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

UC3M cei
CAMPUS DE EXCELENCIA INTERNACIONAL

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

Universidad Carlos III de Madrid

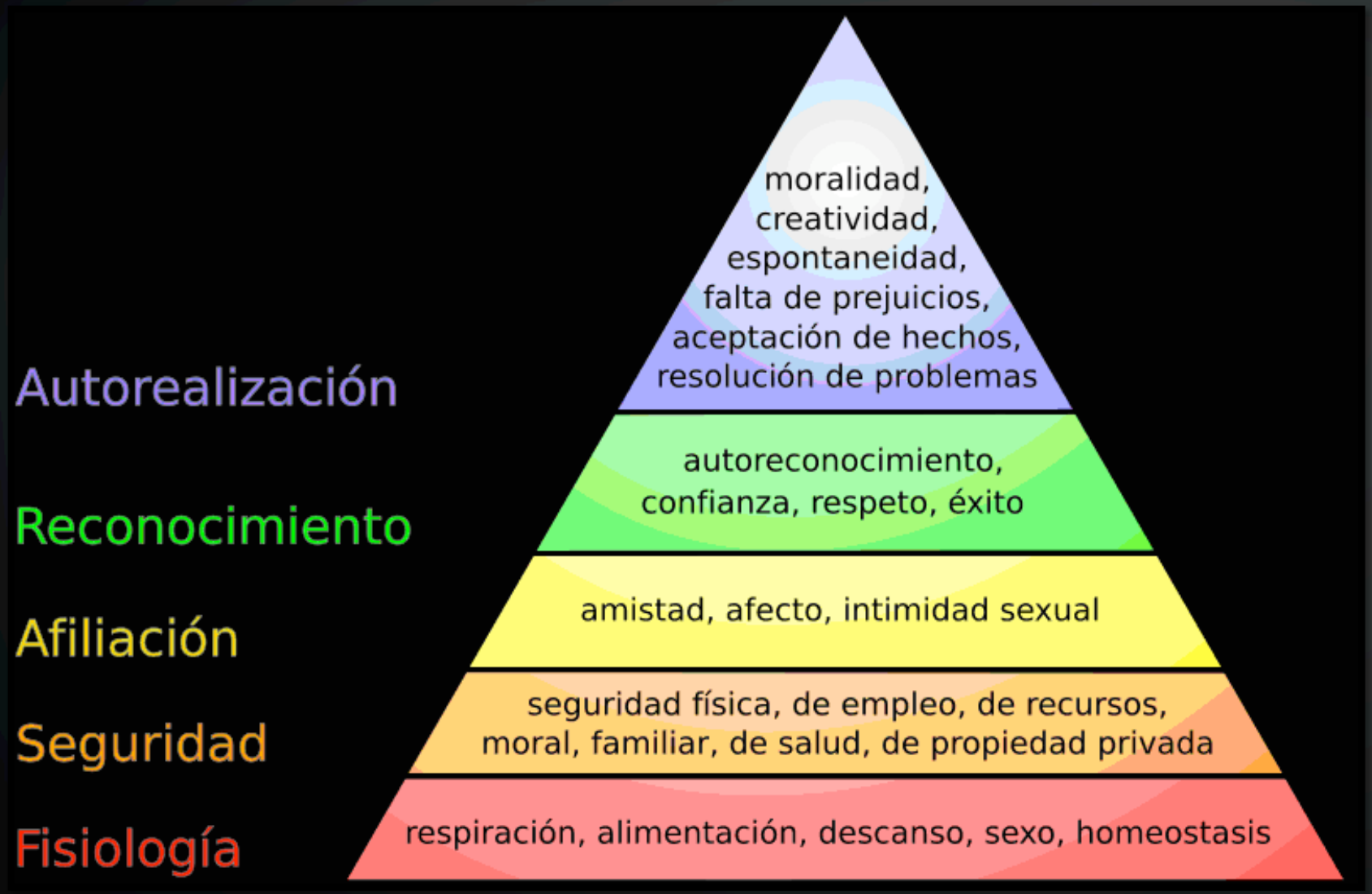
cctv

Circuito cerrado de televisión

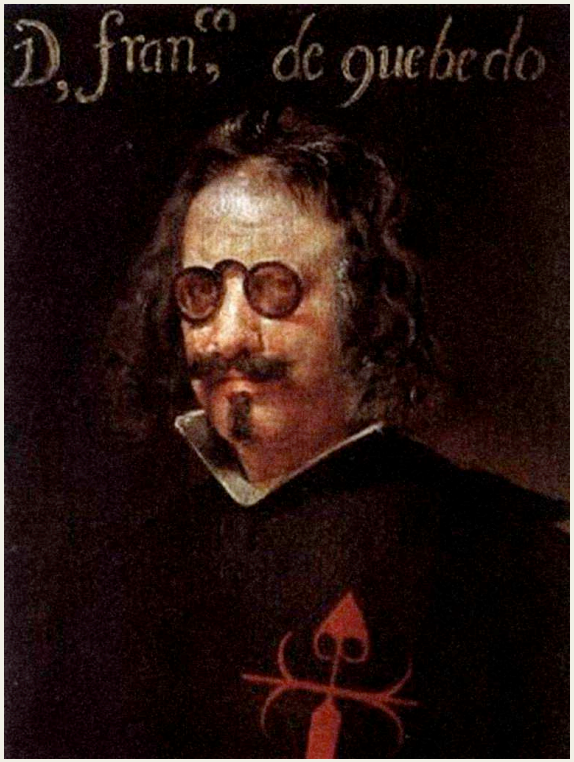
¿Por qué un sistema CCTV?

Seguridad

Pirámide de Maslow



No vive…



…el que no vive seguro.

Quevedo (1580-1645).

¿Dónde?

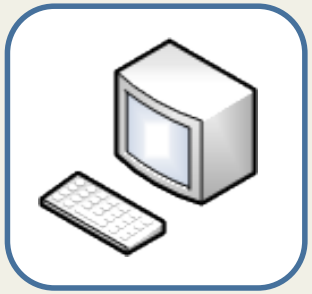
¿Dónde NO?

¿Por qué en la UC3M?

Entorno Abierto → Incidentes

Tres categorías de elementos

Videograbador (servidor)



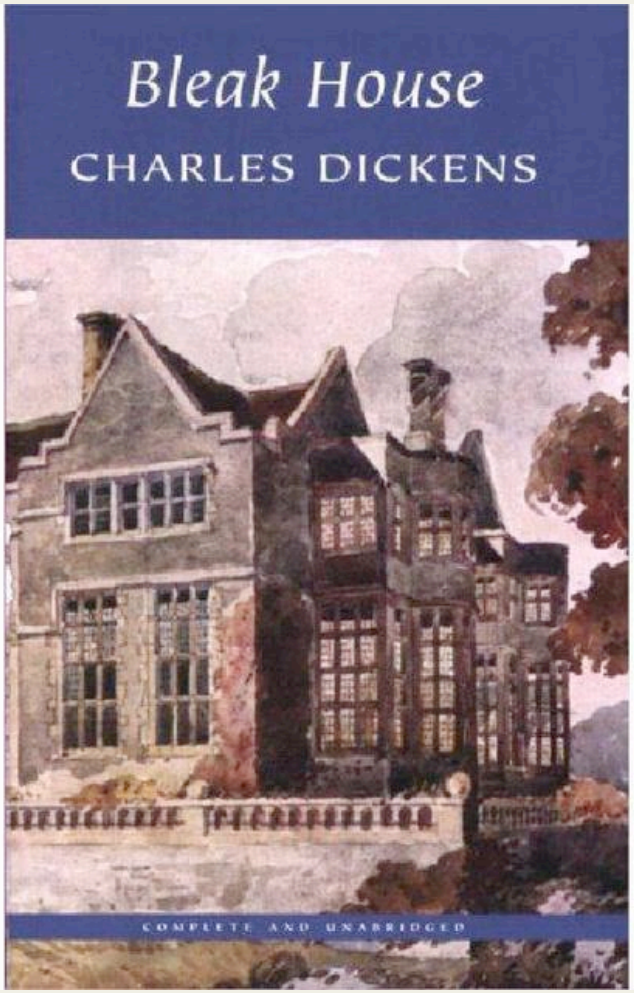
Equipo de monitorización (cliente)

Universidad Carlos III de Madrid

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

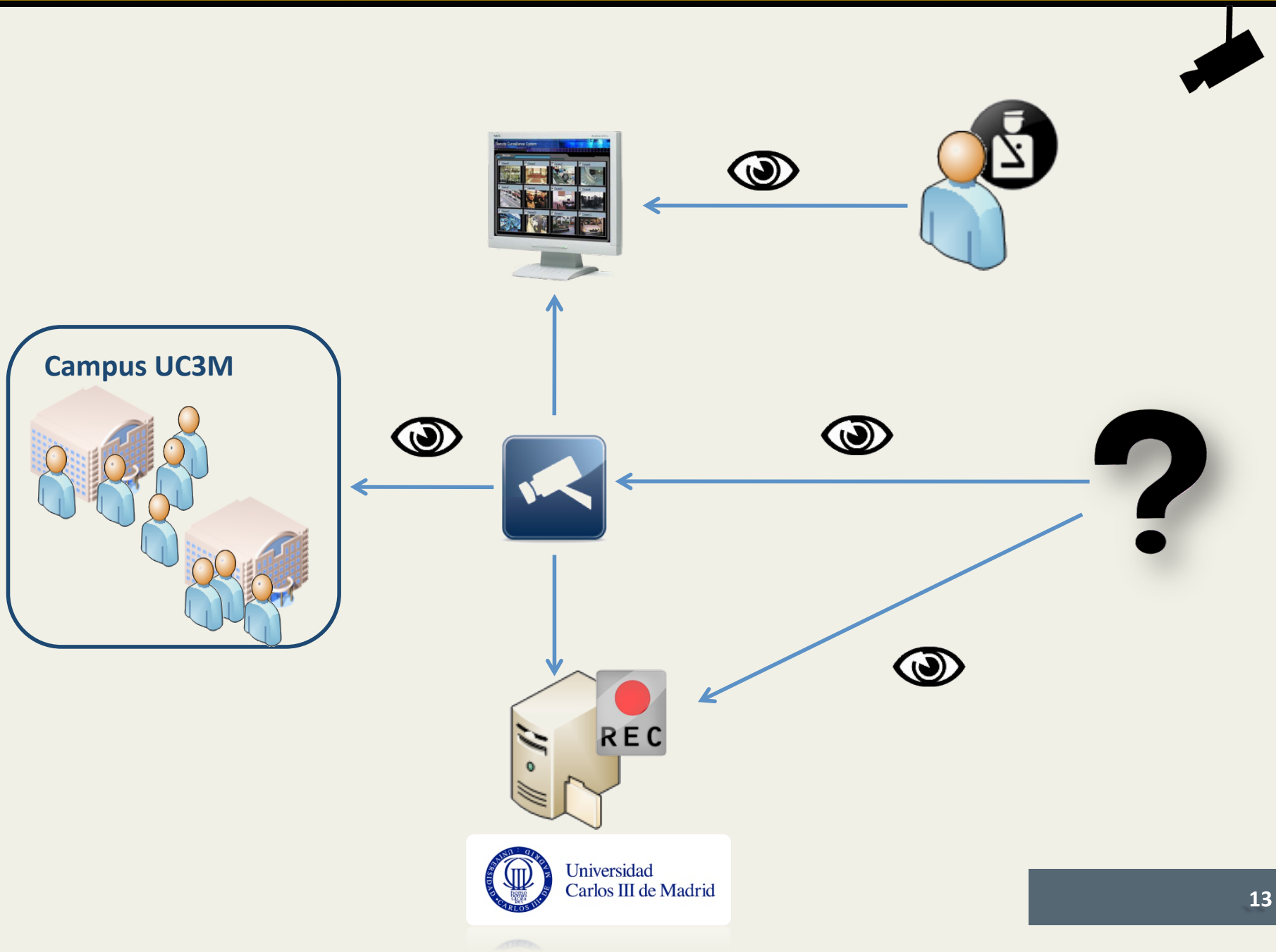
¿Cómo monitorizamos y gestionamos esto?



Universidad Carlos III de Madrid

Sistema de monitorización

¿Por qué un sistema de monitorización?



Universidad Carlos III de Madrid

Estudio de herramientas disponibles

ZABBIX

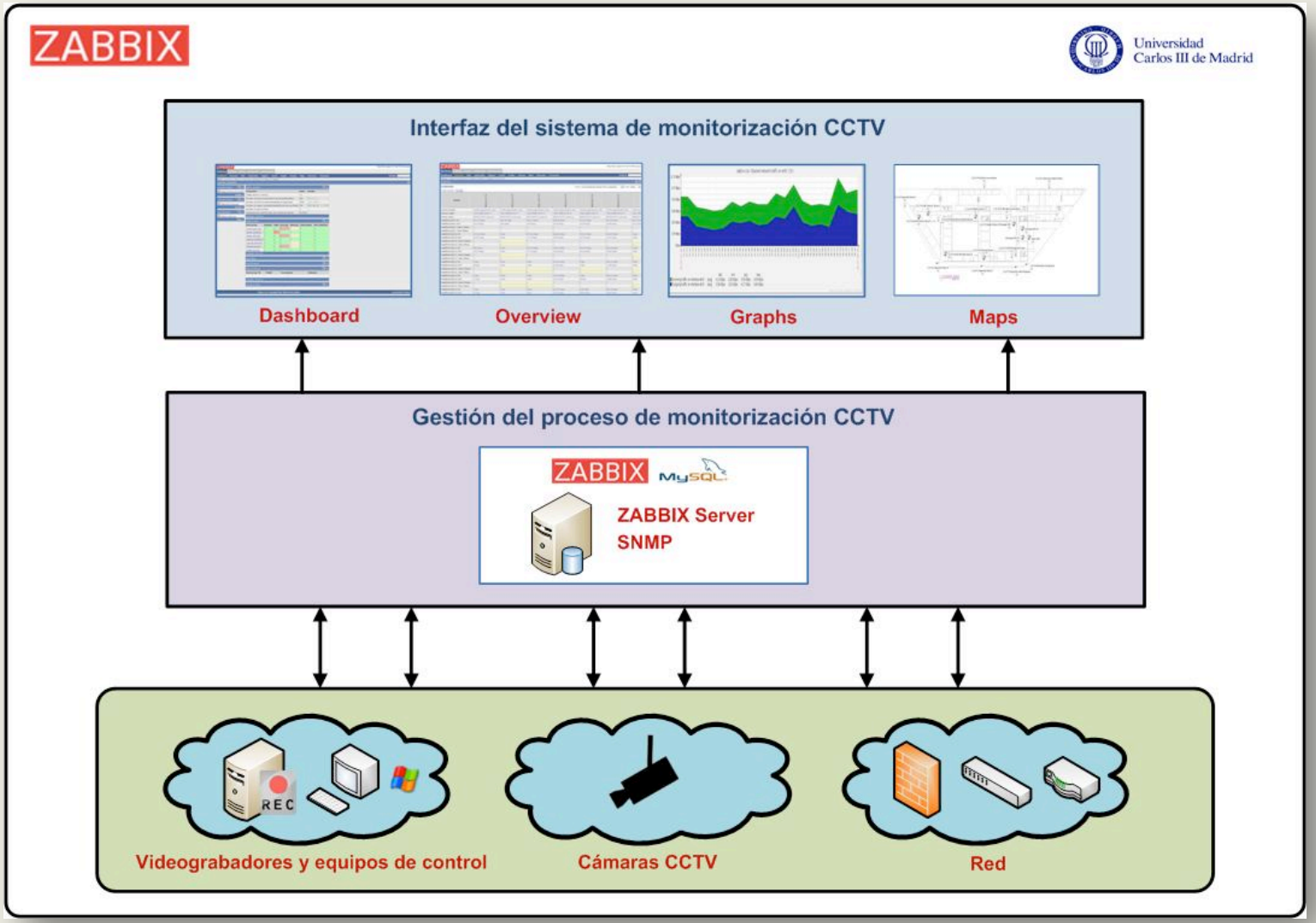
Nagios

Pandora FMS

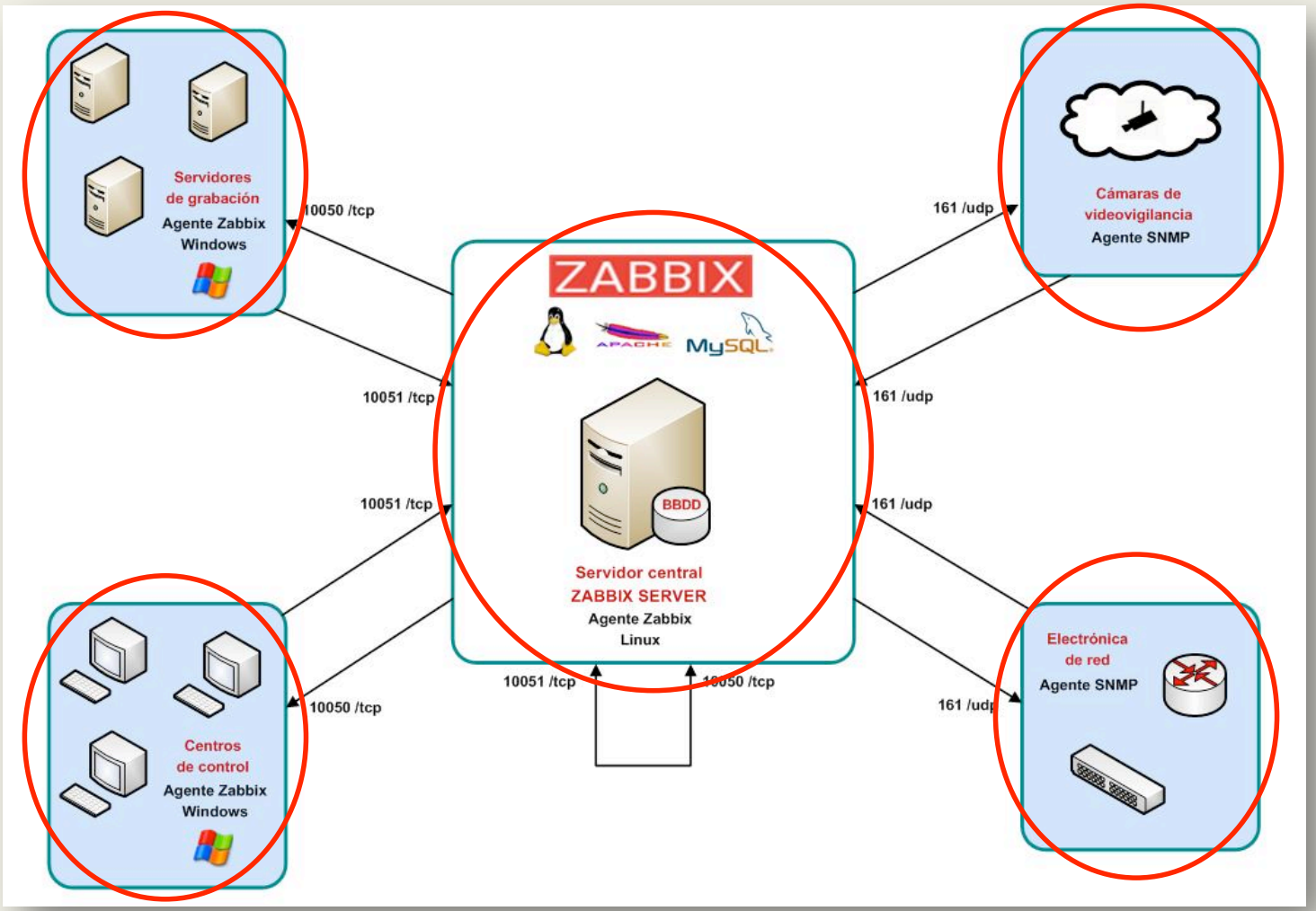
¿Por qué Zabbix?

- 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

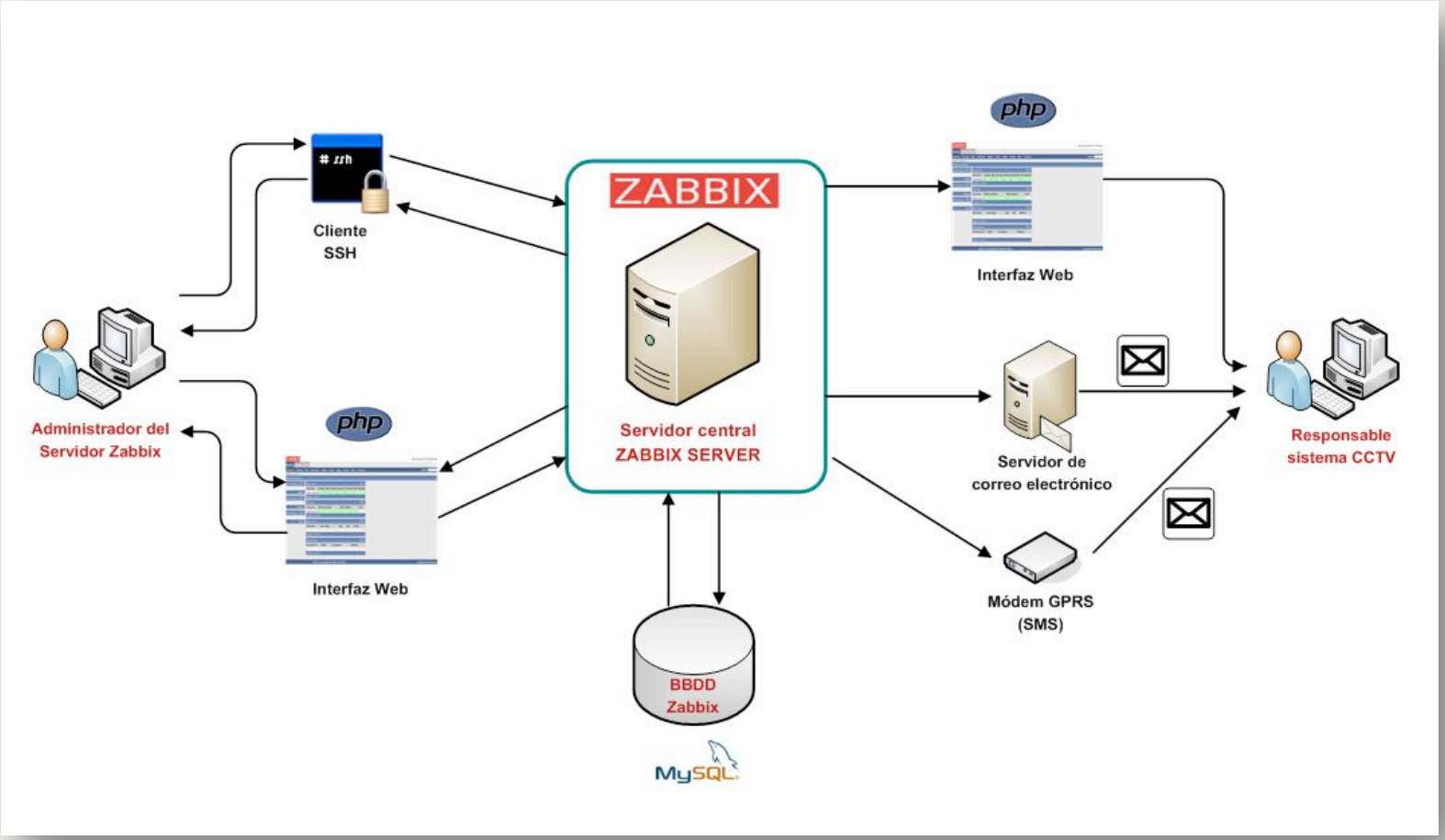
Arquitectura del sistema de monitorización

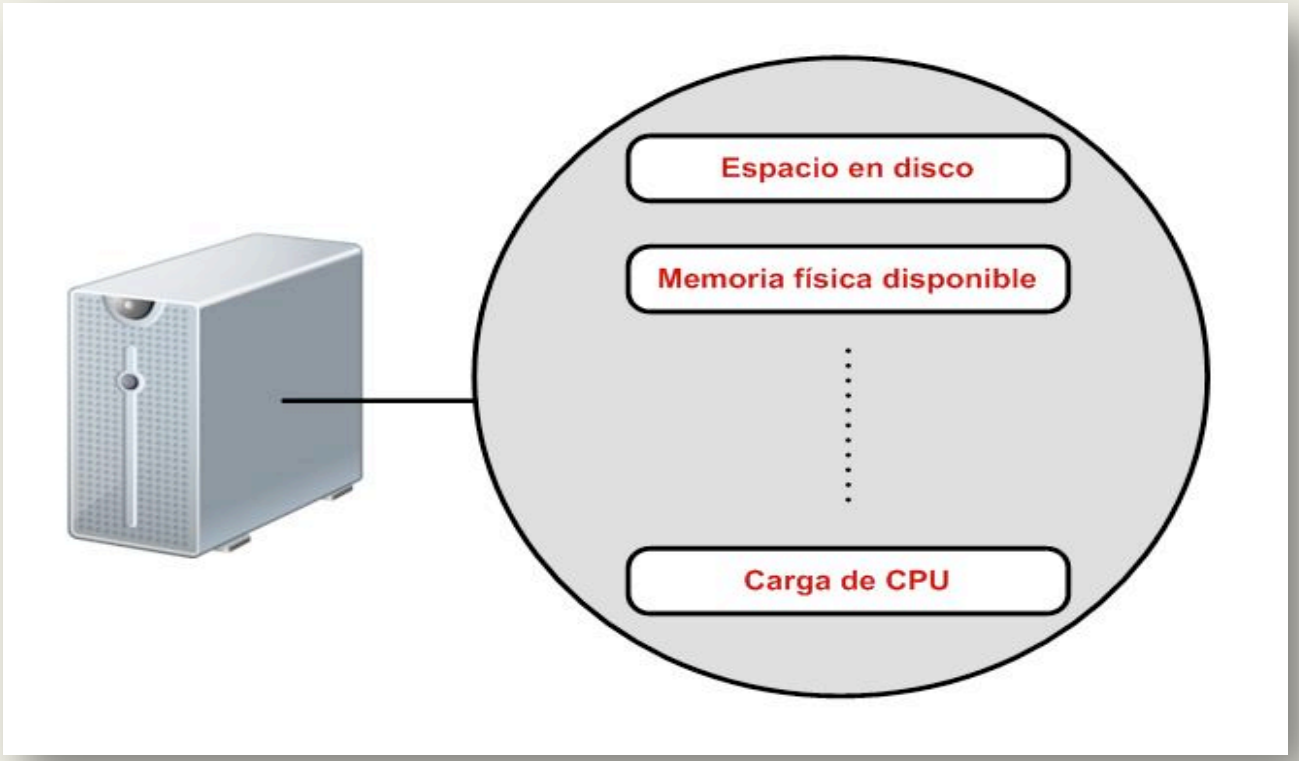


Comunicación entre los componentes de la arquitectura



Canales de comunicación

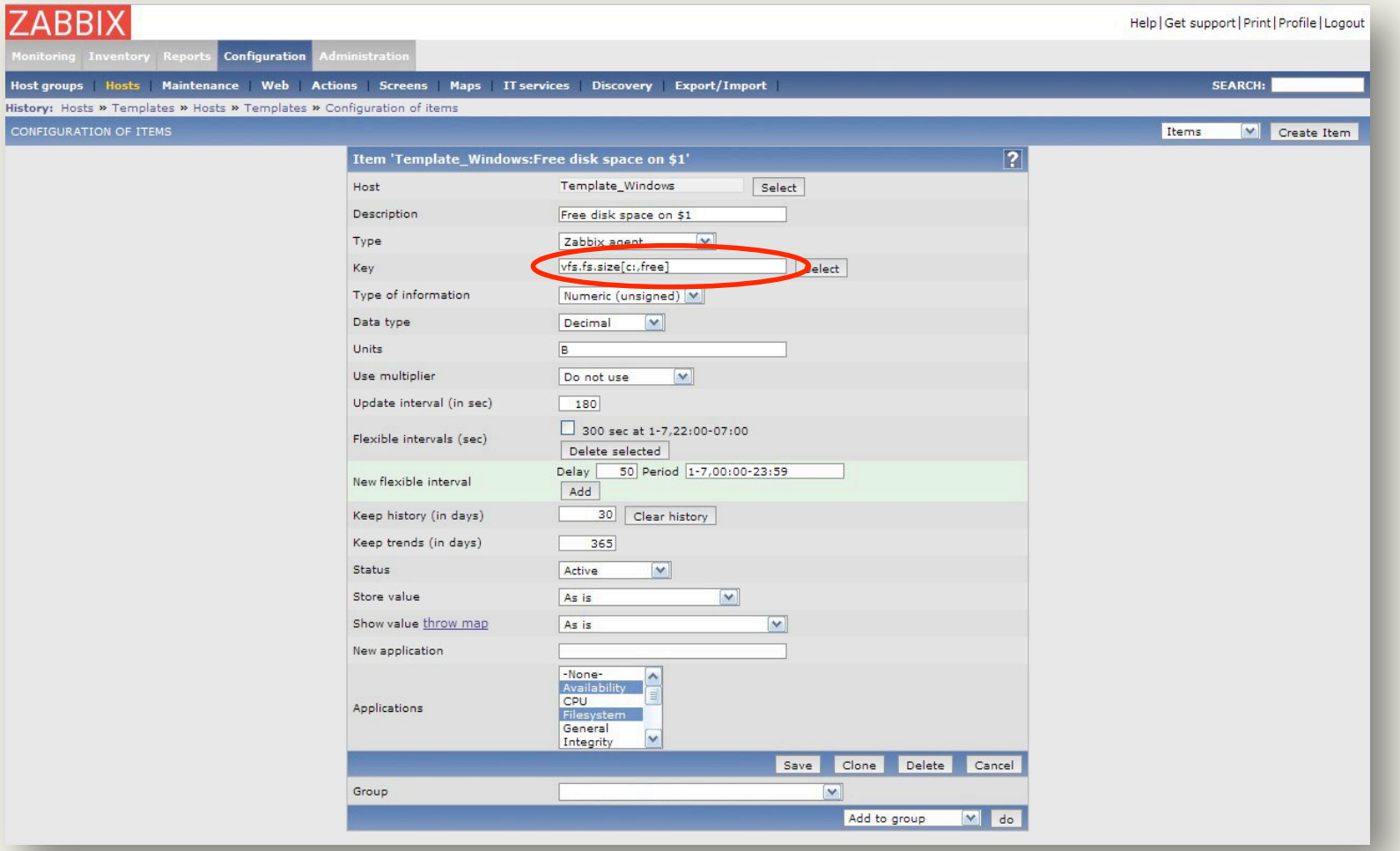




ZABBIX

Host + Items

Estructura de un item Zabbix



Clave (key)

¿Qué es lo que monitorizamos?

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

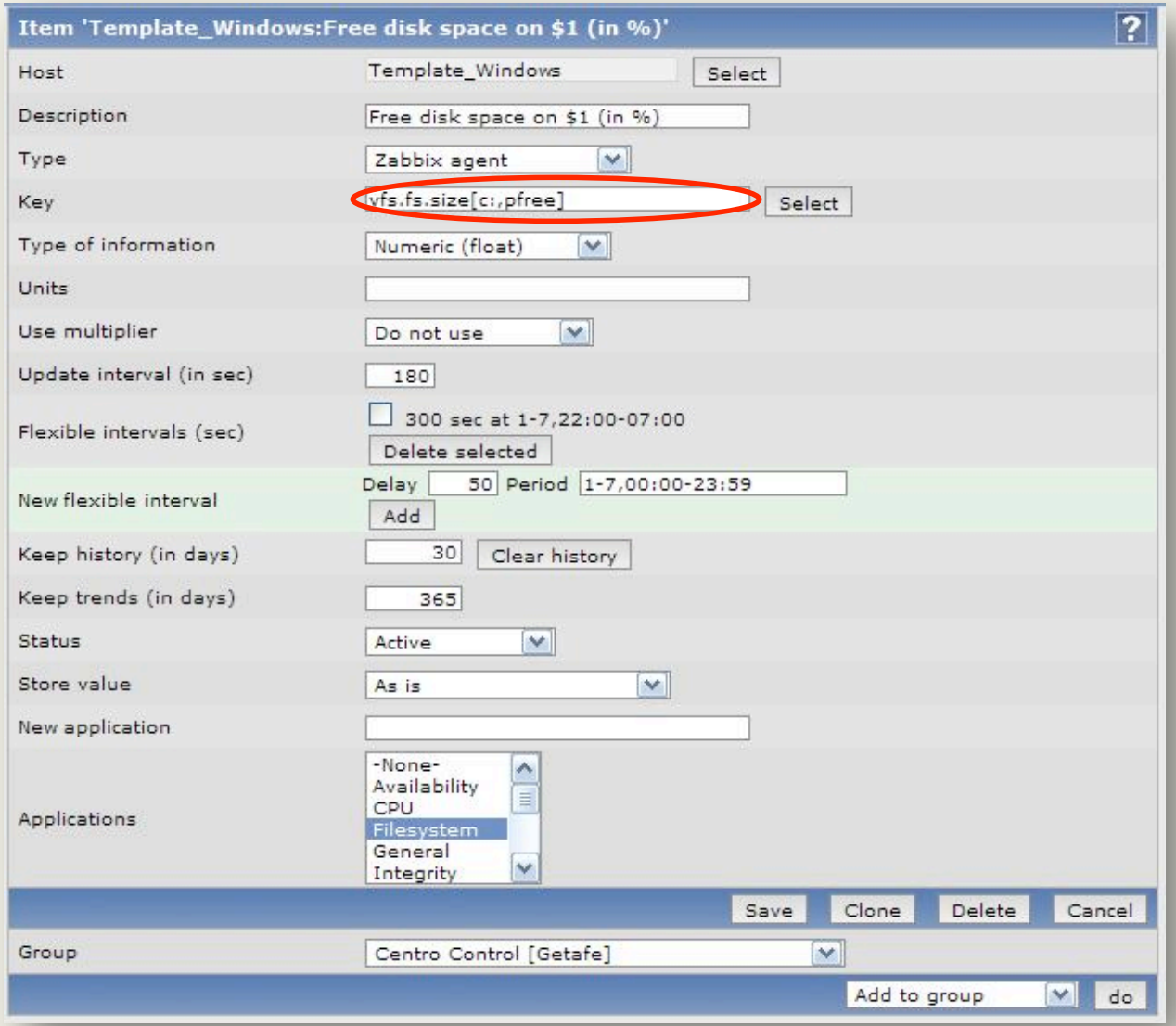
Equipos de red

- 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.

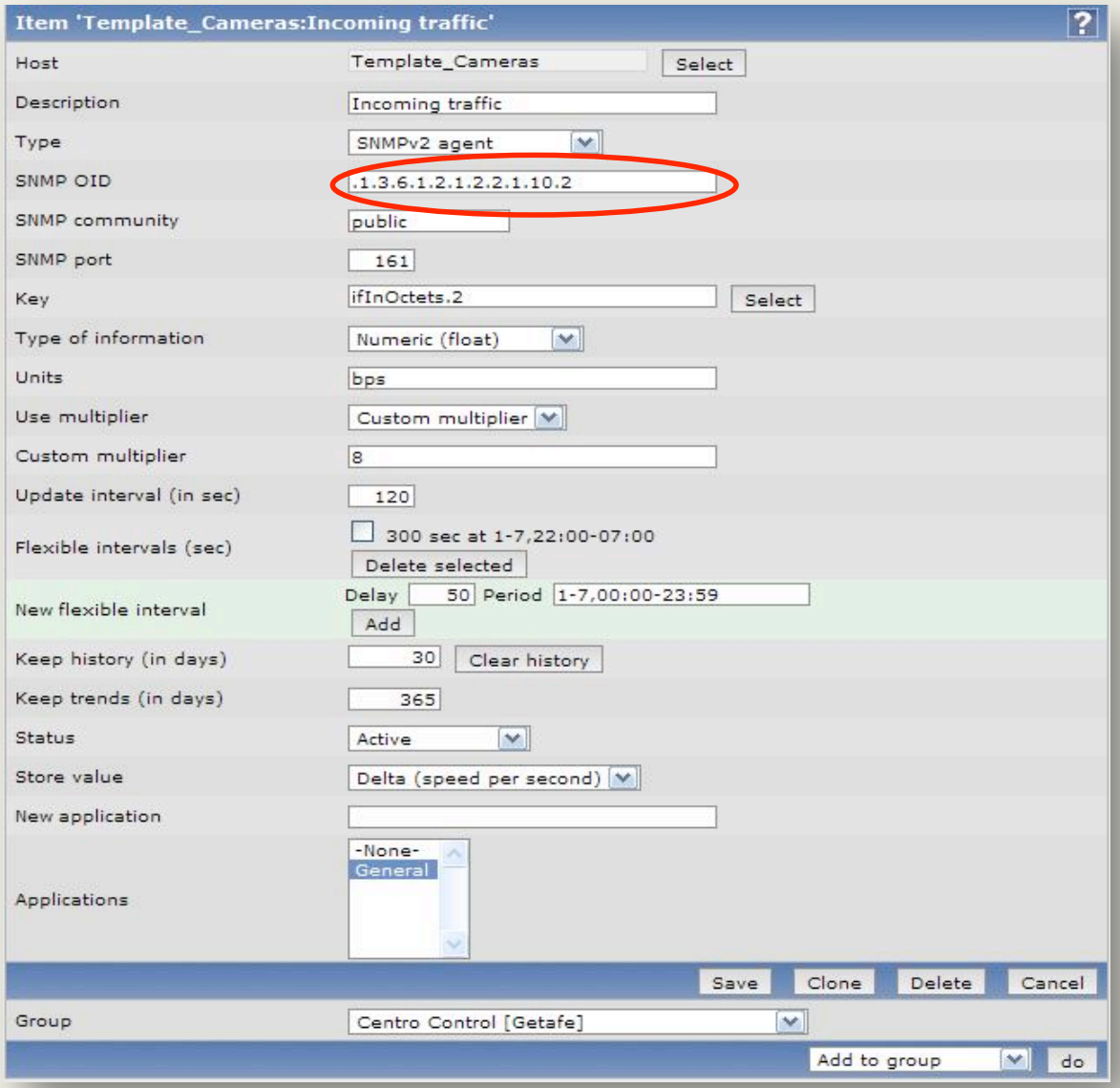
Creación del item correspondiente



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.

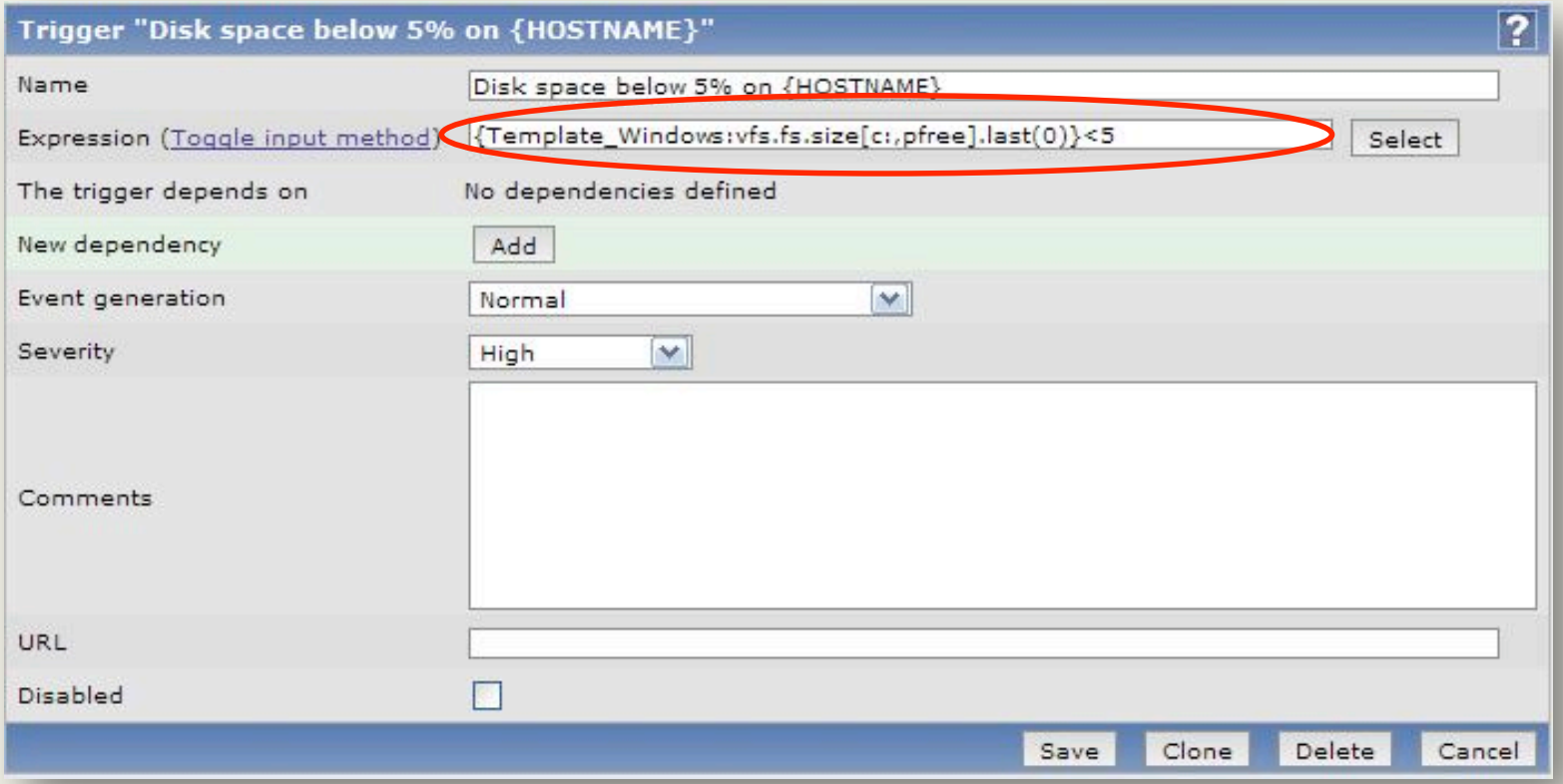
Creación del item correspondiente



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

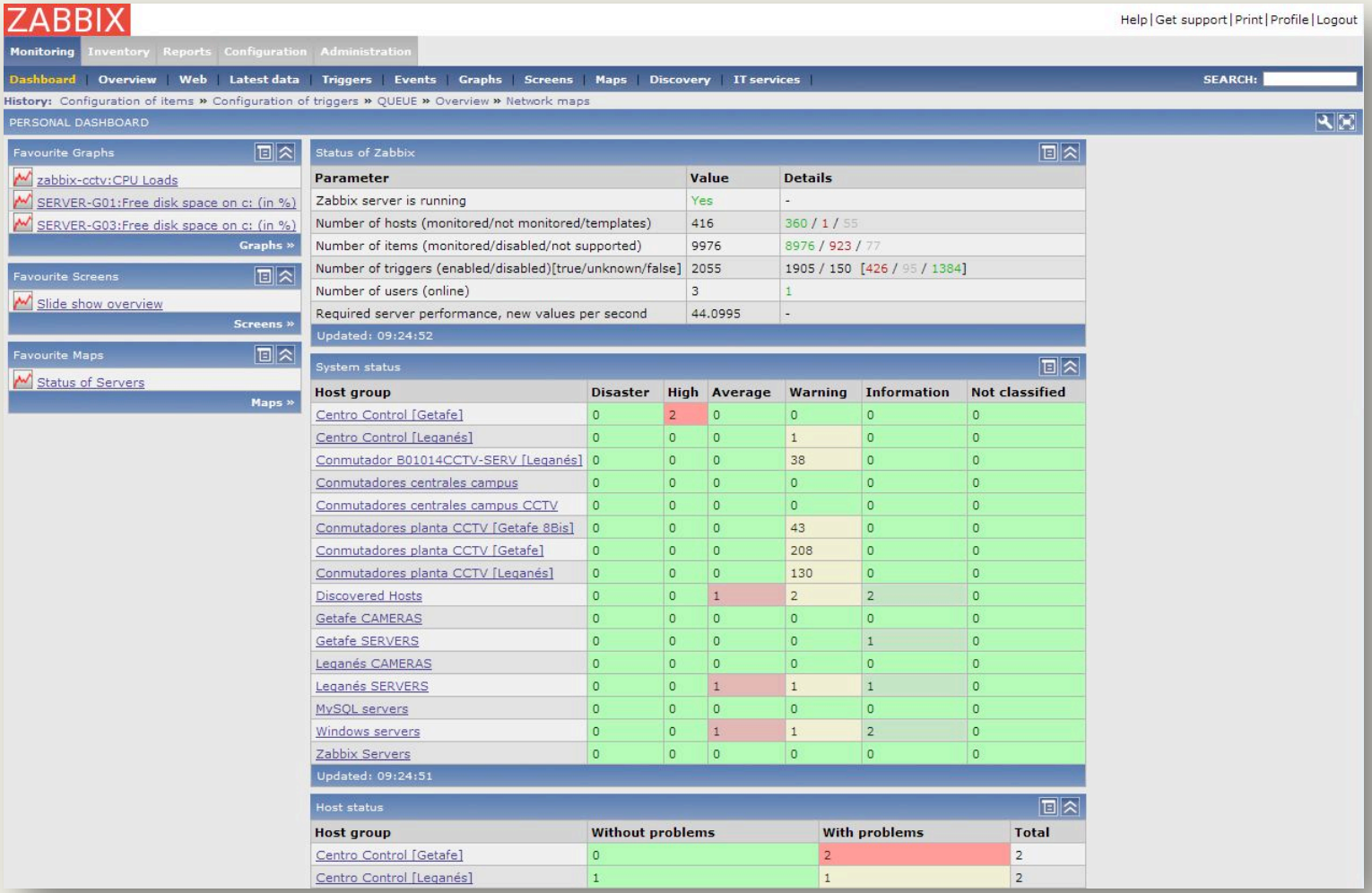
1. Seleccionar la plantilla o *host* al cual se asignará el disparador.
2. En la sintaxis del disparador, seleccionaremos el item y la función que se encargará de controlar el valor de dicho item.

Creación del disparador correspondiente



Interfaz del sistema de monitorización

Dashboard

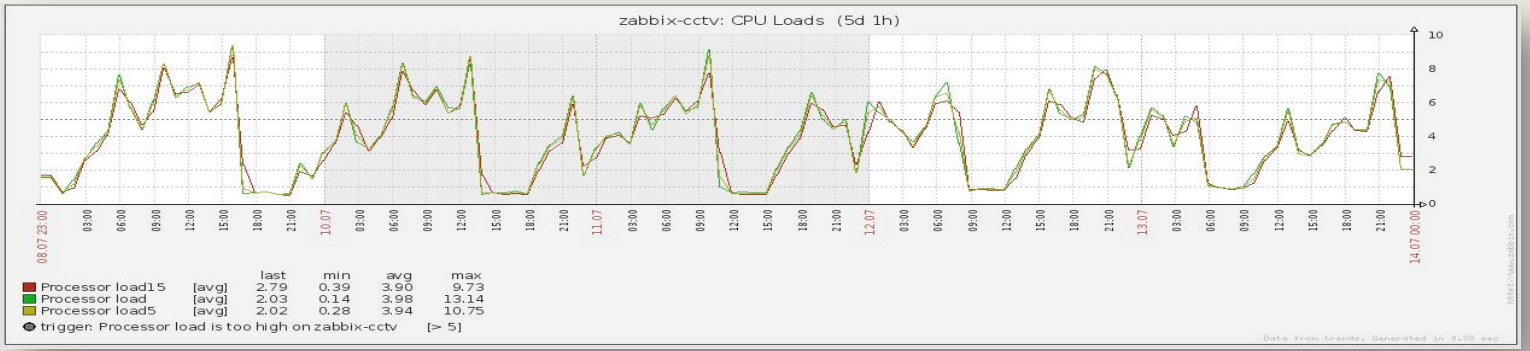


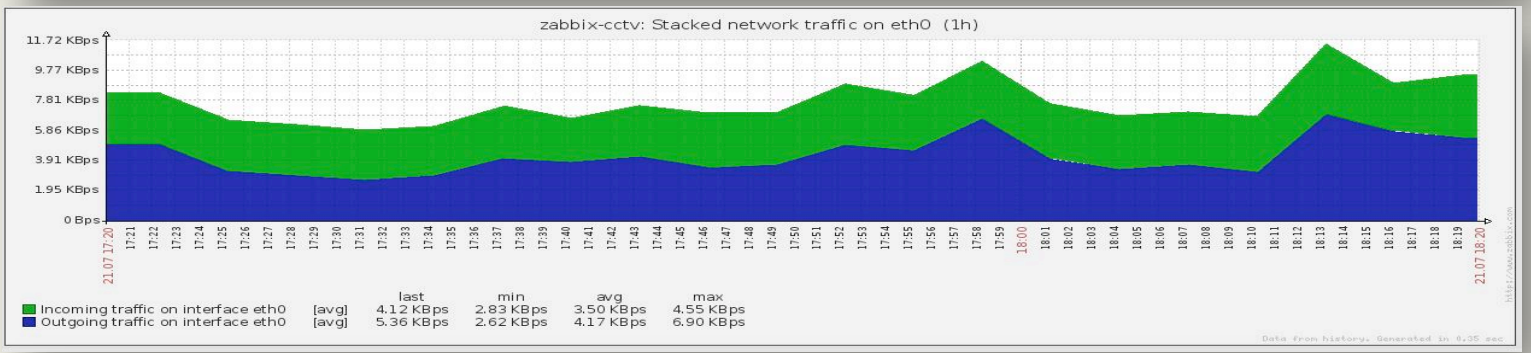
Interfaz del sistema de monitorización

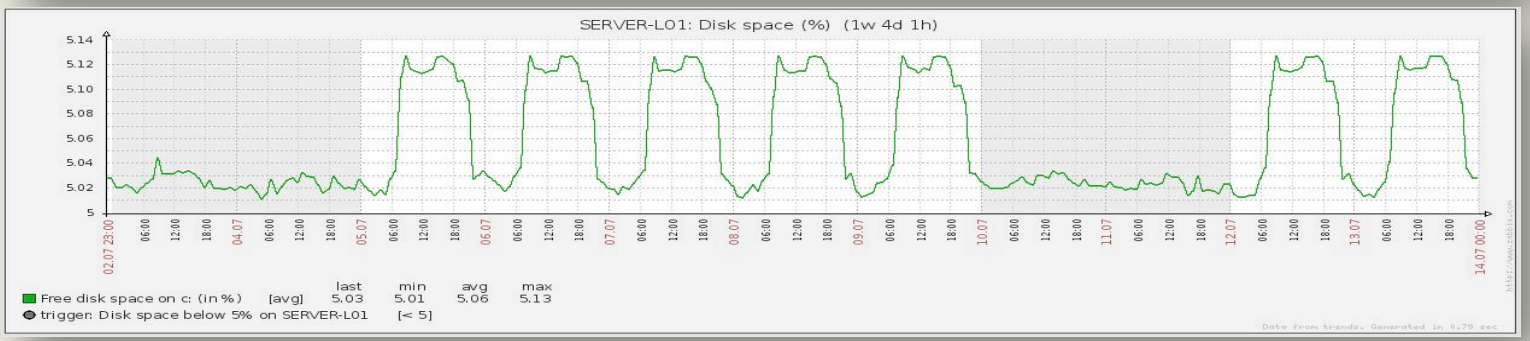
Overview

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 ºC	41 ºC	42 ºC	38 ºC	39 ºC	34 ºC
CPU usage (in %)	41.23	15.97	34.07	28.72	35.65	46.08
DHCP client service state (Dhcp)	Stopped (6)	Stopped (6)	Stopped (6)	Stopped (6)	Stopped (6)	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)	OK (255)	OK (255)	OK (255)	OK (255)	OK (255)
Drive #0 Temperature	38 ºC	35 ºC	35 ºC	25 ºC	34 ºC	30 ºC
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)	OK (255)	OK (255)	OK (255)	OK (255)	OK (255)
Drive #1 Temperature	38 ºC	35 ºC	34 ºC	24 ºC	35 ºC	30 ºC
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)	OK (255)	OK (255)	OK (255)	OK (255)	OK (255)
Drive #2 Temperature	37 ºC	36 ºC	35 ºC	23 ºC	33 ºC	29 ºC
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)	OK (255)	OK (255)	OK (255)	OK (255)	OK (255)
Drive #3 Temperature	37 ºC	35 ºC	35 ºC	23 ºC	33 ºC	29 ºC
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)	OK (255)	OK (255)	OK (255)	OK (255)	OK (255)

Graphs

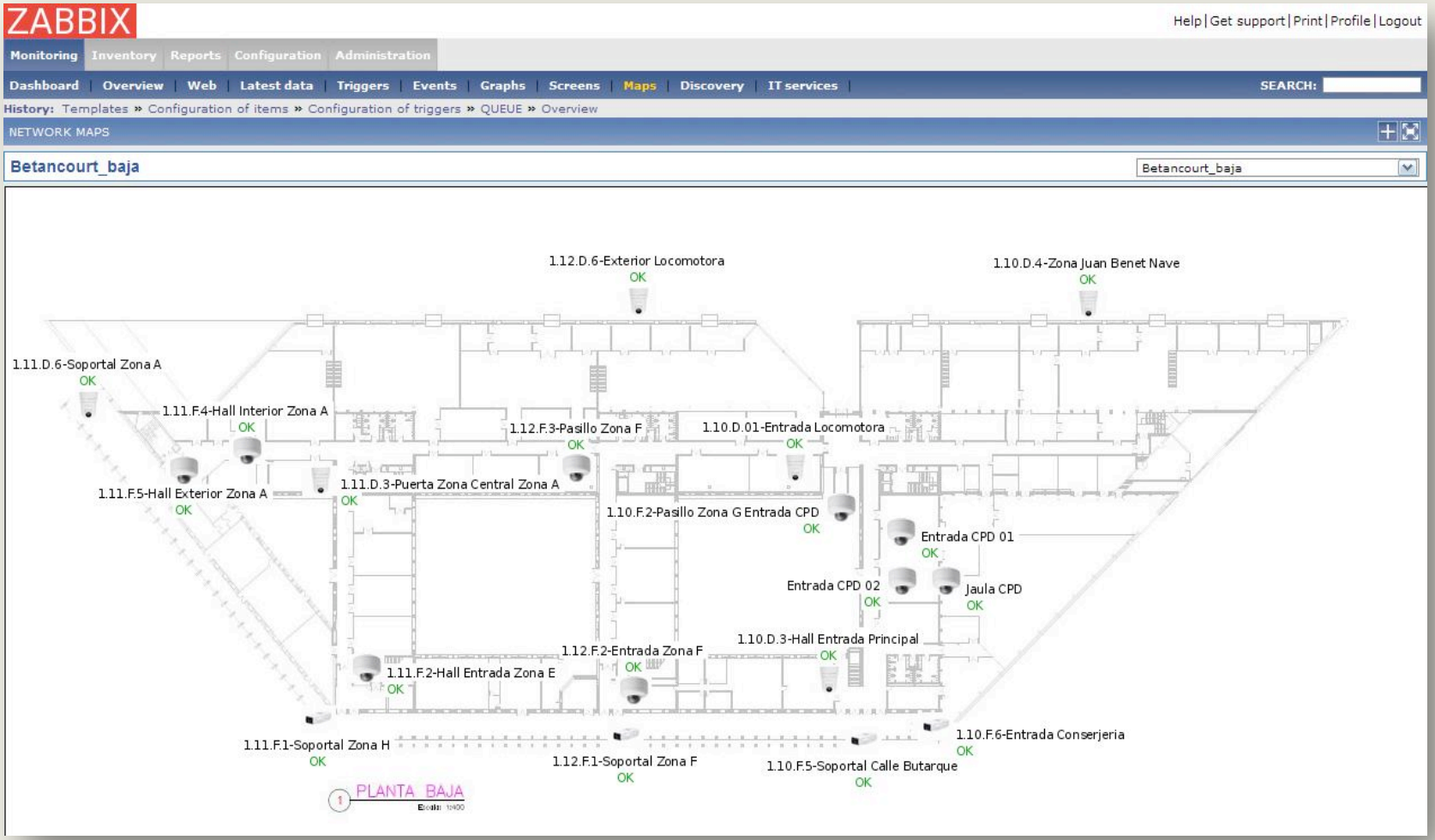

zabbix-cctv: CPU Loads (5d 1h)
last min avg max
Processor load15 [avg] 2.79 0.39 3.90 9.73
Processor load [avg] 2.03 0.14 3.98 13.14
Processor load5 [avg] 2.02 0.28 3.94 10.75
trigger: Processor load is too high on zabbix-cctv [> 5]


zabbix-cctv: Stacked network traffic on eth0 (1h)
11.72 KBps
9.77 KBps
7.81 KBps
5.86 KBps
3.91 KBps
1.95 KBps
0 Bps
last min avg max
Incoming traffic on interface eth0 [avg] 4.12 KBps 2.83 KBps 3.50 KBps 4.55 KBps
Outgoing traffic on interface eth0 [avg] 5.36 KBps 2.62 KBps 4.17 KBps 6.90 KBps


SERVER-L01: Disk space (%) (1w 4d 1h)
5.14
5.12
5.10
5.08
5.06
5.04
5.02
5
last min avg max
Free disk space on c: (in %) [avg] 5.03 5.01 5.06 5.13
trigger: Disk space below 5% on SERVER-L01 [< 5]

Interfaz del sistema de monitorización

Maps



Conclusiones

- 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

Universidad Carlos III de Madrid

- 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

Preguntas

Universidad Carlos III de Madrid