Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Tier-модель администрирования AD: как мы её внедряем

Tier 0/1/2, deny-logon GPO, Protected Users, Authentication Policy Silo, PAW и LAPS на 50 PM

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

В домене до 50 РМ администрирование держат на двух-трёх учётках Domain Admins: ими чинят принтер, ставят 1С, правят права на файлах. Любой заражённый ПК, где такая учётка вводилась, становится входом в контроллер домена — а с ним под контролем почта, 1С, бухгалтерия и бэкапы. Мы разделяем администрирование на три уровня, чтобы взлом рабочей станции не давал доступа к каталогу.

Почему это важно бизнесу

- Восстановление домена из бэкапа — это 1-3 дня без 1С, почты, файлов и терминала: зарплата и отгрузки встают целиком.
- Бэкапы, доступные из-под Domain Admins, шифруются вместе с продуктивом — восстанавливаться будет уже не из чего.
- Разделение уровней не стоит ни рубля лицензий: только штатные средства AD и GPO, работы укладываются в 3-5 дней.
- Появляется журнал привилегированного доступа: события 4624/4672 по t0-учёткам ровно с одной админ-машины.
- Каждое действие требует осознанного выбора учётки — меньше случайных правок прав и удалений «не тем аккаунтом».

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

240 мин

у Protected Users жёстко и жизнь TGT, и продление; короче — только Authentication Policy

Protected Users Security Group, learn.microsoft.com

2 × 10 ч

krbtgt сбрасываем дважды: пауза больше максимума жизни TGT (дефолт 10 ч), берём сутки

AD Forest Recovery — Reset the krbtgt password

5 × Deny

пять прав входа запрещаем в каждой Tier-GPO: locally, RDS, network, batch job, service

наш шаблон Tier-GPO

14 → 20

PasswordLength в Windows LAPS: дефолт 14 (диапазон 8-64), наш стандарт 20 при Complexity=4

Configure Policy Settings for Windows LAPS + наш стандарт

DFL 2012R2

минимум для доменных ограничений Protected Users и Authentication Policies; LAPS-шифр. — 2016

AD DS Functional Levels, learn.microsoft.com

0xC000015B

статус в событии 4625: модель отработала — запрещён тип входа, а не «неверный пароль»

наш стандарт мониторинга

РЕАЛИЗАЦИЯ 1 ИЗ 3

OU-каркас, группы и раздельные административные учётки

Что настраиваем

Домен до 50 PM: 1-2 DC, 3-6 серверов, всё дерево AD и учётки команды из 2-4 админов

Как мы это делаем

1. Создаём OU Tier 0 / Tier 1 / Tier 2, внутри — Servers (для Tier 2 — Workstations), Admins, Groups; -ProtectedFromAccidentalDeletion $true оставляем включённым.
2. Глобальные группы GG-T0-Admins / GG-T1-Admins / GG-T2-Admins плюс доменно-локальные DL-T1-LocalAdmins и DL-T2-LocalAdmins — права раздаём только через DL.
3. Заводим ivanov-t0 / -t1 / -t2 в OU своего уровня; повседневный ivanov для почты и браузера не входит ни в одну админ-группу.
4. Локальные админы на узлах — GPP Local Users and Groups с Action=Update и снятой галкой «Delete all member users», чтобы не затирать чужие членства.
5. Выписываем сервисные учётки бэкапа, мониторинга, EDR и гипервизора: агент, который управляет ОС контроллера домена, относим к Tier 0, а не к Tier 1.

РЕЗУЛЬТАТ

Получаем однозначную карту: каждый объект AD лежит ровно в одном уровне, права выдаются только через доменно-локальные группы. Новый сервер или ПК попадает под нужные политики сразу при вводе в домен, а не после ручной донастройки задним числом.

КЛЮЧЕВОЙ НЮАНС

Tier 0 — это не только DC, но и всё, что ими управляет: гипервизор, бэкап, EDR, патч-менеджмент. Список выписываем первым, иначе первый же агент возвращает права обратно наверх.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Deny-logon GPO: замыкаем границы между уровнями

Что настраиваем

Три GPO, слинкованные крест-накрест на OU Tier 0/1/2 и на Domain Controllers

Как мы это делаем

1. GPO T0-Deny-on-T1T2 линкуем на OU Tier 1/Servers и Tier 2/Workstations: deny log on locally / through RDS / as batch job / as service, deny access from network.
2. Проверяем не GUI, а GptTmpl.inf: SeDenyInteractiveLogonRight, SeDenyRemoteInteractiveLogonRight, SeDenyNetworkLogonRight, SeDenyBatch- и SeDenyServiceLogonRight.
3. В запреты кладём SID-ы, а не имена: -512 Domain Admins, -519 Enterprise Admins, -518 Schema Admins, S-1-5-32-551 Backup Operators, S-1-5-32-549 Server Operators.
4. Первые две недели — наблюдение: собираем 4624 (типы входа 2/3/4/5/10) и 4648 по админ-учёткам, вычищаем легитимные входы, затем включаем встречные запреты.
5. Приёмка: secedit /export /areas USER_RIGHTS на узле каждого уровня плюс контрольный вход — ждём отказ и событие 4625 со статусом 0xC000015B.

РЕЗУЛЬТАТ

Учётка любого уровня перестаёт входить на узел чужого уровня — ни интерактивно, ни по RDP, ни по сети, ни как служба. Хеш админа Tier 2, снятый с заражённой рабочей станции, на сервере не даёт ничего: атака упирается в границу уровня, а не в сигнатуры антивируса.

КЛЮЧЕВОЙ НЮАНС

Deny всегда сильнее Allow и снимается только правкой самой политики. Поэтому каждую Tier-GPO мы выгружаем Backup-GPO и держим наготове Restore-GPO — откат занимает минуты.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Закалка Tier 0: Protected Users, силос, krbtgt, PAW

Что настраиваем

Учётки Tier 0, контроллеры домена и одна выделенная админ-машина (PAW или ВМ Hyper-V)

Как мы это делаем

1. New-ADAuthenticationPolicy с -UserTGTLifetimeMins и -UserAllowedToAuthenticateFrom (SDDL), затем New-ADAuthenticationPolicySilo без -Enforce: сутки аудита.
2. Армируем Kerberos: в Default Domain Controllers Policy System\KDC — «KDC support for claims…» = Always provide claims, на PAW — System\Kerberos.
3. Меняем пароль каждой t0-учётки (нужен AES-ключ), потом Add-ADGroupMember Protected Users: TGT жёстко 240 минут, NTLM, RC4/DES и делегирование отключаются.
4. krbtgt: сброс дважды с паузой больше максимума жизни TGT (дефолт 10 ч, берём сутки) и контролем repadmin /showrepl — раз в 6 месяцев и после инцидента.
5. PAW: Windows 11 Enterprise, VBS и Credential Guard (LsaCfgFlags=1, UEFI lock), RunAsPPL=1, WDAC/AppLocker, без почты и браузера, обновления через WSUS.

РЕЗУЛЬТАТ

Даже полностью украденная учётка Tier 0 живёт не дольше 4 часов TGT, не ходит по NTLM, не делегируется и аутентифицируется только с разрешённых машин. Ротация krbtgt закрывает сценарий с долгоживущими поддельными билетами, а PAW убирает саму площадку для кражи.

КЛЮЧЕВОЙ НЮАНС

Силос создаётся в аудите (аналог WhatIf), а политика в ADAC — сразу enforced, нужен флажок «Only audit policy restrictions». Administrator с RID 500 от политик аутентификации освобождён.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

✕ **Deny-политики включили одним махом**
Ночью встают бэкап и мониторинг: их сервисные учётки ловят SeDenyServiceLogonRight. Мы держим две недели аудита 4624/4648 и только потом enforce.

✕ **Всех Domain Admins сразу в Protected Users**
Обходных путей нет: без AES-ключа (пароль давно не менялся) учётка не аутентифицируется. Меняем пароль, тестируем на одной, затем остальные.

✕ **Jump-сервер считают отдельным уровнем**
Хост наследует доверие любой учётки, которую на нём набирали: RDP-шлюз до DC — это Tier 0. Держим его в OU Tier 0 под теми же GPO, что и DC.

✕ **Агент бэкапа или EDR с правами Domain Admins**
Такой агент делает каждый сервер точкой входа в каталог. Разводим: отдельная gMSA для Tier 1 и отдельная для DC, права строго под задачу.

✕ **Запреты прописаны именами групп**
После переименования или в локализованном домене имя не резолвится и правило молча отваливается. В GptTmpl.inf кладём SID: -512, S-1-5-32-551.

✕ **PAW без канала обновлений**
Изолированная машина за полгода набирает дыры. Точечно открываем WSUS и обновления Defender, раз в месяц проверяем фактическую установку патчей.

✕ **LAPS включили, а DFL остался ниже 2016**
При DFL ниже 2016 шифрование не работает: пароль лежит открытым в msLAPS-Password. Расшифровщик по умолчанию — Domain Admins, сужаем Principal.

✕ **Забыли про 4-часовой TGT**
У Protected Users билет не продлевается: через 4 ч не выдаются новые service ticket, длинные RDP-сессии теряют сетевые ресурсы. Задачи — на gMSA.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Две учётки на админа: t0 для DC и t1 для серверов и рабочих станций
- Deny-logon GPO на Domain Admins везде, кроме OU Domain Controllers
- Все учётки Tier 0 — в Protected Users, после смены пароля и теста на одной
- Windows LAPS: BackupDirectory=2, PasswordLength=20, PasswordAgeDays=30

НОРМАЛЬНО

- Полный OU-каркас Tier 0/1/2 и три встречные deny-GPO, заданные SID-ами
- Полу-PAW: BM Windows 11 Enterprise у админа, только AD-инструменты и RDP
- Authentication Policy Silo для Tier 0, первые сутки — в режиме аудита
- Ротация krbtgt раз в 6 месяцев, дважды, с паузой не меньше 10 часов

ХОРОШО

- Физический PAW: Credential Guard с UEFI-lock, RunAsPPL=1, WDAC-политика
- gMSA с PrincipalsAllowedToRetrieveManagedPassword вместо сервисных учёток
- WEF-подписка на 4624/4625/4672/4768 с алертом на статус 0xC000015B
- ADEncryptedPasswordHistorySize=12 при DFL 2016+ и шифровании LAPS

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Есть ли у каждого админа отдельная учётка на каждый уровень и обычная — для почты и браузера?
- [ ] Проверено ли контрольным входом, что Domain Admin не заходит на рабочую станцию пользователя?
- [ ] Запреты входа в GPO заданы SID-ами, а не именами групп, и видны в GptTmpl.inf?
- [ ] Все учётки Tier 0 в Protected Users, и пароль менялся на DC не ниже Windows Server 2008?
- [ ] Известен ли полный список сервисных учёток с правами на DC и переведены ли они на gMSA?
- [ ] Менялся ли пароль krbtgt дважды за последние 6 месяцев с контролем репликации?
- [ ] Есть ли машина, с которой ведутся работы Tier 0, и точно ли на ней нет почты и браузера?
- [ ] Windows LAPS включён с BackupDirectory=2, DFL не ниже 2016 и шифрованием паролей в AD?
- [ ] Собираются ли события 4625 со статусом 0xC000015B и настроен ли по ним алерт?
- [ ] Работают ли бэкап, мониторинг и EDR без прав Domain Admins на Tier 1 и Tier 2?

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 текущей модели: кто, откуда и какой учёткой входит — по событиям 4624/4672 за 30 дней
- Разворачиваем OU-каркас Tier 0/1/2, группы и раздельные админ-учётки без простоя пользователей
- Ставим три встречные deny-logon GPO поэтапно: аудит, затем enforce, с готовым откатом за минуты
- Закаливаем Tier 0: Protected Users, Authentication Policy Silo, ротация krbtgt, Windows LAPS
- Собираем PAW или полу-PAW с Credential Guard, RunAsPPL и WDAC, отдаём регламент эскалации

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 Tier Model for Privileged Access Security in Windows Server (learn.microsoft.com — 2026)

02 Authentication Policies and Authentication Policy Silos (learn.microsoft.com — 2026)

03 Guidance about how to configure protected accounts (learn.microsoft.com — 2025)

04 AD Forest Recovery — Reset the krbtgt password (learn.microsoft.com — 2025)

05 Configure Policy Settings for Windows LAPS (learn.microsoft.com — 2026)

06 Configure Credential Guard (VBS, LsaCfgFlags) (learn.microsoft.com — 2026)

07 Delegated Managed Service Accounts overview (Windows Server 2025) (learn.microsoft.com — 2025)

08 Шаблон ITfresh: Tier-GPO и чек-лист приёмки домена (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.