Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Время в офисе: NTP-иерархия под 1С, ЭДО и Kerberos

Наша методология: PDC-эмулятор, GPO, гипервизоры, chrony и мониторинг смещения

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Расхождение часов не «тикает тихо»: Kerberos отказывает при отклонении свыше 5 минут, а в ЭДО без штампа времени TSP атрибут времени подписи берётся с локальных часов машины. Мы разворачиваем единую иерархию: внешние пиры только на PDC-эмуляторе корневого домена, остальные узлы — NT5DS через GPO, синхронизация с гипервизором и часами BIOS выведена из цепочки.

Почему это важно бизнесу

- Вход в домен и в 1С падает у всей смены: KDC не выдаёт билет при расхождении свыше 5 минут — это простой офиса, а не мелкий глюк.
- Отклонённые платёжки и УПД: без TSP-штампа время подписи берётся с локальных часов, и приёмная сторона видит документ «из будущего».
- Разбор инцидента рассыпается: журналы 1С, AD, СКУД и видеонаблюдения не сходятся по секундам — сопоставлять события нечем.
- Ночные регламенты наступают друг на друга: бэкапы, обслуживание СУБД и обмены 1С стартуют не в своё окно.
- Диагностика вслепую: «плавающие» ошибки 1С и ЭДО без единой шкалы времени не воспроизводятся и не локализуются.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

5 мин

Допуск Kerberos между клиентом и KDC — жёсткая граница входа в домен

learn.microsoft.com, Accurate Time

1 с

Наш допуск расхождения между узлами кластера 1С и сервером СУБД

наш стандарт для кластера 1С и СУБД

300 → 1 с

MaxAllowedPhaseOffset: default члена домена → наше значение, часы ставятся шагом

learn.microsoft.com, W32Time\Config

6 / 10

MinPollInterval / MaxPollInterval (log2 с): опрос 64–1024 с вместо 32768 с

learn.microsoft.com, W32Time\Config

1024 с

SpecialPollInterval из GPO-шаблона для manual-пиров с флагом SpecialInterval 0x1

learn.microsoft.com, Configure NTP Client

7800 с

ClockHoldoverPeriod: без свежих сэмплов W32Time заново ищет источники времени

learn.microsoft.com, W32Time\Config

РЕАЛИЗАЦИЯ 1 ИЗ 3

Этап 1. Корень времени: PDC-эмулятор

Что настраиваем

Scope: PDC-эмулятор корневого домена, 1 узел, Windows Server 2019/2022/2025

Как мы это делаем

1. Находим владельца роли: netdom query fsmo. Внешние пиры ставим только на PDC-эмуляторе корневого домена, остальные DC берут время по иерархии.
2. Три manual-пира: w32tm /config /manualpeerlist:"ntp1.vniiftri.ru,0x8 ntp2.vniiftri.ru,0x8 ntp.ix.ru,0x8" /syncfromflags:MANUAL /update
3. w32tm /config /reliable:yes ставит AnnounceFlags 5 (0x1 Always + 0x4 Always reliable) вместо default 10 и даёт флаг GTIMESERV; затем перезапуск w32time.
4. Рамка на поправку: MaxAllowedPhaseOffset=1, MaxPos/MaxNegPhaseCorrection=3600 вместо 172800 у DC — абсурдный сэмпл отбрасывается с записью события.
5. Гасим скачки Secure Time Seeding: UtilizeSslTimeData=0 в W32Time\Config (в Windows Server 2025 это уже default, в 2019/2022 значение 1).

РЕЗУЛЬТАТ

Один авторитетный источник вместо тридцати самостоятельных: исходящий UDP/123 разрешён только с этого узла к трём пирам, входящий из интернета закрыт. Смещение корня держим в пределах 50 мс — запас в 6000 раз до порога Kerberos в 5 минут.

КЛЮЧЕВОЙ НЮАНС

Три пира, а не два: с двумя источниками алгоритм W32Time не отбракует сбойный. Либо три, либо второму флаг UseAsFallbackOnly (0x2). Флаг 0x8 (Client) указываем явно, иначе возможен symmetric-active.

Этап 2. Иерархия домена и клиенты через GPO

Что настраиваем

Scope: остальные DC, серверы 1С и СУБД, файловый сервер, RDSH, все рабочие станции

Как мы это делаем

1. GPO «Time Providers → Configure Windows NTP Client»: Type=NT5DS, заготовку NtpServer time.windows.com,0x9 из шаблона стираем — клиент идёт по иерархии.
2. Ускоряем опрос: в Global Configuration Settings MinPollInterval=6, MaxPollInterval=10 вместо 10/15 у члена домена (2^15 = 32768 с между запросами).
3. CrossSiteSyncFlags: при одном сайте оставляем default 2 (All), при нескольких ставим 1 (PdcOnly), чтобы не тянуть время через узкое WAN-плечо.
4. Часовой пояс: штатной ADMX-политики нет — раскатываем GPP-задачей tzutil /s "Russian Standard Time", проверяем w32tm /tz, иначе журналы уедут на 3 часа.
5. Приёмка: w32tm /monitor /domain:corp.local и w32tm /query /source на выборке PM — источник обязан указывать на DC, не на time.windows.com.

РЕЗУЛЬТАТ

Внешний NTP-трафик схлопывается до одного узла, разброс внутри LAN уходит в единицы миллисекунд. Машина, выпавшая из иерархии (была в рабочей группе), возвращается одной командой w32tm /config /syncfromflags:domhier /update с перезапуском службы.

КЛЮЧЕВОЙ НЮАНС

Если NtpServer задан политикой Configure Windows NTP Client, на члене домена значение из ветки Parameters не используется — рабочую конфигурацию читаем через w32tm /query /configuration, а не в regedit.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Этап 3. Гипервизор, Linux-узлы и мониторинг

Что настраиваем

Scope: хосты ESXi/Hyper-V, виртуальные DC, узлы 1С и PostgreSQL на Linux, Zabbix

Как мы это делаем

1. Разрываем петлю «часы хоста → гость»: на виртуальных DC VMICTimeProvider\Enabled=0, в VMware — tools.syncTime = FALSE и все ключи time.synchronize.* = FALSE.
2. Сам хост синхронизируем сверху: esxcli system ntp set -s ntp1.vniiftri.ru -e yes (с 7.0 U3 только esxcli, не правкой файла) и ruleset ntpClient включён.
3. Linux-узлы 1С/СУБД: chrony 4.x — server <DC> iburst maxpoll 10, makestep 1.0 3, rtcsync, bindcmdaddress 127.0.0.1; systemd-timesyncd маскируем.
4. Контроль: chronyc tracking (System time, Last offset, Leap status) и w32tm /stripchart /computer:DC01 /samples:5 /dataonly на Windows-узлах.
5. Мониторинг: счётчик «Windows Time Service → Computed Time Offset» и наш шаблон Zabbix — WARN 500 мс, HIGH 2 с, DISASTER 30 с, алерт «нет синка».

РЕЗУЛЬТАТ

Гость больше не берёт время с невыверенных часов хоста, chrony держит offset в LAN на уровне десятков микросекунд. Дежурный видит дрейф задолго до отказов: порог алерта 500 мс против 1 с допуска кластера 1С и 300 с допуска Kerberos.

КЛЮЧЕВОЙ НЮАНС

Снятая галка «Synchronize guest time with host» не отключает однократный sync при vMotion, снапшоте, сжатии диска и рестарте VMware Tools — глушим ключи time.synchronize.*, включая resume.host и tools.startup.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- **Каждая машина ходит в интернет сама**
  Type=NTP на членах домена вместо NT5DS: десятки исходящих сессий UDP/123 и разброс между PM при живой AD-иерархии.
- **Гипервизор как источник времени**
  VMICTimeProvider или VMware Tools на виртуальном DC замыкают цепочку на часы хоста, которые сами никем не выверены.
- **UDP/123 открыт с WAN на вход**
  Служба времени становится чужим рефлектором. Наружу разрешаем только исходящий 123 с PDC-эмулятора, входящий с WAN режем.
- **Два NTP-пира вместо трёх**
  Алгоритм не отбракует сбойный источник: нужен третий пир либо флаг UseAsFallbackOnly (0x2) на втором — прямая рекомендация доки.
- **Правка реестра при активной GPO**
  Политика Configure Windows NTP Client перекрывает NtpServer в реестре; рабочую конфигурацию смотрим w32tm /query /configuration.
- **Верное UTC, неверная зона**
  Часы синхронны, а журналы и выгрузки расходятся на 3 часа: не выставлены Russian Standard Time на Windows и Europe/Moscow на Linux.
- **Поправка без верхней границы**
  MaxPos/MaxNegPhaseCorrection = 0xFFFFFFFF у члена домена: принимается любой сэмпл, даже уводящий часы на сутки вперёд.
- **Нет мониторинга смещения**
  Дрейф ловят по жалобе бухгалтера. Нужен активный контроль offset и событий W32Time 36/47/50 в журнале System.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- PDC-эмулятор на 3 внешних пира, остальные узлы — NT5DS через GPO
- Зона MSK: tzutil "Russian Standard Time" на Windows, Europe/Moscow на Linux
- Входящий UDP/123 с WAN закрыт, исходящий — только с узла времени
- Синхронизация с гипервизором отключена на всех виртуальных DC

НОРМАЛЬНО

- Три пира с флагом 0x8, резервный — 0x2 UseAsFallbackOnly
- MinPollInterval=6, MaxPollInterval=10, MaxAllowedPhaseOffset=1 на серверах
- MaxPos/MaxNegPhaseCorrection=3600 вместо default 0xFFFFFFFF у члена домена
- chrony 4.x на Linux-узлах 1С и СУБД, systemd-timesyncd замаскирован

ХОРОШО

- w32tm /config /reliable:yes: AnnounceFlags 5 и флаг GTIMESERV на узле времени
- UtilizeSslTimeData=0 на 2019/2022, где Secure Time Seeding включён по умолчанию
- NTS для внешнего плеча (chrony 4.x, NTS-KE на TCP/4460)
- Локальный Stratum-1 от ГЛОНАСС/GPS-приёмника на площадке

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Роль PDC-эмулятора подтверждена через netdom query fsmo, и внешние пиры заданы именно на этом узле?
- [ ] На членах домена Type=NT5DS, а w32tm /query /source указывает на DC, а не на time.windows.com?
- [ ] На виртуальных DC отключена синхронизация с хостом: VMICTimeProvider Enabled=0 или tools.syncTime=FALSE?
- [ ] Однократные синхронизации VMware Tools заглушены всеми ключами time.synchronize.* в настройках ВМ?
- [ ] Входящий UDP/123 из интернета закрыт на периметре, исходящий разрешён только узлу времени?
- [ ] Зона MSK (UTC+3) выставлена на серверах, РМ, роутере, гипервизоре, камерах и СКУД?
- [ ] Узлы кластера 1С и сервер СУБД расходятся между собой менее чем на 1 секунду?
- [ ] На Linux-узлах работает chrony, и chronyc tracking показывает Leap status: Normal?
- [ ] MaxAllowedPhaseOffset и MaxPos/MaxNegPhaseCorrection выставлены явно, а не оставлены по умолчанию?
- [ ] События W32Time 36/47/50 и счётчик Computed Time Offset заведены в алерты дежурного?

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).

- Проектируем иерархию времени: PDC-эмулятор, GPO, гипервизоры, роутер, Linux-узлы 1С — одним документом.
- Аудит за день: w32tm /monitor по домену, chronyc sources, разбор событий 36/47/50, отчёт с параметрами.
- Ставим мониторинг смещения с порогами 500 мс / 2 с / 30 с и алертом дежурному в Telegram.
- Разбираем петли «хост → гость» и возвращаем виртуальные DC в доменную иерархию без простоя.
- На абонентском обслуживании NTP входит в плановые работы: реагируем на дрейф до жалоб.

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 Windows Time Service Tools and Settings: реестр W32Time и GPO-шаблоны (learn.microsoft.com — 2026)

02 Accurate Time for Windows Server 2016: допуск Kerberos 5 минут (learn.microsoft.com — 2025)

03 Secure Time Seeding Recommendations for Windows Server (learn.microsoft.com — 2025)

04 Timekeeping best practices for Windows, including NTP (KB 315346) (knowledge.broadcom.com — 2025)

05 Disabling Time Synchronization for virtual machines (KB 326306) (knowledge.broadcom.com — 2025)

06 Synchronize ESXi Clocks with a Network Time Server (esxcli) (techdocs.broadcom.com — 8.0)

07 chrony.conf(5): makestep, maxpoll, rtcsync, nts, bindcmdaddress (chrony-project.org — 4.x)

08 Администрирование клиент-серверного варианта: кластер серверов (its.1c.ru — 8.3)

Основано на официальной документации продуктов и нашей практике внедрения.