Managing complexity in Zabbix installations with Splunk
What **complexity**?

Operating a Zabbix deployment of a certain size comes with some challenges.

- Huge amount of **Hosts**, Templates, **Items**, Host Groups, Macros, …
- **Unsupported** Items / LLD rules
- **Network** issues / Host **availability**
- **Queue** entries
- Many many **problems**
Questions

What are the hosts generating most of the problems, at what times and generated by which templates?

Did the latest change / upgrade / … have any negative impact on our monitoring?

Can you work on getting rid of those unsupported items?

How many hosts we have that have this specific problem and would be the effect if we fixed those problems?

Where the *** do all these queue entries come from?
Too much information?

Zabbix is:

• A brilliant monitoring tool
• Great ways to organize entities with templates
• Very clear and predictable
• Great visualization capabilities

Zabbix is NOT:

• An analytics utility
• …offering a flexible query language
• …having on-demand statistical functions
• …allowing us to enrich data with arbitrary sources
Analyze Zabbix data with Splunk

- Data Sources depending on use case
  - Indexed data
  - Lookups backed by Key-Value store
  - Scripted lookups
  - Custom Search commands
Zabbix entity inventory

- Hosts
- Items
- Proxies
- Templates
- Triggers
- Discovery Rules (LLD)
- Item Prototypes
- Trigger Prototypes

Zabbix API: `host.get()`, ...

Search

Scheduled search

Custom search command

KV-Store (mongo)

Result Set
More data

- Zabbix Server / Proxy Logs
- Real-Time lookup for status (item, host, trigger)
- Metrics (History / Trends data)
- Problems (custom Media Type)
- Alerts
- Queue items
The Zabbix Queue

### Zabbix - Queue

Group by:  
- Item type  
- Endpoint  
- Host  
- Host Availability  
- Item State

Ignore Hosts:  
- Unavailable  
- Unknown

### Details

<table>
<thead>
<tr>
<th>Item_type</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv2 agent</td>
<td>482</td>
</tr>
<tr>
<td>Zabbix agent</td>
<td>158</td>
</tr>
<tr>
<td>Zabbix agent (active)</td>
<td>24</td>
</tr>
<tr>
<td>SNMPv1 agent</td>
<td>17</td>
</tr>
<tr>
<td>simple check</td>
<td>1</td>
</tr>
</tbody>
</table>

- Free swap space
- Processor load (5 min average per core)
- System IP Addresses
- CPU I/O wait time
- Matches in Category 81
- Free inside on 81 (percentage)
Zabbix Problem Analytics

Zabbix Problems Stats

Problem Creators Drilldown (Template: Tmpl Module OS Windows v1, System Type: Windows)

Events per host (Template: Tmpl Module OS Windows v1, System Type: Windows, Problem: Problem (unified: *)

Total events timeline (Template: Tmpl Module OS Windows v1, System Type: Windows, Host: 9095POS1, Problem: Problem (unified: *)

SECADM
SECURE FOR SURE
Zabbix data for Management Visibility

- Correlation of data
  - Zabbix (Metrics, Status, Problems …)
  - Application Logs
  - Other data sources
  - Inventory (CMDB, …)

- Business Level Visualization
How to get it?

- Open Source License
- Free

Contact us!

Christian.Anton@secadm.de