Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Диагностика GPO: gpresult, RSoP и GroupPolicy/Operational

Как мы находим причину неприменения групповых политик в доменах AD клиентов до 50 РМ

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

У клиента «политика обязана применяться, но не применяется»: не маппится сетевой диск, не ставится прокси, не тянется софт, не блокируется USB. Причина почти всегда не в самой GPO, а в фильтрации, репликации SYSVOL, времени или Slow Link. Мы ставим диагноз по gpresult, RSoP и журналу GroupPolicy/Operational за минуты, а не перебором наугад. Бездействие даёт незакрытые требован…

Почему это важно бизнесу

- Неприменённая политика безопасности = дыра в контуре: незашифрованный USB, открытый RDP, отсутствие блокировки экрана.
- Ручная донастройка каждого PM вместо централизованной GPO — это часы работы инженера на ровном месте.
- Сотрудник переведён в новый отдел, но не получил доступ к папкам — простой рабочего дня.
- Расхождение политик между DC из-за SYSVOL/DFSR даёт разное поведение машин и нестабильность.
- Без методики диагностики один инцидент растягивается на дни и эскалации.

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

4016/5016

События начала/успеха обработки клиентского расширения (CSE) в GroupPolicy/Operational — перво…

по докам GroupPolicy/Operational

1058

Ошибка чтения gpt.ini из SYSVOL — в 90% случаев беды DFSR-репликации между DC, идём проверять…

наш стандарт диагностики

500 Кбит/с

Порог Slow Link по умолчанию: ниже — Software Installation и Scripts не отрабатывают

по докам Group Policy CSE

5 мин

Допуск рассинхрона часов для Kerberos (MaxTolerance); больше — GPO вообще не стартуют

по докам Kerberos Policy

90+30 мин

Фоновый цикл обновления GPO: базовые 90 мин плюс случайный сдвиг до 30 мин

по докам Group Policy Refresh

10.0.22000

Версия ядра Windows 11 — старые WMI-фильтры «Version LIKE 10.%» её ловят не так, как ждут

по докам Win32_OperatingSystem

РЕАЛИЗАЦИЯ 1 ИЗ 2

Быстрый рентген: gpresult и RSoP

Что настраиваем

Клиентская станция или терминальный сервер в домене AD, где политика «не видна»

Как мы это делаем

1. gpresult /h report.html /f — читаем Applied GPOs, Denied GPOs с причиной (Filtering/Empty/Disabled) и Winning GPO по каждой настройке.
2. gpresult /scope computer /v — когда нет интерактивной сессии или нужна только Computer-конфигурация.
3. whoami /groups и Security Group Membership в отчёте — сверяем фактическое членство в группах фильтрации.
4. rsop.msc держим как вторичный взгляд: он по дизайну не показывает Group Policy Preferences — доверяем HTML.
5. Видим Denied by Filtering — идём проверять Security Filtering и WMI-фильтр GPO.

РЕЗУЛЬТАТ

За несколько минут отделяем «политика не долетела до машины» от «долетела, но перекрыта другой GPO». Winning GPO сразу называет объект, который задал итоговое значение, — дальше правим адресно, а не перебором.

КЛЮЧЕВОЙ НЮАНС

Отчёт gpresult /h информативнее RSoP: смотрим именно колонку Winning GPO и раздел Denied GPOs с причиной, а не только список применённых.

РЕАЛИЗАЦИЯ 2 ИЗ 2

Журнал GroupPolicy/Operational и репликация

Что настраиваем

Контроллеры домена и клиент: разбор, когда gpresult молчит, а политика не работает

Как мы это делаем

1. Event Viewer → Applications and Services Logs → Microsoft → Windows → GroupPolicy → Operational, фильтруем по ActivityID одного цикла.
2. Ключевые ID: 4016/5016 CSE, 4017/5017 LDAP, 5312/5313 применённые/отфильтрованные, 7016 ошибка CSE, 1030/1058 доступ к SYSVOL.
3. 1058 или 1030 — идём на DC: dcdiag /test:replications, repadmin /replsummary, repadmin /showrepl.
4. Проверяем время: w32tm /query /status на клиенте и DC, при рассинхроне w32tm /resync /force.
5. При глубоком разборе включаем gpsvc-лог: C:\Windows\Debug\Usermode\gpsvc.log.

РЕЗУЛЬТАТ

Журнал даёт хронологию цикла с таймингами и точной ошибкой CSE. DFSR- и Kerberos-проблемы ловятся до того, как клиент замечает разное поведение машин; правки GPO гарантированно доезжают до всех DC.

КЛЮЧЕВОЙ НЮАНС

1058 почти всегда = SYSVOL/DFSR, а не сама GPO. Смотрим: доезжает ли gpt.ini на все реплики и совпадает ли versionNumber в AD и в SYSVOL.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Убрали Authenticated Users после MS16-072**
  С июня 2016 user-GPO читаются в контексте компьютера. Сняли Authenticated Users полностью — политика перестала читаться. Оставляем Read (без Apply) и…
- ✕ **WMI-фильтр «Version LIKE 10.%» ловит не то**
  Windows 11 имеет ядро 10.0.22000+, а серверы тоже 10.x. Фильтр либо не срабатывает, либо цепляет лишнее. Сверяем через gpresult /scope:computer.
- ✕ **GPO не привязана или висит на Domain Root**
  Link забыт или сделан на корень домена вместо нужной OU. Проверяем свойства Link и дерево OU в gpmc.msc перед любой другой гипотезой.
- ✕ **Block Inheritance против Enforced**
  OU с Block Inheritance не наследует политики сверху, но Enforced-GPO протыкают блокировку. Путаница даёт неожиданный итог — читаем оба флага.
- ✕ **Preferences с Apply once**
  Настройка Preferences отработала один раз и больше не применяется, хотя GPO показана применённой. Смотрим режим item-level и Apply once.
- ✕ **Рассинхрон часов ломает Kerberos**
  Расхождение времени DC и клиента более 5 минут (MaxTolerance) роняет Kerberos — GPO даже не стартуют. Проверяем w32tm до всего остального.
- ✕ **Slow Link режет тяжёлые расширения**
  Канал ниже 500 Кбит/с — Software Installation и Scripts молча не применяются, хотя реестровые политики проходят. Проверяем параметр Slow link detecti…
- ✕ **User-политика без парной Computer-части**
  Часть User-настроек не отрабатывает, когда не применена связанная Computer-конфигурация. Проверяем оба scope, а не только пользовательский.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- gpresult /h как первый шаг любой диагностики GPO
- Authenticated Users с правом Read сохранены на всех GPO
- Синхронизация времени NTP на всех DC и клиентах
- Ссылки (Link) GPO проверены в gpmc.msc

НОРМАЛЬНО

- Разбор журнала GroupPolicy/Operational по EventID
- Регулярная проверка DFSR-репликации SYSVOL (repadmin)
- WMI-фильтры валидированы под актуальные версии ОС
- Loopback (Merge/Replace) осознанно настроен на терминалах

ХОРОШО

- Бэкап и версионирование GPO (Backup-GPO, Get-GPOReport)
- Мониторинг репликации SYSVOL и Kerberos в Zabbix
- Документированная OU-структура и матрица фильтрации
- Плановый аудит и чистка «зоопарка» политик раз в квартал

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Снят ли отчёт gpresult /h и прочитаны ли Denied GPOs с причиной?
- [ ] Сохранено ли право Read у Authenticated Users на всех GPO (MS16-072)?
- [ ] Совпадает ли WMI-фильтр с реальными версиями ОС клиентов (10.0.22000+)?
- [ ] Привязана ли GPO к нужной OU, а не к Domain Root?
- [ ] Проверены ли флаги Block Inheritance и Enforced на цепочке OU?
- [ ] Нет ли ошибок 1030/1058 в GroupPolicy/Operational?
- [ ] В норме ли DFSR-репликация SYSVOL между всеми DC?
- [ ] Расхождение времени DC и клиента менее 5 минут (Kerberos)?
- [ ] Не режет ли Slow Link (порог 500 Кбит/с) Scripts и Software Installation?
- [ ] Настроен ли Loopback (Merge/Replace) на терминальных серверах?

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).

- Удалённая и выездная экспресс-диагностика неприменения GPO по нашей методике
- Аудит и наведение порядка в «зоопарке» политик: фильтрация, WMI, OU-структура
- Проверка и восстановление репликации SYSVOL/DFSR между контроллерами домена
- Настройка Loopback и целевых политик под терминальные серверы и киоски
- Бэкап, версионирование и документирование GPO для стабильных изменений

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 Operational log — event IDs (learn.microsoft.com — 2024)

02 MS16-072 / KB3163622: Security update for Group Policy (support.microsoft.com — 2016)

03 Event ID 1058 — processing of Group Policy failed (gpt.ini) (learn.microsoft.com — 2024)

04 Configure Group Policy slow link detection (learn.microsoft.com — 2024)

05 Kerberos policy — maximum tolerance for clock sync (learn.microsoft.com — 2024)

06 Group Policy processing and refresh interval (learn.microsoft.com — 2024)

07 Наш внутренний шаблон диагностики GPO (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.