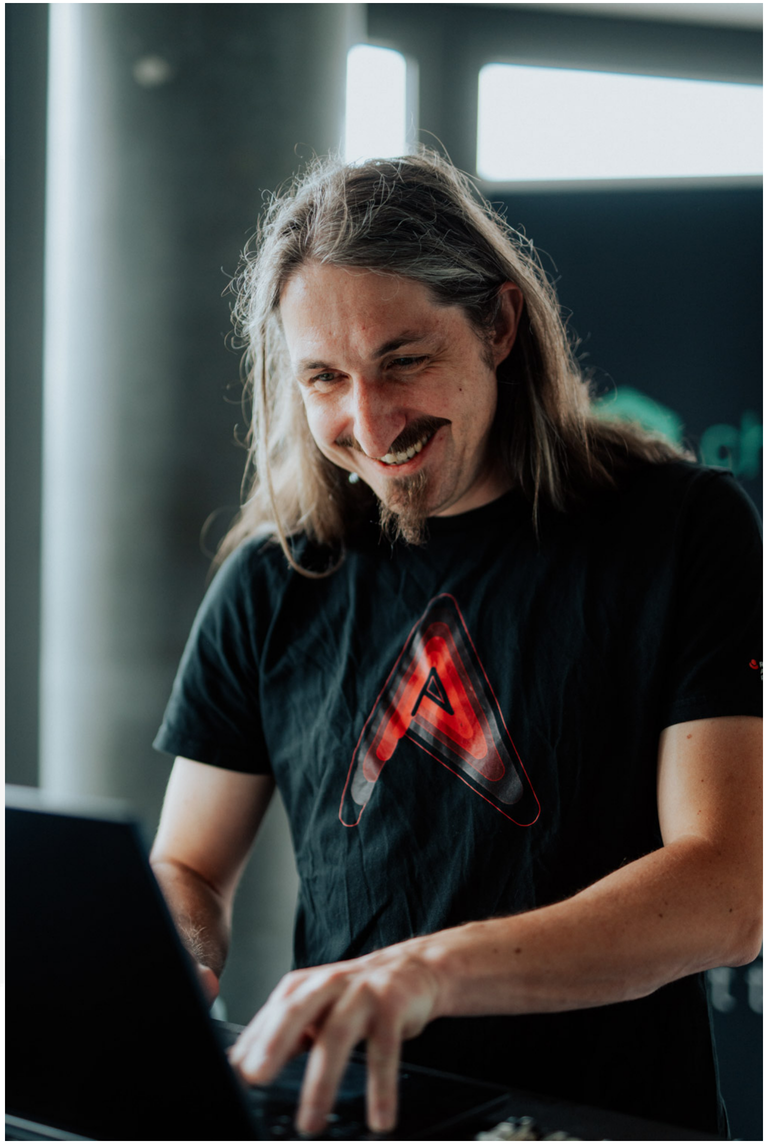
Self-healing with Checkmk and Event-Driven Ansible

How to resolve issues automatically

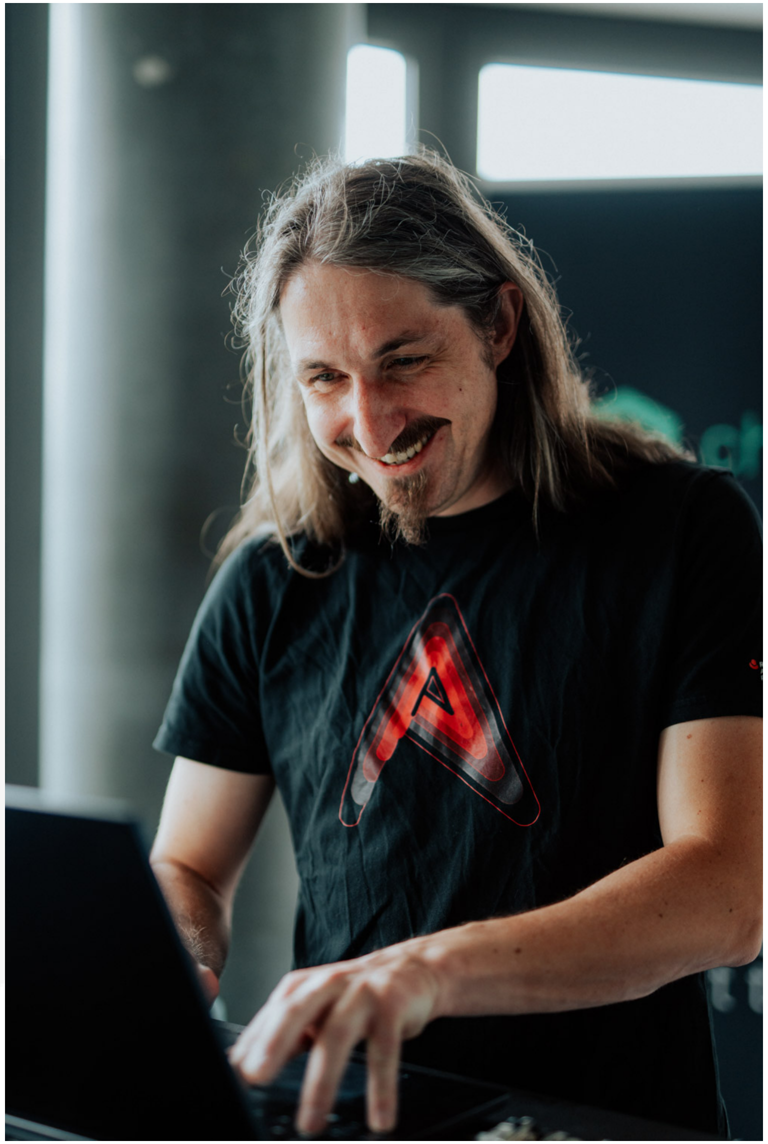
About me

- René Koch
- Self-employed consultant for:
    - Red Hat Ansible (Automation Platform)
    - Red Hat Enterprise Linux
    - Red Hat Satellite
    - Red Hat Identity Management (IPA)
- Experienced monitoring user (Nagios, Icinga, Checkmk)



About me

- René Koch
    - rkoch@rk-it.at
    - +43 660 / 464 0 464
    - https://www.linkedin.com/in/rk-it-at
    - https://github.com/rk-it-at
    - https://github.com/scrat14



Agenda

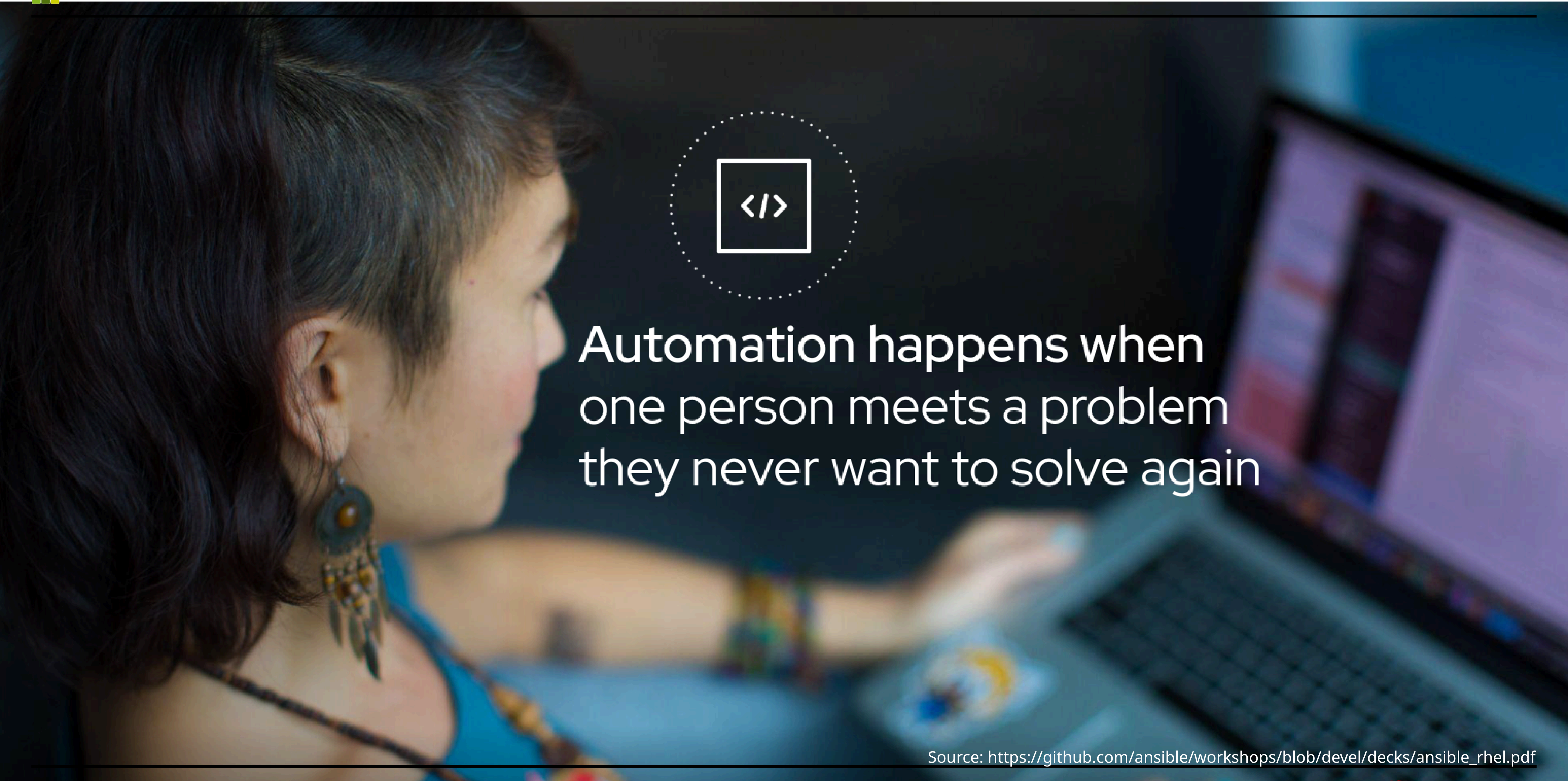
- Monitoring: the past and the present
- What is Checkmk?
- What is Event-Driven Ansible (EDA)?
- Event-Driven Workflow
- Use cases and best practices
- (Live Demonstration)

Monitoring: the past and the present

- 🕰️ 2005: Received email alerts from Nagios 2 for issues with Solaris machines
- 🧩 Manual workflow:
  - 📩 Read email
  - 🔐 Log in to the system
  - 🔎 Check if issue still exists
  - 🛠️ Fix the issue
  - 🤬 **Repeat the same procedure over and over again**

Monitoring: the past and the present

- 🤖 Today: Use EDA to decide if issues can be fixed with Ansible
- ⚡ Automated workflow:
  - 🧠 EDA analyzes the issue
  - 🚀 Triggers an AAP template if it can be fixed
  - 🧾 Ansible playbook solves the issue
  - 🙋 Handle only exceptional issues manually

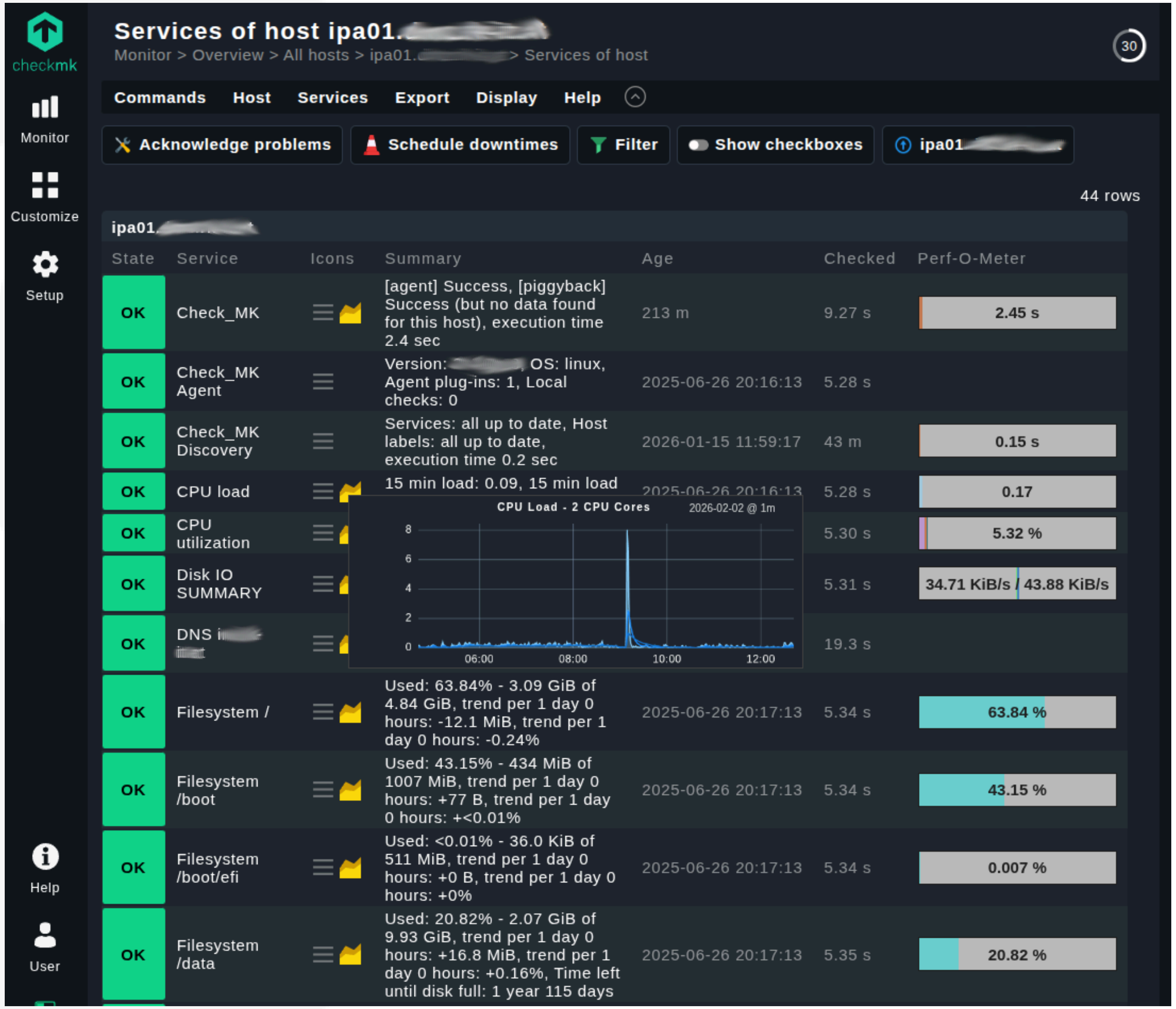


Automation happens when one person meets a problem they never want to solve again

Source: https://github.com/ansible/workshops/blob/devel/decks/ansible_rhel.pdf

What is Checkmk?

- **Monitoring platform** for infrastructure, applications and services
- Provides **agent- and agentless** checks, dashboards, and alerting
- Built for **scale** with distributed monitoring and automation support
- Helps **detect, analyze, and remediate** issues faster



Services of host ipa01.[redacted]

Monitor > Overview > All hosts > ipa01.[redacted] > Services of host

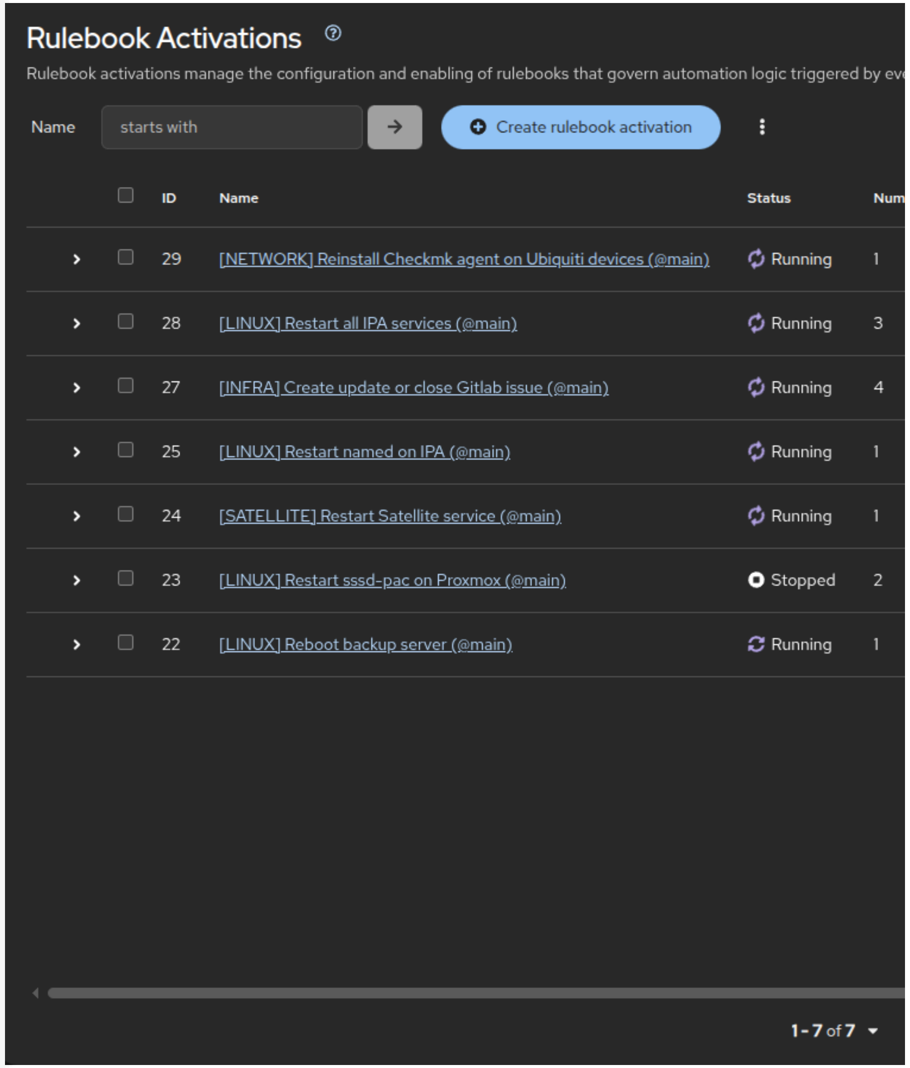
44 rows

ipa01[redacted]

State	Service	Icons	Summary	Age	Checked	Perf-O-Meter
OK	Check_MK		[agent] Success, [piggyback] Success (but no data found for this host), execution time 2.4 sec	213 m	9.27 s	2.45 s
OK	Check_MK Agent		Version: [redacted], OS: linux, Agent plug-ins: 1, Local checks: 0	2025-06-26 20:16:13	5.28 s	
OK	Check_MK Discovery		Services: all up to date, Host labels: all up to date, execution time 0.2 sec	2026-01-15 11:59:17	43 m	0.15 s
OK	CPU load		15 min load: 0.09, 15 min load	2025-06-26 20:16:13	5.28 s	0.17
OK	CPU utilization				5.30 s	5.32 %
OK	Disk IO SUMMARY				5.31 s	34.71 KiB/s / 43.88 KiB/s
OK	DNS i[redacted]				19.3 s	
OK	Filesystem /		Used: 63.84% - 3.09 GiB of 4.84 GiB, trend per 1 day 0 hours: -12.1 MiB, trend per 1 day 0 hours: -0.24%	2025-06-26 20:17:13	5.34 s	63.84 %
OK	Filesystem /boot		Used: 43.15% - 434 MiB of 1007 MiB, trend per 1 day 0 hours: +77 B, trend per 1 day 0 hours: +<0.01%	2025-06-26 20:17:13	5.34 s	43.15 %
OK	Filesystem /boot/efi		Used: <0.01% - 36.0 KiB of 511 MiB, trend per 1 day 0 hours: +0 B, trend per 1 day 0 hours: +0%	2025-06-26 20:17:13	5.34 s	0.007 %
OK	Filesystem /data		Used: 20.82% - 2.07 GiB of 9.93 GiB, trend per 1 day 0 hours: +16.8 MiB, trend per 1 day 0 hours: +0.16%, Time left until disk full: 1 year 115 days	2025-06-26 20:17:13	5.35 s	20.82 %

What is Event-Driven Ansible?

- **EDA is automation that reacts to events** - not schedules
- Events can come from monitoring, webhooks, message queues, logs or cloud services
- Rules decide **when** to run Ansible actions
- Goal: **faster response** and **consistent remediation**



Rulebook Activations

Rulebook activations manage the configuration and enabling of rulebooks that govern automation logic triggered by eve

	□	ID	Name	Status	Num
›	□	29	[NETWORK] Reinstall Checkmk agent on Ubiquiti devices (@main)	Running	1
›	□	28	[LINUX] Restart all IPA services (@main)	Running	3
›	□	27	[INFRA] Create update or close Gitlab issue (@main)	Running	4
›	□	25	[LINUX] Restart named on IPA (@main)	Running	1
›	□	24	[SATELLITE] Restart Satellite service (@main)	Running	1
›	□	23	[LINUX] Restart sssd-pac on Proxmox (@main)	Stopped	2
›	□	22	[LINUX] Reboot backup server (@main)	Running	1

1 - 7 of 7

What Is an "Event" (vs a Source Action)?

- ⚡ Event
  - a *state change* or *signal* that matters (e.g., alert fired, service down)
  - often noisy and hard to filter
- 🔁 Source action
  - a *routine trigger* (e.g., "on every commit")
  - predefined target/action
- 🧪 Examples:
  - 🚫 *Update an AAP project after each commit* (not EDA)
  - ✅ *Send all monitoring alerts to a webhook; EDA decides what to do* (EDA)

Why EDA?

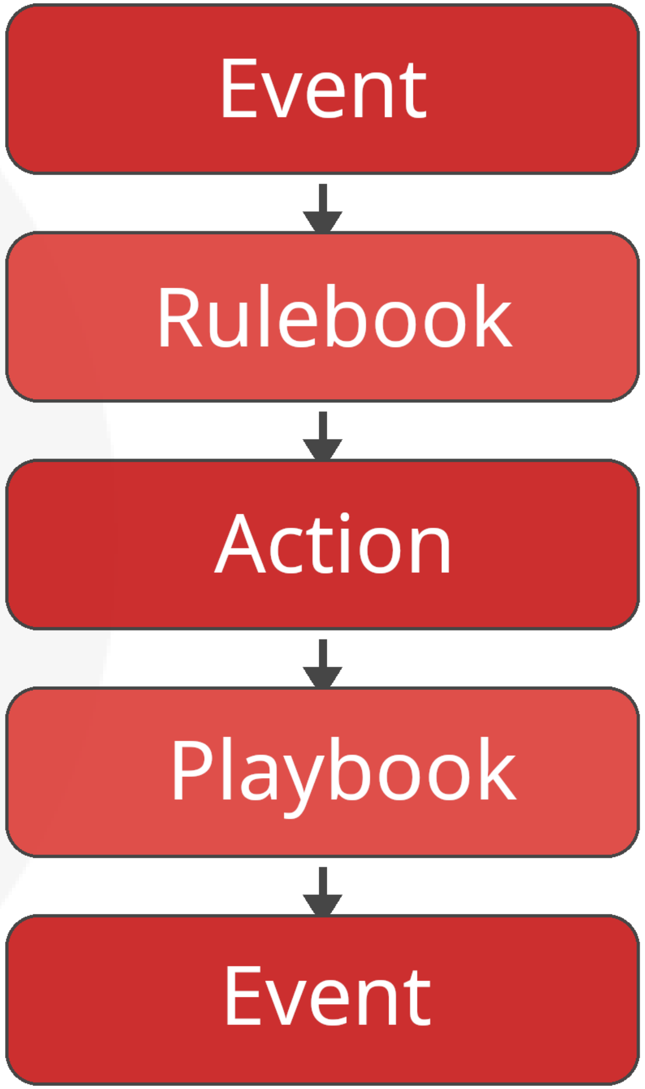
- ⚡ **Reduce MTTR** by acting immediately
- 📈 **Scale operations** without polling
- 🧩 **Standardize** responses to recurring incidents
- 🔄 **Close the loop** between detection and remediation

Core Building Blocks

- 📡 **Event Sources**: where events originate (webhooks, Kafka, logs, etc.)
- 📘 **Rulebook**: conditions + actions
- 🛠️ **Actions**: run playbooks, set facts, send notifications, create tickets
- 🧭 **Controller** (optional): central execution and governance

Event Driven Workflow

1. Event arrives from a source
2. Rulebook evaluates conditions
3. Matching rule triggers an action
4. Action runs playbook or other automation
5. Results can emit **new events** or update systems



Event

Rulebook

Action

Playbook

Event

Rulebook: restart named

```
---

- name: Restart named on IPA server
  hosts: all
  gather_facts: false

  sources:
    - name: Listen on port 5000 for Checkmk events
      ansible.eda.webhook:
        port: 5000

  rules:
    - name: Restart named
      condition: >-
        event['payload']['servicename'] == "DNS example.com" and
        event['payload']['servicestate'] == "CRITICAL"
      action:
        run_job_template:
          name: "[LINUX] Restart named on IPA [@production] - Prompt"
          organization: "Default Organization"
          job_args:
            limit: "{{ event.payload.hostname }}"
```

Checkmk Notification Script

```
#!/usr/bin/env bash

HEADER="X-Checkmk-Token"
TOKEN="${NOTIFY_PARAMETER_1}"
URL="${NOTIFY_PARAMETER_2}"

JSON=`cat <<EOF
{
  "hostname": "${NOTIFY_HOSTNAME}",
  "hostoutput": "${NOTIFY_HOSTOUTPUT}",
  "hoststate": "${NOTIFY_HOSTSTATE}",
  "servicename": "${NOTIFY_SERVICEDESC}",
  "serviceoutput": "${NOTIFY_SERVICEOUTPUT}",
  "servicestate": "${NOTIFY_SERVICESTATE}",
  "date": "${NOTIFY_SHORTDATETIME}",
  "type": "${NOTIFY_NOTIFICATIONTYPE}",
  "what": "${NOTIFY_WHAT}"
}
EOF
`

curl -X POST -H "Content-Type: application/json" -H "${HEADER}: ${TOKEN}" -d "${JSON}" ${URL}
exit $?
```

Playbook: restart named

```yaml
---

- name: Restart named on IPA
  hosts: all
  become: true
  gather_facts: true

  tasks:
    - name: Restart named
      ansible.builtin.service:
        name: named
        state: restarted
```

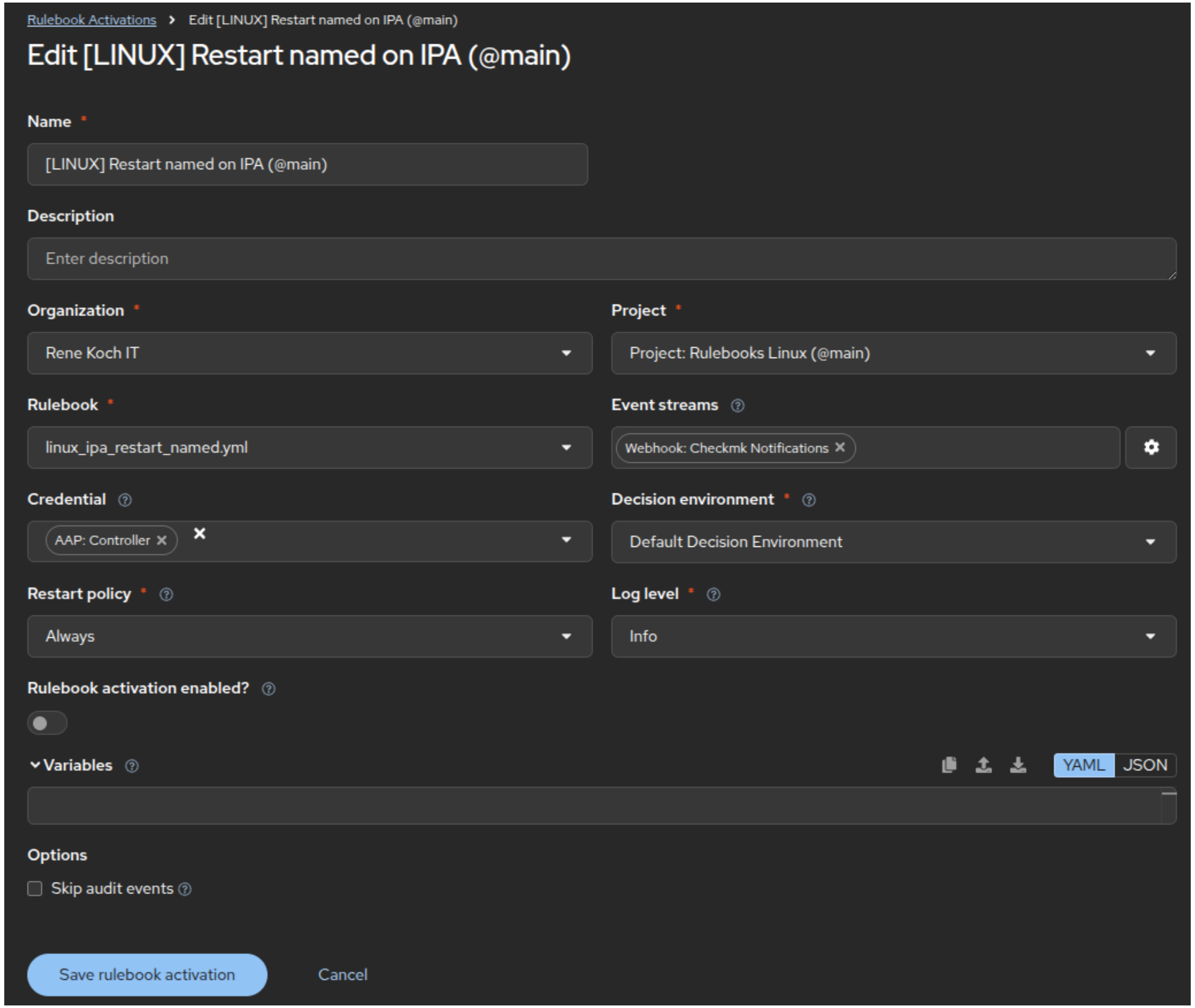
Run a Rulebook (CLI)

```
$ ansible-rulebook -r rulebooks/restart_named.yml -i localhost

PLAY [Restart named on IPA] ****************************************************

TASK [Gathering Facts] *********************************************************
ok: [ipa01.example.com]

TASK [Restart named] ***********************************************************
changed: [ipa01.example.com]

PLAY RECAP *********************************************************************
ipa01.example.com : ok=2 changed=1 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0
```

❗ Use **run_playbook** action instead of **run_job_template** for ansible-playbook command instead of Ansible Automation Platform.

Ansible Automation Platform Integration

- 📦 **Projects**: Git repository configuration
- 🧪 **Decision Environments**: Container images to run rulebooks
- 🔐 **Credentials**: Secrets for Git, Controller, Hub, tokens,...
- 📡 **Event Streams**: Entry points for events (mapped to source definition in rulebook)
- 🚀 **Rulebook Activations**: Rulebook runs



Rulebook Activations › Edit [LINUX] Restart named on IPA (@main)

Edit [LINUX] Restart named on IPA (@main)

Name *
[LINUX] Restart named on IPA (@main)

Description
Enter description

Organization *
Rene Koch IT

Project *
Project: Rulebooks Linux (@main)

Rulebook *
linux_ipa_restart_named.yml

Event streams
Webhook: Checkmk Notifications ✕

Credential
AAP: Controller ✕

Decision environment *
Default Decision Environment

Restart policy *
Always

Log level *
Info

Rulebook activation enabled?

Variables

Options

□ Skip audit events

Event-Driven Ansible Use Cases

- 🚨 **Monitoring alerts**: run remediation playbooks
- 🏗️ **Infrastructure events**: auto-scale or restart services
- 🔐 **Security findings**: isolate hosts or rotate credentials
- 🎟️ **Ticketing**: enrich and open incidents automatically
- 📘 **Documentation**: update asset database or documentation system

Self Healing Best Practices

- Start with **low-risk** automations
- Use **idempotent** playbooks (if possible)
- Add **guardrails** (approvals, maintenance windows, downtimes)
- Emit **metrics and logs** for auditing

✓ Low risk

✓ Idempotent

✓ Guardrails

✓ Auditing

Challenges with Self-healing

- 🔊 Triggering on noisy events (missing filtering)
- 🧪 Insufficient monitoring coverage
- 🧯 Healing the wrong host (issue caused by a backend dependency)
- 📚 Lack of knowledge or runbooks
- 🕒 Triggering during maintenance windows due to missing downtime

Additional Information

- **Products**:
  - Ansible Automation Platform: https://urlr.me/WcXZgR
  - Checkmk: https://urlr.me/BPJs98
- **Product Documentation**:
  - Ansible: https://urlr.me/2x4HfW
  - Automation Decisions: https://urlr.me/HejEDB
  - Rulebooks: https://urlr.me/Qb4TsB
- **Slides**: https://urlr.me/zCPcuK

Summary

- 🛰️ Checkmk **monitors** your IT landscape and **notifies** on state change
- ⚡ EDA turns these events into **real-time automation**
- 🤝 It complements traditional Ansible by **reacting** instead of **scheduling**
- 🎯 Start small, measure impact, and iterate

Thank you!

René Koch

Freelancer

Ansible Anwendertreffen Austria 18.02.2026