Automation, Integrations, Security

Checkmk Conference #7 – June, 15 - 16 2021, online

Lars Michelsen
Head of Development
tribe29
Three roadmap areas important to many enterprise customers

- Observability Integrations
- API-automating Checkmk
- Product Security
01  |  Observability Integrations
02  |  API-automating Checkmk
03  |  Product Security
Observability Integrations: Export vs. Import Use Cases

Export Use Cases
Getting monitoring **data out of Checkmk** and into other tools

Import Use Cases
Getting information **from other tools into Checkmk** and using it there
Extending our observability integrations further

- Already today, we have a number of observability integrations

- For Checkmk 2.1 we will focus our development on building or expanding three key integrations
Export Use Case: Updated Grafana Datasource Plugin

Timeline of Grafana Datasource Plugin

- **Checkmk 1.6**
  - First version launched
  - Basic inclusion of metrics in Grafana
  - Based on ‘old’ Grafana API
  - Enterprise Edition only

- **Checkmk 2.0**
  - Bug fixing
  - Inclusion in Checkmk RAW

- **Checkmk 2.1**

**Technical Improvements**
- Bug fixing
- Update to newest Grafana API version
- Available from Grafana Store

**New Features**
- Authentication by Grafana Server
- Annotations
- Variables (probably)
Export Use Case: InfluxDB – Deep Dive

Setting up InfluxDB connection

- More reliable export of metrics to InfluxDB
- Currently: using Carbon connection (UDP)
- Checkmk 2.1: Using InfluxDB native API to transport metrics reliably using HTTP(S)
- Enables exporting more metadata like labels, tags
- Principle can be used for similar systems ➔ Splunk, Elastic
InfluxDB – Deep Dive

Rule: Send Metrics to InfluxDB

- Metrics can be sent to InfluxDB using rules
- Besides metrics values, other data can be sent along with it
  - Tags & Labels
  - Thresholds
  - States
Datadog Integration Use Case

TEAM 1 uses Datadog Monitors for their systems (i.e. SAP import)

COMPANY uses Checkmk for general IT Ops (infrastructure, support, alerts, notifications etc.)

Solution: Integration to retrieve DD Monitor status & events and integrate into Checkmk alerting and notifications
Datadog Configuration Deep Dive

Configuration of Datadog Integrations

- For Checkmk 2.1: Integrate Datadog Monitors and Events in Checkmk
- Special Agent using Datadog API
- Monitors and events can be filtered to only those relevant to Checkmk
- Can and will be extended further
Display of Datadog Information in Checkmk
01  Observability Integrations
02  API-automating Checkmk
03  Product Security
Towards full Automation

**Our Goal:** Enable **automation of full deployment and configuration cycle** of Checkmk

1. Set up environment
2. Create Checkmk site
3. Configure Checkmk site
3A. Create hosts etc.
3B. Manage sites

Checkmk REST API

![Docker, Kubernetes, Ansible logos]
Missing REST-API functionality to be added next

<table>
<thead>
<tr>
<th>Feature</th>
<th>REST-API</th>
<th>WEB API</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activate changes</td>
<td>Extended</td>
<td></td>
</tr>
<tr>
<td>Folders</td>
<td>Extended</td>
<td></td>
</tr>
<tr>
<td>Hosts, services and groups</td>
<td>Extended</td>
<td></td>
</tr>
<tr>
<td>Downtimes</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>Service &amp; host states</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>Rulesets</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>BI</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>Time periods</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>User mgmt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password mgmt</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>Contact groups</td>
<td>Extended</td>
<td></td>
</tr>
<tr>
<td>Acknowledging problems</td>
<td>New</td>
<td></td>
</tr>
<tr>
<td>Agent mgmt</td>
<td>Extended</td>
<td></td>
</tr>
<tr>
<td>Site mgmt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metrics &amp; Graphs</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Committed for Checkmk 2.1!
Also adding Python API Client

Python API client

- Simplify using REST API further
- Python client enables API calls as functions
- Until then, we can recommend Python client from our partner Heinlein:
  https://github.com/HeinleinSupport/check_mk_extensions/tree/cmk2.0/check_mk_api
01 Observability Integrations

02 API-automating Checkmk

03 Product Security
Upcoming Security Features: Agent Encryption

- Encryption of agent traffic with state-of-the-art TLS encryption
  - Upcoming push agent functionality: TLS-by-default
  - Existing pull agent functionality: currently with optional symmetric encryption, for 2.1 working on TLS-by-default.
  - Key trade-off: balance security mechanism with user configuration effort

- Current POC: Minimal additional effort for users
  - CEE Users can use Agent Bakery
  - Need to configure one additional Bakery plugin
  - Slightly more manual effort for RAW users
Upcoming Security Features: SSO & 2FA

- Single Sign On & Two-factor Authentication
- SAML
Questions?
Stay tuned!

Next up:

*Kubernetes monitoring revisited*

18:45-19:30 CEST / 12:45-1:30 pm EST