



Sistema de monitorización de la infraestructura CCTV en la UC3M con Zabbix

Jornadas Técnicas RedIRIS, Córdoba 2010



Universidad
Carlos III de Madrid

Emilio González Pérez
Juan Manuel Canelada Oset

Área de Seguridad y Comunicaciones





- 1. Introducción CCTV**
- 2. Infraestructura y funcionamiento CCTV UC3M**
- 3. ¿Por qué un sistema de monitorización?**
- 4. ¿Por qué Zabbix?**
- 5. Arquitectura plataforma monitorización Zabbix**
- 6. Monitorización en Zabbix**
- 7. Interfaz del sistema de monitorización Zabbix**
- 8. Conclusiones**
- 9. Líneas futuras**



cctv

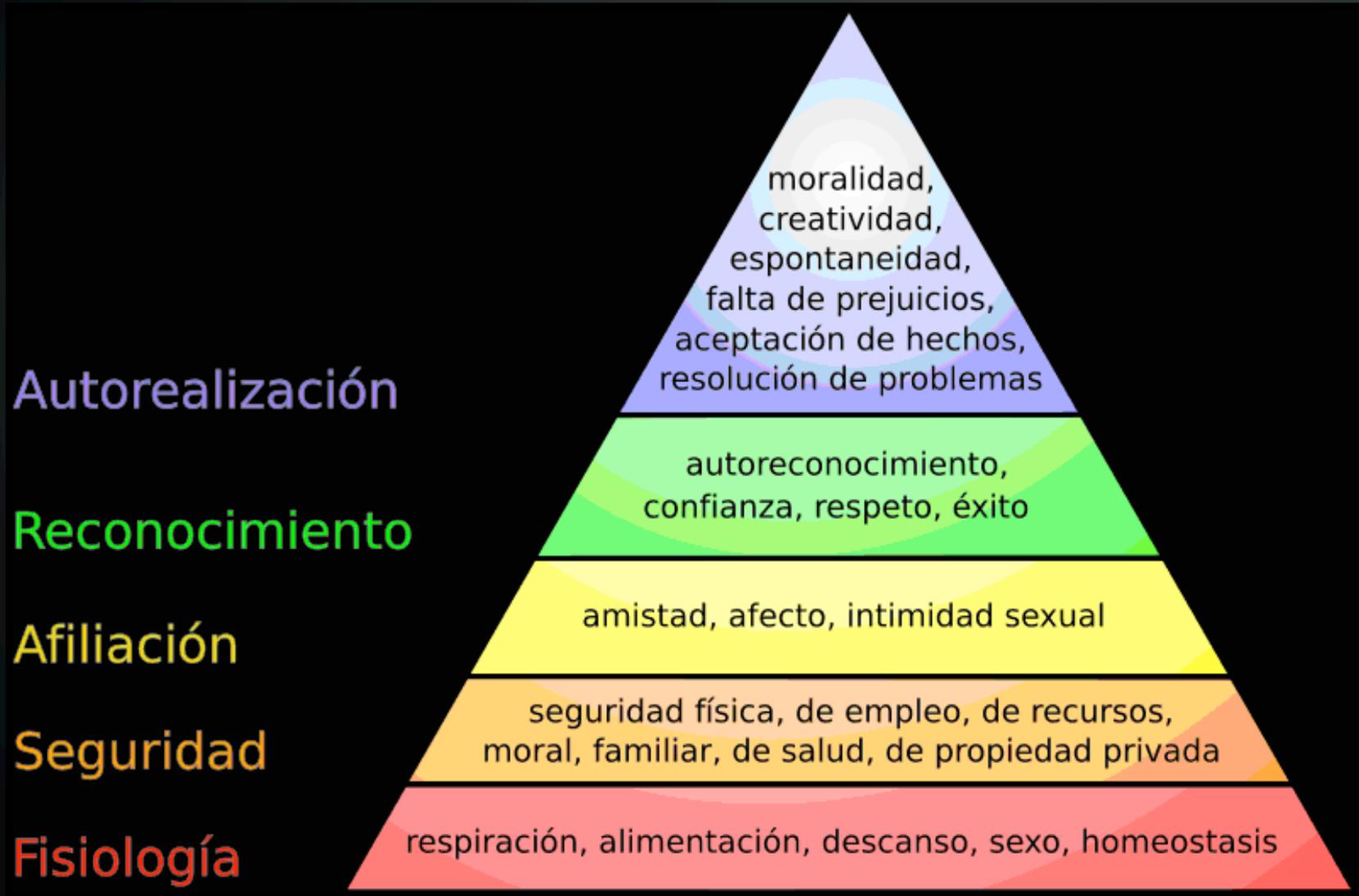
Circuito
cerrado
de
televisión



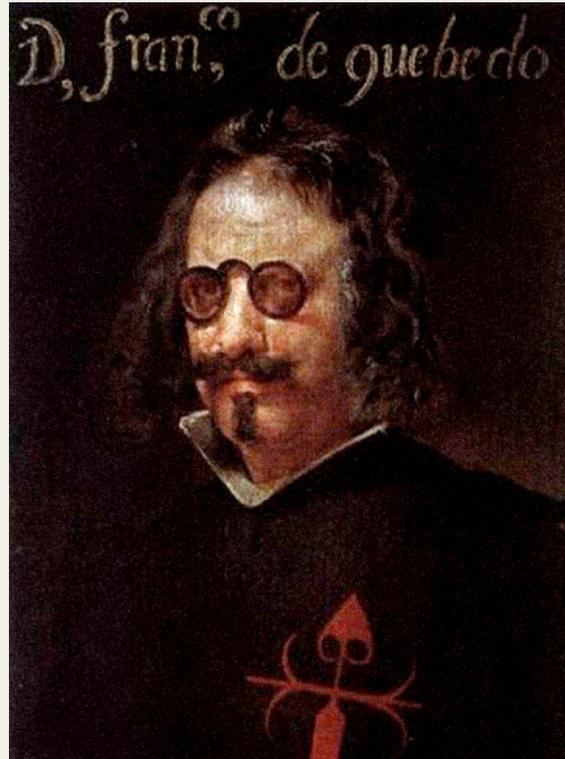
¿Por qué un sistema CCTV?

Seguridad

Pirámide de Maslow



No vive...



...el que no vive seguro.

Quevedo (1580-1645).

¿Dónde?



¿Dónde NO?

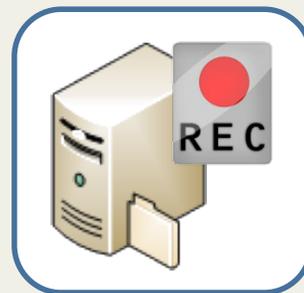
¿Por qué en la UC3M?



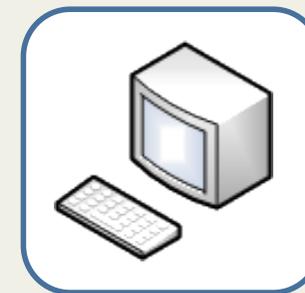
Entorno Abierto → Incidentes



Tres categorías de elementos



**Videograbador
(servidor)**



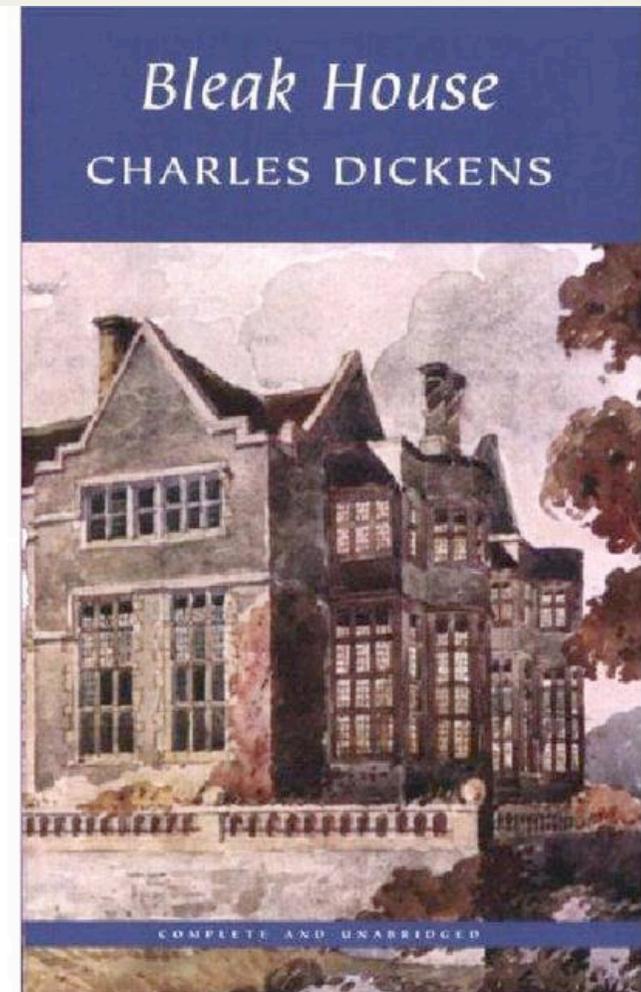
**Equipo de
monitorización
(cliente)**

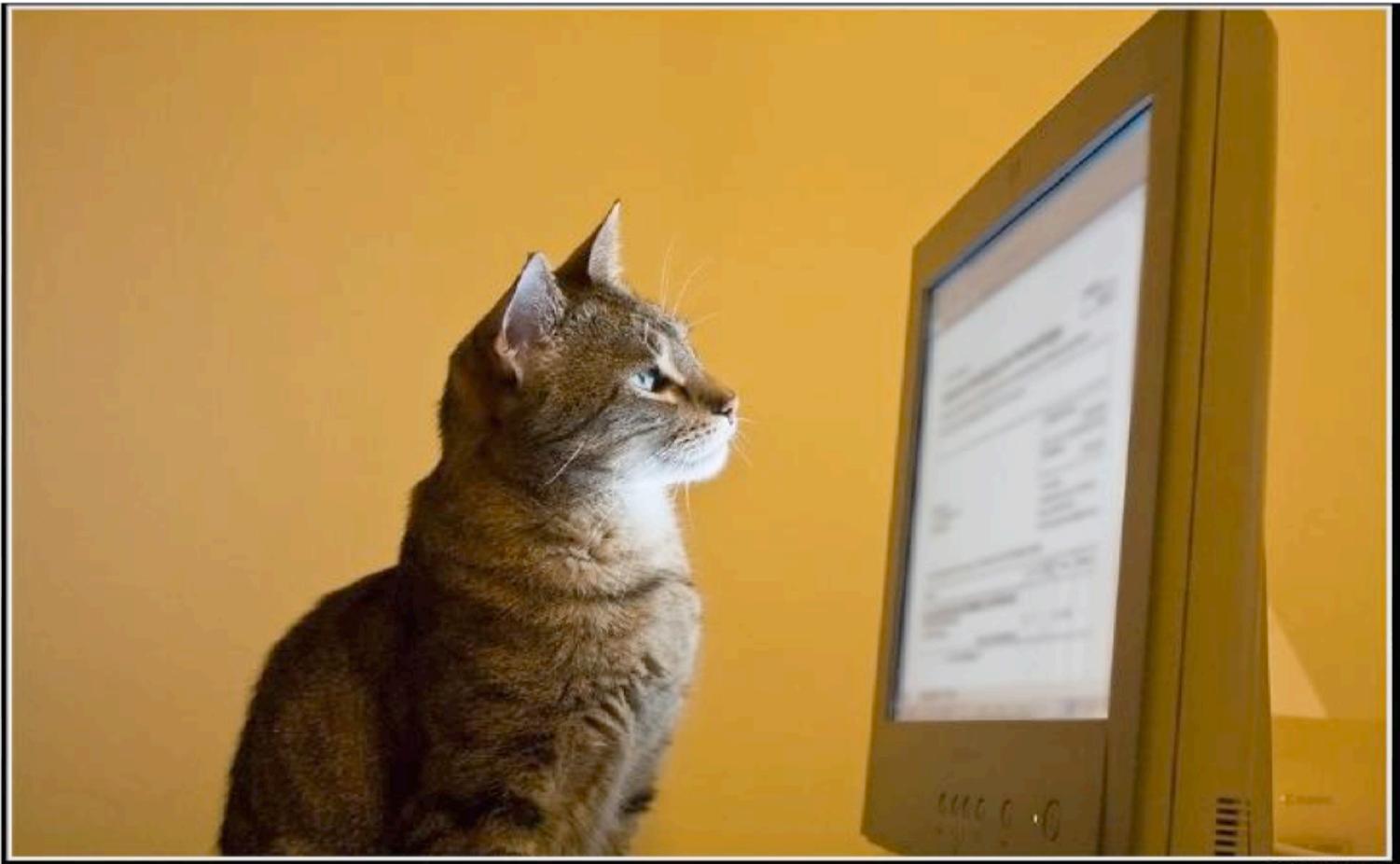


Algunos Datos

- Inversión Importante
- Aproximadamente 250 cámaras
- 12 Servidores de Grabación
- Entorno Windows
- 8 Discos por servidor con elevada carga de entrada/salida
- Múltiples fallos en los discos
- Mala gestión del espacio de almacenamiento (sistema de archivos llenos)
- Desaparición de la UTE de instalación
- Ausencia de Soporte
- Incidentes de Seguridad

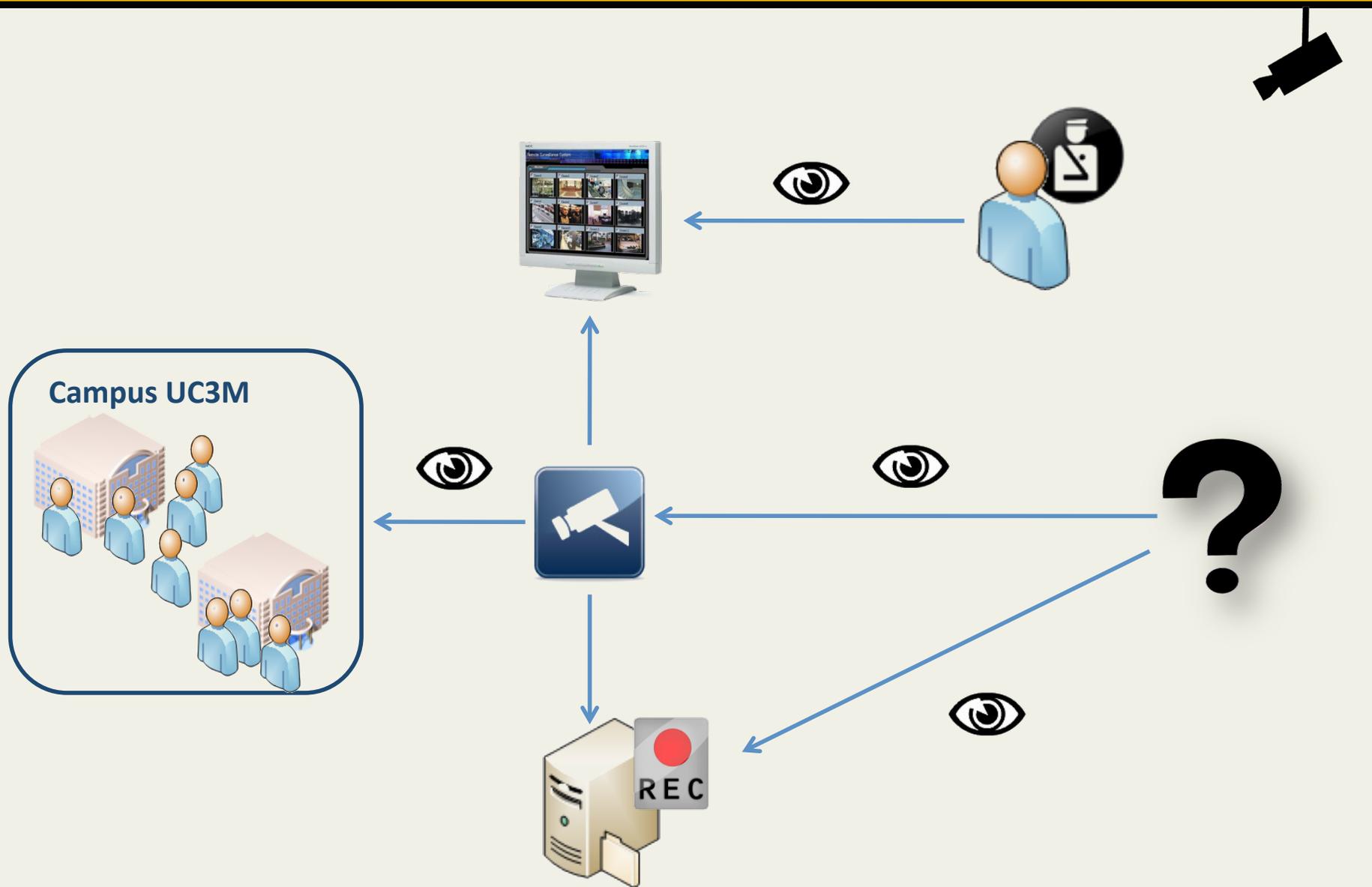
¿Cómo monitorizamos y gestionamos esto?





Sistema de monitorización

¿Por qué un sistema de monitorización?





Estudio de herramientas disponibles

ZABBIX

Nagios

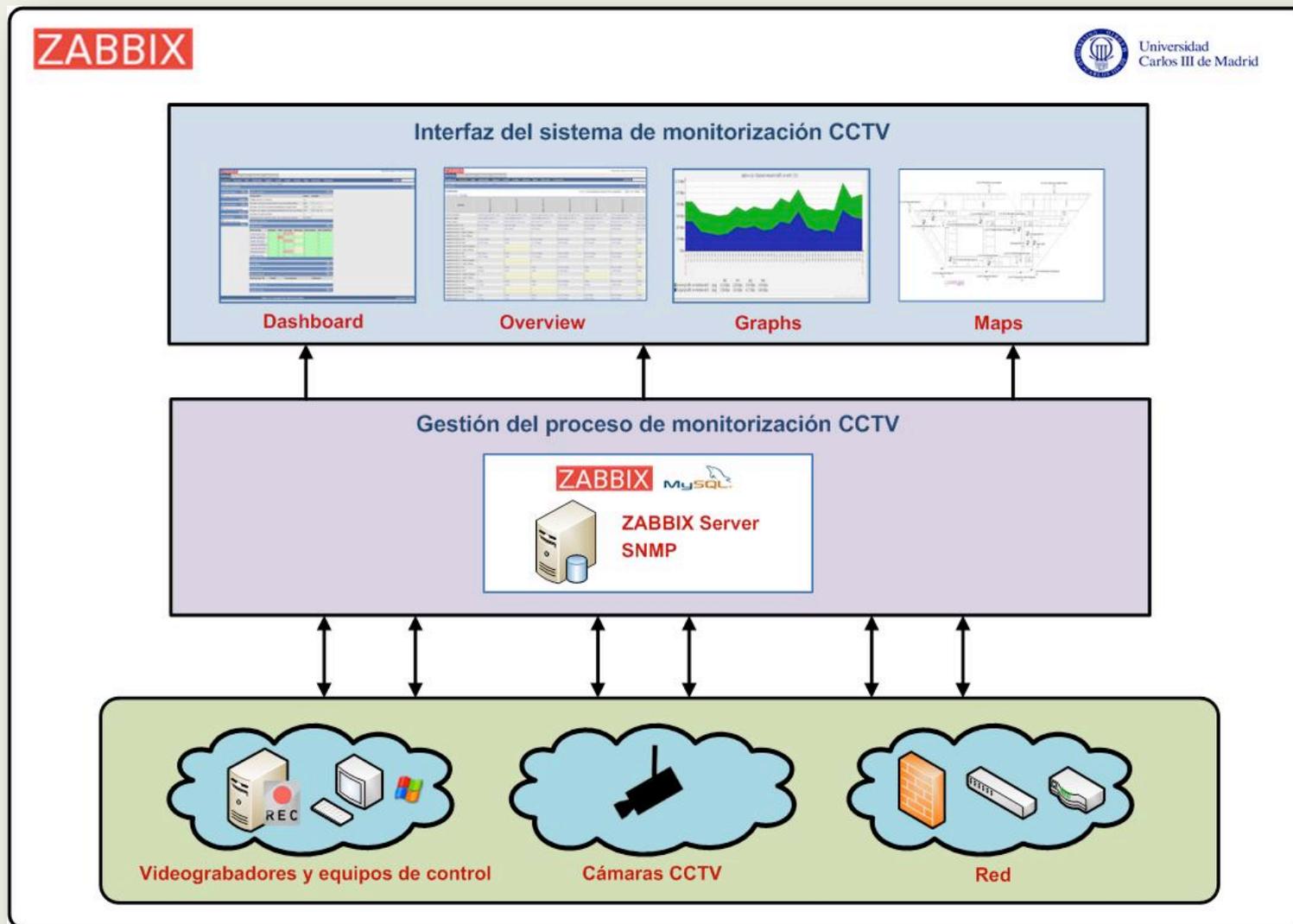




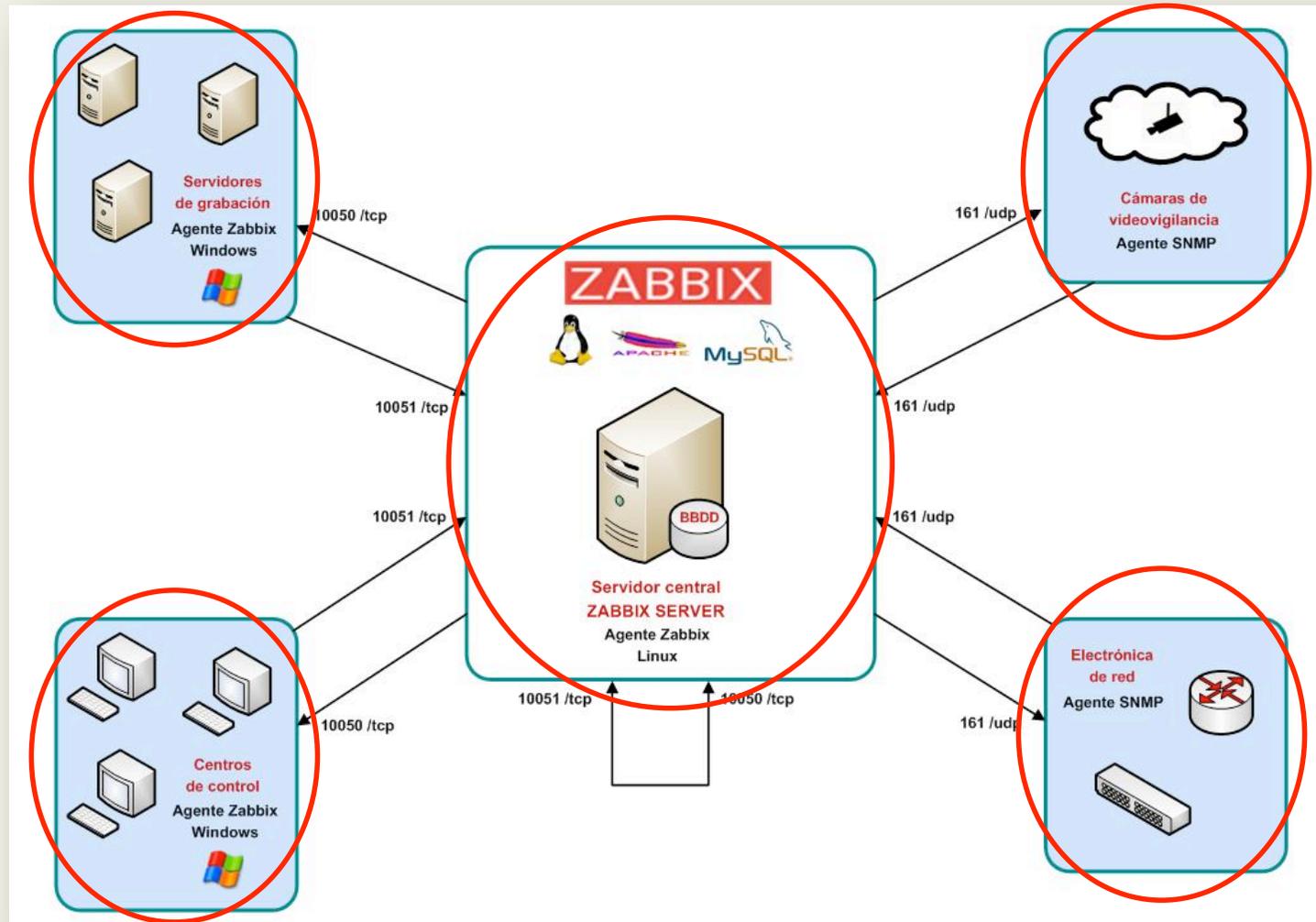
- **OpenSource**
- **Mejor solución para monitorización de sistemas Windows**
- **Configuración de la herramienta y la práctica totalidad de parámetros de monitorización desde la interfaz Web**
- **Creación automática y personalizada de gráficos para presentación y estudio de los datos de monitorización**
- **Historial de datos y estadísticas**
- **Evolución constante**
- **Agentes nativos para multitud de plataformas**
- **Flexibilidad en la configuración de parámetros de monitorización**
- **Gestión de usuarios**
- **Reglas de descubrimiento de equipos en la red**



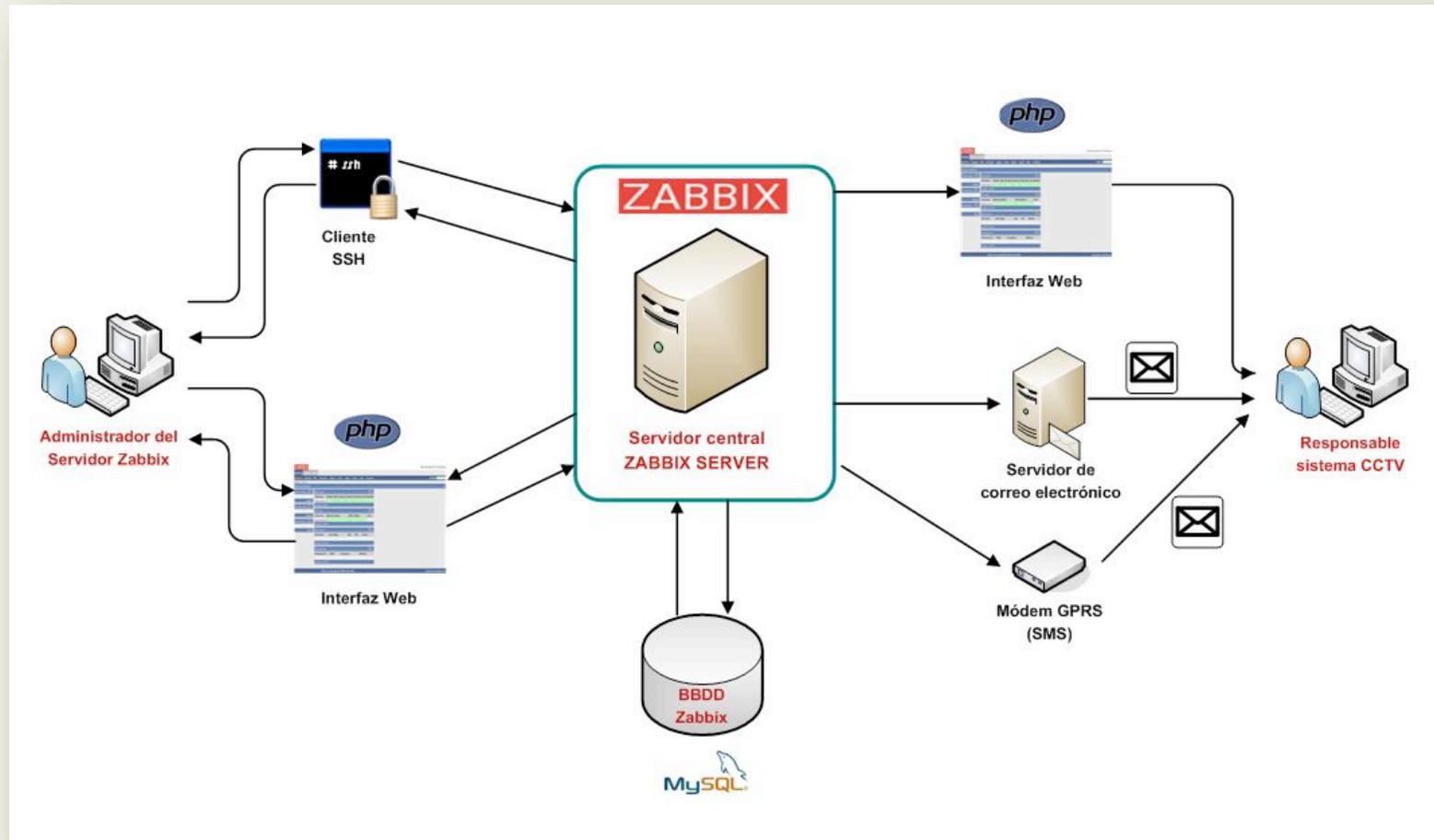
Arquitectura del sistema de monitorización

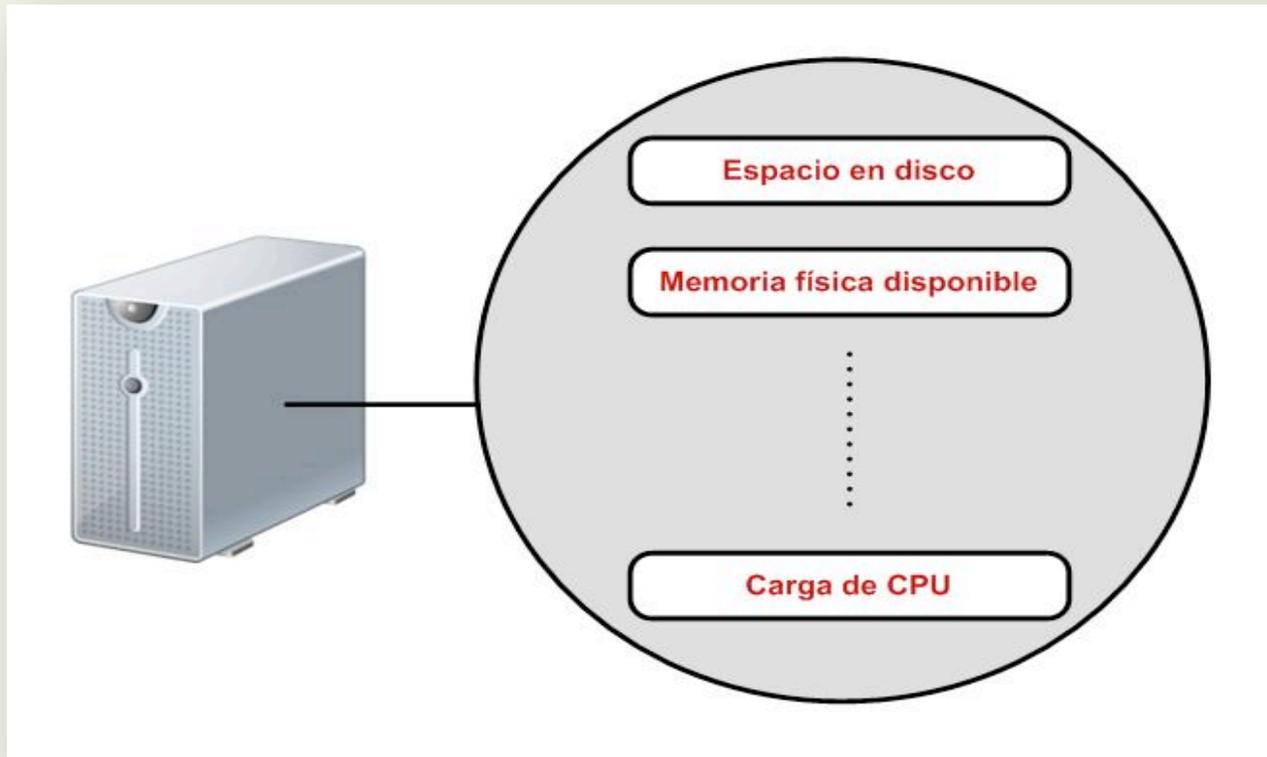


Comunicación entre los componentes de la arquitectura



Canales de comunicación

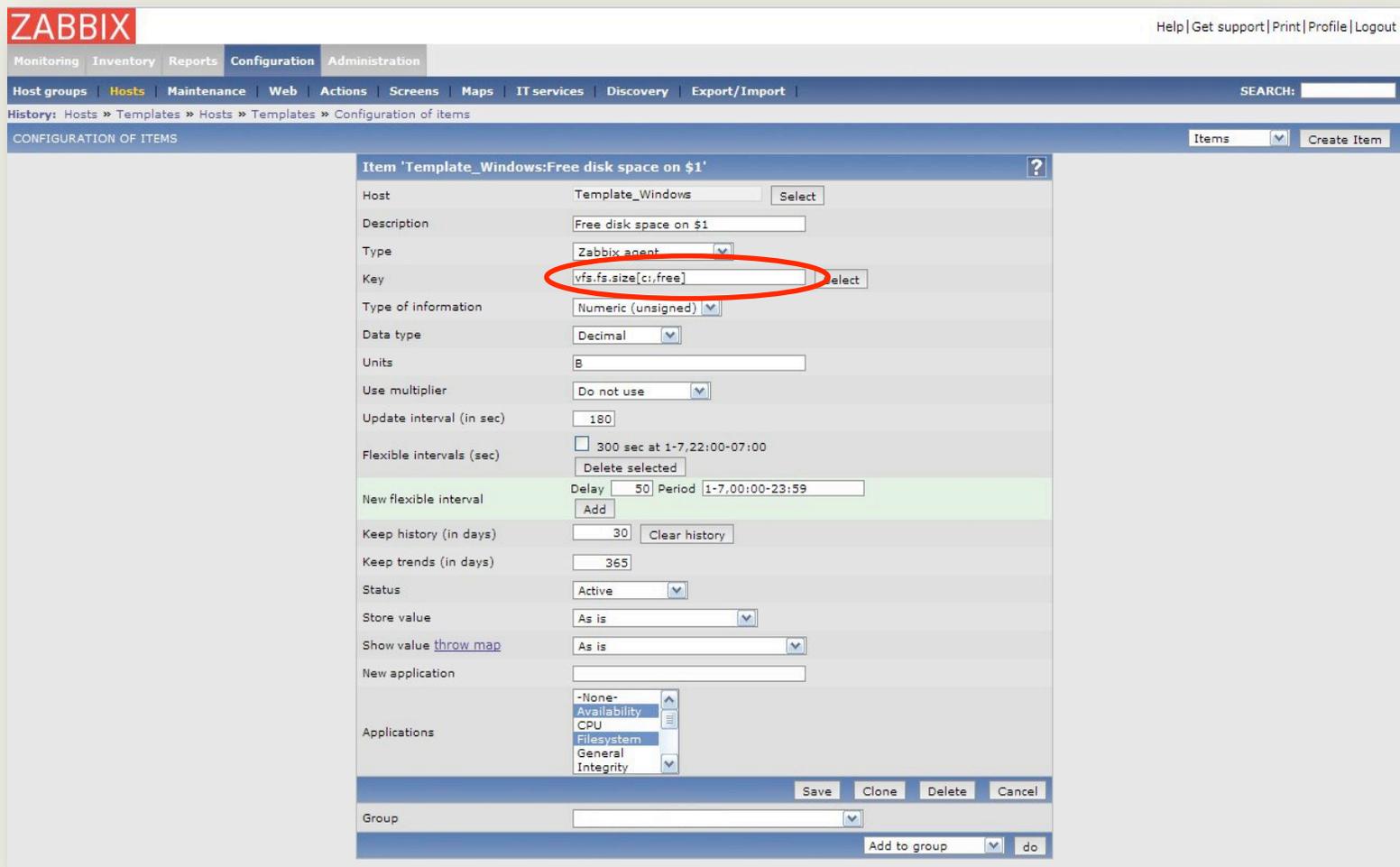




ZABBIX

Host + Items

Estructura de un item Zabbix



The screenshot displays the Zabbix web interface for configuring an item. The breadcrumb trail is: History: Hosts » Templates » Hosts » Templates » Configuration of items. The page title is 'CONFIGURATION OF ITEMS'. The item being configured is 'Template_Windows:Free disk space on \$1'. The 'Key' field is highlighted with a red circle and contains the value 'vfs.fs.size[ci,free]'. Other fields include 'Host' (Template_Windows), 'Description' (Free disk space on \$1), 'Type' (Zabbix agent), 'Type of information' (Numeric (unsigned)), 'Data type' (Decimal), 'Units' (B), 'Use multiplier' (Do not use), 'Update interval (in sec)' (180), 'Flexible intervals (sec)' (300 sec at 1-7,22:00-07:00), 'New flexible interval' (Delay 50, Period 1-7,00:00-23:59), 'Keep history (in days)' (30), 'Keep trends (in days)' (365), 'Status' (Active), 'Store value' (As is), 'Show value throw map' (As is), 'New application' (empty), and 'Applications' (Filesystem). Buttons for 'Save', 'Clone', 'Delete', and 'Cancel' are visible at the bottom.

Item	Template_Windows:Free disk space on \$1
Host	Template_Windows
Description	Free disk space on \$1
Type	Zabbix agent
Key	vfs.fs.size[ci,free]
Type of information	Numeric (unsigned)
Data type	Decimal
Units	B
Use multiplier	Do not use
Update interval (in sec)	180
Flexible intervals (sec)	300 sec at 1-7,22:00-07:00
New flexible interval	Delay 50 Period 1-7,00:00-23:59
Keep history (in days)	30
Keep trends (in days)	365
Status	Active
Store value	As is
Show value throw map	As is
New application	
Applications	Filesystem

Clave (key)



Servidores Windows (videograbadores y equipos de control)

- Información del host
- Espacio de almacenamiento
- Estado de los discos
- Memoria disponible
- Rendimiento CPU
- Procesos en ejecución
- Servicios y aplicaciones
- Tráfico de red
- Temperatura
- Eventos del sistema operativo

Cámaras de CCTV

- Información general
- Tráfico de red

Equipos de red

- Información general
- Tráfico en sus interfaces de red



Ejemplo 1. Monitorización del espacio en disco disponible en un videograbador

1. Instalación del agente Zabbix (plataforma Windows) en el videograbador.
2. Registrar el videograbador como un nuevo *host*.
3. Creación de un *template* (plantilla) que agrupará conjuntos de *items*.
4. Construir el *item* correspondiente al espacio en disco dentro de la plantilla anterior.
5. Modificar el host creado para asignarle la plantilla con el item construido.

Creación del item correspondiente



Item 'Template_Windows:Free disk space on \$1 (in %)'

Host	Template_Windows	Select
Description	Free disk space on \$1 (in %)	
Type	Zabbix agent	
Key	vfs.fs.size[c:,pfree]	
Type of information	Numeric (float)	
Units		
Use multiplier	Do not use	
Update interval (in sec)	180	
Flexible intervals (sec)	<input type="checkbox"/> 300 sec at 1-7,22:00-07:00	
	Delete selected	
New flexible interval	Delay 50 Period 1-7,00:00-23:59	
	Add	
Keep history (in days)	30 Clear history	
Keep trends (in days)	365	
Status	Active	
Store value	As is	
New application		
Applications	-None- Availability CPU Filesystem General Integrity	
Save Clone Delete Cancel		
Group	Centro Control [Getafe]	
	Add to group do	



Ejemplo 2. Monitorización del tráfico de red de entrada en una cámara de videovigilancia

1. Activación del agente SNMP de la cámara según las instrucciones del fabricante (ejecución de un script).
2. Registrar la cámara como un nuevo *host*.
3. Creación de un *template* (plantilla) que agrupará conjuntos de *items*.
4. Construir el *item* correspondiente al tráfico de entrada dentro de la plantilla anterior.
5. Modificar el host creado para asignarle la plantilla con el item construido.



Creación del item correspondiente

Item 'Template_Cameras:Incoming traffic'

Host	Template_Cameras	Select
Description	Incoming traffic	
Type	SNMPv2 agent	
SNMP OID	.1.3.6.1.2.1.2.2.1.10.2	
SNMP community	public	
SNMP port	161	
Key	ifInOctets.2	Select
Type of information	Numeric (float)	
Units	bps	
Use multiplier	Custom multiplier	
Custom multiplier	8	
Update interval (in sec)	120	
Flexible intervals (sec)	<input type="checkbox"/> 300 sec at 1-7,22:00-07:00 Delete selected	
New flexible interval	Delay 50 Period 1-7,00:00-23:59 Add	
Keep history (in days)	30	Clear history
Keep trends (in days)	365	
Status	Active	
Store value	Delta (speed per second)	
New application		
Applications	-None- General	

Save Clone Delete Cancel

Group: Centro Control [Getafe] Add to group do



Ejemplo 3. Control del valor del espacio en disco disponible mediante la creación de un disparador

1. Seleccionar la plantilla o *host* al cual se asignará el disparador.
2. En la sintaxis del disparador, seleccionaremos el item y la función que se encargará de controlar el valor de dicho item.

Creación del disparador correspondiente



Trigger "Disk space below 5% on {HOSTNAME}"

Name: Disk space below 5% on {HOSTNAME}

Expression (Toggle input method): `{Template_Windows:vfs.fs.size[c:,pfree].last(0)}<5`

The trigger depends on: No dependencies defined

New dependency:

Event generation: Normal

Severity: High

Comments:

URL:

Disabled:

Dashboard



ZABBIX Help | Get support | Print | Profile | Logout

Monitoring | Inventory | Reports | Configuration | Administration

Dashboard | Overview | Web | Latest data | Triggers | Events | Graphs | Screens | Maps | Discovery | IT services |

History: Configuration of items » Configuration of triggers » QUEUE » Overview » Network maps

PERSONAL DASHBOARD 🔍 ↻

Favourite Graphs 🔍 ↻

- [zabbix-cctv:CPU Loads](#)
- [SERVER-G01:Free disk space on c: \(in %\)](#)
- [SERVER-G03:Free disk space on c: \(in %\)](#)

Graphs »

Favourite Screens 🔍 ↻

- [Slide show overview](#)

Screens »

Favourite Maps 🔍 ↻

- [Status of Servers](#)

Maps »

Status of Zabbix 🔍 ↻

Parameter	Value	Details
Zabbix server is running	Yes	-
Number of hosts (monitored/not monitored/templates)	416	360 / 1 / 55
Number of items (monitored/disabled/not supported)	9976	8976 / 923 / 77
Number of triggers (enabled/disabled)[true/unknown/false]	2055	1905 / 150 [426 / 95 / 1384]
Number of users (online)	3	1
Required server performance, new values per second	44.0995	-

Updated: 09:24:52

System status 🔍 ↻

Host group	Disaster	High	Average	Warning	Information	Not classified
Centro Control [Getafe]	0	2	0	0	0	0
Centro Control [Leganés]	0	0	0	1	0	0
Conmutador B01014CCTV-SERV [Leganés]	0	0	0	38	0	0
Conmutadores centrales campus	0	0	0	0	0	0
Conmutadores centrales campus CCTV	0	0	0	0	0	0
Conmutadores planta CCTV [Getafe 8Bis]	0	0	0	43	0	0
Conmutadores planta CCTV [Getafe]	0	0	0	208	0	0
Conmutadores planta CCTV [Leganés]	0	0	0	130	0	0
Discovered Hosts	0	0	1	2	2	0
Getafe CAMERAS	0	0	0	0	0	0
Getafe SERVERS	0	0	0	0	1	0
Leganés CAMERAS	0	0	0	0	0	0
Leganés SERVERS	0	0	1	1	1	0
MySQL servers	0	0	0	0	0	0
Windows servers	0	0	1	1	2	0
Zabbix Servers	0	0	0	0	0	0

Updated: 09:24:51

Host status 🔍 ↻

Host group	Without problems	With problems	Total
Centro Control [Getafe]	0	2	2
Centro Control [Leganés]	1	1	2

Overview



ZABBIX Help | Get support | Print | Profile | Logout

Monitoring | Inventory | Reports | Configuration | Administration

Dashboard | Overview | Web | Latest data | Triggers | Events | Graphs | Screens | Maps | Discovery | IT services SEARCH:

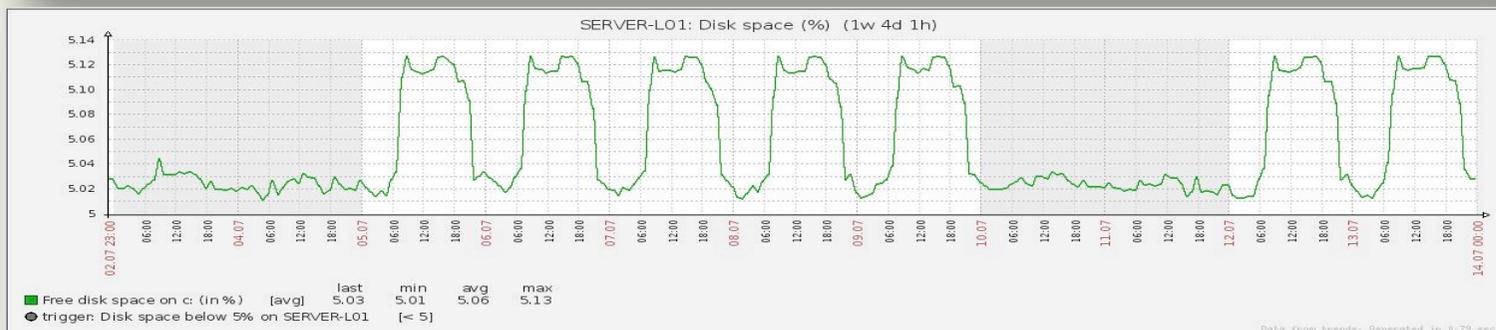
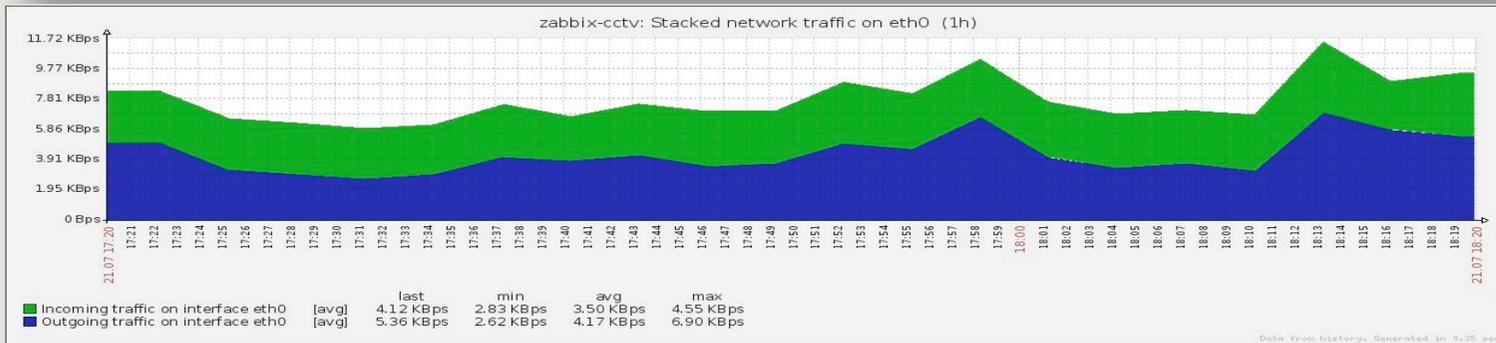
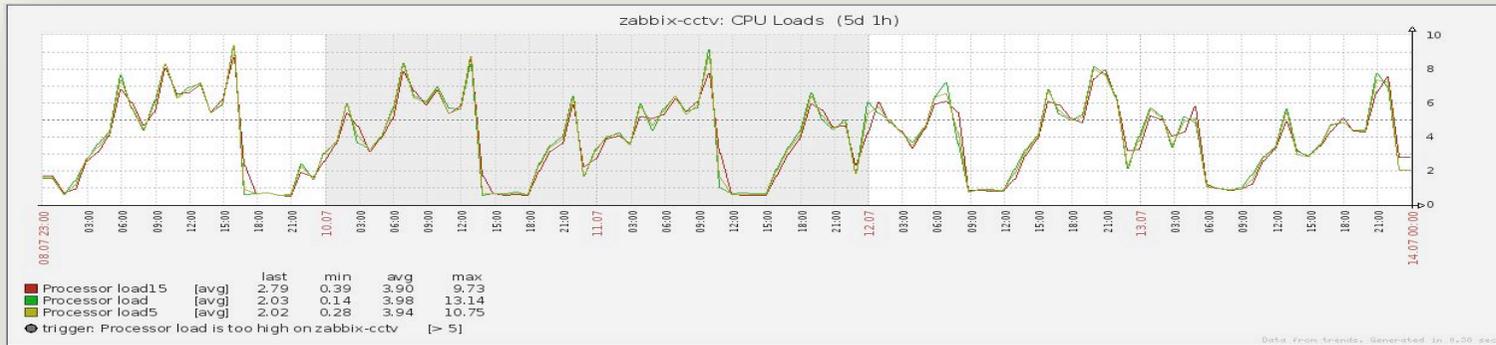
History: Templates » Configuration of items » Configuration of triggers » QUEUE » Overview

OVERVIEW Group Leganés SERVERS Type Data

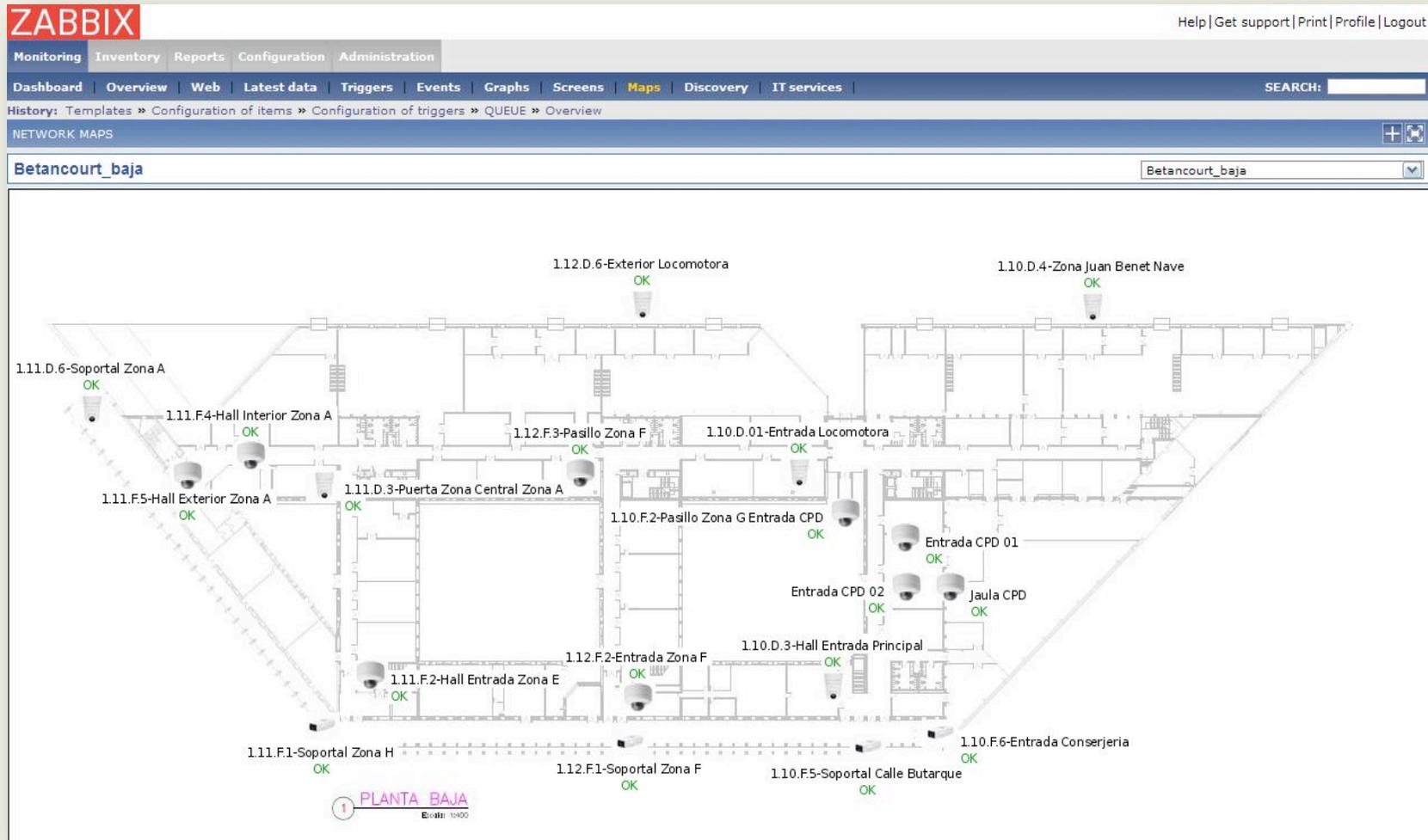
Hosts location

Items	SERVER-L01	SERVER-L02	SERVER-L03	SERVER-L04	SERVER-L05	SERVER-L06
Active TCP connections	528589	1137363	486281	5813006	265734	534267
Application Log	El parámetro TraceLe ...	Server started and a ...	El parámetro TraceLe ...	SNMP Event Log Exten ...	Server started and a ...	wuauclt (2028) Se de ...
Checksum of c:\autoexec.bat	4294967295	4294967295	4294967295	4294967295	4294967295	4294967295
Checksum of c:\config.sys	4294967295	4294967295	4294967295	4294967295	4294967295	4294967295
CPU idle time (in %)	61.07	84.38	72.66	60.94	64.84	51.56
CPU Temperature	43 °C	41 °C	42 °C	38 °C	39 °C	34 °C
CPU usage (in %)	41.23	15.97	34.07	28.72	35.65	46.08
DHCP client service state (Dhcp)	Stopped (6)					
Drive #0 model	"ST3250318AS"	"ST3250310NS"	"ST3250310NS"	"ST3500410AS"	"ST3250310AS"	"ST3500410AS"
Drive #0 power (in days)	335	957	972	302	629	468
Drive #0 status	OK (255)					
Drive #0 Temperature	38 °C	35 °C	35 °C	25 °C	34 °C	30 °C
Drive #1 model	"ST3250310NS"	"ST3250310NS"	"ST3250310NS"	"ST3500410AS"	"ST3250310AS"	"ST3500410AS"
Drive #1 power (in days)	796	575	972	257	621	239
Drive #1 status	OK (255)					
Drive #1 Temperature	38 °C	35 °C	34 °C	24 °C	35 °C	30 °C
Drive #2 model	"ST3250310NS"	"ST3250310NS"	"ST3250310NS"	"ST3500410AS"	"ST3250310NS"	"ST3500410AS"
Drive #2 power (in days)	970	967	972	257	830	468
Drive #2 status	OK (255)					
Drive #2 Temperature	37 °C	36 °C	35 °C	23 °C	33 °C	29 °C
Drive #3 model	"ST3250310NS"	"ST3250310NS"	"ST3250310NS"	"ST3500410AS"	"ST3250310NS"	"ST3500418AS"
Drive #3 power (in days)	970	738	972	257	959	169
Drive #3 status	OK (255)					
Drive #3 Temperature	37 °C	35 °C	35 °C	23 °C	33 °C	29 °C
Drive #4 model	"ST3250310NS"	"ST3250310NS"	"ST3250310NS"	"ST3500410AS"	"ST3250310NS"	"ST3500410AS"
Drive #4 power (in days)	970	867	972	257	911	238
Drive #4 status	OK (255)					

Graphs



Maps





- Mayor control del estado del sistema CCTV
- Menor intervención humana
- Reducción de los tiempos de respuesta frente a fallos
- Monitorización de alrededor de 9000 parámetros repartidos entre 294 equipos
- En torno a 1500 disparadores controlando los valores de monitorización
- Detección de problemas y patrones de comportamiento a partir de los datos históricos





- Integración del sistema de control de accesos 
- Envío de alertas vía SMS
- Creación de un cuadro de mando
- Interpretación mensajes de error controladora RAID 
- Monitorización servidor MySQL
- Replicación base de datos de monitorización
- Creación de una guía de usuario
- Autenticación de usuarios a través de LDAP



