Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Active Directory для офиса до 50 ПК: нужна или нет

Наши критерии, честный расчёт лицензий Windows Server и CAL, рабочая схема двух DC

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

К нам приходят с фразой «без домена работать неправильно». Мы не продаём AD как символ статуса: считаем, сколько ручных операций съедает рабочая группа, какие приложения требуют Kerberos и централизованных прав, и во что обойдётся лицензионный минимум Windows Server Standard (16 core-лицензий, 8 на процессор) плюс CAL на каждого. Дальше выдаём вердикт: домен, NAS или гибрид.

Почему это важно бизнесу

- Увольнение без домена — 3-4 часа обхода NAS, принтеров, RDP и 1С; в домене это блокировка учётки и 10 минут работы.
- Единственный контроллер домена — единая точка отказа: при его падении не входит никто и никуда, включая 1С по Windows-аутентификации.
- Лицензии считаются до старта: минимум 16 core-лицензий на сервер плюс Windows Server CAL на каждого пользователя или устройство.
- Терминал требует отдельных RDS CAL сверх обычных: без них сессии живут только 120 дней grace-периода и перестают открываться.
- Для 10-15 ПК в одном офисе домен часто дороже пользы: деньги эффективнее вложить в NAS и проверенные резервные копии.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

16 core

Минимум core-лицензий на сервер Windows Server Standard, и 8 на каждый процессор

Microsoft Licensing, Windows Server 2025

2 OSE

Столько ОС даёт Standard на хост; следующая пара ВМ — ещё полный комплект core

Microsoft Licensing, Windows Server 2025

120 дней

Grace-период RDS: после него без RDS CAL сессии не открываются

learn.microsoft.com, RDS CAL

180 дней

tombstoneLifetime в лесах от WS2003 SP1; если атрибут пуст — работает 60 дней

MS-ADTS, Tombstone Lifetime

2 vCPU/4 ГБ

Наш стартовый профиль виртуального DC: 4 ГБ RAM, 60 ГБ диск NTFS, не ReFS

наш стандарт + MS hardware requirements

2 DC

Минимум контроллеров на домен, обязательно на разных физических хостах

наш стандарт

РЕАЛИЗАЦИЯ 1 ИЗ 3

Рабочая группа на 12 ПК: почему мы не стали разворачивать домен

Что настраиваем

Юрфирма, 12 ПК, один офис, файловая 1С Бухгалтерия, без удалённых сотрудников

Как мы это делаем

1. Считаем ручные операции: заведение, смена пароля, отзыв доступа. На 12 ПК выходит около 3 часов в месяц — домен не окупается.
2. Ставим NAS с SMB и снапшотами, одинаковые имена шар и локальные группы на всех машинах.
3. Локальные политики: блокировка экрана 10 минут, запрет SMBv1, запрет сохранения паролей в браузере.
4. Резервные копии ежедневно на NAS плюс еженедельная копия на съёмный диск, тест восстановления раз в квартал.
5. Пароли локальных админов — уникальные, в менеджере паролей, ротация раз в полгода.

РЕЗУЛЬТАТ

Клиент не платит ни за Windows Server, ни за 16 core-лицензий, ни за CAL. Администрирование остаётся ручным, но укладывается в 3 часа в месяц. В отчёте фиксируем пороги пересмотра: 20+ ПК, появление RDS, требования к журналу доступа.

КЛЮЧЕВОЙ НЮАНС

Домен не обязателен там, где нет ни удалёнки, ни разграничения прав, ни аудита. Мы записываем пороги пересмотра в отчёт, чтобы через год разговор не начинался с нуля.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Домен с нуля на 30 рабочих мест: наш трёхдневный сценарий

Что настраиваем

Торговая компания, 28-35 рабочих мест, 1С УТ на сервере, RDS для удалённых менеджеров

Как мы это делаем

1. Обследование: перепись ПК и редакций Windows (Home в домен не вводится), инвентарь 1С, СКЗИ и КриптоПро.
2. День 1: Install-WindowsFeature AD-Domain-Services + Install-ADDSForest, NTDS, логи и SYSVOL на NTFS-томе (не ReFS), DSRM-пароль сразу в менеджер паролей.
3. OU по отделам и GPO: парольная политика (дефолт домена — 7 символов, поднимаем), блокировка экрана, LAPS через Update-LapsADSchema.
4. День 2: второй DC — Install-ADDSDomainController на другом физическом хосте, проверка repadmin /replsummary и раскладки 5 ролей FSMO.
5. День 3: включаем корзину AD, System State ежедневно (копия старше tombstoneLifetime бесполезна), гасим DC1 и проверяем вход и 1С.

РЕЗУЛЬТАТ

Увольнение — блокировка учётки и вывод ПК из домена, 10 минут вместо обхода NAS, принтеров, RDP и 1С. Отказ первого DC проверен выключением на живом стенде: вход и 1С работают. Клиент получает схему сети, регламент и пароли в защищённом хранилище.

КЛЮЧЕВОЙ НЮАНС

Отказоустойчивость проверяется выключением, а не верой в репликацию. Пока симуляция отказа DC1 не пройдена, домен считается несданным — акт мы не подписываем.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Entra ID и Intune вместо домена: когда мы выбираем этот путь

Что настраиваем

Сервисная компания, 18 человек, Microsoft 365, ноутбуки в разных городах, локального файлового сервера нет

Как мы это делаем

1. Сверяем матрицу: Entra ID — не замена AD DS, привычных GPO там нет, политики уезжают в Intune.
2. Ищем, что требует Kerberos, LDAP или SMB к локальному серверу. Если такого нет — DC не разворачиваем вовсе.
3. Устройства вводим в Entra join, конфигурации и BitLocker — через Intune, локальный админ — под LAPS.
4. Файлы переносим в SharePoint и OneDrive, NAS оставляем приёмником резервных копий.

РЕЗУЛЬТАТ

Экономим Windows Server, 16 core-лицензий и CAL целиком — вместе с сервером и его обслуживанием. Взамен закладываем зависимость от интернета и переучивание администратора с GPO на Intune: это отдельная строка сметы, а не бонус.

КЛЮЧЕВОЙ НЮАНС

Гибрид с синхронизацией локального AD в Entra ID оправдан от 50+ пользователей или нескольких офисов. На 20 человек это два каталога и две точки отказа вместо одной.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Один контроллер домена**
  Единственный DC — единая точка отказа. Падает его диск — не входит никто: ни в ПК, ни в шары, ни в 1С по доменной аутентификации.
- ✕ **Оба DC на одном гипервизоре**
  Формально два контроллера, фактически один хост. Гибнет хост — гибнут оба, резервирование остаётся только на бумаге.
- ✕ **NTDS и SYSVOL на томе ReFS**
  Документация прямо запрещает держать базу AD, её логи и SYSVOL на томе ReFS. Только NTFS — иначе конфигурация неподдерживаемая.
- ✕ **Бэкап AD старше tombstoneLifetime**
  В лесах от WS2003 SP1 это 180 дней, при пустом атрибуте — 60. Смотрим фактическое значение и держим копию заведомо моложе него.
- ✕ **Плоская структура без OU**
  Все объекты в корне домена — GPO некуда привязать. Избирательные политики потом чинятся на живой работающей системе.
- ✕ **Мёртвые учётные записи**
  Учётка уволенного живёт месяцами. Регламент: блокировка в день ухода, перенос в OU Disabled, удаление через 30 дней.
- ✕ **Дефолтная парольная политика**
  Домен по умолчанию требует всего 7 символов. Длину поднимаем в Default Domain Policy, исключения — через PSO, а не вторым GPO.
- ✕ **Забыли про CAL и RDS CAL**
  Считают только сервер. CAL нужен на каждого пользователя или устройство, терминалу нужен ещё RDS CAL, grace-период всего 120 дней.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Один DC: 2 vCPU, 4 ГБ RAM, 60 ГБ на NTFS, роль DNS на нём же
- OU по отделам, парольная политика и блокировка экрана в GPO
- System State ежедневно, хранение 14 дней, проверка восстановления
- Windows 10/11 Pro на всех ПК: редакция Home в домен не вводится

НОРМАЛЬНО

- Два DC на разных физических хостах, оба — GC и DNS-серверы
- Корзина AD включена, локальные админы под Windows LAPS
- Раскладка 5 ролей FSMO задокументирована, repadmin в чек-листе
- Права — только через группы, доменные админы только именные

ХОРОШО

- Симуляция отказа DC1 при сдаче и раз в год на обслуживании
- Fine-grained password policy (PSO) для админов и сервисных учёток
- Аудит входов и доступа к шарам с выгрузкой в Zabbix или SIEM
- Отдельные админ-учётки и выделенная станция для управления доменом

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Посчитали, сколько часов в месяц уходит на ручное администрирование рабочей группы
- [ ] Проверили редакции Windows на всех ПК: Home требует апгрейда до Pro
- [ ] В смете учтены минимум 16 core-лицензий и Windows Server CAL на каждого
- [ ] Если есть терминал — заложены RDS CAL и активирован сервер лицензирования
- [ ] Второй DC запланирован и стоит на другом физическом хосте
- [ ] NTDS, логи и SYSVOL лежат на NTFS-томе, а не на ReFS
- [ ] System State ежедневно, возраст копии меньше фактического tombstoneLifetime
- [ ] Проверен вход пользователей при выключенном первом контроллере
- [ ] Учётки уволенных блокируются в день ухода и удаляются через 30 дней
- [ ] Пароли DSRM и доменных админов лежат в менеджере паролей, а не в файле

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).

- Считаем экономику: домен, NAS или Entra ID — со сметой лицензий и часов до начала работ
- Разворачиваем два DC, OU и GPO за 2-4 дня, с проверкой КриптоПро, ЭЦП и 1С в домене
- Настраиваем бэкап System State и корзину AD, тестируем именно восстановление
- Сдаём схему сети, регламент увольнения и пароли в защищённом хранилище
- Берём домен на обслуживание: repadmin, мёртвые учётные записи, симуляция отказа DC

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 Active Directory Domain Services (Level 100) (learn.microsoft.com — 2025)

02 Hardware Requirements for Windows Server (learn.microsoft.com — 2025)

03 Windows Server 2025 Licensing Guidance, Per Core/CAL (microsoft.com — 2025)

04 License Remote Desktop Services with CALs (learn.microsoft.com — 2025)

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

06 Set-ADDefaultDomainPasswordPolicy, значения по умолчанию (learn.microsoft.com — 2025)

07 Compare Active Directory to Microsoft Entra ID (learn.microsoft.com — 2025)

08 Наш чек-лист сдачи домена и регламент увольнения (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.