

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

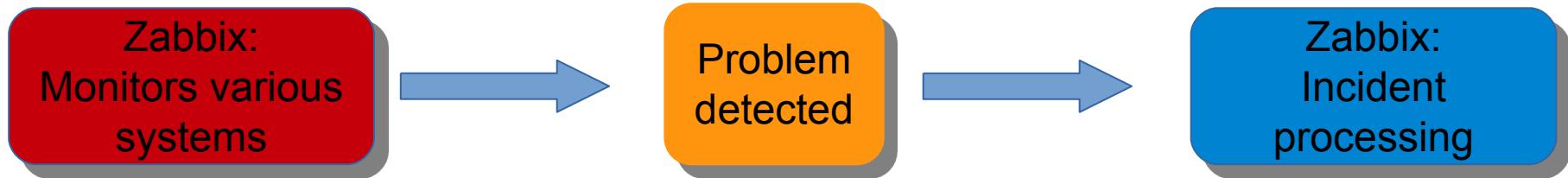
With special thanks to

Deutsche Telekom Technik GmbH



The Clever and the Cool

Lets start simple



The Clever and the Cool

Incident processing



Notifications
(Email, SMS,
Messenger)

Incidents
(Ticketsystem)

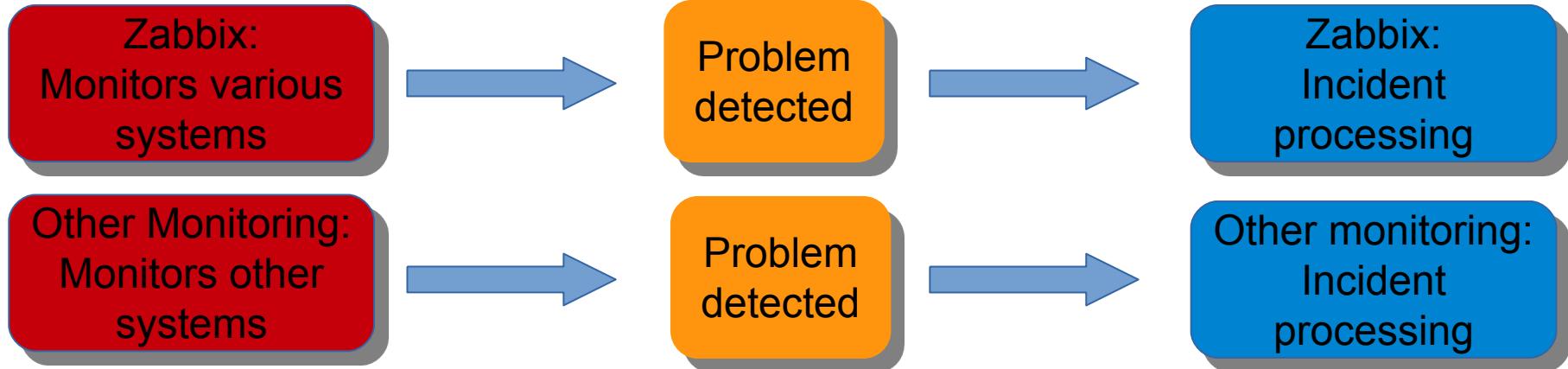
Script Executions
(Direct, Remote,
Taskrunner)

Escalations
(Complex
Scenarios)



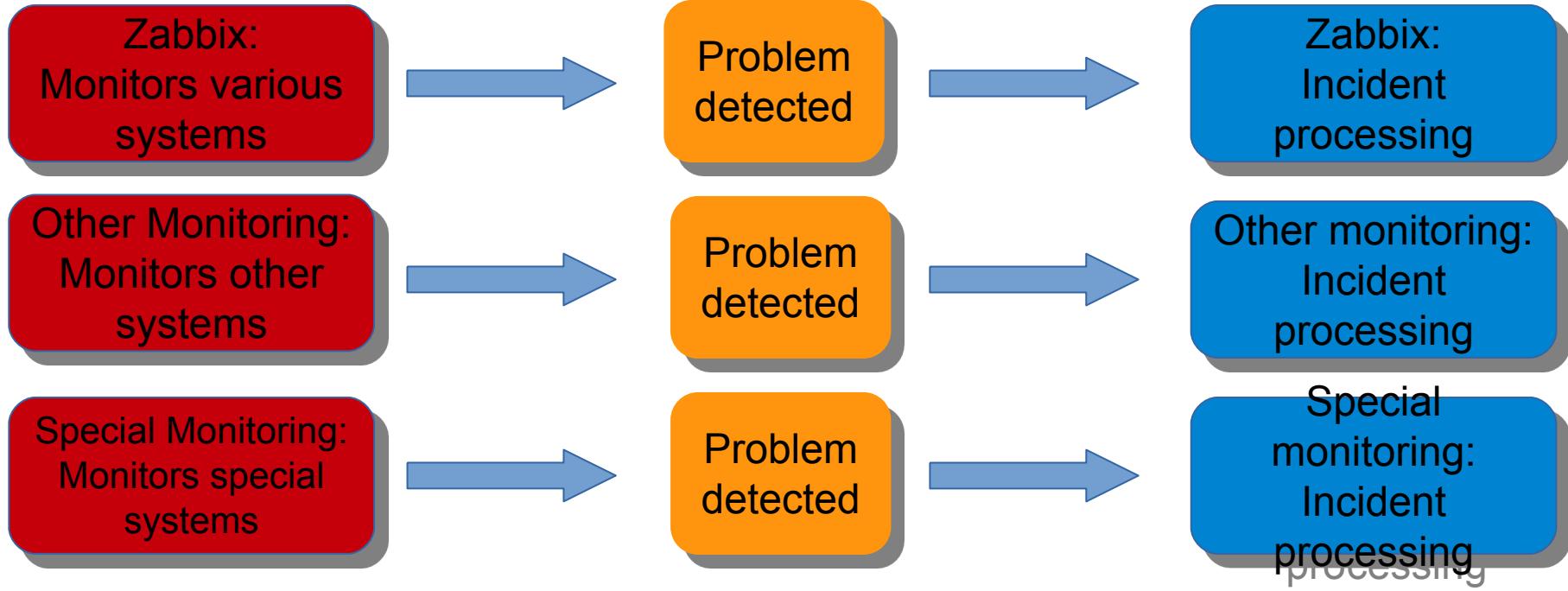
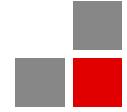
The Clever and the Cool

Different monitoring systems



The Clever and the Cool

And even more ...



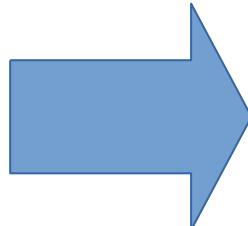
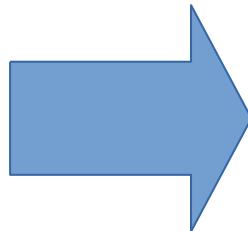
The Clever and the Cool

Incident processing

Incident
processing
Monitoring-A

...

Incident
processing
Monitoring-N



Notifications
(Email, SMS,
Messenger)

Script Executions
(Direct, Remote,
Taskrunner)

Notifications
(Email, SMS,
Messenger)

Script Executions
(Direct, Remote,
Taskrunner)

Incidents
(Ticketsystem)

Escalations
(Complex
Scenarios)

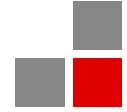
Incidents
(Ticketsystem)

Escalations
(Complex
Scenarios)

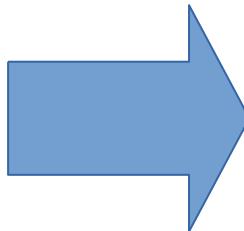


The Clever and the Cool

Incident processing



Incident
processing
Monitoring-A

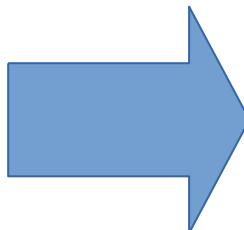


Notifications
(Email, SMS,
Messenger)

Incidents
(Ticketsystem)

...

Incident
processing
Monitoring-N

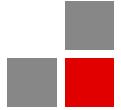


Notifications
(Email, SMS,
Messenger)

Script Executions
(Direct, Remote,
Taskrunner)



The Clever and the Cool Incident processing management

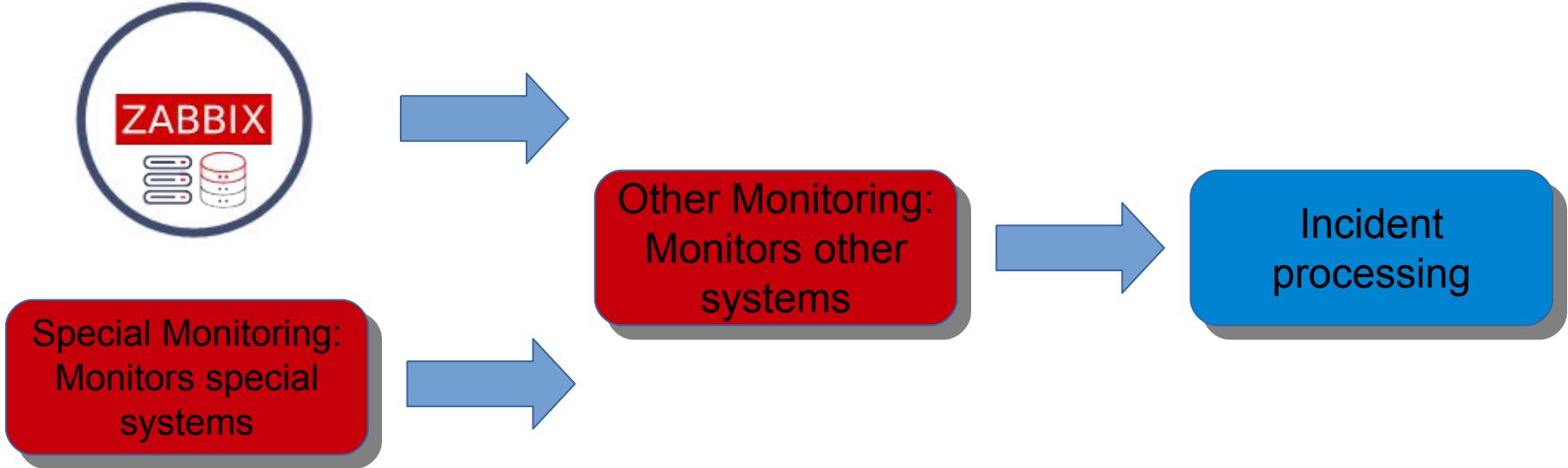
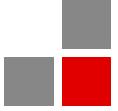


How to manage incident processing across different monitoring systems?



The Clever and the Cool

Incident processing management



Option: Forward to existing monitoring system

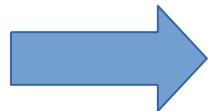


The Clever and the Cool

Incident processing management



Other Monitoring:
Monitors other systems



Special Monitoring:
Monitors special systems



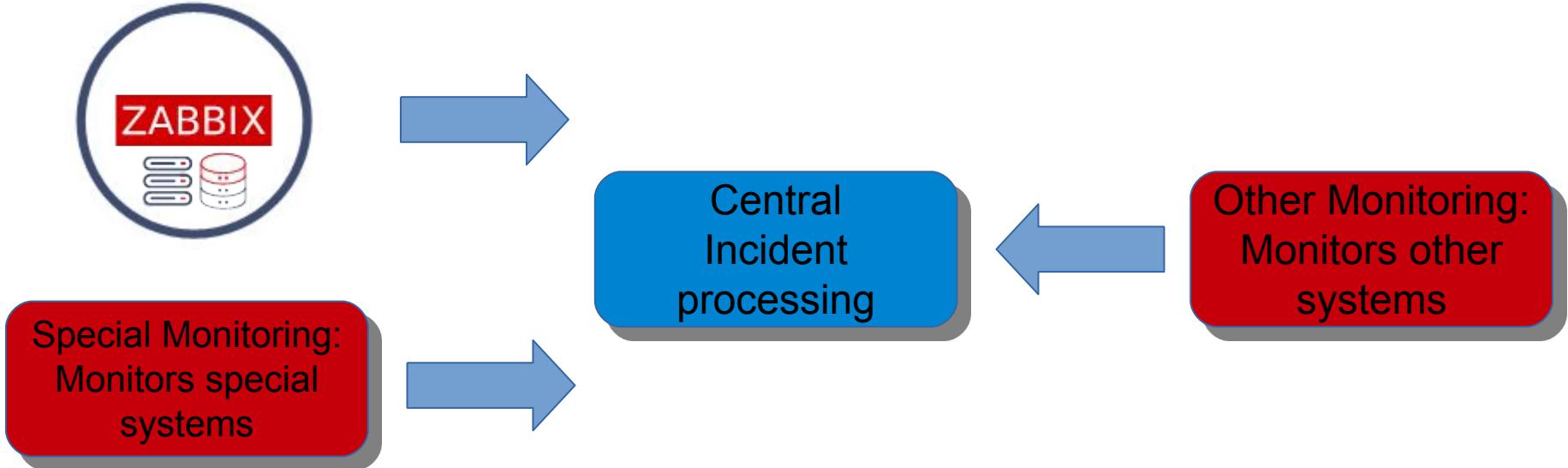
Incident
processing

Option: Forward to Zabbix



The Clever and the Cool

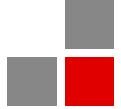
Incident processing management



Option: Forward to central incident processing



The Clever and the Cool Incident processing management

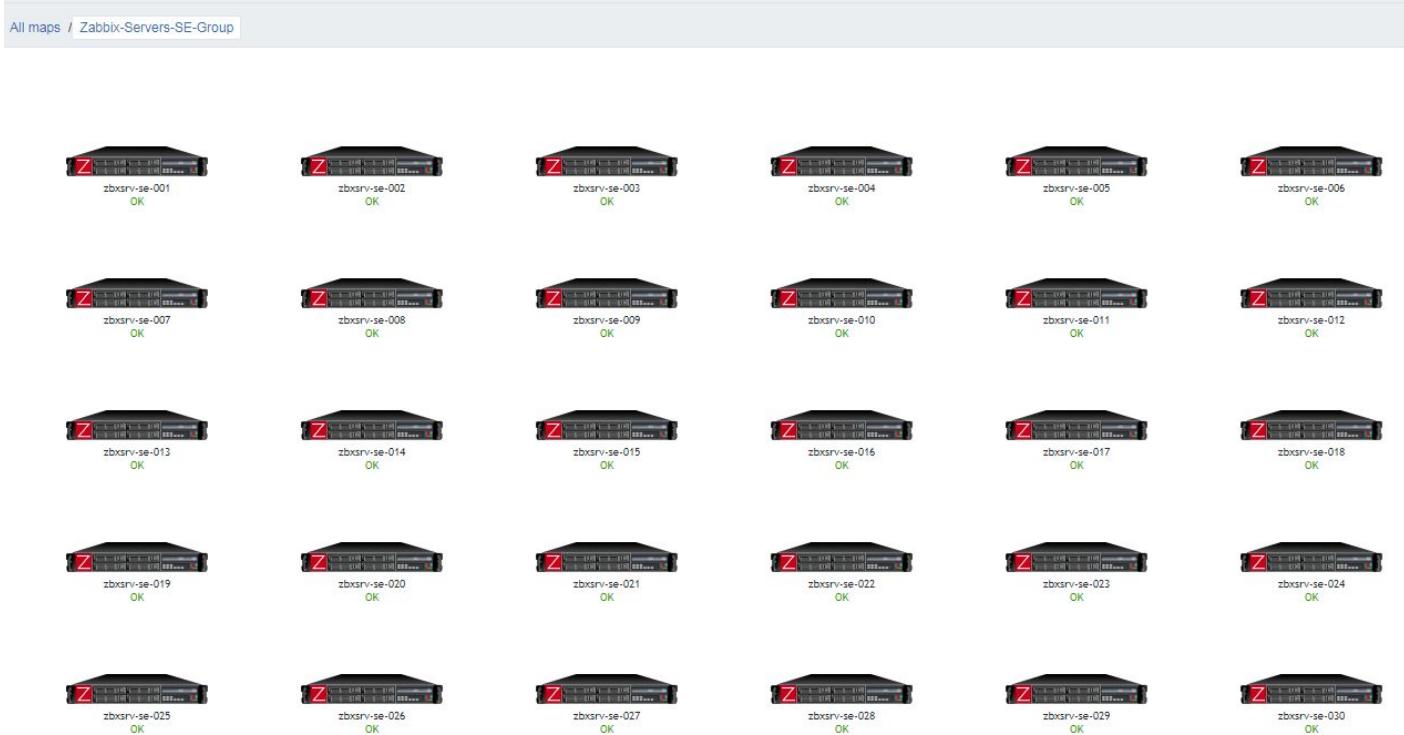


Having more than one Zabbix Server?



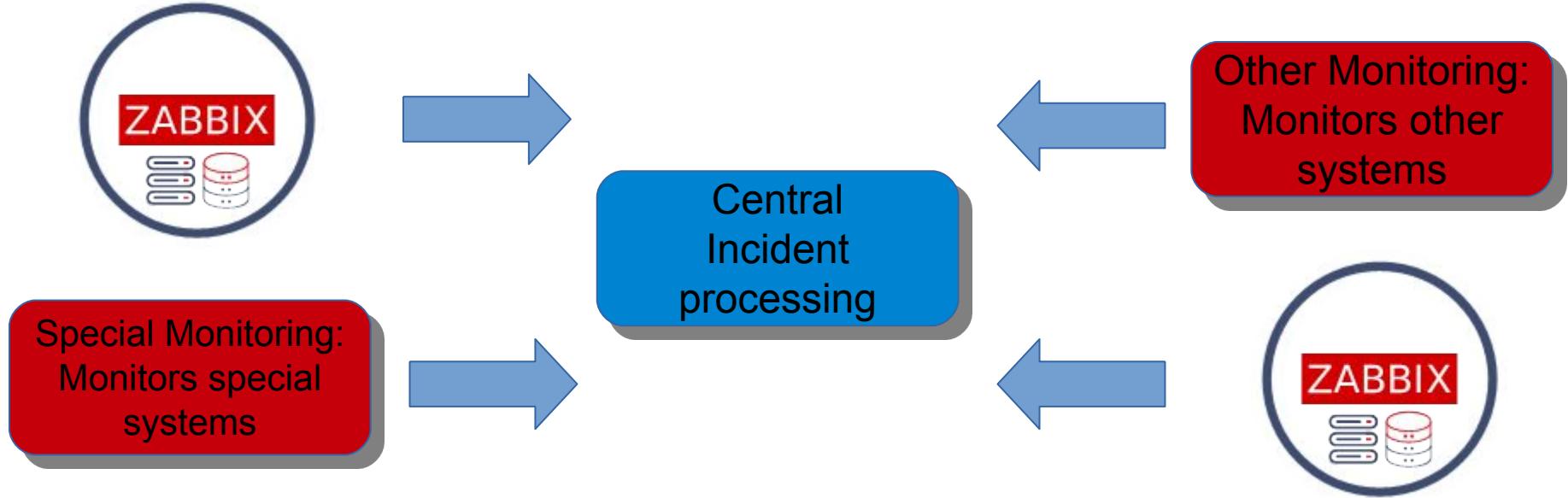
The Clever and the Cool

Adding more Zabbix Systems



The Clever and the Cool

Incident processing management

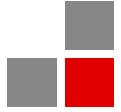


Option: Forward to central incident processing



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

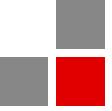


Use SNMP Traps!
(Simple Network Management Protocol)



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.

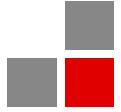
SNMP Traps

- 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



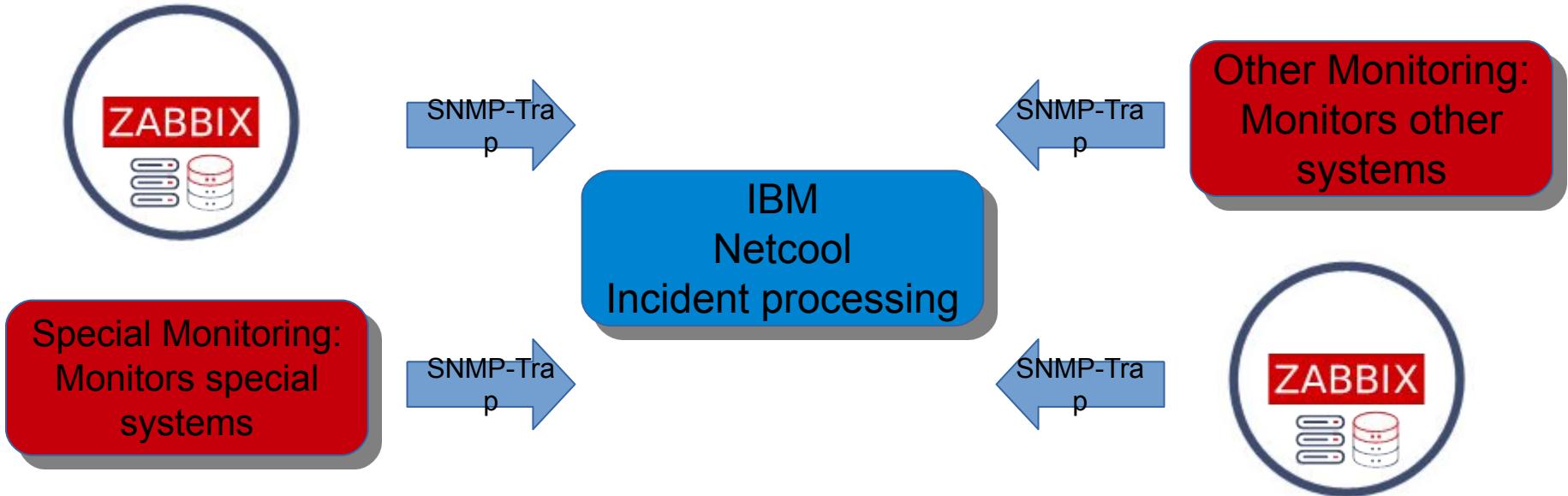
Integration Zabbix



IBM Netcool



The Clever and the Cool Design and Implementation

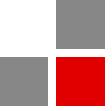


All involved monitoring systems send their alerts via SNMP Traps



The Clever and the Cool

Design and Implementation

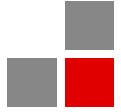


Advantages

- ✓ Easy integration into existing incident and escalation management.
- ✓ Scalability, 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

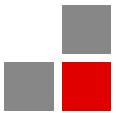
Design and Implementation



- 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

tmIdentifier (1)

tmNode

tmIdentifier (2)

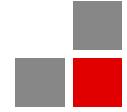
tmSeverity

tmSummary

tmEventID

There are more fields involved ...

The Clever and the Cool Design and Implementation



Implementation



The Clever and the Cool Design and Implementation - Media



IBM-Netcool Script Enabled IBM-Netcool Script name: "Zabbix2IBM-Netcool"

Media type Options

* Name IBM-Netcool

Type Script ▾

* Script name Zabbix2IBM-Netcool

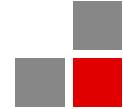
Script parameters Parameter

-atrigger

-m{ALERT.MESSAGE}



The Clever and the Cool Design and Implementation - Action



IBM-Netcool

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

Default subject

Zabbix2IBM-Netcool - Problem: {TRIGGER.NAME}

Default message

```
<zabbix2ibmnetcool>
  <tmSeverity>{EVENT.NSEVERITY}</tmSeverity>
  <tmNode>{HOST.HOST}</tmNode>
  <tmConfigItemID>{INVENTORY.ASSET.TAG}</tmConfigItemID>
  <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>
</zabbix2ibmnetcool>
```

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



Trigger Tags Dependencies

Trigger tags		Inherited and trigger tags	
Name	Value	Action	
netcoolid	453214321	Remove	



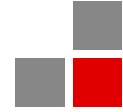
The Clever and the Cool Design and Implementation



Resulting SNMP Trap
send from Zabbix
to IBM-Netcool



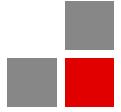
The Clever and the Cool IBM Netcool Trap payload - Problem



```
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

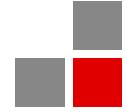


How does it look in IBM Netcool?



The Clever and the Cool

The final result in IBM Netcool



Heartbeat messages

File Edit View Alerts Tools Help

P_SNMP_ZABBIX Probes

ProbeName	Summary	Manager	Agent	Identifier
P_SNMP_ZABBIX	CAEM: Periodischer Heartbeat Zabbix Evolution (zbx_Lasttest)	ZABBIX_EVO	ZABBIX_EVO zbx_Lasttest	ZABBIX_EVO_zbx_Lasttest_Heartbeat
P_SNMP_ZABBIX	CAEM: Periodischer Heartbeat Zabbix Evolution (zbx_...)	ZABBIX_EVO	ZABBIX_EVO zbx_...	ZABBIX_EVO_..._Heartbeat
P_SNMP_ZABBIX	CAEM: Periodischer Heartbeat Zabbix Evolution (zbx_...)	ZABBIX_EVO	ZABBIX_EVO zbx_...	ZABBIX_EVO_zbx_..._Heartbeat
P_SNMP_ZABBIX	CAEM: Periodischer Heartbeat Zabbix Evolution (zbx_...)	ZABBIX_EVO	ZABBIX_EVO zbx_...	ZABBIX_EVO_zbx_..._Heartbeat
P_SNMP_ZABBIX	CAEM: Periodischer Heartbeat Zabbix Evolution (zbx_...)	ZABBIX_EVO	ZABBIX_EVO zbx_...	ZABBIX_EVO_zbx_..._Heartbeat

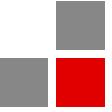
Alarms ...

P_SNMP_ZABBIX	Probe P_SNMP_ did not receive any alerts in the last 20m.	ZABBIX_EVO	ZABBIX_EVO zbxsem	...	The probe P_SNMP_
P_SNMP_ZABBIX	Probe P_SNMP_ : did not receive any alerts in the last 3h.	ZABBIX_EVO	ZABBIX_EVO zbxsem	...	The probe P_SNMP_
P_SNMP_ZABBIX	Probe P_SNMP_ did not receive any alerts in the last 10m.	ZABBIX_EVO	ZABBIX_EVO zbxsem	...	The probe P_SNMP_



The Clever and the Cool

The final result in IBM Netcool



P_SNMP_ZABBIX@ P_SNMP_ZABBIX

File Edit View Alerts Tools Help

P_SNMP_ZABBIX Probes

Alert Status for Serial Number 122485892

Fields Detail Journal

Field	Value
Summary	Probe P_SNMP_ did not receive any alerts in the last 20m.
Node	[REDACTED]
Severity	⚠
Acknowledged	No
LastOccurrence	16:07:57 03.09.2019
AckName	
AckTime	01:00:00 01.01.1970
ActualServerName	[REDACTED]
AdditionalText	The probe P_SNMP_ didn't receive any alerts in the configured minimum interval. The minimum interval is set to 20m.
AffectedNetCo	ID
AffectedUnit	[REDACTED]
Agent	ZABBIX_EVO_zbxsem
AgentGS	
AggregationFirst	01:00:00 01.01.1970
AlarmInService	0
AlarmPrio	0
AlertGroup	CA-EM Application

Probe P_SNMP_ did not receive any alerts in the last 20m.

<< Previous Next >>

Close Help

Event_ID FirstOccurrence

0	12:01:58 02.05.20
0	00:05:50 13.05.20
0	10:57:57 22.05.20
0	09:31:58 21.05.20
0	10:24:12 02.05.20
0	12:04:59 21.05.20
0	23:31:58 31.05.20
0	09:38:15 23.05.20
0	09:57:19 24.05.20
0	10:39:48 24.05.20
0	13:08:37 21.05.20
0	11:30:58 23.05.20
0	12:25:42 07.05.20
0	09:41:33 22.05.20
0	23:43:29 21.05.20
0	09:39:43 24.05.20
0	11:18:12 21.05.20
0	07:12:37 23.05.20
0	11:58:09 02.05.20
42580358	16:07:57 03.09.20
42580358	14:16:32 29.08.20
42580358	14:18:25 29.08.20
42580358	14:16:25 29.08.20
42580358	14:16:25 29.08.20
42580358	14:15:37 29.08.20
42580358	14:16:14 29.08.20

All Events (27)



The Clever and the Cool

Zabbix meets IBM Netcool

Thank You!



IntelliTrend IT-Services GmbH

Contact: Wolfgang Alper

Otto-Brenner-Strasse 119

wolfgang.alper@intellitrend.de

D-33607 Bielefeld, Germany

www.intellitrend.de

