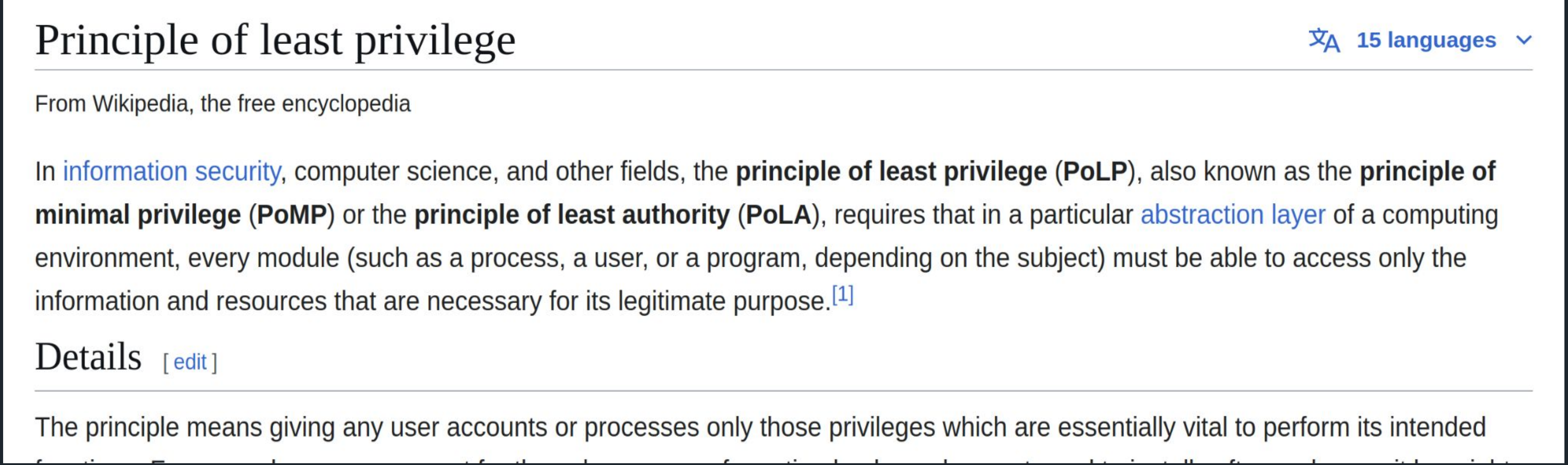
Checkmk Conference #11

How to run the agent as non-root

May 20, 2025 - Live from Paulaner am Nockherberg, Munich

Andreas Umbreit
Software Developer
Checkmk GmbH

IT policies. To fight or not to fight?



Principle of least privilege

15 languages

From Wikipedia, the free encyclopedia

In information security, computer science, and other fields, the **principle of least privilege** (**PoLP**), also known as the **principle of minimal privilege** (**PoMP**) or the **principle of least authority** (**PoLA**), requires that in a particular abstraction layer of a computing environment, every module (such as a process, a user, or a program, depending on the subject) must be able to access only the information and resources that are necessary for its legitimate purpose.[1]

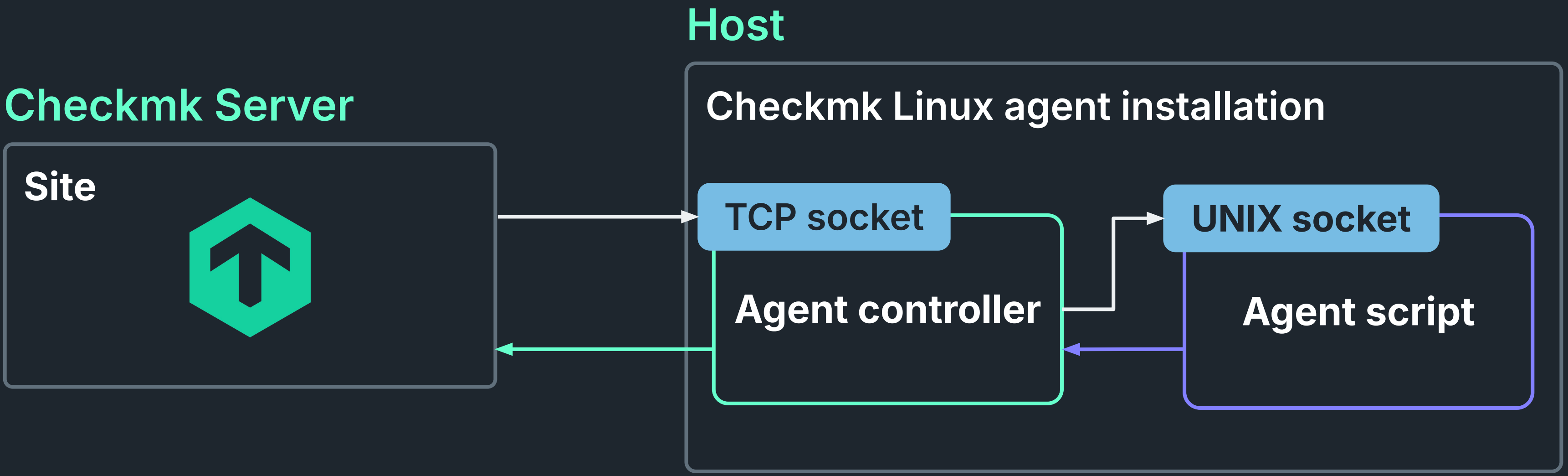
Details [edit]

The principle means giving any user accounts or processes only those privileges which are essentially vital to perform its intended

We want to make your life easier.
Fewer workarounds.

The Checkmk agent is secure ...

... as it is not receiving any incoming data from the network



🟩 Executed as cmk-agent (unprivileged)

🟪 Executed as root

The foundation for ‘non-root agent’ in UNIX/Linux

Foundation

Agent is deployed in one directory

Status quo: Where are files currently installed?

- All over the place
- (Loosely) following the UNIX filesystem hierarchy standard (FHS)
- Violating conventions
- Inconsistent naming

```
/usr/lib/check_mk_agent/
├── local
└── plugins

/etc/check_mk/

/var/lib/check_mk_agent/
├── cache
├── job
├── rtc_remotes
└── spool

/usr/bin

/var/lib/cmk-agent/
└── scripts
```

/../.. = configurable

From 2.4, installation into one directory possible

- Better overview of all agent files
  - And their permissions!
- Only one configuration value needed for custom location
- Not active by default in Checkmk 2.4

```
/opt/checkmk/agent/default/
├── package
│   ├── agent
│   ├── bin
│   ├── config
│   ├── local
│   ├── plugins
│   └── scripts
└── runtime
    ├── cache
    ├── controller
    ├── job
    ├── log
    ├── rtc_remotes
    └── spool
```

/../.. = configurable

From 2.4, installation into one directory possible

Bonus:

Enabler for multiple agents on one host

Ensure that no files of one agent package overwrite a file of a different one.

/../.. = configurable

```
/opt/checkmk/agent/default/
├── package
│   ├── agent
│   ├── bin
│   ├── config
│   ├── local
│   ├── plugins
│   └── scripts
└── runtime
    ├── cache
    ├── controller
    ├── job
    ├── log
    ├── rtc_remotes
    └── spool
```

What about non-root?

New structure required for non-root agent

The ownership of the files depends on the deployment mode:

Root deployment mode

All directories and files

- Owned by **root**
- Exception: The agent controller's home directory is owned by the agent controller user.

Non-root deployment mode

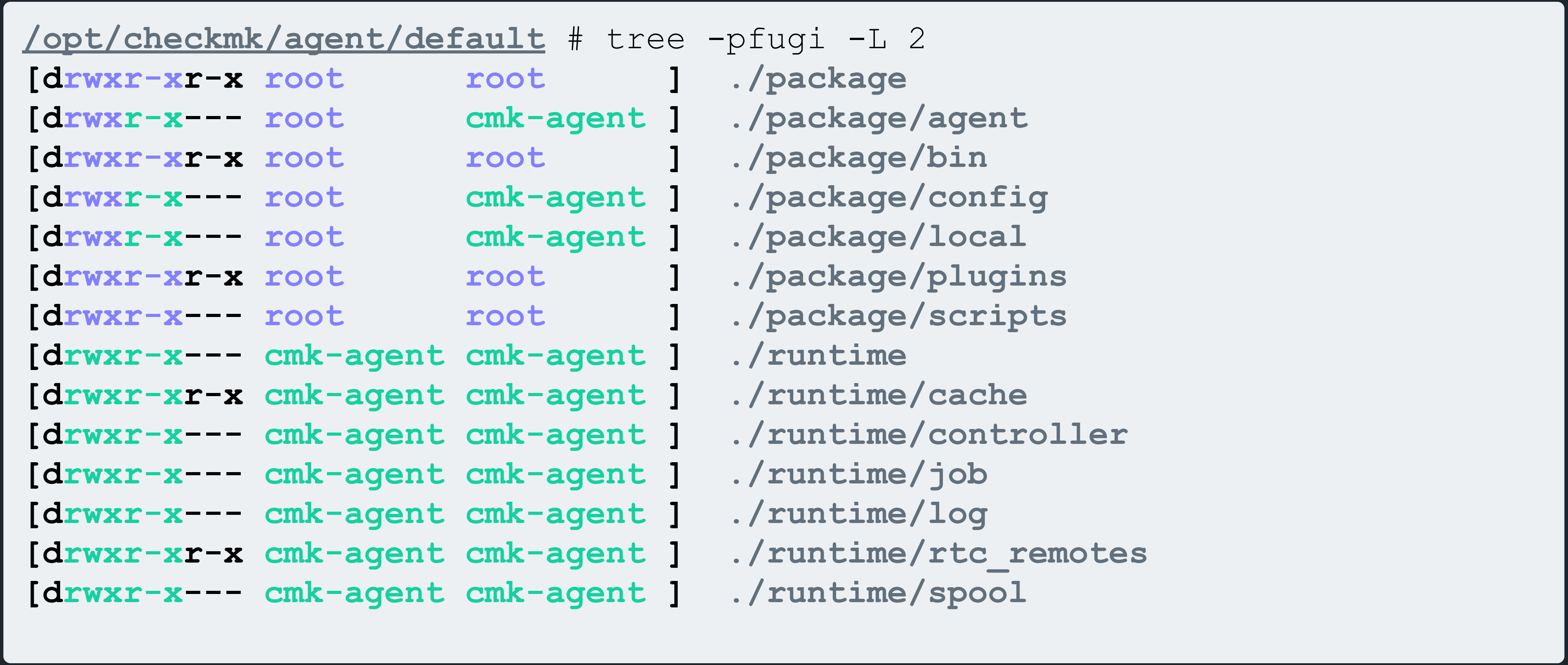
`package` directory & subdirectories

- Owned by **root**
- Group ownership for **agent user** where needed

`runtime` directory

- Owned by **agent user**
- Runtime files will be created and owned by the agent user

What it looks like



```
/opt/checkmk/agent/default # tree -pfugi -L 2
[drwxr-xr-x root      root      ]   ./package
[drwxr-x--- root      cmk-agent ]   ./package/agent
[drwxr-xr-x root      root      ]   ./package/bin
[drwxr-x--- root      cmk-agent ]   ./package/config
[drwxr-x--- root      cmk-agent ]   ./package/local
[drwxr-xr-x root      root      ]   ./package/plugins
[drwxr-x--- root      root      ]   ./package/scripts
[drwxr-x--- cmk-agent cmk-agent ]   ./runtime
[drwxr-xr-x cmk-agent cmk-agent ]   ./runtime/cache
[drwxr-x--- cmk-agent cmk-agent ]   ./runtime/controller
[drwxr-x--- cmk-agent cmk-agent ]   ./runtime/job
[drwxr-x--- cmk-agent cmk-agent ]   ./runtime/log
[drwxr-xr-x cmk-agent cmk-agent ]   ./runtime/rtc_remotes
[drwxr-x--- cmk-agent cmk-agent ]   ./runtime/spool
```

The path to ‘non-root agent’ in UNIX/Linux

Agent script
run unprivileged

Foundation
Agent is deployed in one directory

```
cat /opt/checkmk/agent/default/package/bin/check_mk_agent
...
init_sudo() {
    if inpath sudo && [ "$(whoami)" != "root" ]; then
        ROOT_OR_SUDO="sudo --non-interactive"
    else
        ROOT_OR_SUDO=""
    fi
    export ROOT_OR_SUDO
}
...
if inpath dmsetup; then
    echo '[dmsetup_info]'
    ${ROOT_OR_SUDO} dmsetup info -c --noheadings --separator \ -o
name,devno,vg_name,lv_name
fi
...
echo '<<<postfix_mailq>>
${ROOT_OR_SUDO} mailq 2>&1 | sed 's/^[^:]*: \(.*\)/\1/' | tail -n 6
...
```

```
cat /opt/checkmk/agent/default/package/bin/check_mk_agent
...
init_sudo() {
    if inpath sudo && [ "$(whoami)" != "root" ]; then
        ROOT_OR_SUDO="sudo --non-interactive"
    else
        ROOT_OR_SUDO=""
    fi
    export ROOT_OR_SUDO
}
...
if inpath dmsetup; then
    echo '[dmsetup_info]'
    ${ROOT_OR_SUDO} dmsetup info -c --noheadings --separator \ -o
name,devno,vg_name,lv_name
fi
...
echo '<<<postfix_mailq>>
${ROOT_OR_SUDO} mailq 2>&1 | sed 's/^[^:]*: \(.*\)/\1/' | tail -n 6
...
```

```
cat /opt/checkmk/agent/default/package/bin/check_mk_agent
...
init_sudo() {
    if inpath sudo && [ "$(whoami)" != "root" ]; then
        ROOT_OR_SUDO="sudo --non-interactive"
    else
        ROOT_OR_SUDO=""
    fi
    export ROOT_OR_SUDO
}
...
if inpath dmsetup; then
    echo '[dmsetup_info]'
    ${ROOT_OR_SUDO} dmsetup info -c --noheadings --separator \ -o
name,devno,vg_name,lv_name
fi
...
echo '<<<postfix_mailq>>
${ROOT_OR_SUDO} mailq 2>&1 | sed 's/^[^:]*: \(.*\)/\1/' | tail -n 6
...
```

```
cat /opt/checkmk/agent/default/package/bin/check_mk_agent
...
init_sudo() {
    if inpath sudo && [ "$(whoami)" != "root" ]; then
        ROOT_OR_SUDO="sudo --non-interactive"
    else
        ROOT_OR_SUDO=""
    fi
    export ROOT_OR_SUDO
}
...
if inpath dmsetup; then
    echo '[dmsetup_info]'
    ${ROOT_OR_SUDO} dmsetup info -c --noheadings --separator \ -o
name,devno,vg_name,lv_name
fi
...
echo '<<<postfix_mailq>>
${ROOT_OR_SUDO} mailq 2>&1 | sed 's/^[^:]*: \(.*\)/\1/' | tail -n 6
...
```

Implemented at multiple locations in the agent

Ready to use in your own scripts/plugins

```
cat /opt/checkmk/agent/default/package/agent/checkmk_sudoers_template
# This template contains sudo rules for all commands that currently apply
# the '$ROOT_OR_SUDO' variable set in the agent. Copy to/etc/sudoers.d
# to enable the Checkmk agent user to run these commands successfully.
# After copying, edit with
# 'visudo -f /etc/sudoers.d/checkmk_agent_sudoers_template' for
# further customization.
#
# Disclaimer: This file is called template for a reason.
# Please challenge it with your own security requirements before copying
# it blindly, and modify it accordingly!
...
...
```

Has to be deployed manually.
→ You are in control!

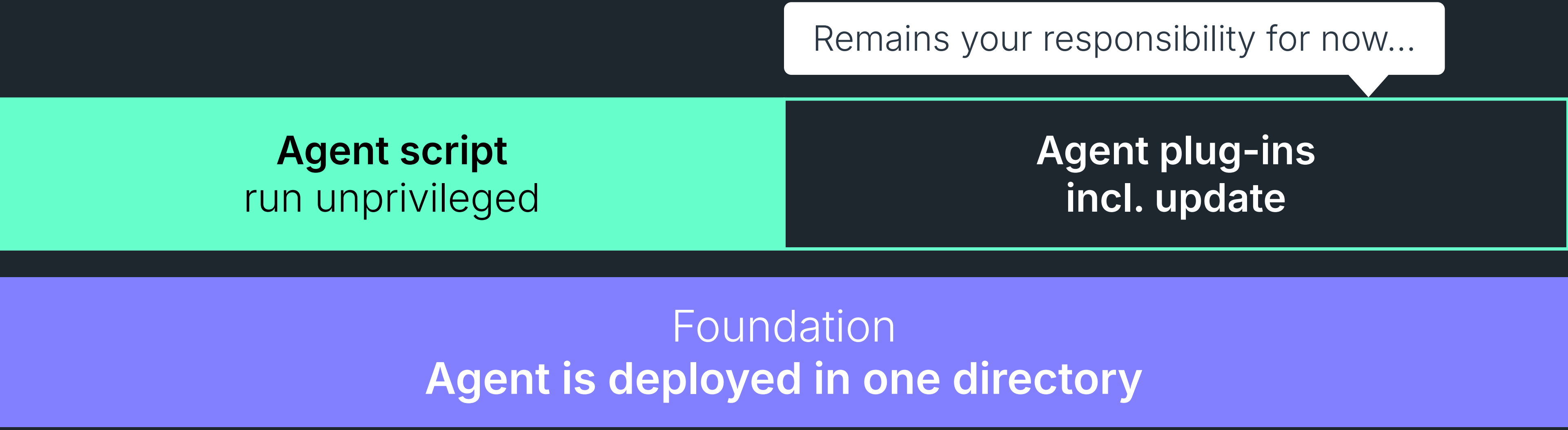
Whole usage is optional.

Add your own

```
...
...
# Common across all agents
cmk-agent ALL=(root) NOPASSWD: /usr/sbin/mailq ""

# Linux specific
cmk-agent ALL=(root) NOPASSWD: /usr/sbin/dmsetup info -c --noheadings
--separator \  -o name\,devno\,vg_name\,lv_name
cmk-agent ALL=(root) NOPASSWD: /usr/bin/omd status --bare
cmk-agent ALL=(%omd) NOPASSWD: /omd/versions/*/bin/cmk-monitor-apache
cmk-agent ALL=(%omd) NOPASSWD: /omd/versions/*/bin/cmk-monitor-broker
cmk-agent ALL=(%omd) NOPASSWD: /omd/versions/*/bin/cmk-monitor-diskusage
cmk-agent ALL=(%omd) NOPASSWD: /omd/versions/*/bin/cmk-monitor-mknotifyd
cmk-agent ALL=(%omd) NOPASSWD: /omd/versions/*/bin/cmk-monitor-core
cmk-agent ALL=(%omd) NOPASSWD: /omd/versions/*/bin/cmk-monitor-mkbackup
cmk-agent ALL=(root) NOPASSWD: /opt/VRTSvcs/bin/haclus
cmk-agent ALL=(root) NOPASSWD: /opt/VRTSvcs/bin/hasys
cmk-agent ALL=(root) NOPASSWD: /opt/VRTSvcs/bin/hagrp
cmk-agent ALL=(root) NOPASSWD: /opt/VRTSvcs/bin/hares
```

But …



Remains your responsibility for now…

Agent script
run unprivileged

Agent plug-ins
incl. update

Foundation
Agent is deployed in one directory

New ruleset

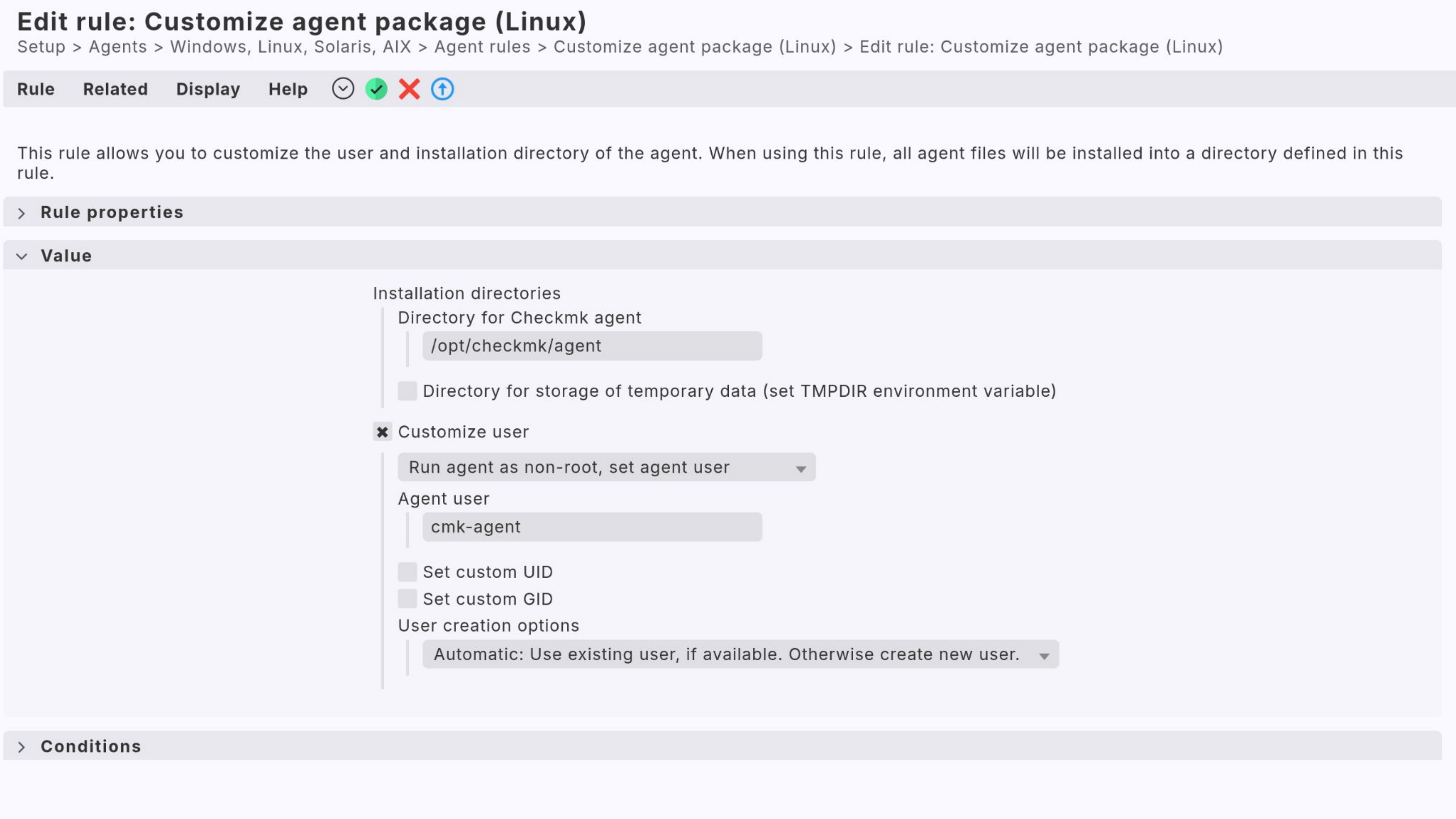
Non-root and one directory is optional for now!

Rulesets becoming obsolete …

- Installation paths for agent files (Linux, UNIX)
- Run agent as non-root user (Linux)

… and unified in one ruleset

- Customize agent package (Linux)
  - To handle eventually all fundamental agent package topics
  - Won’t allow for customizing individual agent paths anymore; one “directory” for all files is better



Edit rule: Customize agent package (Linux)

Setup > Agents > Windows, Linux, Solaris, AIX > Agent rules > Customize agent package (Linux) > Edit rule: Customize agent package (Linux)

This rule allows you to customize the user and installation directory of the agent. When using this rule, all agent files will be installed into a directory defined in this rule.

› Rule properties

⌄ Value

Installation directories

Directory for Checkmk agent: /opt/checkmk/agent

□ Directory for storage of temporary data (set TMPDIR environment variable)

☒ Customize user

Run agent as non-root, set agent user ▾

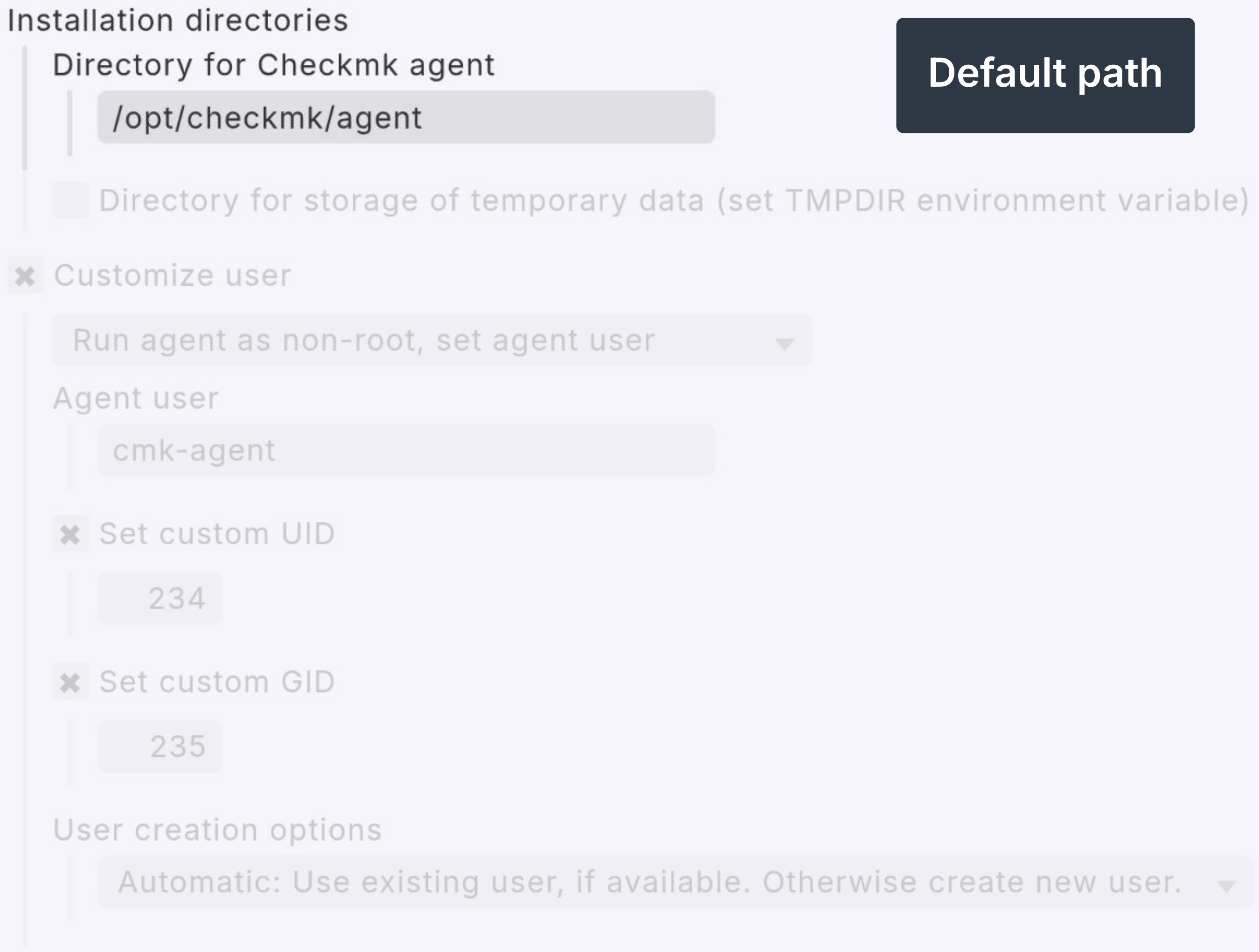
Agent user: cmk-agent

□ Set custom UID

□ Set custom GID

User creation options: Automatic: Use existing user, if available. Otherwise create new user. ▾

› Conditions



Installation directories

Directory for Checkmk agent

/opt/checkmk/agent

Default path

□ Directory for storage of temporary data (set TMPDIR environment variable)

☒ Customize user

Run agent as non-root, set agent user ▾

Agent user

cmk-agent

☒ Set custom UID

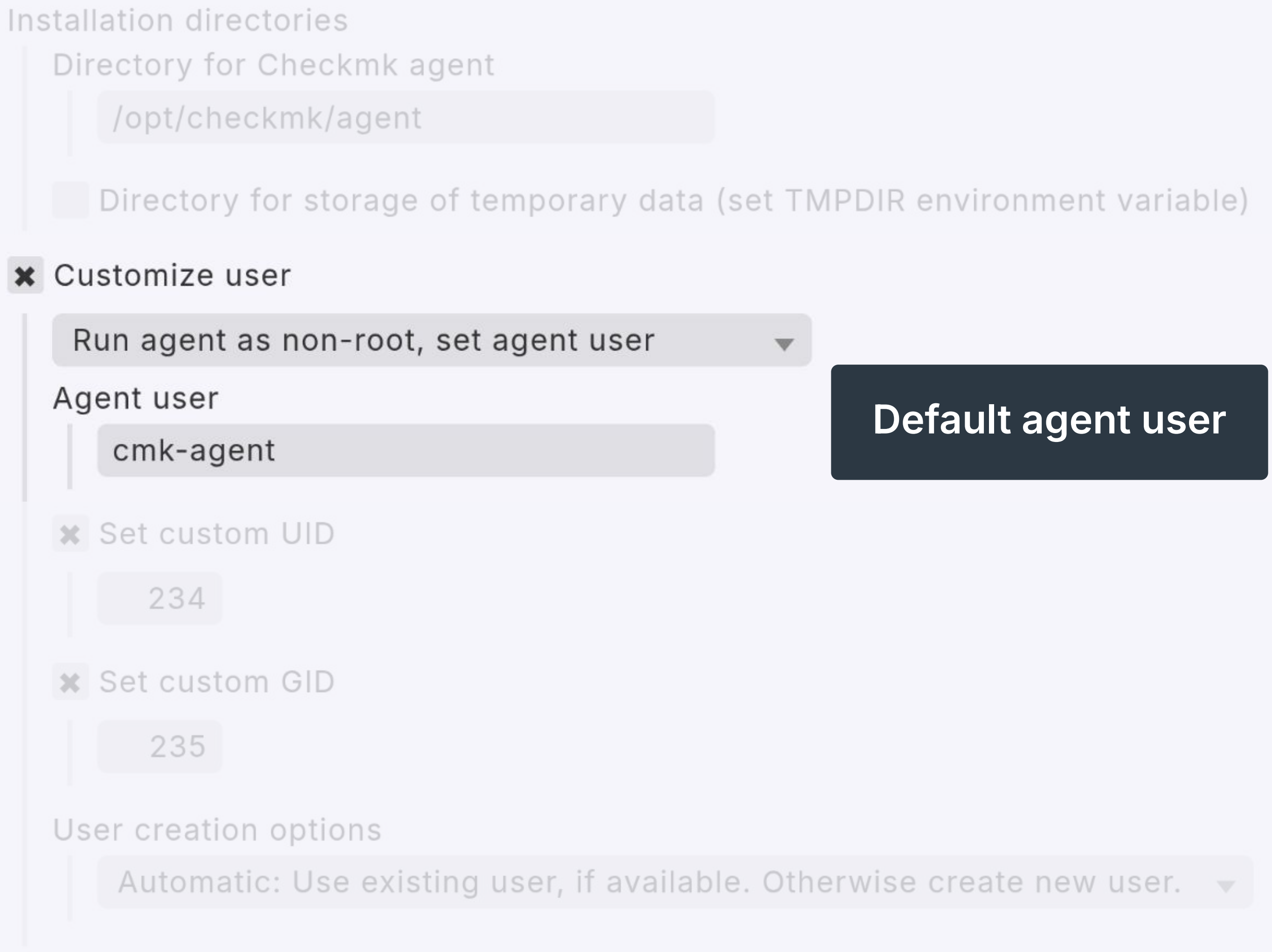
234

☒ Set custom GID

235

User creation options

Automatic: Use existing user, if available. Otherwise create new user. ▾



Installation directories

Directory for Checkmk agent

/opt/checkmk/agent

□ Directory for storage of temporary data (set TMPDIR environment variable)

☒ Customize user

Run agent as non-root, set agent user ▾

Agent user

cmk-agent

☒ Set custom UID

234

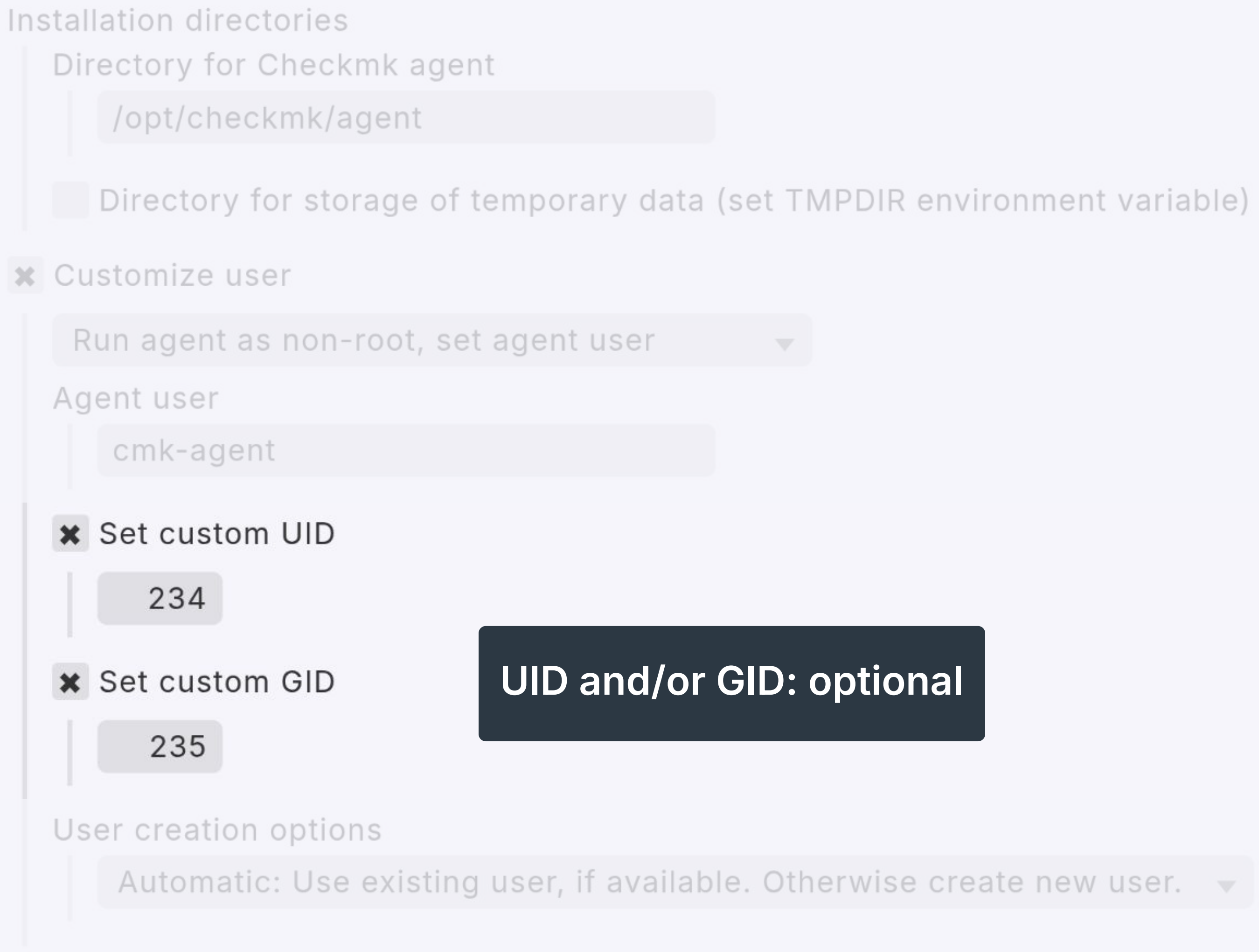
☒ Set custom GID

235

User creation options

Automatic: Use existing user, if available. Otherwise create new user. ▾

Default agent user



Installation directories

Directory for Checkmk agent

/opt/checkmk/agent

□ Directory for storage of temporary data (set TMPDIR environment variable)

☒ Customize user

Run agent as non-root, set agent user ▾

Agent user

cmk-agent

☒ Set custom UID

234

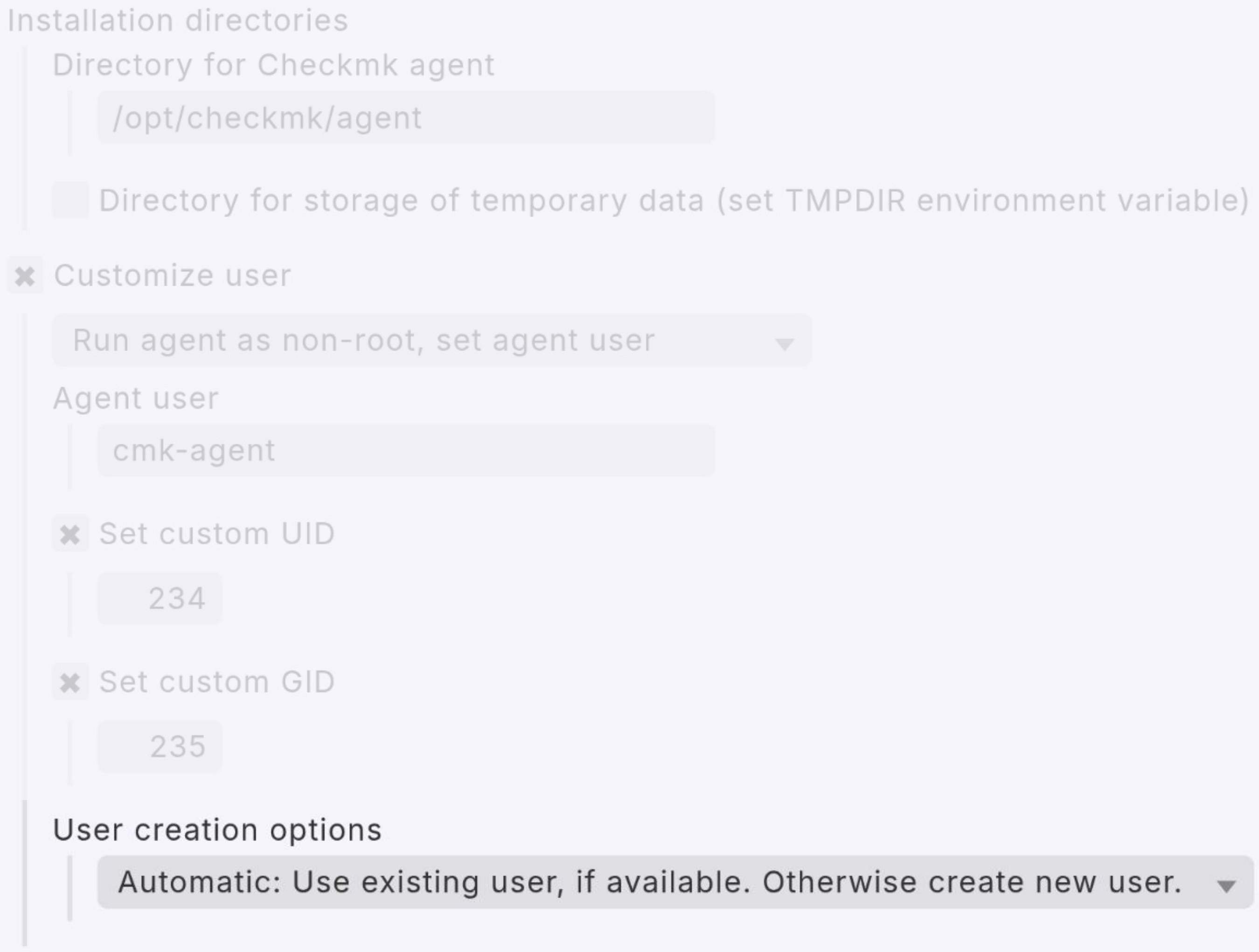
☒ Set custom GID

235

User creation options

Automatic: Use existing user, if available. Otherwise create new user. ▾

UID and/or GID: optional



Installation directories

Directory for Checkmk agent

/opt/checkmk/agent

☐ Directory for storage of temporary data (set TMPDIR environment variable)

☒ Customize user

Run agent as non-root, set agent user ▾

Agent user

cmk-agent

☒ Set custom UID

234

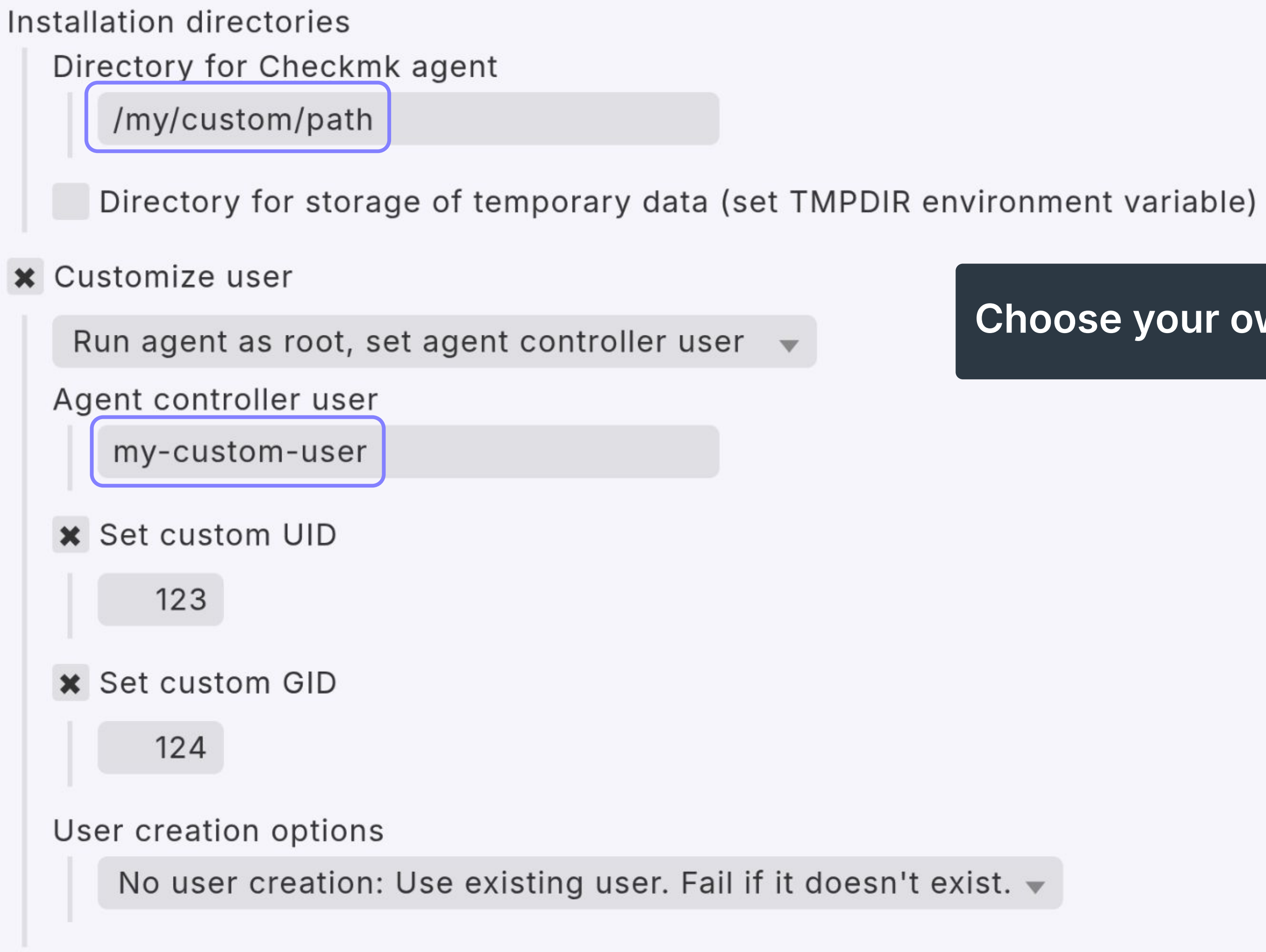
☒ Set custom GID

235

User creation options

Automatic: Use existing user, if available. Otherwise create new user. ▾

Create or reuse



Installation directories

Directory for Checkmk agent

/my/custom/path

□ Directory for storage of temporary data (set TMPDIR environment variable)

☒ Customize user

Run agent as root, set agent controller user ▾

Agent controller user

my-custom-user

☒ Set custom UID

123

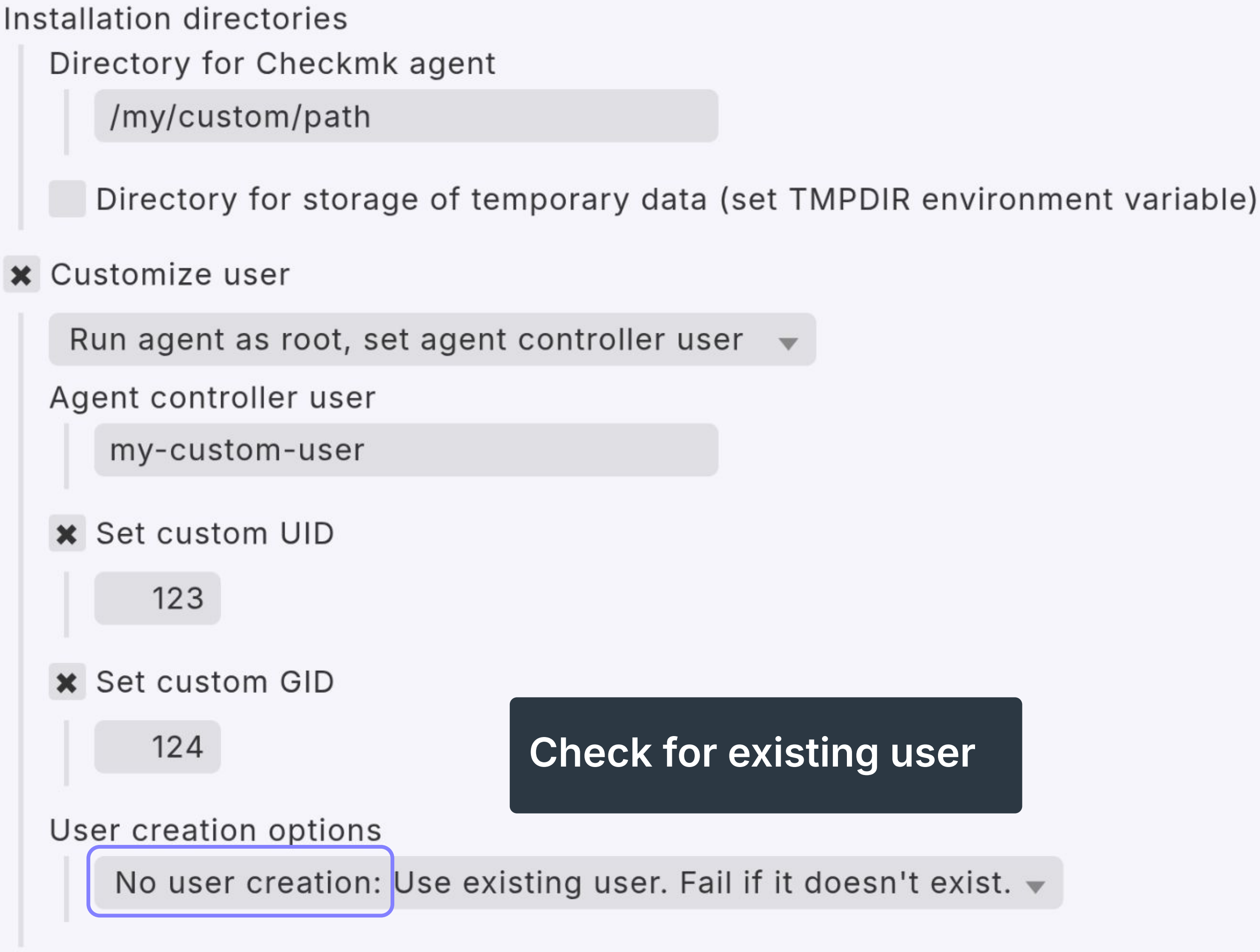
☒ Set custom GID

124

User creation options

No user creation: Use existing user. Fail if it doesn't exist. ▾

Choose your own path and user



Installation directories

Directory for Checkmk agent

/my/custom/path

□ Directory for storage of temporary data (set TMPDIR environment variable)

☒ Customize user

Run agent as root, set agent controller user ▾

Agent controller user

my-custom-user

☒ Set custom UID

123

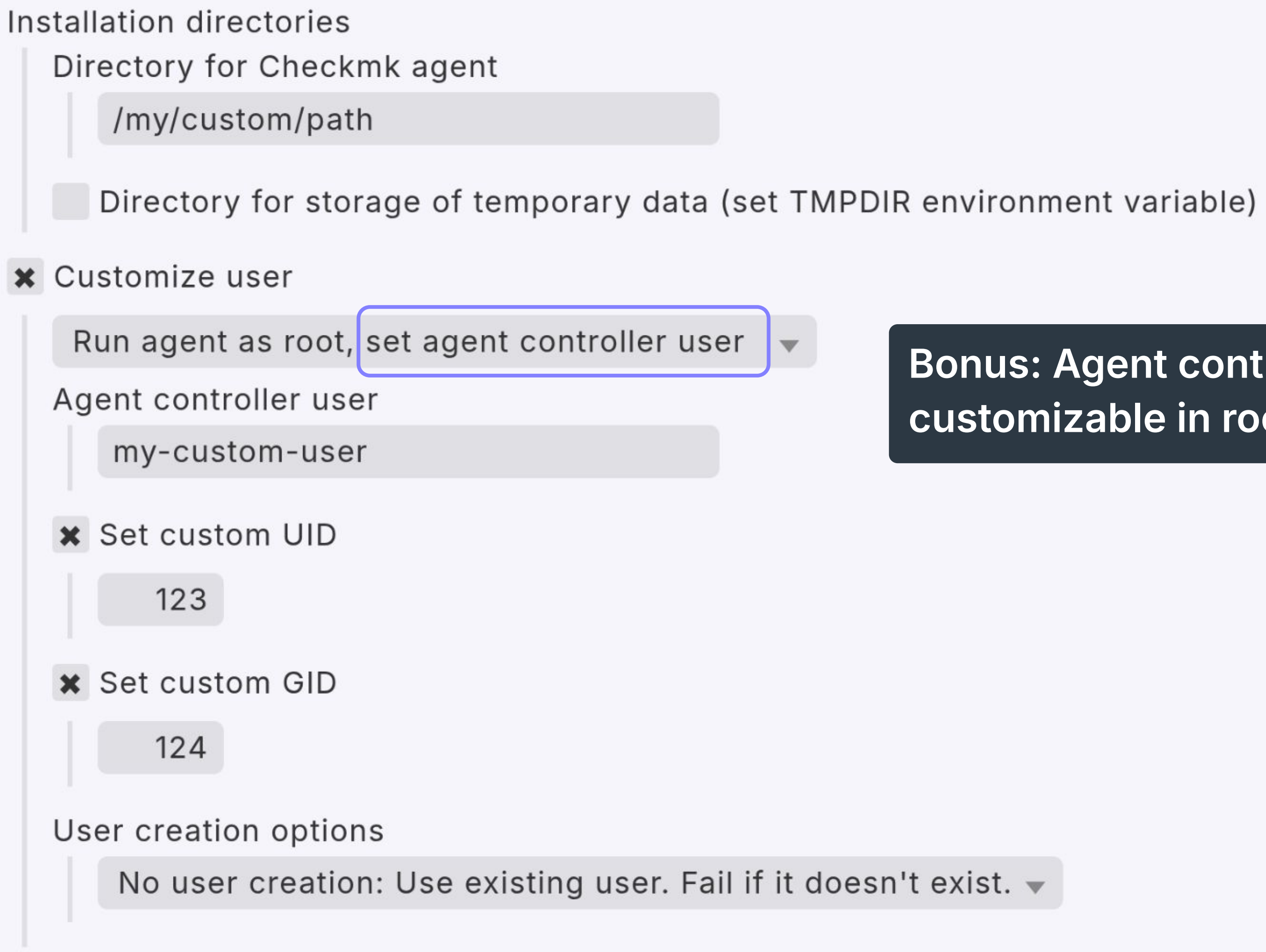
☒ Set custom GID

124

User creation options

No user creation: Use existing user. Fail if it doesn't exist. ▾

Check for existing user



Installation directories

Directory for Checkmk agent

/my/custom/path

☐ Directory for storage of temporary data (set TMPDIR environment variable)

☒ Customize user

Run agent as root, set agent controller user

Agent controller user

my-custom-user

☒ Set custom UID

123

☒ Set custom GID

124

User creation options

No user creation: Use existing user. Fail if it doesn't exist.

Bonus: Agent controller user customizable in root deployment

Further reading

- Werk #17900: Linux agent: Single directory deployment
- Werk #17901: Linux agent: Non-root deployment
- Inline help of ruleset “Customize agent package”
- docs.checkmk.com

11