

sedian

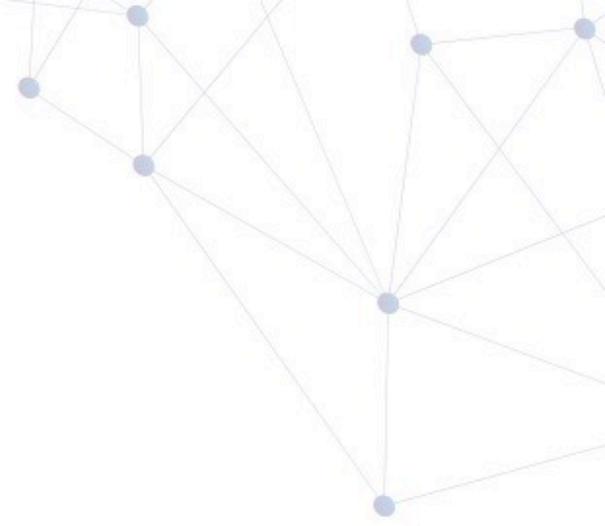
Seguridad Digital
de Andalucía

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), advirtiéndolo 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:**

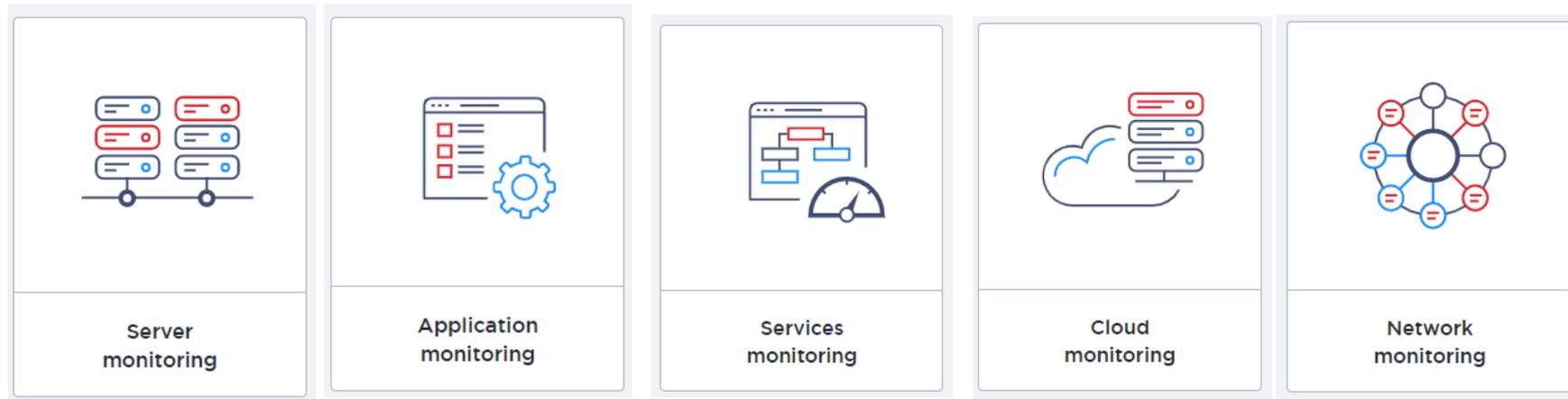
Solo versión de pago, no debes/puedes salirte de lo que te ofrece el fabricante.

- 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.

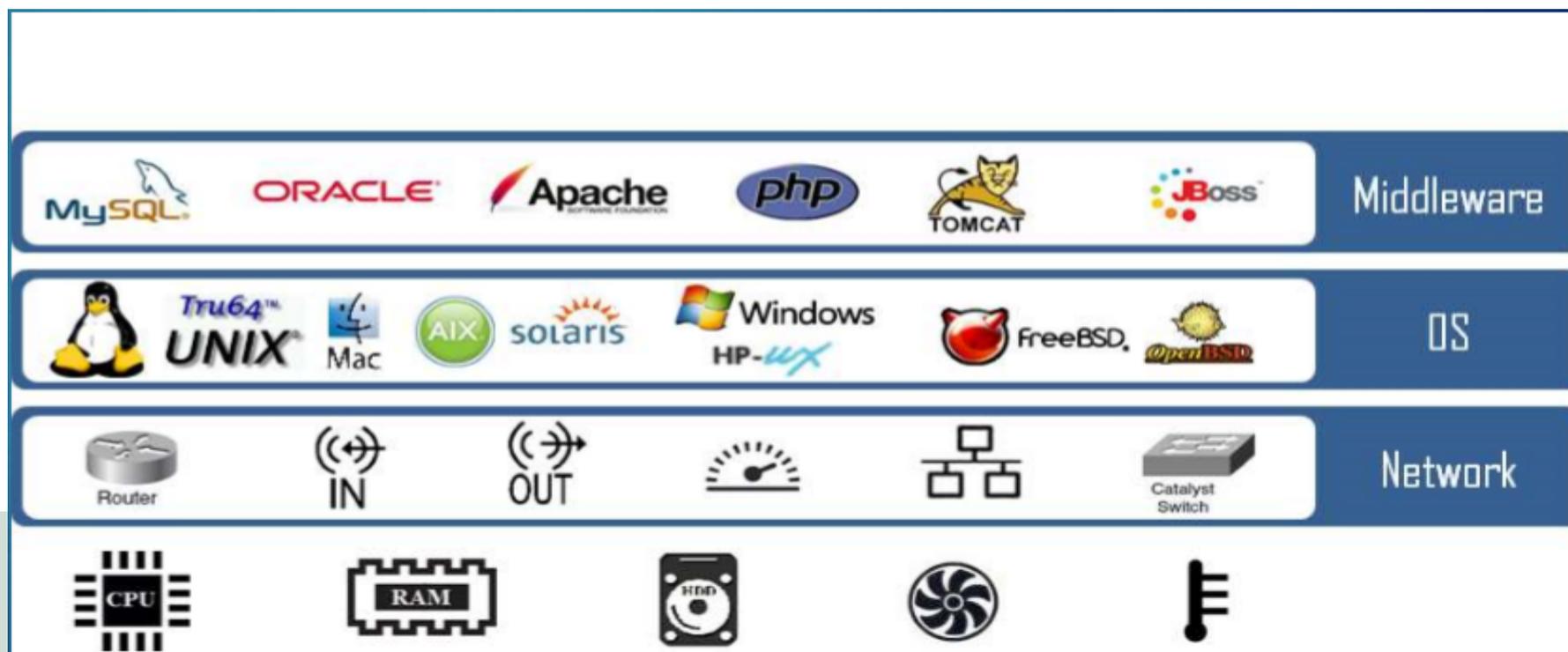
Zabbix es un sistema de monitorización de nivel empresarial, diseñado para monitorizar:

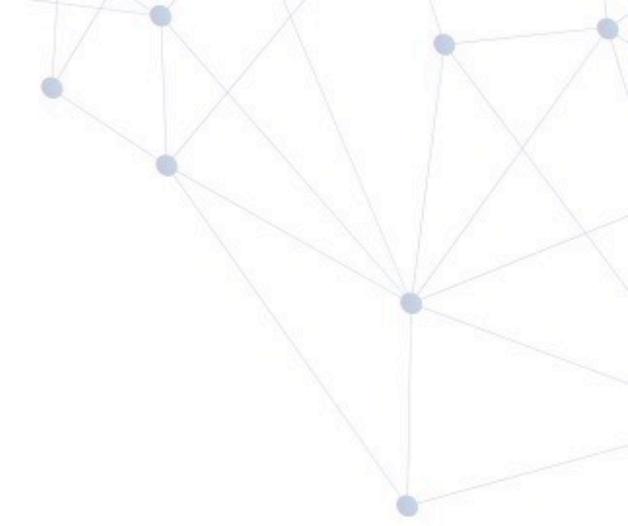


ZABBIX

Zabbix puede monitorizar de diversas formas:

- SNMP v1,2
- Zabbix Agent
- ICMP
- Port Monitoring
- JMX Monitoring
- IPMI Monitoring





Requisitos y despliegue de Zabbix

- 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-monitorizacion-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

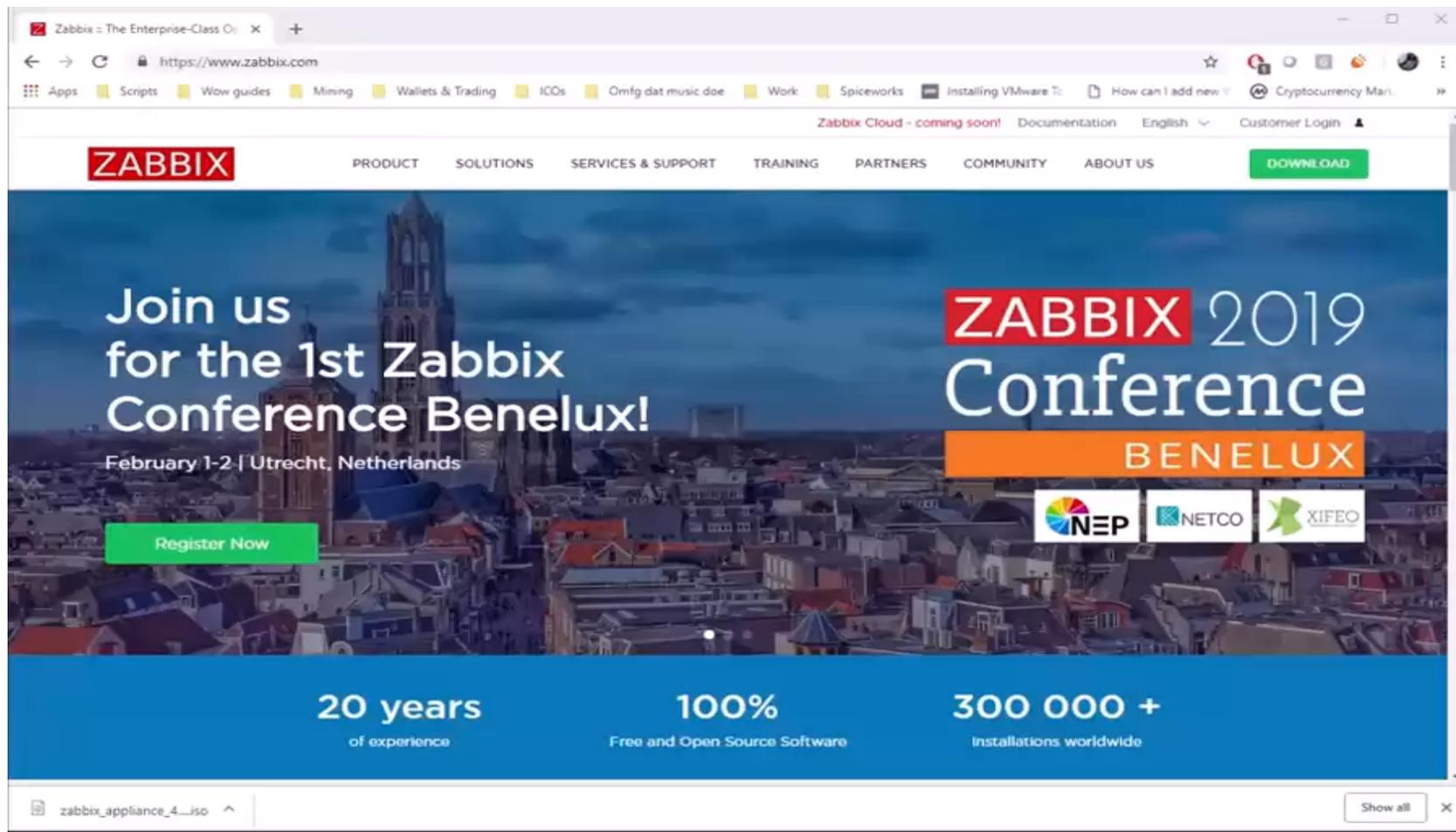
A screenshot of a terminal window showing the 'Zabbix Appliance Installer boot menu'. The 'ubuntu' logo is at the top. The menu lists several installation options, with the first one highlighted in blue. At the bottom, it says 'Press ENTER to boot or TAB to edit a menu entry'.

```
ubuntu®

Zabbix Appliance Installer boot menu

Install Ubuntu Server with Zabbix server (MySQL)
Install Ubuntu Server with Zabbix server (PostgreSQL)
Install Ubuntu Server with Zabbix proxy (MySQL)
Install Ubuntu Server with Zabbix proxy (SQLite3)
Test memory
Boot from first hard disk
Help

Press ENTER to boot or TAB to edit a menu entry
```



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`

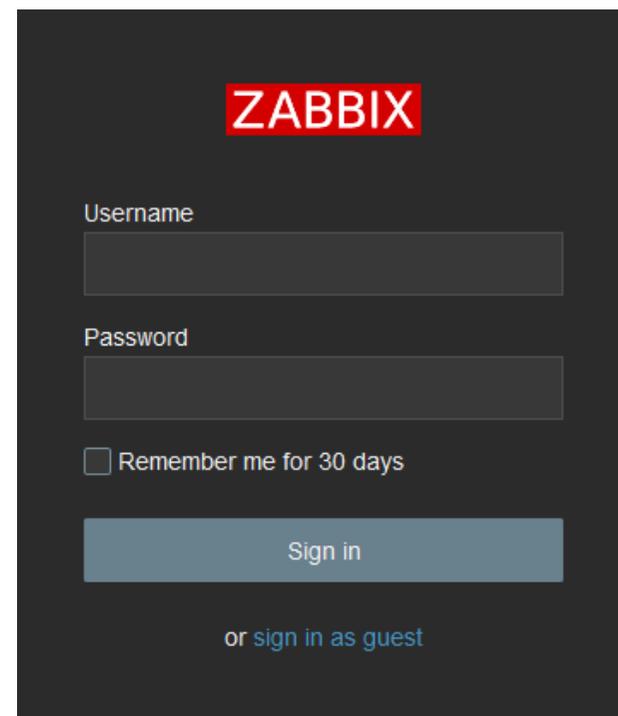
- Cambiar en VM

Database-> `root:zabbix`

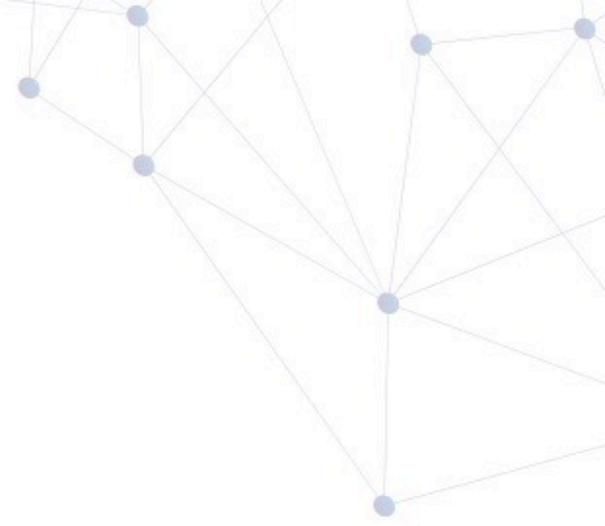
- `/etc/zabbix/zabbix_server.conf;`

- `/etc/zabbix/web/zabbix.conf.php`

Zabbix frontend> `Admin:zabbix`



The image shows the Zabbix login interface. At the top, the word "ZABBIX" is displayed in white text on a red rectangular background. Below this, there are two input fields: "Username" and "Password". Under the "Password" field, there is a checkbox labeled "Remember me for 30 days". A blue "Sign in" button is positioned below the checkbox. At the bottom of the form, the text "or sign in as guest" is displayed in a smaller, lighter blue font.



Elementos

Host

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

Se incluyen en grupos para su gestión.

IP o DNS necesarios.

Grupo

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

Host Templates IPMI Tags Macros Inventory Encryption

* Host name

Visible name

* Groups

* At least one interface must exist.

Agent interfaces

IP address	DNS name	Connect to	Port
<input type="text" value="192.168.6.87"/>	<input type="text"/>	<input type="button" value="IP"/> <input type="button" value="DNS"/>	<input type="text" value="10050"/>

SNMP interfaces

IP address	DNS name	Connect to	Port
<input type="text" value="127.0.0.1"/>	<input type="text"/>	<input type="button" value="IP"/> <input type="button" value="DNS"/>	<input type="text" value="161"/>

Use bulk requests

JMX interfaces

IPMI interfaces

Description

Monitored by proxy

Enabled

Host Templates IPMI Tags Inventory Encryption

Host groups

Description Original

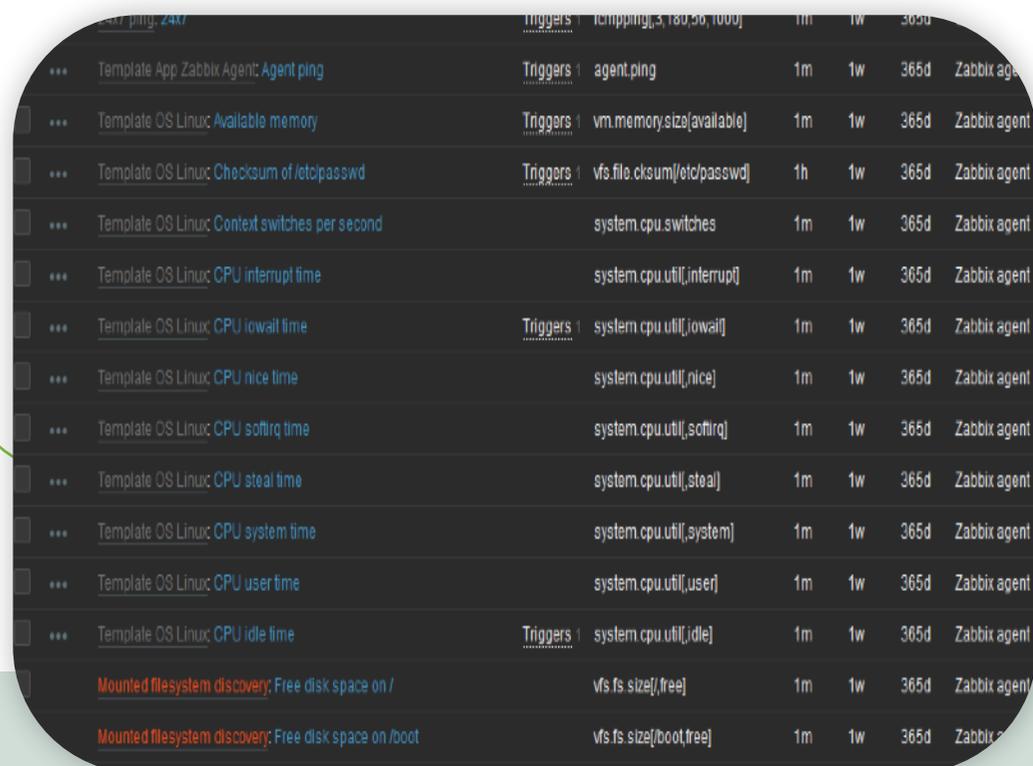
Monitored by proxy

Status Original

Se deben agregar para obtener los datos reales:

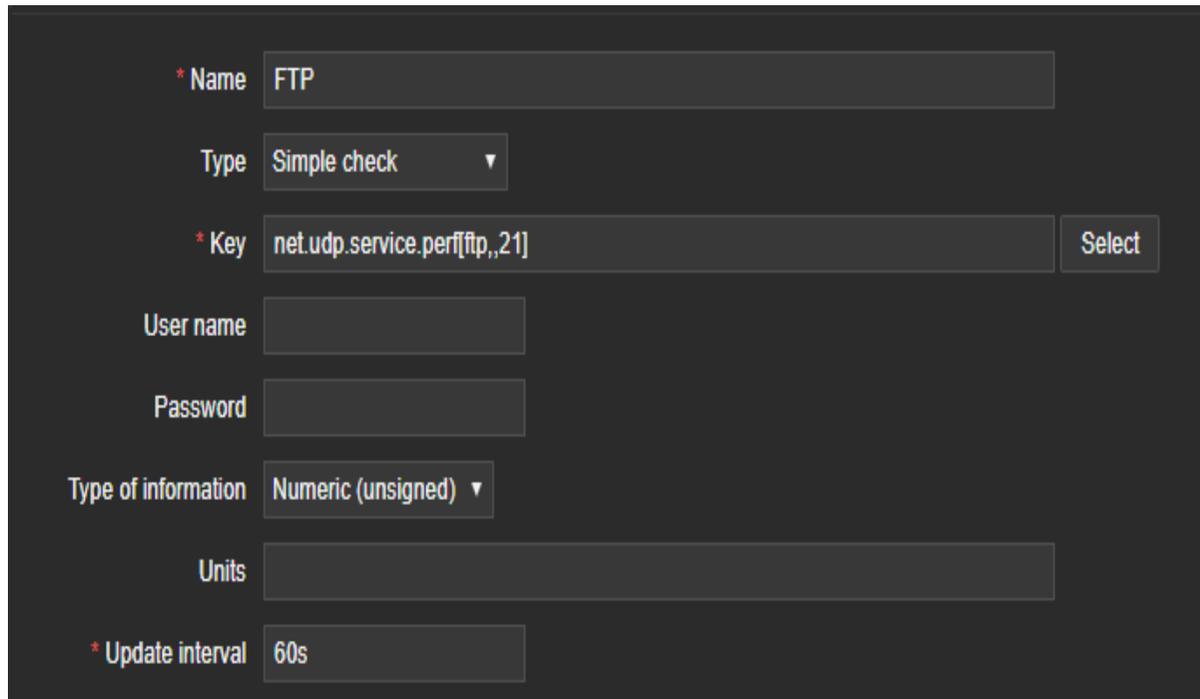
- Se agrupan en un **template**, para aplicar a **hosts concretos**.
- **Simple check**
- **SNMP Agent**
- **Zabbix Agent**

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

A screenshot of the Zabbix web interface showing a list of templates. The table has columns for Template Name, Triggers, and various metrics like Unit, Interval, and Last Update. The templates listed include 'Agent ping', 'Available memory', 'Checksum of /etc/passwd', and several 'CPU' related templates (interrupt, iowait, nice, softirq, steal, system, user, idle). At the bottom, there are two entries for 'Mounted filesystem discovery' for / and /boot.

Template Name	Triggers	Unit	Interval	Last Update	Agent
Template App Zabbix Agent: Agent ping	agent.ping	1m	1w	365d	Zabbix agent
Template OS Linux: Available memory	vm.memory.size[available]	1m	1w	365d	Zabbix agent
Template OS Linux: Checksum of /etc/passwd	vfs.file.cksum[/etc/passwd]	1h	1w	365d	Zabbix agent
Template OS Linux: Context switches per second	system.cpu.switches	1m	1w	365d	Zabbix agent
Template OS Linux: CPU interrupt time	system.cpu.util[,interrupt]	1m	1w	365d	Zabbix agent
Template OS Linux: CPU iowait time	system.cpu.util[,iowait]	1m	1w	365d	Zabbix agent
Template OS Linux: CPU nice time	system.cpu.util[,nice]	1m	1w	365d	Zabbix agent
Template OS Linux: CPU softirq time	system.cpu.util[,softirq]	1m	1w	365d	Zabbix agent
Template OS Linux: CPU steal time	system.cpu.util[,steal]	1m	1w	365d	Zabbix agent
Template OS Linux: CPU system time	system.cpu.util[,system]	1m	1w	365d	Zabbix agent
Template OS Linux: CPU user time	system.cpu.util[,user]	1m	1w	365d	Zabbix agent
Template OS Linux: CPU idle time	system.cpu.util[,idle]	1m	1w	365d	Zabbix agent
Mounted filesystem discovery: Free disk space on /	vfs.fs.size[/,free]	1m	1w	365d	Zabbix agent
Mounted filesystem discovery: Free disk space on /boot	vfs.fs.size[/boot,free]	1m	1w	365d	Zabbix agent

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



The image shows a configuration form for a Zabbix Simple Check. The fields are as follows:

- Name:** FTP
- Type:** Simple check (dropdown menu)
- Key:** net.udp.service.perf[ftp,,21] (with a Select button)
- User name:** (empty text field)
- Password:** (empty text field)
- Type of information:** Numeric (unsigned) (dropdown menu)
- Units:** (empty text field)
- Update interval:** 60s

Simple Check

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.

The screenshot shows the configuration for a Zabbix item named 'CPU utilization'. The configuration includes:

- Name: CPU utilization
- Type: SNMPv2 agent
- Key: system.cpu.util[snAgGblCpuUtil1MinAvg.0]
- SNMP OID: 1.3.6.1.4.1.1991.1.1.2.1.52.0
- SNMP community: {\$SNMP_COMMUNITY}
- Port: (empty)
- Type of information: Numeric (float)
- Units: %
- Update interval: 1m

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

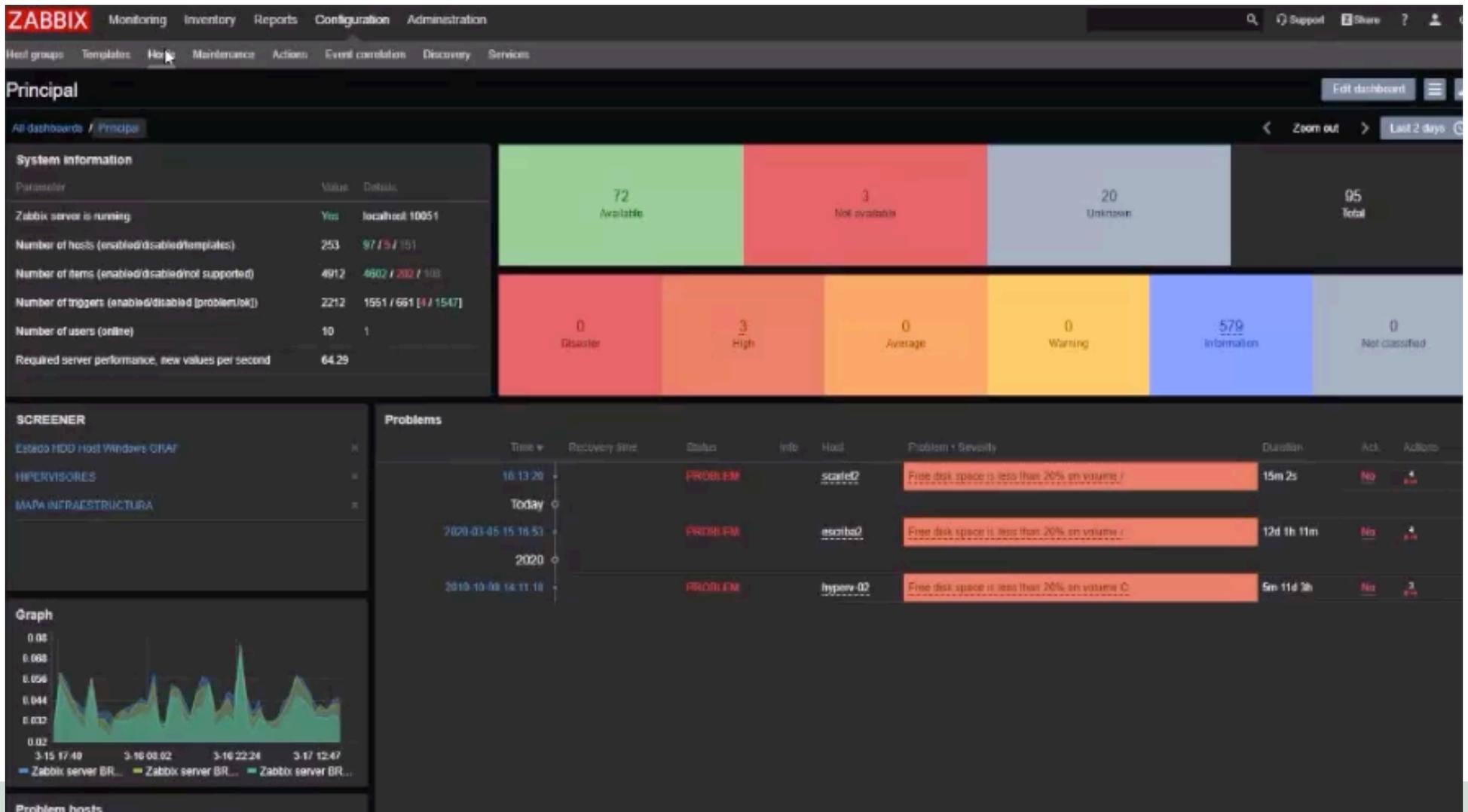
#	SMI	v1 Top OID/v2 MIB OID	MIB Name (File Name)	Traps	TCs	OIDs	Scalars	Tables	Tabulars
1	v1	1.3.6.1.4.1.637.3.1.4.10.44	ADN-MIB (hss1100adn.mib)	55	37	580	176	153	1640
2	v2	1.3.6.1.4.1.6486.800.1.2.1.15.1	ALCATEL-IND1-AAA-MIB (AlcatelIND1AAA.mib)	0	0	9	7	11	94
3	v2	1.3.6.1.4.1.6486.800	ALCATEL-IND1-BASE (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]



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.

Trigger Tags Dependencies

Parent triggers [Template OS Linux](#)

* Name

Operational data

Severity

* Expression

[Expression constructor](#)

OK event generation

PROBLEM event generation mode

OK event closes

Allow manual close

* Name

Operational data

Severity

* Expression

[Expression constructor](#)

Event generation

Event generation mode

OK event closes

Allow manual close

URL

Description

Enabled

Condition ✕

* Item

Function

* Last of (T) Time

* Result

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

Actions

Action Operations Recovery operations Update operations

* Name

Type of calculation A and B

Conditions	Label	Name
A		Problem is not suppressed
B		Host group equals Zabbix servers

New condition equals

[Add](#)

Enabled

* At least one operation, recovery operation or update operation must exist.

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.

Actions

Action Operations Recovery operations Update operations

* Name

Type of calculation A and B

Conditions	Label	Name
	A	Problem is not suppressed
	B	Host group equals Zabbix servers

New condition

[Add](#)

Enabled

* At least one operation, recovery operation or update operation must exist.

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.

Default operation step duration: 1h

Default subject: Problem: {EVENT.NAME}

Default message: Problem started at {EVENT.TIME} on {EVENT.DATE}
Problem name: {TRIGGER.NAME}
Host: {HOST.NAME}
Severity: {EVENT.SEVERITY}
Original problem ID: {EVENT.ID}
{TRIGGER.URL}

Pause operations for suppressed problems:

Operations	Steps	Details	Start in	Duration	Action
1	Send message to user groups: Zabbix administrators1 via Email	Immediately	Default	Edit Remove	
3	Send message to user groups: Managers via SMS	02:00:00	Default	Edit Remove	
4	Run remote commands on current host	03:00:00	Default	Edit Remove	

Operation details

Steps: 3 - 3 (0 - infinitely)

Step duration: 0 (0 - use action default)

Operation type: Send message

* At least one user or user group must be selected.

Send to User groups	User group	Action
	Managers	Remove
	Add	

Send to Users	User	Action
	Add	

Send only to: SMS

Default message:

Conditions	Label	Name	Action
	A	Event acknowledged equals Not Ack	Remove
	New		

[Update](#) [Cancel](#)

* At least one operation, recovery operation or update operation must exist.

[Add](#) [Cancel](#)

ZABBIX Monitoring Inventory Reports Configuration Administration

Host groups Templates **Hosts** Maintenance Actions Event correlation Discovery Services

Details Host updated

Hosts Group: all Create host Import

Name: amon Monitored by: Any Server Proxy

Templates: type here to search Select

DNS: IP: Port:

Proxy: Select

Tags: And/Or Or

tag Contains Equals value Remove

Add

Apply Reset

Name	Applications	Items	Triggers	Graphs	Discovery	Web	Interface	Proxy	Templates	Status	Availability	Agent encryption	Info	Tags	
AMON	Applications 10	Items 32	Triggers 20	Graphs 17	Discovery 2	Web	172.26.11.20:10050		24x7 ping modificado, PUERTO_LINUX_ELASTICSEARCH, PUERTO_LINUX_KIBANA, Servicio_Elasticsearch, Servicio_Kibana, Servicio_Logstash, Template OS Linux (Template App Zabbix Agent)	Enabled	20x	SUP	JOB	ENI	NONE

0 selected Enable Disable Export Mass update Delete

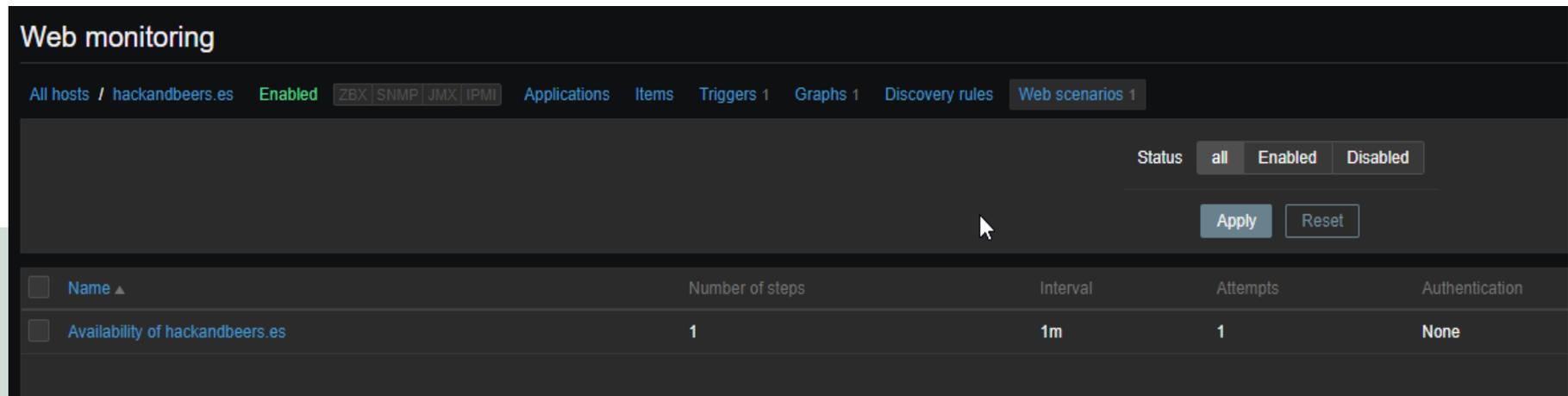
Displaying 1 of 1 found

Zabbix 4.4.4. © 2001–2019, Zabbix SIA

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



The screenshot shows the Nagios XI 'Web monitoring' interface. At the top, there's a breadcrumb trail: 'All hosts / hackandbeers.es' followed by a status indicator 'Enabled' and several monitoring categories: 'ZBX', 'SNMP', 'JMX', 'IPMI', 'Applications', 'Items', 'Triggers 1', 'Graphs 1', 'Discovery rules', and 'Web scenarios 1'. Below this, there are filter buttons for 'Status' with options 'all', 'Enabled', and 'Disabled'. There are also 'Apply' and 'Reset' buttons. The main content is a table with the following columns: 'Name', 'Number of steps', 'Interval', 'Attempts', and 'Authentication'. One row is visible with the following data:

Name	Number of steps	Interval	Attempts	Authentication
Availability of hackandbeers.es	1	1m	1	None

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

Scenario Steps Authentication

* Name Availability of hackandbeers.es

Application No applications found.

New application

* Update interval 1m

* Attempts 1

Agent Zabbix

HTTP proxy [protocol://[user[:password]@]proxy.example.com[:port]]

Variables

Name	Value	
name	value	Remove

Add

Headers

Name	Value	
name	value	Remove

Add

Enabled

Update Clone Clear history and trends Delete Cancel

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, concatenar 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.

Step of web scenario

* Name: home

* URL: http://hackandbeers.es/ Parse

Query fields

Name	Value	
name	value	Remove

Add

Post type: Form data Raw data

Post fields

Name	Value	
name	value	Remove

Add

Variables

Name	Value	
name	value	Remove

Add

Headers

Name	Value	
name	value	Remove

Add

Follow redirects:

Retrieve mode: Body Headers Body and headers

* Timeout: 15s

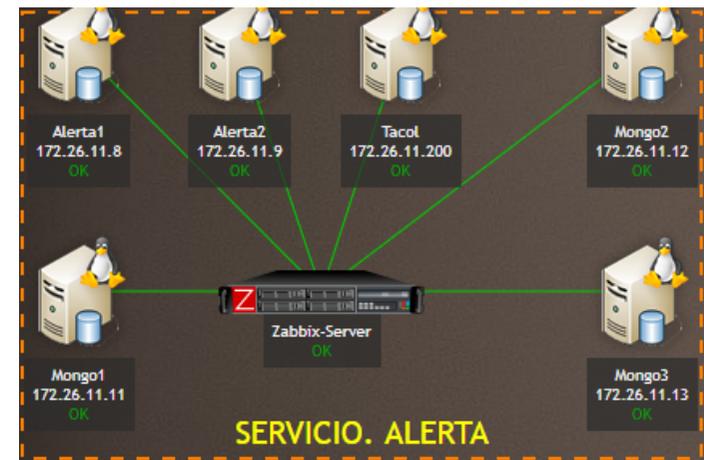
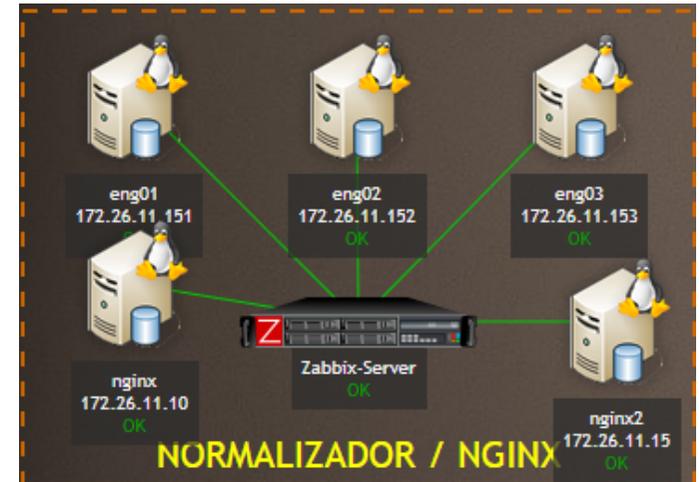
Required string: pattern

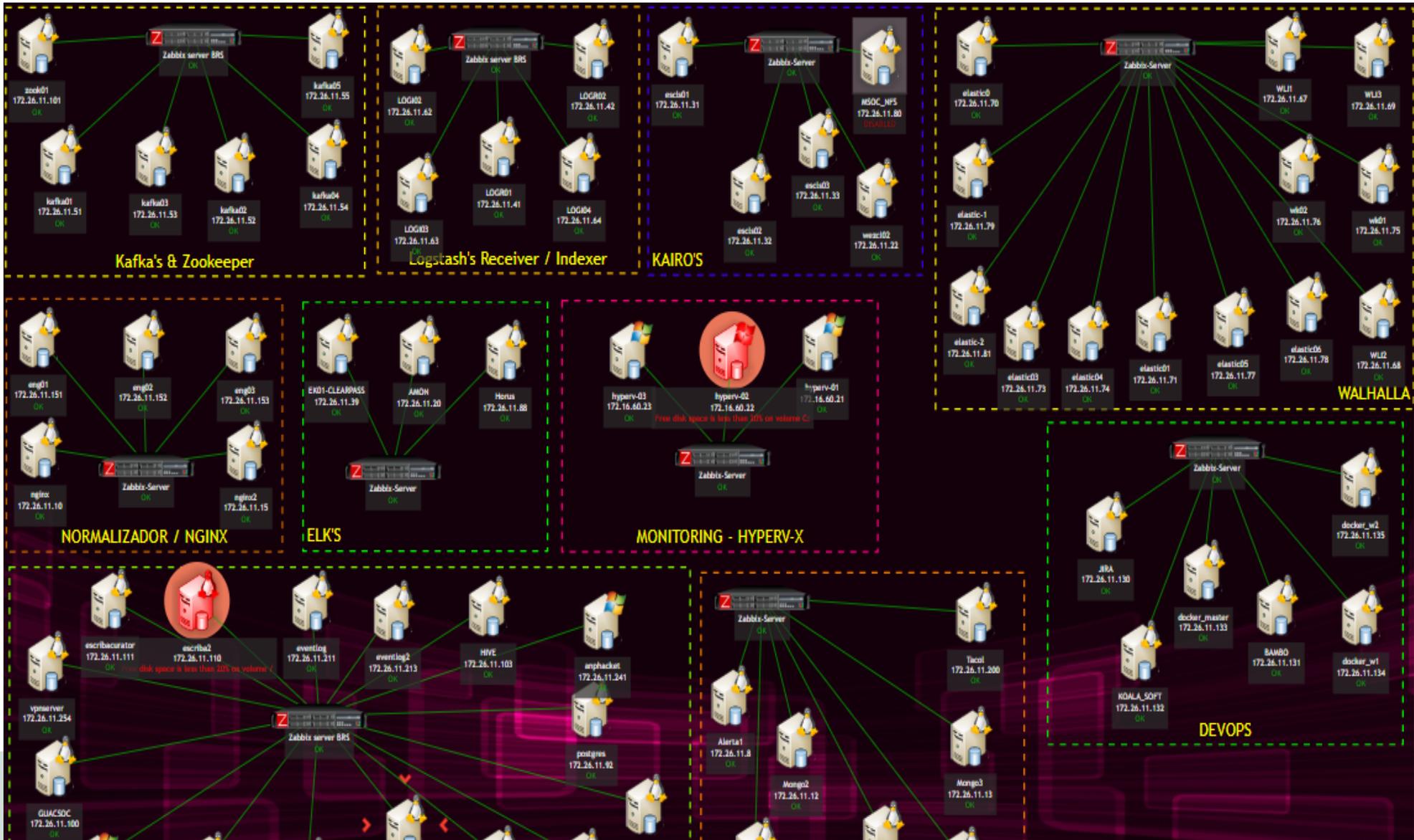
Required status codes: 200

Update Cancel

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

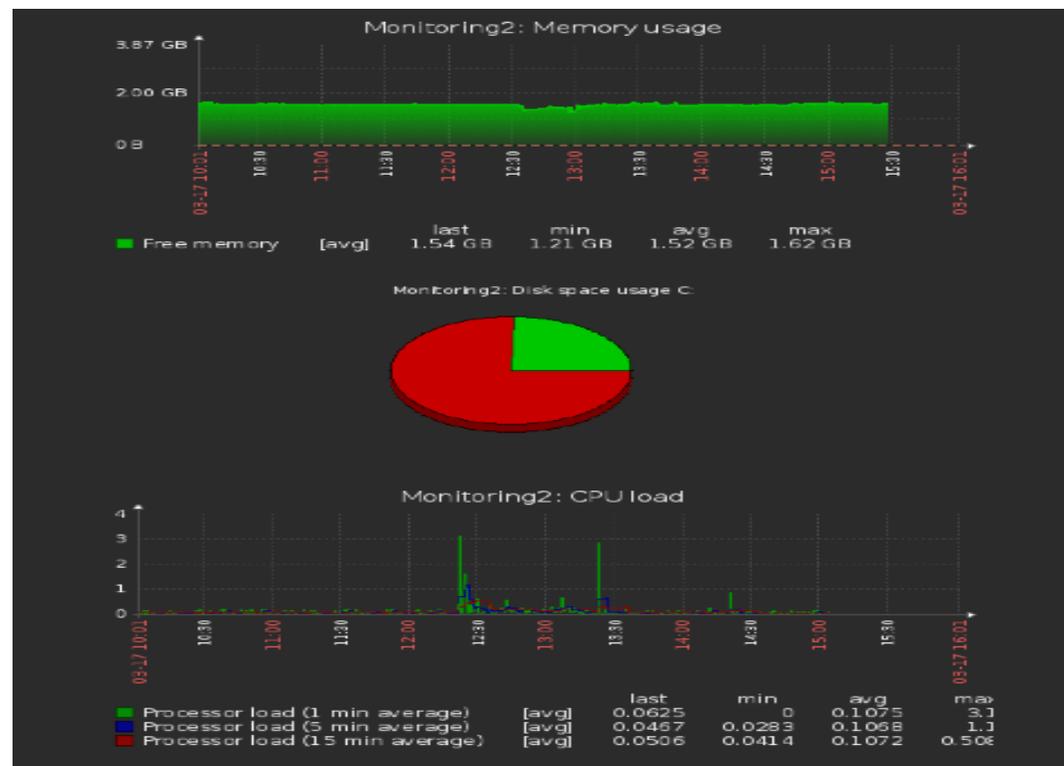




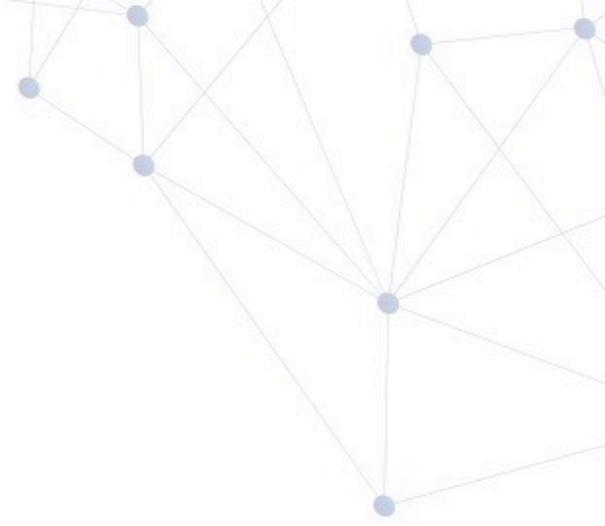
Screens

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



Triggers	anph	BAM	Bridge	brsw	dock	dock	dock	drad	EKO	esds	esds	esds	esdr	esdr	ever
/etc/passwd se ha cambiado en el host {HOST.NAME}, REVISAR															
8x5 - {HOST.NAME} is unavailable by ICMP															
Configured max number of opened files is too low on {HOST.NAME}															
Configured max number of processes is too low on {HOST.NAME}															

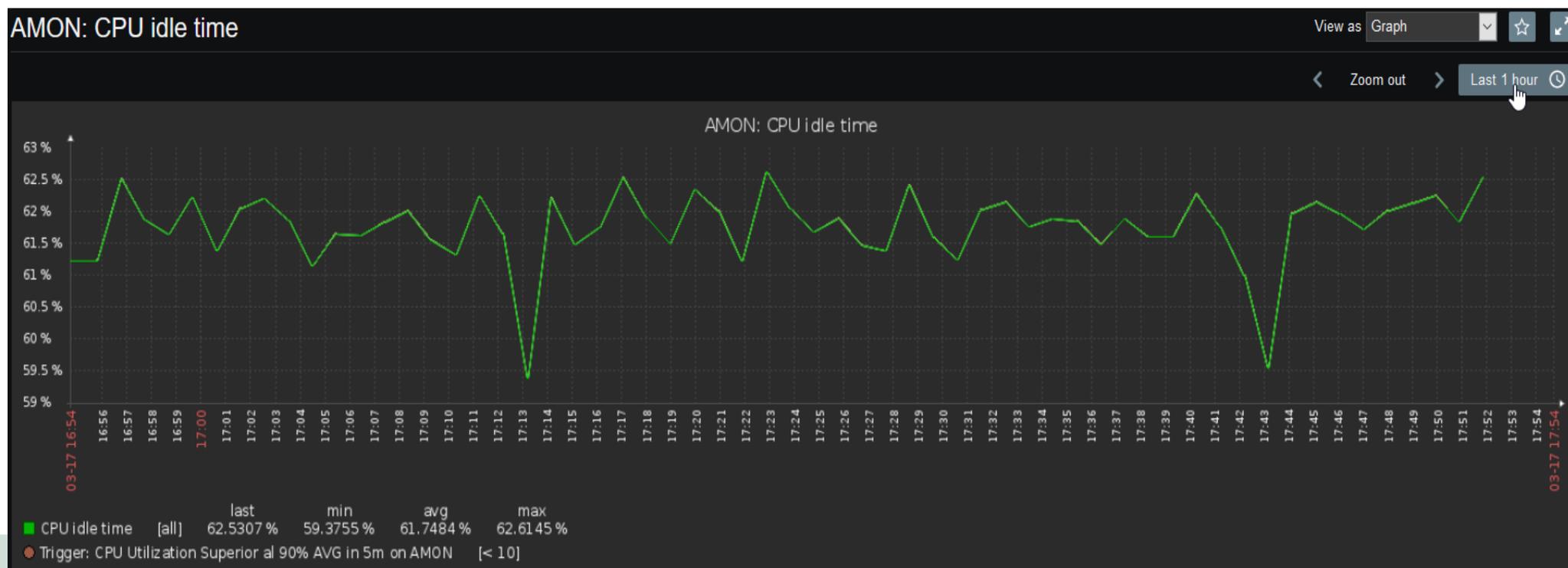


Análisis de la información en BBDD

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 Monitoring Inventory Reports Configuration Administration

Dashboard Problems Overview Web Latest data Graphs Screens Maps Discovery Services

Principal

All dashboards / Principal Edit dashboard 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 / 202 / 94
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

3-16 02:44 3-16 16:57 3-17 05:10

Problems

Time	Recovery time	Status	Info	Host	Problem - Severity	Operational data	Duration	Ack	Actions
17:39:05	17:39:05	RESOLVED		AMON	El aviso que deseamos que salga en la alerta o en nuestra pantalla. MONIT caido.	1	1m	No	1
17:37:05	17:39:05	RESOLVED		AMON	El aviso que deseamos que salga en la alerta o en nuestra pantalla. MONIT caido.	1	2m	No	2
17:32:05	17:33:05	RESOLVED		AMON	El aviso que deseamos que salga en la alerta o en nuestra pantalla. MONIT caido.	1	1m	No	
17:31:05	17:33:05	RESOLVED		AMON	El aviso que deseamos que salga en la alerta o en nuestra pantalla. MONIT caido.	1	2m	No	
17:13:20	17:42:20	RESOLVED		scarlet2	Free disk space is less than 20% on volume /	20.1379 %	29m	No	6
2020-03-05 15:16:53		PROBLEM		escrba2	Free disk space is less than 20% on volume /	3.5807 %	12d 2h 45m	No	4
2019-10-08 14:11:13		PROBLEM		hyperv-02	Free disk space is less than 20% on volume C:	17.5191 %	5m 11d 4h	No	3

sedian Seguridad Digital
de Andalucía