Trouble Ticket Integration with Zabbix in Large Environment
Presentation

Alain Ganuchaud

Cool Monitoring

http://www.coolmonitoring.fr
alain@coolmonitoring.fr
Zabbix Database Monitoring

ORACLE MSSQL MYSQL DB2 & POSTGRESQL
Version 7.0

Zabbix database Model

Zabbix Database Model with main tables used for Reports developments. To be read with Workbench.

It contains comments on main numeric fields contained in Zabbix database tables.
Summary

1. Introduction
2. Issues
3. Plugin Architecture
4. External Specifications
5. Technical Details
Part 1
Introduction

-> What are we talking about ?
-> Large Environment ?
-> Trouble Ticket ?
What are we talking about?

Zabbix TroubleTicket Connexion

→ Two ways connexion
→ APIs
→ Connector Database (Zabbix TroubleTicket Link)

Large Environment
→ 1000 tickets per day
Trouble Ticket?

- Lists of issues (Most of the time: Source = mail or phone)
- Manage issues (Most of the time through HelpDesk)

→ ServiceNow is a SaaS Trouble Ticketing System widely used in Large environments
What is a Large Environment?

- More than 14,000 servers, 1 million items
- Some servers with over 10,000 items
- Some servers with over 10,000 triggers
- More than 100 Zabbix administrators developing Application Templates
Part 2
Issues
The Problem

Large Environments rely on TroubleTicket tool and HelpDesk for managing IT issues. Bridging Zabbix with over 5000 servers and HelpDesk manually is a painful and impossible project.
Case Study

Objective:
Migrate IBM Tivoli monitoring 6.2 to an open source monitoring tool.

Requirements:
More flexibility (upgrade, administration), monitored all servers and devices, create automatic and manual ticket in ServiceSnow.

Outcome:
Reduced administrative operations, low cost, Zabbix support pricings, Zabbix community.
About Swiss Life

The Swiss Life Group is a European leader in pensions and financial solutions. The Swiss Life company offers individuals and comprehensive pension consultations via its own agents and distribution partners.
Swiss Life Group
Turnover: €18.9 billion
Managed assets: €223 billion
7600 employees around the world

Swiss Life France
Turnover: €4.24 billion
Managed assets: €26 billion
1 224 000 clients
2188 employees

IT System Department
220 employees
1500 Servers (Windows / Linux)
97% Virtual servers (VMWare)
Cisco UCS / VNX – EMC (250TB)
Part 3
Plugin Architecture
Plugin Architecture
Plugin Architecture

Plugin Architecture Diagram:
- **Trigger AUTO**
- **Event AUTO**
- **Zabbix Action AUTO**
- **Trigger MANU**
- **Event MANU**
- **Zabbix Action MANU**
- **Connector**
  - **connector.php**
- **SNOW**
- **Galera Cluster**
  - **connector Database**

Diagram showing connectivity and components of the plugin architecture.
Part 4
External Specifications
Some of the Functionalities

→ Opens automatically a ServiceNow Ticket via Snow APIs
  Full Automatic (based on Trigger name TR--A)
  Manual (TR--M), needs acknowledge from operator

→ Fill in automatically Snow fields with Zabbix macros
  Caller, Environment, CI, Application, Server, Team, Category,
  Subcategory, Dates,…

→ Correlate Zabbix events automatically with Snow tickets
  (same trigger source)

→ Correlate Zabbix events manually with Snow tickets
  (different triggers sources)

→ Sends back Correlation confirmations to Operators

→ Monitor Snow tickets status and update Zabbix via APIs
  when ticket is closed or resolved

→ Others: http proxy, debug, logs, …
Triggers Nomenclature

TR--A/M--PRD/HPR--{$SERVICEXXX}--{$CIXXX}--Free Description of Trigger

| Auto/Manu |
| Prod or Non Prod |
| Service (~ Application Name) |
| CI (could be Server or Oracle DB, …) |
| Free Description |

Nota Bene: Some détails come from Host Inventory
Zabbix-SNOW Connector
Close a ticket (daemon)

1. Read Database
   - Read tickets with status <> Close: GOTO 2
   - Read tickets with status = Close: GOTO 1
   - Log Operation

2. Get SNOW
   - Read Snow ticket infos
   - Get SnowID & date_close: GOTO 3
   - Log operation

3. Update Database
   - Update Database for a specific SnowID (New Status = Close): GOTO 4
   - Log Operation

4. Zabbix
   - Update Event Acknowledge with "SnowID close at date_close": GOTO 1
   - Log Operation
Part 5
Technical Details
Automatic Tickets

CONFIGURATION OF ACTIONS

<table>
<thead>
<tr>
<th>Action</th>
<th>Conditions</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>TRIGGER AUTO -&gt; Send Alert to connector</td>
<td></td>
</tr>
<tr>
<td>Default subject</td>
<td>{TRIGGER.STATUS}: {TRIGGER.NAME}</td>
<td></td>
</tr>
</tbody>
</table>
| Default message | Trigger: \{TRIGGER.NAME\}  
Trigger status: \{TRIGGER.STATUS\}  
Trigger severity: \{TRIGGER.SEVERITY\}  
Trigger URL: \{TRIGGER.URL\}  
Item values:  
1. \{ITEM.NAME1\} {{HOST.NAME1}:\{ITEM.KEY1\}}: |
| Recovery message | No |
| Enabled | Yes |

Conditions

<table>
<thead>
<tr>
<th>Label</th>
<th>Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>(A)</td>
<td>Maintenance status not in maintenance</td>
<td>Remove</td>
</tr>
<tr>
<td>(B)</td>
<td>Trigger value = PROBLEM</td>
<td>Remove</td>
</tr>
<tr>
<td>(C)</td>
<td>Trigger name like TR--A--</td>
<td>Remove</td>
</tr>
</tbody>
</table>

New condition

<table>
<thead>
<tr>
<th>Trigger name</th>
<th>like</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td></td>
</tr>
</tbody>
</table>
Automatic Tickets

CONFIGURATION OF ACTIONS

<table>
<thead>
<tr>
<th>Action</th>
<th>Conditions</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Default operation step duration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3600 (minimum 60 seconds)</td>
</tr>
<tr>
<td>Action operations</td>
<td></td>
<td>Run remote commands on current host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Start in</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Immediately</td>
</tr>
</tbody>
</table>

Operation details

<table>
<thead>
<tr>
<th>Step</th>
<th>From</th>
<th>To</th>
<th>Step duration</th>
<th>Operation type</th>
<th>Target list</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>60 (minimum 60 seconds, 0 - use current)</td>
<td>Remote command</td>
<td>Current host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td>New</td>
</tr>
</tbody>
</table>

Type

- Custom script

Execute on

- Zabbix agent
- Zabbix server

Commands

```
/etc/zabbix/connectorSNOW/connector.php AUTO
"{DATE}" "{TIME}" "{HOST.HOST}" "{EVENT.DATE}"
"{EVENT.TIME}" "{EVENT.ID}" "{EVENT.ACK.STATUS}"
"{EVENT.STATUS}" "{ITEM.ID}" "{ITEM.VALUE}"
"{TRIGGER.ID}" "{TRIGGER.NAME}"
"{TRIGGER.SEVERITY}" "{TRIGGER.DESCRIPTION}"```
<table>
<thead>
<tr>
<th>Number</th>
<th>IN0127340</th>
</tr>
</thead>
<tbody>
<tr>
<td>Caller</td>
<td>supervision zabbix (zabt)</td>
</tr>
<tr>
<td>Asset Tag</td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td></td>
</tr>
<tr>
<td>Environment</td>
<td>Test</td>
</tr>
<tr>
<td>Configuration Item</td>
<td>linux627</td>
</tr>
<tr>
<td>Application</td>
<td>Test Appli</td>
</tr>
<tr>
<td>Service</td>
<td>Test Service</td>
</tr>
<tr>
<td>Impact</td>
<td>1 - High</td>
</tr>
<tr>
<td>Urgency</td>
<td></td>
</tr>
<tr>
<td>Priority</td>
<td>3 - Moderate</td>
</tr>
<tr>
<td>Short description</td>
<td>Test Trigger for Snow Auto</td>
</tr>
<tr>
<td>Status</td>
<td>Assigned</td>
</tr>
<tr>
<td>Opened by</td>
<td></td>
</tr>
<tr>
<td>Assignment group</td>
<td>sup team</td>
</tr>
<tr>
<td>Assigned to</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Supervision</td>
</tr>
<tr>
<td>Subcategory</td>
<td>Alerte</td>
</tr>
<tr>
<td>Composant</td>
<td>-- None --</td>
</tr>
<tr>
<td>Contact type</td>
<td>Phone</td>
</tr>
<tr>
<td>Created</td>
<td>2016-08-20 10:04:30</td>
</tr>
<tr>
<td>Opened</td>
<td>2016-08-20 10:04:30</td>
</tr>
<tr>
<td>SLA resolution due date</td>
<td></td>
</tr>
</tbody>
</table>
Automatic Tickets

Date_Alerte: 2016.08.20 10:04:30
Criticité_Alerte: P2
Warning_Alerte: TR-HPR- Test Trigger for Snow
Valeur_de_Déclenchement: 2073642933

### Automatic Tickets

<table>
<thead>
<tr>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ticket IN0127341 opened automatically by Zabbix on 2016-08-20 10:32:29 CEST</td>
<td>Aug 20th, 2016 10:32:29 AM</td>
</tr>
<tr>
<td>Ticket IN0127341 closed in SNOW on 2016-08-20 10:37:04 CEST with code Solved (Permanently) and notes : Close notes from Service Now.</td>
<td>Aug 20th, 2016 10:37:14 AM</td>
</tr>
</tbody>
</table>
# Manual Tickets

## Configuration of Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Conditions</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>TRIGGER_MANU -&gt; Send Alert to connector if acknowledged</td>
<td></td>
</tr>
<tr>
<td>Default subject</td>
<td>(TRIGGER.STATUS): (TRIGGER.NAME)</td>
<td></td>
</tr>
</tbody>
</table>
| Default message | Trigger: (TRIGGER.NAME)  
Trigger status: (TRIGGER.STATUS)  
Trigger severity: (TRIGGER.SEVERITY)  
Trigger URL: (TRIGGER.URL) |   |
| Item values | 1. (ITEM.NAME1): (HOST.NAME1): (ITEM.KEY1): |   |
| Recovery message |   |   |
| Enabled | ✓ |   |

## More Configuration

- **Type of calculation**: AND / OR  
  - (A) and (B)
- **Conditions**
  - (A) Maintenance status not in **maintenance**  
  - (B) Trigger name like **TR---M---**
- **New condition**
  - Trigger name: like  
  - Add: **Remove**
Manual Tickets : noticket

<table>
<thead>
<tr>
<th>Admin (Zabbix Administrator)</th>
<th>Aug 20th, 2016 10:04:07 AM</th>
</tr>
</thead>
<tbody>
<tr>
<td>noticket</td>
<td></td>
</tr>
<tr>
<td>api_rw (api_rw api_rw)</td>
<td>Aug 20th, 2016 10:04:33 AM</td>
</tr>
</tbody>
</table>

Confirmation : This event will not be linked to any SNOW ticket.
**Manual Tickets : link to ticket**

![Image of Zabbix GUI showing manual ticket management](image_url)

**Alarm Acknowledges:**

<table>
<thead>
<tr>
<th>User</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin (Zabbix Administrator)</td>
<td>Aug 20th, 2016 10:40:54 AM</td>
</tr>
<tr>
<td>IN0127341</td>
<td></td>
</tr>
<tr>
<td>api_rw (api_rw api_rw)</td>
<td>Aug 20th, 2016 10:41:36 AM</td>
</tr>
</tbody>
</table>

*Confirmation*: This event is linked to Ticket IN0127341

**Add comment by "Admin (Zabbix Administrator)"**

Message

[Save and return] [Save] [Cancel]
New event (1124) Zabbix on 2016.08.20 at 10:21:24 for this ticket

Assignment group: DOI Prod Pilotage
Caller: supervision zabbix (zabbsup)
Category: [Empty]
Configuration Item: [Empty]
Contact type: Phone
Description:
- Date_Alerte: 2016.08.20 10:04:30
- Criticite_Alerte: P2
- Warning_Alerte: TR-HPR- Test Trigger for Snow Auto
- Valeur_de_Declenchement: 2073642933
- Impact: 2 - Medium
- Location: [Empty]
- Opened by: [Empty]
- Priority: 3 - Moderate
- Short description: Test Trigger for Snow Auto
- Status: Assigned
- Subcategory: Alert
- Urgency: 2 - Medium
- Service: Serveur distribué
- Default JCL: false
- Environment: Test
Connector Database

```
CREATE TABLE zabbix_events
(
    host VARCHAR(64),
    triggerid BIGINT(20),
    eventid BIGINT(20),
    snow_status VARCHAR(64),
    itemid BIGINT(20),
    item_value TEXT,
    trigger_name VARCHAR(255),
    trigger_description TEXT,
    event_status VARCHAR(20),
    event_date DATE,
    event_time TIME,
    event_ack_status VARCHAR(20),
    alert_date DATE,
    alert_time TIME
)

CREATE TABLE snow_tickets
(
    opened_at VARCHAR(80),
    closed_at VARCHAR(80),
    zabbix_eventid BIGINT(20),
    sys_id VARCHAR(200),
    number VARCHAR(100)
)

```

Indexes:

```
snow_tickets
    zabbix_eventid
<references>
zabbix_events
    eventid
on update: CASCADE
on delete: CASCADE
```
## Connector Database

```sql
mysql> select * from zabbix_events;
```

<table>
<thead>
<tr>
<th>host</th>
<th>triggerid</th>
<th>eventid</th>
<th>snow_status</th>
<th>itemid</th>
<th>item_value</th>
<th>trigger_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>linux627</td>
<td>15368</td>
<td>1121</td>
<td>ticket_open</td>
<td>28091</td>
<td>2073642933</td>
<td>TR--A--HPR--Serveur distribue-linux627--</td>
</tr>
<tr>
<td>2016-08-20</td>
<td>10:04:24</td>
<td>No</td>
<td>2016-08-20</td>
<td>10:04:30</td>
<td>10266</td>
<td></td>
</tr>
<tr>
<td>linux627</td>
<td>15369</td>
<td>1119</td>
<td>ticket_not_allowed</td>
<td>28093</td>
<td>2073642933</td>
<td>TR--M--PRD--Serveur distribue-linux627--</td>
</tr>
<tr>
<td>TR--M-- Test Trigger for Snow Manu</td>
<td>PROBLEM</td>
<td>2016-08-20</td>
<td>10:00:24</td>
<td>Yes</td>
<td>2016-08-20</td>
<td>10:04:33</td>
</tr>
<tr>
<td>linux627</td>
<td>15368</td>
<td>1124</td>
<td>ticket_updated</td>
<td>28091</td>
<td>2125759221</td>
<td>TR--A--HPR--Serveur distribue-linux627--</td>
</tr>
<tr>
<td>2016-08-20</td>
<td>10:21:24</td>
<td>No</td>
<td>2016-08-20</td>
<td>10:21:28</td>
<td>10266</td>
<td></td>
</tr>
<tr>
<td>linux627</td>
<td>15368</td>
<td>1126</td>
<td>ticket_open</td>
<td>28091</td>
<td>1262714989</td>
<td>TR--A--HPR--Serveur distribue-linux627--</td>
</tr>
<tr>
<td>2016-08-20</td>
<td>10:32:24</td>
<td>No</td>
<td>2016-08-20</td>
<td>10:32:28</td>
<td>10266</td>
<td></td>
</tr>
<tr>
<td>linux627</td>
<td>15369</td>
<td>1128</td>
<td>ticket_updated</td>
<td>28093</td>
<td>3316395057</td>
<td>TR--M--PRD--Serveur distribue-linux627--</td>
</tr>
<tr>
<td>TR--M-- Test Trigger for Snow Manu</td>
<td>PROBLEM</td>
<td>2016-08-20</td>
<td>10:40:24</td>
<td>Yes</td>
<td>2016-08-20</td>
<td>10:41:34</td>
</tr>
</tbody>
</table>

5 rows in set (0.00 sec)

```sql
mysql> select * from snow_tickets;
```

<table>
<thead>
<tr>
<th>opened_at</th>
<th>closed_at</th>
<th>zabbix_eventid</th>
<th>sys_id</th>
<th>number</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-08-20 10:04:30 CEST</td>
<td>2016-08-20 10:28:02 CEST</td>
<td>1121</td>
<td>e2c60c263799e200489af01643990e40</td>
<td>IN0127340</td>
</tr>
<tr>
<td>2016-08-20 10:32:29 CEST</td>
<td>2016-08-20 10:37:04 CEST</td>
<td>1126</td>
<td>5c3dc42237d9e200489af01643990e90</td>
<td>IN0127341</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1128</td>
<td>5c3dc42237d9e200489af01643990e90</td>
<td>IN0127341</td>
</tr>
</tbody>
</table>
## 2. Connector Code

- **connector.php**  
  launched by Zabbix action, open ticket.

- **connector_daemon.php**  
  launched by scheduler, regularly check if a ticket is closed; if yes, updates Zabbix with the information from Trouble Ticket.

- **connector_library.php**  
  Connector Libraries

- **connector_versions.txt**  
  Versionning

### APIs Zabbix Libraries:

- PhpZabbixApi_Library/ directory

- From [https://github.com/confirm/PhpZabbixApi](https://github.com/confirm/PhpZabbixApi) project
Supported Versions

Connector Release V6 synchronized with:

- Zabbix V2.2.x (must be OK with 2.4 and 3.0 but not tested)
- ServiceNow Fuji Version
Released as OpenSource
On Zabbix Share

Search...

Advanced Search

Applications

Cluster

HelpDesk System

Zabbix Service Now Connector

Zabbix Service Now Connector V6 (2016 August)

Designed by alain@coolmonitoring.fr
Merci pour votre attention !

Alain Ganuchaud

Cool Monitoring

alain@coolmonitoring.fr

Questions?

Follow us on Twitter: @zabbix_fr @AlainGanuchaud