Agent-nadzor (CT206)

Agent-nadzor (CT206): scalenie 16.11.2026

Trzy agenty AI nadzoru (pve, backup, sec) działają w jednym kontenerze **CT206** na mars (192.168.123.206, WireGuard 10.30.8.206). Wcześniej każdy miał własny kontener (CT202, CT204, CT205). **agent-gate (CT200) i agent-boss (CT201) zostają osobno**: gate trzyma bramkę zgód i token Telegrama, a boss celowo nie ma trasy do infrastruktury. Scalenie ich z agentami AI zniosłoby granicę zaufania.

Układ w CT206

Agent	Użytkownik	Aplikacja	Konfiguracja i sekrety	Dane
agent-pve	agent-pve	/opt/agent-pve	/etc/agent-pve	/var/lib/agent-pve
agent-backup	agent-backup	/opt/agent-backup	/etc/agent-backup	/var/lib/agent-backup
agent-sec	agent-sec	/opt/agent-sec	/etc/agent-sec	/var/lib/agent-sec

- Aplikacje mają ścieżki `/etc/agent`, `/var/lib/agent`, `/var/log/agent` wpisane na stałe. Każda usługa systemd dostaje własny widok tych katalogów przez `BindPaths=/etc/agent-<n>:/etc/agent ...`, więc kod aplikacji nie został zmieniony.
- Każdy agent czyta tylko własne tokeny Proxmox i PBS, klucz SSH, token gate i klucz Anthropic. Test 16.11: agent-pve, agent-backup i agent-sec nie czytają nawzajem swoich plików.
- Izolacja jest słabsza niż przy osobnych kontenerach (wspólne jądro kontenera i sieć). Punkt jest na liście zabezpieczeń.

Sieć i adresy

- CT206 ma cztery adresy na wg0: 10.30.8.206 oraz dawne .202 (pve), .204 (backup), .205 (sec).
- Routing według użytkownika (reguły `ip rule uidrange` w PostUp w `/etc/wireguard/wg0.conf`) sprawia, że ruch każdego agenta wychodzi z jego dawnym adresem. To było konieczne, bo klucze SSH na 7 hostach mają `from="10.30.8.202"` i wymuszone polecenie, a Wazuh (10.30.8.211) wpuszcza dawny adres agent-sec.
- Na serwerze WireGuard (slonce, CT150) trzy dawne wpisy klientów zostały usunięte, a klient CT206 ma AllowedIPs na cztery adresy.

Powrót do poprzedniego stanu

1. W CT206: `systemctl stop agent-pve agent-backup agent-sec`.
2. Na slonce w CT150: `cp /root/wg0.conf.przed-przejecie-adresow /etc/wireguard/wg0.conf` i `wg syncconf wg0 <(wg-quick strip wg0)`.
3. Na mars: `pct start 202 204 205` (po jednym), `pct exec <id> -- systemctl start agent-<nazwa>`.
4. Opcjonalnie `pct set 202 --onboot 1` itd. i `pct set 206 --onboot 0`.

Weryfikacja

- W CT206: `systemctl is-active agent-pve agent-backup agent-sec` oraz `journalctl -u agent-<nazwa> --since -10min`.
- Jednorazowe kontrole bez skutków ubocznych (jako dany użytkownik, z `BindPaths`): `python -m agent_pve snapshot`, `python -m agent_backup snapshot`, `python -m agent_sec check`. Po scaleniu: 7 z 7 hostów SSH OK, 4 klastry PVE, oba PBS, Wazuh OK.

Uwagi

- Przy dodawaniu nowego agenta lub zmianie adresu sprawdź `authorized_keys` z `from=` na hostach (konto agent-pve) i zapory Wazuh.
- Stare kontenery CT202, CT204, CT205 są zatrzymane z `onboot=0`. Usunąć po tygodniu obserwacji (punkt na liście TO-DO).
- WGDashboard na slonce może nadpisać ręcznie zmienioną konfigurację WireGuard.

Revision #1
Created 2026-11-16 16:56:23 UTC by Claude (dokumentacja)
Updated 2026-11-16 16:56:23 UTC by Claude (dokumentacja)