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

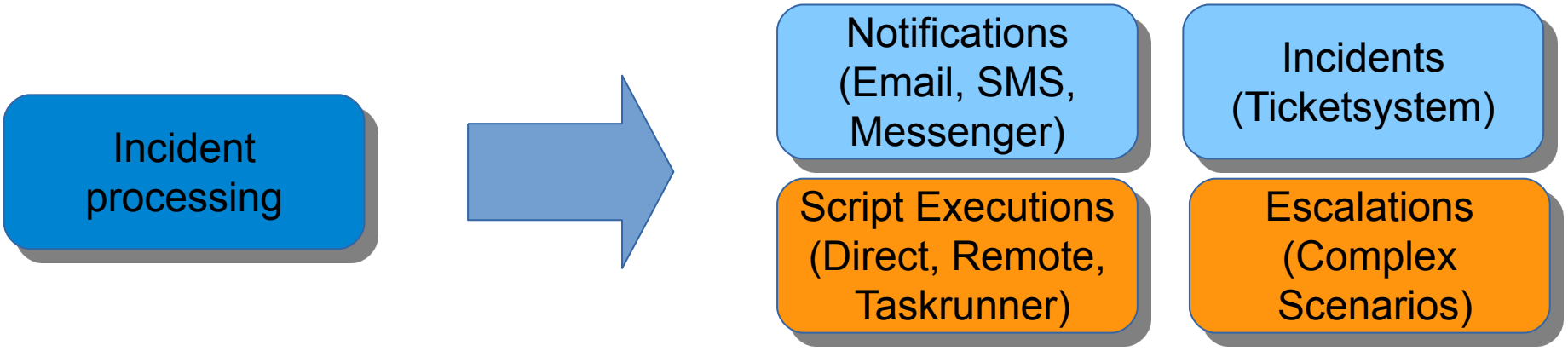
Deutsche Telekom Technik GmbH

ZABBIX
TRAINING PARTNER

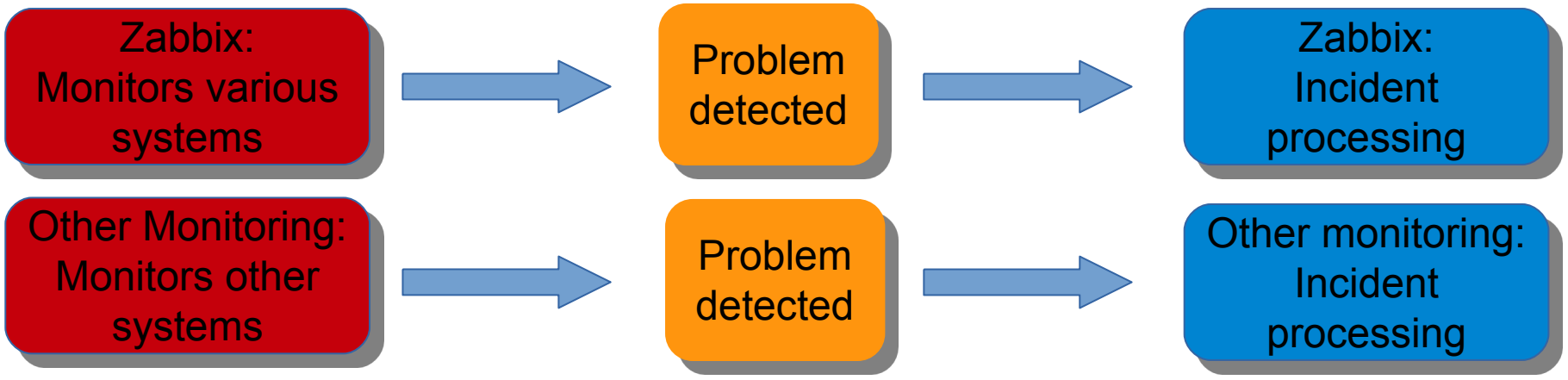
IntelliTrend
IT-Services

The Clever and the Cool
Lets start simple

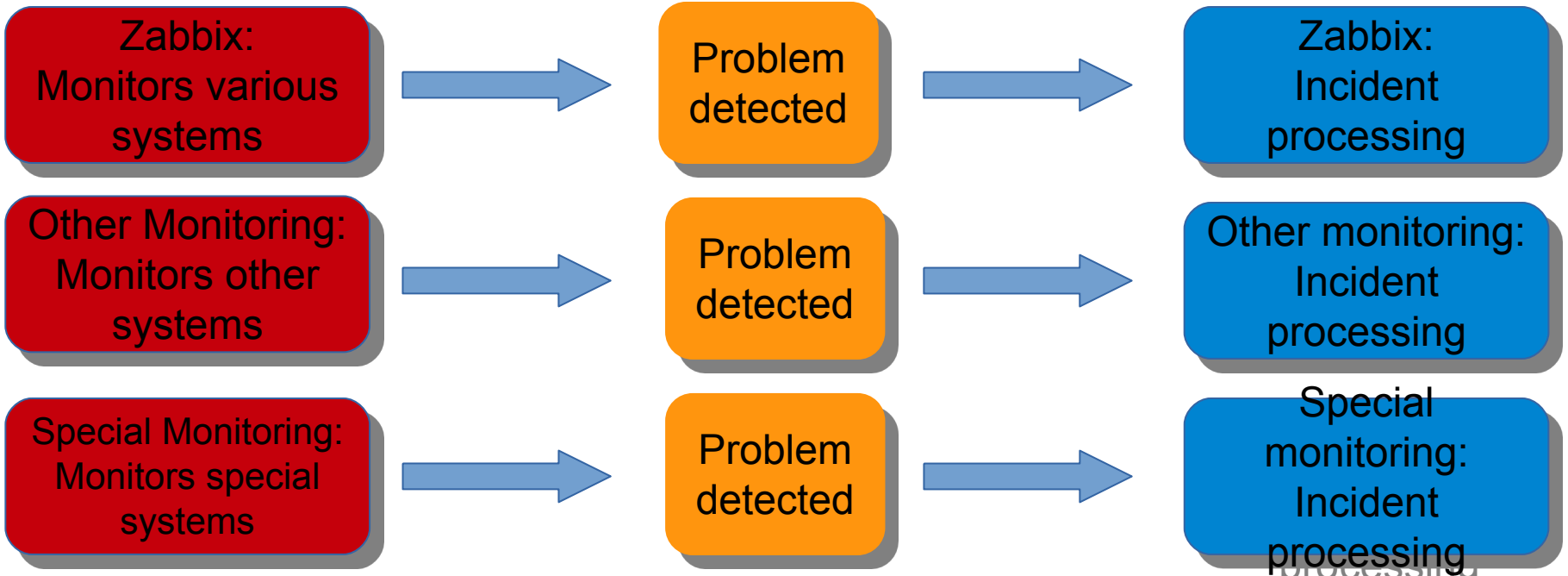
The Clever and the Cool
Incident processing



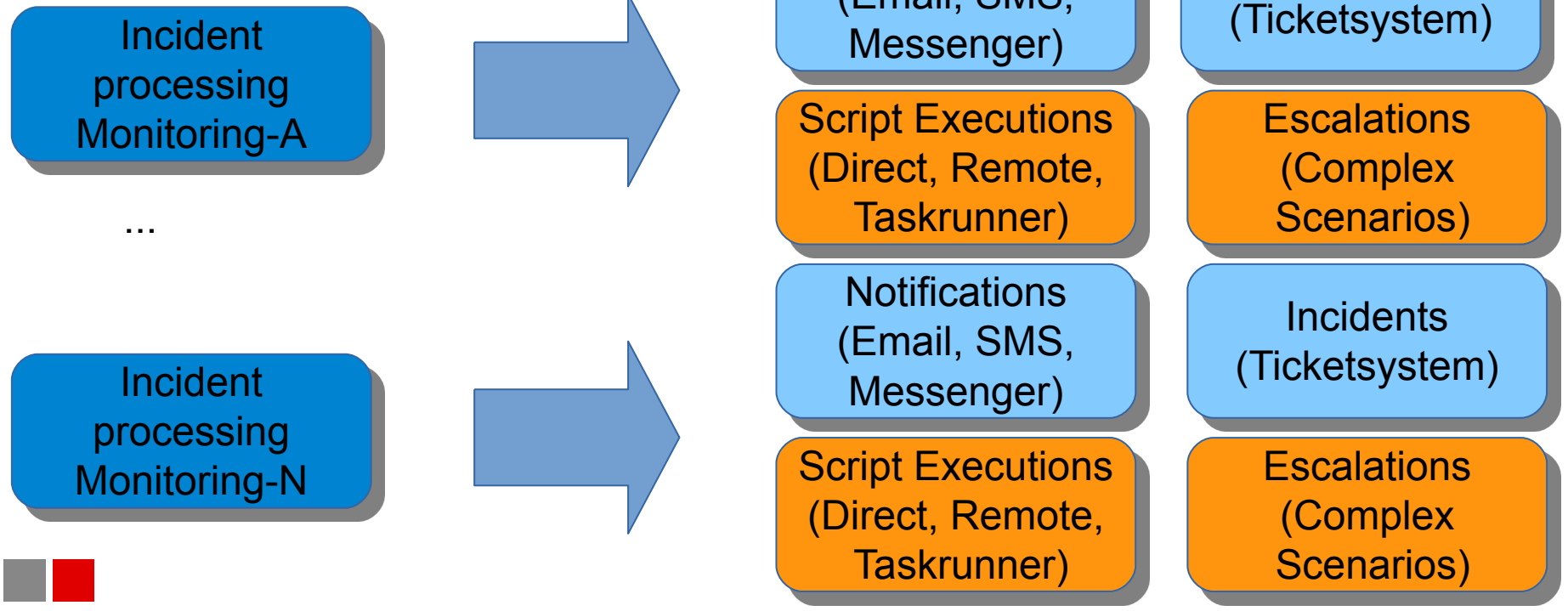
The Clever and the Cool
Different monitoring systems



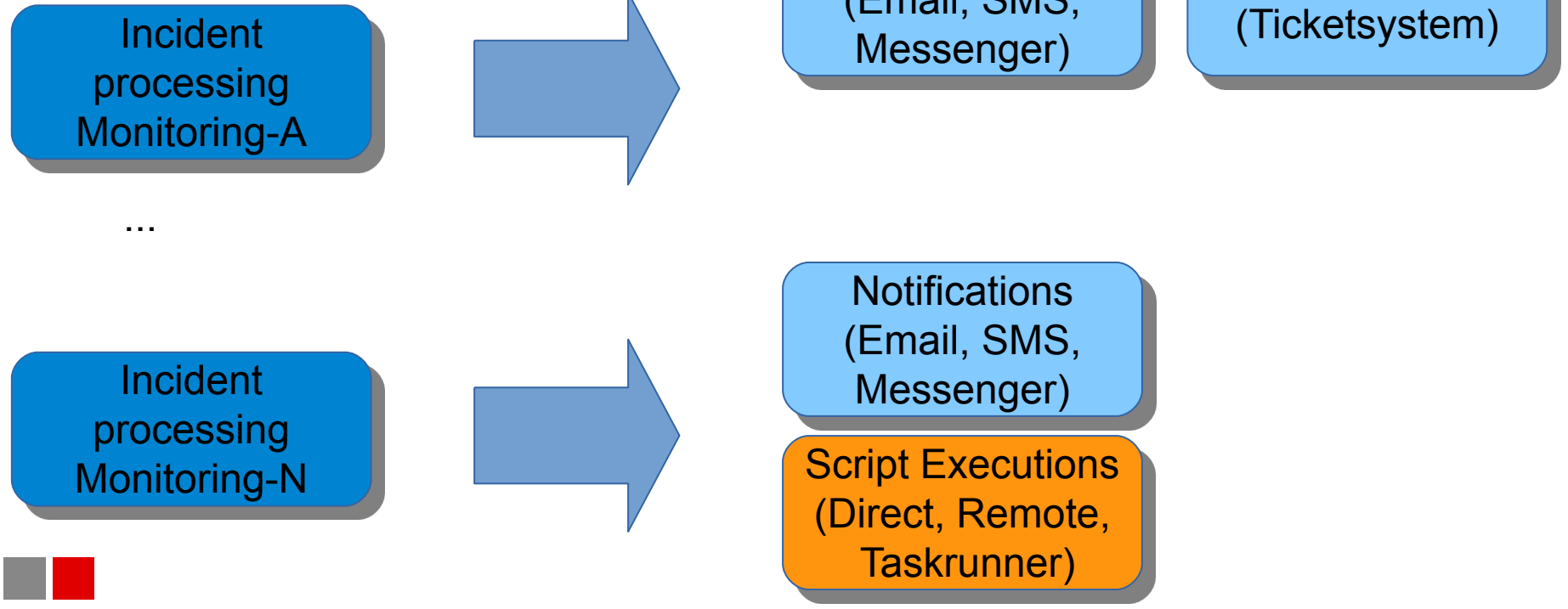
The Clever and the Cool
And even more ...



The Clever and the Cool
Incident processing



The Clever and the Cool Incident processing



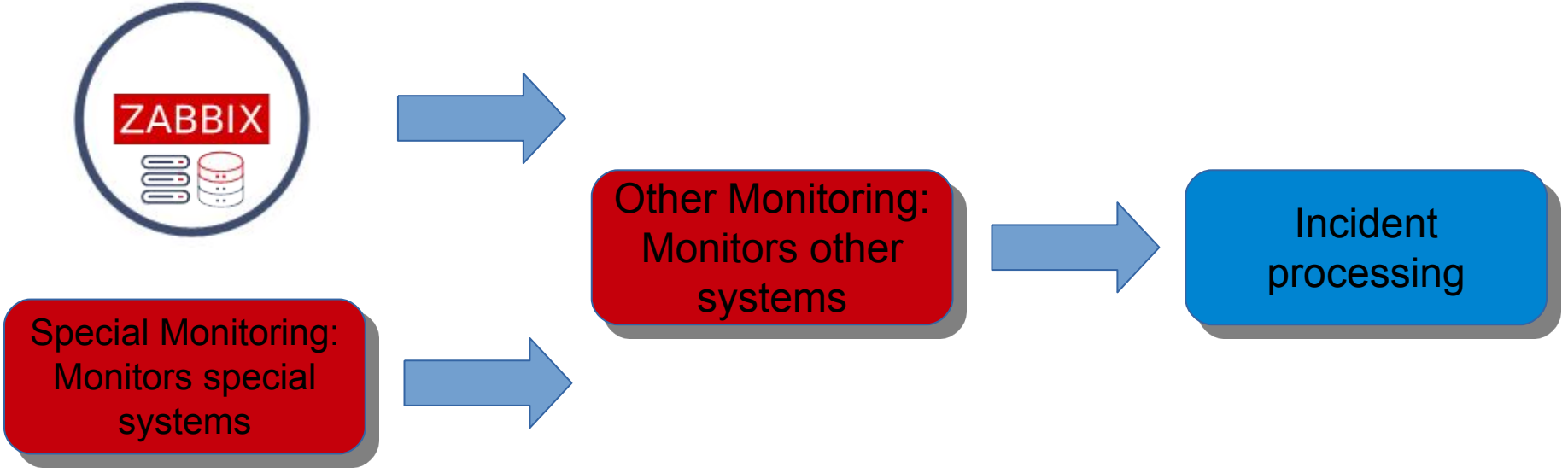
The Clever and the Cool
Incident processing management

How to manage incident processing across different monitoring systems?

ZABBIX TRAINING PARTNER

IntelliTrend IT-Services

The Clever and the Cool
Incident processing management

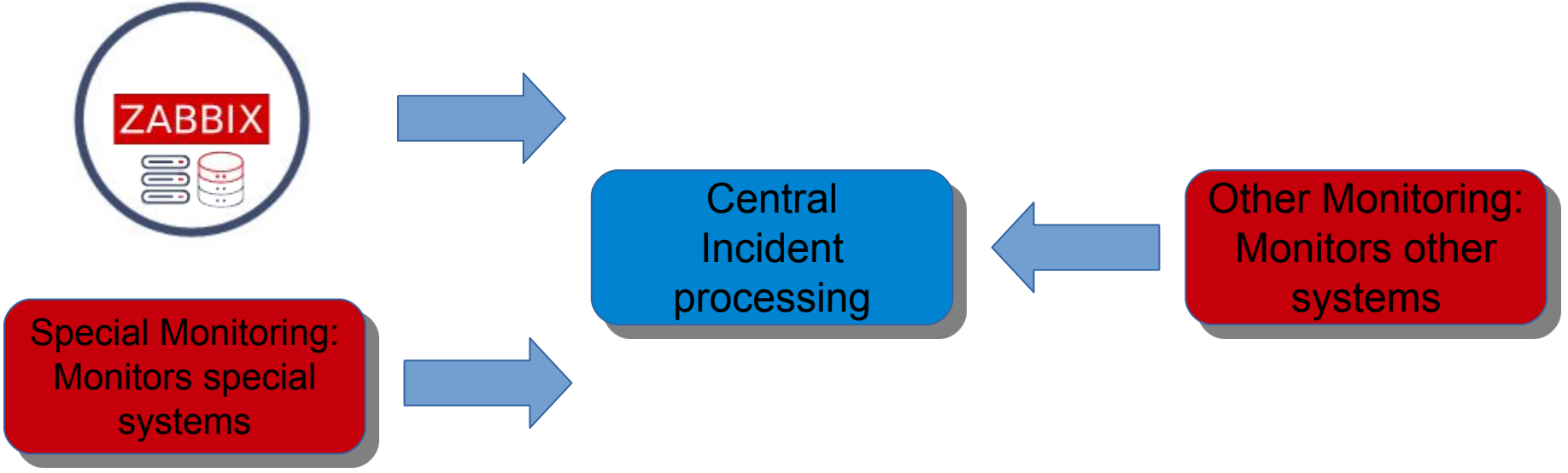


Option: Forward to existing monitoring system

The Clever and the Cool
Incident processing management

Option: Forward to Zabbix

The Clever and the Cool
Incident processing management

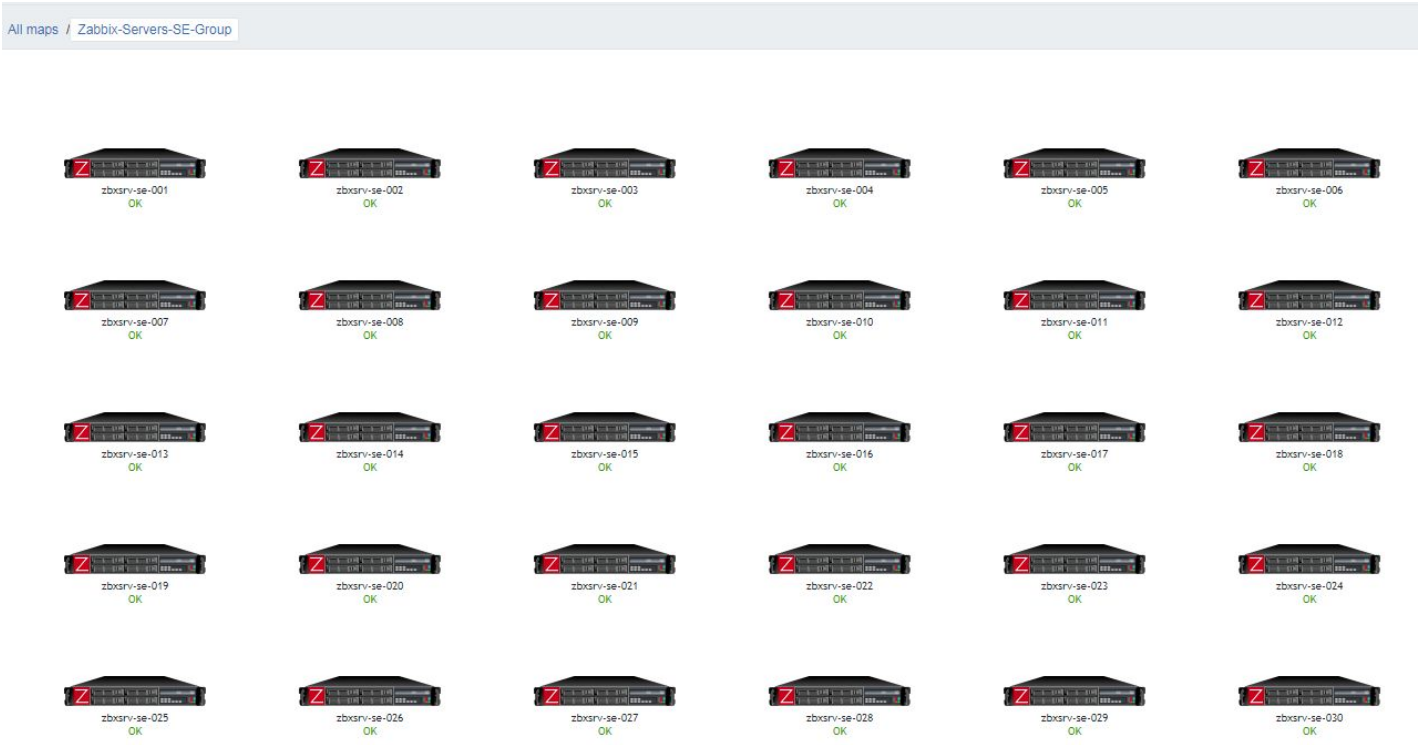


Option: Forward to central incident processing

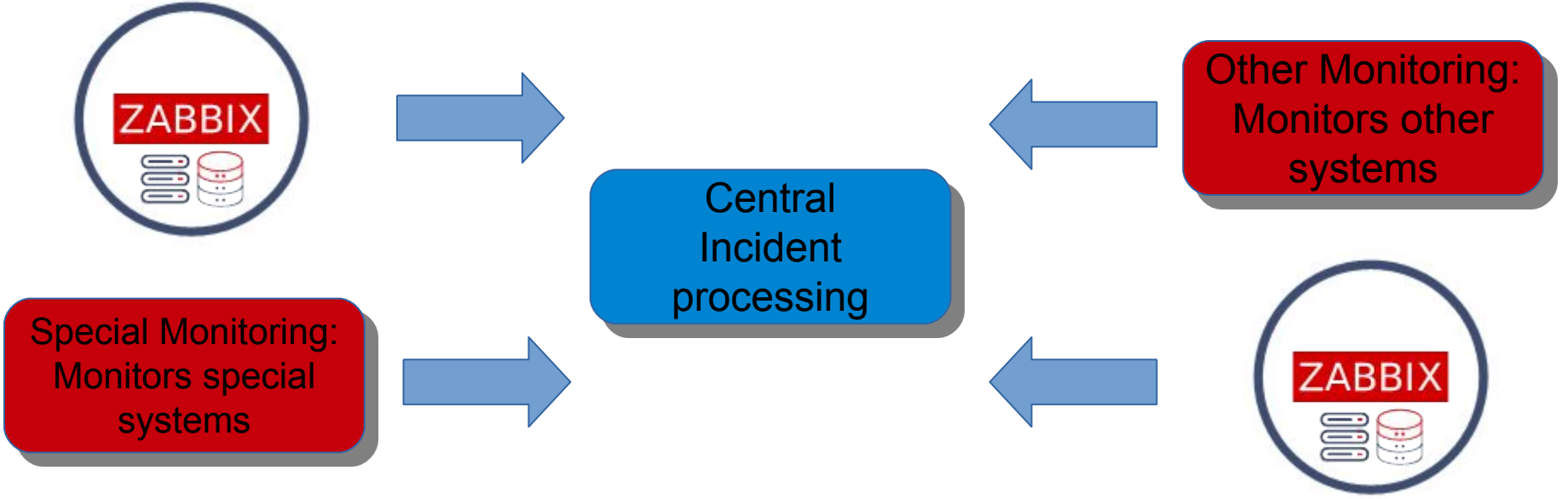
The Clever and the Cool
Incident processing management

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?

ZABBIX TRAINING PARTNER

IntelliTrend IT-Services

The Clever and the Cool
Central incident processing

Use SNMP Traps!
(Simple Network Management Protocol)

ZABBIX TRAINING PARTNER

IntelliTrend IT-Services

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.

ZABBIX TRAINING PARTNER

IntelliTrend IT-Services

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

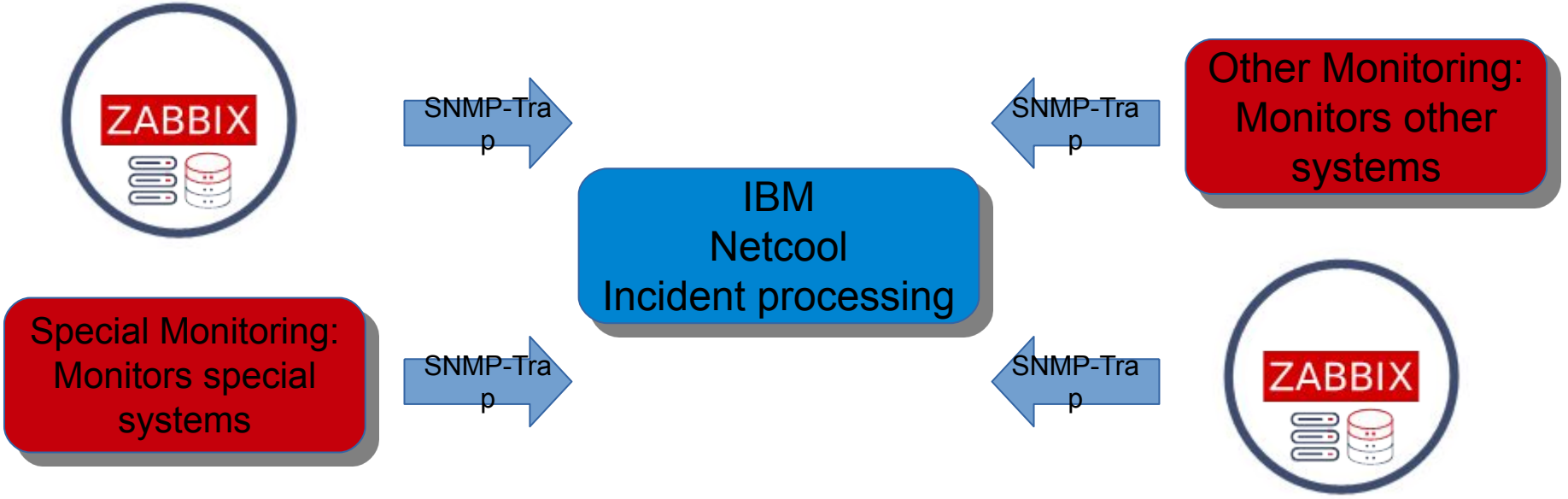
↔

IBM Netcool

ZABBIX TRAINING PARTNER

IntelliTrend IT-Services

The Clever and the Cool
Design and Implementation

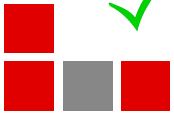


All involved monitoring systems send their alerts via SNMP Traps

The Clever and the Cool
Design and Implementation

Advantages

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

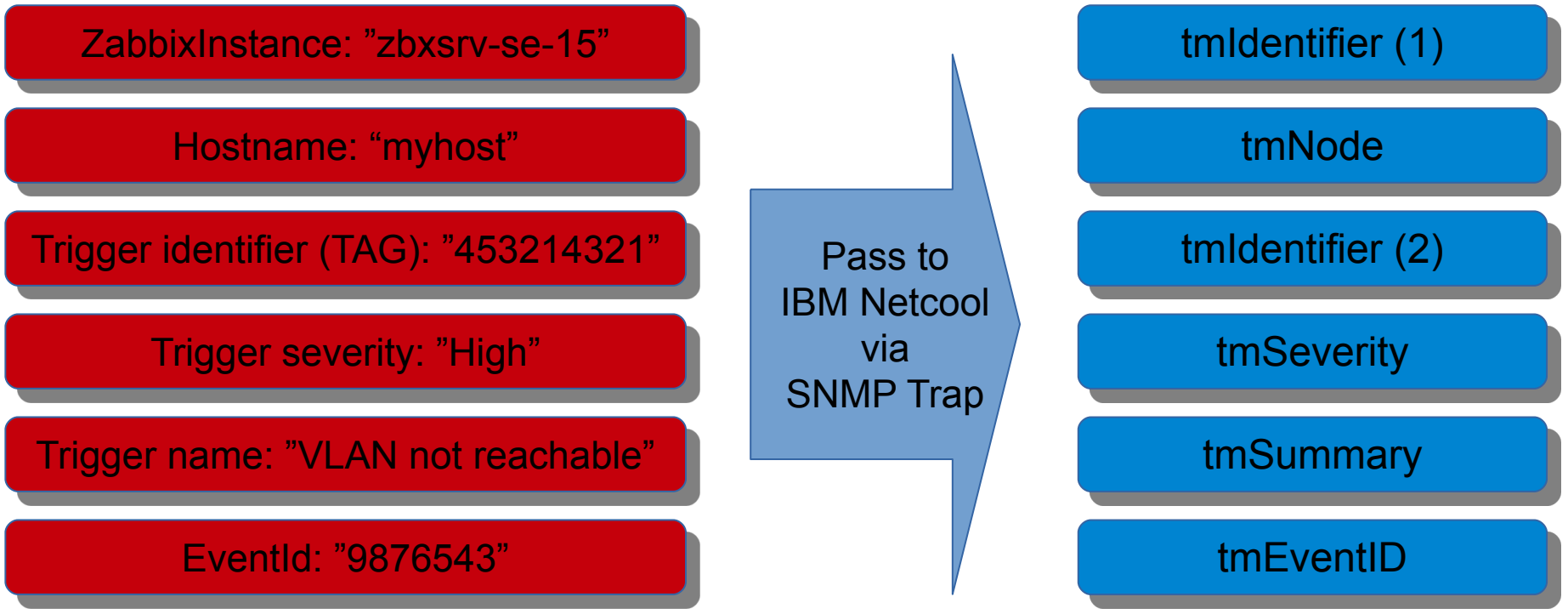


Design Considerations

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

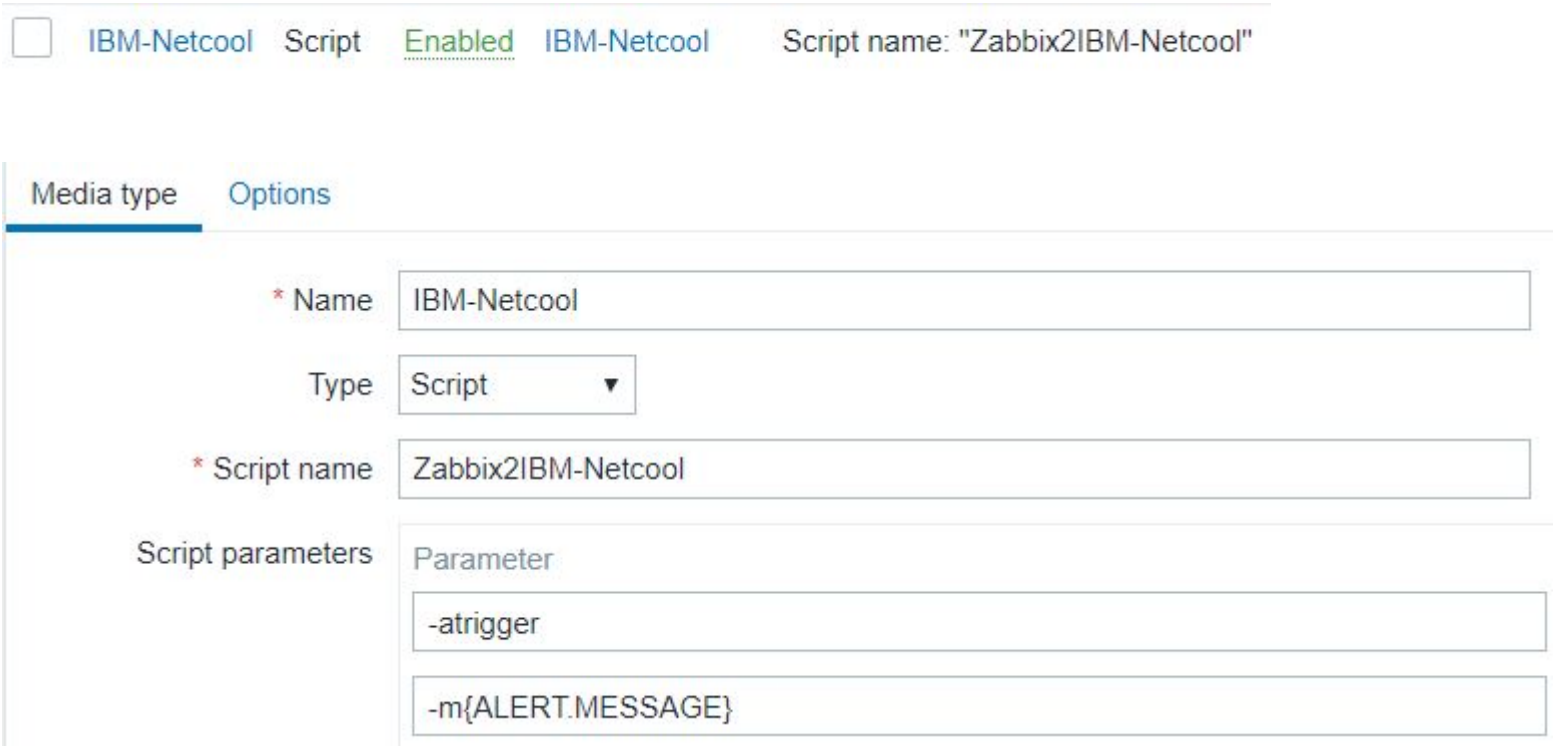


There are more fields involved ...

The Clever and the Cool
Design and Implementation

Implementation

The Clever and the Cool
Design and Implementation - Media



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: ☑

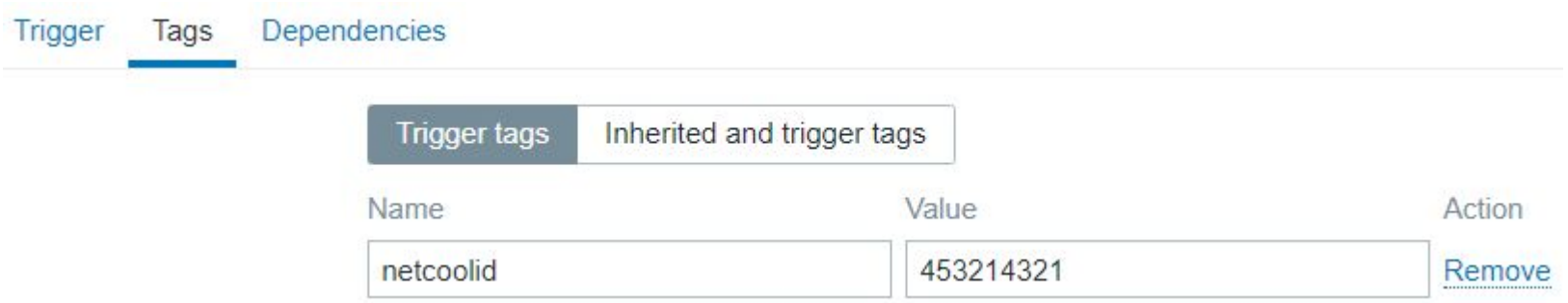
Operations

Steps	Details	Start in	Duration
1	**Send message to users:** IBM-Netcool via IBM-Netcool	Immediately	Default

ZABBIX TRAINING PARTNER

IntelliTrend IT-Services

The Clever and the Cool
Design and Implementation - Trigger



The Clever and the Cool
Design and Implementation

Resulting SNMP Trap send from Zabbix to IBM-Netcool

ZABBIX TRAINING PARTNER

IntelliTrend IT-Services

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

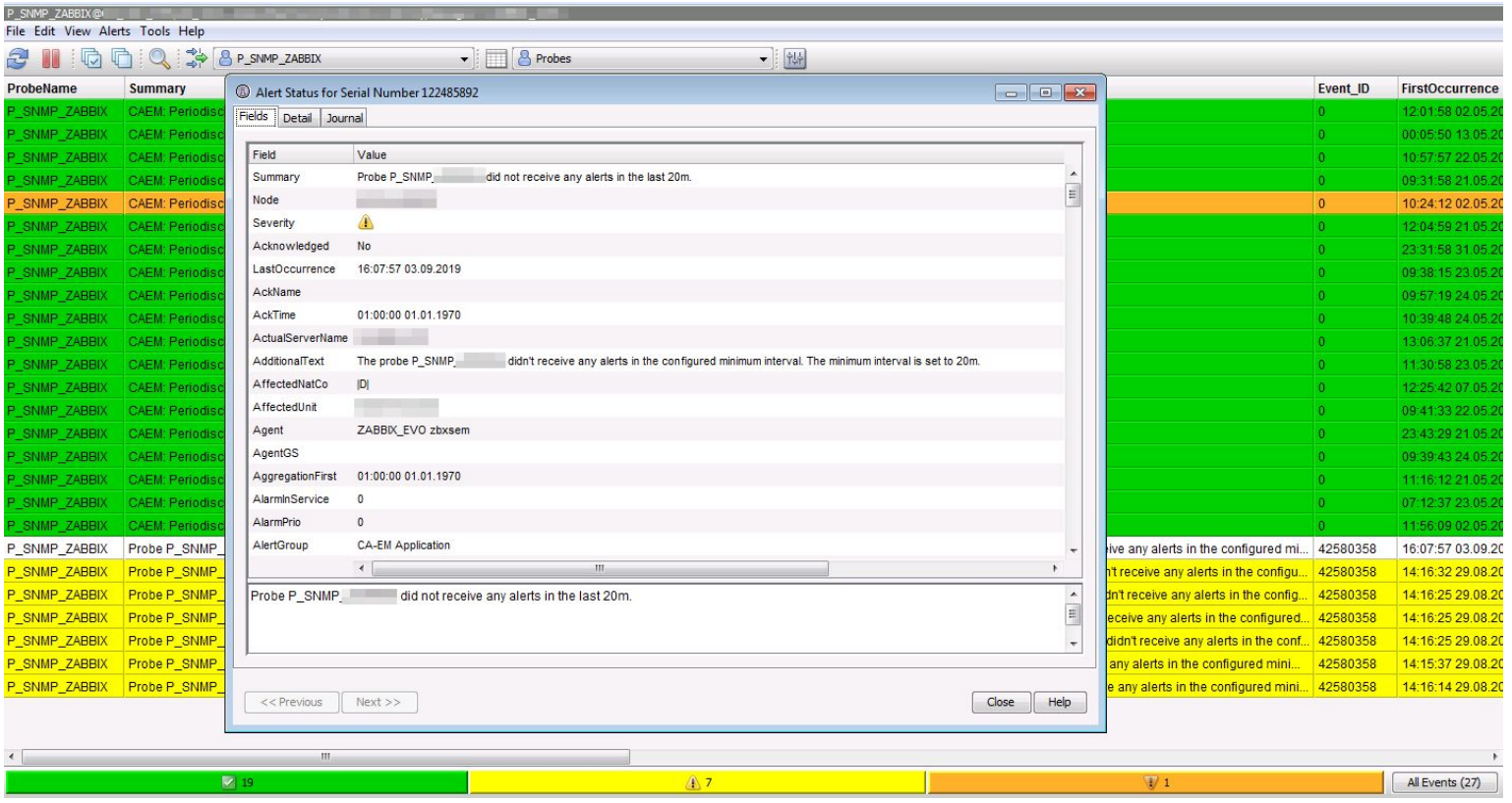
P_SNMP_ZABBIX | Probes

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[redacted])	ZABBIX_EVO	ZABBIX_EVO zbx[redacted]	ZABBIX_EVO_[redacted]_Heartbeat
P_SNMP_ZABBIX	CAEM: Periodischer Heartbeat Zabbix Evolution (zbx-[redacted])	ZABBIX_EVO	ZABBIX_EVO zbx-[redacted]	ZABBIX_EVO_zbx-[redacted]_Heartbeat
P_SNMP_ZABBIX	CAEM: Periodischer Heartbeat Zabbix Evolution (zbx[redacted])	ZABBIX_EVO	ZABBIX_EVO zbx[redacted]	ZABBIX_EVO_zbx[redacted]_Heartbeat
P_SNMP_ZABBIX	CAEM: Periodischer Heartbeat Zabbix Evolution (zbx_[redacted]	ZABBIX_EVO	ZABBIX_EVO zbx[redacted]	ZABBIX_EVO_zbx_[redacted]_Heartbeat

Alarms …

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

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