Zabbix Monitoring System

INTRODUCTION

Zabbix Monitoring System:

- **Unlimited scalability:**
  - From monitoring your smart home to multi-tenant enterprise environments.
- **Secured and safe:**
  - Keep your sensitive information secure by storing it in an external vault.
- **High availability:**
  - Ensure 24/7 uptime and negate the risk of data loss.
- **Flexible:**
  - Monitor whatever you want.

How do Zabbix monitor other devices?

- **How does Zabbix monitor other devices?**
  - **Zabbix Server:**
    - A virtual machine that has Zabbix Server installed on it, configured, and has an IP address in order for his agents to communicate with it.
  - **Zabbix Agent:**
    - On each Linux/Windows based devices that we want to monitor, a Zabbix Agent needs to be installed and to be configured properly in order to communicate with the Zabbix Server.
  - **SNMP:**
    - Other devices such as switches, must use SNMP protocol in order to communicate with the Zabbix Server.
- In this introduction we will go through a few examples of how the Zabbix monitor system works, our main one will be a monitored database events counter.

WeCom Hosts & Host Groups

- WeCom have several Host Groups, such as: Billing, CallUp, CRM, CyberArk, Ericsson, Voice Center & ex.
- Each host group have a number of hosts configured on it, for example, in the host group CRM, we have 14 hosts, some are responsible for the CRM application and some for Joomla database.
- Each host, has a lot of items & triggers(alerts) configured on it.
- In total, we have above 200 hosts that are currently been monitored by Zabbix.
- For those host we have above 70,000 items and above 30,000 triggers.

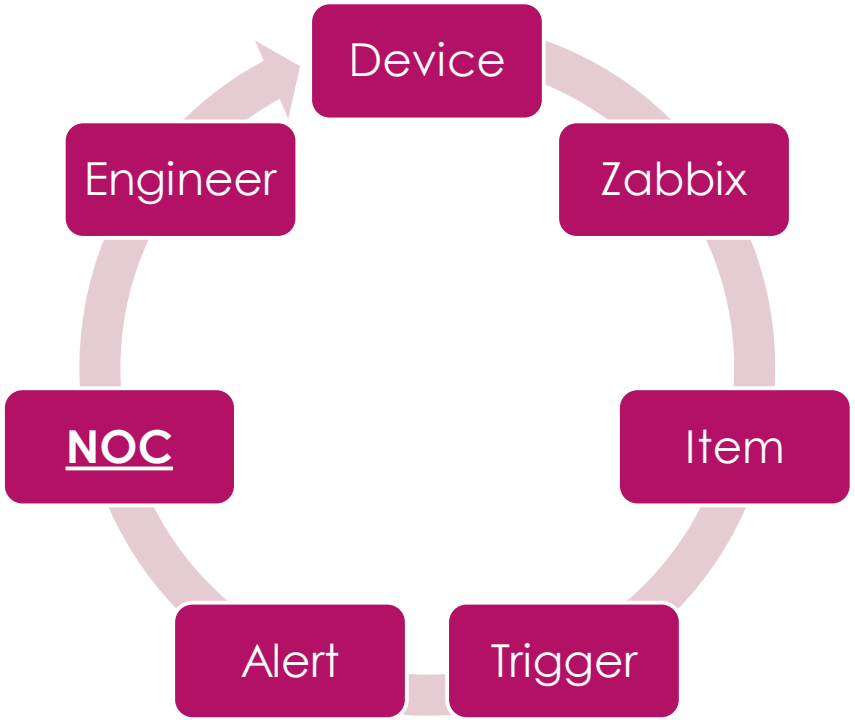
Zabbix Alerts & Severities

- Zabbix can fire many different kind of alerts, such as: Disk space, CPU utilization, Memory usage, Swap usage, Links down & ex.
- Each alert can have its own special procedure.
- In the configuration phase of a trigger(will be shown in the trigger slide) a severity is been selected, this severity will determine when & how the NOC specialist should act.
- There are five kind of severities, Information, Warning, Average, High, Disaster.
- We will see an example of an alert in the Alert slide.

Zabbix Graphs

- One of Zabbix features is its Graphs, any custom graph that has been configured for the host can be displayed, as well as any simple graph.
- In the example below we can see a CPU utilization graph for the host blapp2-hfa, we can see that the last value was 9.4%, the minimum is 2%, maximum 53%, and the average value was 11% in the last five days.

The Complete Process:

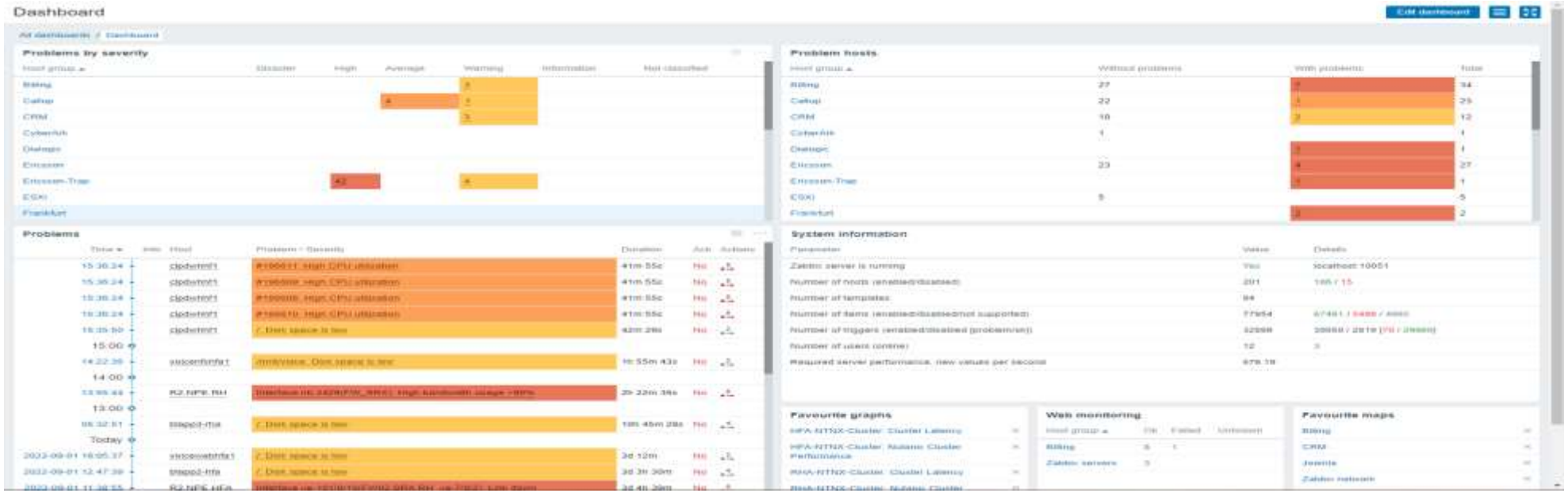


The Complete Process Break Down: **Device** Perspective:

- As we mentioned before, Zabbix can monitor a lot of devices.
- In this presentation, we will use as an example a Virtual Machine as a device.
- Our device IP address is: 10.21.2.30
- Our device is running Mongo Database.

The Complete Process Break Down: **Zabbix** Perspective:

- The way we control Zabbix monitoring system is through a Web GUI:
- Our Zabbix Web address is: http://10.21.14.41/zabbix
- For example, A screenshot of a Zabbix main dashboard page:



The Complete Process Break Down: **Item** Perspective:

- An **item** is a single performance or availability check. In each item configuration we must provide to it the IP address of the Device we want this item to be added for.
- In our example, our item is called “mongo events count”.
- Each item has a key, this key is what the Zabbix server will search for in the device which it is communicating with through Zabbix agent.
- Zabbix will perform this search every minute(can be changed). In other words, it will talk with his agent and ask him about this key every minute.
- On the device side, there is a file with premade commands that will be executed once this key is searched for by the agent.

The Complete Process Break Down: **Trigger** Perspective:

- Triggers are logical expressions that "evaluate" data gathered by items and represent the current system state.
- In WeCom Zabbix monitoring system there are 32,199 triggers at the moment.
- Each trigger can have a different kind of severity, this information is for the NOC in order for them to know what procedure is to be used based on the trigger severity. In our example our severity is **High**.
- In our example, our trigger name is: “Events Counter”.
- Each trigger has a Problem & Recovery expressions (functions).
- In our example, the trigger’s problem expressions is:
- “{blapp1-hfa:event.count.avg(15m)}=0” which basically means, if the average values you summed up from your item in the last 15 minutes is: 0, fire an alert.
- In other words, if there was no events created in the database(our device) in the last 15 minutes at all, fire an alert.

The Complete Process Break Down: **Alert** Perspective:

- Zabbix alert are being fired once one of the triggers problem expression is been activated.
- We will receive an main from Zabbix that will look like this:

Notification:	PROBLEM [High]
Service:	Events Counter
Host group:	Billing
Host:	blapp1-hfa
Host IP:	10.21.2.30
Problem started at:	01:11:04 on 2022.08.25
Description:	Call Ofer from Billrun team Notify Yael as well
Last Value	0
Original problem ID:	2816884395
Monitor Info:	We4G-Zabbix-Nutanix

Notification:	RECOVERY [OK was High]
Service:	Events Counter
Host group:	Billing
Host:	blapp1-hfa
Host IP:	10.21.2.30
Problem has been resolved at:	01:13:04 on 2022.08.25
Description:	Call Ofer from Billrun team Notify Yael as well
Last Value	4
Original problem ID:	2816884395
Monitor Info:	We4G-Zabbix-Nutanix

- **Left:** Alert in its **"Problem Expression",** we can see the host & host group of this alert, the host IP address(device). We can see when the problem has started, at the top we can see the alert severity, and we also have a short description on how to behave with this particular alert.
- **Right:** We can see the same alert but this time in its **"Recovery Expression"**, which means the problem has been resolved.

The Complete Process Break Down: **NOC** Perspective:

- WeCom NOC will receive the alerts via Email from the Zabbix monitoring system.
- There are different procedures based on different Host Groups and different Alerts & different Severities.
- There are kind of severities that will only require a ticket documentation like alerts with “Information” severity.
- There are kind of alerts with “Disaster” severity that will require immediate actions in order to solve the issue as quick as possible.
- WeCom NOC will need in some procedures to escalate to a relevant engineer(system/network) in order to resolve the issue.

The Complete Process Break Down: **Engineer** Perspective:

- After the engineer is being notified by the NOC, depends on the issue of course, he will login to the device and will try to resolve the issue and notify back the NOC that the problem is now resolved.

- In our example, as the alert description says, the NOC needs to notify Ofer from Billrun team in order to solve the issue, and notify Yael as well.

- Once Ofer is done resolving the problem, NOC should receive the recovery expression of the trigger and the process is starting all over again.