Process Isolation pre Claude Code

Bezpečnostné odporúčania pre Windows & macOS — Interný dokument · Marec 2026

Tento dokument popisuje odporúčané postupy pre izoláciu procesov pri práci s Claude Code. Cieľom je obmedziť potenciálne škody v prípade neočakávaného správania AI nástroja – napríklad neúmyselného mazania súborov alebo neautorizovaného prístupu k citlivým dátam.

Claude Code nikdy nespúšťajte s admin/root právami.

—

Windows

1. Windows Sandbox (built-in, zadarmo)

Izolované jednorazové prostredie – po zatvorení všetko zmizne. Ideálne pre rýchle experimenty.

- Zapnutie: *Turn Windows features on/off → Windows Sandbox*
- Claude Code nainštaluj vo Sandboxe – nemá prístup k hostiteľskému disku
- ⚠ Nevýhoda: po každom zatvorení treba znova inštalovať

2. WSL2 s obmedzeným prístupom

Vytvor dedikovaného linuxového usera len pre Claude sessions:

```
# Vytvor dedikovaného usera pre Claude sessions
sudo useradd -m claude-user
sudo chmod 700 /home/claude-user

# Spúšťaj Claude Code len ako tento user
su - claude-user
```

- Nastav explicitné mount pravidlá v `/etc/wsl.conf`
- Claude Code nemá prístup k Windows súborom mimo `/mnt/c/claude-work/`

3. Hyper-V VM (najrobustnejšie)

Dedikovaná virtuálna mašina len pre Claude Code prácu.

- Vytvor **snapshot pred každou session** → jednoduchý rollback
- Shared folder nastav **len na projektový adresár**, nie na celý disk
- Sieťový prístup obmedz cez Hyper-V Virtual Switch

—

macOS

1. sandbox-exec (natívne, bez inštalácie)

Vytvor sandbox profil `/tmp/claude.sb` a spusti Claude s obmedzeniami:

```
(version 1)
(deny default)
(allow process-exec)
(allow file-read* (subpath "/usr/"))
(allow file-read* (subpath "/Library/"))
(allow file-read-write* (subpath "/Users/user/projects/"))
(allow network-outbound (remote tcp "*:443"))
(deny file-write* (subpath "/Users/user/Documents/"))
(deny file-write* (subpath "/Users/user/Desktop/"))
```

```
# Spustenie s profilom
sandbox-exec -f /tmp/claude.sb claude
```

2. Docker container (odporúčané pre dennú prácu)

Mountni **len projektový adresár** – nie celý domovský priečinok:

```
# Spustenie s mountom len na konkrétny projekt
docker run -it \
  -v ~/projects/moj-projekt:/workspace \
  --network=host \
  claude-sandbox
```

3. Dedikovaný macOS User Account

Vytvor separátny systémový účet bez admin práv:

- *System Settings* → *Users & Groups* → *Add User* → "Claude Work"
- Obmedzený user bez admin práv – nemôže meniť systémové nastavenia
- Fast User Switching umožňuje pohodlné prepínanie medzi účtami
- FileVault šifruje každý profil separátne

—

Odporúčanie podľa scenára

Scenár	Odporúčané riešenie	Platforma
Rýchle experimenty	WSL2 user isolation / sandbox-exec	Win / Mac
Produkčný kód	Docker s explicitným mount	Obe

Scenár	Odporúčané riešenie	Platforma
Citlivé firemné projekty	Hyper-V VM / Mac VM so snapshotmi	Win / Mac
Maximálna izolácia	Windows Sandbox / nový Mac user account	Win / Mac

—

> **Kľúčové pravidlo:** Claude Code nikdy nespúšťaj s admin/root právami. Vždy mountuj len konkrétny projektový adresár – nie `~/` ani `/`.

From:
https://w.rakuscinec.eu/ - **Rakuscinec Wiki**

Permanent link:
https://w.rakuscinec.eu/doku.php?id=ai_sandbox

Last update: **2026/03/09 08:03**