ZABBIX 5.0

(MY PERSONAL...) KEY FEATURES IN DETAIL

Christian Anton, secadm GmbH
Christian.Anton@secadm.de
MONITORING ➔ HOSTS AND THE NEW GUI

- New menu respecting modern wide screens
- Changes for handling higher # of hosts to monitor
- Monitoring ➔ Hosts as a new central view
- Minor improvements
LIST OF MONITORED DEVICES
WHERE AM I AND WHAT IS THERE TO SEE?

- Long desired feature
- Overview of non-admins / visibility of Host Availability
- For admins: easier to get from viewing to setting things up and back
BETTER ADDING OF ELEMENTS TO OBJECTS
NO MORE «ADD, ADD, UPDATE»...
MONITORING → HOSTS → GRAPHS
DIRECT ACCESS TO ALL GRAPHS FOR ONE HOST

ZABBIX
Dashboard  Problems  Overview  Web  Latest data  Graphs  Screens  Maps  Discovery  Services

Search: Zabbix server

Hosts
Host  IP  DNS  Latest data  Problems
Zabbix server  10.7.249.10  dataline0016.kuro-group.com  Latest data  Problems

ZABBIX
Dashboard  Problems  Overview  Web  Latest data  Graphs  Screens  Maps  Discovery  Services

Graphs
Graphs  Zabbix server

---

SECADM
SECURE FOR SURE
DEFAULT MESSAGES FOR EACH MEDIA TYPE

- Easier to manage messaging guidelines
- Perform mass changes in Action messages with couple of clicks
- Simplify configuration of Actions
“CPU load is too high on Windows-Server01”

Dear User!
A problem has occurred:
Host: server01
Problem: CPU load is too high
Action Workflow
How do you get your notification?

**Problem / Recovery**

"CPU load is too high on Windows-Server01"

**Action**

Send message

**Email**

**Slack**

**Jira Ticket**

Dear User!

A problem has occurred:

Host: server01
Problem: CPU load is too high
DEFAULT MESSAGES
FOR EACH MEDIA TYPE

- More flexible configuration of complex notification scenarios with less effort
- Manage high amount of actions with a wide variety of media types
- Transferable between Zabbix installations (NEW: import/export media types!!)
DEFAULT MESSAGES
FOR EACH MEDIA TYPE

• Define standard messaging for Media type
• Define standard messaging for every state of a problem
• If needed – **override on Action level**
nodata() triggers are now, by default, sensitive to proxy availability

Turn off sensitiveness to proxy availability with new parameter nodata(5m,strict)

Avoid massive event storms and other issues because of single proxy
NODATA TRIGGERS AND PROXY AVAILABILITY BACKGROUND

ZBXNEXT-1891 – Implicit trigger dependency when monitored via proxy (2003)

- nodata() trigger function – Checking for no data received
- If host is monitored by proxy, but proxy can’t report data to server = no data
- Event and alert storms, other performance issues
- nodata() triggers are used in official Zabbix agent templates
- cheap in calculation
NODATA TRIGGERS
LET’S VISUALIZE

1x
ZABBIX AGENT → ZABBIX PROXY → ZABBIX SERVER

SECADM
SECURE FOR SURE
NODATA TRIGGERS
LET’S VISUALIZE

1x
ZABBIX
AGENT
→
ZABBIX
PROXY
→
ZABBIX
SERVER

Proxy is down
+
1x nodata problem
NODATA TRIGGERS
LET’S VISUALIZE

5000x ZABBIX AGENT  →  ZABBIX PROXY  →  ZABBIX SERVER

Proxy is down
+ 5000x nodata problems
NODATA TRIGGERS
LET’S VISUALIZE – 5.0

5000x

1x Problem
Proxy is down
NODATA TRIGGERS

FINAL NOTES

• Much easier than setting up global event correlation and Trigger dependencies
• Out of the box functionality, just works as expected without any further setup
• What if I don’t want to respect proxy availability? `nodata(5, strict)`!
Exception handling for specific Item and Trigger prototypes in LLD rules
LLD OVERRIDES
AND HOW THEY DIFFER FROM LLD FILTERS

LLD filters define whether an entity is being discovered or not

• Example: do not discover file systems with type «swap» or «proc»

LLD overrides define exceptions for specific prototypes based on content of LLD macros

• Example: set a different severity for a trigger on a root file system
• Example: do not add Trigger/Item for the entity in certain circumstances
• Example: set specific update interval / storage period for item
LLD OVERRIDES USE CASE:
ONE FILE SYSTEM LLD FOR BOTH WINDOWS AND LINUX

Problem:

- Windows does NOT support Inode monitoring: `vfs.fs.inode(fsname, <mode>)`

Solution:
In previous versions it was difficult to tell if a newly-configured item was configured correctly or not.

Now it is possible to test item from UI even before saving it, and get a real value in return.

And even test all pre-processing steps
TEST ITEM
 WHAT WE DID BEFORE?

- Simply wait for next update interval cycle
- `zabbix_agentd -t < item_key >`
- `zabbix_get -s <host> -k <key>`
- In Zabbix 4.0, «Check now» aka «Execute Now» has been added for passive items
TEST ITEM
PROBLEMS

• Waiting is not an option!
• «Check Now» is only available on host level (not templates)
• «Check Now» is executed by the server (Configuration cache, ...)
• Zabbix_agentd and zabbix-get don’t respect pre-processing
• Dependent Items...?
TEST ITEM
5.0

- Works on host and template level (by entering a valid IP and port to connect to for testing)
- Can be used before an item is actually saved in configuration
- Gives instant feedback
- Runs through and visualizes the whole preprocessing chain and outputs of all steps
- Can test items located on hosts behind Proxy
- Also works for calculated and aggregated items
- Allows substitution of macro values (NEW: secret macros)
TEST ITEM
5.0

Test item

Get value from host

Host address: 127.0.0.1
Port: 10050
Proxy: (no proxy)

Value: demo2 zabbix lan
Time: now
Previous value:
Prev. time:

End of line sequence:
LF, CRLF

Preprocessing steps
1: Regular expression
2: Replace
3: Left trim
4: Custom multiplier
5: In range

Result: Result converted to Text

Get value and test  Cancel
SNMP CREDENTIALS AT HOST INTERFACE LEVEL

- SNMP connection related settings where they should be
- Simplify configuration: make templates unique and transportable
- SNMPv1, SNMPv2, SNMPv3 => SNMP Agent
SNMP CREDENTIALS AT HOST INTERFACE LEVEL

- Complexity of authentication parameters
- Simple human mistakes – typos
- In case of many items, chance to make mistake increases
- One mistake in Item prototype can affect whole host

![Image of SNMP credentials at host interface level]
SNMP CREDENTIALS
AT HOST INTERFACE LEVEL

• Instead of suggesting to «be careful!» minimize possibilities to make mistake
• snmpv1, snmpv2, snmpv3 replaced with SNMP Agent
• All configuration is done on interface level
• All items inherit settings from chosen interface
THANK YOU!