Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Аудит последнего входа в AD: PowerShell, CSV, регламент

Наша методика: lastLogonTimestamp для отчётов, lastLogon по всем DC для расследований

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

К нам приходят с одной задачей: показать, кто реально работает в домене, а кто числится. Штатный админ запускает Get-ADUser -Properties lastLogon, получает на разных контроллерах разные цифры и теряет доверие к отчёту. В итоге увольнения не доходят до AD: у бывших сотрудников живы VPN, RDS и доступ к 1С, а лицензии и почтовые ящики оплачиваются за призраков.

Почему это важно бизнесу

- Учётка уволенного с активным VPN и правами в 1С — готовый вход в контур без взлома периметра.
- Аудит по 152-ФЗ требует подтвердить, что доступ прекращён вместе с трудовым договором.
- Каждая спящая учётка тянет лицензию RDS, почтовый ящик и место в бэкапе — деньги ежемесячно.
- Без достоверных дат входа расследование инцидента упирается в «данные противоречивы».
- Ручная сверка 300+ учёток с кадрами занимает дни и всё равно оставляет пропуски.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

9–14 суток

окно обновления lastLogonTimestamp: интервал 14 суток минус случайная часть от 5

AD Schema: ms-DS-Logon-Time-Sync-Interval

все DC

lastLogon не реплицируется: точное время = максимум значений со всех контроллеров

AD Schema: Last-Logon, раздел Remarks

1601-01-01

точка отсчёта FileTime в lastLogon, шаг 100 нс; значение 0 = вход не зафиксирован

AD Schema: Last-Logon

256

объектов на страницу по умолчанию в Get-ADUser -ResultPageSize; на больших доменах поднимаем

Docs: Get-ADUser, параметр -ResultPageSize

30/60/90

наши пороги в сутках: отчёт кадрам, согласование, отключение; удаление после 180

Регламент ITfresh: AD-аудит и чистка учёток

utf8BOM + ;

кодировка и разделитель Export-Csv, чтобы Excel ru-RU не ломал кириллицу и колонки

Docs: Export-Csv, наш шаблон отчёта

РЕАЛИЗАЦИЯ 1 ИЗ 3

Срез за минуту: LastLogonDate по всему домену в CSV

Что настраиваем

Типовой клиент: торговая компания, 45 рабочих мест, домен на 2 DC Windows Server 2019, 310 учёток, RDS и 1С

Как мы это делаем

1. Работаем с RSAT-машины: Import-Module ActiveDirectory, Get-ADUser -Filter 'Enabled -eq $true' -Properties LastLogonDate, Department, Title, PasswordLastSet.
2. LastLogonDate — это конвертированный модулем lastLogonTimestamp, он реплицируется: хватает любого одного DC, отставание до 14 суток.
3. Sort-Object LastLogonDate, затем Export-Csv -Encoding utf8BOM -Delimiter ';' — Excel в ru-RU открывает файл без мастера импорта.
4. Пустой LastLogonDate помечаем отдельно: это не «никогда не входил», а «нет реплицированного значения» — свежая или сервисная учётка.

РЕЗУЛЬТАТ

Полная картина по домену за минуту вместо недели ручной сверки, отчёт сразу читаем кадрами: ФИО, отдел, должность, дата входа. На типовом домене 300+ учёток мы регулярно находим 25–40% записей с датой входа старше 90 суток.

КЛЮЧЕВОЙ НЮАНС

Для еженедельного отчёта точность до минуты не нужна. Один запрос к любому DC по реплицируемому атрибуту закрывает большинство задач — важнее корректно оформить CSV и отделить пустые значения.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Точное время: опрашиваем все контроллеры по lastLogon

Что настраиваем

Запрос службы безопасности: во сколько увольняемый последний раз входил в домен и через какой контроллер прошла аутентификация

Как мы это делаем

1. $dcs = (Get-ADDomainController -Filter *).HostName — собираем список, дальше цикл Get-ADUser -Identity X -Server $dc -Properties lastLogon.
2. Каждое значение через [DateTime]::FromFileTime(); нули и пустые отбрасываем, берём Measure-Object -Maximum — это и есть реальный вход.
3. Сверяем с журналом Security на DC: 4768 (запрос TGT Kerberos), 4776 (проверка учётных данных NTLM), 4624 на целевом сервере.
4. Оформляем таблицей DC → значение → дельта: расхождения между контроллерами сразу показывают, на какой площадке пользователь реально работал.

РЕЗУЛЬТАТ

На домене 300 учёток и 3 контроллера это около 900 LDAP-запросов — 3–7 минут работы. Взамен ИБ получает время с точностью до минуты и подтверждение событиями журнала, а не оценку «примерно две недели назад».

КЛЮЧЕВОЙ НЮАНС

Точный ответ даёт только максимум lastLogon по всем DC плюс события 4768/4776/4624. Если хотя бы один контроллер недоступен, фиксируем это в отчёте: иначе максимум занижен и вывод неверен.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Регламент чистки: отчёт, карантин, удаление с бэкапом

Что настраиваем

Клиенты с текучкой: розница, склад, медцентр — 150–500 учёток, кадры не всегда сообщают об увольнении в тот же день

Как мы это делаем

1. Еженедельно: Search-ADAccount -AccountInactive -TimeSpan 30.00:00:00 -UsersOnly — командлет считает простой по LastLogonDate и работает с любого DC.
2. На 60 сутках согласуем с руководителем; на 90 — Disable-ADAccount, Move-ADObject в OU Disabled, Set-ADUser -Description с датой и причиной.
3. Перед Remove-ADUser выгружаем Get-ADUser -Properties * и MemberOf в JSON; включённая корзина AD (msDS-deletedObjectLifetime) — вторая линия защиты.
4. Компьютеры считаем отдельно: Search-ADAccount -AccountInactive -ComputersOnly, порог 60 суток — забытые ноутбуки хранят секреты Kerberos и права Wi-Fi.
5. Запуск — задача планировщика под gMSA, лог в файл, письмо ответственному; сервисные учётки исключаем по OU и наличию servicePrincipalName.

РЕЗУЛЬТАТ

Домен перестаёт копить мусор: спящих учёток остаются единицы вместо сотен. Отключение становится обратимым — за месяц карантина в OU Disabled любая ошибка кадров чинится одним Enable-ADAccount без потери профиля и членств в группах.

КЛЮЧЕВОЙ НЮАНС

Регламент важнее скрипта: сначала пороги 30/60/90/180 и ответственные, потом автоматизация. Массовое отключение без карантина и бэкапа рано или поздно заденет сотрудника в декрете или в длительном отпуске.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

✕ lastLogon без FromFileTime

Атрибут отдаёт Int64 в формате FileTime: в CSV попадает 18-значное число вместо даты. Конвертация обязательна, ноль трактуем как «нет данных».

✕ Опрос одного контроллера

lastLogon пишется только на аутентифицировавшем DC и не реплицируется. С одного контроллера получаете пустоту или значение годичной давности.

✕ Ждём свежести от lastLogonTimestamp

Атрибут по умолчанию обновляется раз в 9–14 суток. Для вопроса «заходил ли вчера» он не подходит принципиально: это индикатор простоя, не входа.

✕ Сервисные учётки в общем списке

Учётка 1С или SQL месяцами не делает интерактивный вход, но работает по Kerberos. Исключаем по OU и servicePrincipalName, иначе отключите продуктив.

✕ Export-Csv с настройками по умолчанию

PowerShell 7 пишет utf8NoBOM с запятой, и Excel ru-RU ломает кириллицу. В Windows PowerShell 5.1 значения utf8BOM нет — там -Encoding UTF8.

✕ Отключили — и забыли про группы

Отключённая учётка остаётся в группах доступа, у неё живы сертификаты PKI и записи в VPN. Членства чистим и сертификаты отзываем отдельным шагом.

✕ Remove-ADUser без выгрузки

Без JSON-бэкапа атрибутов и MemberOf возврат сотрудника из декрета превращается в ручное восстановление прав по всем системам компании.

✕ Пустое значение читают как «никогда»

Пустой LastLogonDate бывает у новых учёток и при функциональном уровне ниже Windows Server 2003. Такие записи — в отдельный лист, а не в удаление.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Ежемесячно Search-ADAccount -AccountInactive -TimeSpan 90.00:00:00 -UsersOnly
- Экспорт в CSV с -Encoding utf8BOM и -Delimiter ';' под Excel ru-RU
- Отдельная OU Disabled и дата отключения в атрибуте Description
- Проверка msDS-LogonTimeSyncInterval и функционального уровня домена

НОРМАЛЬНО

- Еженедельный отчёт 30 суток кадрам, порог 60 — руководителю подразделения
- Задача планировщика под gMSA, лог выполнения и письмо ответственному
- Отдельный отчёт по компьютерам: -ComputersOnly с порогом 60 суток
- Исключение сервисных учёток по OU и атрибуту servicePrincipalName

ХОРОШО

- Опрос всех DC по lastLogon с выбором максимума для расследований ИБ
- Корзина AD включена, JSON-бэкап атрибутов и MemberOf перед удалением
- Сверка с событиями 4768/4776/4624 и выгрузка отчётов в SIEM или Zabbix
- Связка с кадрами: заявка на увольнение сразу ставит задачу на блокировку

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Функциональный уровень домена не ниже Windows Server 2003 — иначе lastLogonTimestamp пуст
- [ ] Значение msDS-LogonTimeSyncInterval на объекте домена проверено (пусто = 14 суток)
- [ ] Список контроллеров получен через Get-ADDomainController -Filter * и опрошен целиком
- [ ] Значения lastLogon переведены через [DateTime]::FromFileTime(), нули отброшены
- [ ] Сервисные учётки исключены по OU и servicePrincipalName, список согласован с владельцем
- [ ] CSV открывается в Excel: кодировка utf8BOM, разделитель ';', заголовки на месте
- [ ] Пороги 30/60/90/180 суток зафиксированы в регламенте, назначены ответственные
- [ ] Перед удалением сделан JSON-бэкап атрибутов и членств в группах
- [ ] Отчёт по компьютерным учёткам сформирован отдельно, порог 60 суток
- [ ] Отключённые учётки удалены из VPN-групп, сертификаты PKI отозваны

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 скрипт аудита на вашем DC: расписание, лог, письмо ответственному — за один визит
- Собираем выгрузку по всем контроллерам домена и сверяем её со списком кадров
- Пишем регламент 30/60/90/180 с карантинной OU и процедурой возврата учётки
- Подключаем аудит компьютерных учёток и чистку забытых машин из домена
- Ведём домен на аутсорсинге: ежемесячный отчёт директору и в службу безопасности

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 Schema: Last-Logon (lastLogon), раздел Remarks (learn.microsoft.com — 2026)

02 AD Schema: ms-DS-Logon-Time-Sync-Interval (learn.microsoft.com — 2026)

03 AD Schema: Last-Logon-Timestamp (learn.microsoft.com — 2026)

04 PowerShell: Search-ADAccount, модуль ActiveDirectory (learn.microsoft.com — 2026)

05 PowerShell: Get-ADUser — Filter, Properties, ResultPageSize (learn.microsoft.com — 2026)

06 PowerShell: Export-Csv — Encoding, Delimiter, NoTypeInformation (learn.microsoft.com — 2026)

07 MS-ADTS: Tombstone Lifetime and Deleted-Objects Lifetime (learn.microsoft.com — 2026)

08 Шаблон ITfresh: AD-LastLogon-Audit.ps1 и регламент чистки (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.