



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

DHCP на Windows Server: установка и управление парком областей

Роль, области, резервации, политики, failover,
DNS-интеграция, аудит и обслуживание базы

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

Пока адресация живёт на роутере, IP-план держится в чьей-то голове: адреса пересекаются со статикой, принтер и касса меняют IP, гостевой Wi-Fi выдает рабочий пул, в DNS висят записи списанных машин. Падает единственный сервер — сотрудник не получает адрес, не входит в домен и не работает в 1С. Мы переводим адресацию в управляемую роль с failover, политиками и аудитом.

Почему это важно бизнесу

- Простой из-за адресного конфликта — это остановленная касса, печать и обмен с 1С; час простоя дороже второго DHCP-узла.
- Отказ единственного сервера бьёт не сразу, а по мере истечения аренд — авария растянута и плохо диагностируется.
- Мусор в DNS от старых аренд ломает доступ по имени: рабочее место «не видит» шару, принтер и сервер приложений.
- Без аудита и резервных копий восстановление резерваций и опций — это ручной обход офиса и дни работы инженера.
- Чужой DHCP из принесённого роутера раздаёт неверный шлюз и DNS, а авторизация в AD его не остановит — нужен контроль портов.

Ключевые параметры реализации

1 час

MCLT по умолчанию: столько партнёр продлевает аренду при обрыве связи

дока Add-DhcpServerv4Failover (WS2025)

50/50

LoadBalancePercent по умолчанию; в офисе оставляем 50/50, оба узла активны

дока Add-DhcpServerv4Failover (WS2025)

5%

ReservePercent на standby-узле по умолчанию; для растущих пулов поднимаем до 10-20%

дока Add-DhcpServerv4Failover (WS2025)

60 мин

StateSwitchInterval, который задаём мы: он же включает AutoStateTransition

наш стандарт + дока Add-DhcpServerv4Failover

TCP 647

Порт failover; правила Microsoft-Windows-DHCP-Failover-TCP-In/Out ставит роль

дока DHCP failover in Windows Server

85%

Порог PercentInUse из Get-DhcpServerv4ScopeStatistics для алерта

наш стандарт мониторинга



Управление областями, опциями и политиками из кода

Что настраиваем

Все области площадки на паре DHCP-узлов Windows Server 2019/2022/2025; конфигурация как код в PowerShell-репозитории

Как мы это делаем

- 1 Install-WindowsFeature DHCP -IncludeManagementTools, затем Add-DhcpServerSecurityGroup и Restart-Service dhcpserver — без рестарта группы DHCP не активны.
- 2 Add-DhcpServerInDC и контроль Get-DhcpServerInDC: без авторизации служба не выдаёт аренды и пишет событие 1046 в системный журнал.
- 3 Каждый VLAN — свой scope: Add-DhcpServerv4Scope -State Inactive, Add-DhcpServerv4ExclusionRange на статику, затем Set-DhcpServerv4Scope -State Active.
- 4 Опции слоями через Set-DhcpServerv4OptionValue: 006/015 на сервере, 003 и 066/067 на области, точно — политикой; специфичный уровень перекрывает общий.
- 5 Add-DhcpServerv4Policy -Condition Or -MacAddress EQ,00155D* плюс Add-DhcpServerv4PolicyIPRange; МФУ и кассы — Add-DhcpServerv4Reservation -ClientId.

РЕЗУЛЬТАТ

Область перестаёт быть «настроенной руками»: конфигурация воспроизводится скриптом на любом узле за минуты, новый VLAN добавляется правкой одного файла, а телефон или тонкий клиент получает верный набор опций без визита инженера.

КЛЮЧЕВОЙ НЮАНС

Политики области оцениваются раньше серверных, внутри уровня — по возрастанию ProcessingOrder; класс создаём заранее Add-DhcpServerv4Class, иначе условие молча не работает.



Отказоустойчивость: failover вместо кластера

Что настраиваем

Два узла DHCP (failover требует WS2016+), все производственные области в одном отношении failover

Как мы это делаем

- 1 Add-DhcpServerv4Failover -PartnerServer -ScopelId -SharedSecret -Force: общий секрет включает message digest, отношение создаётся сразу на обоих узлах.
- 2 Офис — Load Balance 50/50; филиал — Hot Standby, где -ServerRole Standby задаёт роль локального узла, а -ReservePercent 10-20 вместо дефолтных 5.
- 3 MaxClientLeadTime 1 ч оставляем, но задаём -StateSwitchInterval 60 мин: параметр сам включает AutoStateTransition, иначе узел висит в COMMUNICATION INTERRUPTED.
- 4 Проверяем TCP 647 (правила Microsoft-Windows-DHCP-Failover-TCP-In/Out) и время: расхождение больше минуты останавливает настройку критической ошибкой.
- 5 После ручных правок области гоним Invoke-DhcpServerv4FailoverReplication -Force с узла-эталона: репликация перетирает настройки партнёра.

РЕЗУЛЬТАТ

Падение узла перестаёт быть аварией: партнёр продолжает выдавать и продлевать аренды, а после возврата сервера состояние сходится автоматически. Плановые перезагрузки и обновления уезжают в рабочее время, без ночного окна.

КЛЮЧЕВОЙ НЮАНС

Failover синхронизирует аренды и настройки областей, но не серверные опции, классы и политики уровня сервера — их выравниваем отдельным скриптом.



DNS-интеграция, аудит и обслуживание базы dhcp.mdb

Что настраиваем

Уровень сервера и каждой области: динамические обновления DNS, журналы аудита, резервные копии и перенос роли

Как мы это делаем

- 1 Set-DhcpServerv4DnsSetting -DynamicUpdates Always
-DeleteDnsRROnLeaseExpiry \$true -UpdateDnsRRForOlderClients \$true
-NameProtection \$true на клиентских областях.
- 2 Set-DhcpServerDnsCredential с одной выделенной учёткой на обоих узлах: с разными учётками партнёр не перепишет запись, созданную первым сервером.
- 3 Set-DhcpServerSetting -ConflictDetectionAttempts 2 (допустимо 0–5, по умолчанию 0) — ловим адреса забытой статики до выдачи клиенту.
- 4 Аудит: Set-DhcpServerAuditLog -Enable \$true, свой -Path и -MaxMBFileSize на все файлы; ниже MinMBDiskSpace 20 МБ журнал молча встаёт.
- 5 База: Set-DhcpServerDatabase -BackupInterval 30 -CleanupInterval 120 плюс еженедельный Export-DhcpServer -Leases в хранилище вне узла.

РЕЗУЛЬТАТ

Записи в DNS живут ровно столько, сколько аренда, а мусор от списанных машин не копится. При переносе роли области, резервации и аренды поднимаются из XML одним прогоном Import-DhcpServer -File -BackupPath -Leases.

КЛЮЧЕВОЙ НЮАНС

Экспорт снимает области, резервации и опции, но failover-отношение не переносится: на новом узле создаём его заново, сняв старое у партнёра.



Подводные камни

✗ Роль DHCP на контроллере домена

Без учётки Set-DhcpServerDnsCredential безопасные обновления DNS с DC не работают, а партнёр не перепишет чужую запись. Выносим роль на отдельный узел...

✗ Область активирована без исключений

Диапазон под статику закрываем Add-DhcpServerv4ExclusionRange до перевода области в Active — иначе шлюз, МФУ и коммутатор получают адрес из пула.

✗ Сервер не авторизован в AD

После установки роли забывают Add-DhcpServerInDC: служба стартует, но аренды не выдаёт. Проверяем Get-DhcpServerInDC и событие 1046 в системном журнале...

✗ AutoStateTransition не включён

По умолчанию \$false: при обрыве связи узел висит в COMMUNICATION INTERRUPTED и не берёт весь пул. Задаём -StateSwitchInterval 60 минут.

✗ Один /16 вместо области на VLAN

В общем пуле бесполезны порог заполнения и политики, а диагностика — перебор. Делаем область на VLAN и два ip helper-address, на оба узла DHCP.

✗ Опция 006 указывает на публичный DNS

Клиент перестаёт резолвить внутренние имена и SRV-записи домена. В 006 — только внутренние DNS, форвардеры настраиваем на самом DNS-сервере.

✗ Журналы и база растут без присмотра

Каталог %windir%\System32\dhcp пухнет, а ниже MinMBDiskSpace аудит останавливается. Задаём MaxMBFileSize, DiskCheckInterval и следим за местом.

✗ Бэкап только средствами гипервизора

Снапшот ВМ не даёт вернуть одну область или набор резерваций. Держим Export-DhcpServer -Leases по расписанию и проверяем импорт на тестовом узле.

Как правильно

МИНИМУМ

- Роль вне DC, авторизация Add-DhcpServerInDC, проверка Get-DhcpServerInDC
- Область на каждый VLAN, статика закрыта ExclusionRange до активации
- Резервации на МФУ, кассы, ТСД и сетевое оборудование вместо статики
- Еженедельный Export-DhcpServer -Leases в хранилище вне самого сервера

НОРМАЛЬНО

- Второй узел и failover Load Balance 50/50 с -SharedSecret
- StateSwitchInterval 60 минут — он же включает AutoStateTransition
- DNS: Always, удаление A и PTR по истечении аренды, общая учётка
- Алерт на PercentageInUse 85% и на смену состояния failover

ХОРОШО

- Конфигурация областей, опций и резерваций как код в git
- Политики с PolicyIPRange и ActivatePolicies \$true на сервере
- NameProtection и ConflictDetectionAttempts 2 на клиентских областях
- Ежеквартальный тест Import-DhcpServer -BackupPath на стенде



Чек-лист самопроверки

☐ Роль вынесена с контроллера домена, и Get-DhcpServerInDC показывает оба ваших узла?

☐ Для каждого VLAN есть область, а диапазон статики закрыт ExclusionRange до активации?

☐ Настроен failover, и вы знаете его режим, MCLT и StateSwitchInterval без консоли?

☐ TCP 647 открыт в обе стороны, а время на узлах расходится меньше чем на минуту?

☐ DHCP удаляет A и PTR при истечении аренды, а учётка обновлений DNS одна на оба узла?

☐ Есть алерт на PercentageInUse 85% и на смену состояния failover-отношения?

☐ Аудит включён, задан MaxMBFileSize, и на томе есть запас сверх MinMBDiskSpace 20 МБ?

☐ Копии базы уезжают вне сервера, а Import-DhcpServer хоть раз проверялся на стенде?

☐ Все критичные устройства — МФУ, кассы, ТСД, точки Wi-Fi — на резервациях, а не на статике?

☐ Конфигурация областей и опций описана скриптом, а не только кликами в dhcpgmt.msc?

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).

- Аудит адресации: карта VLAN, областей, резерваций и конфликтов с забытой статикой
- Перевод DHCP с роутера или одиночного сервера на пару узлов Windows Server с failover
- Политики DHCP под IP-телефонию, тонкие клиенты и гостевой Wi-Fi с отдельными пулами
- Интеграция с AD DNS: обновления, выделенная учётка, чистка мусорных записей
- Мониторинг PercentageInUse и состояния failover, бэкап базы и тест 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** DHCP failover in Windows Server — режимы, MCLT, TCP 647 (learn.microsoft.com — 2025)
- 02** Deploy DHCP Using Windows PowerShell — установка и авторизация (learn.microsoft.com — 2025)
- 03** Add-DhcpServerv4Failover — MCLT, LoadBalance, ReservePercent (learn.microsoft.com — WS2025)
- 04** Add-DhcpServerv4Policy и Add-DhcpServerv4PolicyIPRange (learn.microsoft.com — WS2025)
- 05** Set-DhcpServerv4DnsSetting / Set-DhcpServerDnsCredential (learn.microsoft.com — WS2025)
- 06** Set-DhcpServerAuditLog, Set-DhcpServerDatabase, Import-DhcpServer (learn.microsoft.com — WS2025)
- 07** Set-DhcpServerSetting — ConflictDetectionAttempts (0-5) (learn.microsoft.com — WS2025)
- 08** Шаблон ITfresh: dhcp-baseline.ps1 и чек-лист приёмки (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.

