"INTEGRATING ZABBIX INTO YOUR IT ECOSYSTEM - A TO Z"

Eric Doan
Technical Director
Our Agenda Today

Maybe you are thinking towards mixing the value of your CMDB data into Zabbix. Or you want to monitor real user experience. And fancy some cool dashboards.

Who I am

- AXEL IT is a french Zabbix premium partner
- CTO at AXEL IT
- I designed/deployed/supported many monitoring solutions for 20+years

What we’re going to talk about

- Common industry answers to frequent business issues
- Overcome design challenges with Zabbix integration to other software
- Mostly CMDB and ITSM products, but also others!
- Licensing issues

What we’re NOT going to talk about

- Enter the « gory » details
- ITIL
- My choices of webcomics
Monitoring as explained to my granddaughter

Another day starts with something that is not working as it should which goes usually as:

**YOUR BOSS**: « *it’s DOWN! Fix it now!*
**YOU**: *Hope it’s the network*
Starting with an integration for METRICS

Zabbix can monitor the network using SNMP
- Standard data such as bandwidth, errors, buffers
- Custom data for the hardware
- Events with SNMP notifications

We wanted the ability to present network flow information in Zabbix (aka. your L7 Firewall metrics)

But firewalls aren’t really monitoring-friendly with their data. Plus, not every network port is actually a firewall port.
Starting with an integration for METRICS – How?

A previous solution from Zabbix 1.x

Packet Capture

Extract items

Zabbix API was in writing
Bound to agent interface and IP
Capture filters (libpcap)

POC extracting data from a NPM solution (Zabbix 3.4)

Not really scalable
Issues with HA / Zabbix topology
Capture everything, 70 metrics
Cannot LLD flows

Needed to have H5 and Zabbix in touch for a deeper integration

Will scale and adapt to topology
Can exchange object metadata
Monitoring as explained to my granddaughter

So... what part of the Information System is actually down?

YOU : Turn to Zabbix. Identify Root cause. Fix problem.
There are many ways to fix a problem
Do Ops persons have a bias towards « quick fixes » over « permanent fixes » ?

Some efficiency questions arise when there are multiple ongoing incidents:
What should we fix first?
What team should work on the issue?
How do we make sure it does not happen again?
A very brief History of the ITSM Industry

The ITSM industry focuses on aligning IT services with business needs.

ITIL through successive iterations provides an operating model for:
- Service Support and Delivery (v2),
- Service Lifecycle (v3),
- Service Value chain (ITIL 4)

We work with **iTOP**, an open-source ITSM software distributed by Combodo which is based on ITIL.

iTOP is a complete open source, ITIL, web-base IT Service management tool featuring
- Helpdesk and Incident Management
- Service and contract Management
- Change Management
- A fully configurable CMDB
- Web services
A core function of the CMDB is to model **Dependency mapping** and **Impact Analysis**.
Configuration Management Database – Run Impact Analysis

Using Impact analysis we can predict the impact that a change will have to the availability of services.
When a service is unavailable, we can also run reverse and find the root change or incident. We want to provide Incident creation at most levels through Zabbix.

Dependency on Assets

Service is down

Incident and Recent change on switch1

Associate to CI

Zabbix PROBLEMS

Create Incident
BASIC REQUIREMENTS

LIFECYCLE INTEGRATION
1) Open an incident when a problem is detected
   • Manage Single/Multiple generation
2) Close an incident when a problem is closed
   • Using correlation or automation
   • Using manual close
3) Close a problem when the incident is solved

ADVANCED IMPLEMENTATION

TWO-WAY INTEGRATION
A. Synchronize comments and journal entries
B. Update incident when there’s new monitoring data
C. Calculate Incident severity
   • Declare on the correct CI in the service chain
   • Leverage Impact Analysis to find the service
   • Modify priority according to the service SLA
   • Trackback severity change to the Problem
D. Add Monitoring configuration to the CMDB
E. Automate Maintenance Period & Change tracking
#Ways to forward events to an external System

## 1. Open an incident

2. Close an incident

3. Close a problem

### #1 – Use email – Don’t do that
Quick and unreliable solution. Mail poppers WILL get clogged at some point. Will mostly fail at 2) Close incident and 3) Close problem

### #2 – Use Actions Scripts - OK
We can retrieve and store the incident ID and add our own logic (&logs) Which we choose to do through a set of PHP files for create/update/recover

### #3 – Use Webhooks – WAY TO GO
Out of the box integration for many systems (JIRA, SNOW, Teams, Slack...) Can add your logic (&logs) with javascript and leverage notification schemes

**Can update EVENT tags** with return values (e.g: add ticket number) and create menus
You should notify a dedicated integration user
Forward Problems with Action scripts

1) Zabbix Server generates Event
2) Event data is pushed to iTOP
3) A new incident is created. Find and associate to the correct CI
4) Update the trigger URL definition, which works in dashboard and problem menu
   Verify if specific service was listed in TAGs
   (New in v5, event menu from Webhook integrations)
5) We have to check if the EVENT mode is single or multiple
   If it’s SINGLE: Create incident
   If it’s MULTIPLE: Check if there are new/different values
6) Autorun impact analysis on the CI, and attach services. Update Severity and trackback that value to the original EVENT
Update and close problems

1) When the lifecycle of an incident ticket is changed

2) We update the matching problem

Ticket assignment — Acknowledge and log

Journal updates

Ticket closed — Mark problem as resolved

Problem solved — Mark ticket as closed

TO DO LIST:
1. Open an incident
2. Close an incident
3. Close a problem
A. Synchronize comments
B. Update incidents
C. Change problem severity
A problem with PROBLEMS

Zabbix PROBLEMS are issued:
- As EVENTS
- Initiated by TRIGGERs
- From HOSTs
- Within the scope of ITEMs
- May concern APPLICATIONs

They are defined in TEMPLATES

➔ We need to map each of those to the CMDB Data model for efficient declaration and linkage

On this infinite grid of ideal one-ohm resistors, what’s the equivalent resistance between the two marked nodes?

https://xkcd.com/356/
Data model (simplified) – CMDB side

Zabbix hosts

Zabbix items or applications
Data model – A new CMDB class for Zabbix

- A solution: Create a new CMDB class to map Zabbix hosts
  - Zabbixhost will be used as the source to the trigger data
  - Add CMDB logic to represent relations with other Cis (hardware, software, business process...)
  - Add CMDB logic to keep track of host groups and templates
Zabbix configuration data in the CMDB

- This will also allow us to create hosts from iTop to Zabbix
  - Provisioning a new CI in the CMDB will add the host in Zabbix
  - Zabbix hosts may this way be linked to arbitrary CI classes

- Hostgroups can also be linked for the new host
- Templates can also be manually added, or reviewed for existing hosts
Synchronization Model

Model 1: Only hosts

Will you only manage hosts, or are application and services needed?

Model 2: Hosts and Services

Will you only manage hosts, or are application and services needed?
With Change Management, you should create a request prior to any modification. When the Request is approved and planned, this will create a Maintenance order for the Zabbix host / hostgroup that were selected.
Current limits under Zabbix

- Applications provide static grouping mostly for web scenarios
- Services under Zabbix are defined through a static-trigger relationship as well

- Tags are more dynamic, but...
  - Tags are defined at the trigger-level and accept MACROS
  - Although they can be updated through the API, this updates the TRIGGER definition
  - Since tags are added at the EVENT generation, it cannot be changed beforehand
  - EVENT tags are non-modifiable as of 5.0 (unless in the context of an action webhook)
  - What we can do - change severity, acknowledge or add messages to the EVENT
Licence compatibility check

- Zabbix is Free software
  - Licensed under GPL v2
  - Open source model

- iTOP is Free software
  - Licensed under affero GPL v3
  - Open core model

- Commercial software 3rd-parties
  - Closed source

Make sure those and your code are actually compatible!

We choose to release under aGPL
- Part of the interface is scripts and templates for Zabbix for maintainability and customization
- Part of the interface will be a paid iTop extension which could be distributed by iTop
Maybe you are thinking towards mixing the value of your CMDB data into Zabbix. Or you want to monitor real user experience. And fancy some cool dashboards.

Looking forward...

- There’s a lot of ITSM and CMDB software, commercial or open-sourced
- We see many customers inquiries about an likewise integration with their own breed of CMDB
- You may already have some of these features integrated with Zabbix
- We wanted to share our experience with the Zabbix community today

The situation

- We’ve seen that both feature-wise and technically this is not trivial
- Simplest features are usually opening incidents without context
- Advanced features require in-depth knowledge of Zabbix and the CMDB
- Make sure you have good understanding of the CMDB to bring the most value
- There are still some limitations with the API and datamodel

About the things we were NOT supposed to talk about

- I hope there has been not-so-much-gory details.
- There’s of course way more depth to ITIL than I presented
- I’m a big fan of Zabbix and xkcd. Thank you so much!
Thank you for listening
Time for questions!

+33 (0)1 71 11 36 15
contact@axelit.fr

www.axelit.fr