ZABBIX

SUMMIT ONLINE /2020

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

Eric Doan

Technical Director

AXEL IT

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

WHENEVER I LEARN A NEW SKILL I CONCOCT ELABORATE FANTASY SCENARIOS WHERE IT LETS ME SAVE THE DAY.
OH NO! THE KILLER MUST HAVE FOLLOWED HER ON VACATION!
BUT TO FIND THEM WE'D HAVE TO SEARCH THROUGH 200 MB OF EMAILS LOOKING FOR SOMETHING FORMATTED LIKE AN ADDRESS!
IT'S HOPELESS!

Based on a real webstory from xkcd.com

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

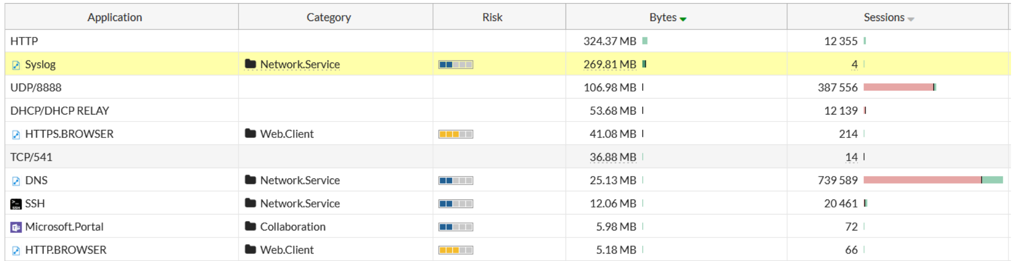
YOUR BOSS : « it's DOWN ! Fix it now ! »
*YOU : *Hope it's the network**

Starting with an integration for METRICS

Zabbix can monitor the network using SNMP

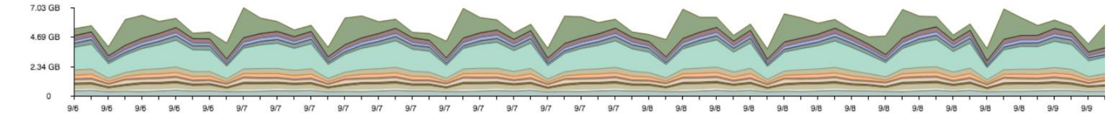
- Standard data such as bandwidth, errors, buffers
- Custom data for the hardware
- Events with SNMP notifications

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



Application	Category	Risk	Bytes	Sessions
HTTP			324.37 MB	12 355
Syslog	Network.Service		269.81 MB	4
UDP/8888			106.98 MB	387 556
DHCP/DHCP RELAY			53.68 MB	12 139
HTTPS.BROWSER	Web.Client		41.08 MB	214
TCP/541			36.88 MB	14
DNS	Network.Service		25.13 MB	739 589
SSH	Network.Service		12.06 MB	20 461
Microsoft.Portal	Collaboration		5.98 MB	72
HTTP.BROWSER	Web.Client		5.18 MB	66

Application Group Usage - Bandwidth

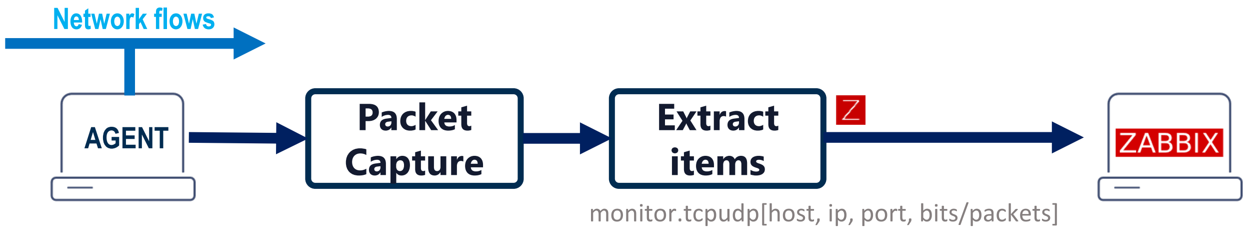


	Name ▲	Bandwidth(Min)	Bandwidth(Max)	Bandwidth(Avg)	Flows(Min)	Flows(Max)	Flows(Avg)	Clients(
■	Advertising	295.62 MB	421.46 MB	361.35 MB	198 K	301 K	254.2 K	1.9 K
■	Business Applications	5.39 MB	10.01 MB	8.17 MB	2.8 K	6.3 K	5 K	352
■	Certificate Validation	10.28 MB	18.64 MB	14.79 MB	8.4 K	14.8 K	11.8 K	638
□	Cloud Computing	60.04 MB	125.44 MB	104.37 MB	49.4 K	99.9 K	82.7 K	2.2 K
■	Cloud Storage	183.78 MB	473.55 MB	376.33 MB	80.3 K	210.4 K	170.7 K	3 K

But firewalls aren’t really monitoring-friendly with their data.
Plus, not every network port is actually a firewall port.

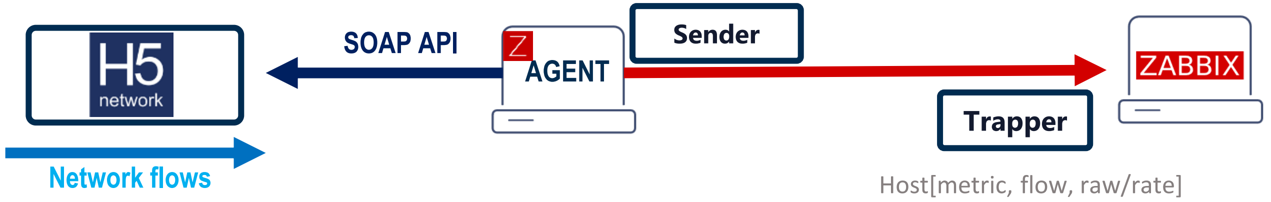
Starting with an integration for METRICS – How ?

A previous solution from Zabbix 1.x



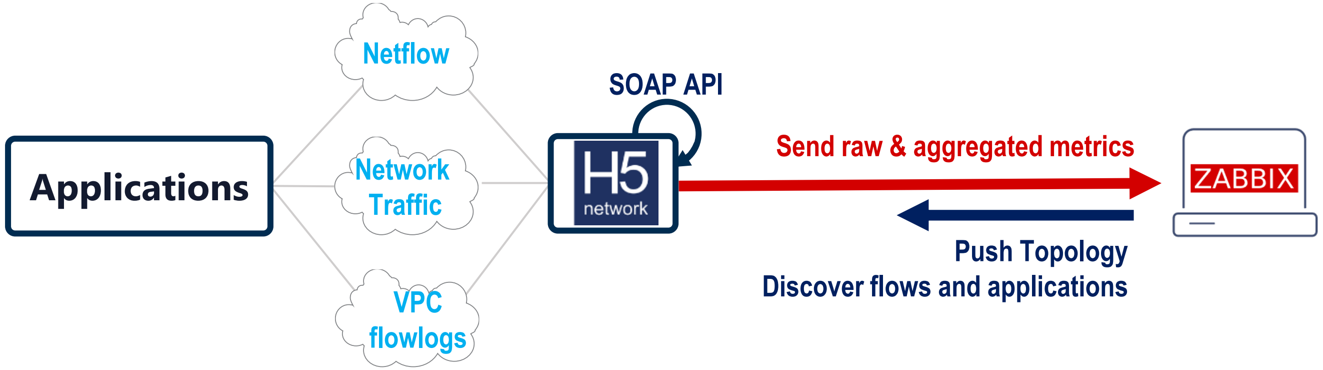
Zabbix API was in writing
Bound to agent interface and IP
Capture filters (libpcap)

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

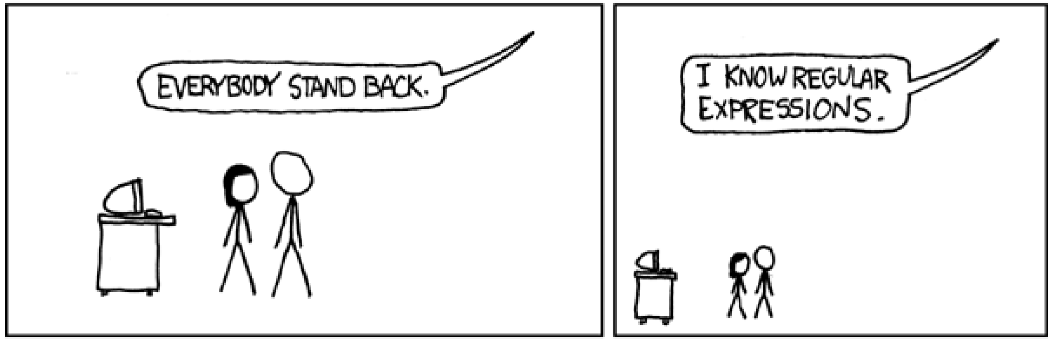
Needed to have H5 and Zabbix in touch for a deeper integration



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 ?

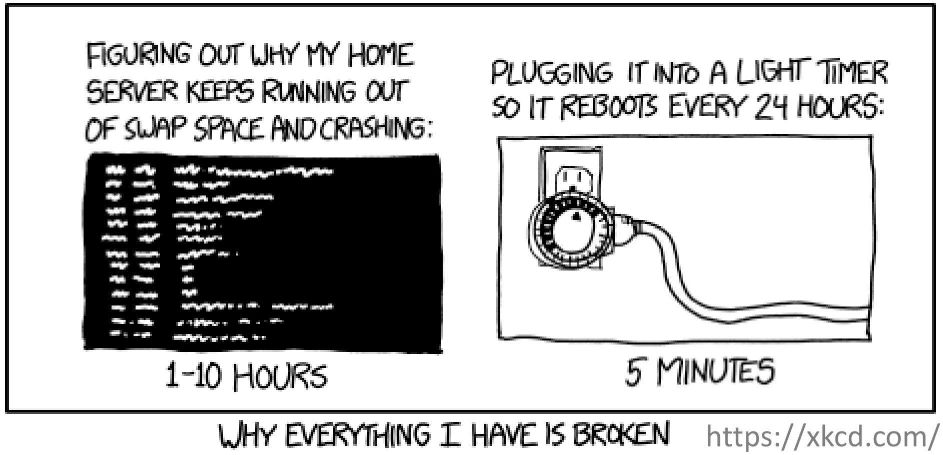


Find more : https://xkcd.com/208/

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 » ?


FIGURING OUT WHY MY HOME SERVER KEEPS RUNNING OUT OF SWAP SPACE AND CRASHING:
1-10 HOURS
PLUGGING IT INTO A LIGHT TIMER SO IT REBOOTS EVERY 24 HOURS:
5 MINUTES
WHY EVERYTHING I HAVE IS BROKEN

https://xkcd.com/1495/

Some efficiency questions arise when there are multiple ongoing incidents :

What should we fix first ?

What team should work on the issue ?

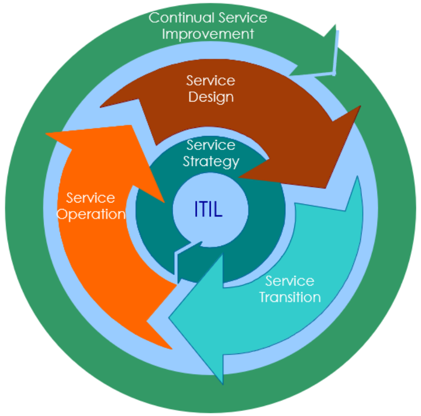
How do we make sure it does not happen again ?

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)



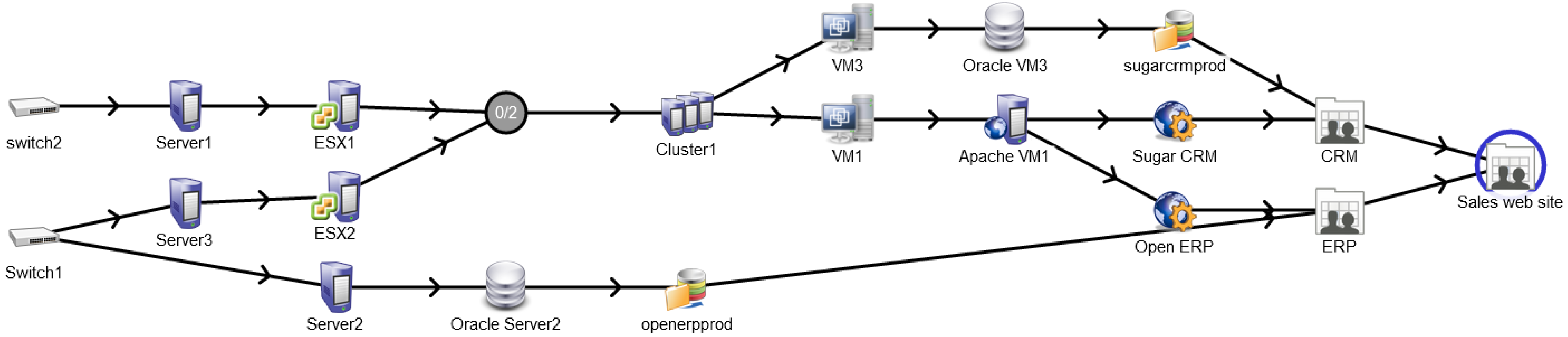
iTop We work with iTOP, an open-source ITSM software distributed by Combodo which is based on ITIL.

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

Configuration Management Database – Run Impact Analysis

A core function of the CMDB is to model **Dependency mapping** and **Impact Analysis**



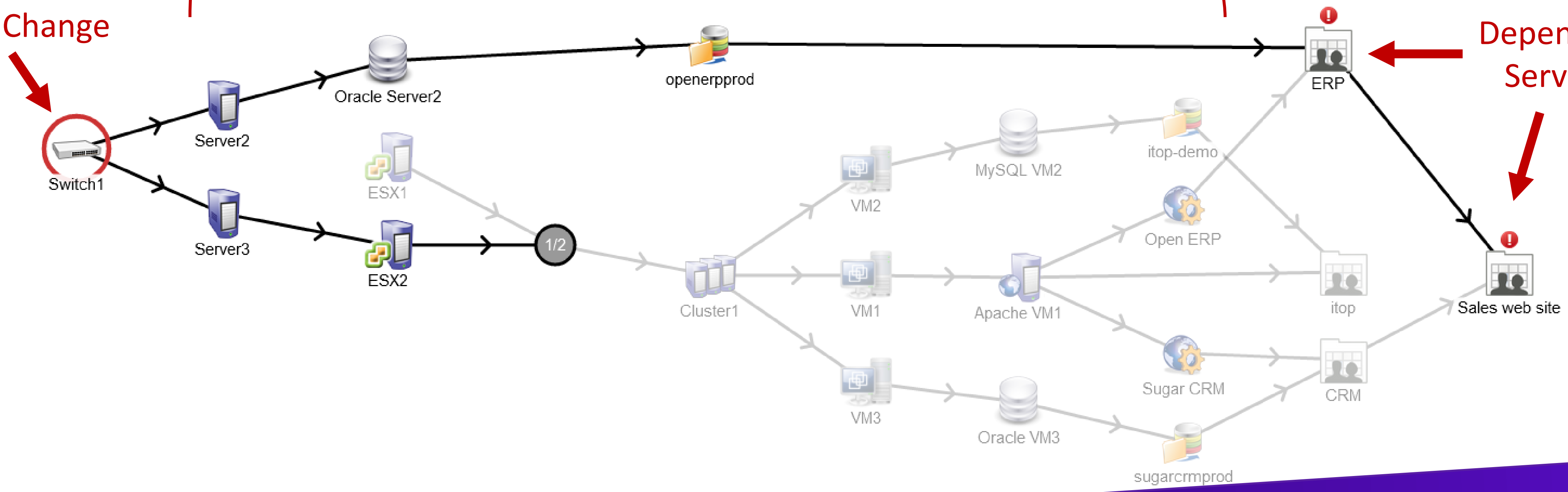
Configuration Management Database – Run Impact Analysis

Using Impact analysis we can predict the impact that a change will have to the availability of services

Impacted Assets

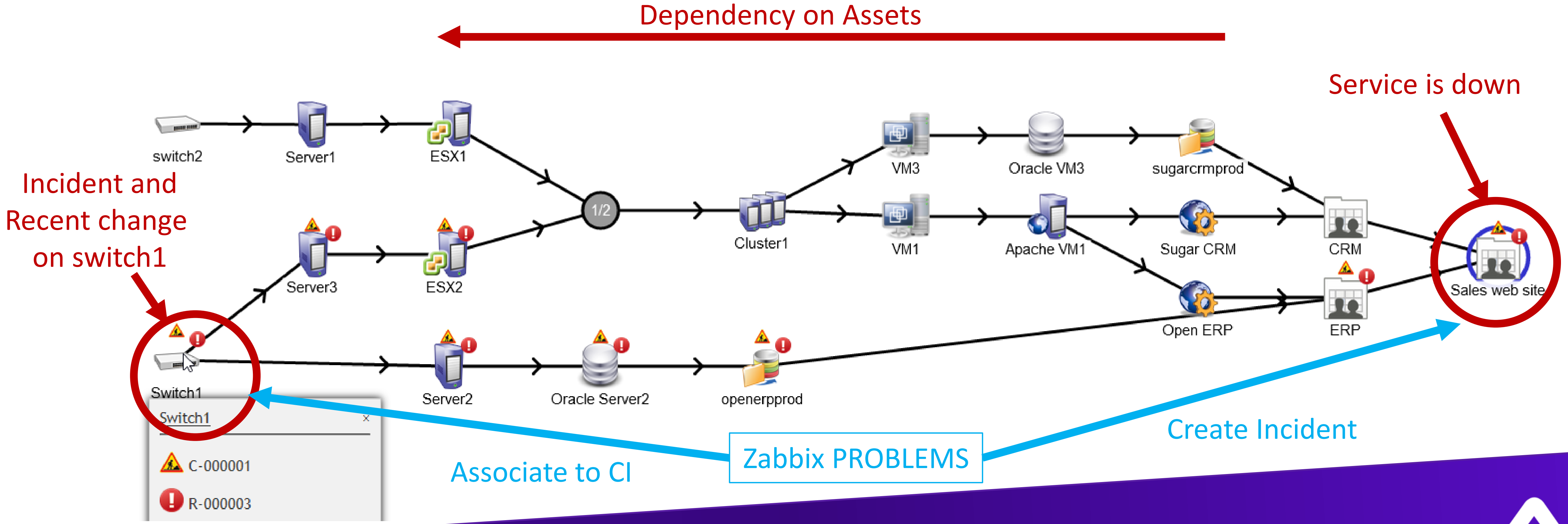
Planned Change

Dependent Services



Configuration Management Database – Run Impact Analysis

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



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

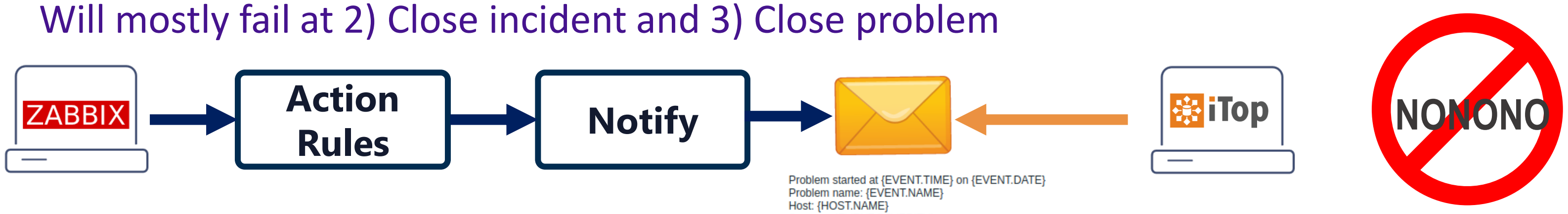
A. Synchronize comments and journal entries
B. Update incident when there’s new monitoring data
C. Calculate Incident severity
   - Declare on the correct CI in the service chain
   - Leverage Impact Analysis to find the service
   - Modify priority according to the service SLA
   - Trackback severity 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

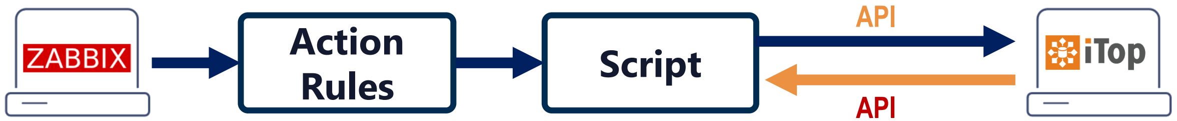
Quick and unreliable solution. Mail poppers WILL get clogged at some point.
Will mostly fail at 2) Close incident and 3) Close problem



```
Problem started at {EVENT.TIME} on {EVENT.DATE}
Problem name: {EVENT.NAME}
Host: {HOST.NAME}
Severity: {EVENT.SEVERITY}
Operational data: {EVENT.OPDATA}
Original problem ID: {EVENT.ID}
{TRIGGER.URL}
```

#2 – Use Actions Scripts - OK

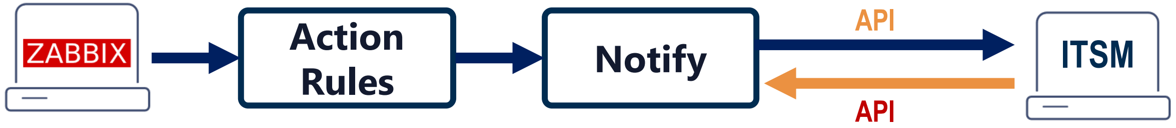
We can retrieve and store the incident #ID and add our own logic (&logs)
Which we choose to do through a set of PHP files for create/update/recover



main.php
create_ticket.php
curl_request.php (mandatory to send request to iTop)
parameters.php (contains all the parameters)
zbx_auth.php (mandatory for zabbix connection)
zbx_logout.php (mandatory to close zabbix connection)
zbx_update_trigger.php (used to update the trigger URI

#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



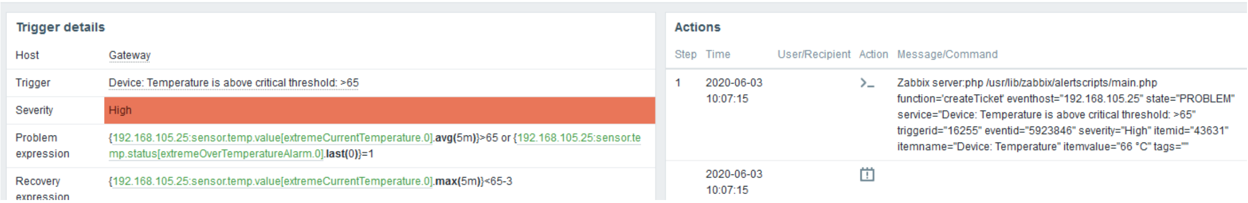
GOOD

Forward Problems with Action scripts

1) Zabbix Server generates Event → 2) Event data is pushed to iTOP → 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

Event details



Trigger details

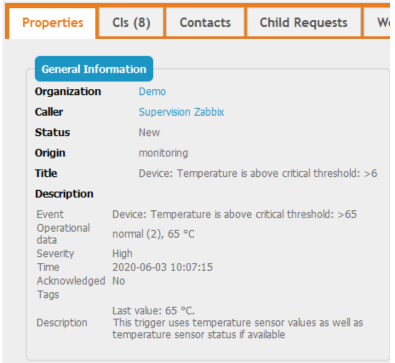
Host	Gateway
Trigger	Device: Temperature is above critical threshold: >65
Severity	High
Problem expression	{192.168.105.25:sensor.temp.value[extremeCurrentTemperature.0].avg(5m)}>65 or {192.168.105.25:sensor.temp.status[extremeOverTemperatureAlarm.0].last(0)}=1
Recovery expression	{192.168.105.25:sensor.temp.value[extremeCurrentTemperature.0].max(5m)}<65-3

Actions

Step	Time	User/Recipient	Action	Message/Command
1	2020-06-03 10:07:15		>_	Zabbix server:php /usr/lib/zabbix/alertscripts/main.php function='createTicket' eventhost="192.168.105.25" state="PROBLEM" service="Device: Temperature is above critical threshold: >65" triggerid="16255" eventid="5923846" severity="High" itemid="43631" itemname="Device: Temperature" itemvalue="66 °C" tags=""
	2020-06-03 10:07:15			

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

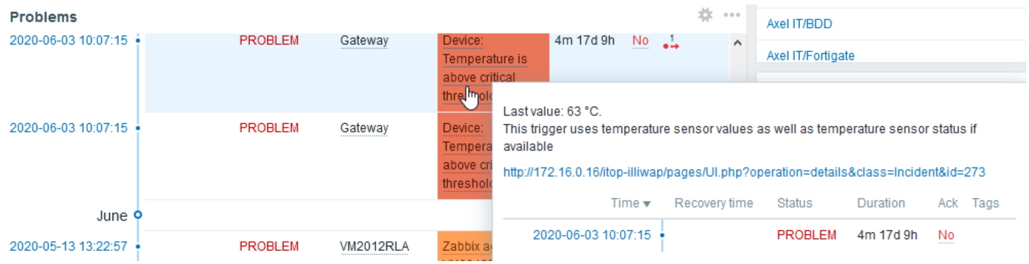
(New in v5, event menu from Webhook integrations)



General Information

Organization	Demo
Caller	Supervision Zabbix
Status	New
Origin	monitoring
Title	Device: Temperature is above critical threshold: >6
Description	

Event	Device: Temperature is above critical threshold: >65
Operational data	normal (2), 65 °C
Severity	High
Time	2020-06-03 10:07:15
Acknowledged	No
Tags	
Description	Last value: 65 °C. This trigger uses temperature sensor values as well as temperature sensor status if available



Problems

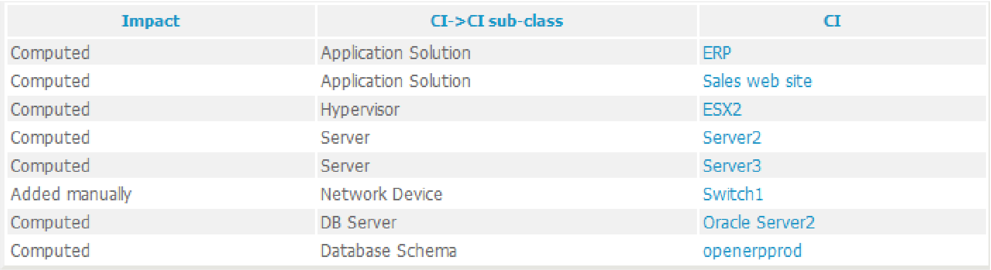
2020-06-03 10:07:15	PROBLEM	Gateway	Device: Temperature is above critical threshol	4m 17d 9h	No
2020-06-03 10:07:15	PROBLEM	Gateway	Device: Tempera above cri threshol		
June					
2020-05-13 13:22:57	PROBLEM	VM2012RLA	Zabbix a		

Last value: 63 °C.
This trigger uses temperature sensor values as well as temperature sensor status if available

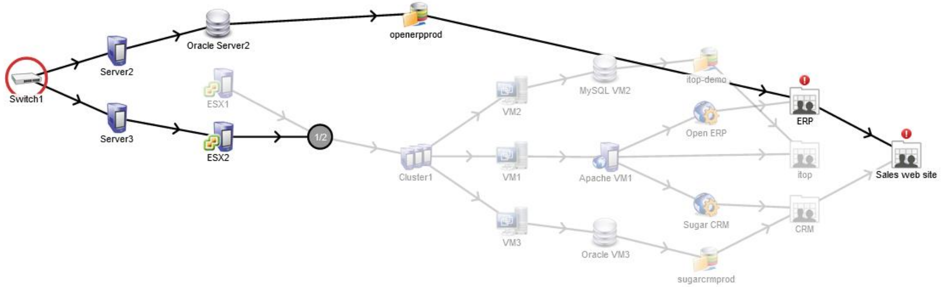
http://172.16.0.16/itop-illiwap/pages/UI.php?operation=details&class=Incident&id=273

Time ▾	Recovery time	Status	Duration	Ack	Tags
2020-06-03 10:07:15		PROBLEM	4m 17d 9h	No	

6) Autorun impact analysis on the CI, and attach services. Update Severity and trackback that value to the original EVENT



Impact	CI->CI sub-class	CI
Computed	Application Solution	ERP
Computed	Application Solution	Sales web site
Computed	Hypervisor	ESX2
Computed	Server	Server2
Computed	Server	Server3
Added manually	Network Device	Switch1
Computed	DB Server	Oracle Server2
Computed	Database Schema	openerpprod



Update and close problems

TO DO LiST

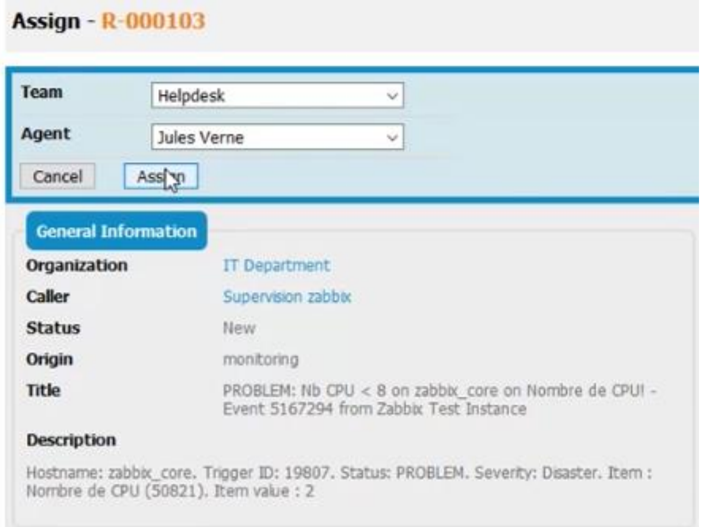
1. ~~Open an incident~~
2. Close an incident
3. Close a problem

A. Synchronize comments

~~B. Update Incidents~~

~~C. Change Problem severity~~

1) When the lifecycle of a incident ticket is changed → 2) We update the matching problem



Assign - R-000103

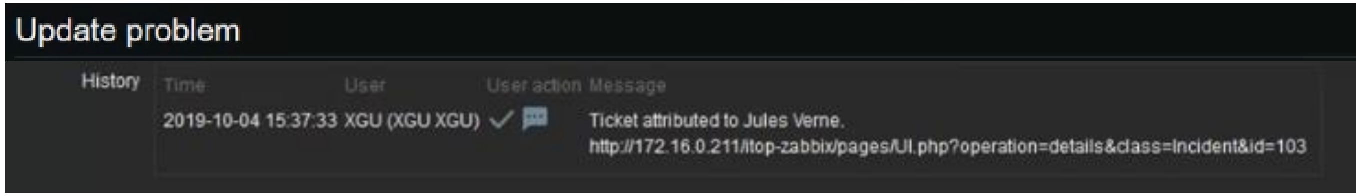
Team	Helpdesk
Agent	Jules Verne

Organization	IT Department
Caller	Supervision zabbix
Status	New
Origin	monitoring
Title	PROBLEM: Nb CPU < 8 on zabbix_core on Nombre de CPU! - Event 5167294 from Zabbix Test Instance

Description

Hostname: zabbix_core. Trigger ID: 19807. Status: PROBLEM. Severity: Disaster. Item : Nombre de CPU (50821). Item value : 2

Ticket assignation – Acknowledge and log

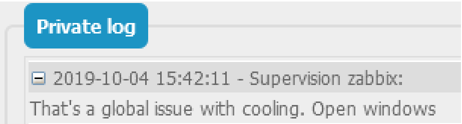


Update problem

History

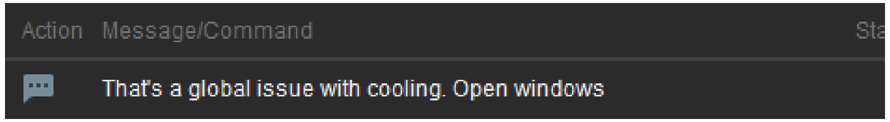
Time	User	User action	Message
2019-10-04 15:37:33	XGU (XGU XGU)	✓ 💬	Ticket attributed to Jules Verne. http://172.16.0.211/itop-zabbix/pages/UI.php?operation=details&class=Incident&id=103

Journal updates



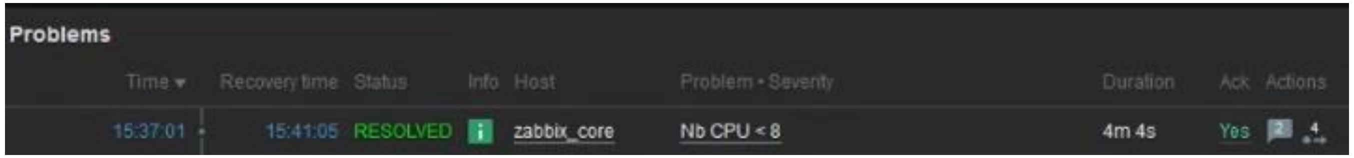
⊟ 2019-10-04 15:42:11 - Supervision zabbix:

That's a global issue with cooling. Open windows



Action	Message/Command	Sta
💬	That's a global issue with cooling. Open windows	

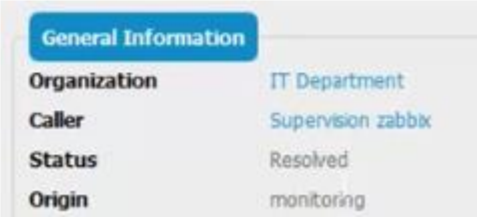
Ticket closed – Mark problem as resolved



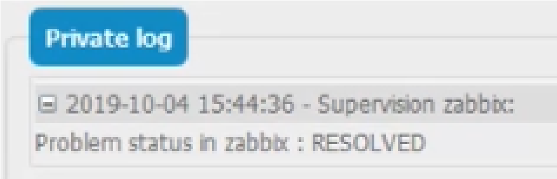
Problems

Time ▾	Recovery time	Status	Info	Host	Problem • Severity	Duration	Ack	Actions
15:37:01	15:41:05	RESOLVED	i	zabbix_core	Nb CPU < 8	4m 4s	Yes	2 4

Problem solved – Mark ticket as closed



Organization	IT Department
Caller	Supervision zabbix
Status	Resolved
Origin	monitoring



⊟ 2019-10-04 15:44:36 - Supervision zabbix:

Problem status in zabbix : RESOLVED

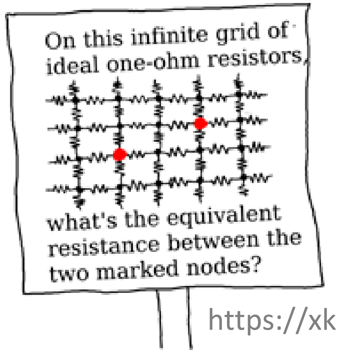
A problem with PROBLEMS

Zabbix PROBLEMS are issued :

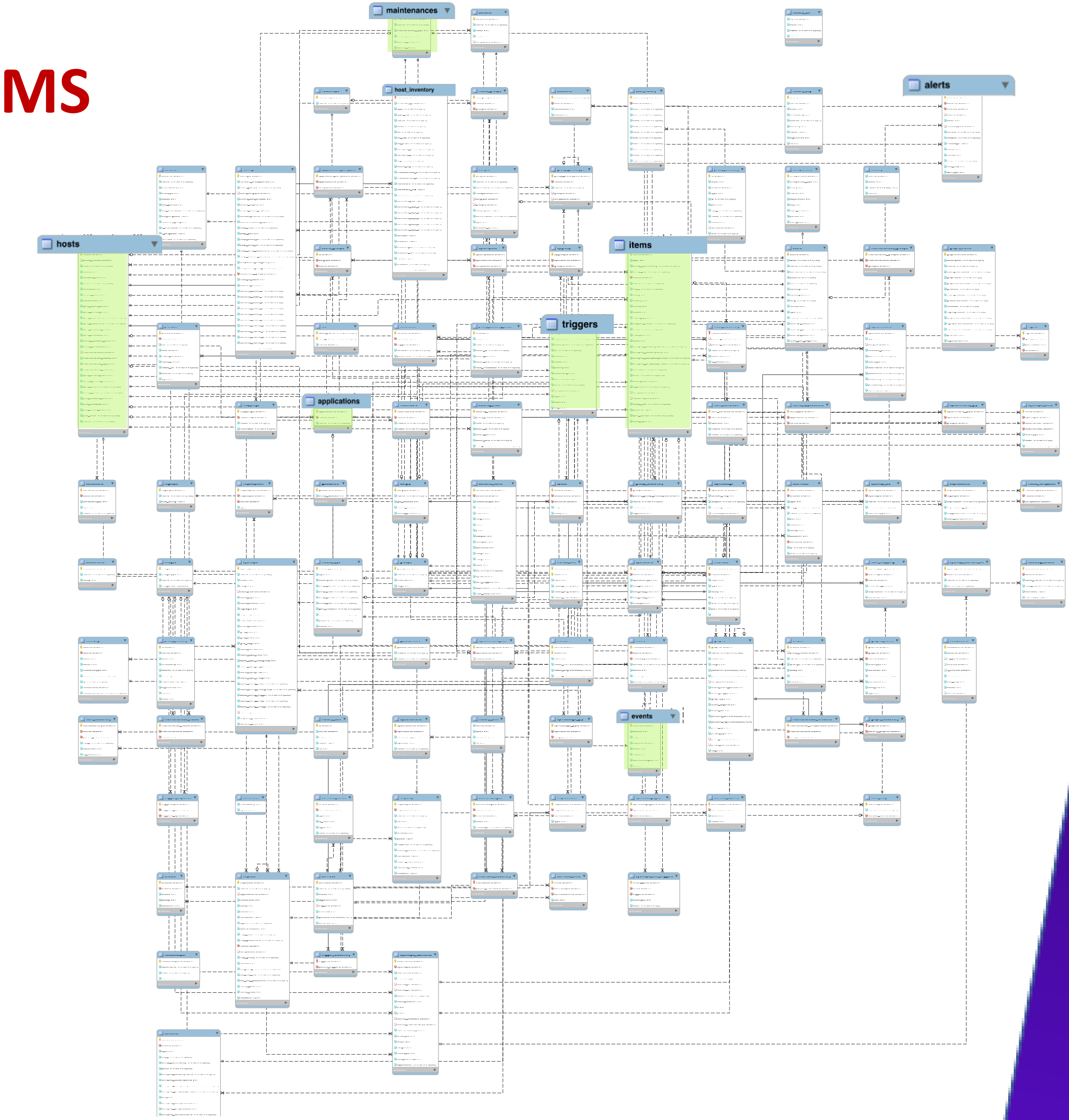
- As EVENTs
- Initiated by TRIGGERs
- From HOSTs
- Within the scope of ITEMs
- May concern APPLICATIONs

They are defined in TEMPLATEs

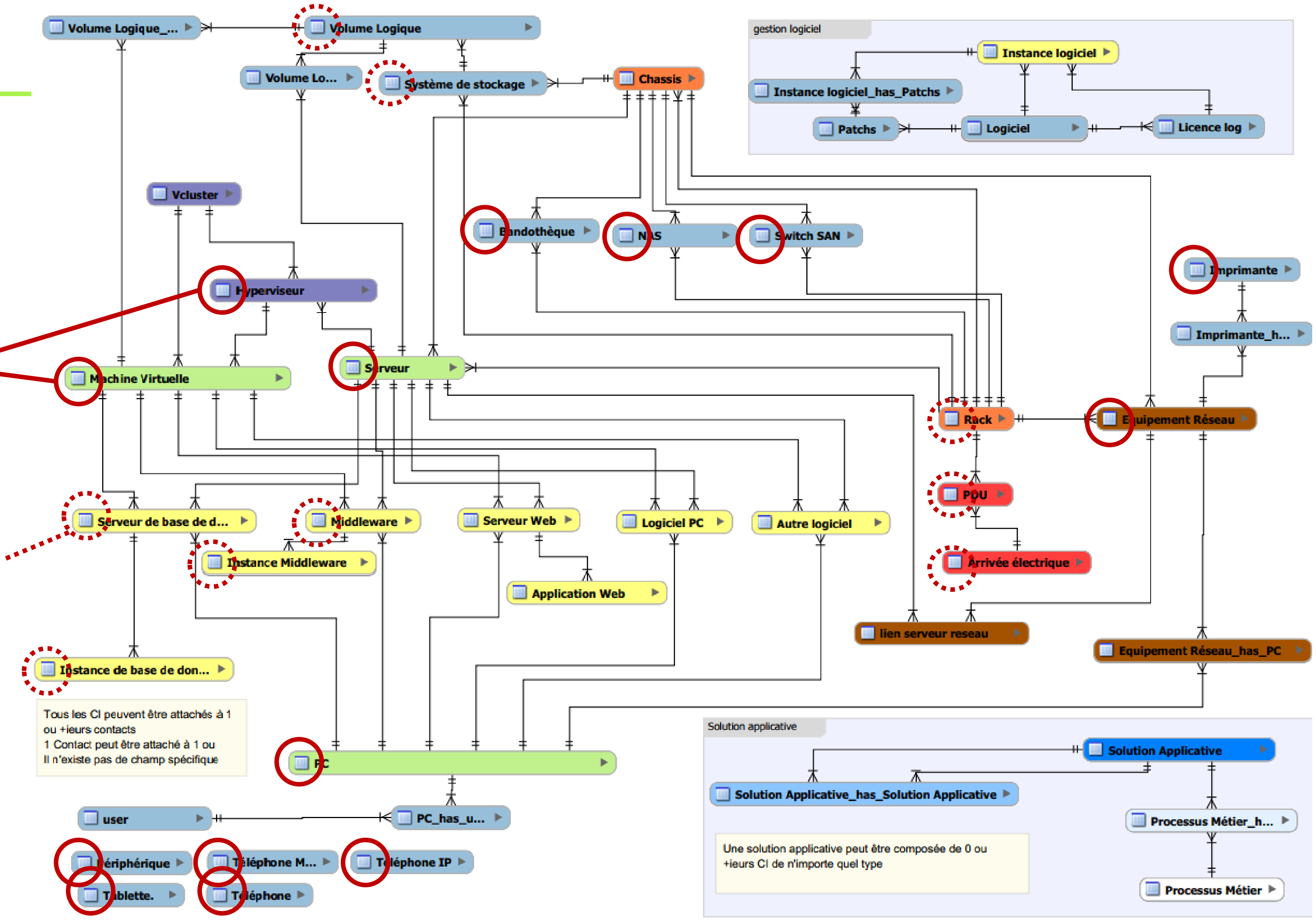
➔We need to map each of those to the CMDB Data model for efficient declaration and linkage


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

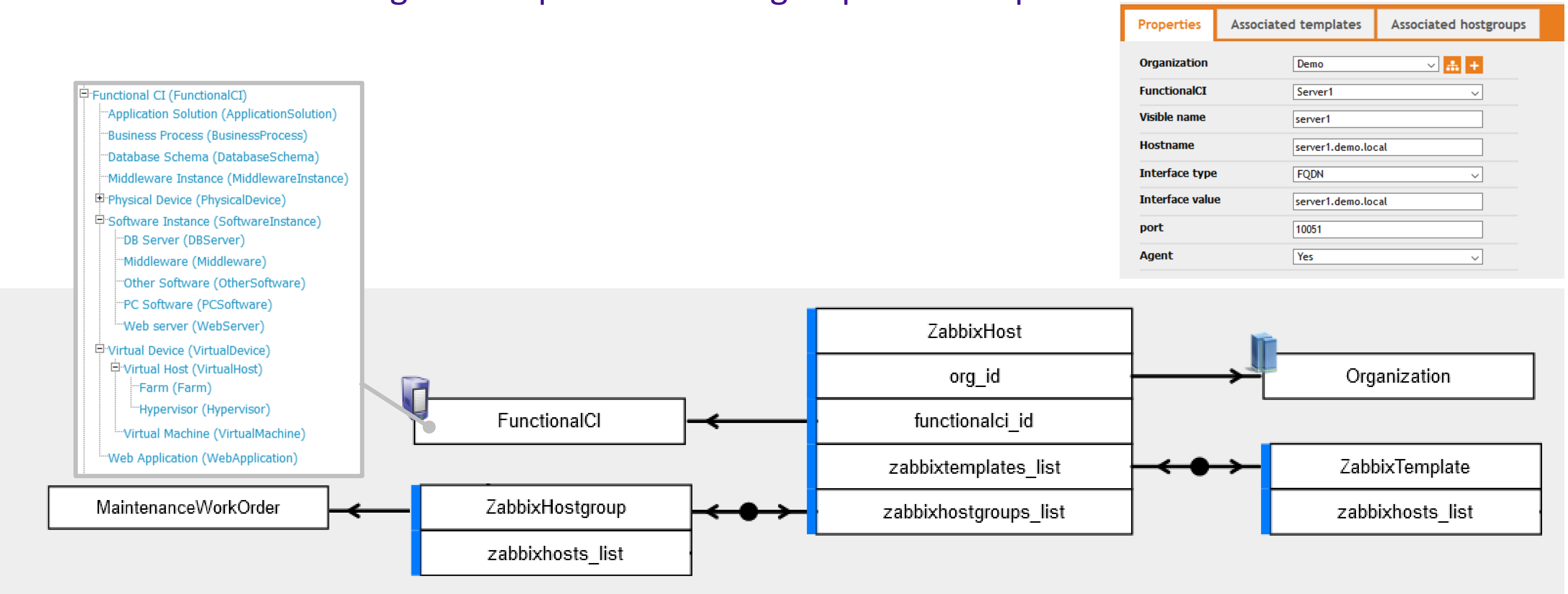
Zabbix
items or applications

Tous les CI peuvent être attachés à 1
ou +leurs contacts
1 Contact peut être attaché à 1 ou
Il n'existe pas de champ spécifique

Une solution applicative peut être composée de 0 ou
+leurs CI de n'importe quel type

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



Properties | Associated templates | Associated hostgroups

Organization	Demo
FunctionalCI	Server1
Visible name	server1
Hostname	server1.demo.local
Interface type	FQDN
Interface value	server1.demo.local
port	10051
Agent	Yes

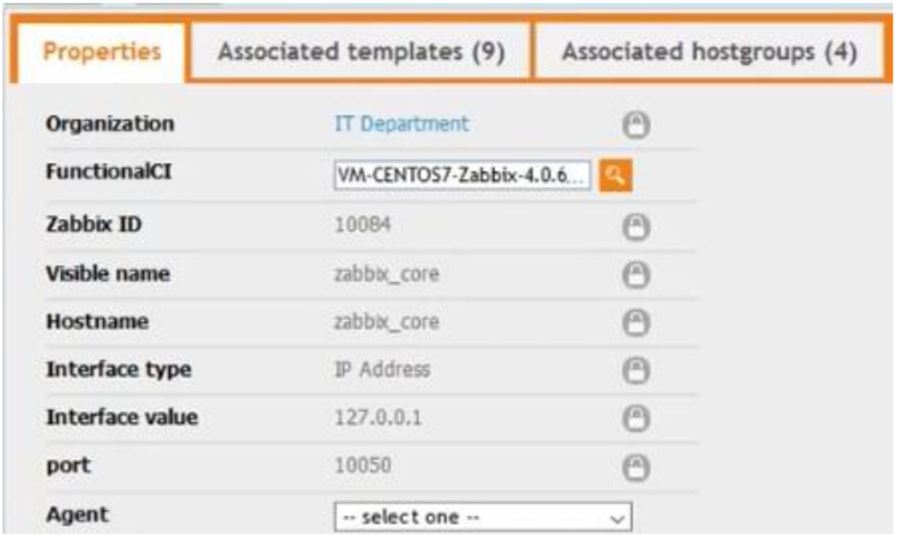
- Functional CI (FunctionalCI)
  - Application Solution (ApplicationSolution)
  - Business Process (BusinessProcess)
  - Database Schema (DatabaseSchema)
  - Middleware Instance (MiddlewareInstance)
  - Physical Device (PhysicalDevice)
  - Software Instance (SoftwareInstance)
    - DB Server (DBServer)
    - Middleware (Middleware)
    - Other Software (OtherSoftware)
    - PC Software (PCSoftware)
    - Web server (WebServer)
  - Virtual Device (VirtualDevice)
    - Virtual Host (VirtualHost)
      - Farm (Farm)
      - Hypervisor (Hypervisor)
    - Virtual Machine (VirtualMachine)
  - Web Application (WebApplication)

Zabbix configuration data in the CMDB

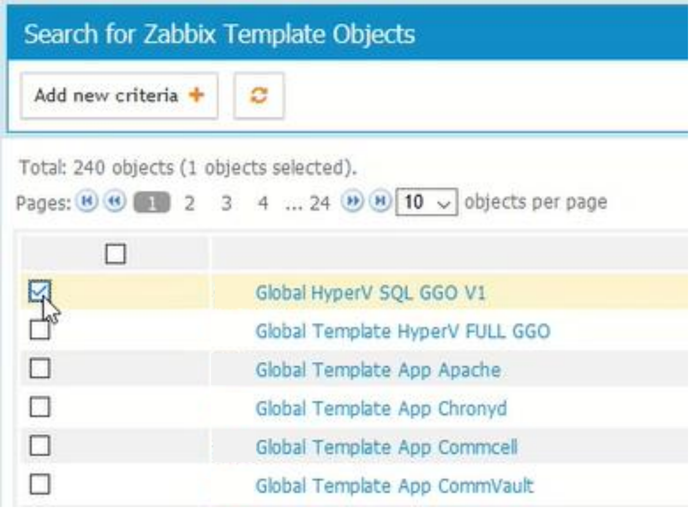
TO DO LiST

D. Add Monitoring configuration to the CMDB

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



Organization	IT Department
FunctionalCI	VM-CENTOS7-Zabbix-4.0.6...
Zabbix ID	10084
Visible name	zabbix_core
Hostname	zabbix_core
Interface type	IP Address
Interface value	127.0.0.1
port	10050
Agent	-- select one --

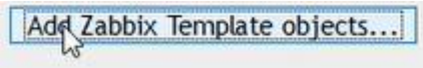


Total: 240 objects (1 objects selected).

Pages: 1 2 3 4 ... 24 10 objects per page

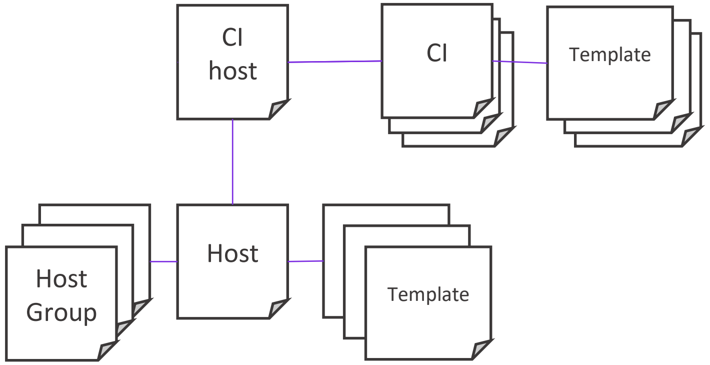
□	
☑	Global HyperV SQL GGO V1
□	Global Template HyperV FULL GGO
□	Global Template App Apache
□	Global Template App Chronyd
□	Global Template App Commcell
□	Global Template App CommVault

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



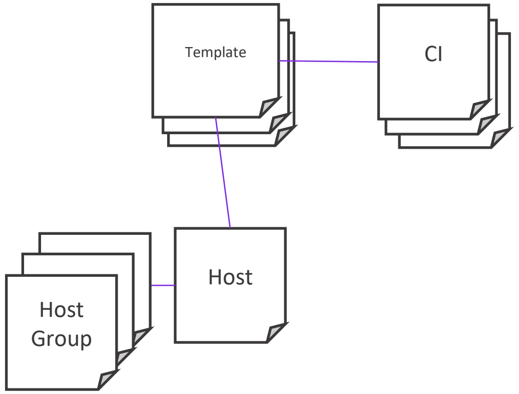
Synchronization Model

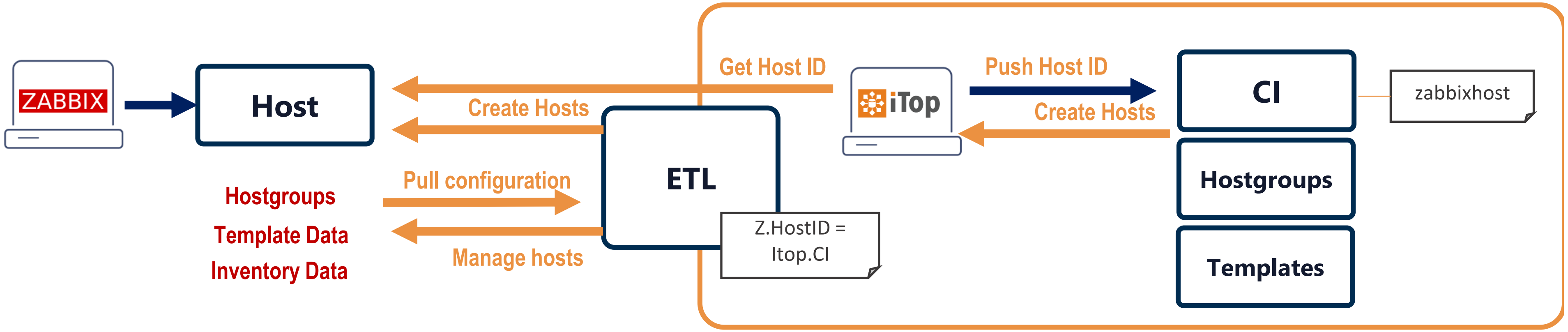
Model 1 : Only hosts



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

Model 2 : Hosts and Services

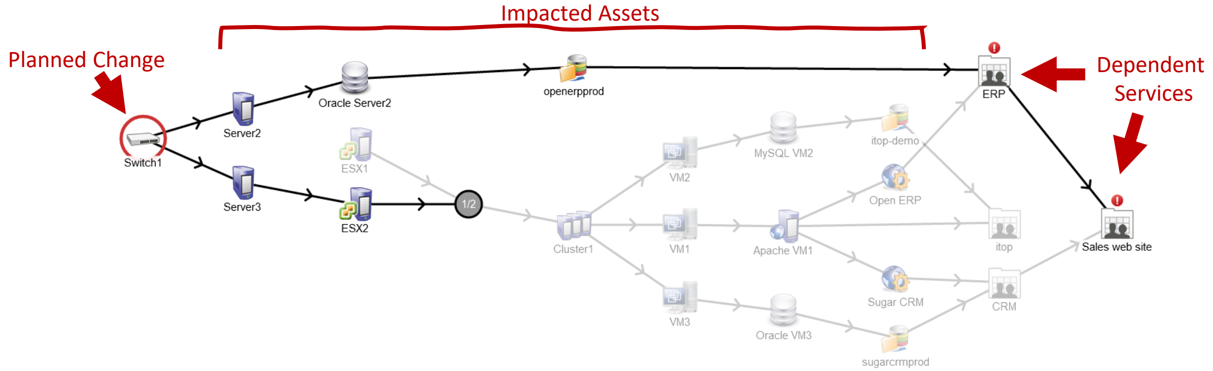




Beyond Incident and Configuration Management

TO DO LiST

E. Automate Maintenance Period & Change tracking

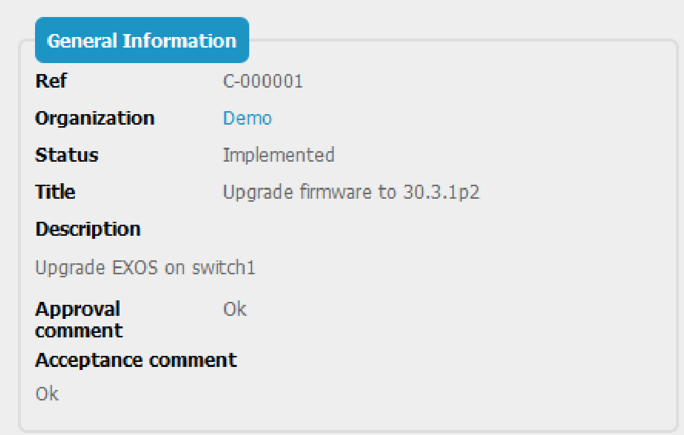


Planned Change

Impacted Assets

Dependent Services

- 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



General Information

Ref	C-000001
Organization	Demo
Status	Implemented
Title	Upgrade firmware to 30.3.1p2

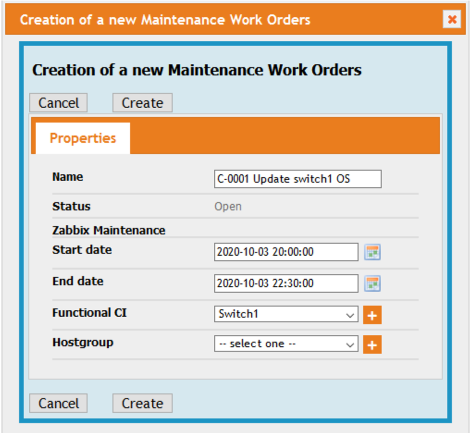
Description

Upgrade EXOS on switch1

Approval comment	Ok

Acceptance comment

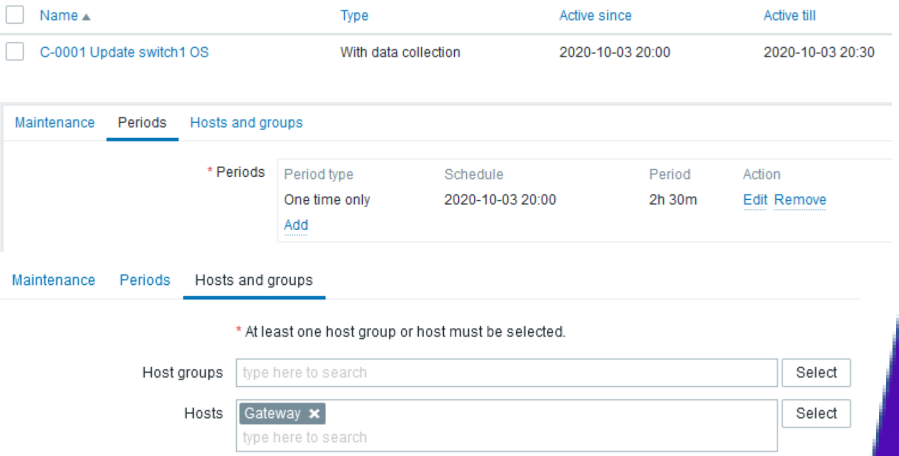
Ok



Creation of a new Maintenance Work Orders

Creation of a new Maintenance Work Orders

Name	C-0001 Update switch1 OS
Status	Open
Zabbix Maintenance	
Start date	2020-10-03 20:00:00
End date	2020-10-03 22:30:00
Functional CI	Switch1
Hostgroup	-- select one --



☐	Name ▲	Type	Active since	Active till
☐	C-0001 Update switch1 OS	With data collection	2020-10-03 20:00	2020-10-03 20:30

* Periods

Period type	Schedule	Period	Action
One time only	2020-10-03 20:00	2h 30m	Edit Remove
Add			

* At least one host group or host must be selected.

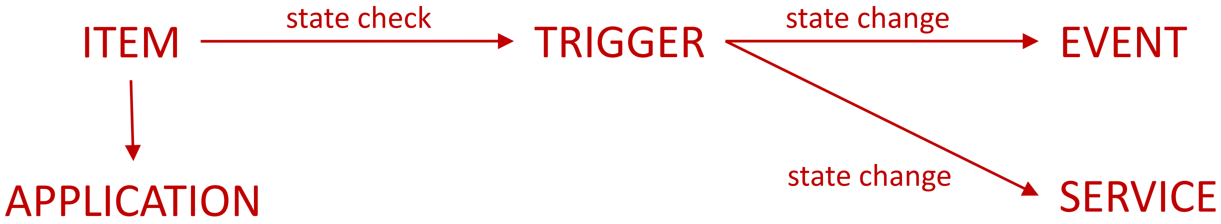
Host groups: type here to search — Select

Hosts: Gateway ✖ type here to search — Select

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



ITEM

state check

TRIGGER

state change

EVENT

APPLICATION

state change

SERVICE

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

Endnotes

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