
Profile instalacji

Poziom bezpieczeństwa wybrany przy instalacji,
stosowany i broniony przez samą pulę

Dokument wyjaśniający dla działu IT

Cellule-PRO, wersja 0.2.157 (obraz v1.0-rc92gj)

Do zapamiętania

„Air-gap domyślnie. Otwarcie na świat zewnętrzny to decyzja Waszego działu IT, nigdy nasza.”

Profil instalacji zamienia to zdanie w konkretne zasady. Wybieracie go raz, w asystencji pierwszego uruchomienia; pula go stosuje, przekazuje pozostałym pulom Waszego klastra, odrzuca pule, które go nie podzielają, i nie powierza ani swoich workerów, ani Waszych danych puli, która od niego odbiega.

Spis treści

1	Dlaczego profile instalacji	2
2	Cztery profile	2
2.1	Blokady i wartości proponowane	2
2.2	Co blokuje profil A	3
3	Który profil wybrać i w jakich ramach	3
3.1	Przewodnik decyzyjny w czterech pytaniach	3
3.2	Przykłady według branży	4
3.3	Co każdy profil zmienia dla pracowników	4
3.4	Ramy prawne	5
3.5	Jedna organizacja, kilka potrzeb	5
3.6	Zmiana profilu w czasie	5
3.7	Najczęstsze pytania	6
4	Wybór profilu przy instalacji	6
4.1	W asystencie pierwszego uruchomienia	6
4.2	Pula, która dołącza do istniejącego klastra	6
4.3	Późniejsza zmiana profilu	7
5	Jeden profil dla całego klastra	7
6	Wejście do klastra: członkostwo	7
6.1	Skąd pula zna profil drugiej puli	7
6.2	Zasady przyjmowania	7
6.3	Wyjątek	8
7	Współpraca z innymi pulami: „Współpracuj tylko z pulami o tym samym profilu”	8
7.1	Trzy stany każdego członka	8
7.2	Czego pula nie powierza już odsuniętemu członkowi	8
7.3	Zabezpieczenia	9
7.4	Co widzicie	9
7.5	Ustawienie	10
8	Co pula robi sama, a czego nie robi	10
9	Co widzicie w Nadzorze	10
10	Scenariusze krok po kroku	11
10.1	Jedna lokalizacja w pełnym air-gapie	11
10.2	Dodanie drugiej lokalizacji do klastra	11
10.3	Jedna pula zaostriżyła profil bez pozostałych	11
10.4	Pula jeszcze niezaktualizowana	11
11	Ustawienia w skrócie	11
12	Znane ograniczenia i kolejne kroki	12
13	Słowniczek	12

1 Dlaczego profile instalacji

Firma, która instaluje Cellule-PRO, ma różne potrzeby zależnie od swojej branży. Dział badawczy objęty klauzulą „ściśle tajne” chce, aby nic, nigdy, nie opuściło budynku. Kancelaria prawna chce tej samej poufności, ale akceptuje, że jej dział IT okazjonalnie otworzy dostęp do zewnętrznego API. Sieć oddziałów lub firma transportowa potrzebuje, aby kierowcy mogli dzwonić i pisać z trasy.

Bez profilu trzeba by ustawiać jedną po drugiej kilkadziesiąt opcji, a najmniejszy błąd otwierałby furtkę. Profil instalacji łączy te wybory w **jedną decyzję**, podejmowaną przy pierwszym uruchomieniu, czytelną dla wszystkich („ten klaster jest w pełnym air-gapie”) i **bronioną przez samą pulę**: najważniejsze zasady nie są już zwykłymi ustawieniami, lecz blokadami.

Cały ten dokument opiera się na trzech zasadach:

1. **Wybór należy do Waszego działu IT.** Pula nie wybiera żadnego profilu za Was; asystent wymaga wyraźnego wyboru.
2. **Zaostrzyć jest łatwo, złagodzić trudno.** Przejście na bardziej rygorystyczny profil to jedno kliknięcie i rozchodzi się samo; powrót wymaga zgody dwóch administratorów.
3. **Klaster łączy tylko pule o tym samym profilu.** Pula przyjmuje, wspiera i informuje tylko pule, które dzielają jej poziom bezpieczeństwa.

2 Cztery profile

Profil	Dla kogo	W praktyce
A. Pełny air-gap	Tajemnica obronna, poufne dane medyczne, wrażliwe B+R.	Nic nigdy nie wychodzi: brak zewnętrznego API, brak dostępu z zewnątrz, każde urządzenie zatwierdzone przez dwóch administratorów. Wszystko jest zablokowane .
B. Firma na miejscu (zalecany)	Kancelarie, MŚP, przemysł.	Domyślnie nic nie wychodzi; zewnętrzne API pozostaje możliwe, jeśli zdecyduje dział IT. Dostęp spoza firmy przez Wasz VPN.
C. Wiele lokalizacji i mobilność	Sieci oddziałów, transport, zespoły terenowe.	Rozmowy i wiadomości z zewnątrz dla zarejestrowanych urządzeń; telefony kierowane do najbardziej dostępnej puli.
D. Demonstracja	Próba, targi, proof of concept.	Nigdy prawdziwe dane. Nie do produkcji.

2.1 Blokady i wartości proponowane

Każdy profil działa na dwa różne sposoby:

Blokady obowiązują bez względu na wszystko: niezależnie od wartości zapisanej w bazie, odebranej z innej puli czy zaimportowanej, pula stosuje wartość blokady. Ma je tylko profil A.

Wartości proponowane są ustawiane tylko raz, przy instalacji, w ustawieniach, których jeszcze nie zmienialiście. Możecie je potem swobodnie zmieniać w Ustawieniach zaawansowanych.

2.2 Co blokuje profil A

Zablokowana zasada	Skutek
Zewnętrzne API (Claude, ChatGPT...)	Wyłączone: klucz odrzucany, ignorowany, konektor zatrzymany. Klucz nigdy nie jest usuwany, jedynie staje się bezużyteczny.
Dostęp z zewnątrz (rozmowy, e-maile, pliki, przesyłanie dokumentów, instalacje zdalne)	Zamknięty.
Prace poufne	Zastrzeżone dla wskazanych przez Was zaufanych serwerów.
Workery	Parowanie obowiązkowe, szyfrowane połączenie obowiązkowe.
Urządzenia CelluleBot	Każde urządzenie zatwierdzone przez administratora; rejestracja wymaga <i>drugiego</i> administratora; brak samodzielnego użycia.
Nadzór	Nazwiska pracowników ukryte.
Poufność inferencji	Tryb ścisły.
Pule klastra	Pula współpracuje tylko z pulami o tym samym profilu (sekcja 7).

3 Który profil wybrać i w jakich ramach

Profil nie jest ustawieniem technicznym: to przełożenie na zasady stosowane przez oprogramowanie decyzji Waszego zarządu i Waszego działu IT o tym, co ma prawo opuścić firmę i skąd można pracować. Wybiera się go więc na podstawie Waszych obowiązków i Waszego sposobu pracy, a nie na podstawie sprzętu.

3.1 Przewodnik decyzyjny w czterech pytaniach

1. **Czy chodzi o próbę, demonstrację, targi?** Bez żadnych prawdziwych danych: profil D. We wszystkich pozostałych przypadkach nigdy nie używajcie profilu D.
2. **Czy przetwarzacie informacje, których wyciek byłby poważny i nad którymi prawo, umowa lub poświadczenie bezpieczeństwa nakłada na Was pełną kontrolę** (informacje niejawne lub objęte poświadczeniem, krytyczna tajemnica przemysłowa, poufne dane medyczne, dochodzenia)? Profil A.
3. **Czy Wasi pracownicy potrzebują CelluleBota poza firmą** (rozmowy i wiadomości w podróży, kierowcy, technicy, oddziały bez VPN)? Profil C.

4. **W przeciwnym razie:** Wasze zespoły pracują na miejscu lub zdalnie przez firmowy VPN. Profil **B**, wybór zalecany dla większości organizacji.

Do zapamiętania

W razie wątpliwości wybierzcie profil **najbardziej rygorystyczny**, na jaki pozwala Wasza działalność. Zaostrzenie później to jedno kliknięcie; złagodzenie wymaga zgody dwóch administratorów. Rygorystyczny start nic nie kosztuje, zbyt otwarty start może kosztować wyciek.

3.2 Przykłady według branży

Organizacja	Profil	Dlaczego
Obronność, podwykonawcy z poświadczeniem bezpieczeństwa, wrażliwe laboratoria	A	Nic nie może wyjść, nawet przez pomyłkę administratora; dwie osoby przy każdej wrażliwej decyzji.
Placówki ochrony zdrowia, badania kliniczne	A lub B	A dla oddziałów, które przetwarzają dokumentację pacjentów; B dla administracji, jeśli zewnętrzne API może kiedyś posłużyć do zastosowań niewrażliwych.
Kancelarie prawne, notariusze, biura rachunkowe	B	Tajemnica zawodowa: domyślnie nic nie wychodzi, ale dział IT zachowuje możliwość okazjonalnego otwarcia zewnętrznego API do zastosowań ogólnych.
Przemysł, biura projektowe, MŚP	B	Know-how chronione na miejscu; praca zdalna przez VPN.
Transport, logistyka, zespoły terenowe	C	Kierowcy i technicy dzwonią i piszą z trasy; bazy wiedzy i e-maile pozostają na miejscu.
Sieci oddziałów, franczyzy, samorządy z wieloma lokalizacjami	C	Kilka lokalizacji i mobilni pracownicy; każdy telefon jest kierowany do najbardziej dostępnej puli.
60-dniowa wersja próbna, proof of concept, targi	D	Ocena bez prawdziwych danych; nigdy nie umieszczajcie w niej dokumentów firmy.

3.3 Co każdy profil zmienia dla pracowników

Możliwość	A	B	C	D
Korzystanie z AI na miejscu (pytania, dokumenty, debaty)	tak	tak	tak	tak
Zewnętrzne API AI do pytań ogólnych	nigdy	decyzją działu IT	decyzją działu IT	decyzją działu IT
Rozmowy i wiadomości z zewnątrz	nigdy	nie (VPN)	tak	nie

Możliwość	A	B	C	D
Wysyłanie plików w komunikatorze spoza firmy	nigdy	nie	tak	nie
Dodawanie do baz wiedzy spoza firmy	nigdy	nie	nie	nie
E-maile z zewnątrz	nigdy	nie	nie	nie
Telefon kierowany do najbardziej dostępnej puli	nie	nie	tak	nie
Nowe urządzenie zatwierdza	2 adminów	1 admin	1 admin	do wyboru

„nigdy” = zablokowane przez profil; „nie” / „tak” = wartość proponowana przy instalacji, którą można potem zmienić w Ustawieniach zaawansowanych.

3.4 Ramy prawne

Profil pomaga Wam wypełniać Wasze obowiązki; nie zastępuje ich i nie jest certyfikacją. Wasz kierownik ds. bezpieczeństwa i Wasz inspektor ochrony danych pozostają tymi, którzy oceniają przyjętą konfigurację.

- **RODO:** minimalizacja i lokalizacja danych. Profile A i B domyślnie zatrzymują całe przetwarzanie w firmie; każde otwarcie na zewnętrzne API jest odnotowaną decyzją działu IT.
- **Tajemnica zawodowa** (adwokaci, radcy prawni, ochrona zdrowia, biegli rewidenci): nic nie wychodzi bez wyraźnej decyzji; w profilu A nic nie może wyjść w ogóle.
- **Informacje wrażliwe lub niejawne:** profil A blokuje każde wyjście i wymaga dwóch administratorów; akredytacja bezpieczeństwa Waszego systemu pozostaje w gestii Waszej i właściwego organu.
- **Hosting danych medycznych:** Cellule-PRO to oprogramowanie, które działa u Was; to Wasza infrastruktura przechowuje dane i to jej dotyczą Wasze obowiązki w zakresie hostingu.
- **NIS2** i bezpieczeństwo systemów informatycznych: zablokowane profile, dziennik profilu, ustalenia i alerty Nadzoru pomagają wykazać kontrolę nad konfiguracją.

3.5 Jedna organizacja, kilka potrzeb

Klaster ma tylko **jeden** profil: wszystkie jego pule dzielą ten sam poziom bezpieczeństwa. Jeśli jeden dział musi być w pełnym air-gapie (badania, dział prawny), a reszta firmy potrzebuje mobilności, zainstalujcie **dwa odrębne klastry**: jeden w profilu A dla wrażliwego działu, drugi w profilu C dla pozostałych. Nie połączą się ze sobą i tak ma być: nic nie może przepłynąć z klastra A do klastra C.

3.6 Zmiana profilu w czasie

- **Na bardziej rygorystyczny** (D → C → B → A): jedno kliknięcie na karcie „Profil tej puli”, zastosowane w całym klastrze w ciągu kilku minut.
- **Na mniej rygorystyczny** (na przykład B → C, gdy Wasze zespoły stają się mobilne): to złagodzenie, które będzie wymagało zgody dwóch administratorów (procedura przewidziana w kolejnej wersji). Uwzględnijcie to już przy pierwszym wyborze.

- **Z D na profil produkcyjny:** wersja próbna staje się prawdziwą instalacją przez zaostrenie profilu; pamiętajcie, aby wcześniej usunąć dane testowe.

3.7 Najczęstsze pytania

Czy profil spowalnia AI? Nie. Decyduje o tym, co może wyjść i skąd się pracuje; moc obliczeniowa i modele są takie same we wszystkich czterech profilach.

Czy każda pula może mieć inny profil? Nie, i jest to zamierzone: mniej rygorystyczna pula byłaby drzwiami, przez które dane klastra mogłyby wyjść. Pula o innym profilu nie wchodzi do klastra, a członek, który od niego odbiega, zostaje odsunięty.

Co się stanie, jeśli administrator się pomyli? W profilu A blokady nie pozwalają mu niczego otworzyć. W pozostałych profilach każda zmiana jest zapisywana w dzienniku, a złagodzenie będzie wymagało dwóch administratorów.

A pula zainstalowana przed wprowadzeniem profili? Działa jak dotąd, dopóki nie wybrano żadnego profilu; gdy tylko jedna pula klastra go wybierze, pozostałe przyjmą go same.

4 Wybór profilu przy instalacji

4.1 W asystencie pierwszego uruchomienia

Dostarczany obraz Cellule-PRO jest czysty: żadnego administratora, żadnego profilu. Krok „Bezpieczeństwo” asystenta przedstawia cztery profile, a dla każdego dokładną listę blokad, odczytaną z kodu samej puli. **Żaden profil nie jest wybrany z góry:** asystenta nie da się zakończyć bez wyboru.

Uwaga

Profil A wymaga **dwóch administratorów** już przy instalacji (różne adresy, sprawdzane przez serwer). To warunek, aby żadna pojedyncza osoba nie mogła później zarejestrować urządzenia ani złagodzić profilu.

Na końcu asystenta pula sprawdza wszystko, zanim cokolwiek zapisze, stosuje profil *przed* utworzeniem kont, a następnie ustawia wartości proponowane w wolnych ustawieniach. Ponowne wysłanie tego samego kroku nie ma żadnego skutku; próba złagodzenia jest odrzucana.

4.2 Pula, która dołącza do istniejącego klastra

Gdy asystent służy do dodania puli do klastra, który już działa, profilu się nie wybiera: zastosowany zostanie profil klastra. Dopóki go nie otrzyma, nowa pula sama przechodzi **na najsurowszy poziom** (blokady air-gapu) i to sygnalizuje:

- karta „Profil tej puli”: „czeka na profil instalacji klastra”;
- Nadzór i stan zdrowia: komunikat „Pula czeka na profil instalacji klastra”.

Profil dociera w ciągu kilku minut, przez podpisane przekazanie opisane w następnej sekcji; oczekiwanie kończy się wtedy samo. Ponowne uruchomienie w trakcie oczekiwania go nie kończy: kończy je tylko prawdziwy profil.

4.3 Późniejsza zmiana profilu

W Ustawieniach zaawansowanych, na karcie „Profil tej puli”, administrator może **zaostrzyć** profil (na przykład przejść z B na A), po ponownym wpisaniu hasła. Zmiana jest zapisywana w dzienniku profilu i natychmiast przekazywana pozostałym pulom.

Złagodzenie (na przykład z A na B) nie jest możliwe z tego ekranu: ta decyzja będzie wymagała zgody dwóch administratorów (procedura przewidziana w kolejnej wersji).

5 Jeden profil dla całego klastra

Klaster Cellule-PRO łączy kilka pul (na przykład po jednej na lokalizację) powiązanych podpisaną federacją (Ed25519). Profil jest właściwością *klastra*, nie tylko pojedynczej puli.

Pula zajmuje się tym sama

- Każda pula ponownie publikuje swój podpisany profil co 5 minut oraz natychmiast po zmianie.
- Pula, która otrzyma profil **bardziej rygorystyczny** niż własny, sama go przyjmuje i odnotowuje to w dzienniku („profil otrzymany z puli X”).
- Profil otrzymany **mniej rygorystyczny** jest zawsze odrzucany: pula nie może osłabić pozostałych.
- Dwa jednoczesne wybory w dwóch pulach zbiegają się do bardziej rygorystycznego.

Ustawienie `INSTALL_PROFILE_ACCEPT_FROM_PEERS` („Akceptuj profil instalacji wysłany przez inne pule”, domyślnie włączone) pozwala puli przyjmować wyłącznie decyzje własnego administratora. To wybór właściwy każdej puli, którego żadna inna pula nie może jej narzucić.

6 Wejście do klastra: członkostwo

Połączenie dwóch pul (Federacja, „Dodaj pool”) nie wystarcza, aby stały się *członkami* tego samego klastra. Pula najpierw sprawdza profil drugiej puli.

6.1 Skąd pula zna profil drugiej puli

Nigdy z prostego pytania bez dowodu. Profil innej puli jest uwzględniany tylko wtedy, gdy dociera w wiadomości **podpisanej** przez tę pulę:

- w podpisanym uzgadnianiu połączenia (handshake), które łączy obie pule;
- w podpisanym poświadczeniu, powiązanim z pulą, która o nie prosi, oraz z unikalnym losowym pytaniem, ważnym dwie minuty (nie da się go odtworzyć ponownie ani przechwycić);
- w podpisaney ponownej publikacji członka.

6.2 Zasady przyjmowania

Sytuacja	Decyzja
Ten sam profil po obu stronach	Przyjęta jako członek.
Różne profile	Odrzucona: pula pozostaje jedynie „znana”.
Druga pula została właśnie zainstalowana i czeka na profil klastra	Przyjęta: przejmie Wasz profil.
Profil drugiej puli nieznany (starsza wersja, ogłoszenie starsze niż 24 h)	Odrzucona, jeśli Wasza pula jest w air-gapie; w przeciwnym razie przyjęta.
Wasza pula sama czeka na swój profil	Na razie nie przyjmuje nikogo.
Nie wybrano żadnego profilu (klastr zainstalowany przed wprowadzeniem profili)	Przyjęta, działanie bez zmian.

6.3 Wyjątek

Gdy pula zostaje odrzucona, ekran „Dodaj pool” wyjaśnia dlaczego („Różne profile instalacji: ta pula ma »Pełny air-gap«, druga »Firma na miejscu«”) i jak to poprawić (wybrać ten sam profil po obu stronach). Jeśli Wasz dział IT mimo to zdecyduje się ją przyjąć, zaznacza „Mimo to łączę tę pulę jako członka” i klika „Połącz mimo to”.

Uwaga

Wyjątek jest możliwy tylko z panelu, przez zidentyfikowanego administratora (nigdy w trybie tylko do odczytu, nigdy przez API). Jest **zapisywany na nazwisko administratora, zanim** pula stanie się członkiem: jeśli zapis się nie powiedzie, pula nie wchodzi do klastra. Pula przyjęta na zasadzie wyjątku otrzymuje dane klastra.

7 Współpraca z innymi pulami: „Współpracuj tylko z pulami o tym samym profilu”

O członkostwie decyduje się tylko raz. Członek może się później zmienić: jego administrator zaostri profil, a Wasz za nim nie podąża (automatyczne przyjmowanie wyłączone), albo nie jest już aktualny. Pula nigdy sama nie *degradowe* członka (byłby to łatwy sposób na zdeorganizowanie klastra); **przestaje mu natomiast cokolwiek powierzać**, dopóki profile się różnią.

7.1 Trzy stany każdego członka

Stan	Znaczenie
Zgodny	Ten sam profil, znany z podpisanej wiadomości sprzed mniej niż 24 h; albo przyjęty na zasadzie wyjątku; albo w Waszej puli nie wybrano żadnego profilu.
Inny	Profil znany, aktualny i inny niż Wasz: rozbieżność jest pewna.
Nieznany	Profil nieobecny lub zbyt stary (pula jeszcze niezaktualizowana) albo w trakcie przyjmowania.

7.2 Czego pula nie powierza już odsuniętemu członkowi

Co jest chronione	W jaki sposób
Zadania inferencji Wyszukiwania w pamięci i dokumentach	Obciążona pula nie przekazuje już pracy temu członkowi. Nie wysyła mu się żadnego pytania; jego własne pytania są odrzucane (nie pobiera żadnego fragmentu z Waszej puli).
Workery i proxy	Członek znika z listy zapasowej przekazywanej przy każdym połączeniu; żadne polecenie przeniesienia nie wskazuje go jako celu (polecenie już wydane zostaje zamknięte, nigdy ponawiane); równoważenie obciążenia i routing według bliskości go pomijają; przełączenie wymuszone przez administratora korzysta z aktualnej listy.
Odciski certyfikatów	Odcisk członka nie jest już przekazywany workerom ani telefonom: nie mogą się już z nim połączyć, nawet gdyby ktoś ich o to poprosił.
Urządzenia CelluleBot	Członek nie jest już proponowany jako „najlepsza pula”.

7.3 Zabezpieczenia

Dane zatrzymują się natychmiast. Gdy tylko profil jest inny (lub nieznany w air-gapie), nie wychodzi już żadne zadanie ani żadne pytanie.

Przełączenia czekają dziesięć minut. Tuż po zmianie profilu Waszej puli pozostałe pule nie otrzymały jeszcze nowego profilu (ponowna publikacja co 5 minut). Przez te dziesięć minut listy zapasowe i polecenia przeniesienia pozostają bez zmian: zwykle zaostrenie nie odcina klastra od rezerw.

Certyfikaty są wycofywane tylko przy pewności. Członek o profilu jedynie *nieznanym* zachowuje swój odcisk: odcisk wycofany przez pomyłkę dużo trudniej przywrócić na stacjach niż adres.

W razie wątpliwości: zamknięte. Jeśli pula nie zdoła odczytać własnego profilu (uruchamianie, baza chwilowo nieczytelna), zachowuje się jak w air-gapie aż do następnego odczytu.

Nic się nie psuje. Jeśli żaden członek nie jest już zgodny, workery po prostu pozostają w swojej puli.

7.4 Co widzicie

W Nadzorze i w stanie zdrowia („@Cellule, jaki jest twój stan?”):

Do zapamiętania

Pula X nie jest już używana przez tę pulę.

Ta pula nie wysyła jej już zapasowych workerów ani proxy, zadań ani wyszukiwań: jej profil instalacji jest inny lub nieznany (pula jeszcze niezaktualizowana).

Wskazówka: wybierz ten sam profil w obu pulach lub zaktualizuj drugą pulę. Aby mimo to jej używać: połącz ją ponownie w „Federacji” i zaznacz „Połącz mimo to”.

W puli w air-gapie komunikat ma rangę błędu, w pozostałych przypadkach ostrzeżenia.

7.5 Ustawienie

`INSTALL_PROFILE_PEER_GATING` — „Współpracuj tylko z pulami o tym samym profilu instalacji”. Właściwe każdej puli, **domyślnie włączone, zawsze aktywne w profilu A**. Bez wybranego profilu nie ma żadnego skutku. Jego wyłączenie (poza profilem A) przywraca Waszej puli możliwość korzystania ze wszystkich członków, niezależnie od ich profilu.

8 Co pula robi sama, a czego nie robi

Pula zajmuje się tym sama

- Stosuje blokady profilu przy każdym uruchomieniu, bez względu na zawartość bazy.
- Przechodzi na najsurowszy poziom, dopóki czeka na profil swojego klastra lub jeśli nie zdoła odczytać własnego.
- Przekazuje swój podpisany profil pozostałym pulom; przyjmuje otrzymany profil bardziej rygorystyczny.
- Odmawia wejścia puli o innym profilu.
- Na bieżąco klasyfikuje członków, z którymi współpracuje, i pokazuje to w Nadzorze.

Czego celowo **nie** robi:

- **Nie łagodzi profilu:** to zastrzeżone dla dwóch administratorów. W przeciwnym razie jedna przejęta pula mogłaby osłabić cały klastr.
- **Nie wymusza niczego na innej puli:** odsuwa ją i Was ostrzega, ale jej nie zmienia.
- **Nie wyklucza członka z klastra:** degradacja pozostaje decyzją człowieka.

9 Co widzicie w Nadzorze

Komunikat	Co zrobić
Pula czeka na profil instalacji klastra	Normalne przez kilka minut po jej połączeniu. Jeśli to trwa: sprawdź Federację lub wybierz profil klastra w „Profil tej puli”.
Pula X nie ma tego samego profilu instalacji	Profil kopiuje się sam; jeśli pozostaje inny, sprawdź, czy pula jest połączona i ma tę samą wersję.
Pula X przyjęła profil instalacji odebrany z puli Y	Jeśli Wasz zespół nie zdecydował o tej zmianie, sprawdź dziennik profilu i wyłącz automatyczne przyjmowanie.
Pula X nie jest już używana przez tę pulę	Ten sam profil po obu stronach, aktualizacja drugiej puli lub wyjątek („Połącz mimo to”).

10 Scenariusze krok po kroku

10.1 Jedna lokalizacja w pełnym air-gapie

1. Uruchom obraz, otwórz asystenta; w kroku „Bezpieczeństwo” wybierz **A**.
2. Wpisz dwóch administratorów (różne adresy).
3. Zakończ: zewnętrzne API i dostęp z zewnątrz są wyłączone i zablokowane; urządzenia wymagają zatwierdzenia przez dwóch administratorów.

10.2 Dodanie drugiej lokalizacji do klastra

1. Zaktualizuj nową pulę do **tej samej wersji** co pozostałe.
2. W jej asystencie wybierz „Dołącz do istniejącego klastra”: przechodzi w stan oczekiwania, na najsurowszym poziomie.
3. Połącz ją z jednej z pul klastra („Dodaj pool”): zostaje przyjęta (czeka na profil).
4. W ciągu kilku minut otrzymuje profil klastra; komunikat „czeka” znika.

10.3 Jedna pula zaostriżyła profil bez pozostałych

Pula w Krakowie przechodzi na A; pula w Warszawie (automatyczne przyjmowanie wyłączone) pozostaje na B.

- Zaraz po ponownej publikacji Warszawa wie, że Kraków jest na A: natychmiast przestaje przekazywać mu zadania i wyszukiwania.
- Ponieważ profil Warszawy się nie zmienił, nie obowiązuje żaden okres karencji: Kraków od razu znika z list zapasowych workerów Warszawy, a jego odcisk nie jest już przekazywany stacjom. (Dziesięciominutowe opóźnienie dotyczy tylko okresu tuż po zmianie profilu samej puli.)
- Nadzór w Warszawie pokazuje „Pula Kraków nie jest już używana przez tę pulę”.
- Naprawa: ponownie włącz automatyczne przyjmowanie w Warszawie (lub wybierz tam A); wszystko wraca do normy samo.

10.4 Pula jeszcze niezaktualizowana

Pula w wersji starszej niż 0.2.156 nie ogłasza swojego profilu: jest „nieznana”. W air-gapie zostaje odsunięta od zadań i rezerw, ale zachowuje swój odcisk. Wystarczy ją zaktualizować.

Uwaga

Zaktualizuj wszystkie pule klastra do tej samej wersji **przed** wyborem profilu A: w przeciwnym razie starsze pule zostaną odsunięte aż do ich aktualizacji.

11 Ustawienia w skrócie

Ustawienie	Domyślnie	Rola
<code>INSTALL_PROFILE_ACCEPT_FROM_PEERS</code>	włączone	Przyjmowanie bardziej rygorystycznego profilu wybranego w innej puli.
<code>INSTALL_PROFILE_PEER_GATING</code>	włączone (zablokowane w A)	Współpraca tylko z pulami o tym samym profilu.

Oba ustawienia są właściwe każdej puli: naprawa „Wyrównaj klaster” nigdy ich nie kopiuje.

12 Znane ograniczenia i kolejne kroki

- **Dane biznesowe między rozbieżnymi członkami.** Wiadomości, pamięć, dokumenty projektów i klucze API nadal kopiują się do członka, który ma już inny profil. Zostanie to poprawione przed jakimkolwiek udostępnieniem klientom (pakiet P3b).
- **Złagodzenie profilu:** procedura z udziałem dwóch administratorów (pakiet P4).
- **Profil D:** baner „brak prawdziwych danych” i blokada po zakończeniu okresu oceny, bez usuwania danych.
- **Naprawa jednym kliknięciem:** „Przywróć tej puli profil klastra” wśród napraw proponowanych w Nadzorze.
- Pula członkowska zawsze może *zaostrzyć* profil pozostałych: tak ma być (bezpieczeństwo może tylko rosnąć), a każde przyjęcie profilu jest zapisywane w dzienniku i widoczne.

13 Słowniczek

Klaster Zbiór połączonych pul Cellule-PRO, które współdzielą tożsamości, wspólne ustawienia i rezerwy.

Członek Pula przyjęta do klastra (zaufanie na poziomie 2 lub wyższym), w odróżnieniu od puli jedynie „znanej”.

Pula Serwer Cellule-PRO danej lokalizacji (obraz Docker).

Worker Stacja robocza lub serwer, który uruchamia modele dla puli.

Proxy Mobilny przekaźnik, który obsługuje jeden lub kilka silników i może przełączać się z jednej puli do drugiej.

Lista zapasowa Pule, na które worker lub proxy przełącza się, gdy jego własna pula przestaje działać.

Odcisk Identyfikator certyfikatu puli; stacja łączy się tylko z odciskiem, który zna.

Wiadomość podpisana Wiadomość opatrzona weryfikowalnym podpisem Ed25519: nie można jej ani sfalszować, ani przypisać innej puli.

Wyjątek Wyraźna decyzja administratora o przyjęciu puli mimo innego profilu, zapisana na jego nazwisko.