Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Гибридная идентификация: связываем AD и Entra ID

Entra Connect 2.6.84.0, PHS + Seamless SSO, ms-DS-ConsistencyGuid, дедлайн 30.09.2026

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Компания платит за Microsoft 365, но каталогов у неё два: локальный AD и облачный тенант. Учётки заводят руками дважды, пароли расходятся, уволенный блокируется в домене и продолжает читать почту в облаке. Мы связываем каталоги в один источник истины: AD остаётся мастером, Entra ID получает объекты и хеши паролей через Entra Connect Sync, вход в облако идёт доменным паролем.

Почему это важно бизнесу

- Двойной ручной ввод: каждый новый сотрудник — 20-30 минут админа в двух системах и гарантированное расхождение данных.
- Уволенный блокируется в AD, но читает почту и файлы в облаке, пока учётку не выключат руками в тенанте.
- С 30.09.2026 сборки Entra Connect Sync ниже 2.5.79.0 перестают синхронизировать: тенант молча замирает на старых данных.
- Один пароль вместо двух снимает половину заявок «не могу войти» и убирает бумажки с паролями на мониторах.
- Гибрид — база для Intune, Conditional Access и MFA: без него облачные политики не видят корпоративные ПК.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

2.6.84.0

сборка от 07.07.2026: LocalDB на SQL 2022, MSAL 4.83.3, вход мастера по FIDO2

документация Entra Connect: история версий, 2026

30.09.2026

дедлайн: ниже версии 2.5.79.0 синхронизация останавливается на стороне сервиса

документация Entra Connect: история версий

30 мин

дефолтный цикл и минимум AllowedSyncCycleInterval — чаще синхронизировать не поддерживается

документация Connect Sync: Scheduler

2 мин

канал синхронизации хешей паролей: интервал не настраивается, heartbeat — событие 654

документация Password Hash Sync

PBKDF2 ×100

MD4 расширяется до 64 байт, плюс 10 байт соли, HMAC-SHA256; наружу уходит 32 байта по TLS

документация Password Hash Sync

15 знач.

потолок userCertificate и userSMIMECertificate; превышение размера объекта → LargeObject

документация Entra Connect: ошибки LargeObject

РЕАЛИЗАЦИЯ 1 ИЗ 3

Готовим AD и ставим Entra Connect Sync на выделенную ВМ

Что настраиваем

Домен до 50 PM: 1-2 DC, тенант Microsoft 365 Business Premium, отдельная ВМ Windows Server 2022 вне контроллера домена

Как мы это делаем

1. Публичный UPN-суффикс: Set-ADForest -UPNSuffixes @{Add="company.ru"}, раскатываем на пользователей и верифицируем домен в тенанте — .local подтвердить нельзя.
2. Прогоняем IdFix: дубли proxyAddresses и UPN, недопустимые символы; помним про потолок 15 значений userCertificate и userSMIMECertificate на объект.
3. ВМ: Windows Server 2022 или 2025 с полным GUI (Core не поддерживается), .NET 4.7.2, TLS 1.2; минимум по доке 6 ГБ и 70 ГБ, берём 4 vCPU / 8 ГБ / 100 ГБ с запасом.
4. К контроллерам открываем 53, 88, 135, 389, 445, 3268 и динамический RPC 49152-65535, при LDAPS — 636; наружу только 443, порт 80 — исключительно под CRL.
5. Ставим в режиме Custom: sourceAnchor = ms-DS-ConsistencyGuid, фильтр по OU, учётной записи AD DS даём право записи в этот атрибут.

РЕЗУЛЬТАТ

Каталог уезжает в облако с первого прохода: UPN совпадают с проверенным доменом, sourceAnchor устойчив к переносу объектов между лесами, а сервер синхронизации живёт отдельно от DC — его можно обновлять и перезагружать, не трогая контроллер домена.

КЛЮЧЕВОЙ НЮАНС

sourceAnchor неизменяем: у выгруженного объекта значение уже не переписать. Переключить objectGUID на ms-DS-ConsistencyGuid можно задачей мастера Configure Source Anchor, любой другой атрибут — только переуста…

РЕАЛИЗАЦИЯ 2 ИЗ 3

PHS + Seamless SSO и перевод AZUREADSSOACC на AES-256

Что настраиваем

Доменные ПК: вход в Microsoft 365 без повторного пароля, компьютерная учётка SSO и ротация ключа Kerberos

Как мы это делаем

1. На шаге User sign-in ставим Password Hash Synchronization и Enable single sign-on: креды администратора домена мастер просит разово и не сохраняет.
2. Мастер создаёт компьютерную учётку AZUREADSSOACC — кладём её в защищённую OU, снимаем делегирование Kerberos и закрываем права на объект всем, кроме админов домена.
3. Смотрим msDS-SupportedEncryptionTypes: с обновлением Windows Server за июль 2026 дефолт в AD DS меняется с RC4 на AES-256 — сначала ротация ключа, потом AES256_HMAC…
4. GPO Site to Zone Assignment List: https://autologon.microsoftazuread-sso.com в зону «Местная интрасеть» со значением 1, там же включаем Allow updates to status bar…
5. Ротация ключа не реже 30 дней: Import-Module .\AzureADSSO.psd1, New-AzureADSSOAuthenticationContext, Update-AzureADSSOForest -OnPremCredentials $creds; на staging н…

РЕЗУЛЬТАТ

Пользователь на доменном ПК открывает Outlook или Teams и попадает внутрь без ввода пароля, а пароль остаётся один — доменный. Обрыв канала до офиса не блокирует работу: аутентификация идёт в облаке по уже синхронизированному хешу, а не на локальном DC.

КЛЮЧЕВОЙ НЮАНС

Seamless SSO работает оппортунистически: при сбое он молча откатывается на ввод пароля, поэтому контролируем сам факт выдачи Kerberos-билета. Update-AzureADSSOForest дважды подряд на один лес запускать нельзя…

РЕАЛИЗАЦИЯ 3 ИЗ 3

Отказоустойчивость, мониторинг и защита от подмены объектов

Что настраиваем

Второй сервер в режиме staging, флаги защиты на уровне тенанта и регламент ежедневных проверок

Как мы это делаем

1. Ставим второй Connect с тем же sourceAnchor и той же конфигурацией в staging: импорт и синхронизация идут, экспорт подавлен, PHS и password writeback выключены.
2. Перед переключением сверяем ожидаемые экспорты: csexport "имя коннектора" %temp%\export.xml /f:x, затем CSExportAnalyzer; порог удалений держим на штатных 500 объек…
3. Держим цикл не реже раза в 7 дней даже на staging, иначе потребуется полная синхронизация; PurgeRunHistoryInterval по умолчанию тоже 7 дней.
4. Включаем BlockSoftMatchEnabled и BlockCloudObjectTakeoverThroughHardMatchEnabled командой Update-MgDirectoryOnPremiseSynchronization из Microsoft Graph PowerShell.
5. Мониторим три точки: Get-ADSyncScheduler, ошибки экспорта и журнал Application (источник Directory Synchronization: heartbeat 654, ошибки 611, 652, 655); Connect He…

РЕЗУЛЬТАТ

Смерть сервера синхронизации перестаёт быть аварией: staging переводится в боевой режим мастером за минуты, а уже уехавшие в облако хеши позволяют людям работать в Microsoft 365 всё это время. Подмена облачных учёток через soft- и hard-match закрыта на уровне тенанта.

КЛЮЧЕВОЙ НЮАНС

После снятия staging канал паролей догоняет очередь от последней метки — свежие пароли доезжают не мгновенно. С 01.07.2026 hard match блокируется, если у облачной учётки заполнен onPremisesObjectIdentifier или…

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Connect ставят прямо на контроллер домена**
  По докам сервер синхронизации — актив Control Plane (Tier 0): он читает хеши всего домена. Любое обслуживание DC превращается в обслуживание тенанта.

- ✕ **UPN пользователей остался на .local**
  Нероутируемый суффикс не верифицируется в Entra ID, и облако подменяет его на onmicrosoft.com. Публичный суффикс добавляем ДО первой синхронизации.

- ✕ **Мастер запускают без IdFix**
  Дубли proxyAddresses и UPN дают InvalidSoftMatch и AttributeValueMustBeUnique. Duplicate attribute resiliency лишь карантинит атрибут.

- ✕ **Синхронизируют весь домен целиком**
  В облако уезжают сервисные учётки, тестовые OU и подрядчики, съедая квоту тенанта: 50 тыс. объектов по умолчанию и 300 тыс. после верификации домена.

- ✕ **Ручная правка miiserver.exe.config**
  Совет по FIPS ломал апгрейд на 2.5.190.0 и 2.6.1.0: ADSync падал с FileLoadException, лечится binding redirect на DiagnosticSource 8.0.0.0.

- ✕ **AZUREADSSOACC оставили на RC4**
  Ключ не ротируют годами, msDS-SupportedEncryptionTypes — RC4. После обновления Windows Server за июль 2026 дефолт AES-256, и SSO падает.

- ✕ **Забыли: accountExpires не синхронизируется**
  Истёкшая по сроку учётка AD остаётся активной в Entra ID. Отключение выносим в задание с Set-ADUser либо в HR-процесс с явной блокировкой.

- ✕ **Флаги тенанта включают не глядя**
  SynchronizeUpnForManagedUsersEnabled после включения не отключить, а BlockSoftMatch ломает регистрацию hybrid-joined устройств.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Версия не ниже 2.5.79.0, лучше 2.6.84.0 — иначе остановка 30.09.2026
- Отдельная ВМ WS2022/2025, полный GUI, .NET 4.7.2, TLS 1.2, от 6 ГБ и 70 ГБ
- PHS + Seamless SSO, публичный UPN-суффикс и верифицированный домен
- IdFix прогнан, ошибок экспорта в тенант перед сдачей — ноль

НОРМАЛЬНО

- sourceAnchor = ms-DS-ConsistencyGuid и фильтрация синхронизации по OU
- Второй сервер в staging с той же конфигурацией и циклом не реже 7 дней
- AZUREADSSOACC на AES256_HMAC_SHA1, ротация ключа Kerberos раз в 30 дней
- BlockSoftMatch, запрет hard-match takeover, порог удалений на 500 объектах

ХОРОШО

- Сервер синхронизации в Tier 0: запрет NTLM, отдельные админ-учётки, LAPS
- Application-Based Authentication на TPM-сертификате вместо старой учётки
- Password Writeback и SSPR (нужен Entra ID P1) для удалённых сотрудников
- Алерты по Get-ADSyncScheduler и событиям 611/652/655 плюс Connect Health

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Верифицирован ли домен в тенанте и совпадает ли UPN-суффикс пользователей с ним, а не с .local?
- [ ] Какая версия Entra Connect Sync стоит и не ниже ли она обязательной 2.5.79.0 к 30.09.2026?
- [ ] Стоит ли сервер синхронизации отдельно от контроллера домена и защищён ли он как актив Tier 0?
- [ ] Выбран ли ms-DS-ConsistencyGuid как sourceAnchor и есть ли у учётки AD право записи в атрибут?
- [ ] Настроена ли фильтрация по OU, или в облако уезжают тестовые, сервисные и подрядные учётки?
- [ ] Что стоит в msDS-SupportedEncryptionTypes у AZUREADSSOACC и ротируется ли ключ Kerberos?
- [ ] Есть ли второй сервер в staging и проверялся ли его перевод в боевой режим на учениях?
- [ ] Кто узнаёт, что синхронизация встала: алерт по Get-ADSyncScheduler или отчёт Connect Health?
- [ ] Включены ли BlockSoftMatch, запрет hard-match takeover и порог удалений при экспорте?
- [ ] За сколько блокировка уволенного в AD доезжает до облака и кто это проверяет по факту?

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 AD до синхронизации: IdFix, UPN-суффиксы, дубли proxyAddresses, запас по квоте тенанта
- Разворачиваем Entra Connect Sync на выделенной ВМ: Custom, фильтр OU, ms-DS-ConsistencyGuid
- Настраиваем PHS и Seamless SSO: GPO на зоны, AES-256 и ротация ключа Kerberos раз в 30 дней
- Ставим второй сервер в staging и отрабатываем перевод в боевой режим на учениях, а не в аварии
- Мониторинг и разбор ошибок экспорта: InvalidSoftMatch, LargeObject, InvalidHardMatch

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 Microsoft Entra Connect: Prerequisites and hardware (learn.microsoft.com — 2026)

02 Microsoft Entra Connect: Version release history (2.6.84.0) (learn.microsoft.com — 2026)

03 Implement password hash synchronization with Connect Sync (learn.microsoft.com — 2026)

04 Microsoft Entra Connect: Seamless SSO — How it works (learn.microsoft.com — 2026)

05 Microsoft Entra Connect Sync: Scheduler (интервалы, staging) (learn.microsoft.com — 2026)

06 Configure Microsoft Entra Connect for an existing tenant (learn.microsoft.com — 2026)

07 Hybrid Identity required ports and protocols (learn.microsoft.com — 2026)

08 Шаблон ITfresh: паспорт гибридной идентификации и чек-лист сдачи (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.