Distributed Monitoring
Which method suits my project?

04.05.2018, Marcel Arentz
Check_MK Conference #4
What’s meant by Distributed Monitoring?

Accessing hosts vs. Accessing sites
When do I need Distributed Monitoring...

- Geography
- Organisation
- Network
- Performance
... and which concepts are on the table?

Central configuration

CMK Master
Site A

Status data

Configuration

Site B

Decentral configuration

CMK Master
Site A

Status data

Site C

Site A

Status data
Available methods in Check_MK?

Direct host access
Livestatus
Business Intelligence
Livedump & CMCDump
Direct host access

Livestatus

Business Intelligence

Livedump & CMCDump
How does it work ...

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request</td>
<td>Access type</td>
</tr>
<tr>
<td>Answer</td>
<td>• Traditional access</td>
</tr>
<tr>
<td>Host A</td>
<td>• SSH</td>
</tr>
</tbody>
</table>

Access type
- Traditional access
- SSH
... and which alternatives do I have?

**Architecture**

- **Request**
- **Answer**
- **Push**

**Comment**

- Access type
  - Traditional access
  - SSH
  - Push

**Diagram**

- CMK Master
- Site A
- Host A
- Host B
- Data transfer
- Request
... and which alternatives do I have?

**Architecture**

- **Request**
  - CMK Master
  - Site A

- **Answer**
  - Host A
  - Piggyback

- **Push**
  - Host B

**Comment**

- **Access type**
  - Traditional access
  - SSH
  - Push
  - Piggyback

- **Data transfer** (from Host A to Host B)
Why not in all situations?

Limitations

- Network latency
- Dependency of connection
- Firewalls
- No native push
- Scalability
Direct host access

Livestatus

Business Intelligence

Livedump & CMCDump
How does it work ...

**Architecture**

- CMK Master
- Site A
- Site B
- Site C
- Livestatus
- Distr. WATO
- Livestatus

**Comment**

Access type
- Unix Socket
- TCP
- Livestatus Proxy
... and what about isolated sites?

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMK Master</td>
<td>Access type</td>
</tr>
<tr>
<td>Site A</td>
<td>• Unix Socket</td>
</tr>
<tr>
<td></td>
<td>• TCP</td>
</tr>
<tr>
<td>Livestatus</td>
<td>• Livestatus Proxy</td>
</tr>
<tr>
<td>Site B</td>
<td>• Cascading</td>
</tr>
<tr>
<td>Livestatus +</td>
<td>Livestatus</td>
</tr>
<tr>
<td>Distr. WATO</td>
<td></td>
</tr>
<tr>
<td>Site C</td>
<td></td>
</tr>
<tr>
<td>Site D</td>
<td></td>
</tr>
</tbody>
</table>

Data transfer
When to use ...

- Direct location monitoring
- High latency
- Unstable network connection
- Many hosts
- Limited network access
... and when not to use Livestatus

Limitations

- Scalable up to +/- 80 Sites
- Needs access to dedicated TCP-Port
- Agent Updater on Master only
Direct host access

Livestatus

Business Intelligence

Livedump & CMCDump
Compress status data

Architecture

CMK Master
Site A

Aggregation A

Aggregation B

Aggregation C

Site B

Site C

Comment

Access type
- Active check (HTTPS)

Options
- Multiple aggregation
- Individual config
- Link to group/site

Data transfer
Why Business Intelligence?

- Large number of sites
How much does it cost me?

Limitations

- No config push
- Not all services in one view
- Complex configuration
- Every location needs a site
Direct host access

Livestatus

Business Intelligence

Livedump & CMCDump
No access is my problem ...

Architecture

CMK Master
Site A

Livestatus

Site B

Comment

Data transfer
... and CMCDump my last option

Architecture

CMK Master

Site A

Livestatus

CMCdump

Site B

Comment

Access type
- SSH
- Email
- ...

Dump types
- Status config
- Status data

Data transfer
With Intermediate if needed

Architecture

CMK Master

Site A

Livestatus

Site B

CMCdump

Host

as intermediate

Comment

Access type
- SSH
- Email
- ...

Dump types
- Status config
- Status data

Data transfer
Why CMCDump?

<table>
<thead>
<tr>
<th>To use if there is ...</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ ... no access at all</td>
<td>▪ No Plug’n’Play</td>
</tr>
<tr>
<td>▪ ... no stable connection</td>
<td>▪ No config push</td>
</tr>
<tr>
<td>▪ ... very limited bandwidth</td>
<td>▪ No live data</td>
</tr>
<tr>
<td></td>
<td>▪ Managing on Slave only</td>
</tr>
</tbody>
</table>
Direct host access
Livestatus
Business Intelligence
Livedump & CMCDump

Individual Configuration Mgt.
A first example

Architecture

Config Manager (e.g. Ansible)

- Config A
- Config B
- Config C

Livestatus

CMK Master

Site A

Site B

Host

Agent

Comment

Configuration...
- of agent
- of plugins
- of sites

Data transfer
## Considerations

<table>
<thead>
<tr>
<th>Pro</th>
<th>Con</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Usage of existing methods</td>
<td>- Higher complexity</td>
</tr>
<tr>
<td>- Multilevel config push</td>
<td>- Error prone</td>
</tr>
<tr>
<td>- Possibility of automation</td>
<td>- Expensive</td>
</tr>
<tr>
<td>- Less self written scripts</td>
<td>- Initial setup</td>
</tr>
<tr>
<td></td>
<td>- Maintenance</td>
</tr>
</tbody>
</table>
Which method to choose first?

1. Direct host access
2. Livestatus
3. Business Intelligence

Individual solutions

Livedump & CMCDump
What aspects affect my decision?

Questions to ask

- Is independent monitoring important?
- Which method scales the best for me?
- Which functions do I need centralized?
- How autonomous are the teams?
- What are my security restrictions?
- What is my network structure?
- …