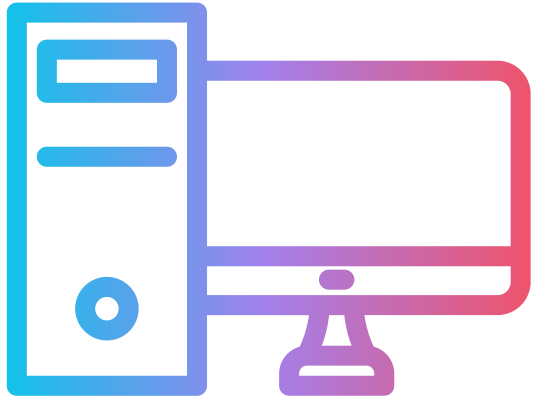




MONITOREO Y ANALISIS DE MI EQUIPO LAN

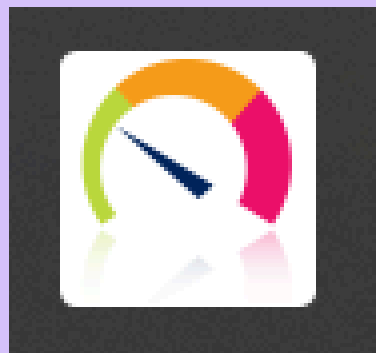


El monitoreo de red se diferencia claramente de los sistemas diseñados para detectar intrusos: este último se encarga de buscar intentos no autorizados de ingresar en la red, mientras que el primero trabaja sobre los potenciales errores internos de los servidores.

Una herramienta de monitoreo de redes es fundamental para asegurar el funcionamiento de los sistemas informáticos y para evitar fallos en la red. también nos ayuda a optimizar la red, ya que nos facilita información detallada sobre el uso de la banda ancha y otros recursos de la red.

MONITOREO :PRTG
VULNERABILIDAD: NESSUS






PRTG

ES UN SOFTWARE DE MONITOREO DE RED


- Instala 2 servicios:
PRTG Core server service
PRTG Probe service

PRTG Core Server Service	Monitorea redes usand...	En ejecu...	Automático	Sistema local
PRTG Probe Service	Performs network moni...	En ejecu...	Automático	Sistema local

Para iniciar, en CMD, se usa los comandos: - **net start PRTGProbeService** y - **net start PRTGCoreServerService**

 PRTG Administration Tool
Aplicación

Aplicaciones

 PRTG Network Monitor
(navegador predeterminado)

Procesos	Rendimiento	Historial de aplicaciones	Inicio	Usuarios	Detalles	Servicios				
Nombre	Estado		13% CPU	74% Memoria	0% Disco	1% Red	3% GPU	Motor de GPU	Consumo de e...	Tendencia de c...
> PRTG Server			0%	37,4 MB	0,1 MB/s	0 Mbps	0%		Muy baja	Muy baja
> Host de servicio: Inicializador de pr...			0%	9,5 MB	0 MB/s	0 Mbps	0%		Muy baja	Muy baja
> Skype (5)			0%	8,7 MB	0 MB/s	0 Mbps	0%		Muy baja	Muy baja
> Application Host Service (32 bits)			0%	14,9 MB	0 MB/s	0 Mbps	0%		Muy baja	Muy baja
> PRTG Probe (32 bits)			0%	6,1 MB	0 MB/s	0,1 Mbps	0%		Muy baja	Muy baja
WMI Provider Host (32 bits)			0%	28,6 MB	0 MB/s	0 Mbps	0%		Muy baja	Muy baja
AV Console (32 bits)			0%	4,4 MB	0 MB/s	0 Mbps	0%		Muy baja	Muy baja
> PRTG Administrator (32 bits)			0%	1,9 MB	0 MB/s	0 Mbps	0%		Muy baja	Muy baja



PRTG Administration Tool

Aplicación

- Abrir
- Ejecutar como administrador
- Abrir ubicación de archivo
- Anclar a Inicio
- Anclar a la barra de tareas
- Desinstalar

PAESSLER PRTG Network Monitor

Servidor web de PRTG | Servidor núcleo de PRTG | Clúster | Administrador

Iniciar/parar servicio | Registros e información | Servidor de aplicaciones de PRTG

Configuración de sonda para conexión al servidor central | Configuración de sonda para monitoreo

Configuración de sonda

Nombre de sonda: | Tiempo de reconexión: seg

Conexión al servidor central de PRTG

Configurada como sonda local: conecte con el servidor núcleo de PRTG en 127.0.0.1

Editar GID | Generar nuevo GID...

clave de acceso:

Ruta al directorio de datos de PRTG en la sonda remota

Ruta: ...

eventir a directorio predeterminad

Utilice "Archivo local de archivos de datos la base de datos de monitoreo" en la pestaña "Servidor núcleo de PRTG" en s

PAESSLER PRTG Network Monitor

Servidor web de PRTG | Servidor núcleo de PRTG | Clúster | Administrador

Iniciar/parar servicio | Registros e información | Servidor de aplicaciones de PRTG

Configuración de sonda para conexión al servidor central | Configuración de sonda para monitoreo

IPv4: Dirección IP saliente para solicitudes de monitoreo

Dirección IPv4	Nombre del adaptador	Tipo de ada...
<input checked="" type="radio"/> auto		

IPv6: Dirección IP saliente para solicitudes de monitoreo

Dirección IPv6	Nombre del adaptador	Tipo de ada...
<input checked="" type="radio"/> auto		

Configuración de sonda para conexión al servidor central

Servidor web de PRTG | Servidor núcleo de PRTG | Clúster | Administrador

Puerto TCP para el servidor web de PRTG

Servidor HTTPS seguro (puerto 443 predeterminado, recomendado, obligatorio para el acceso a Internet)

Servidor HTTP no seguro (puerto 80 predeterminado, no recomendado)

Configuración personalizada

Utilizar HTTPS (asegurado con SSL/TLS) | Puerto de servidor web:

No utilizar seguridad de conexión (no se recomienda)

Dirección IP para el servidor web de PRTG

Localhost, 127.0.0.1 (no se podrá acceder a PRTG desde otros equipos)

Todas las direcciones IP disponibles en este equipo (se recomienda)

Especificar direcciones IP:

127.0.0.1:443/welcome.htm

Página principal | dispositivos | Bibliotecas | sensores

bienvenido

**PR
NI
MONITOR**

Puerto 443: Este puerto es también para la navegación web, pero en este caso usa el protocolo HTTPS que es seguro y utiliza el protocolo TLS por debajo.

¡ Bienvenido Amnesia !

PAESSLER PRTG Network Monitor

Configuración de sonda para conexión al servidor central		Configuración de sonda para monitoreo	
Servidor web de PRTG	Servidor núcleo de PRTG	Clúster	Administrador
Iniciar /parar servicio	Registros e información	Servidor de aplicaciones de PRTG	

Logs

[Abrir carpeta de log...](#) [Mandar archivos log a Paessler...](#) [Abrir tique de asistencia...](#)

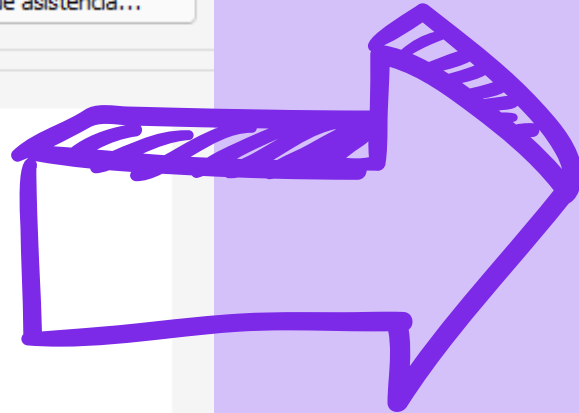
Acerca de

PRTG Network Monitor

© 1996-2022 Paessler AG
Thurn-und-Taxis-Straße 14
D-90411 Nuremberg
Germany

versiones instaladas:

PRTG core server service: V22.4.80.1553
PRTG probe service: V22.4.80.1553
PRTG Administration Tool: V22.4.80.1553



Windows File Explorer: Este equipo > Windows (C:) > ProgramData > Paessler > PRTG Network Monitor >

Nombre	Fecha de modificación	Tipo	Tamaño
Configuration Auto-Backups	26/11/2022 15:03	Carpeta de archivos	
Dumps	16/11/2022 11:09	Carpeta de archivos	
Log Database	26/11/2022 15:02	Carpeta de archivos	
Logs	26/11/2022 19:33	Carpeta de archivos	
Monitoring Database	26/11/2022 15:07	Carpeta de archivos	
Report PDFs	16/11/2022 11:09	Carpeta de archivos	
Sensordata (NonPersistent)	16/11/2022 11:09	Carpeta de archivos	
System Information Database	16/11/2022 12:13	Carpeta de archivos	
Ticket Database	17/11/2022 8:54	Carpeta de archivos	
ToDo Database	16/11/2022 11:09	Carpeta de archivos	
PRTG Configuration.dat	26/11/2022 16:54	Archivo DAT	1.57
PRTG Configuration.old	26/11/2022 15:03	Archivo OLD	1.57
PRTG Graph Data Cache.dat	26/11/2022 15:03	Archivo DAT	2.99

PAESSLER PRTG Network Monitor

Configuración de sonda para conexión al servidor central		Configuración de sonda para monitoreo	
Iniciar /parar servicio	Registros e información	Servidor de aplicaciones de PRTG	
Servidor web de PRTG	Servidor núcleo de PRTG	Clúster	Administrador

Credenciales de inicio de sesión para la cuenta Usuario administrador del sistema PRTG

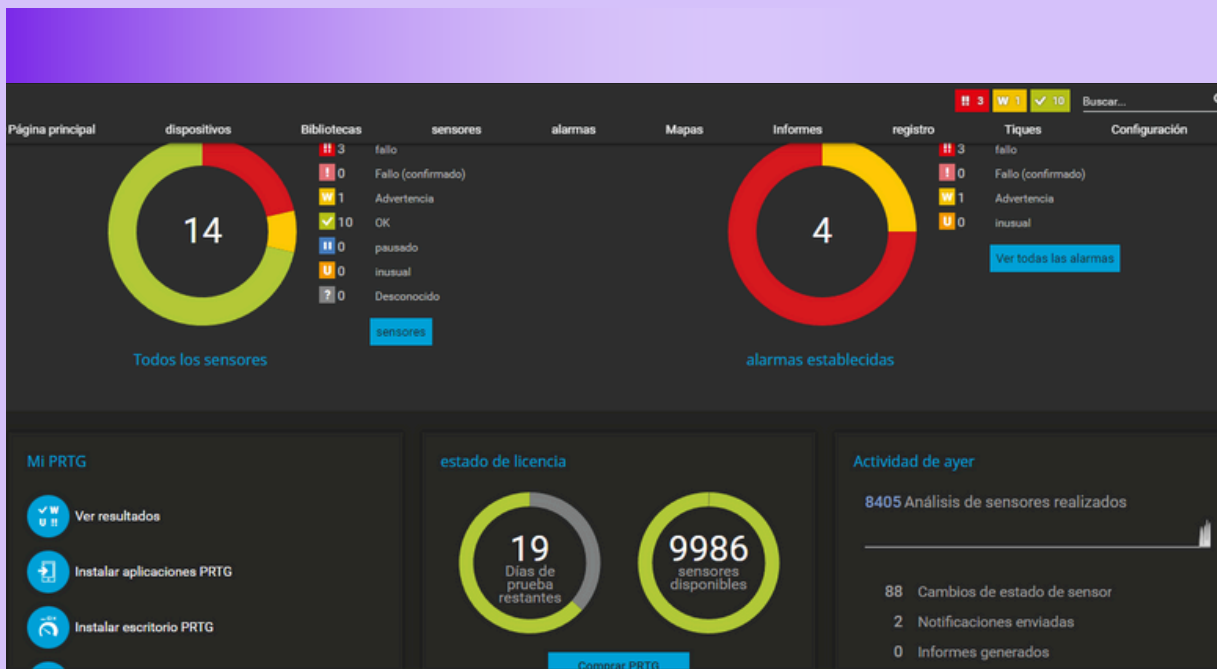
Dirección email:

Nombre de inicio:

Contraseña:

[Generar nueva contraseña](#)

Network Monitor



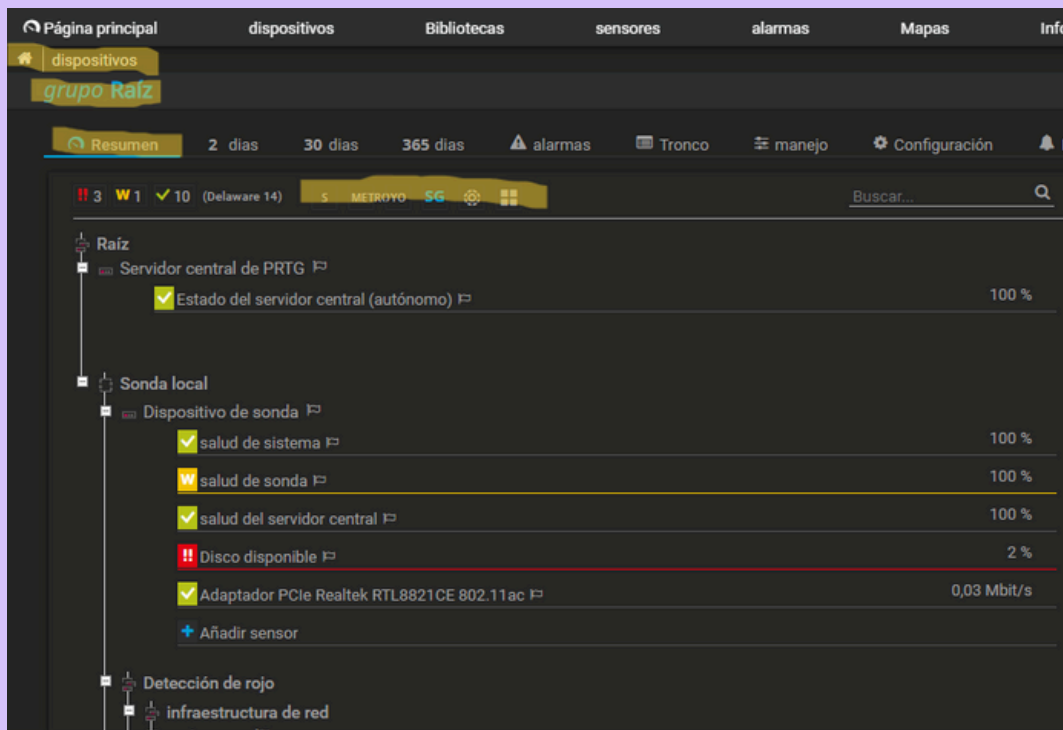
En la página principal

- , aparece el menú (dispositivos, bibliotecas, sensores, alarmas, mapas, informes, registros, tiques configuración)
- Representaciones de datos (sensores y de alarmas establecidas) en gráficos de anillo
- El estado de la licencia (gráfica de anillo)
- La actividad del día de ayer (análisis de sensores realizados)

The footer area contains several elements:

- Two article teasers with titles like 'Cómo agregar y usar fácilmente sensores HPE 3P...' and 'Cómo monitorear servidores HPE ProLiant con Pa...'. Each includes a brief description and a 'Ver artículo' button.
- A video player section with the title 'En nuestro nuevo video, demostramos configurar un mapa dentro de PRTG...' and a 'Ver video (08:30 min)' button.
- A footer bar with the PAESSLER logo, a user profile '22.4.80.1553+ Amnesia', a clock '9:42', and a refresh button 'Actualizar en 25 segundos'.

En el footer de la página principal, aparece la fecha romana actual, seguidamente con boton de parar o iniciar las actualizaciones



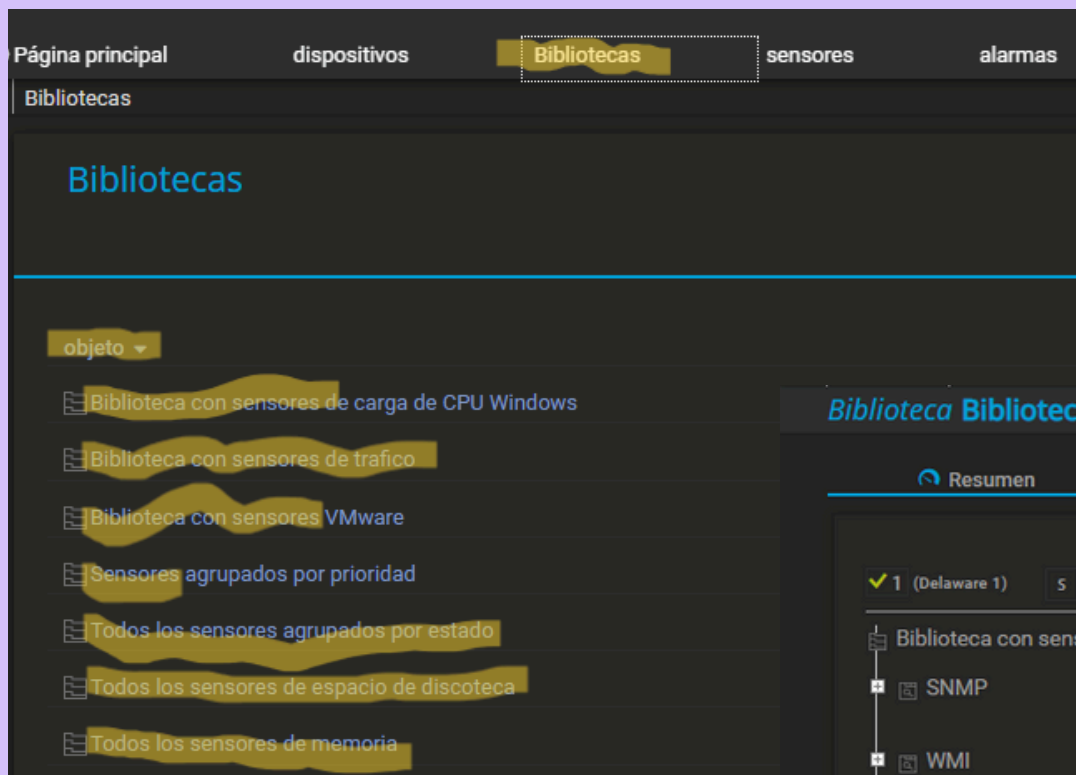
En el menú, DISPOSITIVOS:

- Aparece los dispositivos (raíz = servidor central de PRTG; y ,sonda local,= infraestructura de red, ventanas, sistemas virtuales, Hiper-V, Linux, impresora,.....)
- En menú resumen (2 dias, 30 dias, 365 dias, alarmas, log, manejo, configuración,..)
- Iconos de los sensores y distintas estructuras para el uso(árbol, arbol tamaño s, anillo....)



Se puede añadir dispositivos con distintos sensores.

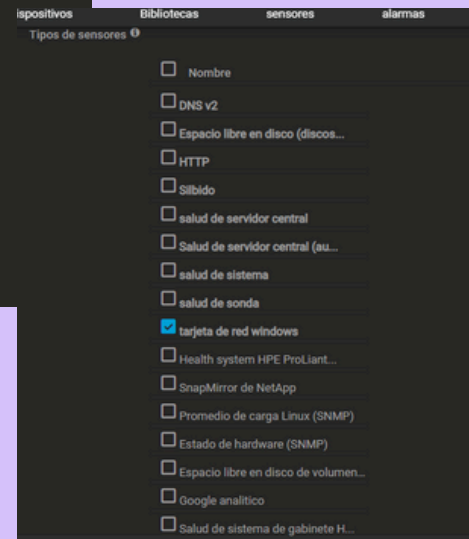
en este caso, añadi el dispositivo con 2 sensores ditintos: -silbido y HTTP



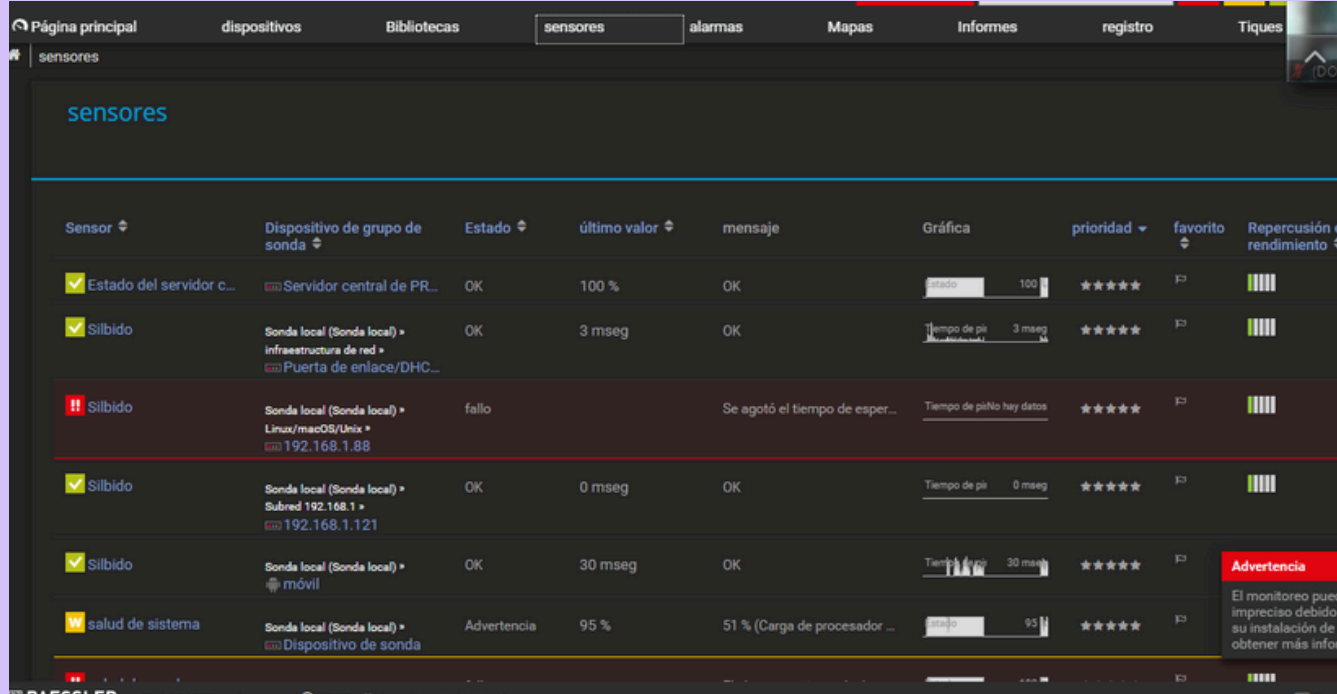
En el menu de la biblioteca, aparece los sensores organizados por bibliotecas



Un ejemplo, biblioteca con sensores de tráfico, En el aparece ,por ejemplo el uso de SNMP , en el que este caso esta activado el sensor el WMI



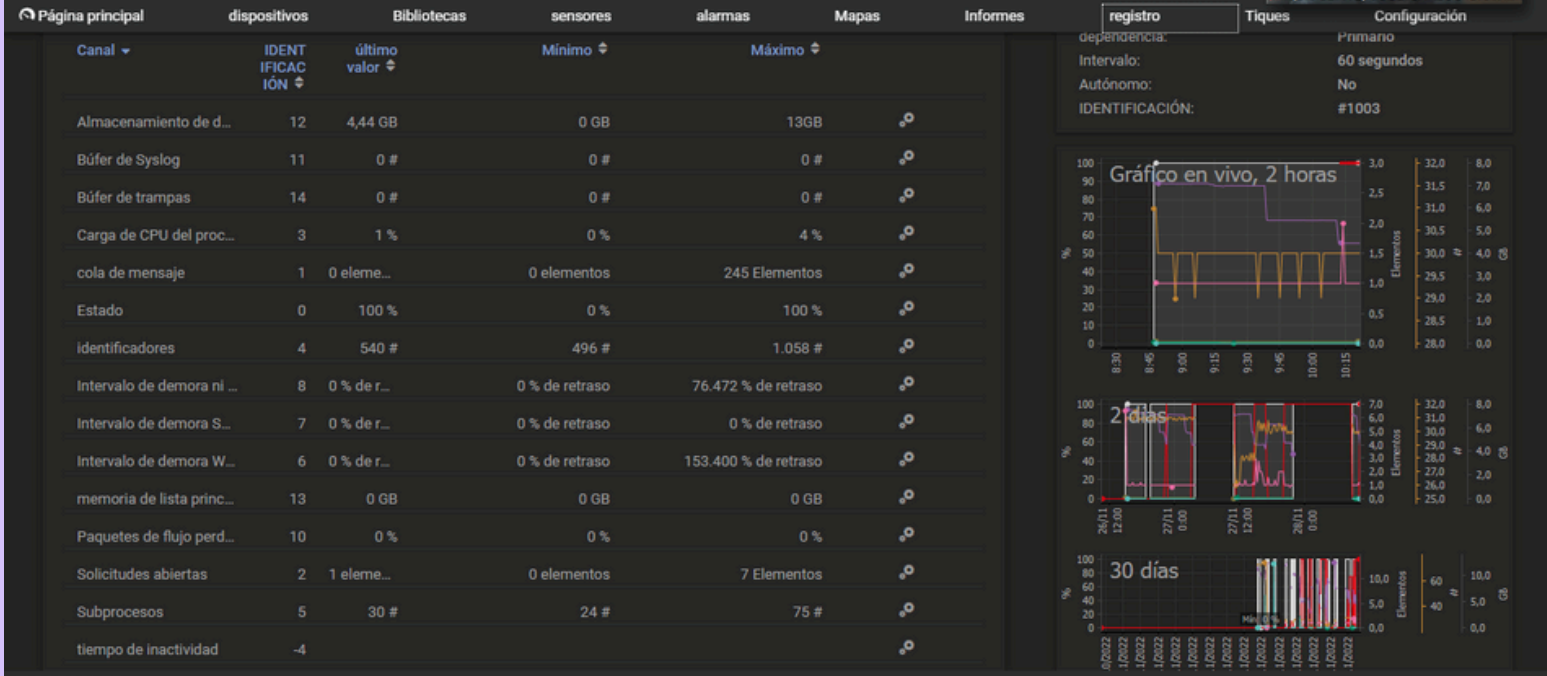
al abrir el nodo de la biblioteca WMI ,detalla su informe del tipo de sensor,(Tipo :tarjeta de red Windows)



En el menú de sensores evalúa detalladamente todos los sensores (dispositivo, estado,, ultimo valor, mensaje,, gráfica. prioridad, favorito, repercursion en el rendimiento



En el sensor de salud de sonda me sale en rojo,, y con gráficas y tablas explica el error (su intervalo de tiempo de error, el motivo causado de que de error el sensor.) El almacenamiento de datos es inferior a 5GBytes (código PE267)



kb.paessler.com/en/topic/64628-my-probe-system-is-running-out-of-disk-space-what-can-i-do

PAESSLER
THE MONITORING EXPERTS

PRODUCTOS SOLUCIONES APOYO COMPAÑÍA SOCIOS

Base de conocimientos

Mi sistema de sonda se está quedando sin espacio en disco. ¿Que puedo hacer?

Votos: 0

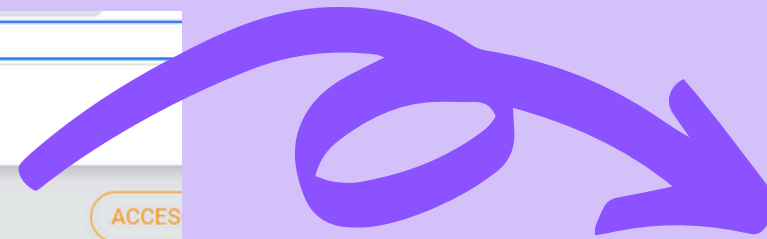
Tu voto: ¿Qué puedo hacer si el espacio en disco disponible en mi sistema de sonda se está agotando?

almacenamiento de datos sin disco espacio en disco probe probe health prtq

Sumérjase PRTG.

Obtenga más OPC UA y MQ

Creado el 21 de mayo de 2015 13:17:30 por Gerald Schoch [Paessler Support]



Nos recomienda esta página para ver el error:
<https://kb.paessler.com/en/topic/64628-my-probe-system-is-running-out-of-disk-space-what-can-i-do>

Página principal dispositivos Bibliotecas sensores alarmas Mapas Informes registro TIK BEATRIZ ROCIO ANTURI MEJIA

alarmas

sensores con alarmas

Mostrar filtros

Sensor	Dispositivo de grupo de sonda	Estado	fallo por	último valor	mensaje	Gráfica	prioridad
!! Silbido	Sonda local (Sonda local) > Linux/macOS/Unix > 192.168.1.88	fallo	7 días 16 horas		Se agotó el tiempo de espera de la ...	Tiempo de piNo hay datos	★★★★★
W salud de sistema	Sonda local (Sonda local) > Dispositivo de sonda	Advertencia		85 %	52 % (Carga de procesador de siste...	Estado 85	★★★★★
!! salud de sonda	Sonda local (Sonda local) > Dispositivo de sonda	fallo	27 m 43 s		El almacenamiento de datos es inf...	Estado 100	★★★★★
!! Disco disponible	Sonda local (Sonda local) > Dispositivo de sonda	fallo	1 hora 52 minutos	2 %	2 % (Espacio disponible C:) está po...	Espacio disc 2	★★★★☆
!! HTTP	Sonda local (Sonda local) > Subred 192.168.1 > 192.168.1.121	fallo	2 días 21 horas 4...		Conexión rechazada Socket Error #...	tiempo de caNo hay datos	★★★☆☆
!! HTTP	Sonda local (Sonda local) > móvil	fallo	1 hora 52 minutos		Conexión rechazada Socket Error #...	tiempo de caNo hay datos	★★★☆☆

1 a 6 de 6

en el menu de alarmas, indica la forma que avisa los sensores añadidos a los dispositivos, (dispositivo, estado, fallo por, ultimo valor, mensaje, gráfica, prioridad

Página principal dispositivos Bibliotecas sensores alarmas Mapas Informes registro Tiques Configuración

Entradas de registro

Ver como XML (máx. 500 elementos)

Fecha	Primario	Tipo	Objeto	Estado
28/11/2022 10:43:46	Dispositivo de sonda	salud de sistema	salud de sistema	Advertencia
Mensaje 60 % (Carga de procesador de sistema) está por encima del límite de advertencia 50 % en Carga de procesador de sistema. Cuando la carga de la ma de sonda es superior al 50%, las mediciones pueden ser incorrectas.				
28/11/2022 10:41:46	Dispositivo de sonda	salud de sistema	salud de sistema	OK
Mensaje 85 %				

```

<datetime_raw>44893.4053935880</datetime_raw>
<parent>Dispositivo de sonda</parent>
<type>Salud de sistema</type>
<type_raw>systemstate</type_raw>
<name>Salud de sistema</name>
<status>Advertencia</status>
<status_raw>609</status_raw>
<message><div class="logmessage">60 % (Carga de procesador de sistema) está por encima del límite de advertencia 50 % en Carga de de la CPU en el sistema de sonda es superior al 50%, las mediciones pueden ser incorrectas.</div></div></message_raw>
<objjid>1001</objjid>
<baselink>/sensor.htm?id=1001</baselink>
<baselink_raw>1001</baselink_raw>
</item>
<item>
<datetime>28/11/2022 10:41:46</datetime>
<datetime_raw>44893.4040047685</datetime_raw>
<parent>Dispositivo de sonda</parent>
<type>Salud de sistema</type>
<type_raw>systemstate</type_raw>
<name>Salud de sistema</name>
<status>OK</status>
<status_raw>607</status_raw>
<message><div class="logmessage">85 %</div></div></message>
<message_raw>85 %</message_raw>
<objjid>1001</objjid>
<baselink>/sensor.htm?id=1001</baselink>
<baselink_raw>1001</baselink_raw>
</item>
<item>
<datetime>28/11/2022 10:39:46</datetime>
<datetime_raw>44893.4026159375</datetime_raw>

```

En el menu de registro, aparece las distintas entradas registradas y se puede descargar el documento (DATABASE) en HTML

Página principal dispositivos Bibliotecas sensores alarmas Mapas Informes registro Tiques Configuración

Tiques

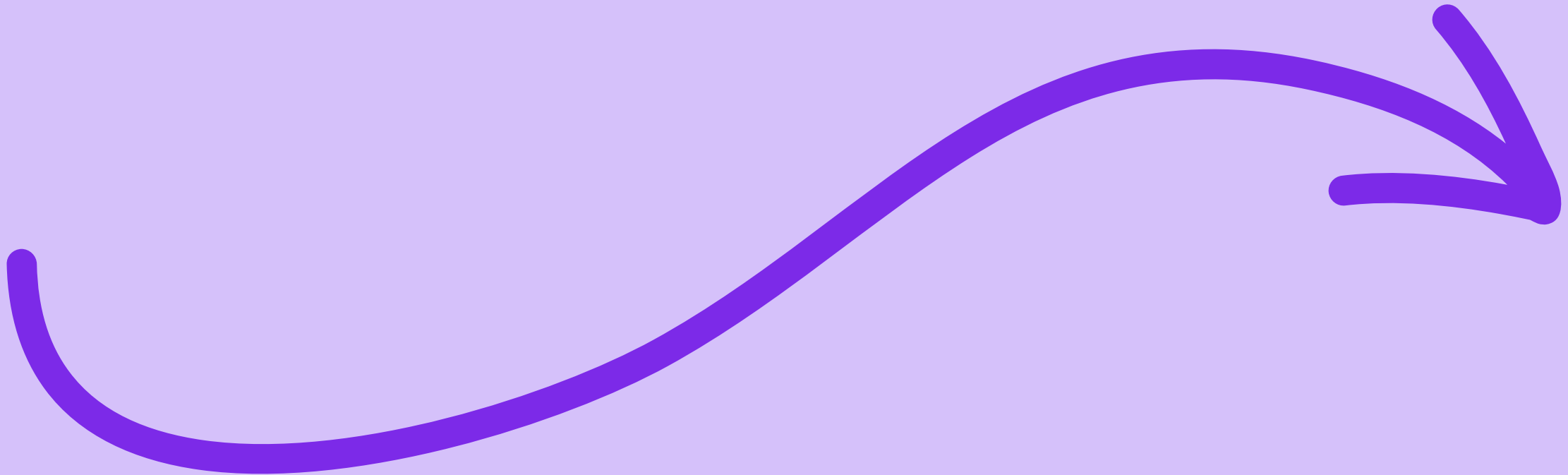
filtros oculares ^

Filtrar por estado abierto Filtrar por tipo Todos los tiques Filtrar por usuario Yo Filtrar por objeto Cualquier objeto Filtrar por fecha

Última modificación	prioridad	Identificación. de tique	Asunto	Asignado a	Estado	objeto	
20/11/2022 16:43:16	★★★★☆	#4	Recomendamos Windows S...	Administradores PRTG	○	Sistema	<input type="checkbox"/>
16/11/2022 11:19:18	★★★★☆	#2	Descubrimiento automático ...	Administradores PRTG	○	Sonda local	<input type="checkbox"/>
16/11/2022 11:09:59	★★★★☆	#1	Bienvenido a PRTG.	Administradores PRTG	○	Raíz	<input type="checkbox"/>

1 a 3 de 3

en el menu de tiques,puedes filtrar por estado, por tipo, por usuario, por objeto o por fecha





Scans

Settings

Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, `nessusd`, que realiza el escaneo en el sistema objetivo, y `nessus`, el cliente que muestra el avance e informa sobre el estado de los escaneos.

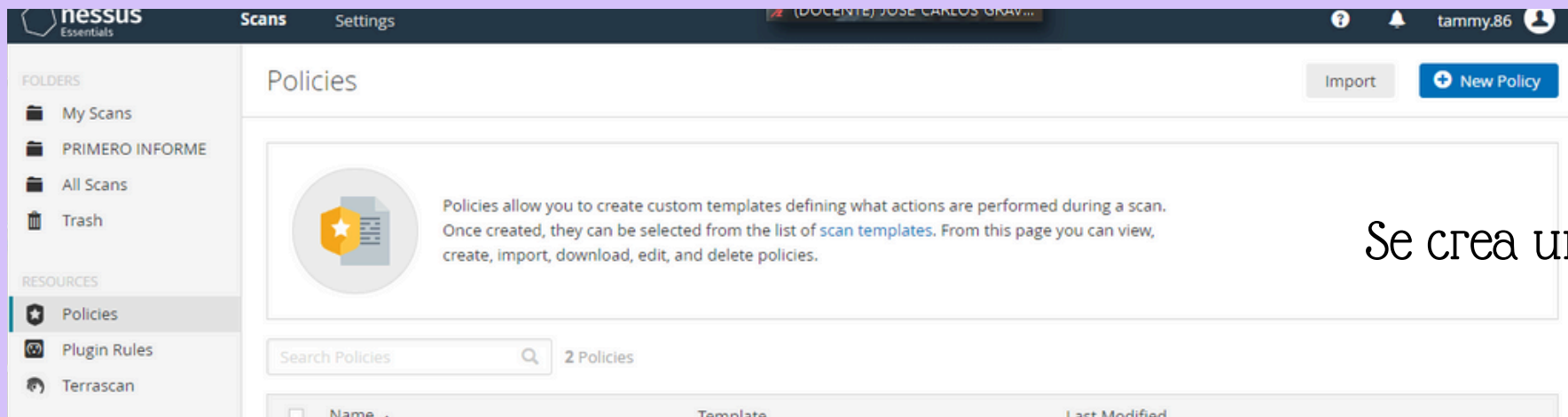
Nessus, usa el puerto 8834

 No seguro | <https://localhost:8834/#/scans/folders/my-scans>

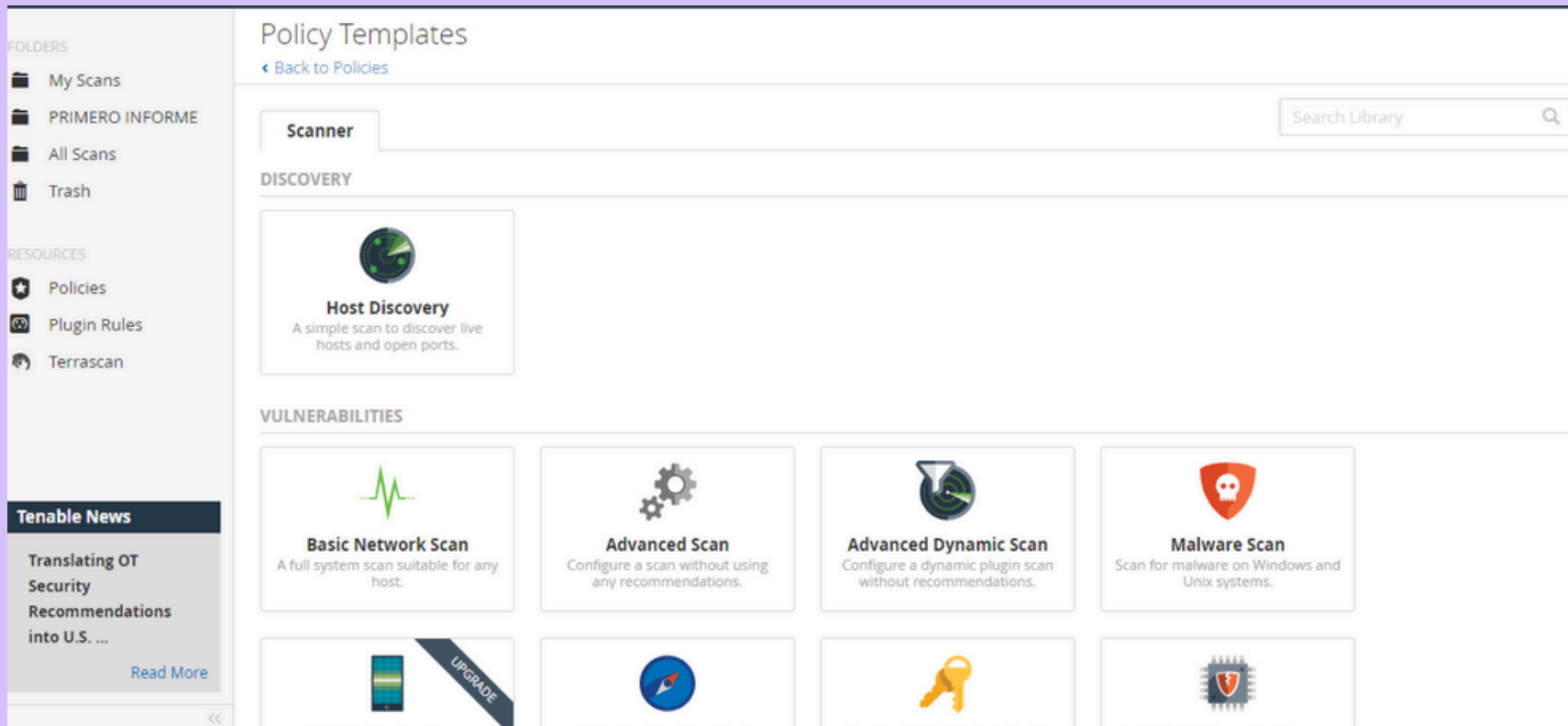
en CMD con permisos de administración : `-netstat -bona | findstr :8834`

y en servicios para iniciar en Tenable Nessus

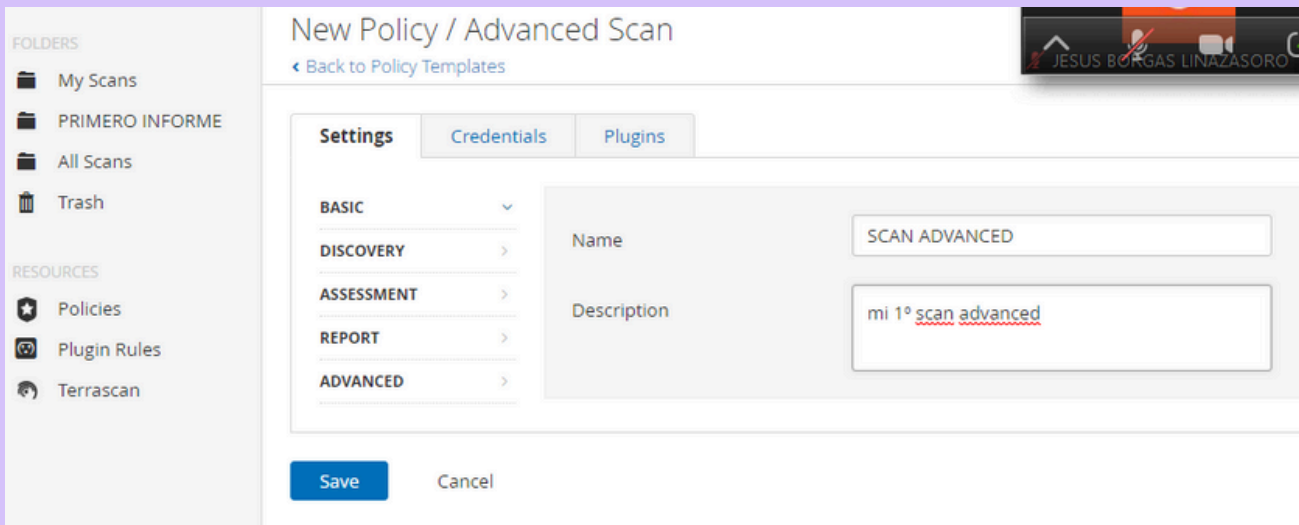
Página para instalación: <https://www.tenable.com/downloads/nessus?loginAttempted = True>



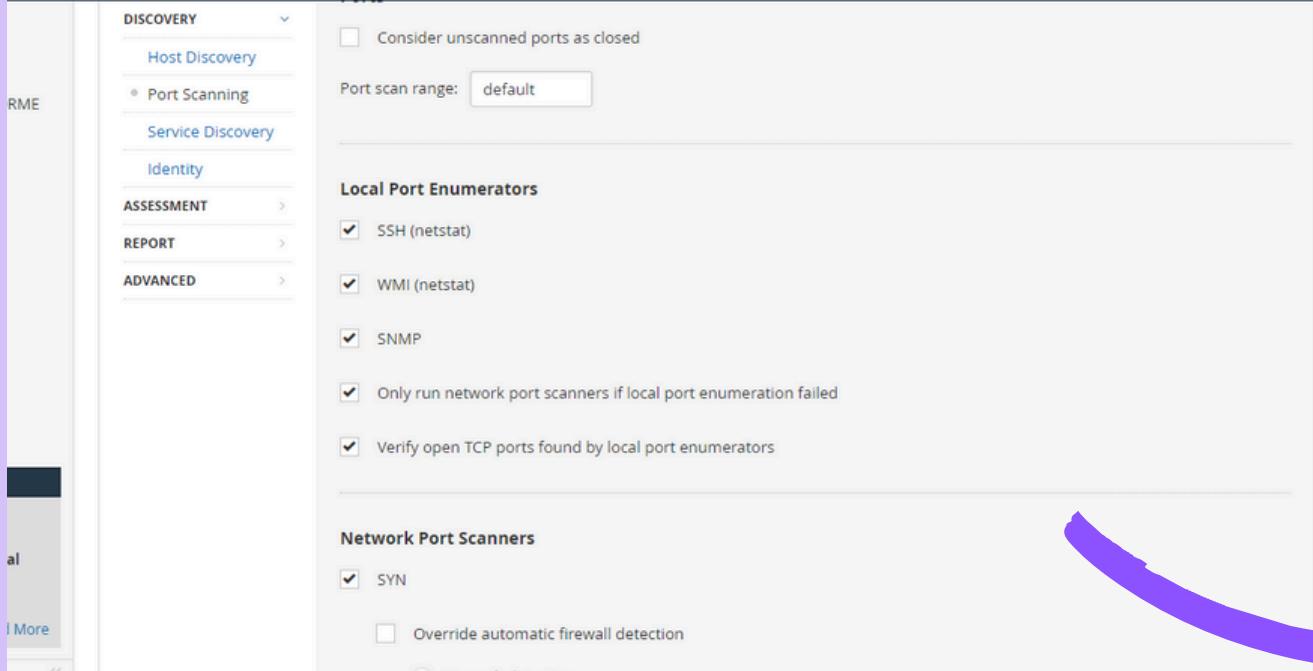
Se crea una nueva politica



Se elige que escaneo realizar....elegi en esta ocasión SCAN ADVANCED



Se añade el nombre y descripción

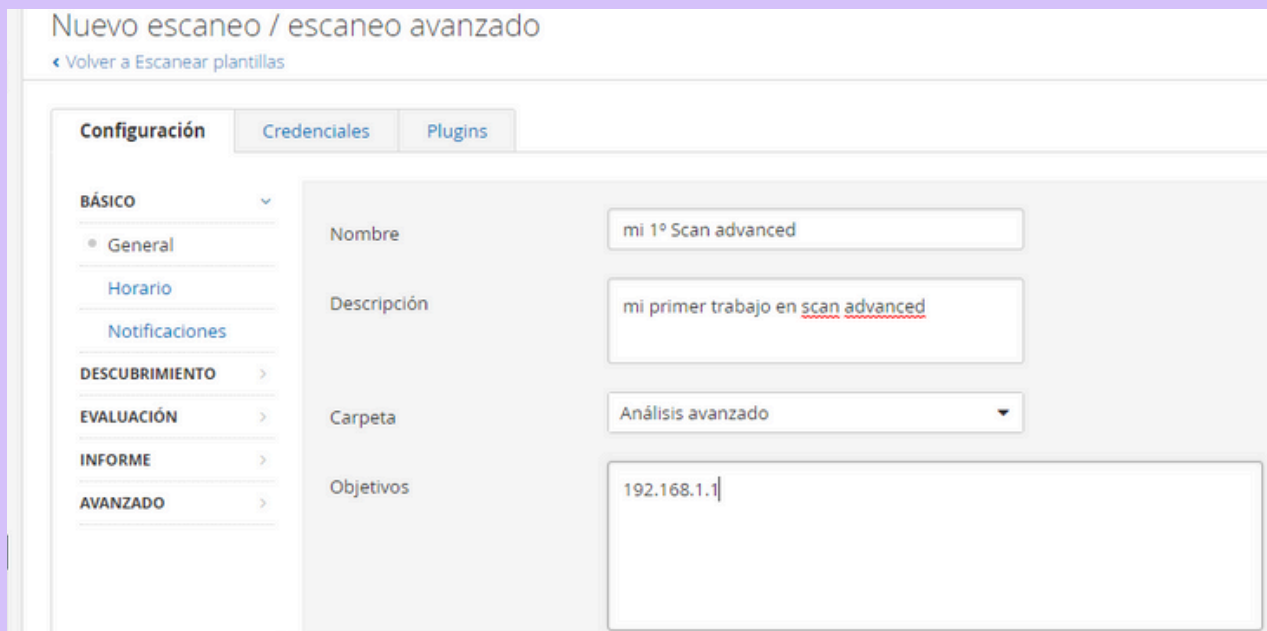


en discovery, se elige los puertos :

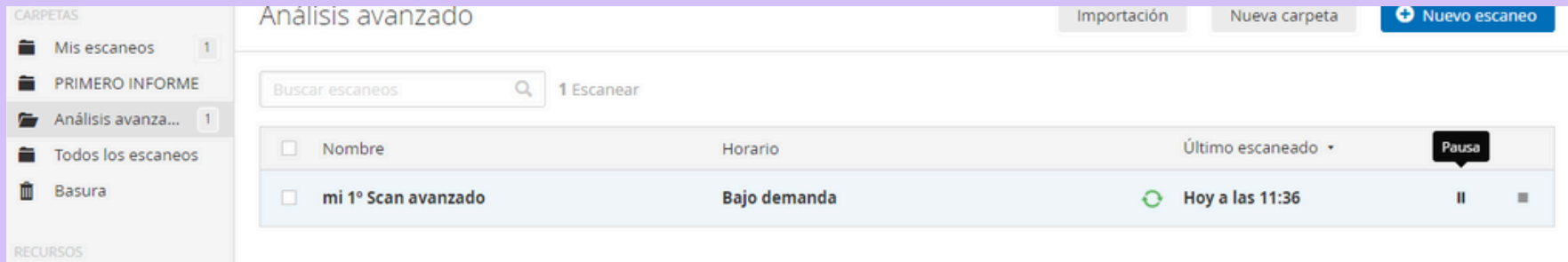
SSH (NETSTAT)
WMI (NETSTAT)
SNMP
ONLY RUN NETWORK PORT SCANNERS IF LOCAL
PORT ENUMERATION FAILED
VERIFY OPEN TCP PORTS FOUND BY LOCAL PORT
ENUMERATORS
NETWORK PORT SCANNERS
SYN



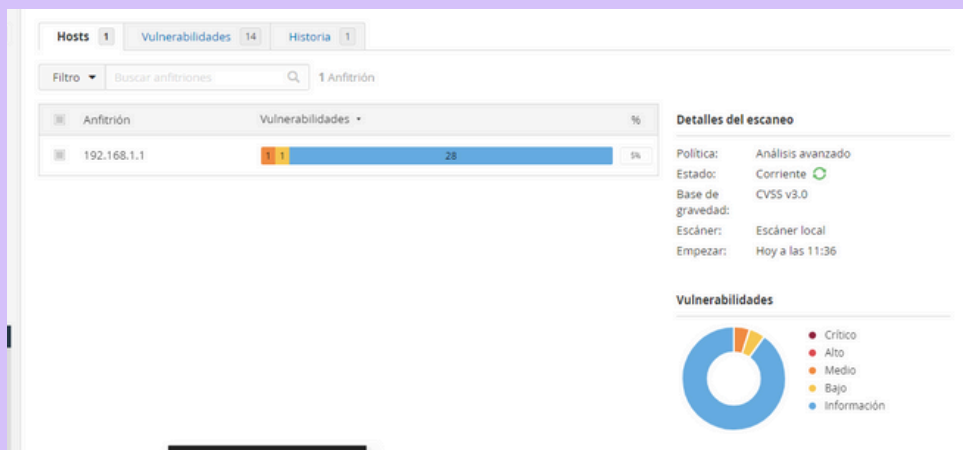
se guarda y se crea una carpeta



Añadir el objetivo (192.168.1.1)



DAR AL PLAY para que inicie el servicio



Podemos ver su evolución de escaneo de puertos con el objeto del 192.168.1.1, clikeando el scan

nessus Essentials Escaneos Configuración (DOCENTE) JOSÉ CARLOS GRAVAL...

Hosts 1 Vulnerabilidades 23 Historia 1

Filtro Vulnerabilidades de búsqueda 23 Vulnerabilidades

Sev	Puntuac...	Nombre	Familia	Contar
MEDIO	6.5	Reenvío de IP habilitado	Cortafuegos	1
MIXTO	...	5 SSL (problemas múlti...	General	5
MIXTO	...	4 TLS (problemas múlti...	Detección de servicios	4
MIXTO	...	2 SMB (problemas múlti...	Misc.	2
BAJO	3.3 *	Detección de servidor DHCP	Detección de servicios	1
INFORMACIÓN	...	6 SMB (problemas múlti...	Windows	7
INFORMACIÓN	...	2 DNS (problemas múlti...	DNS	3
INFORMACIÓN	...	2 HTTP (varios problem...	Servidores Web	3
INFORMACIÓN	...	2 TLS (problemas múlti...	General	2

Detalles del escaneo

Política: Análisis avanzado
 Estado: Corriente
 Base de gravedad: CVSS v3.0
 Escáner: Escáner local
 Empezar: Hoy a las 11:36

Vulnerabilidades

● Crítico
 ● Alto
 ● Medio
 ● Bajo
 ● Información

Noticias de Tenable
 Una receta para el éxito: los CISO comparten los mejores consejos para suc...
[Leer más](#)

en vulnerabilidades, detalla el grado, puntuación, el nombre y familia

Hora de comienzo	Último escaneado	Estado
Actual Hoy a las 11...	N/A	Corriente

Detalles del escaneo

Política: Análisis avanzado
 Estado: Corriente
 Base de gravedad: CVSS v3.0
 Escáner: Escáner local
 Empezar: Hoy a las 11:36

Vulnerabilidades

● Crítico
 ● Alto
 ● Medio
 ● Bajo
 ● Información