The Check_MK monitoring system

Open Source Days 2016, Copenhagen
Speaker: Troels Arvin
Slides: http://troels.arvin.dk/osd/2016/

About me

Section of Infrastructure Development & Architecture, Danish Health Data Authority (Sundhedsdatastyrelsen).

Role: Database administrator.

Systems monitoring experience: Nagios, SCOM, SolarWinds, **Check_MK** (since 2012), OEM, up.time, HP IMC.

Agenda

- History
- Features / demo
- Drawbacks
- If time: How it works
- Questions

History of Check_MK

2008: Check_MK released as plugin to Nagios.

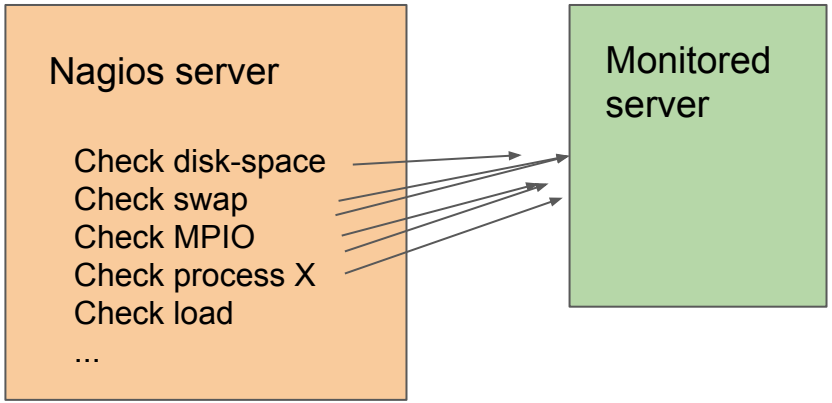
2010: Open Monitoring Distribution (OMD, omdistro.org): A mash-up of Nagios, Check_MK, NagVis, PNP4Nagios, DocuWiki, ...

2015: Check_MK *Raw Edition*: Simplified version of OMD.

Along the way, Nagios has become a minor part of the monitoring solution.

History of Check_MK, continued

Classical Nagios:

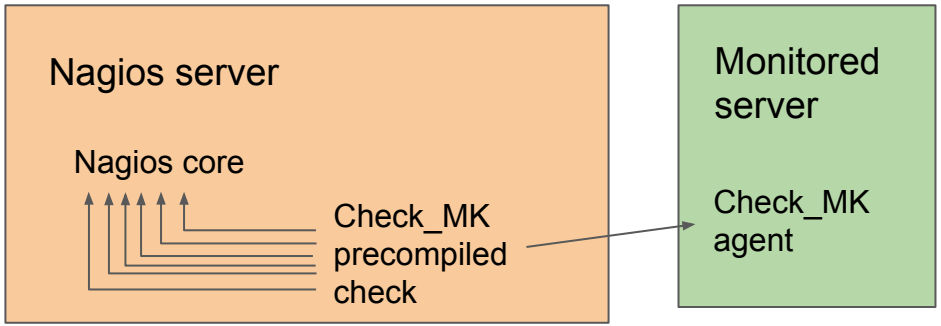


Multiple process creations, multiple connection setups.

History of Check_MK, continued

2008: Nagios + Check_MK:

One connection per poll, generating data for multiple monitoring points.



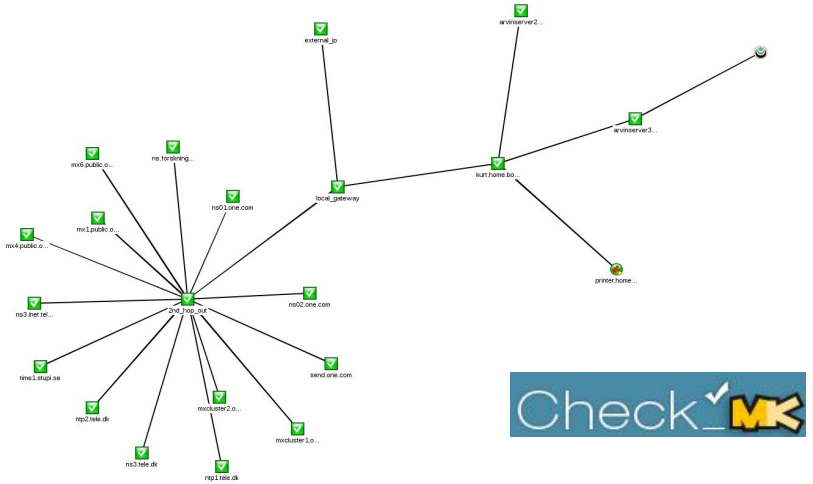
Agent: Bash script invoked by (x)inetd or systemd. Runs as root, but doesn't accept arguments, and can filter access. May call agent-side plugins.

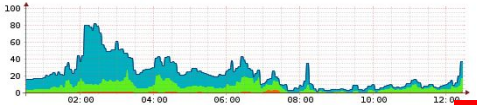
On the monitoring server side: check_mk tool is used to collect inventory for a monitored host. The inventory results in byte-compiled python script per monitored server; this script parses agent output and feeds Nagios.

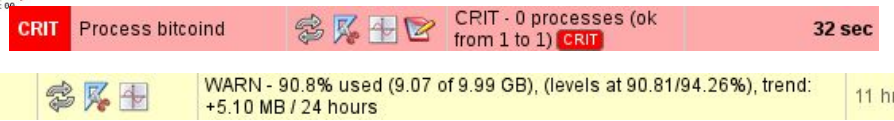
History of Check_MK, continued

2010: Open Monitoring Distribution (OMD):

- Bundled Nagios, Icinga, Check_MK, NagVis, PNP4Nagios, RRDtool, DocuWiki, Shinken, ...
- Distributed via package repositories.
- Included installer.
- Community.







History of Check_MK, continued

2015: Open Monitoring Distribution stagnating, as Check_MK has taken center stage. Nagios is now a small corner of the solution; mainly used for core scheduling.

Leaner derivations of OMD:

- Check_MK Raw Edition
- Check_MK Enterprise Edition

Main developers: Mathias Kettner GmbH, Munich.

Check_MK *Raw Edition* Features

Open source (GPL 2) with public git repo.

Available as a stand-alone bundled package for several distros. Or for DIY-people as separate packages (e.g. in EPEL).

Backed by full-time developers.

Commercial support available (Enterprise Edition + appliance editions).

Consultancy available.

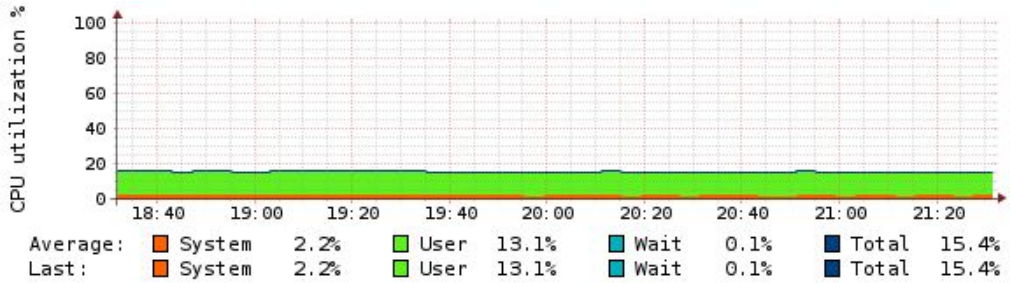
Courses, conferences. Thriving community (IRC, mailing lists, extension repo).

Check_MK *Raw Edition* Features, continued

Very efficient:

- Uses tmpfs at write-intensive paths.
- Byte-compiled checks per monitored host.
- Multiple monitoring points covered by a single agent poll.
- rrdcached

CPU util on monitoring server with 15000+ services at 600+ hosts, 4 minutes between polls (60/sec):



Huge contrast to SCOM, Nagios.

Check_MK *Raw Edition* Features, continued

Graphs are handled so fast that they are actually useful.

(Live demo.)

Check_MK *Raw Edition* Features, continued

Real choice between text-based configuration and web-based configuration. Text-based configuration much more concise than Nagios configuration.

Broad monitoring coverage:

- 100s of checks out-of-the box. Most of high quality.
- 160 contributed checks in Check_MK Exchange ("MKP" packages)
- Compatibility with Nagios plugins.

Examples...

Physical Linux server: SMNP+agent

OK	CPU load	OK - 15min load 24.51 at 24 CPUs	2016-02-04 18:28:58	6 sec	8.8	
OK	CPU utilization	OK - user: 23.3%, system: 1.1%, wait: 16.7%, total: 41.1%	2015-02-03 23:53:42	6 sec	41%	
OK	Disk IO SUMMARY	OK - 304.84 MB/sec read, 34.39 MB/sec write, IOs: 2430.05/sec	2015-02-03 23:57:39	6 sec	304.84 M/s 34.39 M/s	
OK	fs_/	OK - 9.9% used (82.22 of 833.23 GB), (levels at 96.21/97.63%), trend: +107.03 MB / 24 hours, inodes available 873814k/99.96%	2016-01-27 11:49:58	5 sec	9.87 %	
OK	HW Mem 8	OK - Board: 0, Num: 8, Type: n/a, Size: 32768 MB, Status: good , Condition: ok	2016-02-18 16:06:12	3 min		
OK	HW Phydrv 2	OK - Bay: 2, BusNumber: 0, Status: ok, SmartStatus: ok, RefHours: 573, Size: 858483MB, Condition: ok	2016-02-18 16:06:12	3 min		
OK	HW Phydrv 3	OK - Bay: 1, BusNumber: 0, Status: ok, SmartStatus: ok, RefHours: 573, Size: 858483MB, Condition: ok	2016-02-18 16:06:12	3 min		
OK	HW Power Meter	OK - Current reading: 250 Watt	2016-02-18 16:06:12	3 min		
OK	HW PSU 0/1	OK - PSU in chassis 0, bay 1 is in state "ok"	2016-02-18 16:06:12	3 min		
OK	HW PSU 0/2	OK - PSU in chassis 0, bay 2 is in state "ok"	2016-02-18 16:06:12	3 min		
OK	Interface 6	OK - [eno49] (up) MAC: [redacted], 10.00 Gbit/s, in: 6.68 kB/s, out: 5.17 kB/s	2016-02-07 20:06:54	3 min	0.0% 0.0%	
OK	Interface 7	OK - [eno50] (up) MAC: [redacted], 10.00 Gbit/s, in: 185.89 kB/s, out: 44.51 MB/s	2016-02-07 20:06:54	3 min	0.0% 3.7%	
OK	Interface 8	OK - [team0] (up) MAC: [redacted], speed unknown, in: 158.39 kB/s, out: 42.74 MB/s	2016-02-07 20:06:54	3 min	158.4kB/s 42.7MB/s	
OK	Kernel Context Switches	OK - 37477/s	2015-02-03 23:57:39	3 min	37477.1/s	
OK	Kernel Major Page Faults	OK - 0/s	2015-02-03 23:57:39	3 min	0.0/s	
OK	Kernel Process Creations	OK - 50/s	2015-02-03 23:57:39	3 min	50.3/s	
OK	Logical Device /dev/sda	OK - In normal operation mode. Logical Volume Size: 838.33 GB	2016-02-18 16:06:12	3 min		
OK	Logins	OK - 10 logins on system, levels at 20/30	2015-06-05 11:52:51	3 min		
OK	Memory used	OK - 478.60 GB used (478.54 RAM + 0.00 SWAP + 0.06 Pagetables, this is 95.0% of 503.60 RAM (4.00 total SWAP)), 0.7 mapped, 18.8 committed, 0.6 shared	2015-02-03 23:53:42	3 min	95%	
OK	Mount options of /	OK - mount options exactly as expected	2016-02-07 20:06:54	3 min		
OK	Multipath 360[redacted]d	OK - paths expected: 8, paths active: 8	2015-11-22 16:13:46	2 min		
OK	NTP Time	OK - stratum 3, offset 0.0000 ms, reference: [redacted]	13 hrs	2 min	0.00 ms	
OK	Number of threads	OK - 1847 threads	2015-03-04 14:53:58	2 min	1847	
OK	Postfix Queue	OK - The mailqueue is empty	2015-04-10 10:23:26	2 min		
OK	proc_dsmcad	OK - 2 processes 811.3 MB virtual, 12.1 MB resident, 0.0% CPU	2016-02-15 13:20:55	2 min	0.0%	
OK	TCP Connections	OK - ESTABLISHED: 427, TIME_WAIT: 19	2015-02-03 23:53:42	2 min		
OK	Temperature 1 ambient	OK - Temperature Sensor 1 "ambient": 17 Degrees Celsius	2016-02-18 16:06:12	2 min	17 °C	
OK	Temperature 10 system	OK - Temperature Sensor 10 "system": 37 Degrees Celsius	2016-02-18 16:06:12	2 min	37 °C	
OK	Temperature 11 powerSupply	OK - Temperature Sensor 11 "powerSupply": 26 Degrees Celsius (Above -99)	2016-02-18 16:06:12	2 min	26 °C	

Check_MK *Raw Edition* Features, continued

Firewall (SNMP):

OK	Check_MK inventory		OK - no unchecked services found	2016-02-01 14:08:38	22 sec	
OK	Cluster Status		OK - Device is the Active unit	24 hrs	111 sec	
OK	CPU utilization		OK - 9.0% utilization in the last 5 minutes	2015-03-23 10:21:13	111 sec	9 %
OK	Interface 02		OK - [Adaptive Security Appliance Internal-Data0/0 interface] (up) MAC: 00:00:00:01:00:01, 10.00 Gbit/s, in: 94.67 MB/s, out: 94.24 MB/s	2016-02-18 19:39:02	111 sec	7.9% 7.9%
OK	Interface 03		OK - [Adaptive Security Appliance Internal-Data0/1 interface] (up) MAC: 00:00:00:01:00:02, 10.00 Gbit/s, in: 20.55 MB/s, out: 19.02 MB/s	2016-02-10 00:06:44	111 sec	1.7% 1.6%
OK	Mem used MEMPOOL_DMA		OK - 47.3% (361.85 MB) of 764.41 MB used	2015-03-23 10:21:13	111 sec	
OK	Mem used System memory		OK - 28.8% (1.61 GB) of 5.61 GB used	2015-03-23 10:21:13	111 sec	
OK	Uptime		OK - up since Fri Feb 19 15:03:53 2016 (1d 09:58:41)	2015-03-23 10:21:13	111 sec	01d 09h 58m

Switch (SNMP):

OK	CPU utilization		OK - CPU utilization is 2%	2016-02-08 14:49:01	63 sec	
OK	Interface 00		OK - [Trk5 Uplink [redacted]] (up) MAC: [redacted] 1 Gbit/s, in: 51.02 MB/s, out: 179.27 kB/s	2015-06-07 13:06:54	35 sec	42.8% 0.1%
OK	Memory		OK - Memory usage is 45%	2015-02-03 23:55:18	3 min	
OK	Sensor 1		OK - Condition of FAN "Fan Sensor" is good	2015-02-03 23:55:18	3 min	
OK	Sensor 2		OK - Condition of PSU "Power Supply 1 Sensor" is good	2015-02-03 23:55:18	3 min	

Check_MK *Raw Edition* Features, continued

Fibre channel switch (SNMP):

OK	FAN 1		OK - Fans at 8653rpm	2015-02-03 23:53:05	4 min	
OK	Interface 080[redacted]		OK - [eth0] (up) MAC: [redacted], 100 Mbit/s, in: 0.00 B/s, out: 0.00 B/s	2015-02-03 23:53:06	3 min	0.0% 0.0%
OK	Port 00 ISL port0		OK - ISL at 8Gbit/s, In: 1023.68 B/s, Out: 23.83 kB/s, Phy:inSync(6), Op:online(1), Adm:online(1)	2016-01-21 10:19:49	3 min	0.0% 0.0%
OK	Power supply 1		OK - No problems found	2015-02-03 23:53:09	3 min	
OK	Temperature 1		OK - 31 °C	2015-02-03 23:53:09	3 min	

Note: *Not* trap-based (trap-based hw monitoring generally isn't reliable).

MSSQL (agent + agent plugin):

OK	SQLServer tempdb File Sizes	OK - Data Files: 1.37 GB, Log Files: 99.99 MB (Used: 8.05 MB)	2015-07-01 10:02:35	8 sec	
OK	SQLServer tempdb Transactions	OK - Transactions: 0.0/s, Tracked Transactions: 0.0/s, Write Transactions: 0.0/s	2015-07-01 10:06:35	8 sec	
OK	SQLServer:Catalog_Metadata master cache_hit_ratio	OK - 80%	2015-07-01 10:02:35	8 sec	80.3%

Check_MK *Raw Edition* Features, continued

Power distribution unit (SNMP):

OK	Interface 2		OK - [lance] (up) MAC: 00:c0:b7:e9:5f:ba, 100 Mbit/s, in: 96.70 B/s, out: 51.97 B/s	2015-07-28 12:23:39	92 sec	0.0% 0.0%
OK	PDU apcE95FBA		OK - Amperage: 4.400000	2015-07-28 12:23:39	91 sec	

UPS (SNMP):

OK	APC Symmetra status		OK - Battery status: ok, output status: online (calibration invalid), capacity 100% (crit at or below 90%), sys. temp. 29 °C, bat. curr. 0 A, input voltage 230 V, output voltage 230 V, output current 1 A, run time remaining: 01:25:40, current output load 17%	2015-06-04 06:59:28	26 sec	
OK	Interface 2		OK - [(up) MAC: 0 , 100 Mbit/s, in: 246.98 B/s, out: 111.07 B/s	2015-02-03 23:56:06	25 sec	0.0% 0.0%
OK	Self Test		OK - Result of self test: OK, Date of last test: 02/07/2016	2015-02-03 23:56:07	24 sec	
OK	Temperature External 2		OK - 26 °C	2015-08-11 08:36:28	24 sec	

Check_MK *Raw Edition* Features, continued

Backup-server low-level services (agent + agent plugin)

OK	TSM Drive TS3500 / DRIVE12		OK - [0[redacted]] state: LOADED, online: YES	2015-12-10 12:02:05	2 min	
OK	TSM server listening on TCP port 1581		TCP OK - 0.002 second response time on 192.168.208.145 port 1581	2016-02-01 14:08:06	2 min	1.658 ms
OK	TSM Stagingpool ASP01		OK - total tapes: 2, tapes less then 70% full: 2, utilization: 0.0 tapes	2015-12-10 12:02:05	2 min	
OK	TSM Stagingpool TSP01		OK - total tapes: 110, tapes less then 70% full: 74, utilization: 68.0 tapes	2015-12-10 12:02:05	2 min	
OK	TSM Stagingpool TSP02		OK - total tapes: 63, tapes less then 70% full: 16, utilization: 49.6 tapes	2015-12-10 12:02:05	2 min	
OK	TSM Stagingpool TSP03		OK - total tapes: 29, tapes less then 70% full: 27, utilization: 7.5 tapes	2015-12-10 12:02:05	2 min	
OK	TSM Storagepool ASP01		OK - 20.06 GB used - Arch	2015-12-10 12:02:05	2 min	

vCenter-server (agent)

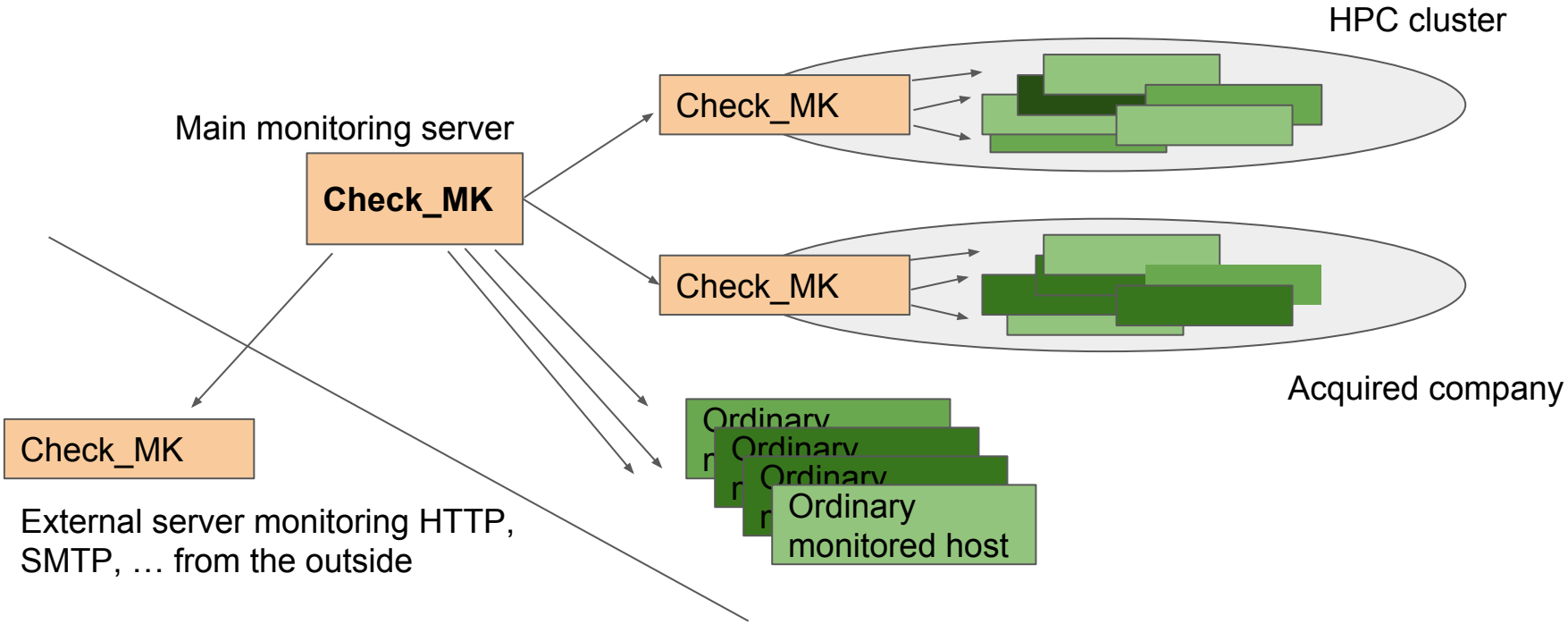
OK	fs_[redacted]_vmware_lun27_t012		OK - 88.0% used (5.28 of 6.00 TB), (levels at 96.18/98.41%), trend: +47.99 kB / 24 hours, uncommitted: 0.00 GB, provisioning: 88.0%	2015-06-13 09:33:39	3 min	87.95% (+0.00%)
OK	HostSystem [redacted]		OK - power state: poweredOn	2015-12-04 13:50:40	3 min	

Check_MK *Raw Edition* Features, continued

- Easy to AD-integrate. Multiple user roles.
- Good support for Linux + Windows (SCCM-friendly) (+ AIX + Solaris + …).
- Multiple dashboards.
- Mostly python-based == easy to understand code, in case deep debugging is needed.
- Optional event console: Collect+process syslog-data and traps.

Check_MK *Raw Edition* Features, continued

Distributed from the get-go:



Some drawbacks

- When the Check_MK monitoring configuration has been changed, it needs to be **converted to Nagios configuration** (which can fail under some circumstances).
- The Check_MK **name is weird** and may make upper management sceptical.
- **Lack of IPv6** support (will be in the 1.6.8 release which is a month or two away).
- In systems which change a lot, you will often see alerts **about unchecked services**; some regard this as a drawback (and it may be turned off).
- Hard to get thresholds right with regards to **low-actvity NIC/FC ports**.
- The **open-core business model** is disliked by some.

How it works: Agent output

```
[user@monsrv ~]$ echo | nc monitoredsrv 6556
Version: 1.2.6p9
AgentOS: linux
…
<<<df>>>
/dev/mapper/monitoredsrv-root xfs         112719872 75760596  36959276  68% /
tmpfs                         tmpfs       2983204     57824   2925380   2% /run
/dev/vda1                     xfs         508588   185704   322884      37% /boot
…
<<<mounts>>>
/dev/mapper/monitoredsrv-root / xfs rw,seclabel,noatime,attr2,inode64,noquota 0 0
/dev/vda1 /boot xfs rw,seclabel,noatime,attr2,inode64,noquota 0 0
<<<ps>>>
(root,208024,6856,00:00:35,1) /usr/lib/systemd/systemd --switched-root --system --deserialize 19
…
<<<mem>>>
MemTotal:         3918412 kB
MemFree:          1406952 kB
...
```

How it works: Adding a monitored host

Live demo:

- ssh to server "monitored.arvin.dk".
- Install check-mk-agent package using "yum".
- Start xinetd.

In Check_MK:

- Add host "monitored".
- Add host "printer".

Links

These slides: http://troels.arvin.dk/osd/2016/

Check_MK: http://mathias-kettner.com/check_mk.html

Questions?