

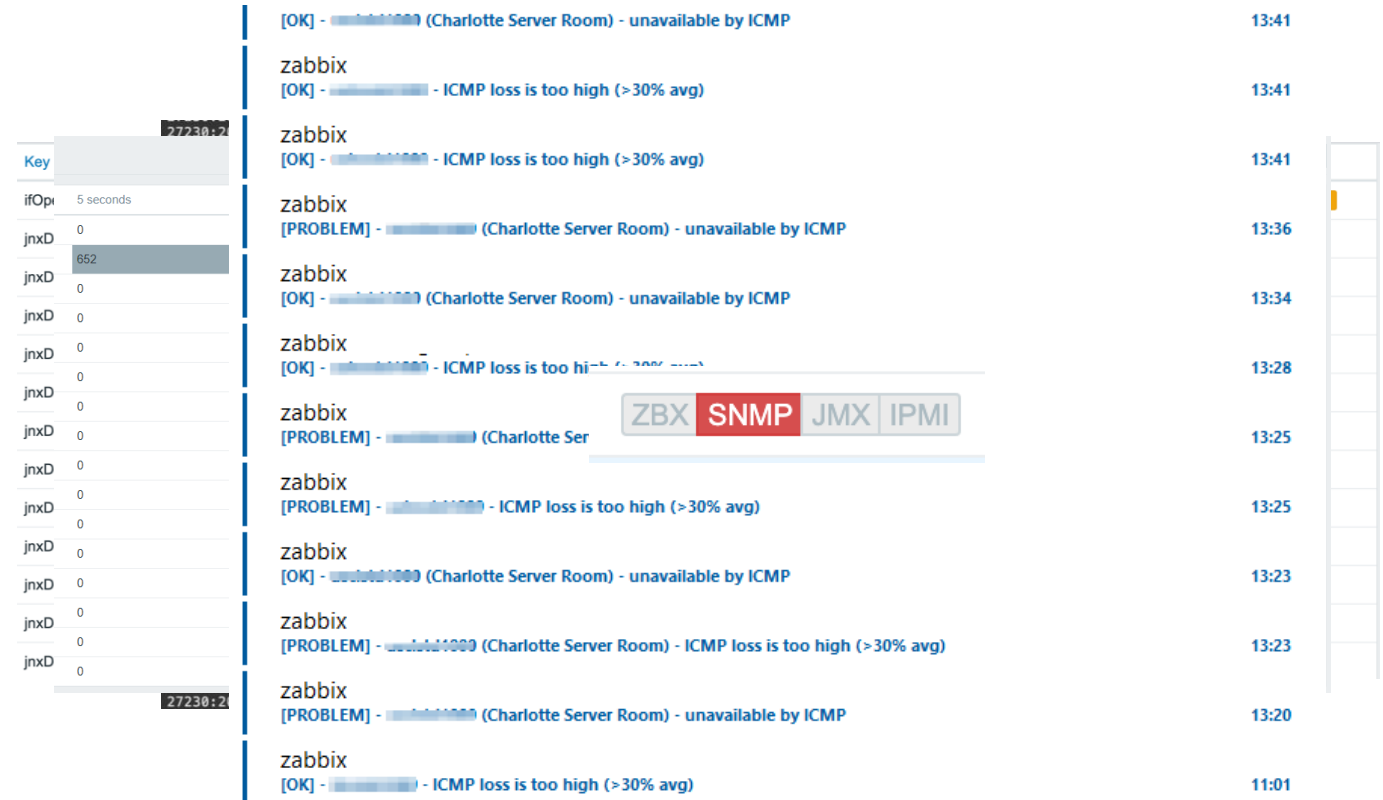
Managing complexity in Zabbix installations with Splunk



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**

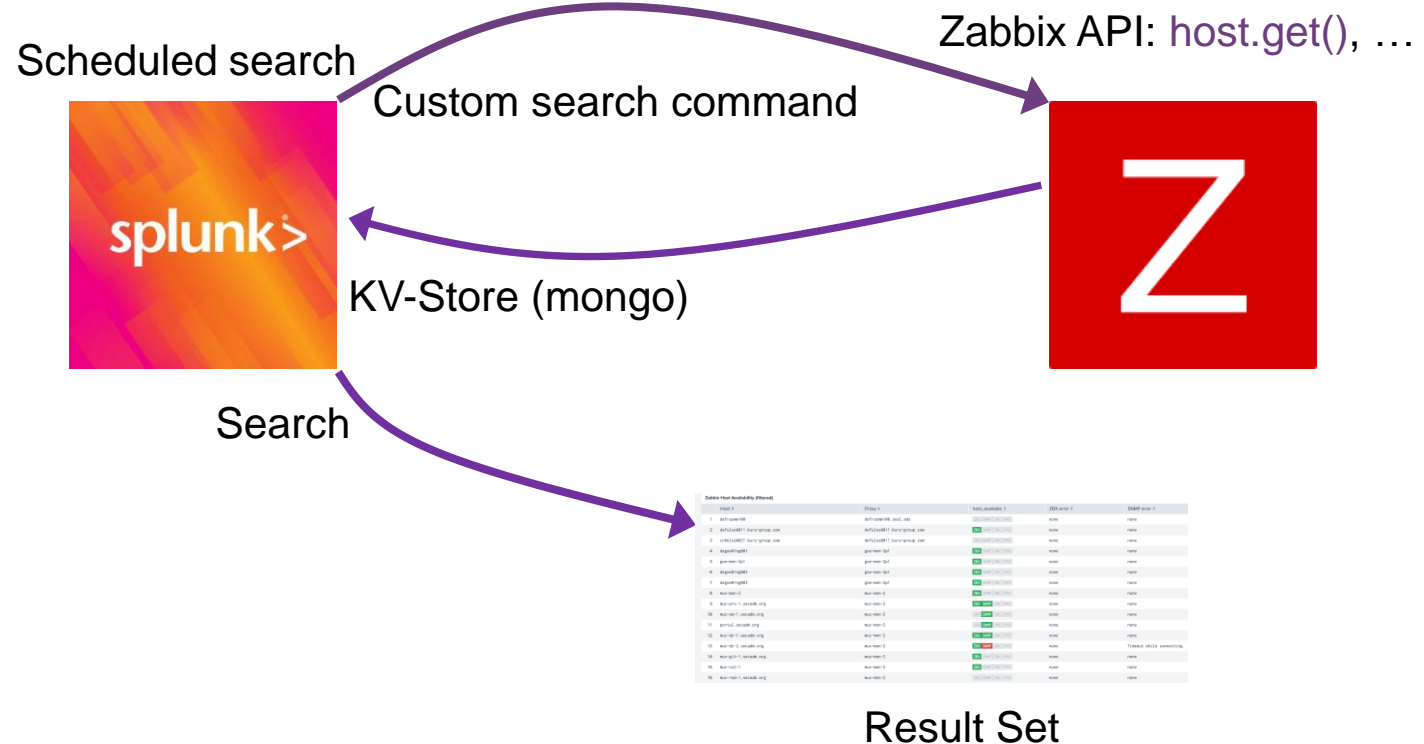


- Data Sources depending on use case
 - Indexed data
 - Lookups backed by Key-Value store
 - Scripted lookups
 - Custom Search commands



Zabbix entity **inventory**

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



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
-

Linux Metrics - Performance by Host

Host: Zabbix server

Time: Last 24 hours

Submit Hide Filters

Media types

Media type Message templates 7 Options

Name: Splunk HEC - PROBLEM

Type: Webhook

Name	Value	Action
action_id	{ACTION.ID}	Remove
action_name	{ACTION.NAME}	Remove
event_ack_status	{EVENT.ACK.STATUS}	Remove
event_age	{EVENT.AGE}	Remove
event_date	{EVENT.DATE}	Remove
event_duration	{EVENT.DURATION}	Remove
event_id	{EVENT.ID}	Remove
event_name	{EVENT.NAME}	Remove
event_object	{EVENT.OBJECT}	Remove
event_opdata	{EVENT.OPDATA}	Remove
event_recovery_date	{EVENT.RECOVERY.DATE}	Remove
event_recovery_id	{EVENT.RECOVERY.ID}	Remove
event_recovery_name	{EVENT.RECOVERY.NAME}	Remove
event_recovery_status	{EVENT.RECOVERY.STATUS}	Remove
event_recovery_tagsjson	{EVENT.RECOVERY.TAGSJSON}	Remove

Number of processes

Number of running processes

Time: 10:00 PM Mon Oct 26 2020 to 10:00 PM Tue Oct 27 2020





The Zabbix Queue

Zabbix - Queue

Bearbeiten

Exportieren ▾

...

Group by

☐ Item type

☐ Endpoint

☐ Host

☐ Host Availability

☐ Item State

Ignore Hosts

☐ Unavailable

☐ Unknown

Group by

☒ Item type

☐ Endpoint

☐ Host

☐ Host Availability

☐ Item State

Ignore Hosts

☒ Unavailable

☒ Unknown

Details

Item_type ↕

count ▾

SNMPv2 agent

482

Zabbix agent

158

Zabbix agent (active)

24

SNMPv1 agent

17

simple check

1

CPU busy time

Zabbix agent

00:00:00

1m

not supported

ZBX

SNMP

JMX

IPMI

normal

Free inodes on \$1 (percentage)

Zabbix agent

00:00:06

1m

not supported

ZBX

SNMP

JMX

IPMI

normal

CPU iowait time

Zabbix agent

00:00:06

1m

not supported

ZBX

SNMP

JMX

IPMI

normal

System IP Addresses

Zabbix agent

00:00:06

10m

not supported

ZBX

SNMP

JMX

IPMI

not supported

Matches in Category \$1

SNMPv3 agent

00:00:06

1m

not supported

ZBX

SNMP

JMX

IPMI

normal

Free swap space

Zabbix agent

00:00:06

1m

not supported

ZBX

SNMP

JMX

IPMI

normal

Processor load (15 min average per core)

Zabbix agent

00:00:06

1m

not supported

ZBX

SNMP

JMX

IPMI

normal

« Prev

1

2

3

4

5

6

7

8

9

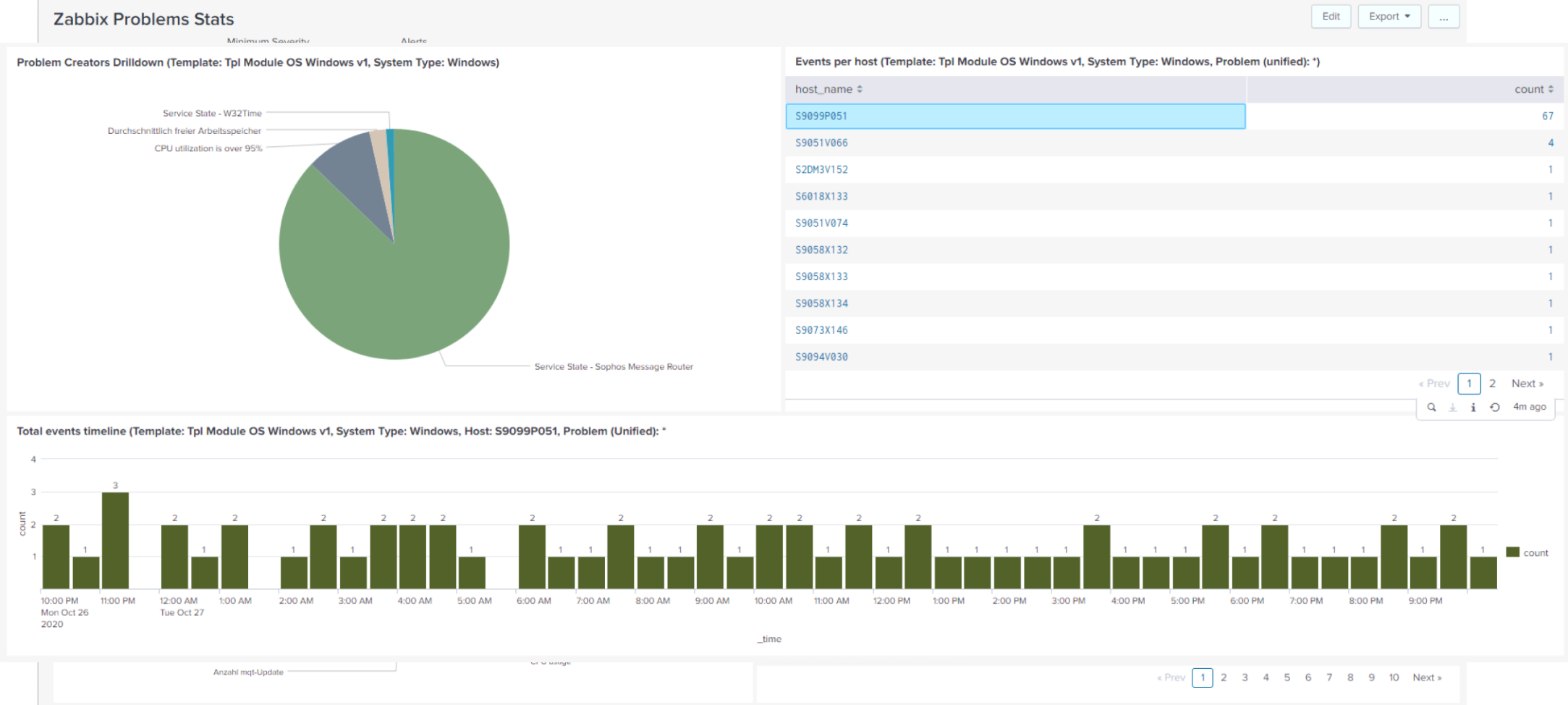
10

Next »

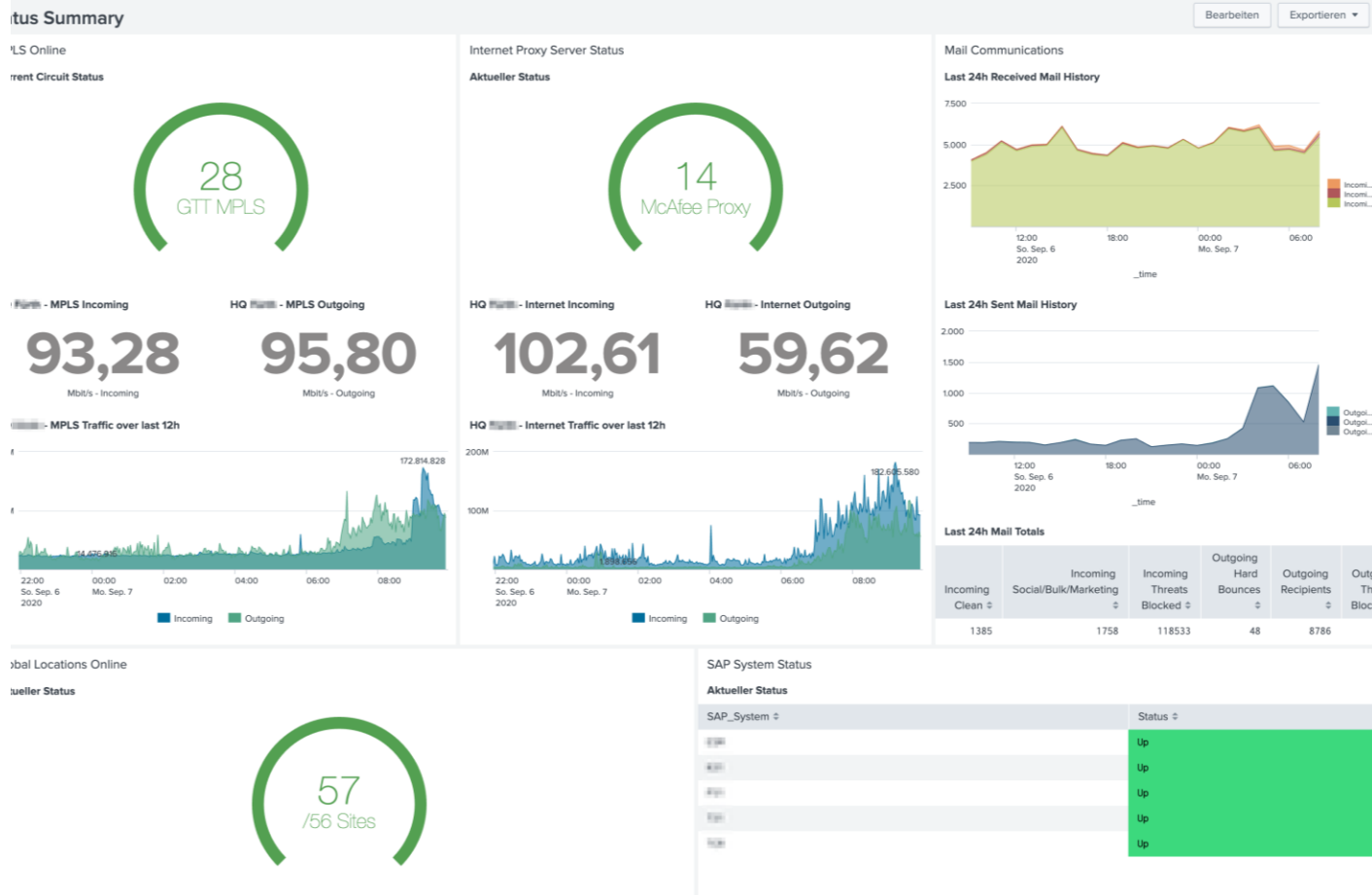
Skype



Zabbix Problem Analytics



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

Sponsor Rooms		
		
🕒 10:00 - 22:00	🕒 10:00 - 22:00	
		
🕒 10:00 - 22:00	🕒 10:00 - 22:00	
		
🕒 10:00 - 22:00	🕒 10:00 - 22:00	
		
🕒 10:00 - 22:00	🕒 10:00 - 22:00	
		
🕒 10:00 - 22:00	🕒 10:00 - 22:00	

