Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

IT-аутсорсинг в Омске: удалённая поддержка из Москвы

Как мы строим удалённый контур: WireGuard + PKI, RMM, Prometheus и дежурство по UTC+6

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Компания в Омске работает по UTC+6, инженеры — в Москве: с 09:00 до 12:00 по местному времени (06:00-09:00 МСК) заявки некому брать. Дальше типовой набор — наружу проброшен RDP/3389, инфраструктура не документирована, инцидент виден только после звонка директора. Мы закрываем это контуром: туннель WireGuard с ключами и своим PKI, RMM-агенты на узлах, метрики с порогами и выдер...

Почему это важно бизнесу

- Час простоя 1С в торговой компании на 40 человек — это вставшие отгрузки, кассы и оплаты: счёт идёт на выручку смены
- Сильный админ в штате стоит дороже пакета аутсорсинга и уходит вместе с паролями: знания живут в голове, а не в документации
- Разрыв в 3 часа между Москвой и Омском без дежурства означает, что авария утром чинится к обеду — половина рабочего дня филиала выпадает
- Windows Server 2012 R2 без обновлений с 10.10.2023 (дальше только платная ESU) и бэкап на USB без теста восстановления — не экономия, а отложенн...
- Недокументированный контур невозможно передать: любая смена подрядчика превращается в повторный аудит и оплату одного и того же дважды

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

UTC+6

Omsk Standard Time, +3 ч к Москве, без перехода на летнее время — по нему строим дежурство, ок…

25 с

PersistentKeepalive в секции [Peer]: держит NAT-сессию у провайдера, задаём на стороне за NAT,…

1420

MTU интерфейса WireGuard при MTU 1500 на маршруте по умолчанию: wg-quick вычитает 80 байт овер…

1m

Глобальные scrape_interval и evaluation_interval Prometheus (значения по умолчанию) — наш базо…

30 с / 5 м

group_wait и group_interval Alertmanager по умолчанию: пачкуем алерты группы, чтобы дежурного…

1560:1591

Диапазон портов рабочих процессов rphost кластера 1С — открываем точечно, вместе с 1540 (ragen…

РЕАЛИЗАЦИЯ 1 ИЗ 3

Канал доступа: WireGuard, свой PKI и терминал с логированием

Что настраиваем

Периметр клиента и наш рабочий терминал в Москве: шлюз GW01, RMM-агенты на серверах и ключевых ПК, доступ инженеров

Как мы это делаем

1. На шлюзе поднимаем WireGuard: отдельный пир на инженера, AllowedIPs строго под подсети клиента, PersistentKeepalive = 25 для пиров за NAT
2. MTU туннеля оставляем 1420 (wg-quick берёт MTU маршрута по умолчанию минус 80 байт); при потерях и «залипаниях» RDP и 1С задаём MTU явно в [Interface]
3. Доступ к RDP только изнутри туннеля: 3389/TCP наружу не публикуем, вход — через RD Gateway по 443/TCP и доменные учётки с MFA
4. Инженеры работают с выделенного терминала: запись сессий, персональные учётные записи, ключи и пароли — в парольном хранилище (Bitwarden), а не в конфигах
5. Резервный путь: второй пир через другого провайдера и OpenVPN как fallback, чтобы падение одного канала не отрезало нас от площадки

РЕЗУЛЬТАТ

Площадка перестаёт светить управляющими портами наружу: сканеры видят только UDP-порт WireGuard, который не отвечает без валидного ключа (протокол молчит на невалидный пакет). Любое действие инженера привязано к конкретной учётке и записанной сессии, а при аварии канала мы заходим резервн…

КЛЮЧЕВОЙ НЮАНС

Ключевой нюанс — AllowedIPs: в WireGuard это одновременно маршрутизация и криптоключевание (cryptokey routing). Широкая маска даёт лишний доступ и ломает маршруты филиалов, поэтому подсети описываем поимённо:…

РЕАЛИЗАЦИЯ 2 ИЗ 3

1С в клиент-серверном режиме на PostgreSQL вместо файловой базы

Что настраиваем

Сервер 1С и СУБД на площадке клиента (Hyper-V), 30-50 сеансов, торговая или учётная конфигурация

Как мы это делаем

1. Выносим базу из файлового режима на SMB в кластер: ragent на 1540, менеджер кластера rmngr на 1541, рабочие процессы rphost в диапазоне 1560:1591
2. Ставим службу RAS (порт администрирования 1545) и снимаем утилитой rac показатели сеансов, соединений и памяти рабочих процессов
3. PostgreSQL: shared_buffers порядка 25 % ОЗУ, effective_cache_size 50-75 % ОЗУ, max_connections под реальное число сеансов, отдельный том NVMe под PGDATA и WAL
4. В кластере задаём «Максимальный объём памяти рабочих процессов» и интервал перезапуска rphost, технологический журнал logcfg.xml ведём по нужным событиям (EXCP, TLO…
5. Проверяем результат замерами: время открытия тяжёлых отчётов до и после переноса фиксируем в отчёте клиенту

РЕЗУЛЬТАТ

Тяжёлые отчёты перестают упираться в сеть и файловые блокировки: нагрузка уходит на сервер СУБД, а не на канал до файлового шара. Пропадают «зависания» и повреждения базы при обрывах SMB, а сеансы становятся управляемыми — их видно в консоли кластера и можно завершить точечно.

КЛЮЧЕВОЙ НЮАНС

Опираемся на руководство администратора по клиент-серверному варианту: без запущенной службы RAS кластер администрируется только локальной консолью, а без открытого диапазона 1560:1591 клиенты подключаются чер…

РЕАЛИЗАЦИЯ 3 ИЗ 3

Мониторинг и дежурство: Prometheus, Alertmanager, смена под Омск

Что настраиваем

Стек мониторинга в дата-центре, экспортеры на всех узлах площадки, эскалация в Telegram дежурного инженера

Как мы это делаем

1. Ставим node_exporter (9100/TCP) на Linux и windows_exporter (9182/TCP) на серверы Windows, глобальный scrape_interval оставляем 1m, критичные цели снимаем с интерва…
2. Правила Prometheus пишем с выдержкой for: свободное место (node_filesystem_avail_bytes / node_filesystem_size_bytes < 0.1, for: 15m), SMART и состояние RAID, доступ…
3. В Alertmanager группируем по площадке и хосту (group_by: [site, instance]), оставляем group_wait 30s и group_interval 5m по умолчанию, ночью маршрутизируем в дежурс…
4. Дашборды Grafana — по подсистемам: СУБД, гипервизор, каналы связи и филиалы; отдельная панель с часовым поясом Asia/Omsk под окна работ
5. Дежурство сдвигаем на 3 часа: смена начинается в 07:00 МСК, что уже 10:00 в Омске, ночью — только critical с эскалацией звонком

РЕЗУЛЬТАТ

Инциденты чинятся до звонка клиента: заполнение диска и деградация RAID уходят в алерт задолго до отказа, а простой филиала видно раньше, чем открывается магазин. Смещённое дежурство закрывает утренний разрыв часовых поясов — сотрудники в Омске получают инженера с первой минуты рабочего д…

КЛЮЧЕВОЙ НЮАНС

Алерт без порога и без for превращается в шум, который перестают читать. Мы отделяем critical (эскалация ночью) от warning (разбор в утреннюю смену) метками severity и маршрутами Alertmanager, а плановые работ…

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **RDP наружу вместо туннеля**
  Проброс 3389/TCP на роутере ловит перебор паролей в первые часы. Управление закрываем в WireGuard, RDP публикуем только через RD Gateway по 443 с MFA

- ✕ **Туннель рвётся каждые пару минут**
  Пир за NAT молчит, и провайдер закрывает UDP-сессию. Лечится PersistentKeepalive = 25 в секции [Peer] на стороне за NAT, а не на обеих сразу

- ✕ **Домашние роутеры между филиалами**
  Бытовые устройства не держат постоянный site-to-site и не обновляются. Ставим маршрутизаторы с аппаратным шифрованием, IKEv2 + AES-GCM и одинаковой в…

- ✕ **1С в файловом режиме на 30+ сеансов**
  Блокировки и обрывы SMB бьют по базе физически. Переводим в клиент-серверный вариант: сервер 1С (1540/1541/1560:1591) и PostgreSQL на отдельном томе

- ✕ **Бэкап без теста восстановления**
  Копия на USB-диск без проверки — это лотерея. Планово поднимаем базу и файловый сервер из копии на тестовый хост и фиксируем RTO в отчёте

- ✕ **Копия рядом с боевым сервером**
  Шифровальщик уносит и данные, и бэкап в том же сегменте. Делаем реплику в дата-центр и включаем в hardened-репозитории immutability от 7 суток

- ✕ **Задачи по московскому времени**
  Обслуживание, запущенное «ночью» по МСК, приходит в Омск к утру. Окна работ, регламентные задания 1С и планировщик выставляем в Omsk Standard Time (U…

- ✕ **Инфраструктура без документации**
  Схемы и пароли в голове одного инженера — риск и для нас, и для клиента. Паспорт площадки и runbook ведём в git, доступ к репозиторию у клиента есть

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Закрыть 3389/22/веб-панели снаружи, доступ — только через WireGuard с персональным п…
- Инвентаризация за 3-5 дней: узлы, версии ОС, локальные и доменные учётные записи, ли…
- Бэкап по расписанию с уведомлением об ошибке задания и одним тестовым восстановление…
- Вывести из эксплуатации ОС без поддержки (Windows Server 2012 R2 и старше) либо изол…

НОРМАЛЬНО

- 1С в клиент-серверном режиме, метрики rphost и PostgreSQL (сеансы, память, блокировк…
- Prometheus с порогами и for по дискам, RAID, службам и каналам, алерты в Telegram че…
- Site-to-site IPsec (IKEv2) между офисом, складами и точками продаж на одной модели м…
- Дежурство со сдвигом на Omsk Standard Time и SLA-реакция, зафиксированная в договоре

ХОРОШО

- Реплика бэкапов в дата-центр, immutability от 7 суток и ежеквартальный тест восстано…
- Два контроллера домена, кластер гипервизора с отказоустойчивостью и резервный канал…
- Паспорт инфраструктуры и runbook в git с доступом клиента к репозиторию
- Ежемесячный отчёт: инциденты, аптайм по метрикам up, ёмкость дисков и план работ на…

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- ☐ Управляющие порты (RDP 3389, SSH 22, веб-панели) закрыты снаружи и доступны только через VPN?
- ☐ У каждого инженера и подрядчика свой пир WireGuard и своя учётная запись, а не общий пароль?
- ☐ Есть актуальная схема сети и паспорт площадки, к которым у вас есть доступ?
- ☐ База 1С работает в клиент-серверном режиме, а не файлом на сетевой шаре?
- ☐ Все серверные ОС получают обновления безопасности, версий без поддержки не осталось?
- ☐ Резервные копии уезжают за пределы площадки и защищены от удаления (immutability)?
- ☐ Когда последний раз восстановление проверяли на практике и сколько оно заняло?
- ☐ Мониторинг присылает алерт до звонка сотрудника, пороги и выдержка for настроены?
- ☐ Дежурство покрывает рабочий день по Omsk Standard Time, а не только по Москве?
- ☐ Зафиксировано ли время реакции по SLA и как оно измеряется в отчёте?

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

ЧТО МЫ ДЕЛАЕМ

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).

- Аудит за 3-5 дней: инвентаризация, учётки, риски и план работ по приоритетам
- Строим удалённый контур: WireGuard с PKI и MFA, RMM на узлах, helpdesk в Telegram
- Переносим 1С в клиент-серверный режим на PostgreSQL и вычищаем тормоза отчётов
- Prometheus и Alertmanager с порогами, дежурство со сдвигом под UTC+6, ночью — только critical
- Бэкап и реплика в дата-центр с immutability и проверкой восстановления, ежемесячный отчёт

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

ДОКУМЕНТАЦИЯ И НАШ СТЕК

Техническая база

01 wg(8) и wg-quick(8): PersistentKeepalive, AllowedIPs, расчёт MTU интерфейса (wireguard.com — 2026)

02 Prometheus Configuration: global scrape_interval и evaluation_interval (prometheus.io — 2026)

03 Alertmanager Configuration: route, group_by, group_wait, group_interval (prometheus.io — 2026)

04 Клиент-серверный вариант работы. Руководство администратора: порты кластер… (its.1c.ru — 8.3)

05 PostgreSQL Resource Consumption: shared_buffers, effective_cache_size, max… (postgresql.org — 2026)

06 Hardened Repository. How Immutability Works: период 7-9999 суток (helpcenter.veeam.com — 2026)

07 Default Time Zones: Omsk Standard Time (UTC+06:00) (learn.microsoft.com — 2026)

08 Windows Server 2012 R2 end of support: 10.10.2023 и программа ESU (learn.microsoft.com — 2023)

09 Наш шаблон: паспорт площадки и runbook дежурного в git (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.