



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

8 шагов миграции в российское облако: как мы это делаем

Наш пайплайн: аудит, IaC на Terraform/OpenTofu, волновой перенос, тесты, переключение и откат

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Компания на 10–50 рабочих мест живёт на 1–2 стареющих офисных серверах: 1С, AD, файлы и терминал на одном гипервизоре, бэкап — на соседнем диске. Отказ железа — дни простоя и потерянные продажи, плановая замена — 1–2 млн ₽ CAPEX. Мы переносим такие инфраструктуры в российское облако по 8-шаговой методологии: предсказуемый счёт, простой в одно ночное окно, откат на каждом шаге.

Почему это важно бизнесу

- Один офисный сервер — единая точка отказа: авария RAID-контроллера или БП останавливает 1С, файлы и продажи сразу у всех
- Плановая замена железа раз в 5 лет — разовый CAPEX 1–2 млн ₽; облако переводит это в прогнозируемый ежемесячный OPEX
- Восстановление на новое железо из бэкапа — дни; из снапшота в облаке — минуты
- Новый филиал или склад — это новая VM за час из кода, а не закупка и доставка сервера
- Без лимитов биллинга облачный счёт непредсказуем — мы закрываем это порогами и авто-стопом ресурсов



Ключевые параметры реализации

~> 8.0

Пин мажорной версии
selectel/selectel в required_providers:
апгрейд мажора — только
осознанно,...
registry.terraform.io, selectel 8.x

0.219.x

Провайдер yandex-cloud/yandex;
ставим через зеркало
terraform-mirror.yandexcloud.net, не
с пуб...
yandex.cloud, Terraform quickstart

50/80/100%

Пороги уведомлений бюджета в
биллинге плюс жёсткий лимит с
остановкой ресурсов — счёт без
скуп...
наш стандарт

/MIR /MT:32

Финальная дельта файлсервера
roboscopy в окно миграции: зеркало
каталога в 32 потока по предсин...
learn.microsoft.com, robocopy

15 мин

Интервал log shipping журналов SQL
Server перед окном —
донакатываем цепочку в облаке за
минут...
learn.microsoft.com, log shipping

3 волны

Порядок переноса: некритичное →
второй DC с FSMO → 1C/SQL/RDS;
весь риск концентрируем в одной...
наш стандарт



Аудит и матрица миграции по каждой VM

Что настраиваем

Охват: гипервизоры VMware/Hyper-V, серверы 1C и SQL, сетевой периметр офиса; результат — матрица миграции по каждой VM

Как мы это делаем

- 1 Инвентаризация: RVTools для VMware, Get-VM/Get-VHD в PowerShell для Hyper-V — CSV со всеми VM, vCPU/RAM/дисками и версиями ОС
- 2 Карта зависимостей: Get-NetTCPConnection на Windows, ss -tnp на Linux плюс логи файрвола за неделю — граф «кто с кем говорит» до отключения чего-либо
- 3 Профиль нагрузки: метрики Zabbix/Performance Monitor за 30 дней; сайзим по p95, а не по установленной памяти
- 4 Лицензионный аудит: Windows Server (SPLA/BYOL), SQL Server, лицензии 1C (HASP или программные) — что едет, что покупаем заново
- 5 Сетевая карта: внешние IP в белых списках банк-клиентов, ЭДО и госсистем — заявки на смену IP подаём за 2 недели до окна

РЕЗУЛЬТАТ

Матрица «VM → метод переноса → целевой flavor → ответственный» снимает 80% споров в окно миграции: каждый шаг заранее согласован, сайзинг обоснован метриками, и клиент не платит в облаке за память, которая годами использовалась на 18%.

КЛЮЧЕВОЙ НЮАНС

Смотрим не паспортные ресурсы, а фактический профиль за месяц: типовой офисный сервер пересайжен вдвое. И заранее ловим EOL-ОС — Windows Server 2008/2003 требует сценария изоляции, а не lift-and-shift.



Целевая инфраструктура как код (Terraform/OpenTofu)

Что настраиваем

Охват: проект в облаке, сети и подсети, ВМ под AD и 1С, балансировщик RDS; код в Git, state — в S3-бэкенде провайдера

Как мы это делаем

- 1 required_providers: selectel/selectel ~> 8.0 плюс terraform-provider-openstack; провайдеры тянем через зеркало terraform-mirror.yandexcloud.net
- 2 Сеть: openstack_networking_network_v2 + subnet 10.20.0.0/24, security-группы deny-by-default, наружу — только VPN-шлюз
- 3 ВМ: ad-dc01 (4 vCPU/8 ГБ, Windows Server 2022 Std) и srv-1c (8 vCPU/32 ГБ, диск на NVMe-тарифе) из образов каталога провайдера
- 4 State — в S3-совместимом бакете с блокировкой use_lockfile (Terraform 1.10+/OpenTofu); terraform plan гоняем в CI на каждый merge request, apply — только после ревью
- 5 Site-to-site: IPsec на шлюзе провайдера или WireGuard на отдельной ВМ; офисный Keenetic/pfSense — вторым концом туннеля

РЕЗУЛЬТАТ

Всю площадку пересобираем с нуля одной командой terraform apply примерно за час — это одновременно DR-план и защита от «инфраструктуры в голове одного админа»: изменения видны в git diff, тестовое окружение поднимается тем же кодом.

КЛЮЧЕВОЙ НЮАНС

Публичный registry из РФ доступен нестабильно: прописываем provider_installation с network_mirror на зеркало Yandex Cloud в ~/.terraformrc либо используем OpenTofu — иначе terraform init падает в самый неудобн...



Волновой перенос данных и переключение

Что настраиваем

Охват: файлсервер, контроллер домена, SQL Server и базы 1С, RDS-ферма; два ночных окна, откат — по плану с таймингами

Как мы это делаем

- 1 Волна 1 (пт→сб): файлы — пресинк robocopy за несколько дней до окна, в окно только финальная дельта /MIR /MT:32 /R:1 /W:1; dev и тест просто импортируем
- 2 Волна 2: DC не копируем образом — поднимаем в облаке второй DC (Install-ADDSDomainController), ждём репликацию, переносим FSMO-роли; так исключаем USN rollback
- 3 Волна 3 (сб→вс): SQL — full заранее, diff вечером, tail-log в окно, RESTORE по цепочке WITH NORECOVERY; 1С до 100 ГБ — DT-выгрузка, крупнее — restore базы средствами...
- 4 Linux-BM конвертируем virt-v2v под KVM провайдера; Windows lift-and-shift — qemu-img convert в qcow2/raw с предустановкой virtio-драйверов
- 5 Переключение: TTL DNS заранее снижаем до 300 с, меняем записи и VPN-маршруты; откат = вернуть DNS, старую площадку держим неделю

РЕЗУЛЬТАТ

Бизнес теряет одно ночное окно на волну: утром пользователи заходят по тем же именам, 1С и общие папки на месте. Основной риск сжат в одну ночь с волной 3, и на неё всегда готов откат с конкретными таймингами и ответственными.

КЛЮЧЕВОЙ НЮАНС

Окно съедает не копирование, а «хвосты»: смена IP в белых списках банков и госсистем, перенос HASP и лицензирование 1С. Эти пункты выносим из окна и закрываем за 1–2 недели до него.



Подводные камни

✗ HASP-ключи 1С не переезжают

Аппаратный ключ не пробросить в облачную ВМ. Заранее меняем на программную лицензию или оставляем HASP-сервер в офисе с доступом по VPN.

✗ Старый IP в белых списках

Банк-клиенты, ЭДО и госсистемы привязаны к офисному IP. Заявки на смену подаём за 2 недели, иначе утром после миграции встают платежи.

✗ DC перенесён копией образа

Клон диска контроллера домена ловит USN rollback и ломает репликацию AD. Только новый DC через Install-ADDSDomainController и штатный перенос FSMO-ро...

✗ RDP/SSH наружу «на время работ»

Опубликованный 3389 собирает брутфорс за часы. Работаем только через site-to-site VPN, security-группы держим deny-by-default.

✗ terraform init падает из РФ

Публичный registry блокируется. Прописываем network_mirror на terraform-mirror.yandexcloud.net в ~/.terraformrc или переходим на OpenTofu.

✗ Сайзинг «как на старом сервере»

Паспортные 32 ГБ RAM часто заняты на 18%. Сайзим по p95 метрик за 30 дней — счёт за облако падает в 1,5–2 раза без потери скорости.

✗ tfstate на ноутбуке инженера

Потеря state — потеря управления инфраструктурой. Держим state в S3-бэкенде с блокировкой use_lockfile, доступ — по отдельным сервисным ключам.

✗ Бэкапы только у провайдера

Один аккаунт — одна точка отказа. Схема 3-2-1: S3 провайдера плюс ночная внешняя копия на офисный NAS под отдельной учёткой.



Как правильно

МИНИМУМ

- Аудит: инвентаризация VM, метрики за 30 дней, карта лицензий и внешних IP
- Site-to-site VPN до облака, ни одного RDP/SSH наружу
- Бюджетные алерты 50/80/100% и жёсткий лимит в биллинге
- Полные бэкапы 1C, AD и файлов в трёх местах до начала работ

НОРМАЛЬНО

- Вся инфраструктура в Terraform/OpenTofu, state в S3, код в Git
- Перенос волнами: некритичное → второй DC с FSMO → 1C/SQL/RDS
- SQL через backup + log shipping, файлы через robocopy /MIR /MT:32
- Чек-лист тестов 40+ пунктов: домен, 1C, печать, банк-клиент, ЭДО

ХОРОШО

- terraform plan в CI на каждый MR, apply — только после ревью
- DR-прогон: пересборка площадки из кода плюс восстановление из бэкапа
- Мониторинг Zabbix/облачный с алертами в Telegram ещё до переключения
- Blue-green по DNS для 24/7-сервисов: откат за минуты сменой записей



Чек-лист самопроверки

- | | |
|---|---|
| ☐ Есть ли матрица миграции: каждая VM → метод переноса → целевой flavor → ответственный? | ☐ Настроены ли бюджетные алерты 50/80/100% и жёсткий лимит расходов в биллинге? |
| ☐ Проверены ли лицензии 1C: программные или HASP, и есть ли план для аппаратного ключа? | ☐ Есть ли план отката с таймингами и решено ли, до какого дня живёт старая площадка? |
| ☐ Поданы ли заявки на смену IP в белых списках банков, ЭДО и госсистем? | ☐ Прогнан ли тест восстановления из бэкапа на пустой VM до боевого окна? |
| ☐ Описана ли целевая инфраструктура кодом и хранится ли tfstate вне ноутбука инженера? | ☐ Замерена ли скорость 1C (тест Гилёва) до и после переезда? |
| ☐ Поднят ли site-to-site VPN и закрыт ли прямой RDP/SSH из интернета? | ☐ Сайзинг VM подтверждён метриками за 30 дней, а не паспортом старого сервера? |

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.



Как поможет ITFresh

ITFresh — ИТ-аутсорсинг для юридических лиц до 50 рабочих мест в Москве и области. 15+ лет практики, собственная инфраструктура в дата-центре МТС (8 серверов Dell Xeon Platinum).

- Бесплатный аудит инфраструктуры до 50 РМ: инвентаризация, TCO в трёх облаках, план миграции
- Миграция под ключ: Terraform-проект, VPN, перенос 1C/AD/SQL/файлов волнами за 1–2 ночных окна
- Пост-миграционное сопровождение: мониторинг, бэкапы 3-2-1, бюджетные лимиты, SLA на инциденты
- Разбор лицензий: SPLA/BYOL по Microsoft, перевод 1С с HASP на программные лицензии
- Настройка DR: пересборка площадки из кода и регулярные тестовые восстановления

15+

лет в ИТ-поддержке

50

рабочих мест — наш профиль

МТС

дата-центр, Москва



КОНТАКТЫ

Обсудить вашу задачу

Сайт **itfresh.ru**

Телефон **+7 903 729-62-41**

Telegram **@ITfresh_Boss**

Бесплатно посмотрим вашу инфраструктуру по этому чек-листу и скажем, где тонко — без обязательств.



itfresh.ru



Техническая база

- 01** Selectel provider — Docs overview, required_providers (registry.terraform.io — 8.x)
- 02** Yandex Cloud: начало работы с Terraform, зеркало провайдеров (yandex.cloud — 0.219)
- 03** robocopy — справочник ключей /MIR, /MT, /R, /W (learn.microsoft.com — 2025)
- 04** About Log Shipping (SQL Server) (learn.microsoft.com — SQL 2022)
- 05** 1С:ИТС — выгрузка/загрузка ИБ (DT), перенос клиент-серверной ИБ (its.1c.ru — 8.3)
- 06** virt-v2v — конвертация ВМ под KVM (libguestfs.org — 2.x)
- 07** Наш шаблон матрицы миграции и чек-лист тестов (40+ пунктов) (itfresh.ru — 2026)

