The Clever and the Cool
Zabbix meets IBM Netcool

IntelliTrend IT-Services GmbH
Otto-Brenner-Strasse 119
D-33607 Bielefeld, Germany

Contact: Wolfgang Alper
wolfgang.alper@intellitrend.de
www.intellitrend.de
The Clever and the Cool
Zabbix meets IBM Netcool

With special thanks to

Deutsche Telekom Technik GmbH
The Clever and the Cool

Let's start simple

Zabbix: Monitors various systems

Problem detected

Zabbix: Incident processing
Incident processing

Notifications (Email, SMS, Messenger)

Incidents (Ticketsystem)

Script Executions (Direct, Remote, Taskrunner)

Escalations (Complex Scenarios)
The Clever and the Cool
Different monitoring systems

Zabbix: Monitors various systems
Problem detected
Zabbix: Incident processing

Other Monitoring: Monitors other systems
Problem detected
Other monitoring: Incident processing

The Clever and the Cool
Different monitoring systems

Zabbix: Monitors various systems
Problem detected
Zabbix: Incident processing

Other Monitoring: Monitors other systems
Problem detected
Other monitoring: Incident processing
The Clever and the Cool
And even more ...

Zabbix:
Monitors various systems

Problem detected

Zabbix:
Incident processing

Other Monitoring:
Monitors other systems

Problem detected

Other monitoring:
Incident processing

Special Monitoring:
Monitors special systems

Problem detected

Special monitoring:
Incident processing
The Clever and the Cool Incident processing

- Incident processing Monitoring-A
- ... (omitted)
- Incident processing Monitoring-N

- Notifications (Email, SMS, Messenger)
- Incidents (TicketSystem)
- Escalations (Complex Scenarios)
- Script Executions (Direct, Remote, Taskrunner)
- Incidents (TicketSystem)
- Escalations (Complex Scenarios)
The Clever and the Cool Incident processing

Incident processing Monitoring-A

... 

Incident processing Monitoring-N

Notifications (Email, SMS, Messenger)

Incidents (Ticket system)

Notifications (Email, SMS, Messenger)

Script Executions (Direct, Remote, Taskrunner)
The Clever and the Cool
Incident processing management

How to manage incident processing across different monitoring systems?
The Clever and the Cool Incident processing management

Special Monitoring: Monitors special systems

Other Monitoring: Monitors other systems

Incident processing

Option: Forward to existing monitoring system
The Clever and the Cool
Incident processing management

Other Monitoring: Monitors other systems

Special Monitoring: Monitors special systems

Option: Forward to Zabbix
The Clever and the Cool
Incident processing management

Special Monitoring: Monitors special systems

Option: Forward to central incident processing

Central Incident processing

Other Monitoring: Monitors other systems
The Clever and the Cool
Incident processing management

Having more than one Zabbix Server?
The Clever and the Cool
Adding more Zabbix Systems
The Clever and the Cool Incident processing management

Special Monitoring: Monitors special systems

Central Incident processing

Other Monitoring: Monitors other systems

Option: Forward to central incident processing
The Clever and the Cool
Central incident processing

How to integrate with a central incident processing system?
The Clever and the Cool
Central incident processing

Use SNMP Traps!
(Simple Network Management Protocol)
The Clever and the Cool
Central incident processing

Why SNMP Traps instead of custom API programming?

SNMP Traps are:

- ...specifically designed to monitor network components.
- ...defined by official RFC's.
- ...provide authentication and encryption.
- ...supported by many vendors.
The Clever and the Cool
Central incident processing

SNMP
- Must use polling.
- Query a system for one or more metrics.
- No other software needed.

SNMP Traps
- Event driven.
- Ask a device to send a message when an event happens.
- Requires a SNMP Trap receiver.

SNMP vs. SNMP Traps
The Clever and the Cool
Design and Implementation

Integration Zabbix ↔ IBM Netcool
The Clever and the Cool Design and Implementation

Special Monitoring: Monitors special systems

IBM Netcool Incident processing

Other Monitoring: Monitors other systems

All involved monitoring systems send their alerts via SNMP Traps
The Clever and the Cool
Design and Implementation

Advantages

☑ Easy integration into existing incident and escalation management.
☑ Scaleability, not limited to a single Zabbix instance.
☑ Easy configuration of problems that must be visible in IBM Netcool.
☑ Automatic central monitoring of availability of Zabbix Servers.
☑ Reusing existing infrastructure.
☑ Well defined interface on the IBM Netcool part.
The Clever and the Cool
Design and Implementation

Design Considerations
The Clever and the Cool
Design and Implementation

- Pass unique Zabbix instance names to Netcool.
- Pass hostname to Netcool.
- Pass trigger identifier and trigger severity to NetCool.
- Pass Zabbix eventid to Netcool on entering “problem” state.
- Pass Zabbix eventid to Netcool on entering “ok” state to clear.
- Control which events should be passed to Netcool.
- Implement heartbeat so Netcool can monitor the middleware.
- Implement the communication based on SNMP v3 Traps.
The Clever and the Cool
Design and Implementation

ZabbixInstance: "zbxsrv-se-15"
Hostname: “myhost”
Trigger identifier (TAG): ”453214321”
Trigger severity: ”High”
Trigger name: ”VLAN not reachable”
EventId: ”9876543”

Pass to IBM Netcool via SNMP Trap

There are more fields involved ...

tmIdentifier (1)
tmNode
tmIdentifier (2)
tmSeverity
tmSummary
tmEventID
The Clever and the Cool
Design and Implementation

Implementation
# The Clever and the Cool

Design and Implementation - Media

<table>
<thead>
<tr>
<th>Media type</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>* Name</th>
<th>IBM-Netcool</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td><strong>Script</strong></td>
</tr>
<tr>
<td>* Script name</td>
<td>Zabbix2IBM-Netcool</td>
</tr>
</tbody>
</table>

**Script parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>-atrigger</td>
</tr>
<tr>
<td>-m{ALERT.MESSAGE}</td>
</tr>
</tbody>
</table>

© Copyright 2019 IntelliTrend GmbH ● Otto-Brenner-Straße 119 ● 33607 Bielefeld ● Germany ● Tel: +49 521 557716-0 ● www.intellitrend.de
The Clever and the Cool
Design and Implementation - Action

Tag equals netcoolid
Send message to users: IBM-Netcool via IBM-Netcool

Default subject: Zabbix2IBM-Netcool - Problem: {TRIGGER.NAME}

Default message:
<zabbix2ibmmnetcool>
<tmSeverity>{EVENT.NSEVERITY}</tmSeverity>
<tnNode>{HOST.HOST}</tnNode>
<tnConfigItemID>{INVENTORY.ASSET.TAG}</tnConfigItemID>
<tmAlertGroup>{$TM_ALERT_GROUP}</tmAlertGroup>
<tmSummary>{TRIGGER.NAME}</tmSummary>
<zbxTriggerState>{EVENT.VALUE}</zbxTriggerState>
<zbxEventTags>{EVENT.TAGS}</zbxEventTags>
<zbxEventID>{EVENT.ID}</zbxEventID>
<zbxEventDate>{EVENT.DATE}</zbxEventDate>
<zbxEventTime>{EVENT.TIME}</zbxEventTime>
<zbxTriggerDescription>{TRIGGER.DESCRIPTION}</zbxTriggerDescription>
</zabbix2ibmmnetcool>

Pause operations for suppressed problems

Operations
Steps Details Start in Duration
1 Send message to users: IBM-Netcool via IBM-Netcool Immediately Default
# The Clever and the Cool

## Design and Implementation - Trigger

<table>
<thead>
<tr>
<th>Trigger</th>
<th>Tags</th>
<th>Dependencies</th>
</tr>
</thead>
</table>

### Trigger tags

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>netcoolid</td>
<td>453214321</td>
<td>Remove</td>
</tr>
</tbody>
</table>
The Clever and the Cool
Design and Implementation

Resulting SNMP Trap
send from Zabbix
to IBM-Netcool
The Clever and the Cool
IBM Netcool Trap payload - Problem

2019-03-24 10:34:21 devzab.intellitrend.loc [UDP: [172.20.20.196]:55795→[172.22.22.2]:16570]:
DISMAN-EXPRESSION-MIB::sysUpTimeInstance = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::snmpTrapOID.0 = OID:
NATNETCOOL::tmIdentifier = STRING: "zbxsrv-se-015_726"
NATNETCOOL::tmManager = STRING: "ZABBIX_EVO"
NATNETCOOL::tmAgent = STRING: "zbxsrv-se-015"
NATNETCOOL::tmNode = STRING: "TestHost1"
NATNETCOOL::tmConfigItemID = STRING: "acc/NetworkElement/453214321"
NATNETCOOL::tmEventID = INTEGER: 9876543
NATNETCOOL::tmAlertGroup = STRING: "EVALUATION ALERT GROUP"
NATNETCOOL::tmAlertKey = ""
NATNETCOOL::tmSeverity = INTEGER: major(4)
NATNETCOOL::tmSummary = STRING: "Test Trigger"
NATNETCOOL::tmOriginalSeverity = INTEGER: 4
NATNETCOOL::tmAdditionalText = STRING: "Example trigger description."
NATNETCOOL::tmAlarmInService = INTEGER: 1
NATNETCOOL::tmEventTime = INTEGER: 1553374417
NATNETCOOL::tmURL = ""
The Clever and the Cool
Design and Implementation

How does it look in IBM Netcool?
The Clever and the Cool
The final result in IBM Netcool

Heartbeat messages

<table>
<thead>
<tr>
<th>ProbeName</th>
<th>Summary</th>
<th>Manager</th>
<th>Agent</th>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>P_SNMP_ZABBIX</td>
<td>CAEM: Periodischer Heartbeat Zabbix Evolution (zbx_LastTest)</td>
<td>ZABBIX_EVO</td>
<td>ZABBIX_EVO zbx_LastTest</td>
<td>ZABBIX_EVO zbx_LastTest_heartbeat</td>
</tr>
<tr>
<td>P_SNMP_ZABBIX</td>
<td>CAEM: Periodischer Heartbeat Zabbix Evolution (zbx_____)</td>
<td>ZABBIX_EVO</td>
<td>ZABBIX_EVO zbx_____</td>
<td>ZABBIX_EVO zbx______heartbeat</td>
</tr>
<tr>
<td>P_SNMP_ZABBIX</td>
<td>CAEM: Periodischer Heartbeat Zabbix Evolution (zbx_____)</td>
<td>ZABBIX_EVO</td>
<td>ZABBIX_EVO zbx_____</td>
<td>ZABBIX_EVO zbx______heartbeat</td>
</tr>
<tr>
<td>P_SNMP_ZABBIX</td>
<td>CAEM: Periodischer Heartbeat Zabbix Evolution (zbx_____)</td>
<td>ZABBIX_EVO</td>
<td>ZABBIX_EVO zbx_____</td>
<td>ZABBIX_EVO zbx______heartbeat</td>
</tr>
</tbody>
</table>

Alarms …

<table>
<thead>
<tr>
<th>ProbeName</th>
<th>Summary</th>
<th>Manager</th>
<th>Agent</th>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>P_SNMP_ZABBIX</td>
<td>Probe P_SNMP_ did not receive any alerts in the last 20m.</td>
<td>ZABBIX_EVO</td>
<td>ZABBIX_EVO zbxsem</td>
<td>... The probe P_SNMP_</td>
</tr>
<tr>
<td>P_SNMP_ZABBIX</td>
<td>Probe P_SNMP_ did not receive any alerts in the last 3h.</td>
<td>ZABBIX_EVO</td>
<td>ZABBIX_EVO zbxsem</td>
<td>... The probe P_SNMP_</td>
</tr>
<tr>
<td>P_SNMP_ZABBIX</td>
<td>Probe P_SNMP_ did not receive any alerts in the last 10m.</td>
<td>ZABBIX_EVO</td>
<td>ZABBIX_EVO zbxsem</td>
<td>... The probe P_SNMP_</td>
</tr>
</tbody>
</table>
The Clever and the Cool
The final result in IBM Netcool
The Clever and the Cool
Zabbix meets IBM Netcool

Thank You!

IntelliTrend IT-Services GmbH
Otto-Brenner-Strasse 119
D-33607 Bielefeld, Germany

Contact: Wolfgang Alper
wolfgang.alper@intellitrend.de
www.intellitrend.de