Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

# Active Directory с нуля: домен для офиса на 30 мест

Разбираем нашу методологию: два DC, функциональные уровни, AGDLP, GPO-baseline и LAPS

Июль 2026

**itfresh.ru · ИТ-аутсорсинг для юридических лиц**

О ЧЁМ ЭТОТ РАЗБОР

# Суть проблемы

Компания выросла до 30 человек, а учётки живут на самих ПК: увольнение — обход всех рабочих мест, права на папки и 1С раздаются вручную, парольную политику применить негде, аудита нет. Мы закрываем это доменом AD DS: единый каталог, GPO, делегирование и восстановление объектов. Без домена каждый доступ — ручная работа, а отказ единственного сервера парализует офис.

## Почему это важно бизнесу

- Увольнение закрывается одной командой Disable-ADAccount вместо обхода 30 ПК — доступ к шарам и 1С пропадает в ту же минуту.
- Права на файловый ресурс и базы 1С выдаются через группы, а не «на честном слове» — разграничение бухгалтерии и юристов проверяемо.
- Второй контроллер стоит одной VM (4 vCPU / 8 ГБ), но снимает риск простоя всего офиса при отказе диска или узла гипервизора.
- Аудит входов и изменений в каталоге даёт доказуемую картину для проверок и разбора инцидентов, а не догадки по логам рабочих станций.
- Единая парольная политика и LAPS убирают вечные «admin/123» на локальных админах рабочих станций.

ЧТО МЫ ЗАКЛАДЫВАЕМ

# Ключевые параметры реализации

## Win2025

Уровень леса и домена 10: поднимаем, когда все DC на WS2025; в смешанном лесу остаёмся на 2016

раздел AD DS Functional Levels

## 2 × DC

Минимум два контроллера на разных узлах гипервизора: один DC — точка отказа даже на 15 PM

наш стандарт

## 0,4 ГБ/1000

Норматив размера NTDS.dit на 1000 пользователей; том под базу и логи отделяем от системного

раздел AD DS Capacity Planning

## 180 дней

tombstoneLifetime по умолчанию; msDS-deletedObjectLifetime пуст и наследует это же окно

спецификация MS-ADTS

## 7 + 7 дней

No-refresh и refresh интервалы DNS scavenging по умолчанию: включаем на всех AD-зонах

раздел DNS Aging and Scavenging

## 14 симв.

Длина пароля Windows LAPS по умолчанию (диапазон 8–64), PasswordAgeDays по умолчанию — 30 дней

раздел Windows LAPS policy settings

РЕАЛИЗАЦИЯ 1 ИЗ 3

# Лес и два контроллера домена

## Что настраиваем

Чистый лес corp.<домен>.ru на двух VM Windows Server (4 vCPU / 8 ГБ / 80+40 ГБ) на разных узлах гипервизора

## Как мы это делаем

1. Готовим DC01: Rename-Computer, статический IP, Set-TimeZone, все накопительные обновления до повышения; предпочитаемый DNS — собственный статический адрес
2. Install-WindowsFeature AD-Domain-Services,DNS -IncludeManagementTools, затем Install-ADDSForest с -DomainNetbiosName (до 15 символов) и -SafeModeAdministratorPasswo…
3. NTDS и логи выносим на отдельный том через -DatabasePath/-LogPath, SYSVOL через -SysvolPath; считаем 0,4 ГБ .dit на 1000 учёток, свободного места держим 20%
4. DC02: Install-ADDSDomainController -SiteName Default-First-Site-Name -InstallDns -Credential; GC включается по умолчанию, проверка repadmin /replsummary и dcdiag /e…
5. Кросс-DNS: на DC01 предпочитаемый — адрес DC02, альтернативный 127.0.0.1; на DC02 зеркально. Форвардеры — на резолверы, стабильно доступные из РФ

**РЕЗУЛЬТАТ**

Домен переживает потерю любого узла гипервизора: вход, DNS, SYSVOL и GPO обслуживает второй контроллер. Накопительные обновления ставим по очереди, без окна простоя, по квартальному регламенту.

**КЛЮЧЕВОЙ НЮАНС**

Повышать до DC надо на полностью обновлённой системе: уровень Win2025 (10) поднимается, только когда все DC на WS2025, а сам WS2025-контроллер вводится в домен с уровнем не ниже WS2016.

РЕАЛИЗАЦИЯ 2 ИЗ 3

# OU, группы безопасности и учётные записи

## Что настраиваем

Структура каталога и права: OU под сотрудников, рабочие станции, серверы, сервисные и привилегированные учётки

## Как мы это делаем

1. Ни одного объекта в CN=Users: на контейнер нельзя слинковать GPO. OU заводим через New-ADOrganizationalUnit и проверяем, что защита от удаления не снята
2. Модель AGDLP: GG_<отдел> с людьми входит в DL_<ресурс>_<право>, и уже DL-группа стоит в ACL шары. Пользователя в ACL не вешаем никогда
3. Импорт 30 учёток из CSV через New-ADUser: UPN, Department, Title, -ChangePasswordAtLogon $true, начальные пароли — в парольном хранилище
4. Две break-glass-учётки, отдельные админ-аккаунты инженеров и группа SG_JoinComputers с делегированным через dsacls правом создавать computer-объекты
5. Enable-ADOptionalFeature 'Recycle Bin Feature' -Scope ForestOrConfigurationSet включаем сразу: операция необратимая и должна опережать первые удаления

**РЕЗУЛЬТАТ**

Права выдаются добавлением в одну группу, доступ отзывается одной командой. Аудит «кто к чему имеет доступ» сводится к списку членов DL-групп, а случайно удалённая OU или учётка возвращается из корзины без восстановления из бэкапа.

**КЛЮЧЕВОЙ НЮАНС**

AD Recycle Bin требует уровень леса не ниже WS2008 R2 и включается один раз навсегда; объект восстановим в течение msDS-deletedObjectLifetime — атрибут по умолчанию пуст и равен tombstoneLifetime, 180 дней.

РЕАЛИЗАЦИЯ 3 ИЗ 3

# GPO-baseline, DNS/DHCP и эксплуатация

## Что настраиваем

Групповые политики на корень домена и OU рабочих станций и серверов, DHCP-failover, Windows LAPS и мониторинг каталога

## Как мы это делаем

1. Default Domain Policy не трогаем: отдельную GPO Password Policy линкуем на корень домена выше неё по приоритету, требования к админам — через PSO (msDS-PasswordSett...
2. Baseline на OU: SMBv1 удалён, «Digitally sign communications (always)», LLMNR off политикой Turn off multicast name resolution, автозапуск USB off, аудит Logon и Di...
3. DNS: обратные зоны на все подсети, Set-DnsServerScavenging -ScavengingState $true -ApplyOnAllZones с NoRefreshInterval и RefreshInterval по 7 суток, форвардеры вмес...
4. DHCP на двух серверах: Add-DhcpServerv4Failover -ServerRole Standby (режим Hot Standby), MCLT по умолчанию 1 час, ReservePercent поднимаем с дефолтных 5% до 20%
5. Windows LAPS на OU Workstations: Update-LapsADSchema, Set-LapsADComputerSelfPermission на OU, BackupDirectory — Active Directory, PasswordLength 20, PasswordAgeDays...

**РЕЗУЛЬТАТ**

Новая рабочая станция въезжает в домен и получает диски, принтеры и hardening без ручной настройки. DHCP переживает перезагрузку любого сервера, DNS не зарастает мусорными записями, локальные админы ротируются автоматически.

**КЛЮЧЕВОЙ НЮАНС**

Каждую GPO обкатываем на тестовой OU и снимаем Invoke-GPUpdate/gpresult /h до привязки к боевой: политику проще не применить, чем потом разбирать, почему у бухгалтерии пропал сетевой диск.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

# Подводные камни

- ✕ **Домен в зоне .local**
  Суффикс .local зарезервирован под mDNS (RFC 6762) и ломает Bonjour-устройства и часть ПО. Берём поддомен внешнего имени: corp.company.ru.

- ✕ **Имя домена = публичный домен**
  Совпадение с company.ru даёт split-brain DNS: внутри резолвится DC, снаружи — сайт и MX. Разруливать приходится ручными записями в зоне.

- ✕ **Единственный контроллер домена**
  Отказ диска — офис без входа, шар и печати. Второй DC на другом узле гипервизора это одна VM, а не второй бюджет проекта.

- ✕ **Пользователи в контейнере CN=Users**
  На контейнер нельзя слинковать GPO, приходится городить фильтры по группам. OU-структуру делаем до заведения учёток, а не после.

- ✕ **FSMO-роли не задокументированы**
  Когда PDC Emulator недоступен, никто не знает, где были роли. Фиксируем вывод netdom query fsmo в паспорт домена и сверяем ежеквартально.

- ✕ **DHCP только на одном сервере**
  Сервер ушёл на обновление — половина офиса без адресов. Ставим failover в режиме Hot Standby либо выносим DHCP на пару роутеров.

- ✕ **Время не привязано к PDC Emulator**
  Расхождение больше допуска Kerberos в 5 минут ломает вход в домен. Внешний NTP настраиваем только на держателе PDC, остальные берут время от него.

- ✕ **Бэкап DC ни разу не проверен**
  System State без теста восстановления — это не бэкап. Раз в квартал поднимаем DC из копии в изолированной сети и смотрим dcdiag.

УРОВНИ РЕАЛИЗАЦИИ

# Как правильно

## МИНИМУМ

- Два DC на разных узлах гипервизора, роль DNS на обоих, кросс-ссылки DNS
- OU-структура вместо CN=Users, группы по AGDLP, AD Recycle Bin включён
- Отдельные GPO: парольная политика, baseline станций, диски и принтеры
- System State Backup обоих DC на хранилище за пределами домена

## НОРМАЛЬНО

- DHCP failover Hot Standby, DNS scavenging 7/7, обратные зоны на все подсети
- Windows LAPS на рабочих станциях, отдельные админ-учётки, две break-glass
- Делегирование ввода в домен отдельной группе вместо Domain Admins
- Квартальный регламент обновлений: DC по очереди, repadmin после каждого

## ХОРОШО

- Мониторинг репликации, тома NTDS и журнала Directory Service в Zabbix
- Тестовое восстановление DC из бэкапа в изолированной сети раз в квартал
- Protected Users и запрет интерактивного входа сервисным учётным записям
- ADCS для LDAPS, контроль LDAP signing и channel binding на DC

ПРОВЕРЬТЕ У СЕБЯ

# Чек-лист самопроверки

- [ ] Имя домена — поддомен внешнего (corp.company.ru), NetBIOS до 15 символов латиницей?
- [ ] Контроллеров домена минимум два и они разнесены по разным узлам гипервизора?
- [ ] repadmin /replsummary и dcdiag /e /v проходят без ошибок на обоих контроллерах?
- [ ] AD Recycle Bin включён, а System State Backup обоих DC уезжает за пределы домена?
- [ ] Есть две break-glass-учётки, пароли лежат в сейфе или парольном хранилище?
- [ ] Все пользователи и компьютеры разложены по OU, а не остались в CN=Users?
- [ ] Права на шары и 1С выданы через Domain Local-группы, а не персонально?
- [ ] Внешний NTP настроен на держателе PDC Emulator, расхождение времени меньше 5 минут?
- [ ] DHCP переживёт перезагрузку одного сервера — есть failover Hot Standby или пара роутеров?
- [ ] Локальные администраторы рабочих станций управляются LAPS с ротацией пароля?

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).

- Проектируем домен: имя, адресный план, OU, группы AGDLP, схема имён серверов и учёток
- Разворачиваем два DC на Windows Server, DNS, DHCP-failover и базовые GPO под ключ
- Мигрируем учётки из рабочих групп, вводим ПК в домен и переносим профили без потери данных
- Настраиваем LAPS, бэкап DC, мониторинг репликации и обучаем администратора заказчика
- Берём домен на аутсорс: квартальные обновления, аудит прав, проверка 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

ДОКУМЕНТАЦИЯ И НАШ СТЕК

# Техническая база


01 Install-ADDSForest / Install-ADDSDomainController (ADDSDeployment) (learn.microsoft.com — 2025)

02 Active Directory Domain Services Functional Levels (learn.microsoft.com — 2025)

03 Capacity planning for Active Directory Domain Services (learn.microsoft.com — 2025)

04 DNS Aging and Scavenging in Windows Server (learn.microsoft.com — 2025)

05 Add-DhcpServerv4Failover / DHCP failover in Windows Server (learn.microsoft.com — 2025)

06 Configure policy settings for Windows LAPS (learn.microsoft.com — 2025)

07 MS-ADTS: Tombstone Lifetime and Deleted-Object Lifetime (learn.microsoft.com — 2025)

08 Шаблон ITfresh: паспорт домена и регламент обслуживания DC (itfresh.ru — 2026)


Основано на официальной документации продуктов и нашей практике внедрения.