

Чек-лист migration gate для агентного workflow

Материал предназначен для отдельного PDF в `downloads/checklist-migration-gate-deepseek.pdf`.

Перед переключением трафика пройдите пункты по состоянию, инструментам, доступам, исполнению и наблюдаемости.

Состояние и воспроизводимость

- Журнал workflow хранится вне модельного провайдера.
- Для вызовов сохранены `tool_call_id`, статусы, версии промптов и схем.
- Ссылки на документы и внешние артефакты доступны из нового контура.
- Кэш провайдера не используется как единственное хранилище истории.
- Холодный и прогретый режимы измеряются отдельно.

Инструменты и политики

- Для каждого tool описаны входная и ожидаемая выходная схема, версия и роль.
- Определены идемпотентный ключ, `retry policy`, тайм-аут и правило `approval`.
- Проверены `auto`, `required`, `none` и `named tool`.
- Parser и chat template закреплены в конфигурации runtime.
- Write-операции блокируются при недостатке данных или отсутствии подтверждения.

Доступы и исполнение

- Для каждой сервисной роли проверен фактический список доступных tools.
- Пройдены сценарии 401, 403, истёкшего токена и отсутствующего scope.
- Проверены секреты, DNS, прокси, `egress`, файловые права и лимиты `sandbox`.
- Тайм-аут действительно прерывает задачу через `runtime-policy`.
- Проверены отмена задачи, повтор после сбоя и отсутствие дубликатов.

Переключение и наблюдаемость

- Подготовлен `contract pack` целевого провайдера и runtime.
- Золотые трассы содержат допустимое действие и отсутствие лишнего write-действия.
- Пройдены негативные сценарии с ошибками интеграции, сети и `streaming`.
- Определены условия отката по критичным операциям.
- Трассы содержат `provider`, `model`, версию, `schema version`, `tool_call_id`, `policy`, `cache`-метрики, задержки и `outcome`.