Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Сброс локальных групповых политик: методология ITfresh

Диагностика слоёв GPO, бэкап LGPO.exe и контролируемый откат Registry.pol и Security Settings

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Мы регулярно принимаем на обслуживание парки, где предыдущий администратор «закрутил» локальные GPO: заблокированы cmd и диспетчер задач, не запускаются exe, ломаются сценарии 1С. Хаотичный сброс «по статьям из интернета» сносит заодно права и аудит. Наш регламент приводит машины к предсказуемому состоянию: диагностика слоя, бэкап, адресный или полный откат, возврат в управлен…

Почему это важно бизнесу

- Заблокированный cmd или запрет запуска exe останавливает 1С и офисные сценарии целого отдела — простой считается в человеко-часах
- Наслоения политик от прошлых админов — скрытый риск: никто не знает, что применено, любое обновление Windows даёт непредсказуемый эффект
- Неграмотный сброс сносит и полезные настройки безопасности (пароли, аудит, права) — машина остаётся без базовой защиты
- Без бэкапа локальных GPO откат невозможен — восстановление превращается в переустановку рабочего места

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

90+30 мин

Интервал фонового применения GPO: пока не пройдёт цикл или gpupdate /force, правка «не видна»

Раздел Group Policy processing (learn.microsoft.com)

16 ч

Security Settings переприменяются каждые 960 мин и без изменений — локальные правки «слетают»

Раздел Security policy settings (learn.microsoft.com)

3 слоя

MLGPO: Local Computer → Administrators/Non-Administrators → per-user (SID в GroupPolicyUsers)

MLGPO, Windows Vista и новее

v3.0

LGPO.exe (Security Compliance Toolkit): /b — бэкап политик до сброса, /g — импорт эталона

Security Compliance Toolkit, LGPO v3.0

2 ветки

Registry.pol в Machine и User в %WinDir%\System32\GroupPolicy — кэш, пересоздаётся gpupdate

Наш стандарт разбора Registry.pol

7016/4016

Event ID в журнале GroupPolicy/Operational: по ним проверяем ошибки применения после сброса

Журнал Microsoft-Windows-GroupPolicy/Operational

Диагностика: какой слой политики виноват

Что настраиваем

Любая машина Windows 10/11 Pro/Home до вмешательства — рабочая группа или домен

Как мы это делаем

1. Снимаем gpresult /h report.html и /r: смотрим Winning GPO и Applied GPOs — отделяем локальный слой от доменного
2. Проверяем журнал Applications and Services → Microsoft-Windows-GroupPolicy/Operational: ошибки CSE, Event ID 7016/4016
3. Инвентаризируем %WinDir%\System32\GroupPolicy и GroupPolicyUsers\<SID>: даты Registry.pol, наличие per-user слоёв MLGPO
4. Сверяем ветки HKLM/HKCU Software\Policies с содержимым Registry.pol (LGPO.exe /parse) — ищем «осиротевшие» ключи
5. Фиксируем состояние: LGPO.exe /b <папка> — полный бэкап локальных GPO до любых изменений

РЕЗУЛЬТАТ

Сброс становится адресным: мы знаем, локальная это политика или доменная, машинная или пользовательская, и не трогаем лишнего. На домашних редакциях без gpedit.msc диагностика полностью закрывается связкой gpresult + LGPO.exe /parse.

КЛЮЧЕВОЙ НЮАНС

Winning GPO «Local Group Policy» в отчёте gpresult — маркер, что лечим на месте; доменная GPO в списке означает, что локальный сброс проживёт только до ближайшего цикла 90+30 мин.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Контролируемый полный сброс на автономной машине

Что настраиваем

Windows 10/11 любой редакции вне домена: Machine- и User-слои плюс Security Settings

Как мы это делаем

1. LGPO.exe /b — бэкап; затем удаляем %WinDir%\System32\GroupPolicy и GroupPolicyUsers (RD /S /Q от администратора)
2. Security Settings откатываем отдельно: secedit /configure /cfg %windir%\inf\defltbase.inf /db defltbase.sdb /verbose
3. gpupdate /force пересоздаёт пустые каталоги; обязательная перезагрузка — часть CSE отрабатывает только при старте ОС
4. Контроль: gpresult /r без локального слоя, журнал GroupPolicy/Operational чист, лог secedit в %windir%\security\logs\scesrv.log

РЕЗУЛЬТАТ

Машина приходит к дефолтному состоянию политик без переустановки ОС: снимаются блокировки cmd, диспетчера задач и запуска exe, а бэкап позволяет вернуть любую нужную настройку через LGPO.exe /g за минуты.

КЛЮЧЕВОЙ НЮАНС

secedit с defltbase.inf откатывает только Security Settings (пароли, права, аудит) и не чистит Administrative Templates — поэтому в нашем регламенте оба шага идут парой, а не «или-или».

РЕАЛИЗАЦИЯ 3 ИЗ 3

Массовый сброс по парку и возврат в управление

Что настраиваем

Рабочая группа 10–50 ПК: прогон Reset-LocalGPO.ps1 через WinRM, затем централизация

Как мы это делаем

1. Раскатываем наш Reset-LocalGPO.ps1 через Invoke-Command (WinRM, 5985/5986): бэкап LGPO → удаление каталогов → secedit → gpupdate
2. На время прогона добавляем исключение в EDR/антивирус на удаление каталогов GroupPolicy* — снимаем сразу после
3. Перезагрузка волнами вне рабочего времени (shutdown /r), затем сбор gpresult /r со всех машин в сводный отчёт
4. Финал: вводим парк в AD-домен или Intune — а политика «Turn off Local Group Policy Objects processing» отключает локальный слой целиком

РЕЗУЛЬТАТ

Типовой парк на 40 ПК проходит полный цикл за один вечер; повторные «сюрпризы» от локальных политик исключены, потому что источником настроек становится DC или Intune, а не наследие предыдущего администратора.

КЛЮЧЕВОЙ НЮАНС

«Turn off Local Group Policy Objects processing» (Computer Configuration → Administrative Templates → System → Group Policy) — штатный способ навсегда исключить локальный слой на доменных машинах.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

✕ Сброс в домене без gpresult

Доменные GPO перезапишут всё за цикл 90+30 мин. Сначала gpresult /h: если Winning GPO доменная — правим на DC через gpmc.msc, а не на клиенте.

✕ Нет бэкапа перед удалением

Удалили каталоги — вернуть нечего. LGPO.exe /b делает полный бэкап локальных GPO за секунды, /g восстанавливает его целиком.

✕ Ручная чистка Software\Policies

Ключи HKLM/HKCU Software\Policies пересоздаются из Registry.pol при gpupdate. Чистим источник (Registry.pol), а не следствие в реестре.

✕ Забытая перезагрузка

Часть клиентских расширений (CSE) применяется только при старте ОС или входе. Наш регламент: gpupdate /force + reboot, иначе «сброс не сработал».

✕ Надежда на secedit для всего

defltbase.inf откатывает только Security Settings. Administrative Templates живут в Registry.pol — их secedit не трогает вообще.

✕ Игнор per-user слоёв MLGPO

GroupPolicyUsers хранит политики по SID: Administrators/Non-Administrators и отдельные юзеры. Сброс одного каталога GroupPolicy их не убирает.

✕ EDR блокирует массовое удаление

EDR-агенты класса SentinelOne/Kaspersky реагируют на RD /S /Q системных каталогов. Заводим временное исключение по хэшу скрипта и снимаем сразу после…

✕ Запуск без elevation

Каталоги в System32 защищены: без прав администратора RD и secedit молча фейлятся. В скрипте держим #Requires -RunAsAdministrator.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- gpresult /h перед любым вмешательством — определить слой (локальный/доменный)
- Бэкап LGPO.exe /b до удаления GroupPolicy и GroupPolicyUsers
- gpupdate /force + перезагрузка после сброса, контроль по gpresult /r

НОРМАЛЬНО

- Пара «Registry.pol-сброс + secedit defltbase.inf» — единый регламент, не «или-или»
- Reset-LocalGPO.ps1 через WinRM для парка, сводный gpresult со всех машин
- Проверка журнала GroupPolicy/Operational (7016/4016) после применения
- Временные исключения в EDR на время прогона, снятие сразу после

ХОРОШО

- Эталонные наборы LGPO по ролям машин, импорт через LGPO.exe /g после сброса
- Централизация: AD-домен или Intune вместо локальных политик
- «Turn off Local GPO processing» на доменных машинах — локальный слой отключён
- Регулярный аудит наслоений: gpresult по парку по расписанию в отчёт

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Снят ли отчёт gpresult /h до вмешательства и определён ли источник проблемной политики — локальный или доменный?
- [ ] Сделан ли бэкап локальных GPO через LGPO.exe /b и проверено ли восстановление из него хотя бы раз?
- [ ] Учтены ли per-user слои MLGPO в GroupPolicyUsers (по SID), а не только машинный Registry.pol?
- [ ] Включён ли в регламент secedit /configure с defltbase.inf для отката Security Settings?
- [ ] Заложена ли перезагрузка после gpupdate /force и проверка журнала GroupPolicy/Operational?
- [ ] Есть ли готовый скрипт массового сброса и рабочий WinRM-доступ ко всем машинам парка?
- [ ] Согласовано ли временное исключение в EDR/антивирусе на операции с каталогами GroupPolicy?
- [ ] Для доменных ПК: правки делаются на DC (gpmc.msc), а не локальным сбросом на клиенте?
- [ ] Есть ли план возврата парка в централизованное управление (AD или Intune) после разовой чистки?

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).

- Диагностика и адресный сброс локальных GPO на парке 10–50 ПК с бэкапом и отчётом по каждой машине
- Разворачивание мини-домена AD или перевод на Intune: политики централизованно, локальный слой отключаем
- Эталонные наборы LGPO под роли (бухгалтерия, 1С-клиенты, терминалы) с импортом через LGPO.exe /g
- Регламент и скрипты массового сброса (WinRM/PsExec) с контролем журналов и EDR-исключениями

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 Group Policy processing for Windows (порядок и интервалы применения) (learn.microsoft.com — 2025)

02 Microsoft Security Compliance Toolkit — LGPO.exe (learn.microsoft.com — v3.0)

03 Secedit command reference (/configure, /validate, /export) (learn.microsoft.com — WS2022)

04 Security policy settings (16-часовой цикл переприменения) (learn.microsoft.com — Win10/11)

05 Gpresult / Gpupdate command-line reference (learn.microsoft.com — WS2022)

06 Наш шаблон Reset-LocalGPO.ps1 (WinRM-прогон, бэкап + secedit) (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.