

Monitorización de equipos por snmp

[web](#), [servicio](#), [zabbix](#), [monitorización](#), [plantilla](#), [SNMP](#), [ítem](#), [trigger](#)

Verificar que tenemos el demonio snmp arrancado

Antes que nada arrancamos el servicio snmpd y lo dejamos habilitado en el arranque por defecto

```
systemctl snmpd enable  
systemctl snmpd start
```

Instalamos los siguientes paquetes

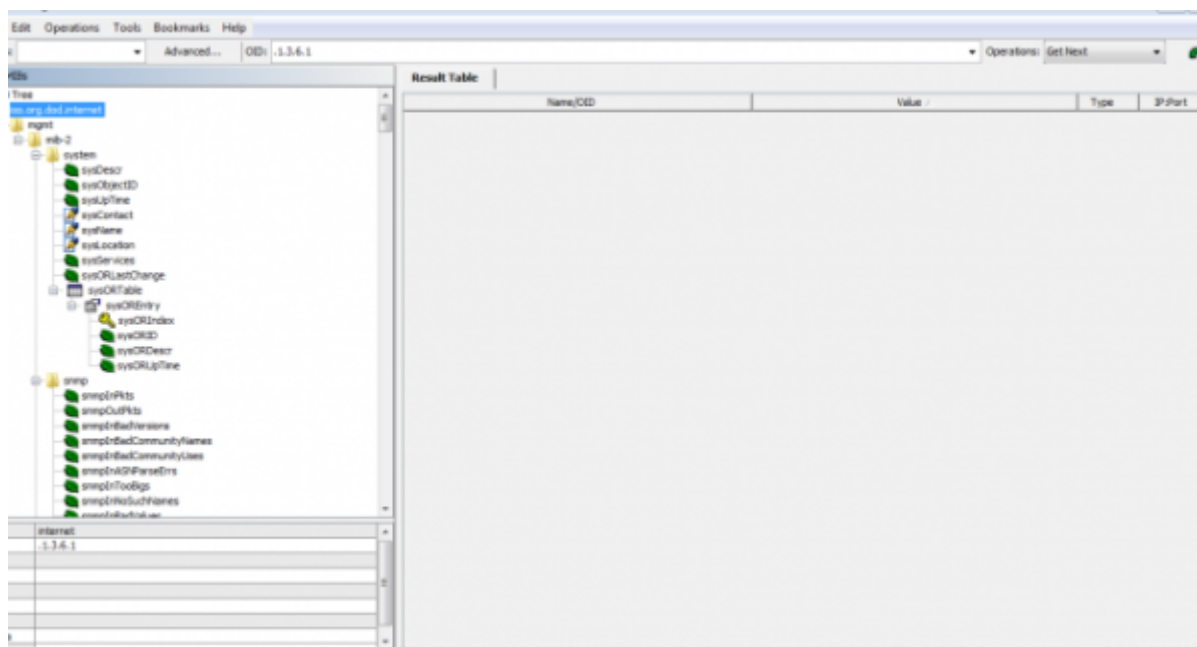
```
yum install -y net-snmp-utils net-snmp-perl
```

Hacemos una prueba para ver que todo está funcionando

```
snmpwalk -v 2c -c public localhost system
```

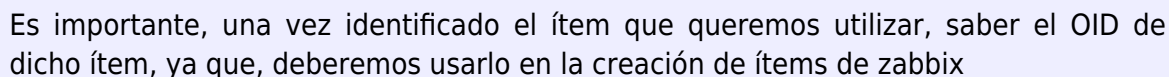
Para monitorear un equipo con zabbix primero debemos localizar un MIB compatible con el equipo que vayamos a monitorear. Podemos buscar en la pagina web del fabricante o buscar en [esta página](#) .

Una vez encontremos el MIB correcto podemos usar varias herramientas para interpretarlo. Una de ellas es el uso de aplicaciones como por ejemplo MibBrowser, que nos permite ver el árbol del MIB y desplegarlo para buscar lo que necesitamos.



También podemos utilizar el comando **SNMPWALK** que nos mostrará todos los OID y los compara con los datos del MIB, además mostrará los datos de aquellos que coincidan.

The screenshot displays the Wireshark network protocol analyzer interface. The top status bar shows the address as 1.3.6.1 and the operation as 'Operations: G'. The left pane shows the packet list and packet details for an Internet packet (1.3.6.1). The right pane shows the MBTree tree structure, including system, sysDescr, sysObjectID, sysUpTime, sysContact, sysName, sysLocation, sysServices, sysORLastChange, sysORTable, sysOREntry, sysORIndex, sysORID, sysORDescr, sysORUpTime, snmp, snmpInPkts, snmpOutPkts, snmpInBadVersions, snmpInBadCommunityNames, snmpInBadCommunityUses, snmpInAShParseErrs, snmpInTooBig, snmpInNoSuchNames, and snmpInNotWritable. The bottom pane shows the packet bytes and hex dump.



Otra manera de encontrar un ítem para monitorizar nuestro equipo es a través de la herramienta **SNMP BUILDER** que nos proporciona zabbix. Para acceder a ella debemos seleccionar “**Configuration/SNMP Builder**”.

configuration

Administration

Maintenance

Actions

Screens

Slide shows

Maps

Discovery

IT services

SNMP Builder

Configuration of hosts » Configuration of items » Configuration of host groups » Configuration of hosts

0

MIB: ---/usr/share/snmp/mibs

Host:

SNMP Version: 2c

OID Data - Click to force view as table

Items list

Items

Interval: 60

History: 90

Trends:

Graphs

Create graph

Name:

Width: 900

Height: 200

Function: avg

Draw style: Line

Y axis side:

Save

Clear

Como podemos ver en la imagen, la pestaña de **SNMP Builder** consta de una cabecera que debemos rellenar. De izquierda a derecha nos encontramos:

- **Template:** aquí debemos seleccionar la plantilla en la que vamos a guardar el ítem. Podemos crear una plantilla nueva o usar una existente.

- MIB: en este desplegable elegiremos un MIB para buscar los ítems.
- Host: IP del equipo que queremos monitorizar.
- SNMP Versión: la versión de SNMP que vamos a usar (1, 2c).
- Community: es una clave que permite acceder al equipo (por defecto suele ser public pero se puede cambiar).

Ahora que hemos configurado los requisitos previos se nos mostrará como en el **MIB Browser** el árbol del MIB a la izquierda. Sin embargo a la derecha se nos mostrará algo diferente.

The screenshot shows the MIB Browser interface. On the left is the 'OID tree' with a list of MIBs. The 'LIEBERT-GP-POWER-MIB' is selected, and the 'lgpPwrBatteryTimeRemaining' object is highlighted. On the right, the 'OID Data' section shows the selected OID name, its type (INTEGER), and its value (131 minutes). Below this, the 'Items list' section shows the same OID name, description, and type. At the bottom, the 'Graphs' section allows creating a new graph with fields for Name, Width, Height, Graph type, Function (set to 'avg'), Draw style (set to 'Line'), and Y axis side (set to 'Right'). There are 'Save' and 'Clear' buttons.

Si seleccionamos uno de los ítems del **“OID tree”**, a la derecha en **“OID name”** se nos mostrará el nombre, el tipo de dato y el valor del mismo (en el caso de que exista algún valor). Clicamos dos veces sobre el nombre del OID y aparecerá abajo en **“Items list”**. Por último, podemos seleccionar el intervalo en el que se va a recoger los datos del ítem y crear una grafica sobre el mismo si así lo deseamos (estos dos elementos pueden modificarse más tarde).

Clicamos en **“save”** para añadir el ítem a la plantilla que hemos seleccionado.

Configuración del Host

Para crear un nuevo host en zabbix debemos ir a **“Configuration/hosts”**, una vez allí clicamos en **“créate host”**.

The screenshot shows the Zabbix Host configuration interface. At the top, there are tabs for Host, Templates, IPMI, Macros, and Host inventory. The Host tab is active. Below the tabs, there are input fields for Host name and Visible name. A section for Groups includes 'In groups' and 'Other groups' lists. A 'New group' section has a text input. The 'Agent interfaces' section contains a table with columns for IP address, DNS name, Connect to, Port, and Default. Below this are sections for SNMP, JMX, and IPMI interfaces, each with an 'Add' button. At the bottom, there are dropdowns for 'Monitored by proxy' and 'Status'.

En la primera pestaña “Host” configuraremos los datos básicos del mismo.

- Host name: el nombre del equipo.
- Groups: seleccionamos a qué grupo queremos añadir el equipo o creamos uno nuevo (new group).
- Agent interfaces: aquí seleccionaremos el agente por el cuál queremos monitorizar nuestro equipo, en nuestro caso por **SNMP interface**. Clicamos en “add” y debemos indicar la IP o el nombre DNS del equipo (el puerto del SNMP es el 161).
- Status: elegimos empezar o no a monitorizar el equipo.

En la siguiente pestaña elegimos la plantilla para nuestro equipo, por lo general la que tenga los ítems que queramos.

The screenshot shows the Zabbix Host configuration interface, specifically the Templates tab. It displays a table for 'Linked templates' with columns for Name and Action, showing 'No templates linked.' Below this is a 'Link new templates' section with a search bar. A dropdown menu is open, showing search results for 'a'. The results include 'APC 7500', 'APCBattery', 'Symmetra PX40', and several 'Template App' services like 'Template App FTP Service', 'Template App HTTP Service', etc. A 'Save' button is visible at the bottom of the search results.



Las otras pestañas no hace falta configurarlas en este momento.

Configuración de los ítems

Nos situamos en “**Configuration/Hosts**” y seleccionamos el equipo que acabamos de añadir y dentro elegimos la pestaña “**Ítems**”.

Aquí crearemos los ítems que buscamos previamente con el **MIB Browser**, en caso de haberlo realizado con **SNMP Builder** aparecerá automáticamente.

Clicamos en “**créate item**”.

The screenshot shows the 'Item' configuration form in Zabbix. The form is titled 'Item' and contains the following fields and sections:

- Name:** A text input field.
- Type:** A dropdown menu with 'Zabbix agent' selected.
- Key:** A text input field with a 'Select' button next to it.
- Host interface:** A text input field with the error message 'No interface found' in red.
- Type of information:** A dropdown menu with 'Numeric (unsigned)' selected.
- Data type:** A dropdown menu with 'Decimal' selected.
- Units:** A text input field.
- Use custom multiplier:** A checkbox with a value of '1' next to it.
- Update interval (in sec):** A text input field with the value '30'.
- Flexible intervals:** A table with columns 'Interval', 'Period', and 'Action'. The table is currently empty with the text 'No flexible intervals defined.' below it.
- New flexible interval:** A section with fields for 'Interval (in sec)' (50), 'Period' (1-7,00:00-24:00), and an 'Add' button.
- History storage period (in days):** A text input field with the value '90'.
- Trend storage period (in days):** A text input field with the value '365'.
- Store value:** A dropdown menu with 'As is' selected.
- Show value:** A dropdown menu with 'As is' selected and a 'show value mappings' link.
- New application:** A text input field.
- Applications:** A dropdown menu with '-None-' selected.
- Populates host inventory field:** A dropdown menu with '-None-' selected.
- Description:** A large text area.
- Enabled:** A checkbox that is checked.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom.

- Name: el nombre del ítem.
- Type: el protocolo por el cuál se va a buscar el ítem (en nuestro caso SNMPv1 o SNMPv2).
- Key: nombre clave del ítem (se usará para llamarlo en los triggers). Si elegimos SNMP aparecerá:

- SNMP OID: la OID que buscamos con el **"MIB Browser"**.
- SNMP Community: la clave para acceder al equipo.
- Port: el puerto por el que trabaja el SNMP (161).
- Type of information: declarar si es numérico, texto, etc.
- Update interval (in sec): cada cuanto tiempo se va a recoger el dato.
- Description: una breve descripción de ítem.

El resto de parámetros no los usaremos para este ejemplo.

Cuando hayamos guardado en la pestaña ítems de nuestro equipo deberá aparecer todos los ítems que hayamos creado, para saber que estos funcionan correctamente debe aparecer a la derecha del todo una columna llamada **"Status"** en la que debe aparecer **"enabled"** si lo tenemos activado y a su derecha debe de haber un icono verde que indica que no hay errores al recoger el dato.

(0) Items (8) Triggers (9) Graphs (3) Discovery			
	Key	Interval	Histo
:)	upsAdvBatteryTemperature	30	7
:)	upsBasicBatteryStatus	30	7
:)	inputVol	30	90
:)	upsAdvRunTimeRemaining	30	7



Puede darse el caso de que tengamos varios dispositivos similares a los que queramos monitorizar los mismos ítems, por lo que, sería conveniente crear los ítems y los triggers en la plantilla para no tener que crearlos para cada uno de los equipos.

Creación de Triggers

Los triggers o disparadores son elementos que envían una notificación cuando se cumple una condición previamente establecida. Estos se refieren a un ítem en concreto.

Seleccionamos **"triggers/Create trigger"**:

Trigger Dependencies

Name

Expression Add

[Expression constructor](#)

Multiple PROBLEM events generation ☐

Description

URL

Severity **Not classified** Information Warning Average High Disaster

Enabled ☒

Save Cancel

- Name: Nombre del trigger.
- Expresión: aquí indicaremos la condición que debe cumplirse para que se desencadene el disparador.
- Description: breve descripción de lo que hace el trigger.
- Severity: aquí podemos elegir la magnitud del problema (se mostrará en la tabla de incidencias de monitoring).

Respecto a **“Expresión”** la nomenclatura que hay que seguir es [esta](#).

Ejemplo:

```
{nombreDelHost:NombreDelItem.función}(<, >, >=, <=, #, etc.) valor  
{UPS0004:upsAdvRunTimeRemaining.last(0)}<10m
```

Este trigger nos avisará cuando el último valor (last) recogido del tiempo de carga restante (upsAdvRunTimeRemaining) del equipo UPS0004 es menor que 10 minutos ($\{x\} < 10m$). Si se cumple la condición mandará un aviso por zabbix según la importancia de la incidencia que hayamos indicado.

Referencias

- <http://panicoenelcpd.blogspot.com.es/2011/07/plantilla-de-dispositivos-snmp-en.html>

From:
<https://intrusos.info/> - LCWIKI

Permanent link:
<https://intrusos.info/doku.php?id=seguridad:monitorizacion:zabbix2:snmp&rev=1425909911>

Last update: **2023/01/18 14:39**

