ZABBIX '25

CONFERENCE

GERMANY

From Alert to Action: A Unified Monitoring with Zabbix, Grafana & ServiceNow

5Ŝ&Ωαω·ΊΨŜΩ

IT Operations Specialist, netpoint GmbH

Agenda

▶ Challenge: Alert Routing

▶ Integration Framework
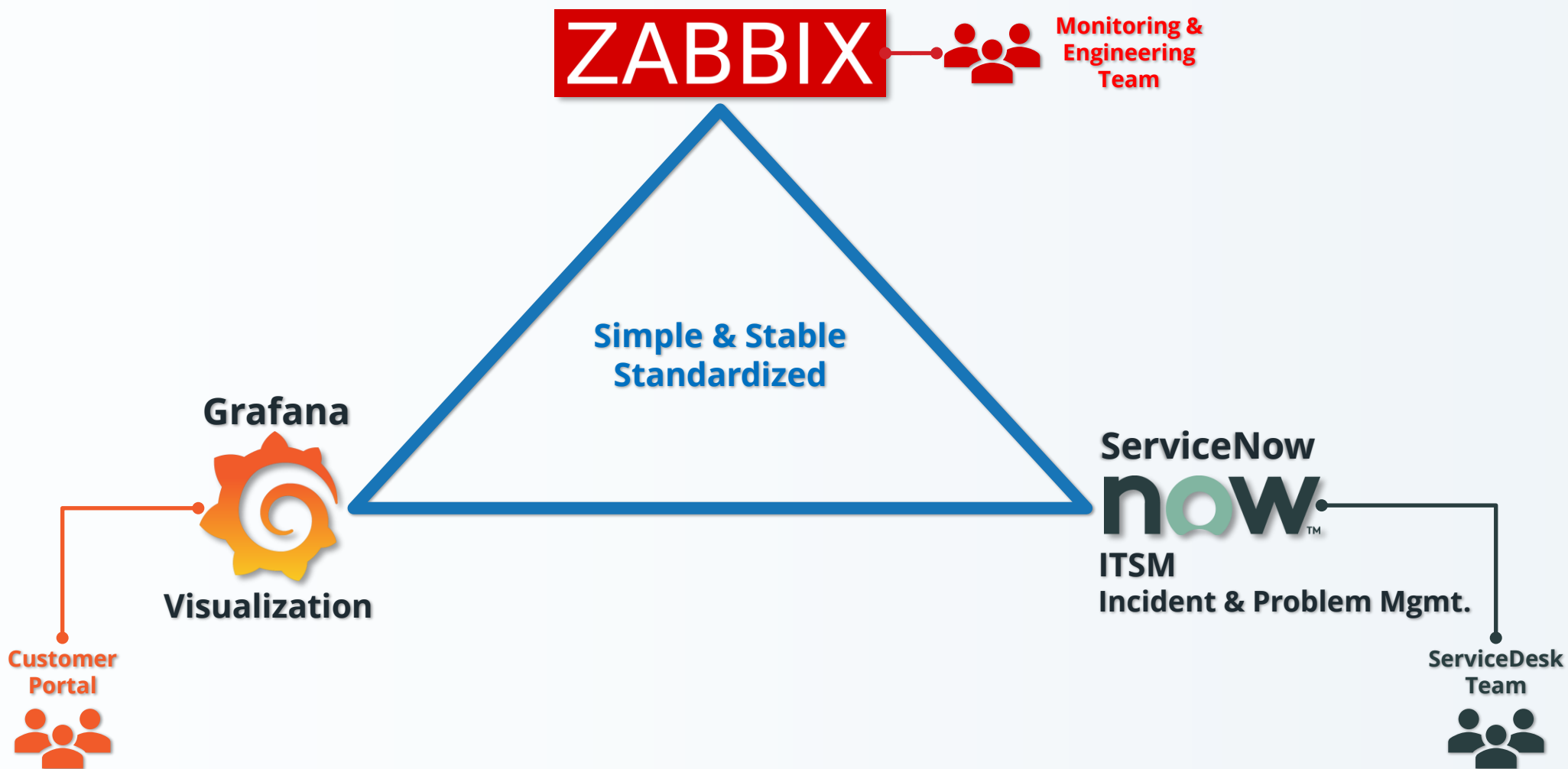
▶ Our Infrastructure

▶ Customer View

▶ One more thing

Who am I?

5 Ŝœœ˞aɯ·ɪΨŜΩ

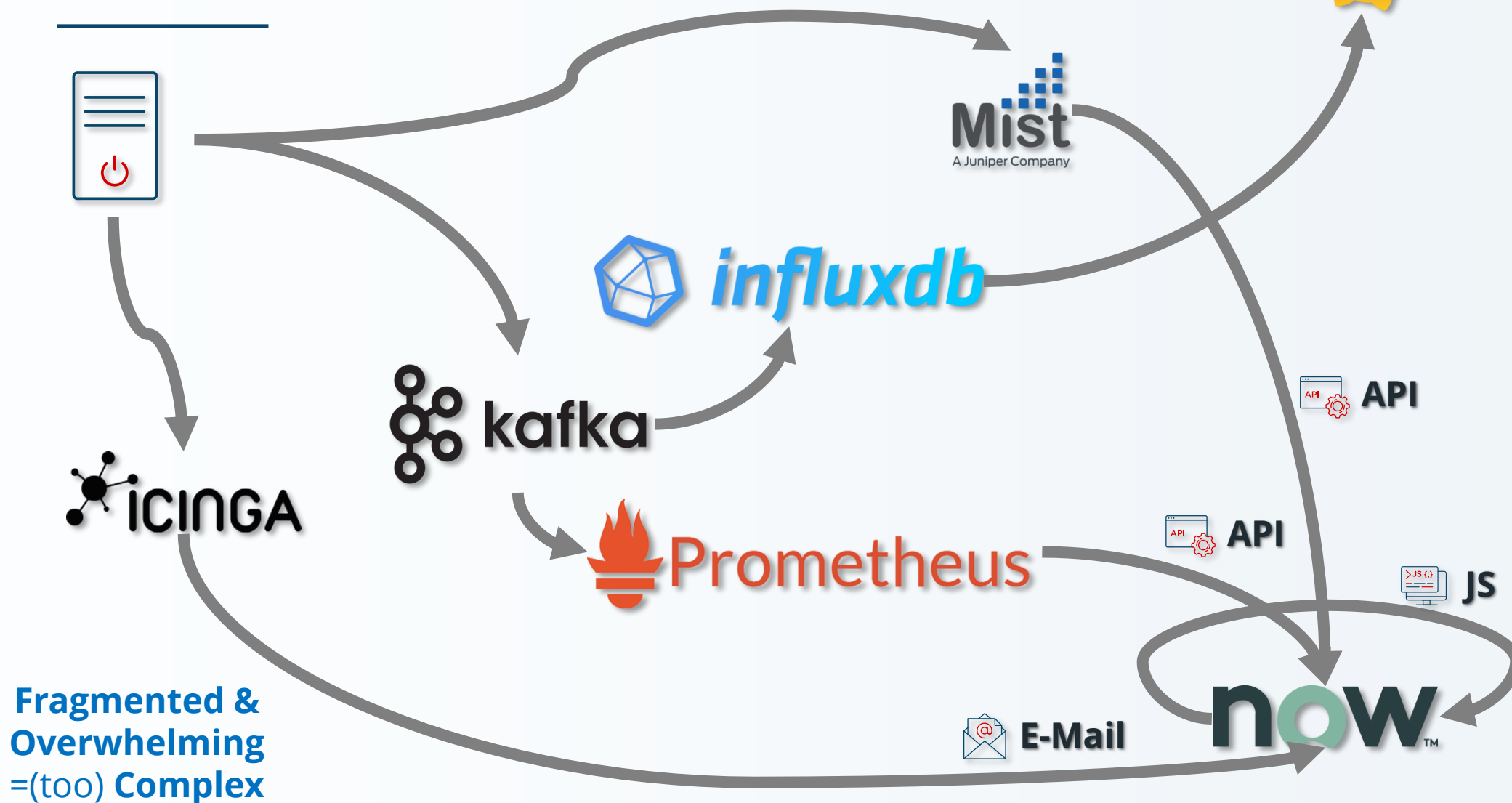IT Operations Specialist,
netpoint GmbH

ƌœ‐ŜŘœ˷Ψũœ˷Řˆœˑ೨˦·ɪΨŜΩ

°ฒɪɾฮ˷Ψũ˷ŘŜˆœฒ˦·ɪΨŜΩ

netpoint.

innovation technology.
Datacenter • Endpoint • Cloud

Challenge: Alert Routing

Fragmented &
Overwhelming
=(too) Complex

ZABBIX '25
CONFERENCE
GERMANY

4

Integration Framework

ZABBIX — Monitoring & Engineering Team

Simple & Stable Standardized

Grafana — Visualization — Customer Portal

ServiceNow — ITSM Incident & Problem Mgmt. — ServiceDesk Team

Core Zabbix Components
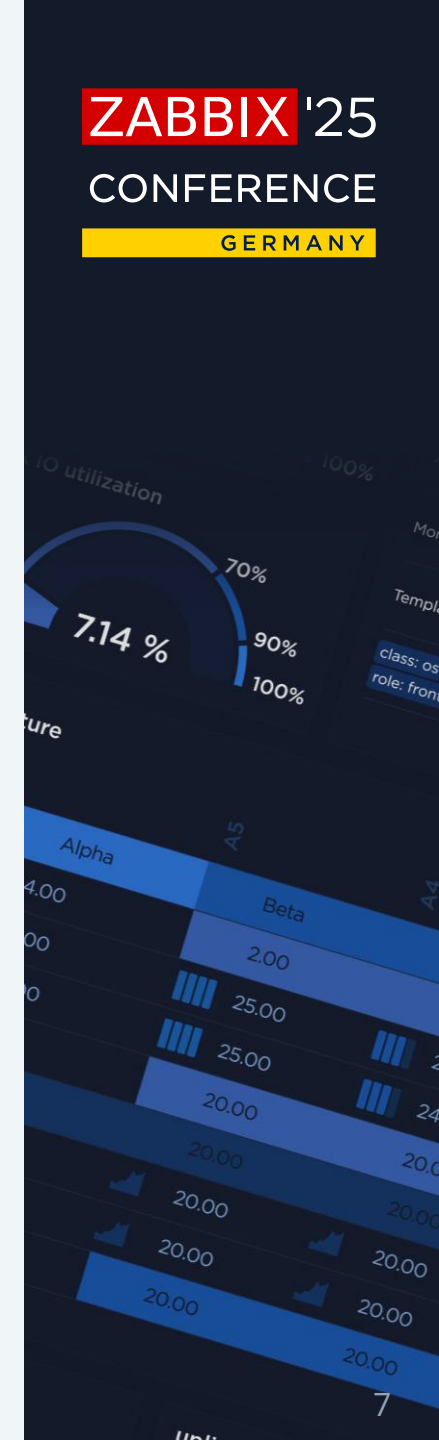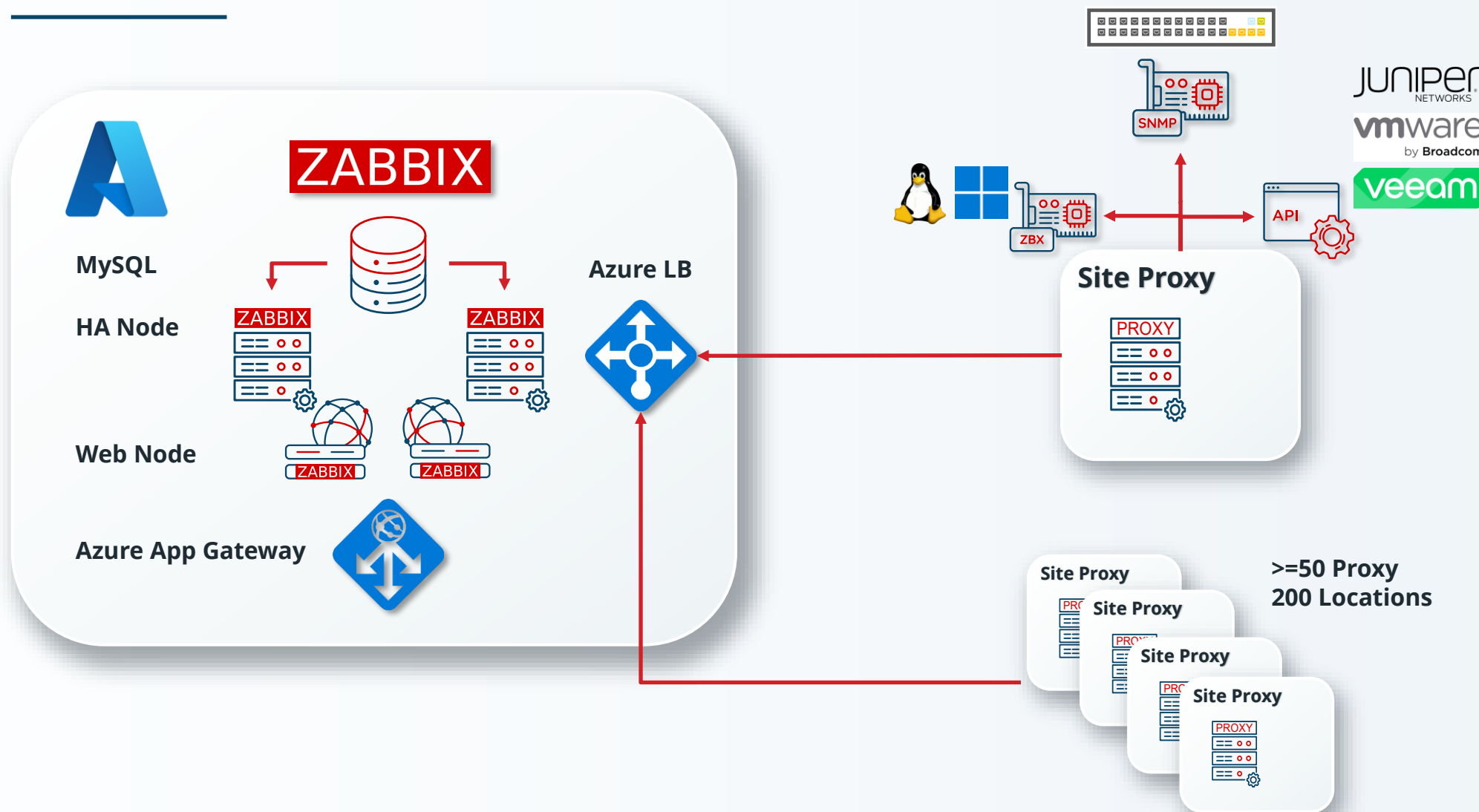
Alerting

servicenow

Custom ServiceNow REST API

for incident handling

ZABBIX
Problem ID

ZABBIX

Time	User/Recipient	Action	Message/Command	Status
2025-04-27 11:58:16 AM	svc_servicenow (ServiceNow)	✉	ServiceNow Netpoint	Sent
2025-04-27 11:58:15 AM				

Trigger details

Host	APP01.
Trigger	Windows: High CPU utilization (over 95% for 20m)
Severity	Warning
Problem expression	min(,5m)>90
Recovery expression	
Event generation	Normal
Allow manual close	Yes
Enabled	Yes

Number	INC0331
Correlation display	5062723
∗ Caller ⊘	Event Management Netpoint
∗ Company ⊘	
Location ⊘	MEX
∗ Category ⊘	Datacenter
∗ Subcategory ⊘	Server
∗ Service ⊘	Central Service - ■ - Datacenter
Service offering	
Configuration item ⊘	APP01.
∗ Short description ⊘	[RESOLVED] Windows: High CPU utilization (over 95% for 20m)

Monitoring Alert

Problem Started At	08:25:36 on 03.05.2025
Problem Name	Windows: High CPU utilization (over 95% for 20m)
Host	APP01.
Severity	Warning
Operational Data	Current utilization: 100 %
Original Problem ID	5062723
Knowledge Base Article	KB0012851

8

Bi-Directional Status Updates

- Status updates in SNOW reflect in Zabbix
- Acknowledgements in Zabbix are added to the incident as comments

Host Sync

- ServiceNow hosts using the "**Monitoring**" flag in the CMDB for syncing

- Import of hosts to Zabbix "Discovered Hosts"

- Import hosts from Zabbix inventory into SNOW CMDB

- Host GUID saved in Zabbix inventory

servicenow

Name ❓
APP01.▮▮▮▮

Asset ❓
AT0079▮▮▮ ⓘ

✳ Company ❓
▮▮▮▮▮▮▮▮ 🔍 ⓘ

Class
Server ⌄

Is Virtual
☑

Serial number ❓
VMWARE-52 fb 4b 6f 07 59 79-▮▮▮

ZABBIX

| Serial number A | VMware-42 32 2a 8b cc e7 ▮▮▮ |
| Serial number B | 1d41899ac3c765765b4321f05013102 |

10

Why Zabbix?

- **Central** item and template config
- Configurable **without Linux** knowledge
- **Easily** configurable alert parameters
- **Reliable** deadman checks and actions
- Trackable **problem IDs**
- Supported **Grafana** plugin

Customer View

Grafana Integration

Grafana Customization Cheat-sheet

Categories of customization commands

Configuration	Cleaning	Visual	Hands-On

What do the commands do

update configuration defaults	remove unused plugin files	replace SVG files	update JS, HTML code

https://shorturl.at/wrWQs

np.

Welcome to nView

Sign in with Entra ID

- Entra ID login
- Fully custom docker image
- Azure MySQL as storage

RBAC

- Customer separation via organizations

- Location separation via teams

Dashboards

One more thing

AI

Disk IO utilization

90%
100%

0%
70%
7.14 %
90%
100%

Temperature

Items A1

D1
A2   Alpha   A5
B1   14.00
B2   21.00   Beta
A1   25.00   2.00   Gamma
A3   25.00   19.00   Delta
C1   20.00   25.00   24.00   89.00
C2   20.00   20.00   24.00   23.00
A1   20.00   20.00   20.00   23.00
                        20.00   20.00   20.00
                        20.00   20.00   20.00
                                       20.00   20.00
                                       20.00

uplink: outgoing

2.12 Kbps

...und Reckoner

Availability

ZBX   SNMP

Monitored by

Templates   Nebula

Linux by Za..., Nebula
Template w..., Zabbix serv...,
class: os class: software environment: product
role: frontend target: linux target: server

AI-Powered Knowledge Base

- Why generate KB Articles:
  - General information online available
  - **Conquer the flood**
  - Create a starting point
- More potential in the future
  - Escalation matrix
  - Reference existing articles
  - **Local models**

27

Customized Templates

206

Active Triggers

OpenAI Model Workflow

Titel, Description, Expression

Prompt

```
prompt = (
    f"You are a helpful assistant with knowledge of Zabbix triggers."
    f"Use your own knowledge about '{trigger_name}' from the template '{template_name}'. "
    f"Dont mention the template or trigger name in the content."
    f"Below is an existing HTML template for a ServiceNow Knowledge article:\n"
    f"{base_html}\n\n"
    "Please produce a final, refined HTML article that includes:\n"
    " - Explanation of what this Zabbix trigger does\n"
    " - Potential Steps for the first level to take before escalating to second lvl, keep i
    " - Escalation, the agent already has a ticket from that trigger so it should be send t
    " - Dont add anything to the Special cases section, this is done manually later on.\n"
    "Return only valid HTML (no markdown) and keep the original structure and design just u
)
```

HTML-Template

```
1 > <style>...
27    </style>
28
29    <div class="section">
30        <h4>Description</h4>
31        <p>This trigger is activated when ...</p>
32    </div>
33
34    <div class="section">
35        <h4>Potential Steps</h4>
36        <ul>
37            <li>Check ...</li>
38            <li>Identify ...</li>
39        </ul>
40    </div>
41
42    <div class="section">
43        <h4>Escalation</h4>
44        <ul>
45            <li>Escalate to Second Level support for ...</li>
46            <li>On-Call support ..</li>
47        </ul>
48    </div>
```

ServiceDesk Team

Monitoring & Engineering Team

AI-Powered Knowledge Base

General information →

Internal escalation matrix →

Teams add more information →

Windows: High memory utilization

KB0012842

☆☆☆☆☆   1 Views

Description

This trigger is activated when the system's memory utilization exceeds a defined threshold, indicating that the host is running low on available memory. This can impact system performance and may be caused by memory leaks, heavy application usage, or insufficient hardware resources.

Potential Steps

- Check the memory usage graph, is this a one time problem or accours more often.
- Check the host criticality is it a domain controller or otherwise critical to the infrastructure.

Escalation

- Escalate to 2nd lvl for further investigation.
- It is generally not needed to inform OnCall!

Special Cases

- **Industry PC:** Local IT must assess and address any hardware limitations or local software causing memory pressure.

AI-Powered Knowledge Base

Windows: High memory utilization

KB0012842

☆☆☆☆☆   40 Views

Description

This trigger is activated when the system's memory utilization exceeds a defined threshold, indi
on available memory. This can impact system performance and may be caused by memory lea
insufficient hardware resources.

Potential Steps

- Check the memory usage graph, is this a one time problem or accours more often.
- Check the host criticality is it a domain controller or otherwise critical to the infrastructure

Escalation

- Escalate to 2nd lvl for further investigation.
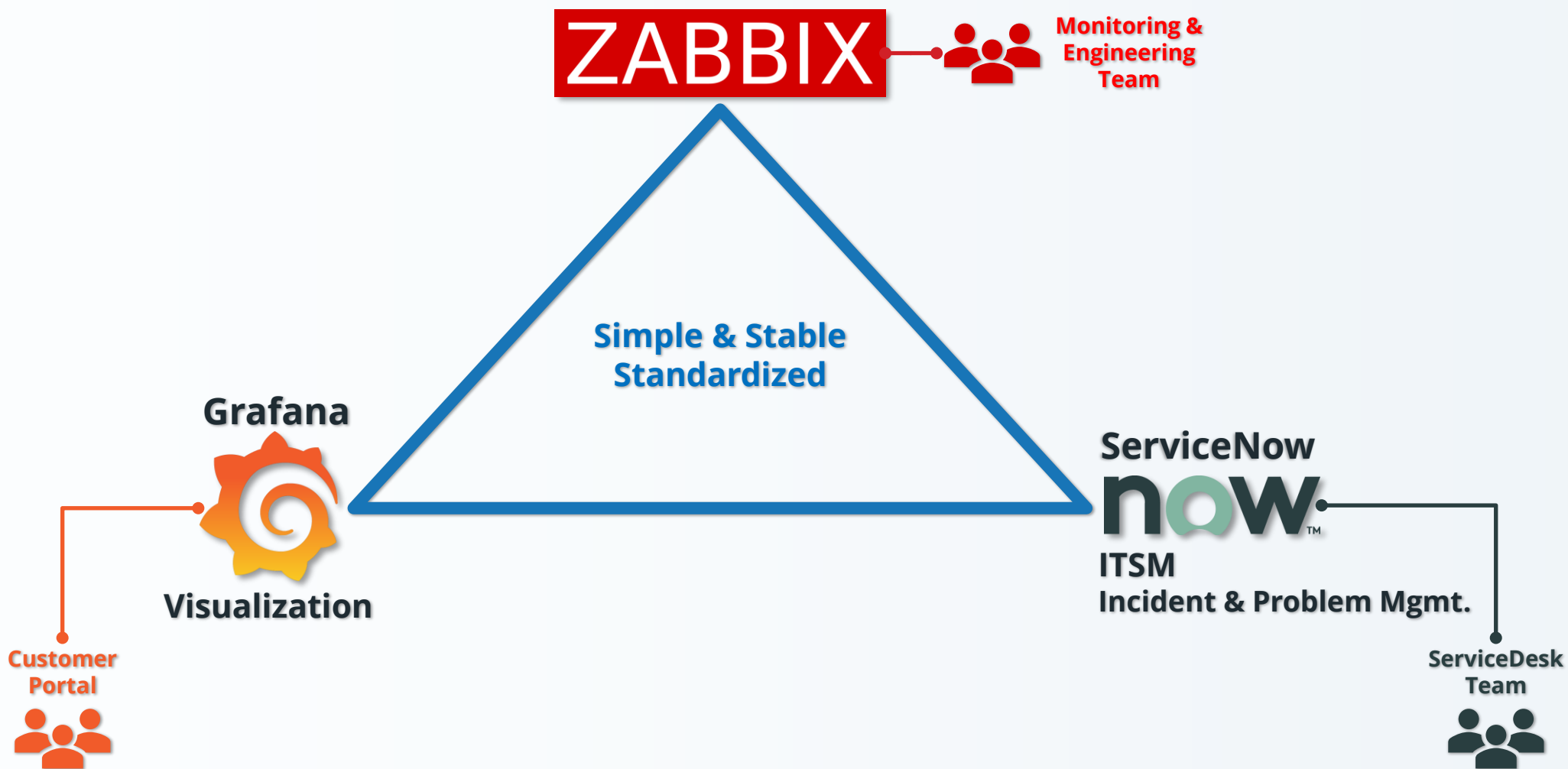- It is generally not needed to inform OnCall!

Special Cases

- Industry PC: Local IT must assess and address any hardware limitations or local software causing memory pressure.

```html
1 > <style>...
27   </style>
28
29   <div class="section">
30       <h4>Description</h4>
31       <p>This trigger is activated when ...</p>
32   </div>
33
34   <div class="section">
35       <h4>Potential Steps
36       <ul>
37           <li>Check ...</
38           <li>Identify ..
39       </ul>
40   </div>
41
42   <div class="section">
43       <h4>Escalation</h4>
44       <ul>
45           <li>Escalate to
46           <li>On-Call sup
47       </ul>
48   </div>
49
50   <hr/>
51
52   <div class="section not
53       <h4 style="margin-t
54       <ul>
55           <li><span class
56       </ul>
57   </div>
```

```python
1   import requests
2   import sys
3   import urllib3
4   import re
5   import os
6   from openai import OpenAI
7
8   client = OpenAI(api_key="xxx")
9
10  # Disable warnings about insecure SSL/TLS connections
11  urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
12
13  # ------------------------
14  # Configuration
15  # ------------------------
16
17  # Set your OpenAI API key here or via environment variables
18
19  # Zabbix details
20  ZABBIX_API_URL = "https://mon.netxxxpoint.de/api_jsonrpc.php"
21  ZABBIX_USERNAME = "svc_import"
22  ZABBIX_PASSWORD = "xxx"
23  # The name of the Template Group you want to search (change as needed)
24  TEMPLATE_GROUP_NAME = "Netpoint"
25
26  # ServiceNow details
27  SERVICENOW_INSTANCE = "https://xxx.service-now.com"
28  SERVICENOW_USERNAME = "svc_sn_zabbix"
29  SERVICENOW_PASSWORD = "xxx"
30  SERVICENOW_KB_ID = "xxx"
31  SERVICENOW_CATEGORY_ID = "xxx"
32  SERVICENOW_KB_AUTHOR_ID = "xxx"  # Author ID for the KB article (Dennis Rahmen)
33
34  # Name of local HTML file containing article content (must be in the same folder as script)
35  HTML_FILE_NAME = "article_content.html"
36
37  # ------------------------
38  # Zabbix API Function
39  # ------------------------
```

21

Integration Framework

ZABBIX — Monitoring & Engineering Team

Simple & Stable Standardized

Grafana — Visualization — Customer Portal

ServiceNow — ITSM — Incident & Problem Mgmt. — ServiceDesk Team