K0NSULT / ClaudCNC — Misja 3

Stabilizacja, zrównoważenie działań i ochrona infrastruktury • Dokument wdrożeniowy 5-dniowy

Podstawa operacyjna: dokument został zbudowany dla ClaudCNC na bazie bieżącej architektury K0nsultu, rytmu raportowego 15 min / 1h / 6h / 24h oraz modelu 7-warstwowego, 12-modułowego kernela, Capability Registry i Skill Graph.

1. Charakter dokumentu

Misja 3 domyka fazę wzrostu przez wzmocnienie odporności operacyjnej. Jej zadaniem jest ustabilizowanie intensywnie rozbudowanej sieci, ochrona pamięci, infrastruktury i zasobów, wykrywanie przeciążeń oraz zapobieganie awariom, split-brain i driftowi decyzyjnemu.

2. Mission główna

Mission: W ciągu 5 dni obniżyć ryzyko operacyjne K0nsultu przez wzmocnienie continuity, security, backupów, rollbacków, kontroli dostępu, source discipline i wykrywania przeciążeń w całej sieci agentowej.

3. Cele strategiczne

Kod	Cel	Wynik docelowy
M3.1	Ustabilizować wzrost	Zwiększona sieć działa bez utraty spójności i jakości.
M3.2	Chronić infrastrukturę i pamięć	Backup, restore, provenance i role-lock są sprawdzone.
M3.3	Wykrywać przeciążenia i anomalia	Traffic Control i Mierniczy mają pełny obraz hot-spotów.
M3.4	Utrzymać bezpieczeństwo decyzji	High-stakes przechodzą przez simulation + override path.
M3.5	Zabezpieczyć dalsze cykle	Kolejne misje nie niszczą fundamentów systemu.

4. Organ misji i zakres odpowiedzialności

Organ / komórka	Rola	Zakres działania
ClaudCNC	Chief Stability Orchestrator	Bilansuje sieć i zleca działania ochronne.
Traffic Control	Równoważenie ruchu	Wykrywa przeciążenia, kolejki, dryf i zapętlenia.
OPS/Security Cell	Ochrona infrastruktury	Backup, restore, hardening,

Organ / komórka	Rola	Zakres działania
		monitoring, fail-safe.
Epistemics Office	Prawdziwość stanu systemu	Freshness, conflicts, confidence, truth maintenance.
Simulation Office	Testy kontrfaktyczne	Ćwiczy rollbacki, incydenty i skutki II rzędu.
Human Override Layer	Finalny bezpiecznik	Utrzymuje możliwość zatrzymania i cofnięcia zmian.

5. Zasoby i infrastruktura

Typ	Zasób / rola	Znaczenie
Zasób istniejący	Monitoring i rytm raportowy	Umożliwia szybkie wykrywanie dryfu i blockerów.
Zasób istniejący	Decision Log + Delegation Trace	Pokazuje, gdzie rodzi się przeciążenie lub konflikt.
Zasób istniejący	Source-of-truth / authority map	Pozwala rozdzielić błąd wiedzy od błędu mandatu.
Uzupełnienie	Incident manager	Prowadzi reakcję na P0/P1.
Uzupełnienie	SRE / resilience specialist	Ustawia limity, retry, backupy i przywracanie.
Uzupełnienie	Security reviewer	Weryfikuje dostępy, sekrety, fail-open i ślady naruszeń.

6. Harmonogram 5-dniowy

Etap	Mission dnia	Rezultat
Dzień 1	Mapa ryzyk i zasobów krytycznych	Lista systemów, pamięci, integracji i ról wymagających ochrony.
Dzień 2	Hardening i continuity	Backupy, restore drills, role lockdown, critical path mapping.
Dzień 3	Testy incydentowe	Split-brain drill, source-conflict drill, fail-open drill, rollback drill.
Dzień 4	Kalibracja obciążenia	Przerzut ruchu, wyrównanie klas, reguły throttlingu i kolejek.
Dzień 5	Ocena stabilności i release gate	Raport stabilizacji, backlog

Etap	Mission dnia	Rezultat
		poprawek i zgoda na kolejny cykl.

7. Kwalifikacje i umiejętności do uzupełnienia

Priorytet	Kwalifikacja	Cel uzupełnienia
1	Resilience engineering	Stabilność ponad pozorną szybkość.
2	Backup / restore literacy	Każda zmiana ma odwracalność.
3	Threat & anomaly detection	Sieć musi umieć rozpoznać swoje własne symptomy.
4	Authority enforcement	Ochrona przed dryfem mandatu i nieuprawnionym ruchem.
5	Counterfactual readiness	High-stakes są testowane przed wykonaniem.

8. KPI i warunki przejścia

KPI / warunek	Wartość docelowa
Czas wykrycia anomalii	krótki / w granicach godzinowych raportów
Skuteczność restore drill	100% scenariuszy krytycznych
Liczba krytycznych naruszeń authority	0
Liczba nierozwiązanych source conflicts	0 krytycznych
Rollback readiness	100% dla systemów krytycznych
Split-brain incidents po korektach	tendencja malejąca / niski poziom

9. Ryzyka i odpowiedź sterująca

Ryzyko	Odpowiedź
Fałszywe poczucie stabilności	Obowiązkowe testy drill zamiast deklaracji.
Przeciążenie kontrolerów	Delegacja do gildii i automatycznych sentinel agents.
Zabezpieczenia tylko na papierze	Renderować status przez KPI i testy przejścia.
Ukryte konflikty źródeł	Epistemics Office ma prawo hard-escalate.

Ryzyko	Odpowiedź
Brak odwrotności zmian	Żadna zmiana krytyczna bez restore/rollback path.

10. Warunek zamknięcia i handoff

Wyjściem z misji jest aktywacja kolejnego etapu rozwojowego: po ustabilizowaniu można przejść do produktizacji, federacji, ekspansji sektorowej lub misji specjalnych bez nadmiernego ryzyka utraty sterowalności.

11. Dyspozycja dla ClaudCNC

- utrzymuj pełny rytm raportowy: 15 min / pełna godzina / faza / raport dobowy;
- nie uruchamiaj żadnego ruchu high-stakes bez ścieżki approval i override;
- aktualizuj Capability Registry i Skill Graph po każdej zmianie strukturalnej;
- nie ukrywaj konfliktów źródeł, przeciążeń ani driftu mandatu;
- zostawiaj pełny ślad provenance dla decyzji, delegacji i zmian architektury.