. Observium Community Edition
2. Observium Pro/Ent Edition stable (requires account at https://www.observium.org/subs/)
3. Observium Pro/Ent Edition rolling (requires account at https://www.observium.org/subs/)
4. Install the UNIX-Agent
5. Install the SNMPD (snmpd-config will be overwritten)
(1-5):
```

Damos siguiente y siguiente.

Configuración de paquetes

Configuración de grub-pc

El gestor de inicio GRUB se instaló previamente en un disco que ya no está presente o cuyo identificador único ha cambiado por alguna razón. Es importante asegurarse de que la imagen del núcleo de GRUB instalada se mantiene sincronizada con los módulos de GRUB y el fichero «grub.cfg». Asegúrese que GRUB se instala en los dispositivos de inicio adecuados.

Si no está seguro cuál es la unidad de inicio de la BIOS, a menudo es una buena idea instalar GRUB en todas ellas.

Nota: también es posible instalar GRUB en los registros de inicio de particiones, aquí se ofrecen algunas particiones apropiadas. Sin embargo, esto obliga a GRUB a utilizar el mecanismo de la lista de bloqueo, que lo hace menos fiable, y por tanto no es recomendable.

<Aceptar>

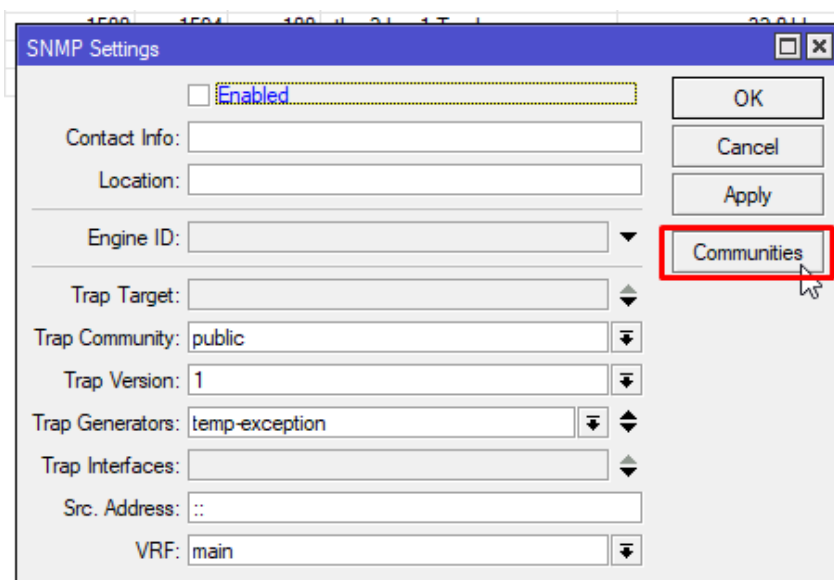
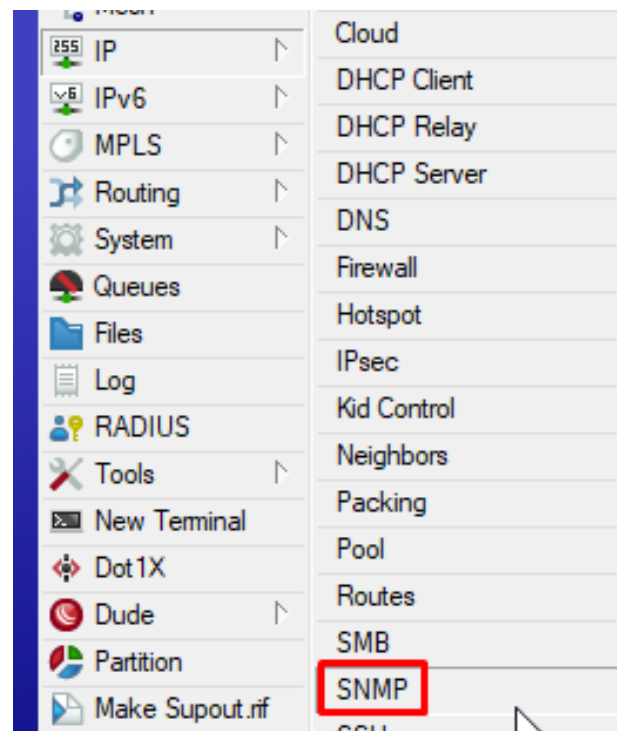
En algún punto nos pedirá introducir una contraseña de root.

Y con esto podemos dar por finalizada la instalación de Observium.

Antes de ponernos a configurar el Observium vamos a activar el protocolo SNMP en los diferentes dispositivos que vamos a monitorizar.

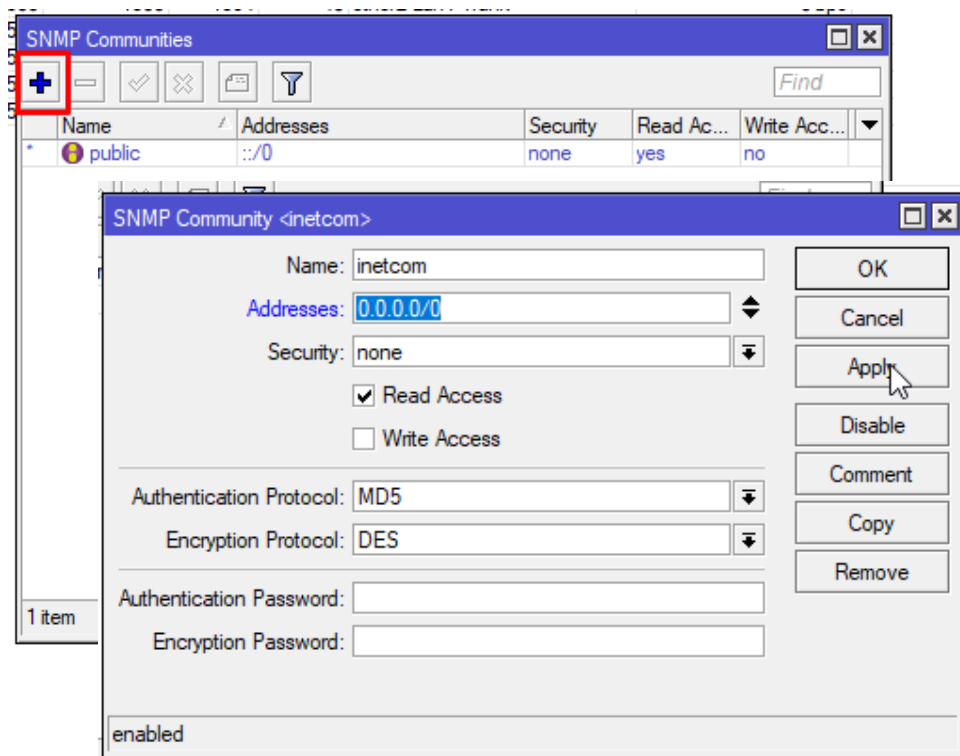
ACTIVAR EL PROTOCOLO SNMP EN MIKROTIK

Para activar el protocolo de SNMP en Mikrotik debemos ir a IP -> SNMP

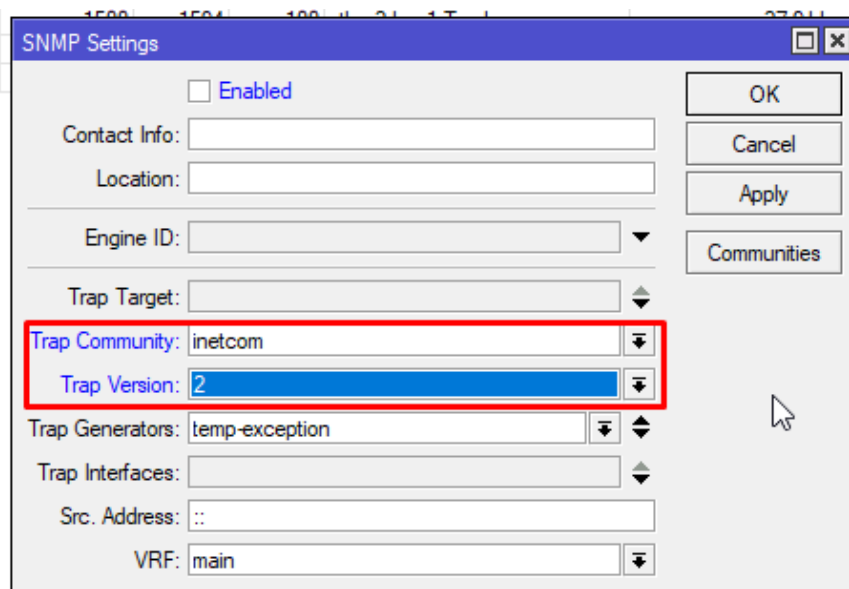


Debemos ir a **Comunities** que es donde configuraremos el nombre de comunidad que tendrá nuestra red.

Daremos al plus macado en la foto y añadimos el nombre de la comunidad que aquí es "inetcom" y le damos a aplicar.



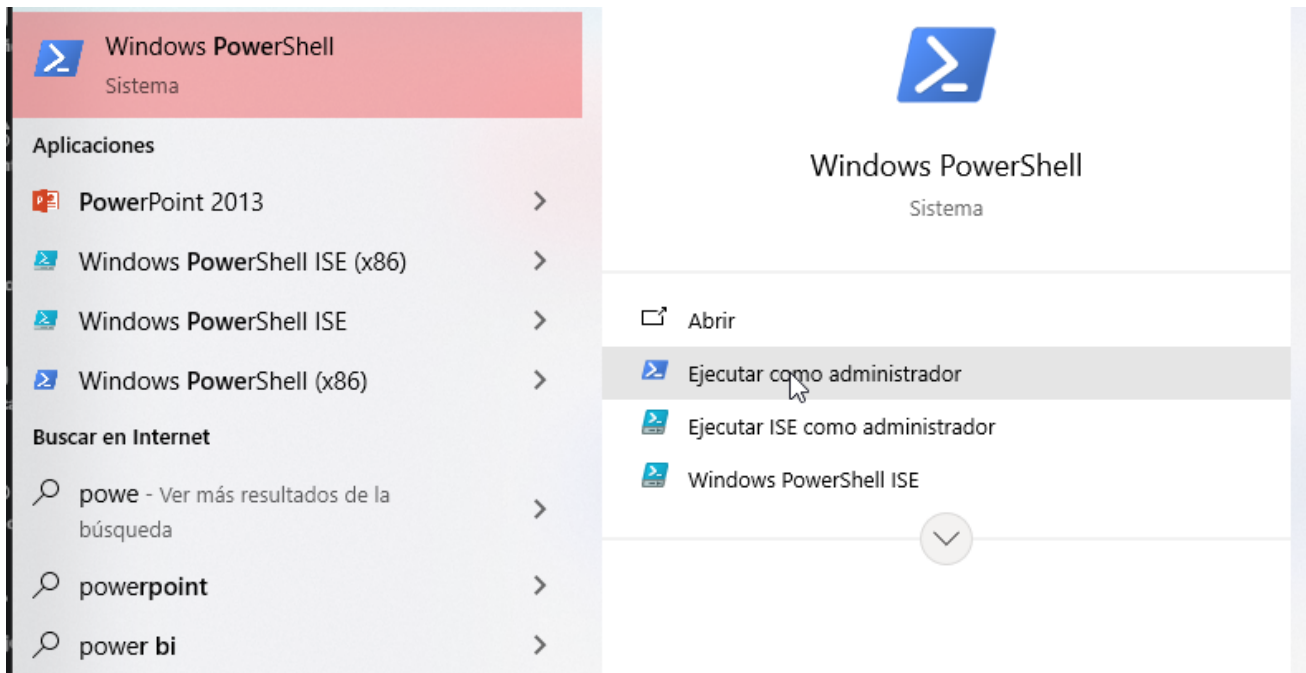
Volvemos a la ventana anterior y en Trap Community seleccionamos la comunidad que acabamos de crear.



Y con esto estaría activado el SNMP en Mikrotik.

ACTIVAR EL PROTOCOLO SNMP EN WINDOWS

Abriremos el powershell en modo administrador



Una vez dentro del powershell pondremos el siguiente comando:

```
get-windowscapability -Online -Name "SNMP*"
```

```
PS C:\WINDOWS\system32> get-windowscapability -Online -Name "SNMP*"
```

Con este comando nos indicara si tenemos o no instalado SNMP en nuestro equipo.

State:

- NotPresent: No esta instalado
- Installed: Ya lo tenemos

```
PS C:\WINDOWS\system32> get-windowscapability -Online -Name "SNMP*"

Name       : SNMP.Client~0.0.1.0
State      : NotPresent
DisplayName : Protocolo simple de administración de redes (SNMP)
Description : Esta característica incluye los agentes de Protocolo simple de administración de redes (SNMP) que supervisan la actividad en los dispositivos de red y notifican a la estación de trabajo de la consola de red
DownloadSize : 596276
InstallSize : 1153358
```


En el caso de que no este instalado introduciremos el siguiente comando.

```
Add-WindowsCapability -Online -Name "SNMP.Client~~~~0.0.1.0"
```

Y comenzara a instalarse.

```
PS C:\WINDOWS\system32> Add-WindowsCapability -Online -Name "SNMP.Client~~~~0.0.1.0"

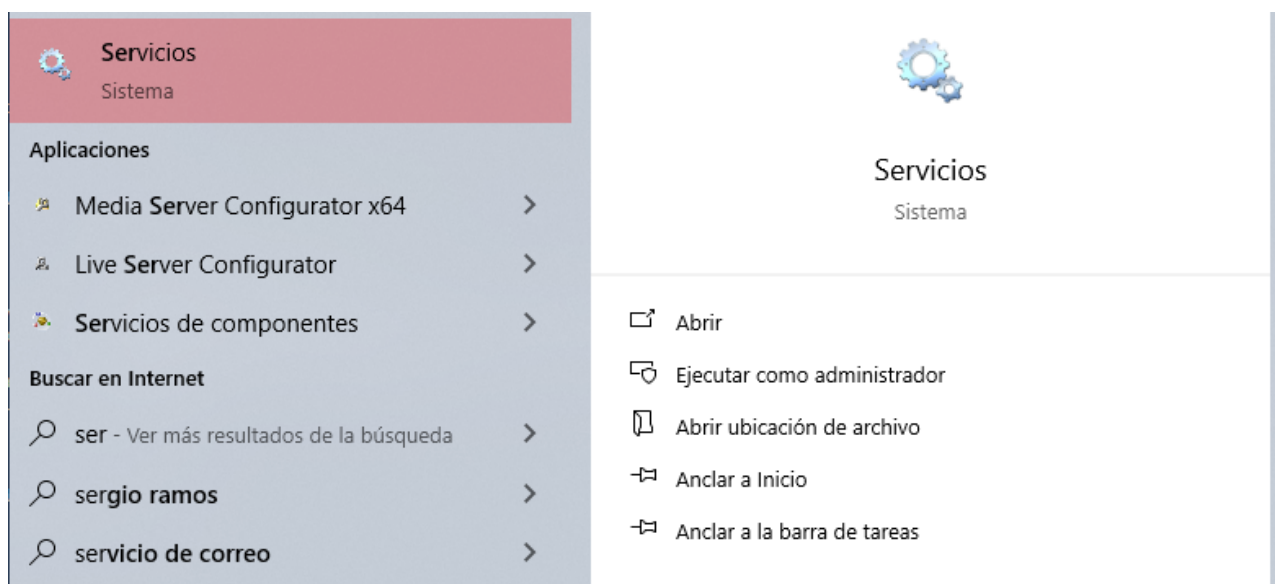
Path           :
Online         : True
RestartNeeded  : False
```

Una vez instalado volvemos a poner el comando del principio para verificar que se ha instalado.

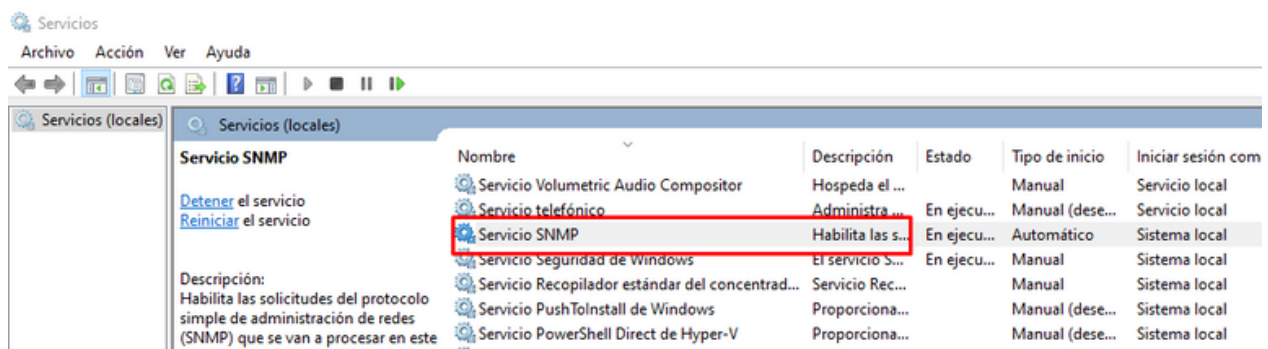
```
PS C:\WINDOWS\system32> Get-WindowsCapability -Online -Name "SNMP*"

Name           : SNMP.Client~~~~0.0.1.0
State          : Installed
DisplayName    : Protocolo simple de administración de redes (SNMP)
Description    : Esta característica incluye los agentes de Protocolo simple de administración de redes (SNMP) que supervisan la actividad en los dispositivos de red y notifican a la estación de trabajo de la consola de red
DownloadSize   : 596276
InstallSize    : 2306716
```

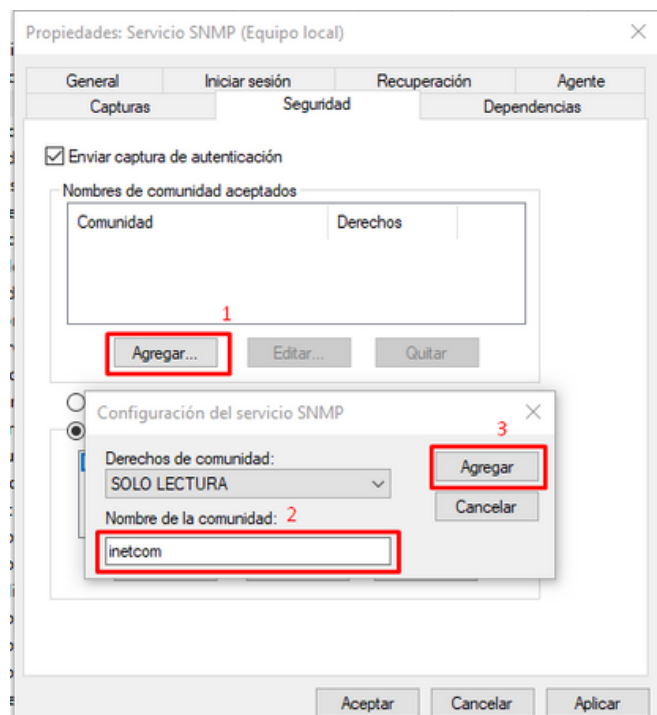
Ahora vamos a Servicios



Seleccionamos el Servicio SNMP



Vamos a la sección Seguridad y le damos a agregar y escribiremos el nombre de comunidad de la red.



ENTRAR A OBSERVIVUM

Una vez que tenemos el Observium instalado deberemos de acceder a su interfaz grafica.

En este caso tenemos la IP: 192.168.100.22 por lo que vamos a escribir esa IP en nuestro navegador de confianza y nos aparece la siguiente pantalla,

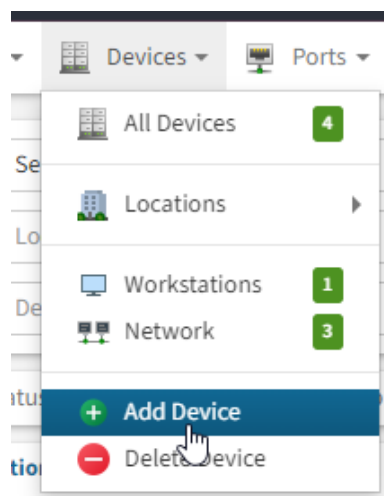
Introducimos el usuario y contraseña que hemos colocado antes.

Una vez que tenemos el Observium instalado deberemos de acceder a su interfaz grafica.

En este caso tenemos la IP: 192.168.100.22 por lo que vamos a escribir esa IP en nuestro navegador de confianza y nos aparece la siguiente pantalla,

Introducimos el usuario y contraseña que hemos colocado antes.

AÑADIR EQUIPOS



Una vez dentro de la interfaz grafica procederemos a añadir los dispositivos que les hemos activado el SNMP.

Para ello deberemos de ir a Devices -> Add Device

Rellenamos los siguientes campos:

- Hostname: IP que tiene el dispositivo
- Transport: el protocolo que usa
- Protocolo versión: la versión que hemos seleccionado en el dispositivo anteriormente.
- SNMP Community: el nombre de comunidad que hemos creado

Basic Configuration

Hostname: 192.168.100.1

Skip PING: ☐ Skip ICMP echo checks

Protocol Version: v2c

Transport: UDP

Port: 1-65535. Default 161.

Timeout: 1-120 sec. Default 1 sec.

Retries: 1-10. Default 5.












Max Repetitions: 0-500. Default 10. 0 for disable snmpbul

Ignore existing RRDs: ☒ Ignore pre-existing RRD directory and files

SNMP v1/v2c Authentication

SNMP Community: inetcom

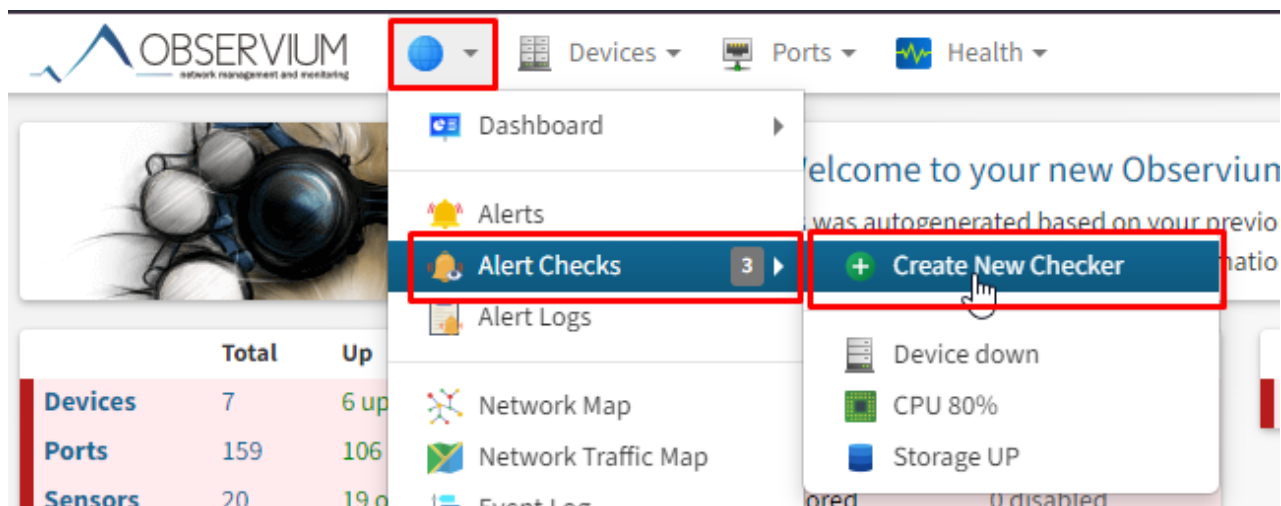
Al añadir mas dispositivo la pagina principal empezaría a coger forma de esta manera

Hostname / Domain / Location		Operating System / Hardware Platform		Uptime / sysName
 192.168.100.1 CPD		24	Mikrotik RouterOS 7.7 (Level 4)	9d 1h 31m 40s
		5 1	RBD53G-5HacD2HnD	mikrotik-router-g2
 192.168.100.2 CPD		43	Mikrotik RouterOS 6.45.9 (Level 5)	11d 3h 5m 40s
		3 1	RB4011iGS+	sw distribución
 192.168.100.5		29	Cisco IOS 12.1(13)EA1b (I6Q4L2)	11d 3h 5m 24s
		1 1	WS-C2950T-24	inetcom.inetcom
 localhost CPD		2	Linux 6.2.0-39-generic (Ubuntu 22.04)	3d 2h 38m 23s
			KVM Virtual Machine x86 [64bit]	inetcom-standard-pc-i440fx-pi

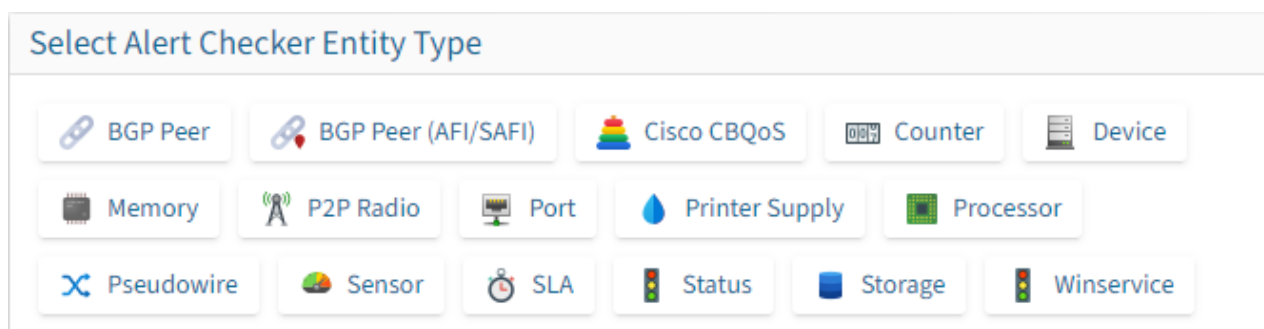
CREAR ALERTAS

Para tener un seguimiento de los dispositivos y ver el estado en el que están se pueden crear alertas.

Para ello iremos al logo del mundo -> Alert Checkers -> Create New Checker



Nos aparecerá un listado de diferentes alertas que podemos crear.



ALERTA HOST CAÍDO


Vamos a crear una alerta de host caído.

Para ello de la lista anterior seleccionamos **Device**.

Damos un nombre a la alerta y un mensaje para cuando se active dicha alerta.

New Checker Details

Entity Type

 Device

Alert Name

Host Down

Message

Host Down


Alert Delay

Nº of checks to delay alert

Send recovery


☒

Severity

 Critical

En el apartado de Test Conditions introduciremos **device_status 0**

Test Conditions

 Require all conditions

device_status 0

Seleccionamos Device Status | equals | false

Association Ruleset


AND OR


↕


Device Status


equals


False

 Delete

 Add rule

 Add group

 Clear Rules

 Add Checker

ALERTA ALMACENAMIENTO

Vamos a crear una alerta de ocupación de almacenamiento.

Para ello de la lista anterior seleccionamos **Storage**.

Damos un nombre a la alerta y un mensaje para cuando se active dicha alerta.

New Checker Details

Entity Type

☒ Storage

Alert Name

Storage 80%

Message

Alert message


Alert Delay

Nº of checks to delay alert

Send recovery


☒

Severity

 Critical

En el apartado de Test Conditions introduciremos `storage_perc 80`

Test Conditions


 Require all conditions

`storage_perc 80`

Seleccionamos Device | in | false


Association Ruleset


AND OR


 Device

in

7 items selected

 Delete

 Clear Rules

 Add Checker


ALERTA MEMORIA

Vamos a crear una alerta de ocupación de memoria.

Para ello de la lista anterior seleccionamos **Memory**.

Damos un nombre a la alerta y un mensaje para cuando se active dicha alerta.

New Checker Details

Entity Type  Memory

Alert Name Memoria 80%

Message Alert message

Alert Delay Nº of checks to delay alert

Send recovery ☒

Severity  Critical

En el apartado de Test Conditions introduciremos mempool_perc 80

Test Conditions

 Require all conditions

mempool_perc 80

Seleccionamos Device | in | seleccionamos los equipos

Association Ruleset

AND OR



Device

in

7 items selected

Delete

Clear Rules

Add Checker



ALERTA CPU AL 80%

Vamos a crear una alerta de ocupación de memoria.

Para ello de la lista anterior seleccionamos **Proccesor**.


Damos un nombre a la alerta y un mensaje para cuando se active dicha alerta.

New Checker Details

Entity Type	 Processor
Alert Name	<input type="text" value="CPU 80%"/>
Message	<div>Alert message</div>
Alert Delay	<input type="text" value="Nº of checks to delay alert"/>
Send recovery	<input checked="" type="checkbox"/>
Severity	<div> Critical</div>

En el apartado de Test Conditions introduciremos **processor_usage 80**

Test Conditions

 Require all conditions

processor_usage 80

Seleccionamos Device | in | seleccionamos los equipos

Association Ruleset









AND OR

↕↕

 Device ▲ in ▼

7 items selected ▲

Como podemos ver tenemos cuatro alertas configuradas.

Name	Tests	Device Match / Entity Match	Entities
CPU 80%	 AND (ALL) processor_usage 80	device.device_id in 6 5 4 8 10 9 1	 Default Notifier
Device down	 AND (ALL) device_status equals 0	device.hostname match *	 1 Notifiers
Memoria 80%	 AND (ALL) mempool_perc 80	device.device_id in 6 5 4 8 10 9 1	 Default Notifier
Storage UP	 AND (ALL) storage_perc 70	storage.storage_size gt 70	 1 Notifiers