Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Active Directory для офиса до 50 PM: как мы строим домен

Пара DC на Windows Server 2025, GPO-базлайн, Windows LAPS и эксплуатация без простоев

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

У компаний до 50 рабочих мест домен часто держится на единственном стареющем контроллере: пароли локальных админов одинаковые, GPO копились годами, бэкап DC никто не проверял. Любой сбой такого узла останавливает вход, 1С, печать и файловые шары на день и больше. Разбираем нашу схему: отказоустойчивая пара DC на Windows Server 2025, базовая линия безопасности и регламент экспл…

Почему это важно бизнесу

- Отказ единственного DC — простой всего офиса: вход, 1С, почта, файлы; восстановление без проверенного бэкапа занимает дни
- Один общий пароль администратора на всех ПК превращает заражение одной машины в захват всей сети
- Без аудита и корзины AD вопрос «кто удалил пользователя или файл» остаётся без ответа, а ошибки исправляются днями
- Windows Server 2012 R2/2016 без поддержки — незакрываемые уязвимости и несовместимость с новым ПО

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

2×DC

минимум контроллеров в каждом внедрении — отказ одного узла не останавливает вход и GPO

наш стандарт

уровень 10

функциональный уровень леса и домена Windows Server 2025 (ForestLevel/DomainLevel 10); открыва…

по докам AD DS Functional Levels

30 дней

ротация паролей локальных админов в Windows LAPS (PasswordAgeDays), длина 14, сложность 4

по докам Windows LAPS

180 дней

msDS-deletedObjectLifetime — окно восстановления объектов из корзины AD без отката из бэкапа

по докам AD DS

90+30 мин

фоновый цикл применения GPO (90 мин + случайный сдвиг до 30); критичное форсим gpupdate

по докам Group Policy

±5 мин

Maximum tolerance for computer clock synchronization — допуск времени для Kerberos; PDC-эмулят…

по докам Kerberos policy

РЕАЛИЗАЦИЯ 1 ИЗ 3

Развёртывание пары контроллеров на Windows Server 2025

Что настраиваем

Два узла на разных гипервизорах, роли AD DS + DNS + DHCP; охват — весь офис до 50 PM

Как мы это делаем

1. Ставим Windows Server 2025 Standard, Install-ADDSForest с ForestLevel/DomainLevel 10, DNS-зона интегрирована в AD
2. DNS на DC: первым — партнёр, вторым — свой адрес, loopback 127.0.0.1 — только последним; внешние резолверы задаём форвардерами, на клиентах — никаких 8.8.8.8
3. Время: PDC-эмулятор → внешний NTP (w32tm /config /manualpeerlist), остальные машины — по доменной иерархии NT5DS
4. Второй DC через Install-ADDSDomainController; доводим repadmin /replsummary и dcdiag /e /q до нуля ошибок
5. Сразу включаем корзину AD: Enable-ADOptionalFeature 'Recycle Bin Feature' — фича необратимая, и это нормально

РЕЗУЛЬТАТ

Отказ любого одного узла не валит вход, DNS и DHCP; перезагрузка контроллера в рабочее время перестаёт быть событием. Ноль ошибок dcdiag фиксируем как базовое состояние — любое отклонение видно в мониторинге сразу.

КЛЮЧЕВОЙ НЮАНС

Новые леса на Server 2025 создаются с БД, готовой к 32k-страницам, но работают в режиме симуляции 8k. Опциональную фичу «Database 32k pages» включаем только когда все DC леса — на Server 2025 и уровень поднят…

РЕАЛИЗАЦИЯ 2 ИЗ 3

Базовая линия безопасности: Windows LAPS, GPO, Kerberos

Что настраиваем

Домен целиком: OU станций и серверов, отдельные политики и учётки для администрирования

Как мы это делаем

1. Расширяем схему Update-LapsADSchema и включаем Windows LAPS: BackupDirectory=AD, ротация 30 дней, длина 14, сложность 4, сброс после входа (PostAuthenticationAction...
2. Админов домена — в группу Protected Users: запрет NTLM и RC4/DES, запрет делегирования, TGT 4 часа вместо 10
3. NTLM сначала в аудит («Network security: Restrict NTLM: Audit NTLM authentication in this domain»), разбираем Event 8004 на DC, затем точечные исключения и полный з...
4. Пароли по ролям через FGPP (объекты msDS-PasswordSettings): 15+ знаков для сервисных и административных учёток при обычной политике для пользователей
5. После внедрения дважды меняем пароль krbtgt с паузой больше времени жизни TGT — и далее по регламенту

РЕЗУЛЬТАТ

Компрометация одного ПК не даёт горизонтального перемещения по общему локальному паролю; административные билеты короткоживущие и не защищаются устаревшими протоколами; пароль любой машины достаём из AD за секунды командой Get-LapsADPassword.

КЛЮЧЕВОЙ НЮАНС

Windows LAPS встроен в ОС начиная с обновлений апреля 2023 (Win10/11, Server 2019+). Legacy LAPS (AdmPwd) сносим: у них разные атрибуты схемы и политики, друг друга они не видят.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Эксплуатация: репликация, бэкап, восстановление

Что настраиваем

Регламент на обоих DC + файловые сервисы DFS и DHCP Failover

Как мы это делаем

1. Ежедневно по расписанию: repadmin /replsummary и dcdiag /e /q, алерт в Telegram при любом ненулевом fail
2. Бэкап system state обоих DC через wbadmin на отдельный том; откат DC снапшотом гипервизора не используем — это путь к USN rollback
3. Файлы: DFS Namespaces поверх шар + DFS-R со staging-квотой не меньше суммы 32 самых крупных файлов папки; SYSVOL — только DFSR
4. DHCP Failover в режиме Load balance 50/50 (MCLT 1 час) — отказоустойчивость без кластера
5. Удалённые объекты возвращаем Restore-ADObject из корзины — членство в группах и SID сохраняются

РЕЗУЛЬТАТ

Удаление объекта или сбой репликации перестают быть авариями: восстановление пользователя — минута, отказ DHCP пользователи не замечают, состояние домена видно по ежедневному отчёту, а не по звонкам «не могу войти».

КЛЮЧЕВОЙ НЮАНС

Откат DC из снапшота гипервизора — типовая причина USN rollback: контроллер молча выпадает из репликации (Event 2095). Сейфгард VM-Generation ID спасает не во всех сценариях, поэтому только штатное восстановле…

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Один DC на весь домен**
  любой сбой останавливает вход и 1С; второй DC — это лицензия Standard и 4 ГБ RAM, разворачиваем его даже в самом малом офисе
- ✕ **8.8.8.8 в DNS клиентов**
  клиенты перестают находить SRV-записи домена — медленный вход и «домен недоступен»; внешние резолверы задаём только форвардерами на DC
- ✕ **Снапшот вместо бэкапа DC**
  откат снапшота даёт USN rollback и тихий развал репликации (Event 2095); только system state и штатное восстановление
- ✕ **Legacy LAPS вместо Windows LAPS**
  AdmPwd и встроенный LAPS — разные схемы, атрибуты и GPO-шаблоны; держим только Windows LAPS, старый клиент удаляем со всех машин
- ✕ **krbtgt не менялся годами**
  старый пароль krbtgt обесценивает защиту билетов Kerberos; меняем дважды с паузой больше времени жизни TGT (10 часов)
- ✕ **Все правки в Default Domain Policy**
  монолитную DDP тяжело диагностировать и откатывать; в ней оставляем только пароли и Kerberos, остальное — отдельные GPO на OU
- ✕ **Время уплыло на контроллере**
  расхождение больше 5 минут ломает Kerberos-вход; PDC — на внешний NTP, у виртуальных DC отключаем синхронизацию времени с хоста
- ✕ **Старый DC выключили «на живую»**
  остаются метаданные и мёртвые SRV-записи — ошибки репликации и таймауты входа; чистим ntdsutil metadata cleanup и DNS

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Два DC на разных физических хостах, DNS клиентов — только на них
- Корзина AD включена, ежедневный system state бэкап обоих DC
- Windows LAPS на всех ПК и серверах, ротация 30 дней
- Еженедельная проверка dcdiag /e /q и repadmin /replsummary

НОРМАЛЬНО

- GPO-базлайн: блокировка экрана, запрет LM/NTLMv1 и SMBv1, аудит 4624/4625/4740
- Отдельные админ-учётки в Protected Users, работа без прав Domain Admins
- Централизованные обновления (WSUS) и контроль pending reboot по парку
- Мониторинг служб DC и репликации с алертами, а не ручные проверки

ХОРОШО

- Тиринг доступа (Tier 0/1/2), отдельная станция для работы с DC
- NTLM в запрет после аудита 8004, SMB signing обязателен
- DHCP Failover, DFS-N/DFS-R для файлов, регулярный DR-тест восстановления DC
- Функциональный уровень 2025 и план включения 32k-страниц БД

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Контроллеров домена минимум два, и они разнесены по разным физическим хостам?
- [ ] Пароль локального администратора на каждом ПК уникален и ротируется автоматически (Windows LAPS)?
- [ ] Корзина AD включена, и восстановление удалённого пользователя реально проверяли?
- [ ] Бэкап system state обоих DC делается ежедневно, восстановление тестировалось?
- [ ] repadmin /replsummary показывает ноль ошибок репликации прямо сейчас?
- [ ] PDC-эмулятор берёт время с внешнего NTP, а не с гипервизора?
- [ ] NTLMv1 и SMBv1 запрещены политиками, аудит NTLM разобран?
- [ ] Пароль krbtgt менялся за последний год (дважды, с паузой более 10 часов)?
- [ ] У админов отдельные учётки, и они состоят в Protected Users?
- [ ] Для любого ПК можно показать итоговый набор политик (gpresult /h) без конфликтов?

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).

- Разворачиваем домен под ключ: пара DC на Windows Server 2025, DNS/DHCP, GPO-базлайн, Windows LAPS
- Мигрируем домены с Windows Server 2012 R2/2016/2019 на новые контроллеры без простоя пользователей
- Проводим аудит безопасности AD: NTLM, krbtgt, делегирования, права на OU и GPO, устаревшие объекты
- Настраиваем мониторинг контроллеров, репликации и бэкапов с алертами в Telegram
- Берём эксплуатацию на себя: обновления, восстановления, регламентные DR-проверки

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

02 Database 32k pages optional feature (AD DS) (learn.microsoft.com — 2025)

03 Windows LAPS: policy settings и key concepts (learn.microsoft.com — 2025)

04 Active Directory Recycle Bin / deletedObjectLifetime (learn.microsoft.com — 2025)

05 Protected Users security group (learn.microsoft.com — 2025)

06 Windows Time Service (w32tm) configuration (learn.microsoft.com — 2025)

07 DHCP Failover in Windows Server (learn.microsoft.com — 2025)

08 Шаблон ITfresh: GPO-базлайн офиса до 50 PM (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.