



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

IIS на Windows Server: развёртывание по нашей методологии

Роль Web Server (IIS) 10.0, пулы приложений, TLS/HSTS, URL Rewrite + ARR и публикация 1С

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Компании до 50 РМ держат на IIS критичные сервисы: веб-клиент 1С, OWA, RD Web Access, внутренние порталы. Типовая картина «поставили роль и забыли»: пулы на дефолтах, recycle попадает в рабочие часы, сертификаты продлеваются вручную и просрочиваются, наружу торчит лишнее. Мы разворачиваем IIS по скриптовому стандарту, где каждый параметр задан осознанно.

Почему это важно бизнесу

- Просроченный сертификат = встали веб-клиент 1С и сдача отчётности: бухгалтерия теряет день, сроки перед ФНС не двигаются
- Recycle пула в рабочие часы рвёт сеансы 1С — потерянные документы и повторный ввод данных сотрудниками
- Открытый наружу порт 80 с дефолтной страницей и включённым TLS 1.0 — готовая точка входа для атак на периметр
- «Уникальный» сервер, собранный руками: любой сбой или переезд — дни восстановления вместо часа по скрипту



Ключевые параметры реализации

10.0

Версия IIS одна для WS 2016–2025
— методология едина, отличия в
сборке HTTP.sys и поддержке TL...

по докам learn.microsoft.com

0

Idle Time-out пула в production:
дефолтные 20 мин выгружают
w3wp — первый запрос утром
холодный

наш стандарт (default 20 мин)

03:00

Recycling по Specific Times вместо
дефолтных 1740 мин — перезапуск
пула не попадает на пользов...

наш стандарт

70%

Private Memory Limit пула от RAM
сервера: авторестарт при утечке
памяти до исчерпания хоста

наш стандарт

2.1 + 3.0

URL Rewrite и ARR — отдельные
модули, в состав роли не входят;
ARR работает поверх URL Rewrite

по докам iis.net

55 дней

Порог продления Let's Encrypt
(сертификат на 90 дней):
ежедневная задача wacs в Task
Scheduler

win-acme 2.2.x



Роль Web Server и каркас сайта через PowerShell

Что настраиваем

Сервер приложений Windows Server 2022/2025, роль Web Server (IIS), модуль IISAdministration

Как мы это делаем

- 1 Install-WindowsFeature Web-Server,Web-Asp-Net45,Web-Windows-Auth,Web-Filtering,Web-Mgmt-Console — фиксированный список фич, воспроизводим на любом сервере одинаково
- 2 Контент выносим с системного диска: D:\Sites\<имя>, под каждый сайт свой пул New-WebAppPool; processModel.identityType оставляем ApplicationPoolIdentity
- 3 Права через icacls: виртуальная учётка IIS AppPool\<пул> получает (OI)(CI)RX только на каталог сайта, запись — точно в App_Data/upload
- 4 Пул: idleTimeout=0, periodicRestart.time=0 + schedule на ночь, queueLength 2000-5000 — держим пиковые всплески без 503.2 (QueueFull в HTTPERR)
- 5 Default Web Site останавливаем, binding *:80 освобождаем; логи W3C переносим на D:, добавляем поле cs-host (Time-Taken уже в дефолтном наборе — не отключать)

РЕЗУЛЬТАТ

Новый сервер поднимается по скрипту за 15-20 минут в идентичной конфигурации. Падение одного приложения не задевает соседние (изоляция пулов), первый утренний запрос отвечает без прогрева, пики нагрузки не превращаются в 503.

КЛЮЧЕВОЙ НЮАНС

Дефолты пула рассчитаны на shared-хостинг, а не на корпоративный сервер: 20 мин idle и 29 ч recycle обязаны быть переопределены. Все правки делаем через IIS:\AppPools, чтобы они попали в applicationHost.config.



TLS: сертификаты, HSTS и заголовки безопасности

Что настраиваем

HTTPS-биндинги всех сайтов узла: внутренние имена — AD CS, внешние — Let's Encrypt

Как мы это делаем

- 1 Внутренние сервисы: дубликат шаблона Web Server в AD CS с правом Autoenroll и SAN в запросе — продление идёт автоматически, руками ничего не трогаем
- 2 Внешние имена: win-acme (wacs.exe), валидация http-01 прямо через IIS, установка в binding и задача автопродления в Task Scheduler
- 3 HSTS включаем штатным блоком `<hsts enabled="true" max-age="31536000">` (доступен в IIS 10 с версии 1709), а не через customHeaders
- 4 TLS 1.0/1.1 гасим на уровне Schannel, TLS 1.3 в WS2022+ уже включён; добавляем X-Content-Type-Options, X-Frame-Options
- 5 Несколько HTTPS-сайтов на одном IP:443 — биндинги с SNI (Require SNI), проверяем соответствие отпечатков через Get-WebBinding

РЕЗУЛЬТАТ

Сертификаты живут без участия инженера: внутренние продлевает AD CS, внешние — win-acme с автоматической заменой в биндинге. Внешний SSL-тест стабильно проходит на класс A, устаревшие протоколы не принимаются.

КЛЮЧЕВОЙ НЮАНС

Главная причина «упавшего HTTPS» — продлённый сертификат, не попавший в binding. Поэтому продление и установка в биндинг обязаны быть одним автоматическим процессом, а срок действия — метрикой мониторинга.



ARR как reverse проху и публикация веб-клиента 1С

Что настраиваем

Фронтный IIS перед backend'ами: веб-клиент 1С, OWA, внутренние ASP.NET-приложения

Как мы это делаем

- 1 Ставим URL Rewrite 2.1 + ARR 3.0, включаем Server Proxy Settings → Enable proxy; передаём HTTP_X_FORWARDED_PROTO через serverVariables
- 2 Backend'ы заводим в Server Farm с health-тестом по URL и интервалом опроса — упавшая нода выводится из ротации автоматически
- 3 1С публикуем штатным webinst.exe -publish -iis: приложение с wsisapi.dll и default.vrd, обязательно в отдельном пуле
- 4 Пул под wsisapi — No Managed Code, разрядность по платформе 1С (enable32BitAppOnWin64), recycling согласован с сеансами
- 5 Request Filtering: maxAllowedContentLength поднимаем под обмены 1С и загрузку файлов, служебные пути backend'ов наружу не публикуем

РЕЗУЛЬТАТ

Один вход по 443 для всех сервисов вместо зоопарка проброшенных портов: маршрутизация по путям /1с, /mail, /portal, отказавший backend выпадает из балансировки без звонков пользователей, периметр сокращён до одного узла.

КЛЮЧЕВОЙ НЮАНС

ARR — это надстройка над URL Rewrite: без установленного Rewrite-модуля и разрешённых server variables прокси-правила молча не работают. Backend должен получать X-Forwarded-Proto, иначе ломаются редиректы и ку...



Подводные камни

✗ Recycle 1740 мин попадает в день

Дефолтные 29 часов «дрейфуют» по суткам и рано или поздно рвут сеансы днём. Обнуляем Regular Time Interval и задаём Specific Times в ночное окно.

✗ Выгрузка пула по Idle 20 минут

Первый запрос после простоя ждёт старта w3wp и JIT — до десятков секунд. Ставим idleTimeout=0 и добавляем Application Initialization (Web-Applnit) с...

✗ Права выданы не той учётке

После переноса контента ловят 401.3/500.19: ACL дают Users вместо виртуальной учётки. Права назначаем icacis на IIS AppPool\<имя пула> — и только на...

✗ ARR без X-Forwarded-заголовков

Backend видит http и IP прокси: ломаются редиректы, куки Secure, логи. Прописываем serverVariables и разрешаем их в allowedServerVariables конфига Re...

✗ HSTS через customHeaders

Заголовок уходит и в HTTP-ответах, что нарушает спецификацию. В IIS 10 (1709+) используем штатный <hsts> — он отдаёт заголовок только по HTTPS и умеет...

✗ Логи IIS забивают системный диск

C:\inetpub\logs\LogFiles растёт без ротации и валит сервер по месту. Переносим на диск данных, чистим по расписанию, но оставляем Time-Taken — без не...

✗ Разрядность ISAPI не совпала

wsisapi.dll от 32-битной платформы 1С в 64-битном пуле даёт 500 без внятного лога. Разрядность пула (enable32BitAppOnWin64) ставим по разрядности пла...

✗ Продлённый сертификат не в биндинге

Renewal прошёл, а binding держит старый отпечаток — HTTPS падает «внезапно». Установку в binding делает сама задача win-асме; после продления сверяем...



Как правильно

МИНИМУМ

- Роль ставится скриптом Install-WindowsFeature — состав фич зафиксирован
- Отдельный пул на сайт, ApplicationPoolIdentity, контент вне системного диска
- HTTPS-биндинг с валидным сертификатом, HTTP — 301-редирект на HTTPS
- Default Web Site остановлен, логи W3C с полем Time-Taken

НОРМАЛЬНО

- Пулы: idle 0, recycle по ночному расписанию, Private Memory Limit ~70% RAM
- Автопродление сертификатов (AD CS / win-acme), штатный HSTS, TLS 1.0/1.1 выключены
- Правила URL Rewrite в web.config сайта — версионироваться и попадают в бэкап
- Мониторинг: доступность URL, коды 5xx из логов, срок сертификата, очередь пула

ХОРОШО

- ARR reverse proxy: один вход 443, Server Farm с health-check по backend'ам
- Application Initialization: прогрев после recycle, пользователи не ждут старта
- Регулярный appcmd add backup + выгрузка логов в централизованный сбор
- Второй узел IIS за балансировщиком, деплой обоих одним скриптом (IaC)



Чек-лист самопроверки

☐ Роль IIS разворачивается скриптом — новый сервер в той же конфигурации можно поднять за 15 минут?

☐ Пулы приложений: idle 0, recycle ночью, лимит памяти задан — или всё осталось на дефолтах?

☐ Первый запрос после ночи отвечает сразу, или пользователи каждое утро ждут прогрева w3wp?

☐ Сертификаты продлеваются автоматически и попадают в биндинг без ручных действий инженера?

☐ TLS 1.0/1.1 отключены, HSTS включён, внешний SSL-тест проходит на класс A?

☐ Логи IIS пишутся не на системный диск, ротация настроена, поле Time-Taken включено?

☐ Наружу отвечает только нужное: Default Web Site остановлен, лишних биндингов и портов нет?

☐ Публикация 1С живёт в отдельном пуле, и его recycling не рвёт сеансы пользователей?

☐ Есть свежий бэкап конфигурации (appcmd add backup) и отработанный план отката?

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).

- Разворачиваем IIS под ключ: роль, пулы, TLS, публикация 1С и ASP.NET — по скрипту, с документацией заказчику
- Переносим существующие сайты и публикации на новый Windows Server без простоя в рабочие часы
- Настраиваем ARR reverse proxy: единый вход 443 для 1С, OWA и порталов с балансировкой и health-check
- Автоматизируем сертификаты: AD CS для внутренних имён, win-acme Let's Encrypt для внешних
- Ставим веб-контур на мониторинг: доступность, 5xx, очереди пулов, сроки сертификатов — с алертами

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** Web Server (IIS) role, Application Pools configuration reference (learn.microsoft.com — IIS 10.0)
- 02** Using the URL Rewrite Module (learn.microsoft.com — 2.1)
- 03** Application Request Routing: Reverse Proxy and Server Farms (iis.net — 3.0)
- 04** IIS 10.0 Version 1709 HSTS Support, <hsts> configuration reference (learn.microsoft.com — 1709+)
- 05** Protocols in TLS/SSL (Schannel SSP) — TLS 1.3 в WS2022+ (learn.microsoft.com — 2022+)
- 06** win-acme: automatic renewal via Task Scheduler (win-acme.com — 2.2.x)
- 07** Публикация информационной базы на веб-сервере (webinst) (its.1c.ru — 8.3)
- 08** Наш шаблон деплоя IIS: PowerShell, пулы, ACL, логи (itfresh.ru — 2026)

