Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Миграция Active Directory на новые контроллеры домена

Swing-миграция с WS2012 R2/2016 на WS2022/2025 без окна простоя: наша методика

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

У заказчика домен на WS2012 R2 или 2016: железо Gen8/Gen9 без запчастей, SYSVOL местами ещё на FRS, схема не расширялась годами. Каталог надо перевезти на WS2022/2025 так, чтобы 40-50 рабочих мест, 1С, RDS и файловые шары не заметили переключения. In-place upgrade не делаем: поднимаем новые DC рядом, переносим FSMO и DNS, старые гасим через Uninstall-ADDSDomainController.

Почему это важно бизнесу

- WS2016 теряет поддержку 12.01.2027, WS2012 R2 вне её с 10.10.2023 — домен остаётся без патчей LSASS, Kerberos и LDAP.
- Падение единственного живого DC на старом железе останавливает вход в 1С, RDS и файловые шары всего офиса.
- In-place upgrade тащит наверх мусор схемы, битые GPO и навсегда оставляет базу NTDS в 8k-формате страниц.
- Без корректного понижения старые DC остаются в метаданных: KCC вечно долбится в мёртвый сервер, логи в ошибках.
- База 32k pages, LDAP sealing по умолчанию и TLS 1.3 для LDAPS есть только у чистых установок WS2025.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

2016

Минимальный DFL и FFL домена и леса для промоушна контроллера на Windows Server 2025

learn.microsoft.com / AD DS functional levels

2008

Минимальный DFL для ввода DC на WS2019/2022 плюс обязательный DFSR вместо FRS

learn.microsoft.com / upgrade domain controllers

180 дней

Tombstone lifetime по умолчанию: DC вне репликации дольше — источник lingering objects

learn.microsoft.com / lingering objects

15 с

Уведомление об изменениях внутри сайта; между сайтами интервал по умолчанию 180 минут

learn.microsoft.com / determining the interval

0→1→2→3

Состояния dfsrmig при переводе SYSVOL с FRS на DFSR; переход в состояние 3 необратим

learn.microsoft.com / migrate SYSVOL to DFSR

5

FSMO-ролей переносим одной командой Move-ADDirectoryServerOperationMasterRole 0,1,2,3,4

learn.microsoft.com / Move-ADDirectoryServer…Role

РЕАЛИЗАЦИЯ 1 ИЗ 3

Swing-миграция WS2012 R2 → WS2022 в одном сайте

Что настраиваем

Бухгалтерская компания, 45 рабочих мест, 2 DC на HP Gen8, один AD-сайт, сервер 1С и файловая шара внутри домена

Как мы это делаем

1. День 1: repadmin /replsummary и /showrepl * /csv, dcdiag /v /c /e, dfsrmig /getmigrationstate. Стартуем только при нулевых ошибках репликации.
2. День 2: две VM WS2022, Install-WindowsFeature AD-Domain-Services, промоушн Install-ADDSDomainController с NTDS, логами и SYSVOL на томе D:.
3. День 3: adprep отработал автоматически при промоушне; проверяем objectVersion схемы (88 у WS2019/2022) и её репликацию по всем DC.
4. День 4: Move-ADDirectoryServerOperationMasterRole -OperationMasterRole 0,1,2,3,4, контроль netdom query fsmo, сутки наблюдения нагрузки.
5. День 5: DHCP option 6 на новые DC, правка статических DNS на серверах, Uninstall-ADDSDomainController на старых строго по одному.

РЕЗУЛЬТАТ

Переключение прошло в рабочие часы, ни одной заявки от пользователей. Домен на WS2022, NTDS вынесена на отдельный том, отклик LDAP-запросов 1С упал вдвое после ухода с дисков Gen8. Старые серверы остались member-серверами на две недели как точка отката.

КЛЮЧЕВОЙ НЮАНС

Промоушн сам запускает adprep, но требует связи со Schema Master, Infrastructure Master и RID Master. Доступность держателей ролей проверяем до старта — иначе установка падает на prerequisite check.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Домен с SYSVOL на FRS: сначала DFSR, только потом новые DC

Что настраиваем

Производство, две площадки, 70 рабочих мест, домен развёрнут в 2008 году, SYSVOL так и остался на FRS, DFL 2008 R2

Как мы это делаем

1. dfsrmig /getglobalstate на PDC показал состояние Start. WS2019 и новее в домене на FRS не промоутятся — миграцию SYSVOL делаем первой.
2. Проходим состояния по одному: /setglobalstate 1, ждём /getmigrationstate по всем DC, затем 2, снова проверка, и только потом 3.
3. После Eliminated ставим два WS2022 DC в центре и один на второй площадке: уровня 2008 R2 для ввода WS2022 достаточно, поднимать заранее не нужно.
4. Второй сайт заводим отдельно: site link 15 минут вместо дефолтных 180 и change notification на канале между площадками.
5. Понижаем старые DC по одному, чистим DNS SRV-записи, контролируем nltest /dclist, и только теперь поднимаем DFL/FFL до 2016.

РЕЗУЛЬТАТ

SYSVOL переехал на DFSR без потери GPO, домен вышел на FFL 2016 — максимум до появления уровня WS2025. Обе площадки сходятся за минуты вместо трёх часов: изменения GPO приезжают в тот же день, а не на следующий.

КЛЮЧЕВОЙ НЮАНС

dfsrmig /setglobalstate работает только через PDC Emulator и падает, если он недоступен. Переход в состояние 3 (Eliminated) необратим, поэтому держим бэкап системного состояния двух DC перед каждым шагом.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Двухступенчатый переезд домена на Windows Server 2025

Что настраиваем

Медклиника, 30 рабочих мест, домен на WS2012 R2 с FFL/DFL 2012 R2, задача — сразу на WS2025 и новую платформу виртуализации

Как мы это делаем

1. WS2025 не промоутится при уровне 2012 R2: нужны DFL и FFL 2016, поэтому первым слоем вводим промежуточные DC на WS2022.
2. Понижаем контроллеры 2012 R2, затем Set-ADDomainMode/Set-ADForestMode в Windows2016Domain и Windows2016Forest, проверяем dcdiag.
3. Вводим два WS2025 DC чистой установкой: база сразу 32k-capable, но работает в режиме 8k-симуляции, схема уходит на objectVersion 91.
4. Переносим FSMO, понижаем WS2022, поднимаем DFL и FFL до Windows Server 2025 (DomainLevel/ForestLevel 10).
5. Database 32k pages включаем отдельным шагом: он необратим и обесценивает все 8k-бэкапы, поэтому сначала свежая копия и проверка ПО.

РЕЗУЛЬТАТ

Клиника получила домен целиком на WS2025 без единого окна простоя: новые DC по умолчанию требуют sealing после SASL bind, channel binding в режиме When supported, LDAPS умеет TLS 1.3. Промежуточный слой WS2022 прожил три недели и снят штатным понижением.

КЛЮЧЕВОЙ НЮАНС

In-place upgrade оставляет базу NTDS в 8k-формате навсегда — 32k-страницы получают только DC чистой установки WS2025. Поэтому мы не апгрейдим DC поверх, а вводим новые и понижаем старые.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Понижение DC до переноса FSMO**
  Уезжает PDC Emulator — рушится иерархия времени, Kerberos и смена паролей. Переносим все пять ролей и ждём сутки.

- ✕ **Выключение DC вместо demote**
  В AD остаются метаданные, KCC бесконечно строит связи к мёртвому серверу. Чистим ntdsutil metadata cleanup или удалением объекта в ADUC.

- ✕ **Старт при ошибках репликации**
  Lingering objects и ошибка 8614 переедут на новые DC и умножатся. Сначала repadmin /removelingeringobjects в /advisory_mode.

- ✕ **Игнор миграции SYSVOL с FRS**
  WS2019 и новее не промоутятся, пока dfsrmig не доведён до Eliminated. WS2016 — последняя версия с поддержкой FRS.

- ✕ **Старые DC в DHCP option 6**
  После выключения старых DC клиенты перестают резолвить SRV-записи домена. Меняем option 6 и статические DNS заранее.

- ✕ **Раннее повышение уровня домена**
  Уровень 2016 отрежет ввод DC на 2012 R2, а понижение возможно не всегда. Поднимаем только после ухода всех старых DC.

- ✕ **ForceRemoval как штатный путь**
  -ForceRemoval теряет нереплицированные изменения и требует ручного metadata cleanup. Применяем, только когда DC физически мёртв.

- ✕ **Снятие роли AD DS без demote**
  Удалять AD-Domain-Services средствами DISM или Server Manager на живом DC нельзя. Сначала Uninstall-ADDSDomainController.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Два новых DC на разных хостах, оба глобальные каталоги, оба с ролью DNS
- Полный бэкап системного состояния всех контроллеров перед первым шагом
- repadmin /replsummary и dcdiag /v /c без ошибок до начала миграции
- Пароль DSRM записан в парольный менеджер, а не в блокнот админа

НОРМАЛЬНО

- NTDS, логи и SYSVOL на отдельном томе, а не на системном диске
- SYSVOL доведён до DFSR: dfsrmig /getmigrationstate = Eliminated
- 24-48 часов наблюдения после переноса FSMO до понижения старых DC
- DHCP option 6 и статические DNS переведены до отключения старых DC

ХОРОШО

- Отдельные AD-сайты, site link 15 минут и change notification на канале
- AD Recycle Bin включён, настроены аудит входов и Protected Users
- Мониторинг Get-ADReplicationFailure по расписанию в Zabbix с алертом
- Старые DC хранятся выключенными 14 дней как точка отката

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Срез: Get-ADForest, Get-ADDomain, Get-ADDomainController -Filter *, netdom query fsmo
- [ ] repadmin /showrepl * /csv и /replsummary — ноль ошибок и ни одной паузы длиннее 180 дней
- [ ] dfsrmig /getglobalstate = Eliminated; иначе сначала FRS→DFSR по состояниям 1, 2 и 3
- [ ] Проверить связь со Schema Master, Infrastructure Master и RID Master до промоушна
- [ ] Install-ADDSDomainController с -DatabasePath, -LogPath и -SysvolPath на отдельном томе
- [ ] После промоушна dcdiag /v /c /e и repadmin /replsummary на всех DC без failures
- [ ] Move-ADDirectoryServerOperationMasterRole -OperationMasterRole 0,1,2,3,4, затем netdom
- [ ] Перевести DHCP option 6, форвардеры DNS и статические записи на адреса новых DC
- [ ] Uninstall-ADDSDomainController по одному DC, после каждого — nltest /dclist и dcdiag
- [ ] DFL/FFL поднимать, только когда Get-ADDomainController показывает лишь новые ОС

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 домена перед миграцией: репликация, lingering objects, состояние SYSVOL, схема и GPO
- Разворачиваем новые DC на WS2022/2025 и ведём swing-миграцию без окна простоя
- Переносим FSMO, DNS и DHCP-опции, корректно понижаем старые DC с проверкой метаданных
- Чиним унаследованное: FRS→DFSR через dfsrmig, lingering objects, orphaned metadata
- Ставим мониторинг репликации и бэкап системного состояния DC, передаём runbook админу

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 Upgrade domain controllers to a newer version of Windows Server (learn.microsoft.com — 2026)

02 Active Directory Domain Services functional levels (learn.microsoft.com — 2025)

03 Windows Server Active Directory schema updates (learn.microsoft.com — 2025)

04 Migrate SYSVOL replication from FRS to DFS Replication (learn.microsoft.com — 2025)

05 Demote domain controllers and domains (Level 200) (learn.microsoft.com — 2025)

06 Clean up AD DS domain controller server metadata (learn.microsoft.com — 2025)

07 Database 32k pages for Active Directory on Windows Server (learn.microsoft.com — 2025)

08 Runbook swing-миграции AD — внутренний шаблон ITfresh (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.