CHECK MK
CONFERENCE # 3
Werks
New Feature-Werks

#8350 #8476 #3646 #8541

#8574 #8567 #8642 #8403 #8579 #8674 #8411 #8560 #8327
Werk #8350
Real-time checks
The check interval problem

• 1min is OK, but not always sufficient

• Lowering it can be problematic
  – Connection overhead for TCP/SSH
  – Agents run more often
  – More check results to process
  – Not all checks need it
Solution: 1 second push model via UDP

Diagram:
- **Server**: Micro Core
- **Client**: Agent
- **Trigger (1/min)**: TCP connection
- **Check Results**: UDP connection
- **Check Results (1/s)**: UDP connection
- **RT Agent**

Connections:
- Micro Core to Agent via TCP
- Agent to RT Agent via UDP
- RT Agent to Micro Core via UDP
Security

• Problem: Anybody could push check results to the server
  – Can be a problem, but doesn’t have to be (Firewalls, Router, etc.)

• Solution: UDP packets can be encrypted, like normal agent output

• Downside: Slightly higher load on client and server
Configuration

- Rule-based via WATO plus Agent Bakery
- Configurable set of checks
  - Currently CPU/memory-related ones
  - Easily extendable on request
- Configurable agent timeout and server port
Pro-Tips

• Configure a rule for finer-grained RRDs to get more detailed graphs

• Own scripts/programs can easily push check results. Details on request!

• Be careful with alerts and Graphite connections
Werks #8476 #8574 #8567

Make the Graphite Interface Great Again!
The Graphite interface

- Simple text-based protocol for metrics
- Basically consists of triples what/value/when
- Programs/tools with Graphite interface
  - Graphite
  - InfluxDB
  - Grafana
Improvements

New rules for services

#8476  Sending metrics for a service can be disabled

#8574  Warn/crit/min/max levels can be sent

New option for Graphite connections

#8567  New mangling for metric names: Ugly, but invertible
Werk #8642
Improved Logging
Logging problems

- Low logging levels: Potentially missing interesting information
- High logging levels: Overwhelming amount of messages (several MB/s)
- Inconsistent logging configuration of different parts of the Micro Core
Solution

- Partition logging into 9 separate areas
  - Alerts
  - Downtimes
  - RRD processing...
- Each area has a separate logging level, ranging from *Emergency* to *Debug*
- ToDo: Improve check helper logging
Livestatus improvements

#8403 Handle large Livestatus queries up to 500MB

#3646 Improved Livestatus output formats, including correct CSV and Python 3

#8579 Generalized Livestatus filter operators

#8674 Improved query capabilities for some list-valued columns
Werks #8541 #8411 #8560 #8327

Bits and Pieces
Miscellaneous Werks

#8541 Service check timeouts can now be configured per service

#8411 Optionally ignore TCP RST packets as "host up" indication

#8560 Output warning message to cmc.log when detecting new open file descriptors after running checks

#8327 Set HOSTNOTES and SERVICENOTES attributes for notification plugins
Checks & Agents

Marcel Arentz & Simon Betz
Devices – Classification

Networking

Storage

Device

Environment
New devices – Environment (1)

- Acme Packet Net-Net (#4525)
- APC Netbotz (#3311)
- Bachmann Bluenet2 Powerrails (#3428)
- Didactum EMS (#3863)
- Eltek Valere USV (#2976)
- EMKA Electronic Locking Modules (#4522)
New devices – Environment (2)

- Gude Power Control (#3913)
- Intel True Fabric Scale (#3639)
- Intersept Pro (#3712)
- Papouch TH2E (#3423)
- Tinkerforge (#2941)

... and more
New devices – Networking & others (1)

- Arbor Networks (#2710)
- Artec Appliance (#2634)
- Aruba WLAN Controller (#2977, #2979)
- Avaya, IP telephony (#4096)
- Barracuda Mail Appliance (#2840)
- Checkpoint Firewall (#2916)
New devices – Networking & others (2)

- Fireeye Appliance (#3403)
- Infoblox Network Control (#3683)
- Palo Alto Firewall (#2456)
- Perle Mediaconverter (#3688)

... and more
New applications

- MS-Exchange (#2870)
- Proxmox Virtual Environment (#3308)
- Mongo DB (#2985)
- Skype for Business (#3132)
- Varnish HTTP Accelerator Statistics (#3184)

... and more
New check plugins

... and many more!
#Plugins

![Graph showing the increase in plugins over time, with versions v1.1.0, v1.2.2, v1.2.6, and 'now' marked.](image)

- **Check plugins**
  - 0 in 2011
  - 200 in 2013
  - 800 in 2015
  - 1200 in 2017

- **Inventory plugins**
  - 0 in 2011
  - 10 in 2013
  - 30 in 2015
  - 70 in 2017
Check plugin development

Marcel Arentz & Simon Betz
State of affairs

• Additional five to 15 requests per week
• Fully booked until end of June
• Lead time about two months
• 320 feature werks during 380 workdays

(since last conference, Oct. 2015)
Development process

Customers’ request → Team checks & agents

Developer, tasks:
- Research
- Testing
- Implementation
- MKP

Review → Release
We need information about ... (1)

- what should be monitored?
- how to get data?
  - Agent (cmk -d HOST)
  - SNMP (cmk -v --snmpwalk HOST)

Test data absolutely necessary!

- MIBs (SNMP case)
We need information about ... (2)

- WATO configuration?
- metrics?
- cluster-aware?
- backport needed? (extra costs)
- MKP/patch? (if possible)
Obstacles and difficulties

Marcel Arentz & Simon Betz
General problems

- Commands/OIDs have changed  
  (stay compatible to older versions)
- Only outdated/no documentation available
- Third party libraries  
  (eg. Netapp: license required)
- Complex outputs/structures  
  (Cisco QoS tables)
Werk #4158
SNMP components
Werk #4158

Inventorize all physical components of arbitrary SNMP devices

- Fans, sensors, PSUs, modules, ...
  (no ports → extra view)
- Data from ENTITY-MIB
  (nearly every SNMP device supports that)
- Organized as tree structures
Cisco Nexus m9500
# Check_Mk HW/SW inventory system

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Physical Components</th>
</tr>
</thead>
</table>

## Backplanes

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Description</th>
<th>Serial Number</th>
<th>Model Name</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>406</td>
<td>Backplane</td>
<td>Backplane</td>
<td>FOX122GAGQK</td>
<td>DS-C9509</td>
<td>Chassis (149)</td>
</tr>
</tbody>
</table>

## Chassis

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Description</th>
<th>Serial Number</th>
<th>Model Name</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>149</td>
<td>MDS 9509 (9 Slot) Chassis</td>
<td>MDS 9509 (9 Slot) Chassis</td>
<td>FOX122GAGQK</td>
<td>DS-C9509</td>
<td>Stack (10)</td>
</tr>
</tbody>
</table>

## Fans

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Description</th>
<th>Serial Number</th>
<th>Model Name</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>534</td>
<td>Fan Module-1</td>
<td>Fan Module-1</td>
<td>DCH12120786</td>
<td>DS-9SLOT-PAN</td>
<td>Container (342)</td>
</tr>
</tbody>
</table>

## Modules

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Description</th>
<th>Serial Number</th>
<th>Model Name</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>1/2/4 Gbps FC Module</td>
<td>1/2/4 Gbps FC Module</td>
<td>JAE11517UC</td>
<td>DS-X9124</td>
<td>Container (126)</td>
</tr>
<tr>
<td>25</td>
<td>Supervisor/Fabric-2</td>
<td>Supervisor/Fabric-2</td>
<td>JAE1252QYFK</td>
<td>DS-X9530-SF2-K9</td>
<td>Container (126)</td>
</tr>
<tr>
<td>27</td>
<td>Supervisor/Fabric-2</td>
<td>Supervisor/Fabric-2</td>
<td>JAE1252QWXX</td>
<td>DS-X9530-SF2-K9</td>
<td>Container (126)</td>
</tr>
<tr>
<td>22</td>
<td>1/2/4 Gbps FC Module</td>
<td>1/2/4 Gbps FC Module</td>
<td>JAE1259W0PL</td>
<td>DS-X9124</td>
<td>Container (126)</td>
</tr>
<tr>
<td>23</td>
<td>1/2/4 Gbps FC Module</td>
<td>1/2/4 Gbps FC Module</td>
<td>JAE1242XQQQ</td>
<td>DS-X9148</td>
<td>Container (126)</td>
</tr>
</tbody>
</table>

## Power Supplies

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Description</th>
<th>Serial Number</th>
<th>Model Name</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>470</td>
<td>PowerSupply-1</td>
<td>DS-CAC-3000W</td>
<td>AZS12210NN7</td>
<td>DS-CAC-3000W</td>
<td>Container (278)</td>
</tr>
<tr>
<td>471</td>
<td>PowerSupply-2</td>
<td>DS-CAC-3000W</td>
<td>AZS12210NN6</td>
<td>DS-CAC-3000W</td>
<td>Container (279)</td>
</tr>
</tbody>
</table>

## Sensors

<table>
<thead>
<tr>
<th>Index</th>
<th>Name</th>
<th>Description</th>
<th>Serial Number</th>
<th>Model Name</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>21912</td>
<td>module-6 Intake1</td>
<td>module-6 Intake1</td>
<td></td>
<td></td>
<td>Module (27)</td>
</tr>
<tr>
<td>21910</td>
<td>module-6 Outlet1</td>
<td>module-6 Outlet1</td>
<td></td>
<td></td>
<td>Module (27)</td>
</tr>
<tr>
<td>21911</td>
<td>module-6 Outlet2</td>
<td>module-6 Outlet2</td>
<td></td>
<td></td>
<td>Module (27)</td>
</tr>
<tr>
<td>21848</td>
<td>module-5 Intake1</td>
<td>module-5 Intake1</td>
<td></td>
<td></td>
<td>Module (26)</td>
</tr>
<tr>
<td>21846</td>
<td>module-5 Outlet1</td>
<td>module-5 Outlet1</td>
<td></td>
<td></td>
<td>Module (26)</td>
</tr>
<tr>
<td>21847</td>
<td>module-5 Outlet2</td>
<td>module-5 Outlet2</td>
<td></td>
<td></td>
<td>Module (26)</td>
</tr>
<tr>
<td>21720</td>
<td>module-3 Intake1</td>
<td>module-3 Intake1</td>
<td></td>
<td></td>
<td>Module (24)</td>
</tr>
<tr>
<td>21718</td>
<td>module-3 Outlet1</td>
<td>module-3 Outlet1</td>
<td></td>
<td></td>
<td>Module (24)</td>
</tr>
<tr>
<td>21719</td>
<td>module-3 Outlet2</td>
<td>module-3 Outlet2</td>
<td></td>
<td></td>
<td>Module (24)</td>
</tr>
<tr>
<td>21590</td>
<td>module-1 Intake1</td>
<td>module-1 Intake1</td>
<td></td>
<td></td>
<td>Module (22)</td>
</tr>
<tr>
<td>21591</td>
<td>module-1 Outlet1</td>
<td>module-1 Outlet1</td>
<td></td>
<td></td>
<td>Module (22)</td>
</tr>
<tr>
<td>21655</td>
<td>module-2 Outlet2</td>
<td>module-2 Outlet2</td>
<td></td>
<td></td>
<td>Module (23)</td>
</tr>
<tr>
<td>21652</td>
<td>module-1 Intake1</td>
<td>module-1 Intake1</td>
<td></td>
<td></td>
<td>Module (22)</td>
</tr>
<tr>
<td>21654</td>
<td>module-2 Outlet1</td>
<td>module-2 Outlet1</td>
<td></td>
<td></td>
<td>Module (22)</td>
</tr>
<tr>
<td>21656</td>
<td>module-2 Intake1</td>
<td>module-2 Intake1</td>
<td></td>
<td></td>
<td>Module (23)</td>
</tr>
</tbody>
</table>

---

[Image of a table showing hardware inventory details]
Prominent Werks
- Reorganized temperature checks
- One rule for all Temperature checks
- Spreading this principle to other checks
Werk #2934

Parameters

- Upper Temperature Levels
- Lower Temperature Levels
- Display values in
- Override unit of sensor
- Interpretation of the device's own temperature status
- Trend computation
- Logs on Windows: Common configuration
- Oracle on Windows: Oracle Wallet support
- MTR plugin: detailed connection information
<table>
<thead>
<tr>
<th>State</th>
<th>Service</th>
<th>Icons</th>
<th>Status detail</th>
<th>Age</th>
<th>Checked</th>
<th>Perf-O-Meter</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>Mtr to mathiaskettner.de</td>
<td>![Image]</td>
<td>OK - Number of Hops: 8, Packet loss 0.0%, Round trip average 27.7ms, Standard deviation 7.1ms</td>
<td>26 m</td>
<td>59.3 s</td>
<td>0% / 27.7 ms</td>
</tr>
<tr>
<td>OK</td>
<td>Mtr to <a href="http://www.google.com">www.google.com</a></td>
<td>![Image]</td>
<td>OK - Number of Hops: 10, Packet loss 0.0%, Round trip average 34.6ms, Standard deviation 3.5ms</td>
<td>26 m</td>
<td>59.3 s</td>
<td>0% / 34.6 ms</td>
</tr>
<tr>
<td>OK</td>
<td>Mtr to <a href="http://www.hsx.vn">www.hsx.vn</a></td>
<td>![Image]</td>
<td>OK - Number of Hops: 15, Packet loss 10.0% <strong>WARN</strong> (Levels at 10%/25%), Round trip average 311.6ms <strong>CRT</strong> (Levels at 150ms/250ms), Standard deviation 15.0ms</td>
<td>4 m</td>
<td>59.4 s</td>
<td>10% / 312 ms</td>
</tr>
</tbody>
</table>
- Supporting new HPE 3PAR Storage
- Information about CPGs, Virtual Volumes, etc
- Mostly compatible with known rulesets
- HW/SW Inventory is not activated by default

- Configurable state of failing check:

  (Check can be OK in case of unreachable Host)
- API over HTTP for exporting full inventory
- Request single/multiple hosts or information
- Different output formats: json, python, xml
Werk #3585

```
"software": {
  "applications": {
    "check_mk": {
      "is_cluster": false
    },
    "inventory": {
      "oldest_section": 1493567030,
      "sections": [
        { "age": 1493567030,
          "section": "dmidecode",
          "until": 1493578359
        },
        { "age": 1493567030,
          "section": "lnx_packages",
          "until": 1493578359
        },
        { "age": 1493567030,
          "section": "lnx_cpuinfo",
          "until": 1493578359
        },
        { "age": 1493567030,
          "section": "lnx_video",
          "until": 1493578359
        },
        { "age": 1493567030,
          "section": "lnx_ip_r",
          "until": 1493578359
        },
        { "age": 1493567030,
          "section": "lnx_distro",
          "until": 1493578359
        }
      ]
    }
  }
}

▼<packages type="list">
▼<item type="dict">
  <name type="str">acl</name>
  <package_version type="str">2</package_version>
  <package_type type="str">deb</package_type>
  <summary type="str"/>
  <version type="str">2.2.52</version>
  <arch type="str">x86_64</arch>
</item>
▼<item type="dict">
  <name type="str">acpi</name>
  <package_version type="str">1</package_version>
  <package_type type="str">deb</package_type>
  <summary type="str"/>
  <version type="str">1.7</version>
  <arch type="str">x86_64</arch>
</item>
▼<item type="dict">
  <name type="str">acpi-support-base</name>
  <package_version type="str">6</package_version>
  <package_type type="str">deb</package_type>
  <summary type="str"/>
  <version type="str">0.142</version>
  <arch type="str">all</arch>
</item>
▼<item type="dict">
  <name type="str">acpid</name>
  <package_version type="str">2</package_version>
  <package_type type="str">deb</package_type>
  <summary type="str"/>
  <version type="str">1:2.0.23</version>
  <arch type="str">x86_64</arch>
</item>
```

Check_MK Conference #3 – Checks & Agents
News in the Core System

Konstantin Büttner
New Feature-Werks

#2771 #8360 #3342 #3155 #3114

#3039 #2881 #3721 #3342 #3414 #3993
#3531 #3806 #3580 #3853 #3155 #4036
Werk #2771

Errors in Check_MK configuration do not prevent the core from being restarted anymore.
Warning instead of preventing activation

<table>
<thead>
<tr>
<th>Actions</th>
<th>Site</th>
<th>Status</th>
<th>Version</th>
<th>Changes</th>
<th>Last result</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Warnings:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• check_mk: The following host names have duplicates: heute. This might lead to invalid/incomplete monitoring for these hosts.</td>
</tr>
</tbody>
</table>

Pending changes
No entries.
Wait, this doesn’t seem new?

- Implemented for CMC in July 2015 (Werk #8294)
- Now also for other cores (Nagios, Icinga)
Werk #8360

Recurring downtimes now for nth day of month and xth weekday
Examples

- Have a downtime repeat every
  - 23rd of the month
  - Second-to-last Tuesday of the month
  - First monday

- Counting backwards from the end of the month currently only for weekdays
Werk #3155
Implemented dual monitoring for systems with management boards (like HP iLO)
Situation before

• No support for devices with multiple IP addresses

• Want to monitor hardware information via management board SNMP? Better create a second host in Check_MK

• 😞
Situation now

Properties of host heute

- General Properties
- Basic settings
- Host tags

Management Board
- Protocol: empty (Default value)
- Address: empty (Default value)
- SNMP credentials: none (Default value)
Werk #3114

Linux and Windows Agent can now encrypt their output
Situation before

Encryption possible through alternative datasource programs but:

- Tedious and difficult
- Lacking bakery integration
Situation now

Edit rule: Encryption

Control encryption of data sent from agent to host.

Value

Encryption secret

Please note that Check_MK needs this password in clear text during normal operation and thus stores it unencrypted on the Check_MK server.

Encryption for Agent

- Enforce (drop unencrypted data)

Encryption for Realtime Updates

- Enforce (drop unencrypted data)

Conditions

Save
Situation now

• Single rule controls both agent bakery and server-side enforcement

• Configurable to accept only clear-text, only encrypted or both

• Data for real-time checks configurable in the same ruleset
### Situation now

#### Services of Host heute

<table>
<thead>
<tr>
<th>State</th>
<th>Service</th>
<th>Icons</th>
<th>Status detail</th>
<th>Age</th>
<th>Checked</th>
<th>Perf-O-Meter</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRIT</td>
<td>Check_MK</td>
<td></td>
<td>Cannot get data from TCP port 127.0.0.1:6556: Agent output is plaintext but encryption is enforced by configuration, execution time 3.5 sec</td>
<td>6 m</td>
<td>29.5 s</td>
<td>3.50 s</td>
</tr>
<tr>
<td>WARN</td>
<td>Check_MK Discovery</td>
<td></td>
<td>3 unmonitored services (livesystem_status:1, miknotifyd:1, omd_apache:1) WARN, no vanished services found</td>
<td>5 m</td>
<td>5 m</td>
<td></td>
</tr>
<tr>
<td>OK</td>
<td>Check_MK HW/SW Inventory</td>
<td></td>
<td>OK - found 23 entries</td>
<td>34 m</td>
<td>37.5 s</td>
<td></td>
</tr>
<tr>
<td>CRIT</td>
<td>APT Updates</td>
<td></td>
<td>CRIT - 75 normal updates WARN, 14 security updates (chromium-browser=101, libnss4, libnss3-sssd, libnss3-id, libnss3, chromium-browser, chromium-codecs-fmpg-extra, ghostscript, ghostscript-x, libge9-common, libge9, libxmlt1.1, mysql-common, libmysqld/client20) CRIT</td>
<td>34 m</td>
<td>6 m</td>
<td>75/14</td>
</tr>
<tr>
<td>OK</td>
<td>CPU load</td>
<td></td>
<td>OK - 15 min load 0.32 at 8 Cores (0.04 per Core)</td>
<td>34 m</td>
<td>6 m</td>
<td>0.350</td>
</tr>
<tr>
<td>OK</td>
<td>CPU utilization</td>
<td></td>
<td>OK - user: 2.7%, system: 0.7%, wait: 0.1%, steal: 0.0%, guest: 0.0%, total: 3.6%</td>
<td>34 m</td>
<td>6 m</td>
<td>3.6%</td>
</tr>
<tr>
<td>CRIT</td>
<td>ClusterFoo</td>
<td></td>
<td>CRIT - Das ist der neue Infotext</td>
<td>34 m</td>
<td>6 m</td>
<td></td>
</tr>
</tbody>
</table>

Check_MK Conference #3 - News in the Core System
Further Werks (1)

#3039 Added more useful debugging infos to crash reports

#2881 Automatically restart core instead of reload after changes in local check plugins

#3721 Host macros are now replaced in datasource program command lines

#3342 MKP: local/lib and local/bin of sites can now be packed

#3414 New declarator BINARY(...) for OIDs – returning a list of byte values
Further Werks (2)

#3531 Reduced Check_MK helper size for certain dists/python versions

#3806 Sped up „Activate Changes“

#3580 The macro $HOSTNAME$ is now available for host checks which are based on service states

#3853 cmk --list-tag can now also list offline hosts

#4036 Measurement of time used by Check_MK now includes time waited for agent

#3993 Some minor performance improvements during config generation
Why WATO Web-API?

• Integration of CMDBs
• Automated monitoring management
• Automated lifecycle management
• Standard interface for automated actions
Situation in 1.2.8

- Add, edit, delete host
- Query attributes of host or hosts
- Service discovery of host
- Bake agents
- Activate changes
Werk #4023
Local user management
Werk #4018
Management of groups
Werk #3805
Support cluster
Werk #2785

Input validation
Upcoming features

- Configuration of WATO rules
- Configuration of Host Tags
- Configuration of folders
- Configuration of distributed monitoring sites
- Configuration of Customers (Managed Services Edition)
Thanks for listening!

YOUR FEEDBACK IS WELCOME