sedian

Seguridad Digital
de Andalucía

Monitorización y supervisión activa y pasiva de los sistemas

Junta de Andalucía
Consejería de Economía, Conocimiento,
Empresas y Universidad

Contenidos

Qué vamos a tratar

1. Monitorización Pasiva vs Activa, beneficios y limitaciones
2. Evolución y experiencias de campo con diferentes herramientas de monitorización
    1. Nagios
    2. Pandora FMS
    3. PRTG
    4. Zabbix
3. Requisitos y despliegue de Zabbix
4. Configuración Servidor
5. Elementos
    a. Host e Item, Trigger y Action, Web Monitoring, Maps y Screens
6. Realidad de uso

    Análisis de la información BBDD

Cada grupo tiene sus beneficios y limitaciones y deben considerarse complementarias y usarse conjuntamente.

- **Pasiva**: es realizada por aplicaciones externas.
  - Asíncrona, es reactiva, error -> aviso -> reacción.
- **Activa:** Es iniciada y realizada por la solución de monitorización.
  - Chequeos regulares y en base a reglas realiza ella misma acciones de mitigación y/o notificación.

Ambas son necesarias para proporcionar visibilidad del rendimiento de nivel de servicio (SLA), advirtiendo una degradación del rendimiento, incluso antes de que nos avise el cliente.

- Objetivo principal Administrador, infraestructura correcta y pleno rendimiento, **100% del tiempo.**
- Análisis de los **recursos,** planificar **ampliaciones o mejoras.**
- Pasar de un modelo de asistencia **reactivo** a un modelo **preventivo.**
- Visibilidad de los **errores,** generación incidencias en **cascada.**
- El **coste** de la inactividad de un servicio/servidor es alto.
- **Pérdida** de confianza de los clientes.

Nagios

- Es considerada la primera herramienta de monitorización Opensource, creada hace 17 años.
- Evolución a través de add-ons o complementos de terceros para suplir las funcionalidades que le faltan.
- Todo se configura con archivos de configuración (aumento de errores no forzados).
- Librerías desactualizadas o mal mantenida.

- **Pandora FMS**:

Considerado un framework de monitorización completo, pero sus máximas opciones son de pago, mayoría de librerías de pago.

- **PRTG:**

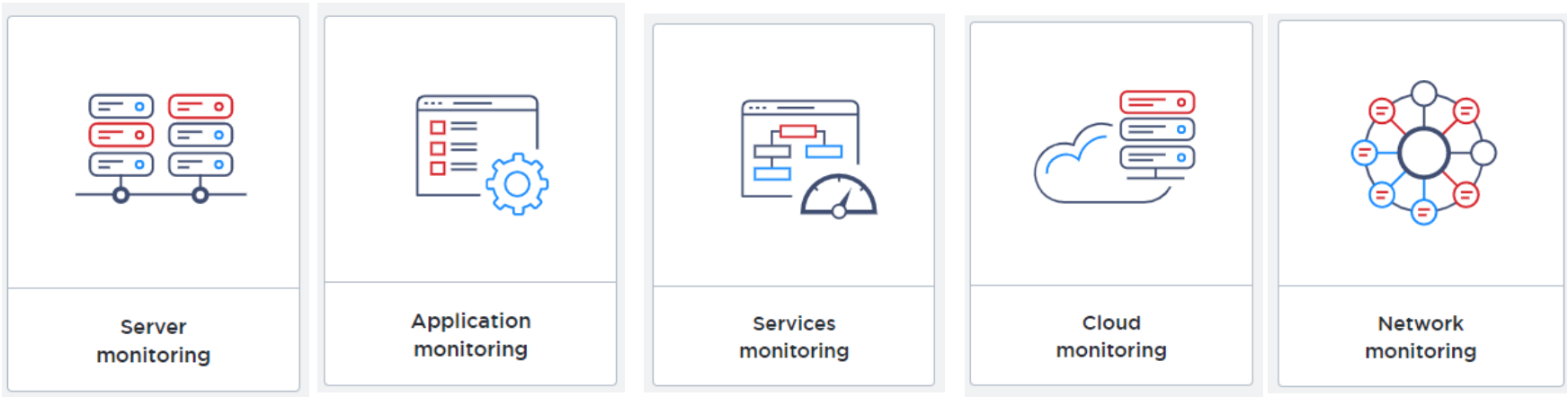
Solo versión de pago, no debes/puedes salirte de lo que te ofrece el fabricante.

- Monitorización en tiempo real de alto rendimiento.
- Recopilación y almacenamiento de datos, así como las características de visualización.
- Chequeos simples para verificar la disponibilidad y el nivel de respuesta de servicios estándar , SMTP, HTTP, LDAP, sin necesidad de instalar ningún software en el host.
- Monitoreo centralizado a través del administrador Web (FrontEnd).
- Definición de alertas basadas en sus necesidades y umbrales.

- Implementación de usos de script y programación.
- Mapas definidos por el usuario y dashboard personalizables.
- SLA que le permite analizar la calidad de los servicios prestados de su IT a su organización.
- Opensource y muy fácil ejecución de scripts para comunicación con otras plataformas o aplicaciones.
- Desarrollo continuo y activo por la comunidad.

- **Zabbix:**
- Instalación y configuración de un sistema de monitorización completo
- Supervisión activa y pasiva de incidencias.
- Análisis de datos recopilados para actuar proactivamente ante sucesos que pueden originar incidencias en un futuro.

Zabbix es un sistema de monitorización de nivel empresarial, diseñado para monitorizar:



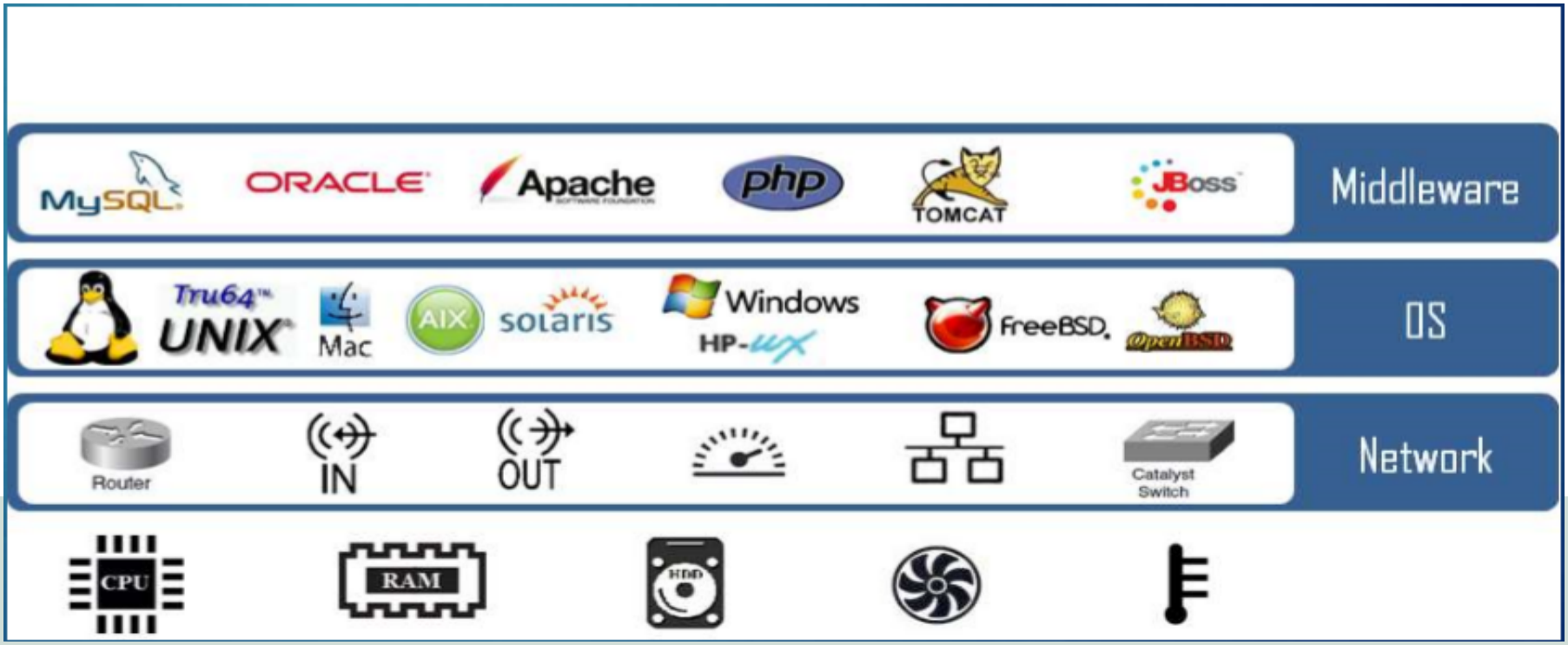
ZABBIX

Zabbix puede monitorizar de diversas formas:

- SNMP v1,2
- Zabbix Agent

- ICMP
- Port Monitoring

- JMX Monitoring
- IPMI Monitoring



¿Funcionalidades?

Requisitos y despliegue de Zabbix

sedian Seguridad Digital de Andalucía

- Instalación del appliance en una VM directamente:

https://www.zabbix.com/documentation/current/manual/appliance

- Por separado en una VM Unix (manuales en paginas reputadas):

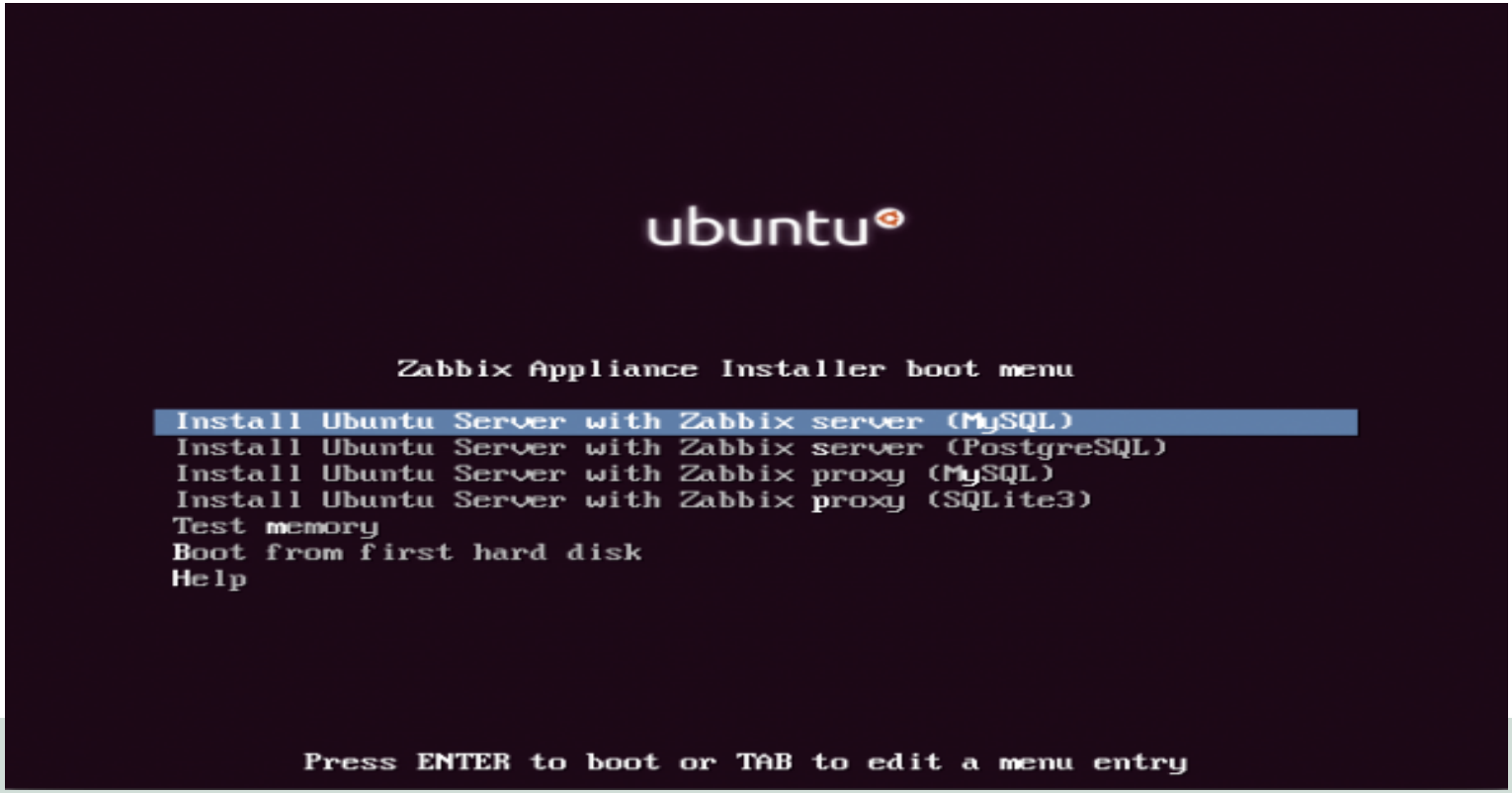
https://ubunlog.com/llega-la-nueva-version-de-zabbix-4-4-un-sistema-de-nonitorizacion-de-redes/

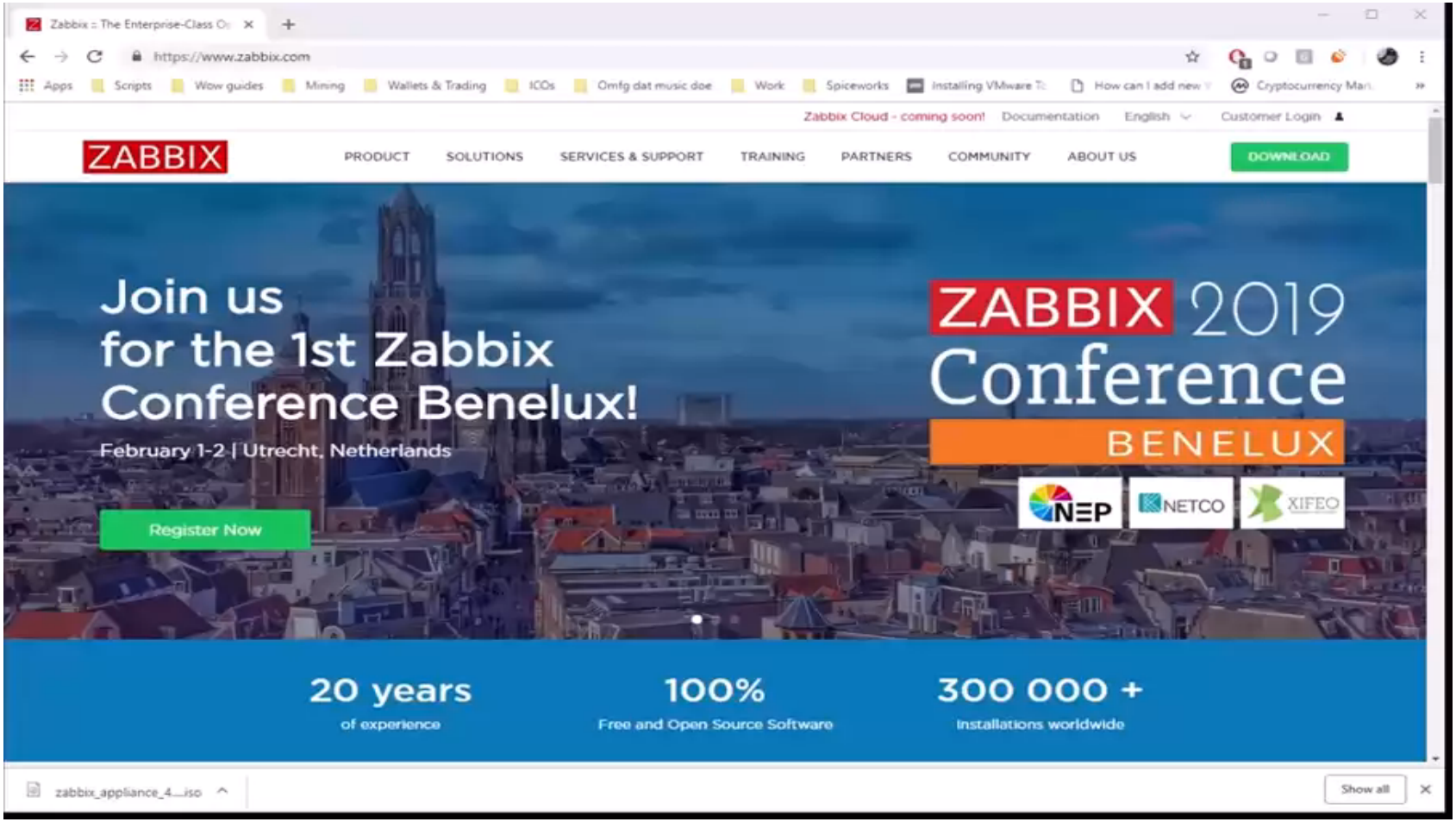
https://techexpert.tips/es/zabbix-es/zabbix-4-4-instalacion-con-nginx-en-ubuntu-linux/

- A través de paquetes distribuidos:

https://www.zabbix.com/documentation/current/manual/installation/install_from_packages

El método mas rápido es a través de un appliance





Vídeo instalación

Debemos modificar varios archivos del zabbix-server:

- Cambiar zona horaria

/etc/apache2/conf-available/zabbix.conf;

Cp /usr/share/zoneinfo/Europe/Riga /etc/localtime

- Credenciales (login:Password):

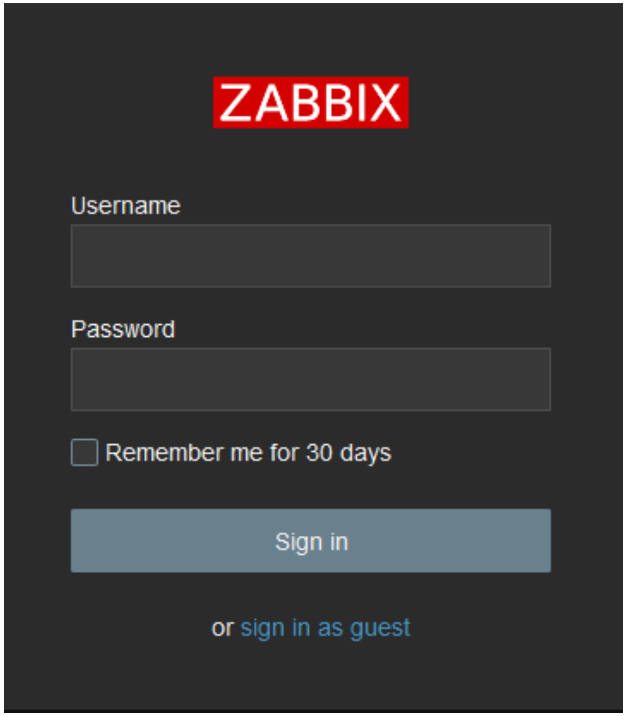
Sistema-> appliance:zabbix

- Cambiar en VM

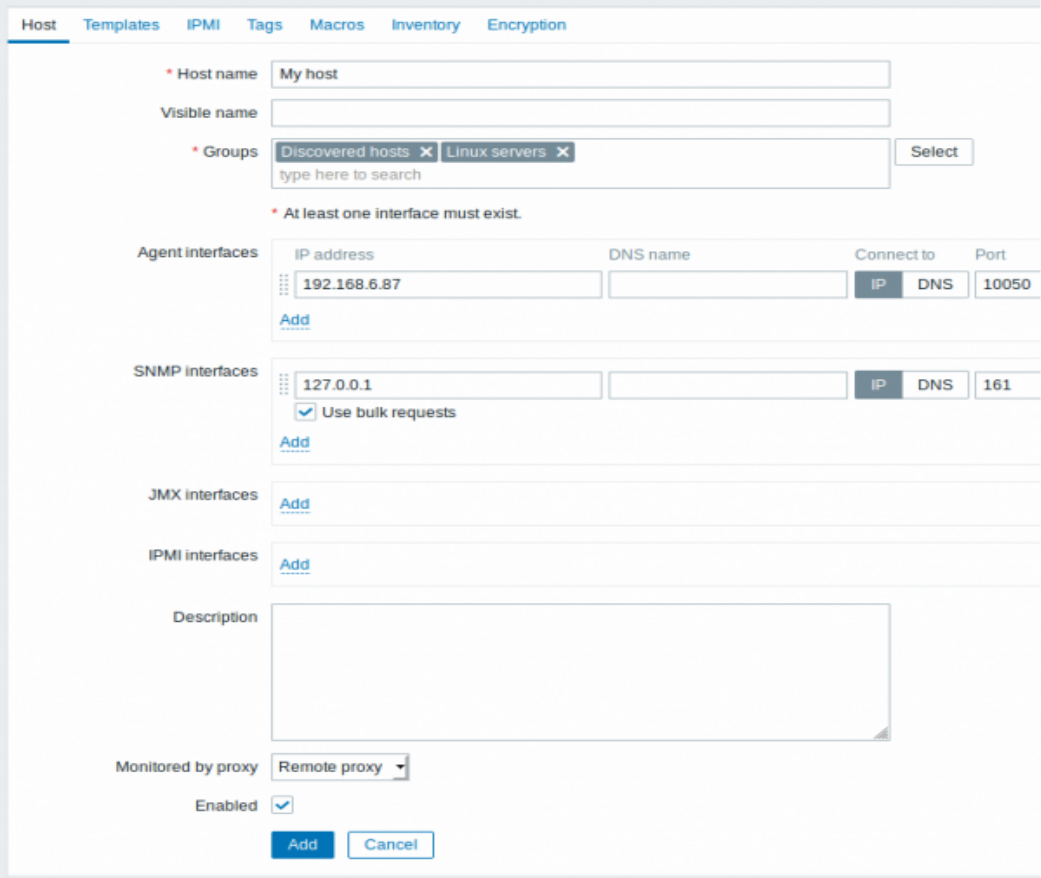
Database-> root:zabbix

- /etc/zabbix/zabbix_server.conf;
- /etc/zabbix/web/zabbix.conf.php

Zabbix frontend> Admin:zabbix



Elementos



Host

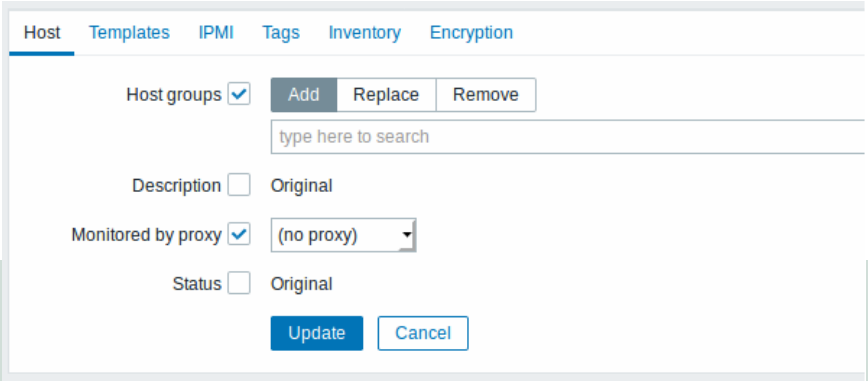
Es la entidad monitorizada (dispositivos, aplicaciones, BBDD, servicios, etc).

Se incluyen en grupos para su gestión.

IP o DNS necesarios.

Grupos

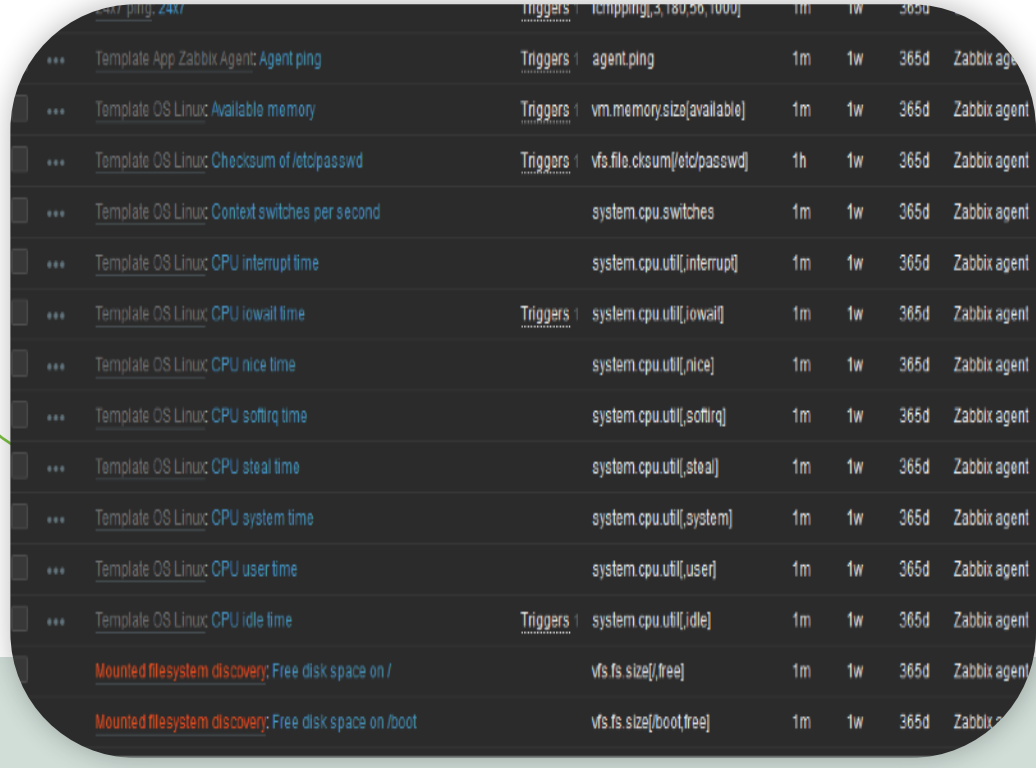
Permite cambiar atributos a todos los host del grupo y navegar por los mismos.



Se deben agregar para obtener los datos reales:

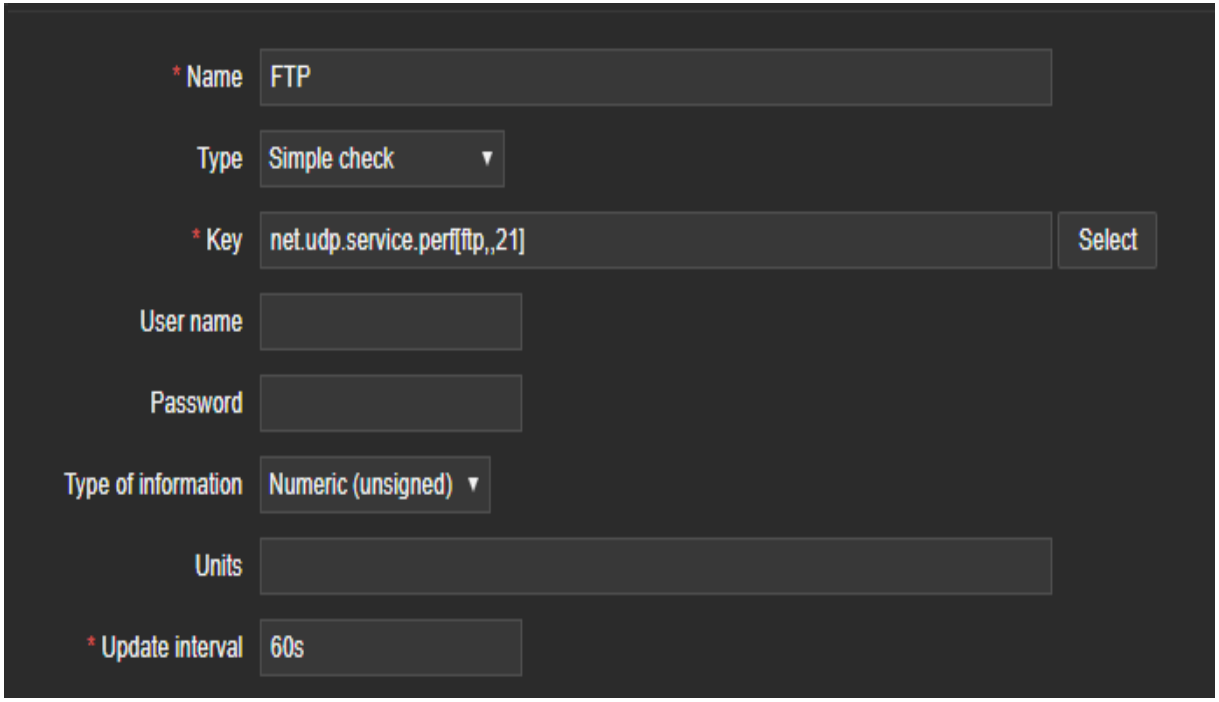
- **Se agrupan en un template, para aplicar a hosts concretos.**
- **Simple check**
- **SNMP Agent**
- **Zabbix Agent**

Son los elementos que recopilan datos de un host. Estos datos se almacenan en la BBDD.



Simple Check

Comprobaciones remotas sin agentes de los servicios, el responsable es el zabbix server.



Los más comunes:

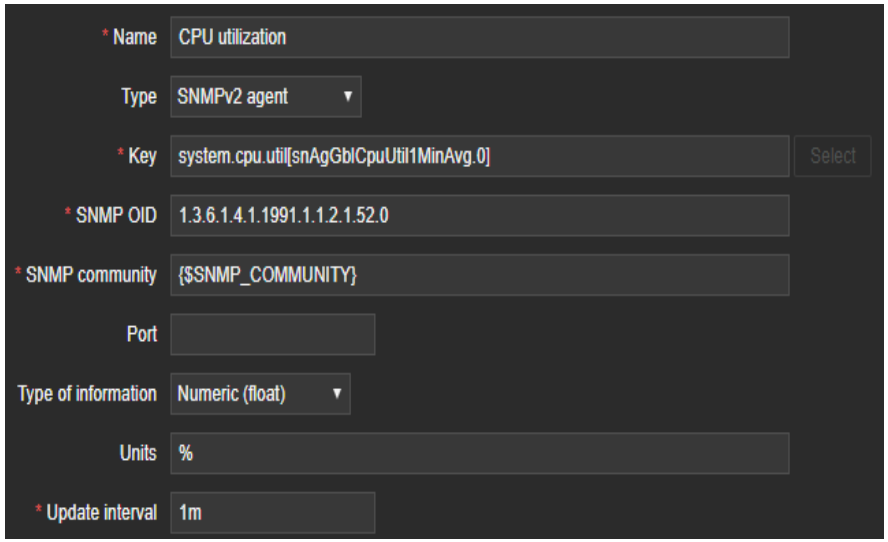
- **ICMP:** Disponibilidad por ping.
- **Servicio / Puerto:** Comprueba si el puerto es accesible.
- **Servicio / Tiempo:** Comprueba el tiempo de respuesta.

SNMP Agent

A través de protocolo SNMP en UDP, se consulta al dispositivo y devuelve valores que son traducidos por el zabbix server.

Es necesario configurar en el dispositivo:

- IP del servidor zabbix.
- Puerto de escucha del servidor zabbix.
- Comunidad o Clave.



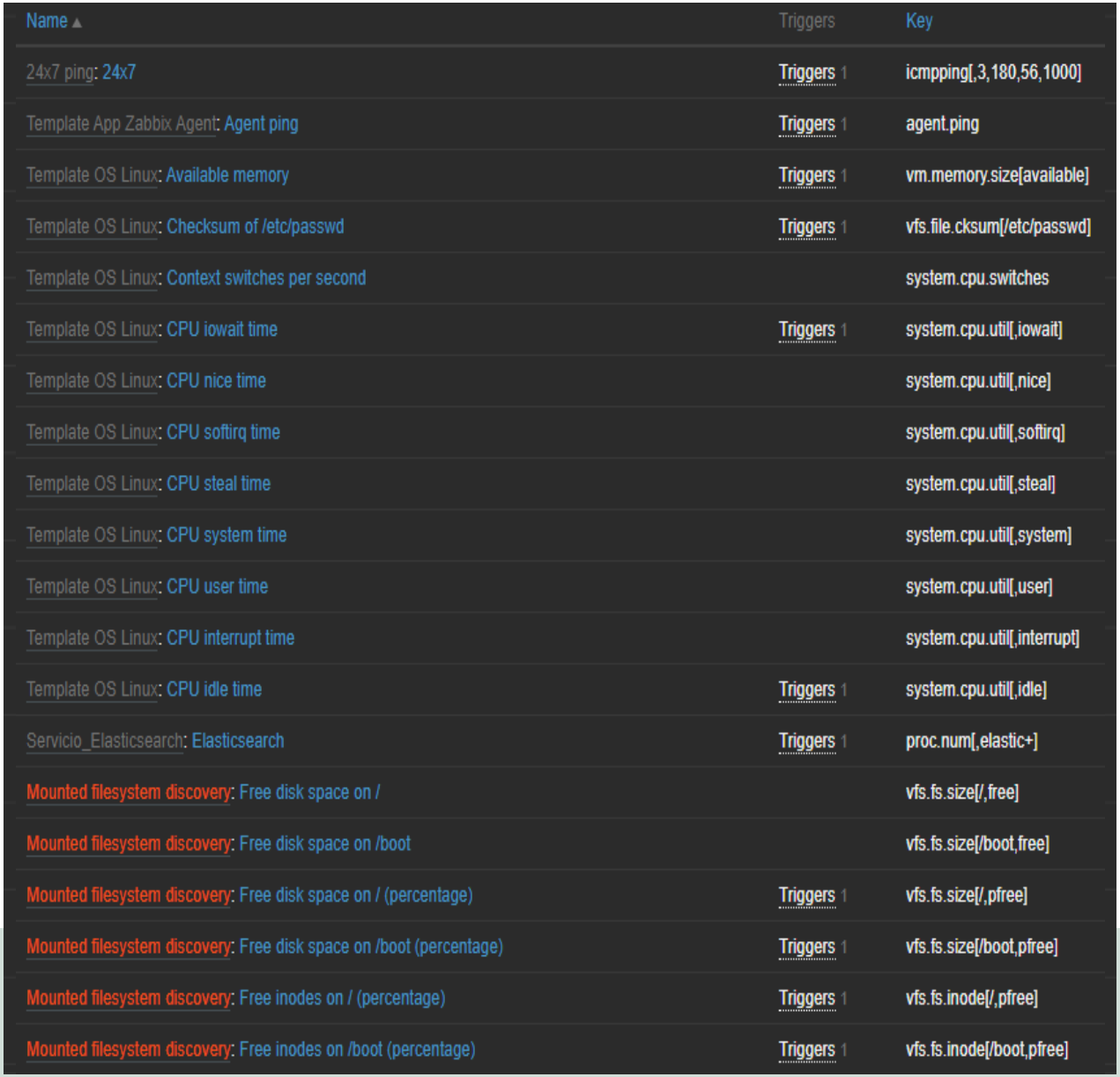
- **Templates configurados**.
- **Trabajar con MIBs**.

#	SMI	v1 Top OID/v2 MIB OID	MIB Name (File Name)	Traps	TCs	OIDs	Scalars	Tables	Tabulars
1	v1	1.3.6.1.4.1.637.3.1.4.10.44	ADN-MIB (hss1100adn.mib)	55	37	580	176	153	1640
2	v2	1.3.6.1.4.1.6486.800.1.2.1.15.1	ALCATEL-IND1-AAA-MIB (AlcatelIND1AAA.mib)	0	0	9	7	11	94
3	v2	1.3.6.1.4.1.6486.800	ALCATEL-IND1-BASE (AlcatelIND1Base.mib)	0	0	64	0	0	0
4	v2	1.3.6.1.4.1.6486.800.1.2.1.10.5.1	ALCATEL-IND1-BGP-MIB (AlcatelIND1Bgp.mib)	0	0	6	38	14	163
5	v2	1.3.6.1.4.1.6486.800.1.1.1.3.1	ALCATEL-IND1-CHASSIS-MIB (AlcatelIND1Chassis.mib)	3	12	10	13	4	22

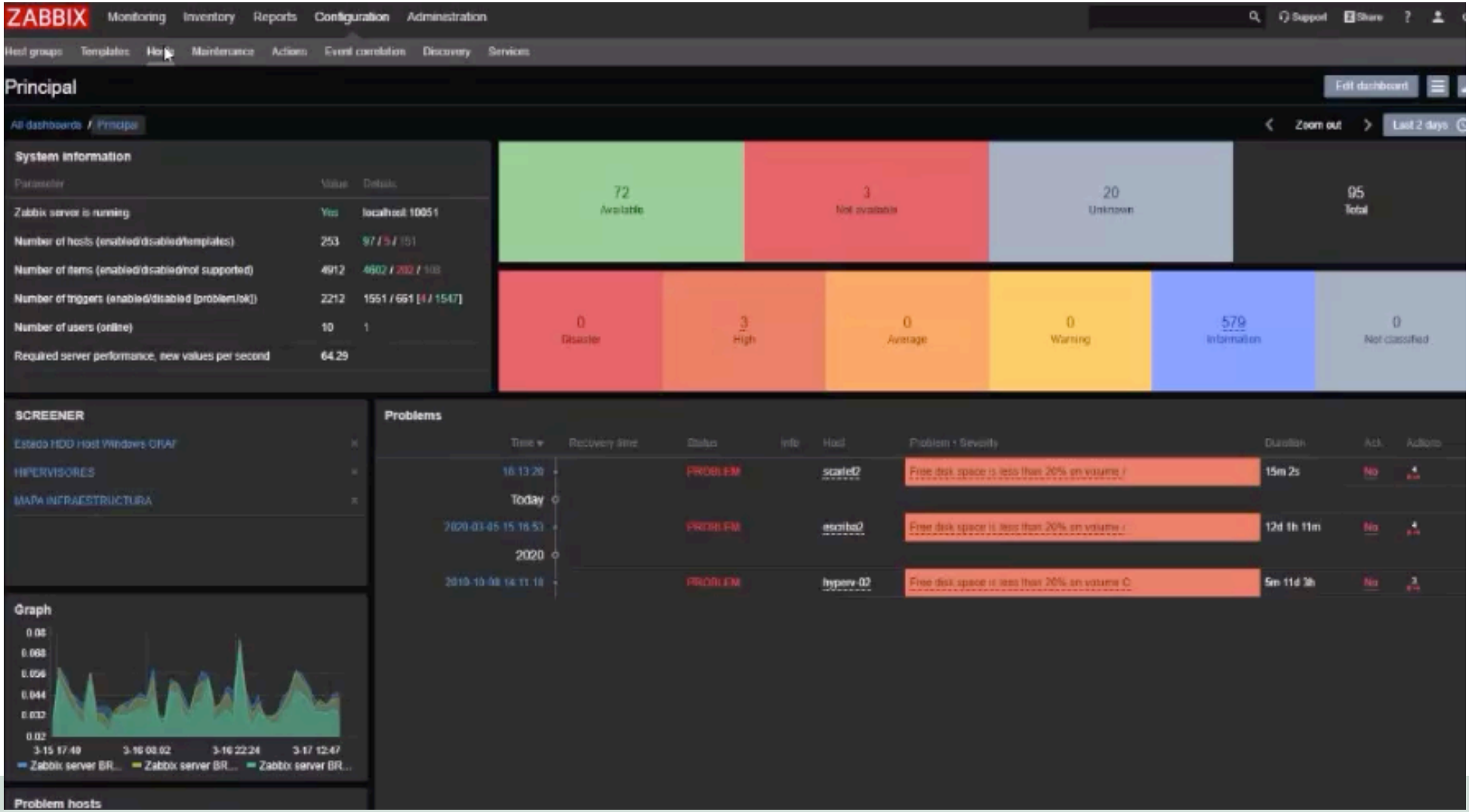
Zabbix Agent

Programas recolectores los cuales reciben peticiones del servidor y devuelven datos.

- Es necesario un S.O.
- Descubren y monitorizan:
- A) CPU
- B) Memory
- C) Disk
- D)Service
- E)Network
- Uptime, Users...
- * Particularidades...



Name ▲	Triggers	Key
24x7 ping: 24x7	Triggers 1	icmpping[,3,180,56,1000]
Template App Zabbix Agent: Agent ping	Triggers 1	agent.ping
Template OS Linux: Available memory	Triggers 1	vm.memory.size[available]
Template OS Linux: Checksum of /etc/passwd	Triggers 1	vfs.file.cksum[/etc/passwd]
Template OS Linux: Context switches per second		system.cpu.switches
Template OS Linux: CPU iowait time	Triggers 1	system.cpu.util[,iowait]
Template OS Linux: CPU nice time		system.cpu.util[,nice]
Template OS Linux: CPU softirq time		system.cpu.util[,softirq]
Template OS Linux: CPU steal time		system.cpu.util[,steal]
Template OS Linux: CPU system time		system.cpu.util[,system]
Template OS Linux: CPU user time		system.cpu.util[,user]
Template OS Linux: CPU interrupt time		system.cpu.util[,interrupt]
Template OS Linux: CPU idle time	Triggers 1	system.cpu.util[,idle]
Servicio_Elasticsearch: Elasticsearch	Triggers 1	proc.num[,elastic+]
Mounted filesystem discovery: Free disk space on /		vfs.fs.size[/,free]
Mounted filesystem discovery: Free disk space on /boot		vfs.fs.size[/boot,free]
Mounted filesystem discovery: Free disk space on / (percentage)	Triggers 1	vfs.fs.size[/,pfree]
Mounted filesystem discovery: Free disk space on /boot (percentage)	Triggers 1	vfs.fs.size[/boot,pfree]
Mounted filesystem discovery: Free inodes on / (percentage)	Triggers 1	vfs.fs.inode[/,pfree]
Mounted filesystem discovery: Free inodes on /boot (percentage)	Triggers 1	vfs.fs.inode[/boot,pfree]

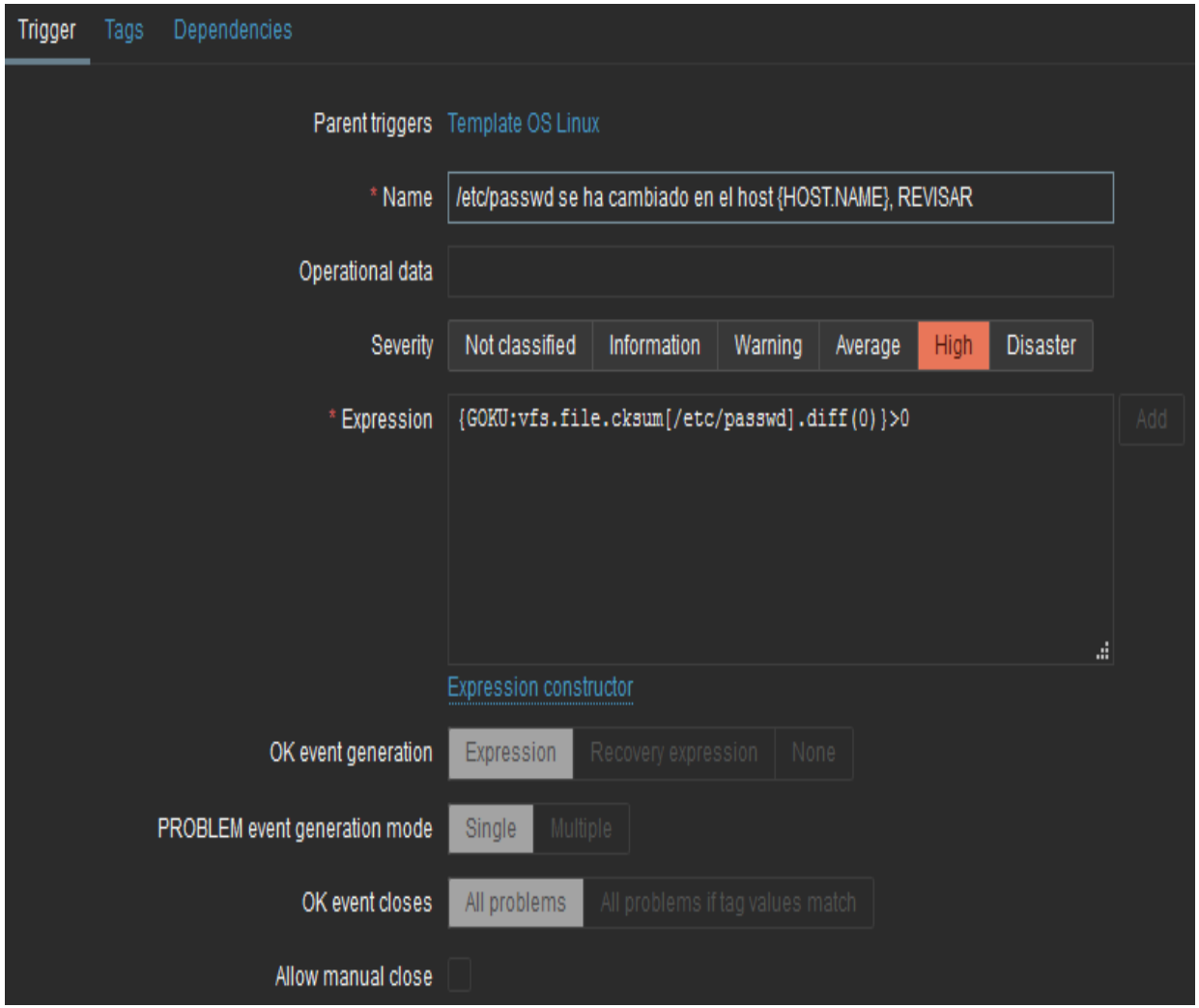


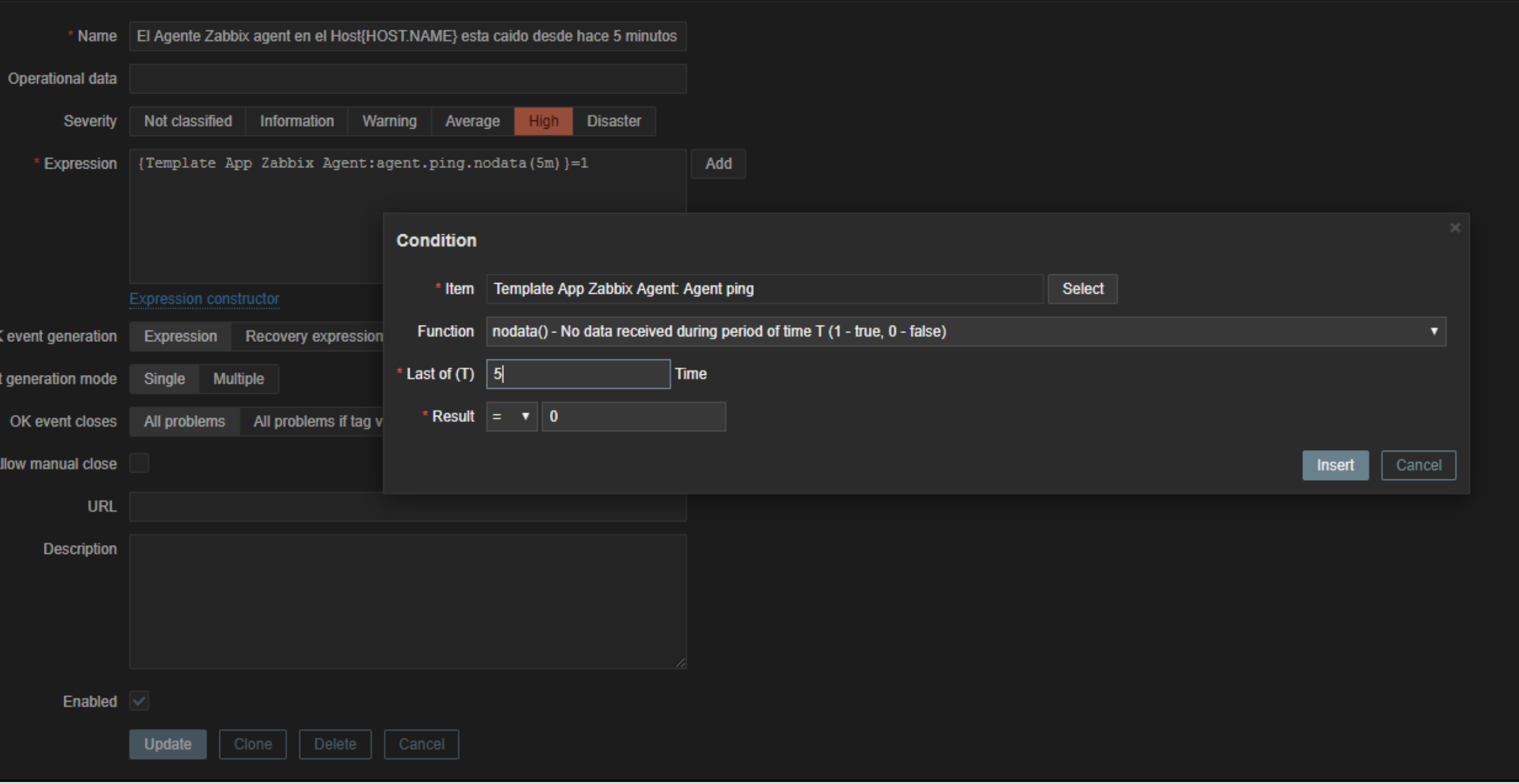
Vídeo 2: Host – Item – Template - Agente

Los Ítems solo recopilan, para evaluar los mismos, necesitamos triggers.

En él se define un umbral de lo que es aceptable, si se supera dicho umbral, se “dispara” un estado de problema.

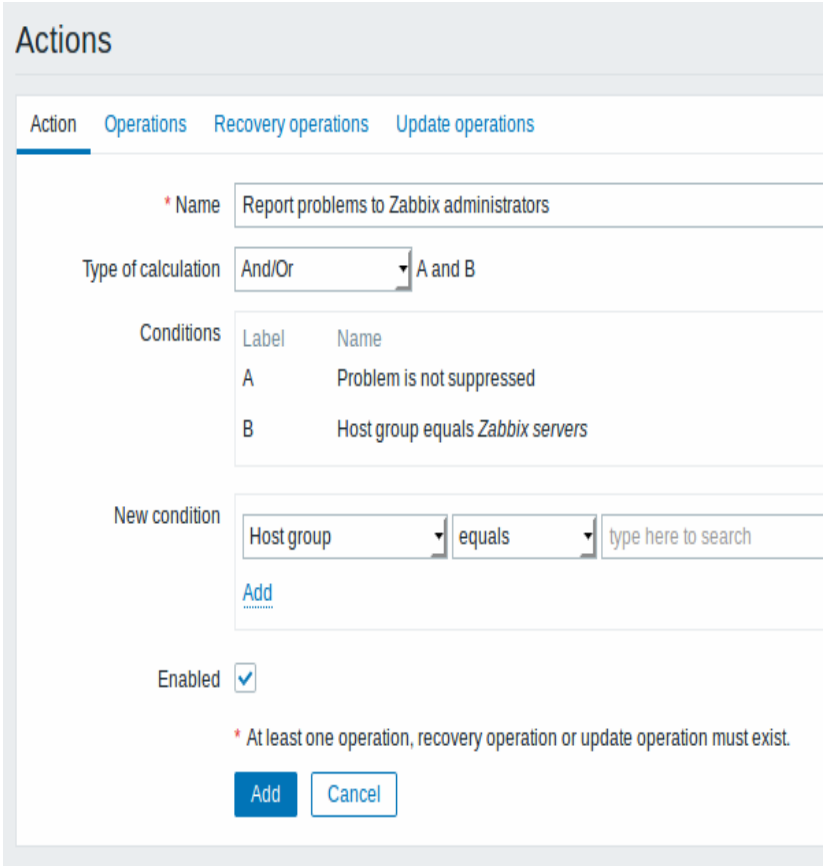
Si vuelve a estar en nivel aceptable, se vuelve al estado OK.




* Name
El Agente Zabbix agent en el Host{HOST.NAME} esta caido desde hace 5 minutos
Operational data
Severity
Not classified
Information
Warning
Average
High
Disaster
* Expression
{Template App Zabbix Agent:agent.ping.nodata(5m)}=1
Add
Expression constructor
event generation
Expression
Recovery expression
generation mode
Single
Multiple
OK event closes
All problems
All problems if tag v
llow manual close
URL
Description
Enabled
Update
Clone
Delete
Cancel
Condition
* Item
Template App Zabbix Agent: Agent ping
Select
Function
nodata() - No data received during period of time T (1 - true, 0 - false)
* Last of (T)
5
Time
* Result
=
0
Insert
Cancel

Nos permiten realizar operaciones como resultado de eventos, por ejemplo enviar notificaciones.

- Trigger Events: cuando el estado cambia de OK a PROBLEM o viceversa.
- Discovery Events: cuando se llevan a cabo detección de redes.
- Discovery Events: cuando existen nuevos agentes activos.
- Internal Events: cuando los elementos no son compatibles o los triggers pasan a estado desconocido



Name: debe ser único.

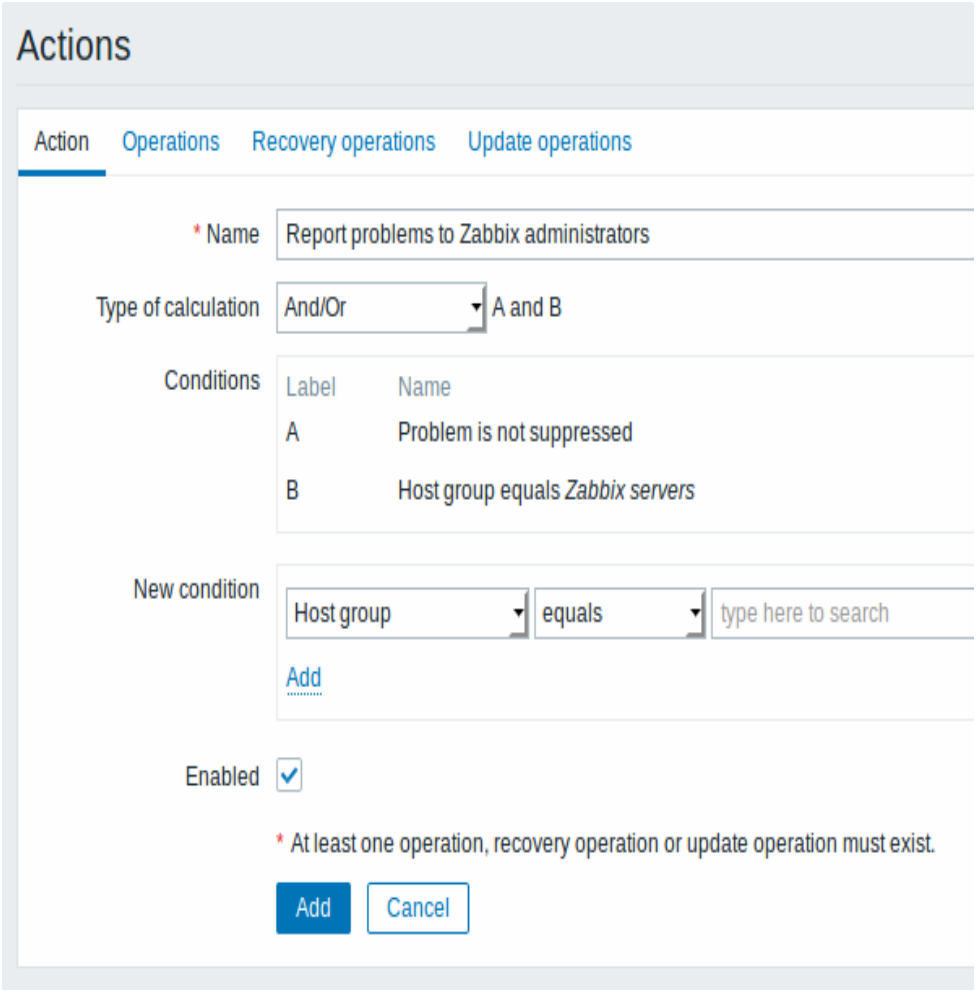
Type of calculation: selección de la opción de evaluación (una o varias)

- AND
- OR
- AND/OR

Conditions: lista de condiciones que deben cumplirse para ejecutarse.

New condition: selecciona una nueva condición para añadir a las existentes

Enabled: activar la acción.



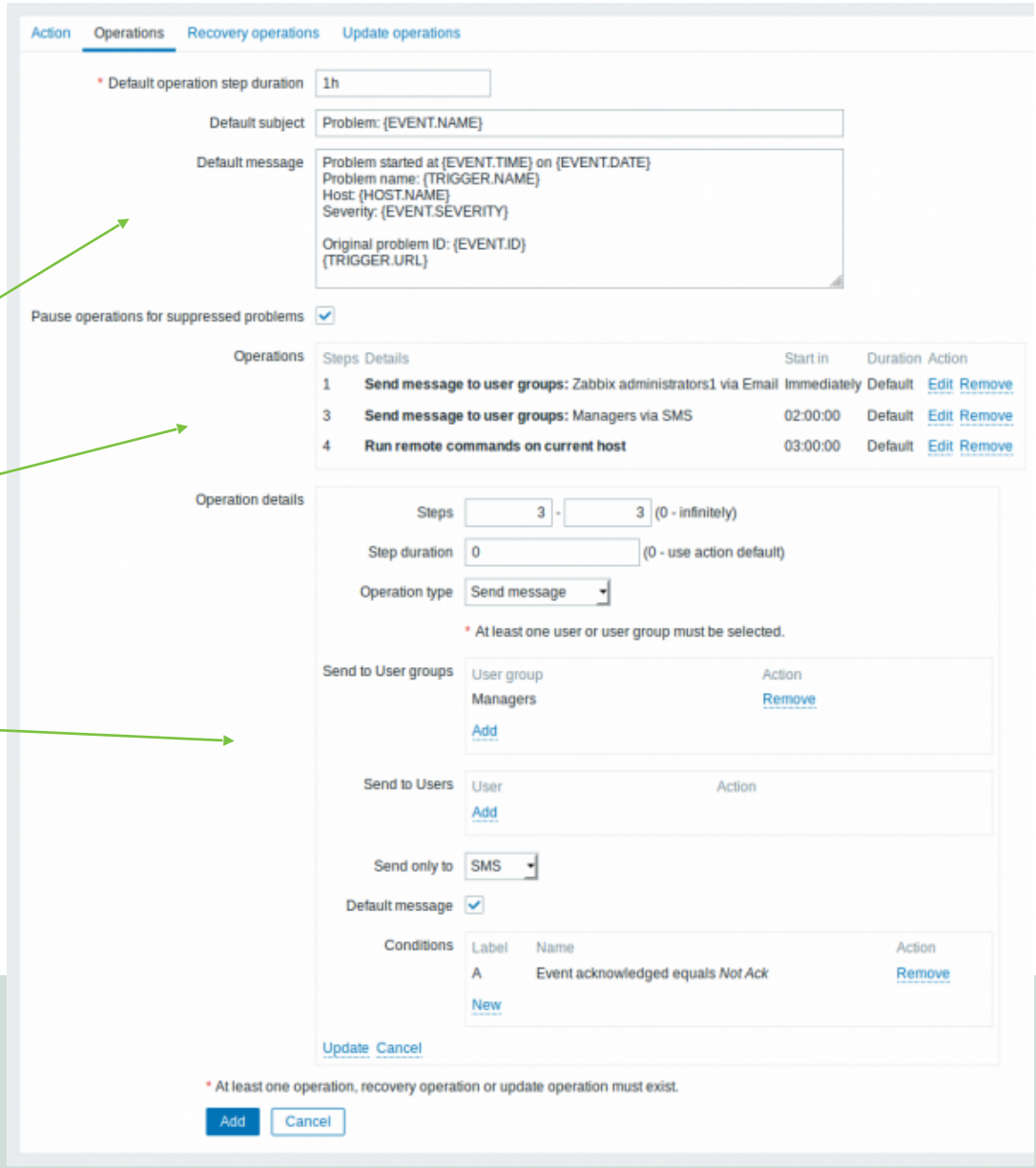
Operations

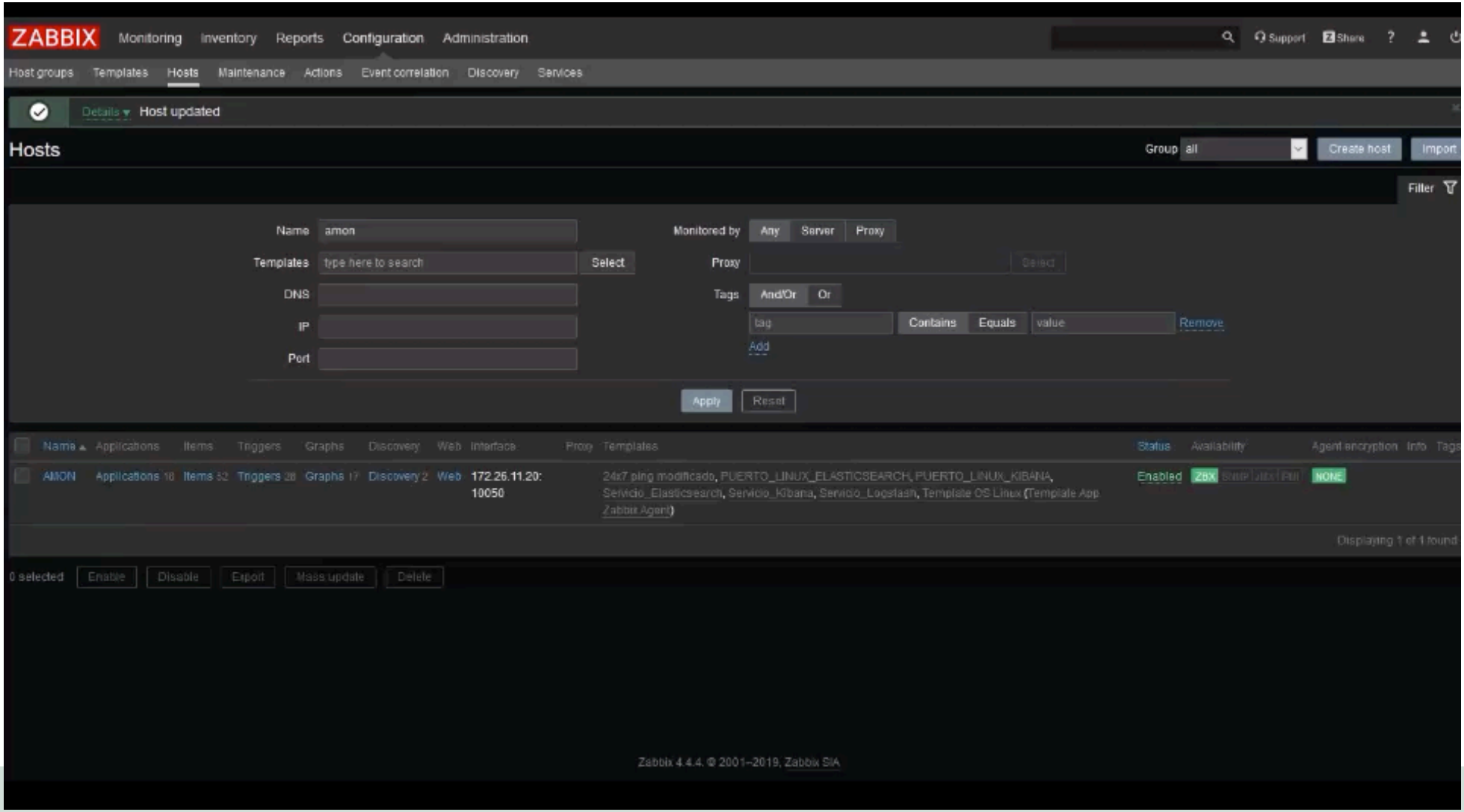
Nos permite configurar acciones a realizar:

a) Mensaje

b) b) Ejecutar comandos/Scripts

- Formato de la comunicación.
- Orden de actuaciones.
- Configuración de métodos de comunicación.





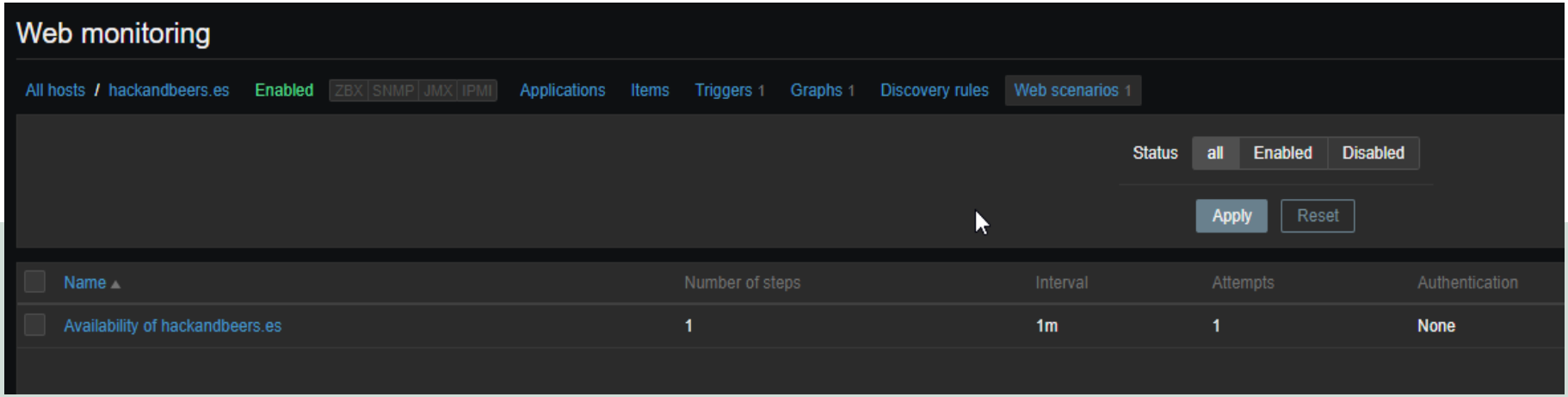
sedian Seguridad Digital de Andalucía

Vídeo 3: Triggers - Actions

Web Monitoring

Nos permite chequear la disponibilidad de los sitios web, teniendo su propio apartado en el hosts (Web Scenarios)

- Permite HTTP y HTTPS
- Velocidad de descarga por segundo
- Tiempo de respuesta
- Código de respuesta



Name: debe ser único.

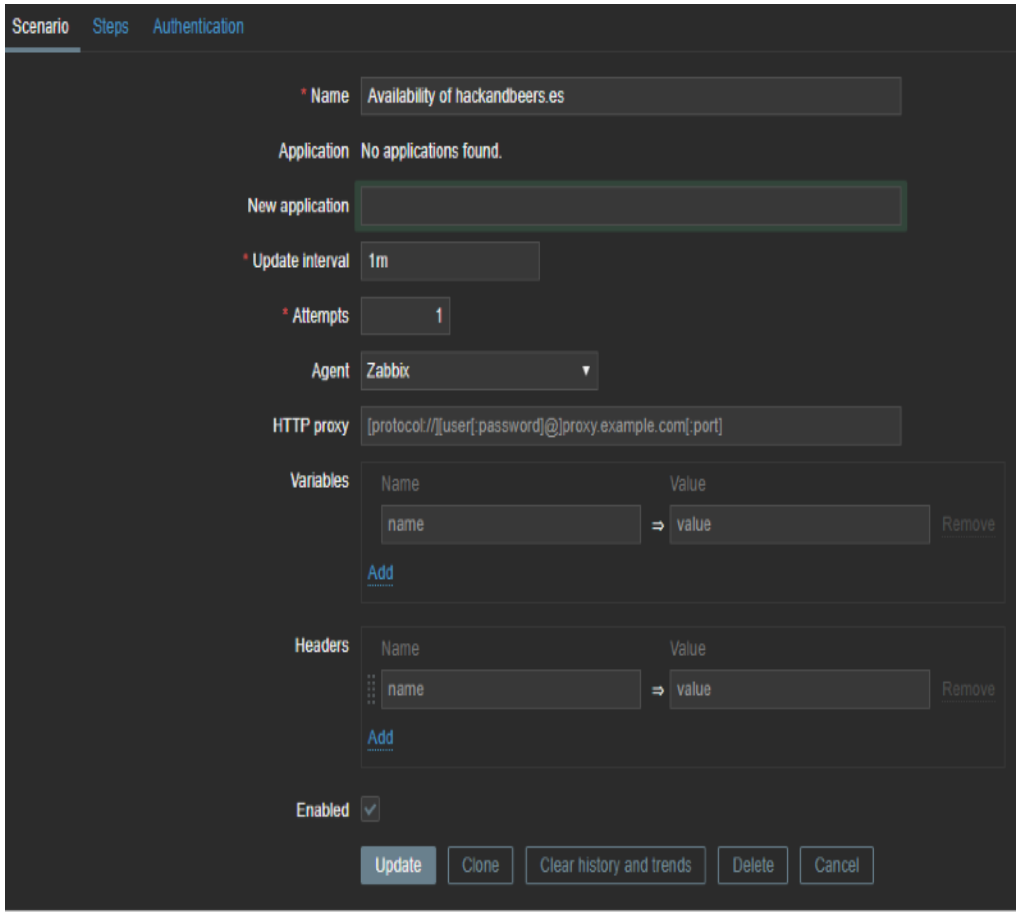
Application: para agrupar, mostrar en la monitorización.

Update Interval: mínimo 30s.

Agent: navegadores o zabbix.

Attempts: intentos de ejecución.

HTTP proxy: especificar los datos si debemos pasar por un proxy



Name: debe ser único.

Permite monitorizar varios sitios o s

URL: URL a conectar para recibir los datos. (limite 2048 caracteres).

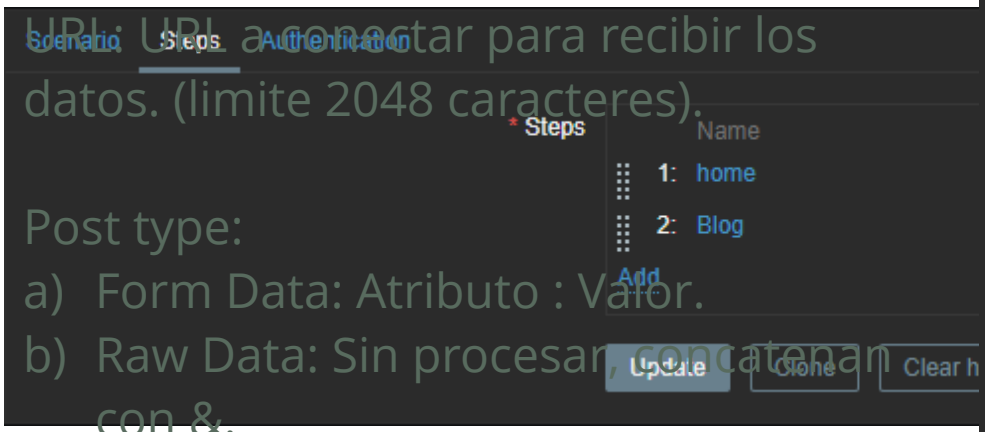
Post type:

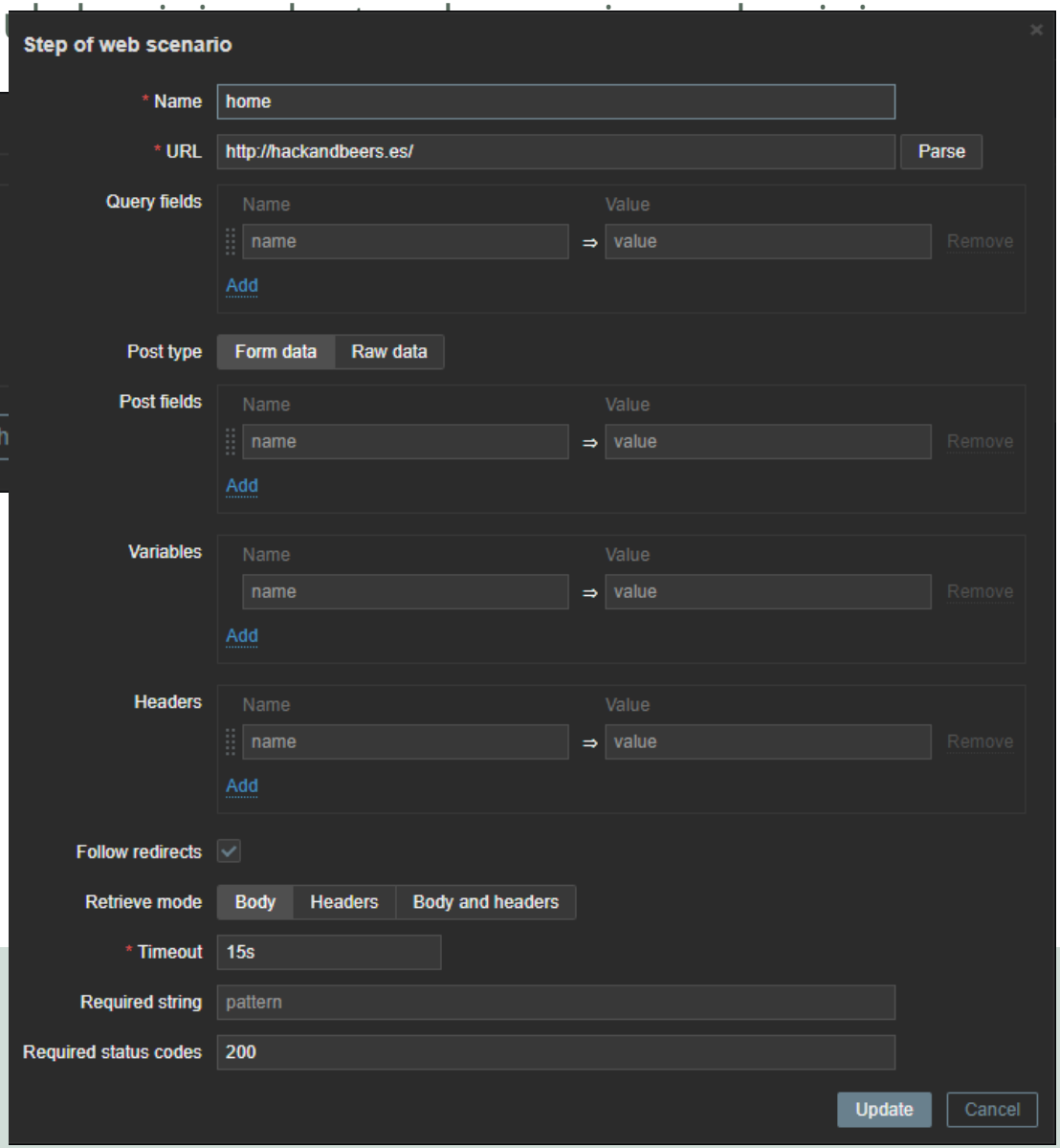
a) Form Data: Atributo : Valor.
b) Raw Data: Sin procesar, concatenan con &.

Follow redirects: permite redirecciones.

Required string: comprueba si recoge el valor de la cadena.

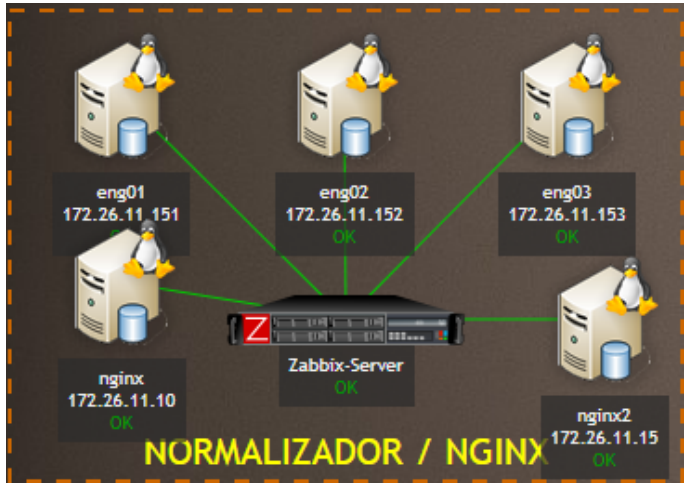
Required Status codes: si recibe otro código, se produce un problema.

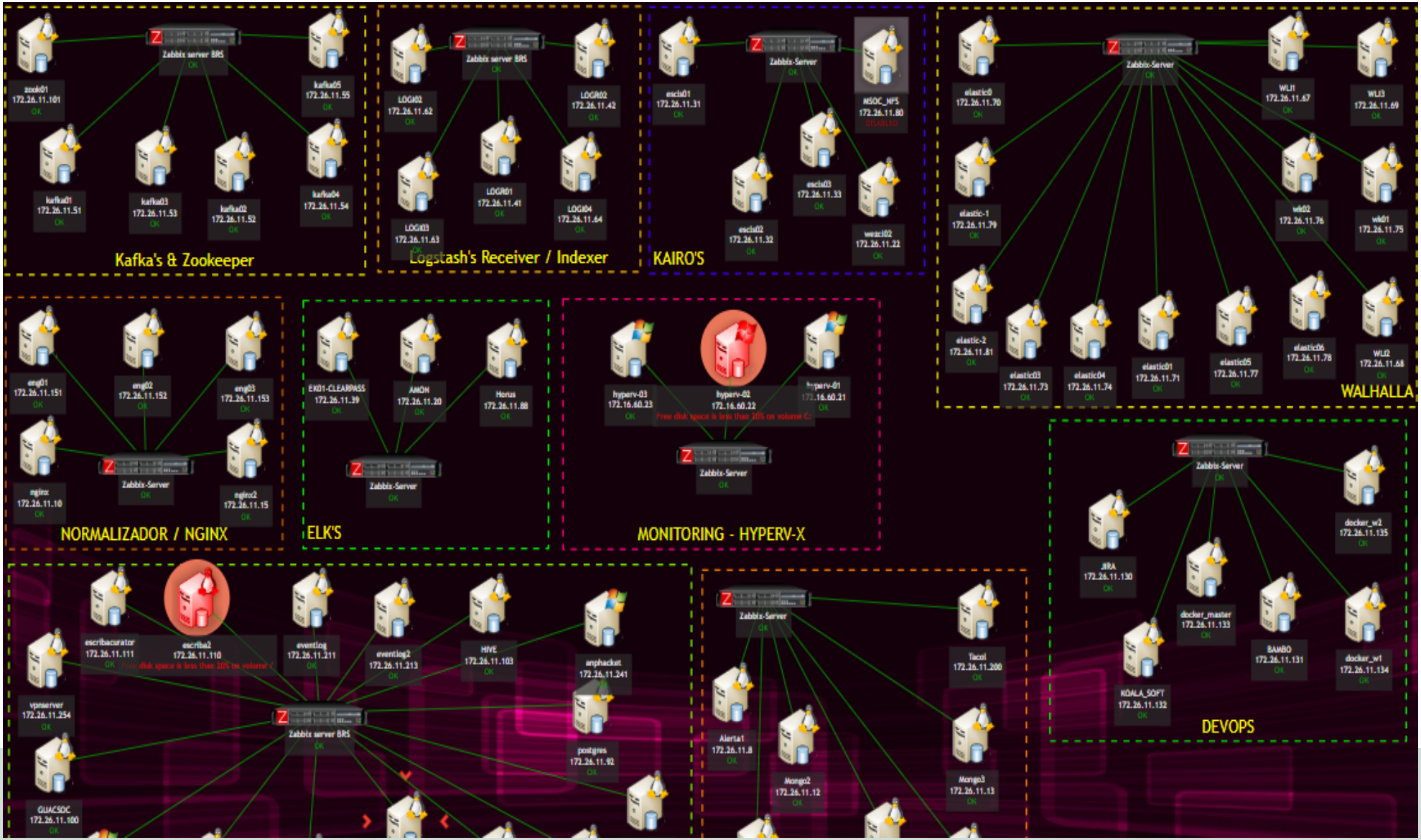




Representación grafica e interactiva de los elementos y su estado.

- Añadir Hosts
- Añadir Relaciones entre hosts
- Añadir estado Triggers
- Submapas de otras estructuras
- Imágenes customizables, formato distinto según estado
- Se basan en mapas vectoriales
- Públicos / privados





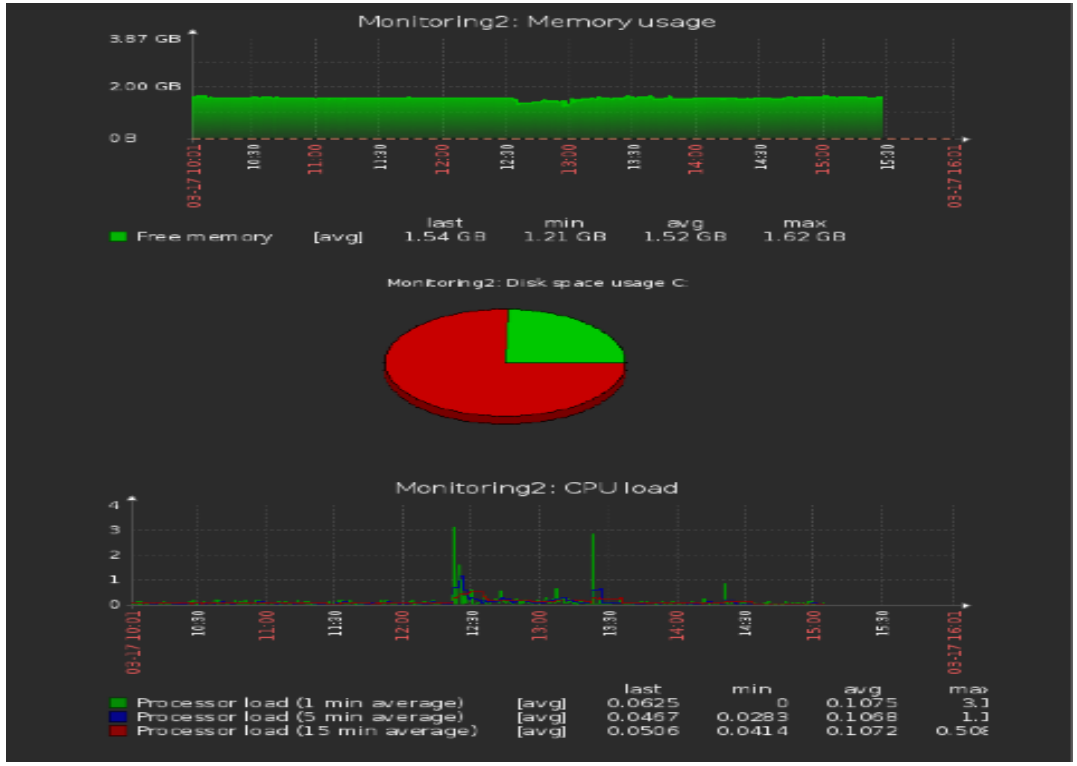
sedian Seguridad Digital de Andalucía

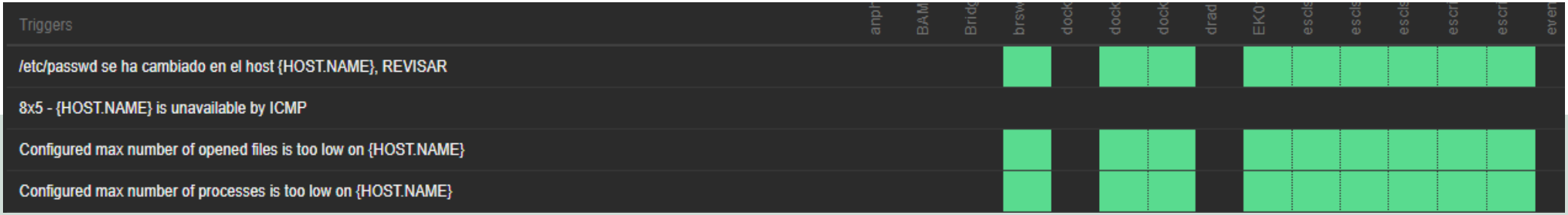
Network Maps

Screens

Nos permite agrupar información de varias fuentes (Ítems), organizada por grupos o hosts.

- Gráficos simples
- Histórico de datos
- Información de eventos
- Información de la BBDD





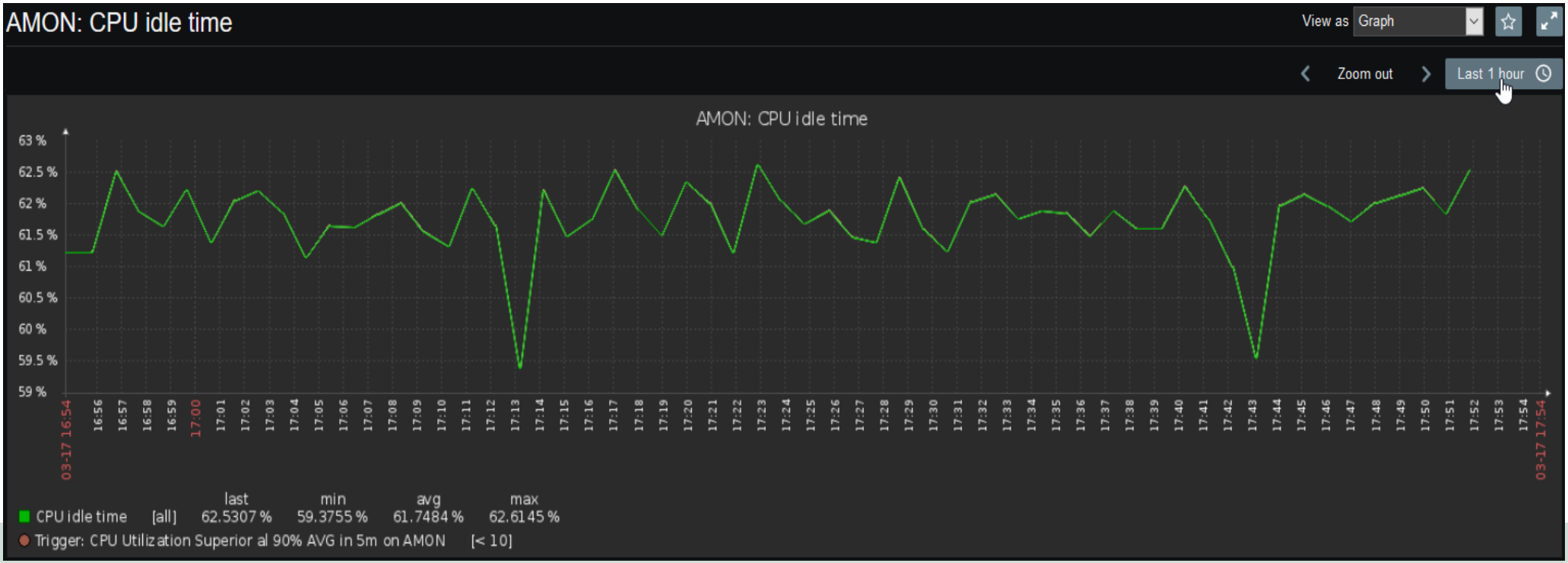
Análisis de la información en BBDD

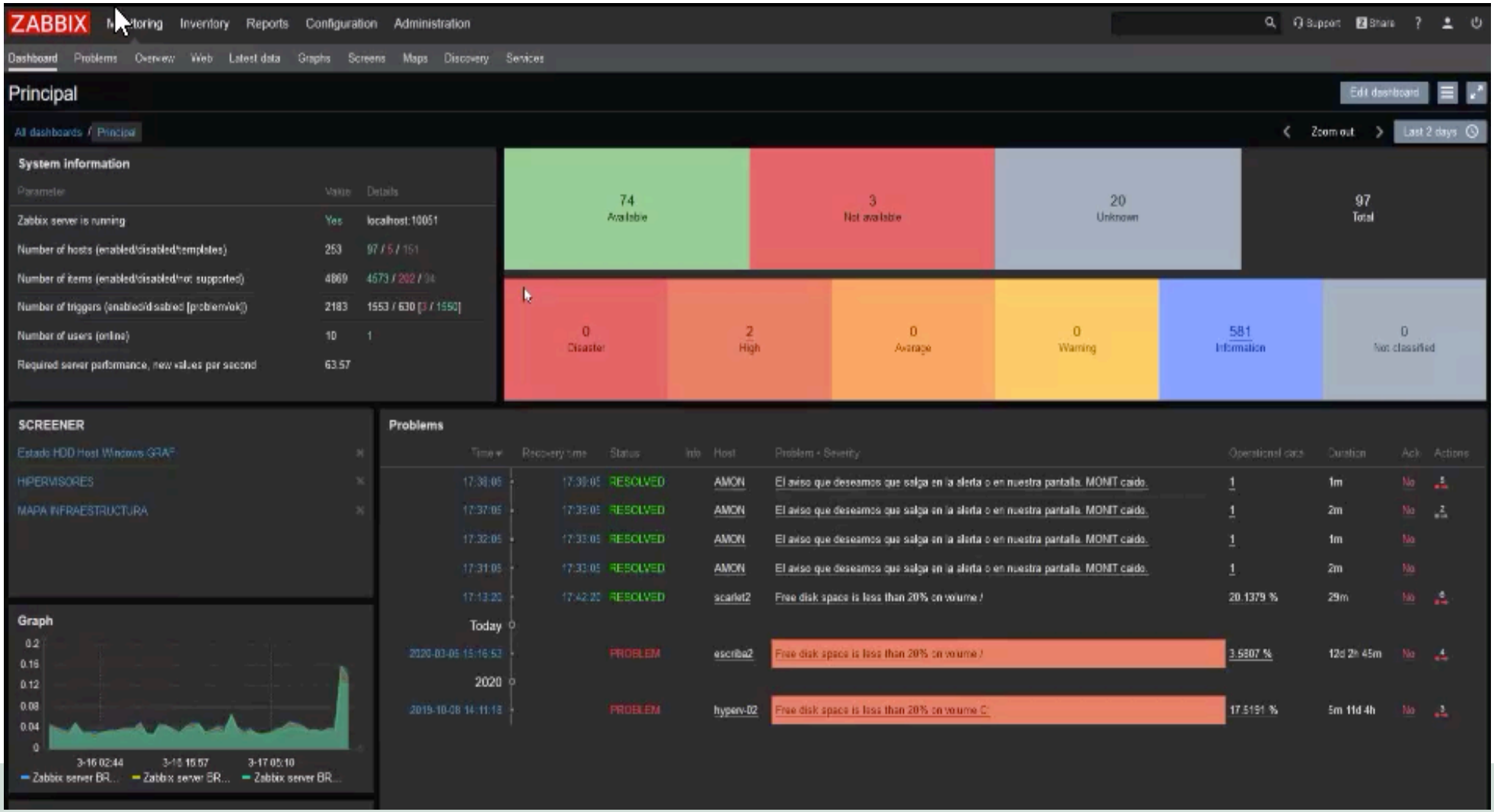
sedian Seguridad Digital de Andalucía

Para obtener todos los registros de un hosts, debemos irnos a la siguiente ruta:

Monitoring -> Latest Data

Seleccionamos el dispositivo y pulsamos en Apply:




ZABBIX
Inventory
Reports
Configuration
Administration
Dashboard
Problems
Overview
Web
Latest data
Graphs
Screens
Maps
Discovery
Services
Principal
Edit dashboard
All dashboards / Principal
Zoom out
Last 2 days
System information
Parameter
Value
Details
Zabbix server is running
Yes
localhost:10051
Number of hosts (enabled/disabled/templates)
253
97 / 5 / 151
Number of items (enabled/disabled/not supported)
4869
4573 / 292 / 34
Number of triggers (enabled/disabled [problem/ok])
2183
1553 / 630 [3 / 1550]
Number of users (online)
10
1
Required server performance, new values per second
63.57
74
Available
3
Not available
20
Unknown
97
Total
0
Disaster
2
High
0
Average
0
Warning
581
Information
0
Not classified
SCREENER
Estado HDD Host Windows GRAF
HIPERVISORES
MAPA INFRAESTRUCTURA
Graph
0.2
0.16
0.12
0.08
0.04
0
3-16 02:44
3-16 15:57
3-17 05:10
Zabbix server BR...
Zabbix server BR...
Zabbix server BR...
Problems
Time
Recovery time
Status
Info
Host
Problem • Severity
Operational data
Duration
Ack
Actions
RESOLVED
AMON
El aviso que deseamos que salga en la alerta o en nuestra pantalla. MONIT caido.
1
1m
No
RESOLVED
AMON
El aviso que deseamos que salga en la alerta o en nuestra pantalla. MONIT caido.
1
2m
No
RESOLVED
AMON
El aviso que deseamos que salga en la alerta o en nuestra pantalla. MONIT caido.
1
1m
No
RESOLVED
AMON
El aviso que deseamos que salga en la alerta o en nuestra pantalla. MONIT caido.
1
2m
No
RESOLVED
scarlet2
Free disk space is less than 20% on volume /
20.1379 %
29m
No
Today
PROBLEM
escriba2
Free disk space is less than 20% on volume /
3.5807 %
12d 2h 45m
No
2020
PROBLEM
hyperv-02
Free disk space is less than 20% on volume C:
17.5191 %
5m 11d 4h
No

sedian Seguridad Digital de Andalucía