



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

DHCP failover Windows Server: аренды — не вся конфигурация

Как мы реплицируем резервации, опции и фильтры между узлами failover-пары

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

DHCP failover между двумя WS2025: аренды синхронизируются по протоколу failover поверх TCP 647, а резервация принтера с первого сервера на втором не появилась — при переключении принтер получил случайный IP. Причина: протоколом идут binding update по арендам, а конфигурация scope (резервации, опции, политики, исключения) переносится только по команде Replicate Scope / Invoke-D...

Почему это важно бизнесу

- Резервация — не аренда: без ручной репликации после правки партнёр выдаёт клиенту адрес из общего пула, ломая привязки firewall и правил NAT по...
- При переходе в PARTNER DOWN клиенты, чей scope не реплицирован, теряют закреплённый адрес — падают проброски портов и ACL, завязанные на IP.
- Фильтры MAC allow/deny и server-политики не входят в scope-репликацию — расхождение остаётся незамеченным до инцидента с доступом.
- Ручная репликация без регламента — человеческий фактор: инженер забыл нажать Replicate, и второй сервер месяцами живёт по старой конфигурации.
- Простой критичного устройства по IP (принтер, касса, сканер) — это остановка процесса на время диагностики, а не мелкое неудобство.

Ключевые параметры реализации

1 час

MCLT по умолчанию — временная аренда, которую партнёр выдаёт при потере связи (ноль недопустим)

DHCP failover, раздел «Hot standby mode»

5%

ReservePercent по умолчанию в hot standby — доля пула активного сервера под новые аренды stand...

DHCP failover, раздел «Hot standby mode»

50:50

LoadBalancePercent по умолчанию в load balance — хеш MAC по RFC 3074 делит запросы поровну

DHCP failover, раздел «Load balance mode»

TCP 647

порт протокола failover: правила Microsoft-Windows-DHCP-Failover-TCP-In/Out канал binding upd...

DHCP failover, раздел «Windows Firewall»

31

максимум failover-отношений на один DHCP-сервер (партнёров, не score) — переиспользуем отношен...

DHCP Failover Relationships

60 с

расхождение времени свыше минуты: мастер настройки падает с критической ошибкой, в работе пише...

DHCP failover, раздел «Time synchronization»



Репликация scope через Invoke-DhcpServerv4FailoverReplication

Что настраиваем

Failover-пара WS2025 в load balance, 6 scope с резервациями периферии (принтеры, МФУ, кассы)

Как мы это делаем

- 1 После правки резервации на активном сервере сразу запускаем `Invoke-DhcpServerv4FailoverReplication -ComputerName dhcp1 -ScopeId 10.0.10.0 -Force`
- 2 Проверяем вывод команды — в нём перечислены ID всех реплицированных scope; пустой вывод или ошибка = расхождение осталось
- 3 Для массовых правок реплицируем на уровне отношения: `-Name dhcp1-dhcp2 -Force`, чтобы не забыть отдельный scope; без `-Name` и `-ScopeId` идёт server-репликация всех fai...
- 4 Правило: иницилируем репликацию ТОЛЬКО с сервера с более новыми настройками (и со старшей версии ОС) — `Replicate` перезаписывает конфигурацию партнёра
- 5 Еженедельно сверяем конфигурацию скриптом: `Compare-Object (Get-DhcpServerv4Scope -ComputerName dhcp1) (Get-DhcpServerv4Scope -ComputerName dhcp2) -Property ScopeId,...`

РЕЗУЛЬТАТ

Резервации, опции и политики синхронны в течение минуты после изменения, а не обнаруживаются постфактум на инциденте; при PARTNER DOWN партнёр выдаёт тот же IP, что и активный сервер.

КЛЮЧЕВОЙ НЮАНС

`Replicate` не запускается по расписанию сам — это ручная или скриптовая операция, в отличие от аренд, которые едут `binding update`'ами по протоколу failover непрерывно.



Синхронизация server-level настроек, которые Replicate не берёт

Что настраиваем

Тот же стенд — allow/deny фильтры MAC-адресов и server-политики на обоих узлах failover

Как мы это делаем

- 1 Фиксируем: MAC-фильтры и server-level политики НЕ входят в scope-репликацию — синхронизируем их отдельным скриптом
- 2 Переносим allow-лист: `Get-DhcpServerv4Filter -ComputerName dhcp1 -List Allow | Add-DhcpServerv4Filter -ComputerName dhcp2 -List Allow -Force`
- 3 Полный слепок: `Export-DhcpServer -ComputerName dhcp1 -File C:\exports\dhcp.xml`, затем `Import-DhcpServer -ComputerName dhcp2 -File C:\exports\dhcp.xml -BackupPath C:...`
- 4 SharedSecret отношения на кластерных нодах реплицируем вручную с активной ноды через `Set-DhcpServerv4Failover`
- 5 Ставим запланированную задачу на активном узле: `Invoke-DhcpServerv4FailoverReplication -Name <relationship> -Force` раз в сутки как страховка от забытого Replicate

РЕЗУЛЬТАТ

Фильтры доступа и политики не расходятся между узлами; при аварии партнёр подхватывает и защиту по MAC, а не только IP-пул.

КЛЮЧЕВОЙ НЮАНС

Replicate — это scope-уровень (резервации, опции, политики, исключения). Заданное на уровне сервера (MAC-фильтры, определения опций и классов, DNS credentials) синхронизируем отдельно.



Мониторинг состояния failover через event log и счётчики

Что настраиваем

Оба узла failover-пары, каналы DHCP-Server/Admin и /Operational, агент Zabbix

Как мы это делаем

- 1 Собираем из Microsoft-Windows-DHCP Server Events/Admin события смены состояния (OpCode FailoverStateChange, пример Event ID 20252) — Level Error при выходе из NORMA...
- 2 Отдельно берём Event ID 20253 (OpCode TimeOutOfSync, Level Error): в описании указано расхождение в секундах — чиним NTP до срыва настройки
- 3 Ловим CommDown/CommUp (OpCode Admin-канала) — интервал между ними и есть окно, в котором конфигурация партнёров может разойтись
- 4 В канале Operational снимаем AddFailoverScope/RemoveFailoverScope/ChangeFailoverConfig — фиксируем факт правки MCLT, режима, процентов
- 5 В Zabbix кладём счётчики DHCP Server: Number of transitions into COMMUNICATION INTERRUPTED state и Number of transitions into PARTNER DOWN state — рост говорит о не...

РЕЗУЛЬТАТ

Видим момент расхождения конфигурации партнёров задолго до жалобы пользователя на IP принтера.

КЛЮЧЕВОЙ НЮАНС

Событие смены состояния failover не значит «реплицировано»: это разные подсистемы — протокол шлёт binding update по арендам, конфигурацию двигает только Replicate.



Подводные камни

✗ **Путают binding update с репликацией scope**

Протокол failover непрерывно шлёт по TCP 647 только состояние аренд; резервации, опции и политики он не трогает — их двигает только явный Replicate.

✗ **Забывают повторный Replicate после правки**

Создание отношения переносит конфигурацию один раз; каждое следующее изменение резервации требует нового Invoke-DhcpServerv4FailoverReplication.

✗ **Иницируют репликацию не с того сервера**

Replicate перезаписывает настройки партнёра версией сервера-инициатора; при разных версиях ОС репликацию запускают со старшей — только там узнаются н...

✗ **Не синхронизируют server-level фильтры**

Allow/deny листы MAC и server-политики не входят в scope-репликацию — переносим их Get-DhcpServerv4Filter | Add-DhcpServerv4Filter или Import-DhcpSer...

✗ **Указывают ноду, а не имя кластера**

Партнёром для кластерного DHCP указываем имя или IP кластера: при переезде роли на другую ноду сервер уходит в COMMUNICATION INTERRUPTED.

✗ **Игнорируют рассинхронизацию времени**

Расхождение свыше одной минуты останавливает мастер настройки критической ошибкой, а в работе даёт Event 20253 — держим NTP на партнёрах в норме.

✗ **DNS dynamic update под разными учётками**

Оба партнёра должны обновлять DNS одними credentials: владельцем записи становится первый сервер, второй её не перезапишет — помогает DnsUpdateProxy.

✗ **Ждут failover для IPv6-областей**

Failover поддерживает только DHCPv4-scope; для stateless DHCPv6 избыточность делаем двумя серверами с идентичной конфигурацией опций.

Как правильно

МИНИМУМ

- Load balance 50:50 или hot standby с ReservePercent 5% — дефолт без ручной подгонки
- Invoke-DhcpServerv4FailoverReplication -Force сразу после правки scope
- Общий SharedSecret и синхронное время (NTP, расхождение < 60 с) на обоих партнёрах

НОРМАЛЬНО

- Регламент: Replicate сразу после правки резервации/опции/политики, чек-лист инженера
- Мониторинг Admin-канала: Event 20252 (FailoverStateChange), 20253 (TimeOutOfSync), C...
- Еженедельная сверка Compare-Object по Get-DhcpServerv4Scope и Get-DhcpServerv4Reserv...
- Синхронизация MAC-фильтров через Get-DhcpServerv4Filter | Add-DhcpServerv4Filter -Fo...

ХОРОШО

- Запланированная задача Invoke-DhcpServerv4FailoverReplication -Name <relationship> -...
- Export-DhcpServer / Import-DhcpServer -BackupPath -ServerConfigOnly как полный слепо...
- Алертинг на счётчики transitions into COMMUNICATION INTERRUPTED / PARTNER DOWN state
- DnsUpdateProху и единые DNS credentials для общего владения записями клиентов

Чек-лист самопроверки

☐ Настроен ли failover на имя/IP кластера, а не на отдельную ноду?

☐ Запускается ли Invoke-DhcpServerv4FailoverReplication после каждой правки резервации/опции/политики?

☐ Синхронизированы ли server-level allow/deny фильтры и политики отдельным скриптом?

☐ Расходится ли время (NTP) между партнёрами менее чем на 60 секунд?

☐ Настроен ли сбор Event 20252/20253 и CommDown/CommUp в канале DHCP-Server/Admin?

☐ Используется ли единый SharedSecret, вручную разнесённый по всем нодам кластера?

☐ Проверено ли, что оба сервера обновляют DNS одними credentials (DnsUpdateProxy)?

☐ Есть ли регламент, с какого сервера инициировать Replicate при расхождении?

☐ Когда проводилась последняя сверка Compare-Object по Get-DhcpServerv4Scope между партнёрами?

☐ Учтён ли лимит 31 failover-отношения на сервер при планировании новых партнёров?

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 DHCP failover между площадками и настраиваем регламент Replicate под ключ
- Пишем скрипт-синхронизатор server-level MAC-фильтров и политик между партнёрами
- Подключаем мониторинг каналов DHCP-Server/Admin и /Operational и счётчиков failover в общий Zabbix
- Проводим аудит текущей failover-пары: находим резервации и опции, разошедшиеся между узлами
- Настраиваем NTP, SharedSecret и правила Microsoft-Windows-DHCP-Failover-TCP-In/Out для устойчивого канала failover

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, ReservePercent, TCP 647, си... (learn.microsoft.com — 2025)
- 02** Replicate DHCP failover in Windows Server (Server / Relationship / Scope r... (learn.microsoft.com — 2025)
- 03** DHCP failover events in Windows Server (каналы Admin/Operational, Event 20... (learn.microsoft.com — 2025)
- 04** DHCP Failover Relationships (лимит 31 отношения на сервер) (learn.microsoft.com — 2025)
- 05** Invoke-DhcpServerv4FailoverReplication, Set-DhcpServerv4Failover (модуль D... (learn.microsoft.com — WS2025)
- 06** Export-DhcpServer / Import-DhcpServer (-BackupPath, -ServerConfigOnly, -Le... (learn.microsoft.com — WS2025)
- 07** Get-DhcpServerv4Filter / Add-DhcpServerv4Filter (списки Allow/Deny) (learn.microsoft.com — WS2025)
- 08** наш регламент репликации конфигурации failover-пар (наш стандарт — 2026)

