

The new checkmk Windows Agent

CHECKMK CONFERENCE #5 – MUNICH, APRIL 29, 2019

Agenda

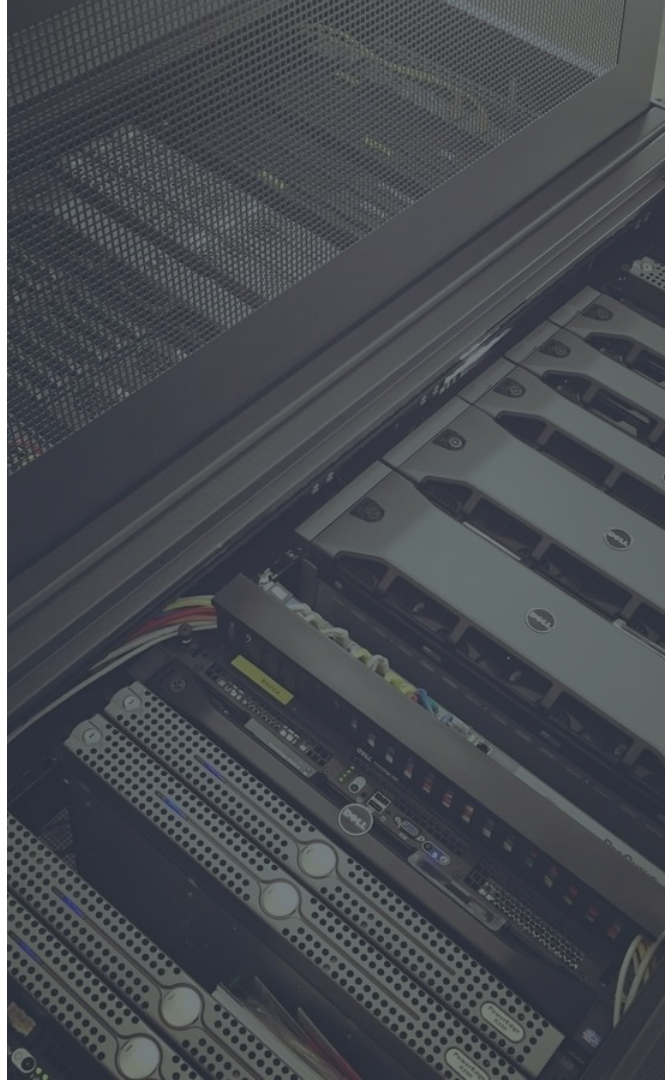
1. THE OLD WINDOWS AGENT – REACHING ITS LIMITS
2. GREENFIELD REVAMP – THE NEW WINDOWS AGENT
3. ARCHITECTURE OF WINDOWS AGENT 2.0
4. CHANGES FROM A USER'S PERSPECTIVE
5. SHOWCASE
6. GOING FORWARD



THE OLD WINDOWS AGENT

The old Windows Agent has reached its limits

- Windows Agent: A reliable work horse, used by a large share of our customers
- But: Has become hard to maintain and extend
 - Still solves low level problems, abstractions available today
 - Linux-based toolchain, hybrid world causes tricky issues
 - Limited diagnostic tools
 - Plug-in set written in multiple languages





THE OLD WINDOWS AGENT

This is the guy to fix this:

Sergey Kipnis

Time for a greenfield
revamp...



The new Windows Agent

- ◆ Principles of the new Windows Agent
 - ◆ Complete rewrite – 30.000 lines of code
 - ◆ Available from check**mk** 1.6
 - ◆ Simple logic, high quality, modern & clean code
 - ◆ Written Windows-native – compilation, installation, only MS-approved APIs
 - ◆ Only uses top-level C++ 17-20 code and modern tools
 - ◆ Standards-based MSI agent updates – no custom actions

Working on updates
30% complete
Don't turn off your computer

GREENFIELD REVAMP

New Agent Improvements



Better config structure (YAML; ini still possible)



Great diagnostic tools



Allows automatic migration from old to new Windows Agent



Easier extensible



Very high test coverage; integration tests across multiple Windows platforms

Examples

Config – ini...

```
[global]
    crash_debug = yes

[ps]
    use_wmi = no
    full_path = no

[winperf]
    counters = 10332:msx_queues
    counters = 638:tcp_conn
    counters = Terminal Services:ts_sessions
```

... vs. YaML

```
global:
  logging:
    public: yes
    file :
    debug: yes
    windbg: yes
    eventlog: yes

ps:
  enabled: yes
  use_wmi: yes
  full_path: yes

winperf:
  enabled: yes
  exe: agent
  prefix: winperf
  timeout: 10
  counters:
    - 234: phydisk
    - 510: if
    - 638: tcp_conn
    - Terminal Services: ts_sessions
```

EXAMPLES

Diagnostic command: **Help**

Command Line Prompt: **-help**

```
C:\Program Files (x86)\check_mk_service>check_mk_agent.exe -help
```

Normal Usage:

```
check_mk_service32.exe <-install|-remove|-help>  
-install      - install as a service  
-remove       - remove service  
-help         - usage
```

Common Testing:

```
check_mk_service32.exe <test|-test [self seconds]|-exec>  
test           - legacy test  
-test          - short test. If self added, then agent simulates connection from monitoring site with seconds period  
-exec          - exec as app(adhoc)
```

Realtime Testing:

```
check_mk_service32.exe <-rt>  
-rt            - test realtime data with all sections and encryption
```

To Convert Legacy Agent Ini File into Agent Yml file:

```
check_mk_service32.exe -cvt <inifile> [yamlfile]  
inifile - from Legacy Agent  
yamlfile - name of an output file(optional)
```

To Activate/Deactivate Legacy Agent:

```
check_mk_service32.exe <-stop_legacy|-start_legacy>  
-stop_legacy - stop and deactivate legacy agent  
-start_legacy - activate and start legacy agent(only for testing)
```

To Upgrade Legacy Agent:

```
check_mk_service32.exe -upgrade [force]  
force - optional parameter to force upgrading
```

To Install Bakery Files, plugins.cap and check_mk.ini, in install folder:

```
check_mk_service32.exe -cap
```

To test Sections individually:

```
check_mk_service32.exe -section <name> [number [trace]]  
name - allowed only df  
number - not 0: pause between tests in seconds, count of tests are infinite. 0 - test once  
trace - log output on the stdio  
example 'check_mk_service32 -section df 5 trace'  
test section df infinitely long with pause 5 seconds and log output on stdio
```

EXAMPLES

Diagnostic command: **Realtime**

Command Line Prompt: **-rt**

<<<df:sep(9)>>>

OS	NTFS	716858364	620179244	96679120	87%	C:\
D:\	FAT32	98304	25926	72378	27%	D:\
TOSHIBA_EXT	NTFS	976656608	950003572	26653036	98%	F:\

<<<mem>>>

MemTotal:	33278368	kB
MemFree:	10172112	kB
SwapTotal:	28986784	kB
SwapFree:	18014398509020740	kB
PageTotal:	62265152	kB
PageFree:	9710868	kB
VirtualTotal:	2097024	kB
VirtualFree:	2005468	kB

<<<winperf_processor>>>

1555583560.18 238 2156255

13 instances: 0 1 2 3 4 5 6 7 8 9 10 11 _Total

-232 2435814687500 2519840156250 2475045937500 2549546718750 2505817187500 2584949531250 2509664531250 2566684531250 239902203

1250 2609585781250 2414627500000 2587123281250 2513143489583 100nsec_timer_inv

-96 132573281250 91308593750 139624687500 88634062500 115795625000 101409375000 125902656250 108052812500 154456250000 6808359

3750 145389843750 78991562500 112518528645 100nsec_timer

-94 168925781250 126160000000 122638125000 99127968750 115695937500 50949843750 101741562500 62571250000 183830312500 59639218

750 177291250000 71193750000 111647083333 100nsec_timer

-90 781340117 586171180 630977687 401690895 745946324 489103813 594864758 407948862 781774906 458263411 1085623289 473690719 3

142428665 counter

458 21418593750 12300000000 528281250 129062500 553906250 409843750 265781250 177968750 196093750 154687500 431875000 263437500

2146627604 100nsec_timer

460 38614218750 3464062500 1583750000 882031250 1202812500 635000000 933437500 805937500 1217812500 770625000 1480937500 88578

1250 4373033854 100nsec_timer

1096 56229422 10069685 13226485 4969105 9129139 7446563 7615267 5250273 8327567 5111658 11946164 7009386 146330714 counter

1098 11 0 0 0 0 0 0 0 0 0 0 1 12 rawcount

1508 2312539152992 2405106196010 2339118670893 2483865119175 2372162499351 2502746725209 2386133434073 2482249094655 221338729

3555 2520190494945 2208209389499 2507119079657 2394402262501 100nsec_timer

1510 13742592555 8045878029 14136824392 9832118385 9978373193 8507699891 13866354475 7882867833 15487434473 5659444036 1632051

0978 6876123881 10861351843 100nsec_timer

1512 27124007238 20916640870 30383528441 22575411762 21386151661 27820901382 28358650674 18763340105 26005804934 13289400683 2

9260717813 17549792659 23619529018 100nsec_timer

1514 2271672553199 2376143677111 2294598318060 2451457589028 2340797974497 2466418123936 2343908428924 2455602886717 217189405

4148 2501241650226 2162628160708 2482693163117 2359921381639 100nsec_timer

1516 18018284 6159378 14239213 5913381 11291452 6291559 12758200 5657344 16374343 6571409 17872127 7132303 128278993 bulk_count

1518 15650994 6546575 14237392 5064975 11020314 7752819 11969280 4935343 14037321 6511574 17923447 8061840 123711874 bulk_count

1520 574754581 392439283 442993732 221966910 530322412 390762906 415190141 307243411 546044104 351257224 816775147 378918669 5

368668520 bulk_count

Press any key to STOP testing Realtime Sections

EXAMPLES

Diagnostic command: **Individual Sections (df)**

Command Line Prompt:

```
-section df 5
```

To test Sections individually:

check_mk_service32.exe -section <name> [number [trace]]

name - allowed only df

number - not 0: pause between tests in seconds, count of tests are infinite. 0 - test once

trace - log output on the stdio

example 'check_mk_service32 -section df 5 trace'

test section df infinitely long with pause 5 seconds and log output on stdio

C:\Program Files (x86)\check_mk_service>check_mk_agent.exe -section df 5

<<<df:sep(9)>>>

OS	NTFS	716858364	620179960	96678404	87%	C:\
D:\	FAT32	98304	25926	72378	27%	D:\
TOSHIBA_EXT	NTFS	976656608	950003572	26653036	98%	F:\

<<<df:sep(9)>>>

OS	NTFS	716858364	620179960	96678404	87%	C:\
D:\	FAT32	98304	25926	72378	27%	D:\
TOSHIBA_EXT	NTFS	976656608	950003572	26653036	98%	F:\

<<<df:sep(9)>>>

OS	NTFS	716858364	620179960	96678404	87%	C:\
D:\	FAT32	98304	25926	72378	27%	D:\
TOSHIBA_EXT	NTFS	976656608	950003572	26653036	98%	F:\

<<<df:sep(9)>>>

OS	NTFS	716858364	620179960	96678404	87%	C:\
D:\	FAT32	98304	25926	72378	27%	D:\
TOSHIBA_EXT	NTFS	976656608	950003572	26653036	98%	F:\

<<<df:sep(9)>>>

OS	NTFS	716858364	620179960	96678404	87%	C:\
D:\	FAT32	98304	25926	72378	27%	D:\
TOSHIBA_EXT	NTFS	976656608	950003572	26653036	98%	F:\

AC

C:\Program Files (x86)\check_mk_service>

EXAMPLES

Diagnostic command: **Self Diagnostic**

Command Line Prompt:

```
-test self 10
```

```
Program Files (x86)\check_mk_service>check_mk_agent.exe -test self 10
Successful start of thread
Press any key to stop
Pre Start actions
cma::provider::PluginsProvider::loadConfig: entering
Plugin Entry C:\ProgramData\CheckMK\Agent\plugins\win_license.bat has invalid config async: false and cache_age: 600. Setting
as async.
Important params changed, reset retry
Plugin C:\ProgramData\CheckMK\Agent\plugins\mk_inventory.vbs changes this mode to SYNC
breakAsync C:\ProgramData\CheckMK\Agent\plugins\mk_inventory.vbs
Important params changed, reset retry
Plugin C:\ProgramData\CheckMK\Agent\plugins\netstat_an.bat changes this mode to SYNC
breakAsync C:\ProgramData\CheckMK\Agent\plugins\netstat_an.bat
Important params changed, reset retry
Plugin C:\ProgramData\CheckMK\Agent\plugins\win_license.bat changes this mode to ASYNC
Data 'C:\ProgramData\CheckMK\Agent\plugins\win_license.bat' is obsolete, age is '403712' seconds
restarting async plugin 'C:\ProgramData\CheckMK\Agent\plugins\win_license.bat'
restarted thread for plugin 'C:\ProgramData\CheckMK\Agent\plugins\win_license.bat'
Process 28976 is active
cma::provider::PluginsProvider::loadConfig: entering
Pre Start actions ended
cma::world::ExternalPort::ioThreadProc: started
main wait loop
Starting IO ipv6:false, proposed port:0...
Modes for a key set correctly
Testing mode enabled for RT Thread
Received 3323 bytes
Process 28976 is active
Process 28976 is active
Process 28976 is active
Process 28976 is active
Testing mode enabled for RT Thread
Process 28976 has exit code 0
Thread OFF: C:\ProgramData\CheckMK\Agent\plugins\win_license.bat
Testing mode enabled for RT Thread
Testing mode enabled for RT Thread
Testing mode enabled for RT Thread
Server is going to stop
cma::srv::ServiceProcessor::stopService: called
Stop request is set
main wait loop END
Thread is stopped
Shutting down IO...
Stopping execution
```

EXAMPLES

Diagnostic command: **Self Diagnostic Part 2**

```
Skipping 'skype' by config
Skipping 'spool' by config
openhwaremonitor is skipped by config
Skipping 'openhwaremonitor' by config
openhwaremonitor is skipped by config
Looking for default agent
Using file 'C:\Program Files (x86)\check_mk_service\check_mk_agent.exe' for winperf
Max Timeout set to valid value 10
Exec C:\Program Files (x86)\check_mk_service\check_mk_agent.exe for winperf started
waiting futures(only start)
asynRunStdCmd: "C:\Program Files (x86)\check_mk_service\check_mk_agent.exe" -runonce winperf mail:\\.\mailslot\Global\WinAge
ntTest_0 id:403878584849194 timeout:10 ip:127.0.0.1 234:phydisk 510:if 638:tcp_conn Terminal*Services:ts_sessions
futures ready in 22 milliseconds
Testing mode enabled for RT Thread
Testing mode enabled for RT Thread
Testing mode enabled for RT Thread
Testing mode enabled for RT Thread
Testing mode enabled for RT Thread
Testing mode enabled for RT Thread
Testing mode enabled for RT Thread
Testing mode enabled for RT Thread
Server is going to stop
cma::srv::ServiceProcessor::stopService: called
Stop request is set
main Wait Loop END
Thread is stopped
Shutting down IO...
Stopping execution
Testing mode enabled for RT Thread
Testing mode enabled for RT Thread
c:\z\m\check_mk\agents\wnx\src\engine\service_processor.h:490: no full answer: awaited 1, received 0
cma::provider::CheckMk::makeBody: entering
Absent/Empty node 'only_from' type is 1
The section "systemtime" is disabled in config
Nothing
Send 715 from 715 data to send 715
Send 715 bytes of data
Received 715 bytes
cma::world::ExternalPort::ioThreadProc: one shot ended 1
cma::world::ExternalPort::ioThreadProc: terminated from outside 2
IO ends...
breakAsync C:\ProgramData\CheckMK\Agent\plugins\win_license.bat
waiting for testing thread
Leaving testing thread
```

EXAMPLES

Upgrade from old to new **without force**

Command Line Prompt:

-upgrade

```
C:\Program Files (x86)\check_mk_service>check_mk_service.exe -upgrade
Starting upgrade process...
Protocol File C:\Program Files (x86)\check_mk_service\upgrade.protocol exists, upgrade not required
End of!
```

EXAMPLES

Upgrade from old to new **with force**

Command Line Prompt:

```
-upgrade force
```

```
C:\Program Files (x86)\check_mk_service>check_mk_service.exe -upgrade force
Starting upgrade process...
Update is forced by command line
Legacy Agent is found in 'C:\Program Files (x86)\check_mk'
Find, stop and deactivate
Stopping check_mk_agent...
Service check_mk_agent stopping ...
Service 'check_mk_agent' is already stopped.
Checking check_mk_agent status...
Deactivate check_mk_agent ...
Killing open hardware monitor...
Stopping winring0_1_2_0...
Service winring0_1_2_0 stopping ...
Service 'winring0_1_2_0' is already stopped.
Processing 'C:\Program Files (x86)\check_mk\config':
Copy from 'C:\Program Files (x86)\check_mk\config' to 'C:\ProgramData\CheckMK\Agent\config'
Processing 'C:\Program Files (x86)\check_mk\plugins':
Copy from 'C:\Program Files (x86)\check_mk\plugins' to 'C:\ProgramData\CheckMK\Agent\plugins'
    Copy 'C:\Program Files (x86)\check_mk\plugins\mk_inventory.vbs'
    Copy 'C:\Program Files (x86)\check_mk\plugins\windows_if.ps1'
Processing 'C:\Program Files (x86)\check_mk\local':
Copy from 'C:\Program Files (x86)\check_mk\local' to 'C:\ProgramData\CheckMK\Agent\local'
Processing 'C:\Program Files (x86)\check_mk\mrpe':
Copy from 'C:\Program Files (x86)\check_mk\mrpe' to 'C:\ProgramData\CheckMK\Agent\mrpe'
Processing 'C:\Program Files (x86)\check_mk\state':
Copy from 'C:\Program Files (x86)\check_mk\state' to 'C:\ProgramData\CheckMK\Agent\state'
    Copy 'C:\Program Files (x86)\check_mk\state\eventstate.txt'
    Copy 'C:\Program Files (x86)\check_mk\state\eventstate_10_3_1_214.txt'
    Copy 'C:\Program Files (x86)\check_mk\state\logstate.txt'
    Copy 'C:\Program Files (x86)\check_mk\state\mk_inventory.10.3.1.214'
    Copy 'C:\Program Files (x86)\check_mk\state\mk_inventory.local'
Removing C:\ProgramData\CheckMK\Agent\check_mk.user.yml
Removing C:\ProgramData\CheckMK\Agent\bakery\check_mk.bakery.yml
Local ini File is absent or has no data
File C:\Program Files (x86)\check_mk\check_mk.ini is successfully converted
User ini File C:\Program Files (x86)\check_mk\check_mk.ini was converted to YAML file C:\ProgramData\CheckMK\Agent\check_mk.user.yml
End of!

C:\Program Files (x86)\check_mk_service>
```

EXAMPLES

Realtime Log Output mit DbgView



#	Time	Debug Print
1...	60816.015...	[42268] agent: [Trace] Skipping 'wmi_webservices' by config
1...	60816.015...	[42268] agent: [Trace] msexch is skipped by config
1...	60816.015...	[42268] agent: [Trace] Skipping 'msexch' by config
1...	60816.01562500	[42268] agent: [Trace] Skipping 'mrpe' by config
1...	60816.015...	[42268] agent: [Trace] Skipping 'skype' by config
1...	60816.015...	[42268] agent: [Trace] Skipping 'spool' by config
1...	60816.015...	[42268] agent: [Trace] openhardwaremonitor is skipped by config
1...	60816.019...	[42268] agent: [Trace] Skipping 'openhardwaremonitor' by config
1...	60816.019...	[42268] agent: [Trace] openhardwaremonitor is skipped by config
1...	60816.019...	[42268] agent: Looking for default agent
1...	60816.019...	[42268] agent: Using file 'C:\Program Files (x86)\check_mk_service\check_mk_agent.exe' for winperf
1...	60816.019...	[42268] agent: Max Timeout set to valid value 10
1...	60816.019...	[42268] agent: Exec C:\Program Files (x86)\check_mk_service\check_mk_agent.exe for winperf started
1...	60816.019...	[42268] agent: waiting futures(only start)
1...	60816.019...	[42268] agent: async RunStdCmd: "C:\Program Files (x86)\check_mk_service\check_mk_agent.exe" -runonce winperf mail:\\.\mailslot\Global\W...
1...	60816.023...	[42268] agent: futures ready in 2 milliseconds
1...	60816.035...	[17920] agent: From ip 10.3.1.214
1...	60816.085...	[17920] agent: [Trace] Key Index Terminal Services is not found, looking in registry
1...	60816.179...	[17920] agent: [Trace] We are using mail with address \\.\mailslot\Global\WinAgentTest_0
1...	60816.179...	[17920] agent: [Trace] Sending data 'winperf' id is [403995621597167] length [2608]
1...	60816.179...	[17920] agent: Send to 403995621597167 2608
1...	60816.195...	[42268] agent: [Trace] Received 2736 bytes from winperf
1...	60816.195...	[42268] agent: [Trace] cma::provider::CheckMk::makeBody: entering
1...	60816.195...	[42268] agent: [Trace] Absent/Empty node 'only_from' type is 1
1...	60816.195...	[42268] agent: [Trace] The section "systemtime" is disabled in config
1...	60816.195...	[42268] agent: [Trace] Nothing
1...	60816.195...	[42268] agent: Send 3324 from 3324 data to send 3324
1...	60816.195...	[42268] agent: Send 3324 bytes of data
1...	60816.199...	[42268] agent: [Trace] cma::world::ExternalPort::ioThreadProc: one shot ended 1
1...	60816.542...	[42268] agent: Testing mode enabled for RT Thread
1...	60817.542...	[42268] agent: Testing mode enabled for RT Thread
1...	60818.542...	[42268] agent: Testing mode enabled for RT Thread
1...	60819.546...	[42268] agent: Testing mode enabled for RT Thread
1...	60820.546...	[42268] agent: Testing mode enabled for RT Thread
1...	60821.542...	[42268] agent: Testing mode enabled for RT Thread
1...	60822.546...	[42268] agent: Testing mode enabled for RT Thread
1...	60823.546...	[42268] agent: Testing mode enabled for RT Thread

CHANGES FROM A USER PERSPECTIVE

What changes, what doesn't?

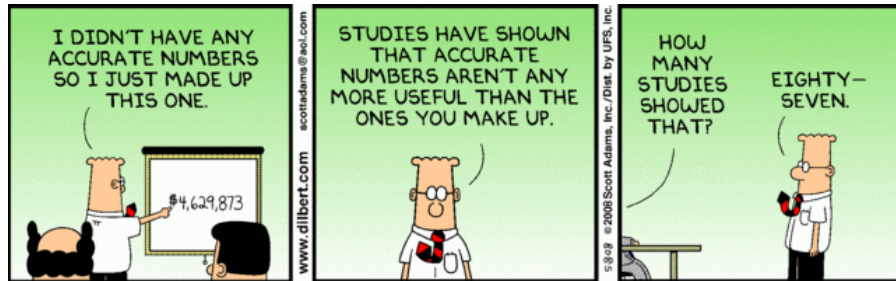
- RELAX, not much changes...
 - Programmed in C++
 - Installation as a Windows service
 - Same system requirements
 - Same checks, same plugins



CHANGES FROM A USER PERSPECTIVE

Comparison shows near identical resource need

	OLD	NEW
CPU Load (avg)	< 1%	< 1%
CPU Load (max)	8-20%	8-20%
RAM	2-6 MB	2-3 MB
Disk Space	2.2 MB	2.2 MB
Latency	< 1 Sec	< 1 Sec



What about the old agent?

- Windows Server
- Windows 10
- Windows 8 / 8.1
- Windows 7
- Windows Vista



New Windows Agent

-
- Windows XP
 - Windows ME
 - ...



Old Windows Agent
(still maintained)



GOING FORWARD

Our Windows Agent Roadmap

checkmk 1.6

Everything you saw
today...

checkmk 1.7 and on

- First Ideas:
 - Adding Python
 - GUI for Diagnostics
 - Better homogeneity of plugins
 - Extension into other Windows domains

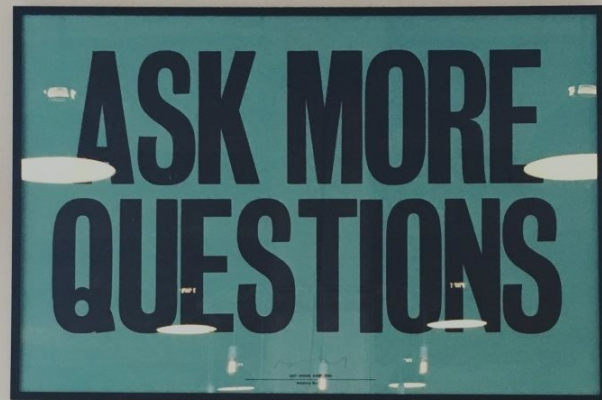


GOING FORWARD

A final thought...

- ◆ The new Windows Agent...
 - ◆ ...brings a new level of Windows systems monitoring
 - ◆ ...offers the quality that checkmk delivers for Linux world
- ◆ But...
 - ◆ ...the agent is only the first step
 - ◆ ...**it's your ideas and requirements driving us further!**

So let us know!



Any questions?

Thank you!



tribe29 GmbH
Kellerstraße 29
81667 München
Deutschland

Web — tribe29.com
E-Mail — mail@tribe29.com