Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Администрирование Active Directory в 2026: методология ITfresh

Как мы разворачиваем и защищаем AD DS на Windows Server 2022/2025 в офисах до 50 рабочих мест

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

У клиентов до 50 PM домен AD — единая точка входа во всё: логоны, файловые шары, 1С, печать, VPN. Типовая картина «в наследство от прошлого подрядчика»: один DC, бэкап годами не проверялся, krbtgt не менялся с установки, у эникея — Domain Admin. Отказ такого DC останавливает офис целиком, а компрометация одной рабочей станции отдаёт злоумышленнику весь домен и все данные.

Почему это важно бизнесу

- Отказ единственного DC = стоит весь офис: никто не логинится, 1С и шары недоступны — день простоя бухгалтерии и продаж
- Компрометация Domain Admin отдаёт все базы и документы разом; восстановление захваченного домена — недели работ
- Случайное удаление OU без Recycle Bin и проверенного бэкапа — потеря учёток и прав, восстановление вручную по памяти
- Порядок в AD ускоряет рутину: новый сотрудник получает все доступы добавлением в одну группу, а не за день переписки

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

x2

Минимум контроллеров домена в любом нашем проекте — отказ одного DC не останавливает офис

наш стандарт

32k

Страница ESE-базы NTDS.dit после включения фичи Database 32k pages (нужен FFL 2025) вместо 8k

по докам Windows Server 2025

180 дней

Период двойной ротации пароля krbtgt (скрипт New-KrbtgtKeys.ps1) — обесценивает украденные TGT

наш стандарт

5 мин

Максимальный clock skew Kerberos: дальше логоны падают с KRB_AP_ERR_SKEW, время сверяем по PDC

по докам Kerberos (MS-KILE)

15 с

Задержка уведомления партнёров при внутрисайтовой репликации — от неё считаем пороги алертинга

по докам AD DS

2 ГБ

Размер журнала Security на каждом DC — иначе события 4624/4768 затираются за считанные часы

наш стандарт аудита

РЕАЛИЗАЦИЯ 1 ИЗ 3

Развёртывание домена: два DC на Windows Server 2025

Что настраиваем

Типовой офис 30–50 PM: DC01 + DC02 (виртуальные, на разных хостах), роли AD DS + DNS + DHCP failover

Как мы это делаем

1. Install-ADDSForest с -DomainMode/-ForestMode Win2025 (уровень 10), база NTDS на отдельном диске; второй узел — Install-ADDSDomainController, все FSMO на DC01
2. DNS: зоны AD-integrated, reverse-зоны на все подсети, scavenging no-refresh/refresh 7+7 дней, forwarders 77.88.8.8 и 1.1.1.1; клиентам в DNS — только контроллеры
3. OU-каркас: Sotrudniki / Workstations / Servers / ServiceAccounts / PrivilegedAccounts; группы по AGDLP (GG_* → DL_* → NTFS), ничего не оставляем в CN=Users
4. GPO-базлайн: пароли от 12 символов, отключение SMBv1/NTLMv1/LLMNR, SMB signing, Windows LAPS в режиме AD, Advanced Audit Policy по подкатегориям
5. Финал: Enable-ADOptionalFeature Recycle Bin, DHCP failover Load Balance 50/50, dcdiag /e /v и repadmin /replsummary — в приёмочный протокол

РЕЗУЛЬТАТ

Домен переживает отказ любого одного сервера: аутентификация, DNS и DHCP продолжают работать со второго DC. Случайно удалённые объекты возвращаются штатным Restore-ADObject за минуты, без восстановления из бэкапа и без простоя пользователей.

КЛЮЧЕВОЙ НЮАНС

FFL 2025 включаем сразу при чистой установке: позже поднять уровень помешает любой забытый старый DC. Database 32k pages — forest-wide optional feature: включается Enable-ADOptionalFeature только при FFL 2025…

РЕАЛИЗАЦИЯ 2 ИЗ 3

Защита привилегий: tier-модель и делегирование

Что настраиваем

Tier 0: контроллеры домена, jump-хост администратора, учётки Domain Admins (максимум две) и сервисные аккаунты

Как мы это делаем

1. Админ-операции только с выделенного jump-хоста без интернета и почты; повседневная работа инженера — под обычной учёткой без прав в AD
2. Все админ-учётки — в группу Protected Users: запрет NTLM и RC4, TGT 4 часа без продления, без делегирования и кэширования учётных данных
3. Делегирование вместо Domain Admin: SG_HelpDesk получает Reset password и unlock только на OU=Sotrudniki через Delegate Control
4. Сервисы переводим на gMSA (на WS2025 — dMSA с привязкой аутентификации к машинной учётке): случайный пароль 240 байт ротируется автоматически, интервал ManagedPassw…
5. krbtgt: двойной сброс New-KrbtgtKeys.ps1 каждые 180 дней с паузой больше времени полной репликации; фиксируем в регламенте

РЕЗУЛЬТАТ

Кража пароля с обычной рабочей станции больше не отдаёт домен: привилегированные сессии живут только на Tier 0, пароли сервисов не знают даже админы, а плановая ротация krbtgt обесценивает ранее добытые тикеты и дампы.

КЛЮЧЕВОЙ НЮАНС

AdminSDHolder (процесс SDProp) каждые 60 минут возвращает ACL защищённых групп к эталону — делегирование, навешанное прямо на Domain Admins, молча откатится. Права выдаём только через OU и отдельные SG-группы.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Эксплуатация: мониторинг, аудит, восстановление

Что настраиваем

Оба DC + бэкап-сервер вне домена; Zabbix 7.0 LTS как единая точка алертинга по всей площадке

Как мы это делаем

1. Zabbix: триггеры на repadmin /replsummary (fails > 0, delta > 60 мин), сервисы NTDS/DNS/KDC/Netlogon, место на диске с NTDS.dit < 20%
2. Аудит через Advanced Audit Policy; алерты на Event ID 4625, 4740, 4728/4732 (изменение админ-групп) и 1102 — очистка журнала у нас всегда инцидент
3. System State backup обоих DC ежесуточно (wbadmin start systemstatebackup) на сервер вне домена + недельная копия средствами Veeam B&R
4. Ежеквартально — тестовое восстановление DC в изолированной сети и прогон PingCastle с разбором каждого пункта риска до закрытия

РЕЗУЛЬТАТ

Сбой репликации или подозрительная активность видны за минуты, а не после жалоб пользователей. Проверенный бэкап-контур закрывает и отказ железа, и шифровальщика: домен поднимается в изолированной сети по отработанному сценарию, а не по статье из интернета в ночь аварии.

КЛЮЧЕВОЙ НЮАНС

DC, простоявший выключенным дольше Tombstone Lifetime (180 дней), в репликацию не возвращается — только metadata cleanup и повторное повышение. Поэтому у каждого DC в мониторинге есть контроль аптайма и доступ…

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

✕ Один контроллер домена

Отказ единственного DC кладёт логоны, DNS и 1С разом. Всегда ставим второй DC (можно ВМ на другом хосте) с полной репликой каталога и DNS.

✕ Объекты в CN=Users и CN=Computers

На контейнеры по умолчанию нельзя привязать GPO. Переносим всё в OU-каркас и перенаправляем новые объекты командами redircmp/redirusr.

✕ Domain Admin у эникейщика

Помощнику хватает делегированного Reset password на конкретной OU. Держим максимум две учётки в Domain Admins, Enterprise Admins — пустая.

✕ DC выключен дольше 180 дней

Tombstone Lifetime истёк — вернуть такой DC в репликацию нельзя, реанимация плодит lingering objects. Только metadata cleanup и переустановка роли.

✕ Внешний DNS первым на клиентах

Клиент не находит SRV-записи _ldap._tcp — логоны и GPO тормозят или падают. На клиентах только DNS контроллеров, форвардеры — на самих DC.

✕ Журнал Security по умолчанию

Стандартные 128 МБ на DC переполняются за часы — расследование слепнет. Ставим 1–2 ГБ и выносим ключевые события в Zabbix/коллектор.

✕ krbtgt не менялся с установки

Старый хеш krbtgt — готовый Golden Ticket при компрометации DC. Двойной сброс раз в 180 дней с паузой на полную репликацию между сбросами.

✕ GPO правят сразу в бою

Ошибка в базлайне разлетается на весь домен за цикл обновления 90 минут. Сначала тестовая OU и Group Policy Modeling, перед каждой правкой — Backup-G…

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Два DC с DNS AD-integrated, все FSMO задокументированы (netdom query fsmo)
- System State backup ежесуточно на узел вне домена + включённая AD Recycle Bin
- Пароли от 12 символов, блокировка после 10 неудач; SMBv1 и NTLMv1 отключены
- Еженедельный прогон repadmin /replsummary и dcdiag /e /v с разбором ошибок

НОРМАЛЬНО

- OU-каркас + модель AGDLP, делегирование хелпдеску вместо Domain Admin
- Windows LAPS на всех станциях и серверах, gMSA для сервисных учёток
- Advanced Audit Policy, журнал Security 2 ГБ, алерты на ключевые Event ID
- Мониторинг репликации, служб NTDS/DNS/KDC и дисков в Zabbix

ХОРОШО

- Tier-модель: jump-хост Tier 0, Protected Users, Credential Guard на станциях
- Ротация krbtgt каждые 180 дней, ежеквартальный PingCastle с закрытием рисков
- Тестовое восстановление DC из бэкапа раз в квартал в изолированной сети
- Новые домены на WS2025: FFL 2025, Database 32k pages, dMSA вместо legacy-сервис-учёт…

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] В домене минимум два DC, и отказ любого из них реально проверялся на практике?
- [ ] Известно, на каком DC какие FSMO-роли, и есть инструкция переноса и аварийного захвата?
- [ ] System State backup делается ежесуточно на узел вне домена, а восстановление тестировалось?
- [ ] AD Recycle Bin включена (Enable-ADOptionalFeature) до первого случайного удаления, а не после?
- [ ] В Domain Admins не больше двух учёток, а Enterprise Admins вне лесных операций пустая?
- [ ] Пароль krbtgt менялся за последние 180 дней двойным сбросом?
- [ ] Локальные админ-пароли станций ротируются через Windows LAPS, а не одинаковые на всём парке?
- [ ] Репликация и службы DC под мониторингом — алерт придёт раньше звонка пользователей?
- [ ] SMBv1, NTLMv1 и LLMNR отключены базлайн-политикой на всех компьютерах домена?
- [ ] Журнал Security увеличен, а события 1102/4728/4740 попадают в алертинг?

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: два DC на Windows Server 2022/2025, DNS/DHCP failover, OU-каркас и GPO-базлайн
- Берём на сопровождение существующие AD: аудит PingCastle, починка репликации, разбор наследия прежних подрядчиков
- Внедряем защиту привилегий: tier-модель, делегирование, Windows LAPS, регламентная ротация krbtgt
- Строим мониторинг и бэкап-контур: Zabbix-алертинг, System State вне домена, квартальные тесты восстановления
- Планово мигрируем домены со старых Windows Server на 2022/2025 без простоя пользователей

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 AD DS Functional Levels (уровень леса/домена 2025) (learn.microsoft.com — WS2025)

02 Enable Database 32k pages optional feature in AD DS (learn.microsoft.com — WS2025)

03 Delegated Managed Service Accounts (dMSA) overview (learn.microsoft.com — WS2025)

04 Windows LAPS: режим хранения в Active Directory (learn.microsoft.com — 2025)

05 Best Practices for Securing Active Directory (learn.microsoft.com — 2025)

06 Advanced Audit Policy Configuration (learn.microsoft.com — 2025)

07 Protected Users Security Group (learn.microsoft.com — 2025)

08 Шаблон ITfresh: OU-каркас и GPO-базлайн малого офиса (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.