The New Windows Monitoring – One Year Later

CHECKMK CONFERENCE #6 – MUNICH, APRIL 28, 2020

Marcel Arentz
Product Manager
tribe29

Sergey Kipnis
Developer
tribe29
Agenda

1. LESSONS LEARNT SINCE RELEASE
2. NEW FEATURES FOR WINDOWS AGENT 1.7
3. WINDOWS ROADMAP AFTER 1.7
Smoooth first months in operation

**TICKETS**
Less than 80 support tickets since launch

**WERKS**
Less than 10 bug fixes required

**TYPICAL ISSUES**
- Migrating from 1.5 to 1.6
- Architecture changes in 1.6
- Agent Updater vs. AV scanner
LESSONS LEARNT SINCE RELEASE

Uncertainties with migration from windows agents 1.5 to 1.6

Typical questions

- Why is the new agent not replacing the old?
- When should I remove the old agent?
- Why are not all files of the old agent deleted?

Installation procedure of the agent has mostly not changed...
...however the removal of the old agent is different
Best practice for Windows agent update

1. Install new agent
2. Remove old agent
3. Update firewall
4. Check files & folders

- Install new agent either...
  - ...execute MSI file
  - ...bake and sign agents after update of Checkmk server
- Legacy agent will not be removed by default – however disabled
- Preserve old agent in case something goes wrong
Best practice for Windows agent update

1. Install new agent
2. Remove old agent
3. Update firewall
4. Check files & folders

- Remove the old agent once you tested and/or productive system for some hosts work well
- Either...
  - ...execute the uninstaller
  - ...use automatic removal by enabling checkbox in the installer (e.g. for the rollout to remaining hosts)
  - ...use automatic removal by creating a rule in ‘Legacy Agent Management’
LESSONS LEARNT SINCE RELEASE

Best practice for windows agent update

1. Install new agent
2. Remove old agent
3. Update firewall
4. Check files & folders

- Adjust manually set firewall rules if needed:

**New firewall**

```
C:\Windows\System32> netsh advfirewall firewall add rule name="Check_MK" ^
More? description="Monitoring" dir=in localport=6556 protocol=tcp action=allow ^
More? program="%ProgramFiles(x86)\checkmk\service\check_mk_agent.exe" ^
More? profile=private,domain enable=yes
OK.
```

**Adjust firewall**

```
C:\Windows\System32> netsh advfirewall firewall set rule name="Check_MK" ^
More? new program="%ProgramFiles(x86)\checkmk\service\check_mk_agent.exe"
Updated 1 rule(s).
Ok.
```
**LESSONS LEARNT SINCE RELEASE**

Best practice for windows agent update

1. Install new agent
2. Remove old agent
3. Update firewall
4. Check files & folders

- Manually added files in the old agent folder will remain (together with the folder) after the removal of the old agent
- Common behavior (of all operating systems) so that you need to remove unwanted files manually

More details to architecture difference on following slides

All information can also be found in our handbook:

Chapter 4.3
LESSONS LEARNT SINCE RELEASE

Architecture changes from 1.5 to 1.6

Typical questions

- What is the difference between old and new agent?
- Where do I add my custom configuration options?
- How do I specify which plugins to execute?
- Where do I store the configuration for my plugins?
- What is the new folder ‘C:\ProgramData\checkmk\agent’?
# LESSONS LEARNT

## Differences between 1.5 and 1.6

<table>
<thead>
<tr>
<th>Topics</th>
<th>Version 1.5</th>
<th>Version 1.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent &amp; folders</td>
<td>Old agent not following Windows best practices</td>
<td>Files and folders differentiated</td>
</tr>
<tr>
<td></td>
<td>● Program and user files in same folder</td>
<td>● Application files shipped with installer:</td>
</tr>
<tr>
<td></td>
<td>● No transparency on which files have been shipped with the software and</td>
<td>‘C:\Program Files (x86)\Checkmk\service\’</td>
</tr>
<tr>
<td></td>
<td>which have been added later</td>
<td>● Custom configurations, log files of the</td>
</tr>
<tr>
<td></td>
<td>● All files: ‘C:\Program Files (x86)\check_mk’</td>
<td>agent itself, plugins to execute:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>‘C:\ProgramData\checkmk\agent’</td>
</tr>
</tbody>
</table>
## Differences between 1.5 and 1.6

<table>
<thead>
<tr>
<th>Topics</th>
<th>Version 1.5</th>
<th>Version 1.6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Config file</td>
<td>• Format ini</td>
<td>• Format yaml</td>
</tr>
<tr>
<td>format</td>
<td>• check_mk.ini</td>
<td>• check_mk.yml</td>
</tr>
<tr>
<td></td>
<td>• check_mk.local.ini</td>
<td>• check_mk.bakery.yml</td>
</tr>
<tr>
<td></td>
<td>• Relatively flat structure</td>
<td>• check_mk.user.yml</td>
</tr>
<tr>
<td></td>
<td>• Ease to use for simple configurations</td>
<td>• Also classical key-value pair to configure your agent</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Easier to use if you want to handle structured data (e.g. complex</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configurations)</td>
</tr>
<tr>
<td>Topics</td>
<td>Version 1.5</td>
<td>Version 1.6</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Plugins | - Manually download each plugin from Checkmk server into plugins folder  
                  - Configuration of plugin execution with several independent keys  
                  - No distinction between bakery and default configuration; user configuration not well known | - Plugins executed by default saved in ‘C:\ProgramData\checkmk\agent\plugins’  
                  - No need to download plugins from Checkmk server anymore  
                  - Simply copy plugin from application folder to ‘ProgramData’ folder |

Planned: Enhance result page of installer, include read me.txt

All information can also be found in our handbook: Chapter 3, 6 & 7
Agent Updater vs. Anti Virus scanner

**False positives**
- AV creates false positives due to pyinstaller binaries
- Issue inherited by pyinstaller perceived as threat
- As long as pyinstaller is used, issue will persist

**Quick fix**
- Step 1: Get MSI package on windows system
  - Encrypt installation package
- Step 2: Execute agent with plugins
  - Configure exceptions in AV

**True solution**
- Avoid pyinstaller
- Needs larger rework hence will come with 1.7
Agenda

1. LESSONS LEARNT SINCE RELEASE
2. NEW FEATURES FOR WINDOWS AGENT 1.7
3. WINDOWS ROADMAP AFTER 1.7
New Features for Windows agent 1.7

- Native Python plug-in support
  - Automatic firewall configuration
  - Execute plugins with specific permission
  - Control removal of agent
Native Python plug-in support

**Packaging**
- Python 3.8
- Defined set of useful modules
- Configurable

**Advantages**
- Unified Python preconditions on every Windows host
- Plugins can be created in Python
- Cross platform plugins are possible
- Increased reliability and performance
- Standard plugins (logwatch, agentupdater, etc.) can be delivered without pyinstaller,
  - no more issues with AV
  - increased transparency
# New Features for Windows Agent 1.7

## Automatic firewall configuration

### Integration
- Enabled by default
- Fully automated delivery
- Simple toggle in GUI

### Advantages
- Centralized firewall configuration and administration on Checkmk server
- Both initial setup and subsequent changes included
- Reduction in efforts and increase in quality
- Less error prone
NEW FEATURES FOR WINDOWS AGENT 1.7

Execute plugins with specific permission

Specific permission
- Define user group to obtain specific permissions
- Alternatively specify required credentials
- Fully automated execution

Groups
- No credentials in config files on Checkmk server and host
- Definition of correct user group is sufficient
- ActiveDirectory not supported

Specific
- No limitation for specific permissions, e.g. ActiveDirectory is supported
- Credentials in plain text in Checkmk and host
# New Features for Windows Agent 1.7

## Control removal of agent

### Deinstallation
- Remove own files per default – „smart clear“
- Simple toggle in GUI for full removal or full preservation
- Fully automated execution

### Advantages
- Full control over agent / removal behavior
- Clean status / installation
- User files can be preserved or fully removed if wanted
Agenda

1. LESSONS LEARNT SINCE RELEASE
2. NEW FEATURES FOR WINDOWS AGENT 1.7
3. WINDOWS ROADMAP AFTER 1.7
## Windows Roadmap After 1.7

### Focus on Windows Application Monitoring

<table>
<thead>
<tr>
<th>Windows Application Monitoring</th>
<th>Cross Platform Monitoring</th>
<th>Windows Agent Improvements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New applications</strong></td>
<td><strong>New</strong></td>
<td></td>
</tr>
<tr>
<td>- Microsoft 365</td>
<td>- Db2</td>
<td>- Diagnostic</td>
</tr>
<tr>
<td>- IIS</td>
<td>- mongoDB</td>
<td>- Performance</td>
</tr>
<tr>
<td>- ...</td>
<td>- SAP (maybe)</td>
<td>- Features</td>
</tr>
<tr>
<td><strong>Improvements</strong></td>
<td>- mysql (maybe)</td>
<td>- ...</td>
</tr>
<tr>
<td>- Exchange</td>
<td>- ...</td>
<td></td>
</tr>
<tr>
<td>- Hyper-V</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
It’s your ideas and requirements that drive us!

Let us know by posting your wishes in our Slack channel
Any questions?
Thank you