Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

DNS-зоны и записи Windows Server через PowerShell

Модуль DnsServer: стандарт зон, массовые правки, scavenging и перенос на новые DC

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

В сети до 50 PM DNS правят руками в dnsmgmt.msc: A-записи «на пять минут», CNAME на списанные серверы, разнобой TTL, aging выключен. За два-три года зона превращается в свалку — 1С и почта резолвятся в мёртвые адреса, миграция сервера растягивается на дни, каждая правка требует ручного обхода всех DC. Мы описываем зону кодом на модуле DnsServer: правки идемпотентны и обратимы.

Почему это важно бизнесу

- Мёртвая A-запись на списанный сервер — это «1С не запускается» у всего офиса, а причину ищут в 1С, а не в DNS.
- Правка на одном DC из двух даёт плавающий сбой: у половины сотрудников работает, у половины нет.
- Разнобой TTL превращает переезд сервера в сутки ожидания вместо 15 минут переключения.
- Свалка из тысяч записей списанных ноутбуков ломает reverse-зону и разбор инцидентов.
- Правки кодом с логом и откатом снимают зависимость от одного «того самого админа».

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

168 ч

NoRefresh и Refresh по умолчанию: запись остаётся живой ещё ~14 суток после отключения ПК

Set-DnsServerScavenging, дефолт

0

заводской ScavengingInterval — уборка выключена, включаем явно 7.00:00:00

Set-DnsServerScavenging

2500

SocketPoolSize по умолчанию, диапазон 0-10000 — рандомизация исходящих портов

Set-DnsServer, SocketPoolSize

100%

CacheLockingPercent: кэш не перезаписывается до истечения TTL, оставляем как есть

Set-DnsServerCache

5/сек

RRL ResponsesPerSec по умолчанию (LeakRate 3, WindowInSec 5) — для внешних DNS

Set-DnsServerResponseRateLimiting

100k QPS

поток, на котором analytic-лог даёт ~5% деградации; до 50k QPS влияния не видно

DNS Logging and Diagnostics

РЕАЛИЗАЦИЯ 1 ИЗ 3

Базовая линия зон и перенос DNS на новые контроллеры

Что настраиваем

Все DC с ролью DNS: прямые и reverse-зоны, forwarders, conditional forwarders, root hints

Как мы это делаем

1. Снимаем инвентарь: Get-DnsServerZone, Get-DnsServerForwarder, Get-DnsServerRootHint с каждого DC через -ComputerName, сводим в CSV и сравниваем DC между собой.
2. Фиксируем эталон: Export-DnsServerZone принимает только имя файла и кладёт его в %SystemRoot%\System32\dns — забираем оттуда в репозиторий как точку отката.
3. Ставим роль DNS на новые DC: AD-integrated зоны (-ReplicationScope Domain) приезжают репликацией AD, файловые primary поднимаем импортом зонного файла.
4. Сверяем построчно: (Get-DnsServerResourceRecord -ZoneName ... -ComputerName dcNN).Count на старом и новом DC должен совпасть до записи.
5. Переключаем DHCP option 006 на новые адреса, держим 72 часа наблюдения и только потом выводим старые DC из домена.

РЕЗУЛЬТАТ

Переезд DNS проходит без окна недоступности: клиенты переключаются по обновлению аренды DHCP, а не по команде «перезагрузите всё». Откат — возврат прежних адресов в option 006 и импорт эталонного зонного файла, обе операции занимают минуты.

КЛЮЧЕВОЙ НЮАНС

Совпадения имён зон мало: сверяем ZoneType, ReplicationScope, DynamicUpdate и точное число записей. AD-integrated зона реплицируется сама, а forwarders и root hints — настройки сервера, они не едут никуда.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Массовые правки записей из CSV без разрушения зоны

Что настраиваем

Прямая корпоративная зона, пакеты по 50-500 записей A/CNAME/MX/TXT/PTR, один управляющий хост с RSAT

Как мы это делаем

1. Источник истины — CSV вида Name,Type,Value,TTL; скрипт сначала гоняет проверку на дубли и коллизии с уже существующими записями зоны.
2. Создание — Add-DnsServerResourceRecordA/CName/MX с явным -TimeToLive; для TXT отдельного командлета нет, идём через Add-DnsServerResourceRecord -Txt.
3. Изменение — только пара Clone плюс Set-DnsServerResourceRecord -OldInputObject/-NewInputObject: правка на месте, без удаления и пересоздания.
4. Прогон в два прохода: весь пакет с -WhatIf в лог на согласование, затем боевой запуск с -PassThru и записью результата в CSV-отчёт.
5. Удаление — Remove-DnsServerResourceRecord с обязательным -RRType и явным -RecordData: без RecordData уйдут все записи этого типа с таким именем.

РЕЗУЛЬТАТ

Пакет из 300 записей выкатывается за минуты и полностью описан в git: видно, кто, когда и что менял. Ошибочный пакет откатывается обратным CSV, а не поиском по памяти админа.

КЛЮЧЕВОЙ НЮАНС

Set-DnsServerResourceRecord не меняет Name и Type — смена имени или типа только через пересоздание. В -OldInputObject нужен объект из Get- того же прогона: собранный руками «похожий» даст ошибку.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Гигиена зоны: aging, scavenging и корректный DDNS от DHCP

Что настраиваем

AD-integrated зоны с DynamicUpdate Secure и DHCP-серверы, регистрирующие записи за клиентов

Как мы это делаем

1. Включаем уборку на сервере: Set-DnsServerScavenging -ScavengingState $true -ScavengingInterval 7.00:00:00, NoRefresh и Refresh оставляем по 168 ч.
2. Отдельно включаем старение зоны: Set-DnsServerZoneAging -Name <zone> -Aging $true — без этого серверная настройка не чистит ничего.
3. DHCP обновляет DNS под выделенной непривилегированной доменной учёткой, а группу DnsUpdateProxy держим пустой.
4. Включаем Name Protection на scope DHCP: DHCID закрывает захват чужого имени при регистрации клиента.
5. Первые два цикла уборки идут под наблюдением — кандидатов снимаем через Get-DnsServerResourceRecord с фильтром по TimeStamp.

РЕЗУЛЬТАТ

Зона держит реальный состав парка: мёртвые записи уезжают за 14-21 сутки, reverse-зона снова годится для разбора инцидентов, а не отдаёт имена давно списанных ноутбуков. Поиск «чей это IP» перестаёт быть гаданием.

КЛЮЧЕВОЙ НЮАНС

Aging бьёт только по записям с ненулевым TimeStamp — статические A/CNAME серверов он не тронет. Учётку для DDNS в DnsUpdateProxy не добавляем: её записи создадутся без ACL и станут перехватываемыми.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Scavenging включили только на сервере**
  Set-DnsServerScavenging без Set-DnsServerZoneAging не чистит зону: старение включается отдельно на каждой зоне.

- ✕ **Запись правят удалением и созданием**
  Между Remove и Add клиенты ловят NXDOMAIN. Правим на месте: Clone плюс Set-DnsServerResourceRecord с -OldInputObject.

- ✕ **Разнобой TTL перед переездом**
  TTL в 4 часа держит старый IP полдня, а без -TimeToLive запись берёт TTL из SOA зоны. За сутки до миграции ставим 300 с.

- ✕ **Правку внесли на одном DC**
  В AD-integrated зоне это вылечит репликация, в файловой primary — нет. Проверяем ZoneType и IsDsIntegrated до правки.

- ✕ **Учётка DHCP в группе DnsUpdateProxy**
  Записи любого члена этой группы создаются без защиты и перехватываются по имени. Группу держим пустой, DDNS — по выделенной учётке.

- ✕ **Забытые conditional forwarders**
  С зонами они не едут: на новом DC переносим руками через Add-DnsServerConditionalForwarderZone с -MasterServers.

- ✕ **Reverse-зоны нет вовсе**
  Без in-addr.arpa ломается разбор логов и часть почтовых проверок. Заводим Add-DnsServerPrimaryZone -NetworkId 10.0.0.0/24 -ReplicationScope Domain.

- ✕ **Analytic-лог включили и забыли**
  На потоке около 100k QPS он стоит ~5% производительности и быстро съедает диск. Включаем адресно и с лимитом размера файла.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Все зоны AD-integrated, DynamicUpdate = Secure, реплика на уровне домена
- Инвентарь зон и записей выгружается скриптом и хранится в CSV и git
- Reverse-зоны заведены под каждую используемую подсеть
- Export-DnsServerZone делается перед любой массовой правкой

НОРМАЛЬНО

- Aging включён и на сервере, и на каждой динамической зоне
- Массовые правки только из CSV: прогон -WhatIf, боевой запуск -PassThru
- DHCP пишет в DNS выделенной учёткой, Name Protection на scope включён
- Единый стандарт TTL: 3600 с для статики, 300 с перед переездами

ХОРОШО

- Зоны и репликация проверяются dcdiag /test:DNS /DnsAll по расписанию
- Мониторинг Get-DnsServerStatistics и Test-DnsServer с алертом в Telegram
- GlobalQueryBlockList (wpad, isatap) и RRL на внешних DNS включены
- DNS-политики: client subnet и zone scope для split-brain и фильтрации

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Знаем ли мы точное число зон и записей на каждом DC и совпадает ли оно между контроллерами?
- [ ] Включено ли старение и на сервере (ScavengingInterval), и на каждой динамической зоне (Aging)?
- [ ] Есть ли свежий Export-DnsServerZone как точка отката перед массовыми изменениями?
- [ ] Все ли зоны AD-integrated и стоит ли на них DynamicUpdate = Secure?
- [ ] Заведены ли reverse-зоны под все рабочие подсети и живут ли в них актуальные PTR?
- [ ] Обновляет ли DHCP записи под выделенной учёткой и включён ли Name Protection?
- [ ] Перенесены ли на новые DC forwarders, conditional forwarders и root hints?
- [ ] Приведён ли TTL сервисных записей к стандарту и снижается ли он перед переездом?
- [ ] Настроен ли внешний мониторинг резолвинга ключевых имён (1С, почта, шлюз)?
- [ ] Знает ли второй инженер, где лежат скрипты и CSV с описанием зоны?

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 DNS всех контроллеров домена: зоны, записи, forwarders, репликация — отчёт в CSV
- Наводим порядок: aging и scavenging, единый TTL, reverse-зоны, чистка мёртвых записей
- Скрипты массовых правок из CSV с прогоном -WhatIf, отчётом и точкой отката
- Миграция зон и роли DNS на новые контроллеры без окна недоступности
- Мониторинг резолвинга и статистики DNS с оповещением до жалоб пользователей

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 DnsServer Module — справочник командлетов PowerShell (learn.microsoft.com — WS2025)

02 DNS aging and scavenging in Windows Server (learn.microsoft.com — 2025)

03 Manage DNS resource records using DNS server (learn.microsoft.com — 2025)

04 Set-DnsServerResponseRateLimiting (RRL) (learn.microsoft.com — WS2025)

05 Dynamic DNS Update in Windows and Windows Server (learn.microsoft.com — 2025)

06 Enable DNS Logging and Diagnostics in Windows Server (learn.microsoft.com — 2025)

07 DNS Policies Overview: client subnet и zone scopes (learn.microsoft.com — WS2016+)

08 Шаблон ITfresh: dns-zone-baseline.ps1 и CSV-пакеты правок (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.