Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Диагностика групповых политик Active Directory

Как мы находим причину неприменения GPO и ускоряем логон: логи, CSE, SYSVOL, WMI

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Пользователь жалуется «политика не применилась», а логон тянется минутами. Мы разбираем это как инженерную задачу: цепочка LSDOU, права на GPO после MS16-072, WMI-фильтры, доступность SYSVOL и время работы каждого CSE. Без методики домен обрастает дублями GPO, настройки безопасности молча не доезжают до части машин, а день начинается с ожидания рабочего стола.

Почему это важно бизнесу

- Минута ожидания логона на 100 ПК — это 33 человеко-часа простоя в месяц при 20 рабочих днях
- Не применившаяся политика безопасности = машина без парольных правил и ограничений, и об этом никто не узнаёт
- Аудит и требования 152-ФЗ проверяют фактическое состояние настроек по gpresult /h, а не намерения в gpmc.msc
- Каждый тикет «у меня нет диска P:» — разбор события 4098 GPP в Application-логе, 20-40 минут инженера
- Сбой репликации SYSVOL между площадками откатывает настройки половины офиса без единой ошибки у пользователя

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

90-120 мин

Фактическое окно фонового обновления GPO: 90 минут плюс случайный сдвиг до 30 минут

learn.microsoft.com, Group Policy processing

5 мин

Интервал обновления политик на контроллерах домена — там изменения видны почти сразу

learn.microsoft.com, GP refresh for DC

0x30002

GPSvcDebugLevel в ветке Diagnostics — включаем подробный gpsvc.log при неочевидных сбоях

learn.microsoft.com, GP troubleshooting

8000-8007

События окончания обработки: дают время в мс на старт компьютера и вход пользователя

Журнал GroupPolicy/Operational

500 Кбит/с

Порог медленного канала по умолчанию: ниже него CSE пропускают скрипты, установку ПО, перенапр…

learn.microsoft.com, slow link detection

State 3

Целевое состояние dfsrmig (Eliminated): SYSVOL только на DFSR, иначе реплику на Server 2025 не…

learn.microsoft.com, SYSVOL Migration Guide

РЕАЛИЗАЦИЯ 1 ИЗ 3

Экспресс-диагностика: от события до виновной GPO

Что настраиваем

Проблемная рабочая станция или RDSH плюс контроллер домена, с которого клиент брал политику в сбойном цикле

Как мы это делаем

1. Снимаем базу: gpresult /h GPResult.htm и gpresult /r — видны отклонённые GPO с причиной: Denied (Security), Not Applied (Empty), Denied (WMI Filter)
2. В System-журнале берём Correlation ActivityID сбойного события и строим Custom View по Microsoft-Windows-GroupPolicy/Operational — один цикл обработки без чужого шу…
3. Сводим пары стартовых и конечных событий: 4016/5016 по каждому CSE, 8000-8007 — суммарное время в мс; расширение с задержкой в секундах видно сразу
4. Если событий не хватает — GPSvcDebugLevel=0x30002 в HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Diagnostics, создаём %windir%\debug\usermode, gpupdate /force,…
5. Проверяем инфраструктуру: dcdiag /test:sysvolcheck /test:dfsrevent и repadmin /replsummary — исключаем расхождение SYSVOL между DC

РЕЗУЛЬТАТ

Причина находится за один заход, а не перебором. Типовые находки — 1058 (нет доступа к gpt.ini), 1129 (не поднялась сеть или закрыт LDAP 389), 1097 (не определена учётная запись компьютера: обычно рассинхрон времени с DC) — каждая имеет однозначное лечение, а не «попробуйте перезагрузитьс…

КЛЮЧЕВОЙ НЮАНС

После каждого gpupdate ActivityID меняется — фильтр в Event Viewer надо обновлять, иначе смотрите прошлый цикл. Папку %windir%\debug\usermode Windows сама не создаёт: без неё gpsvc.log не появится.

РЕАЛИЗАЦИЯ 2 ИЗ 3

Права на GPO и фильтры: почему политика «не видна»

Что настраиваем

Все GPO домена: Security Filtering, Delegation и WMI-фильтры — правим на уровне объектов политики, а не на клиенте

Как мы это делаем

1. Инвентаризируем права: Get-GPO -All с Get-GPPermission -All — ищем GPO без Read у Authenticated Users или Domain Computers
2. Возвращаем модель после MS16-072 (KB3163622): Set-GPPermission -PermissionLevel GpoRead для Authenticated Users плюс GpoApply на целевую группу
3. Чистим WMI-фильтры от Win32_Product: класс не оптимизирован под запросы и запускает проверку целостности всех MSI (события 1035 MsiInstaller)
4. Переписываем условия на Win32_OperatingSystem (Version, ProductType) и Win32_ComputerSystem (PCSystemType) — выполняются за доли секунды
5. Проверяем каждый фильтр на эталонной машине через Get-CimInstance -Query до привязки к боевой OU

РЕЗУЛЬТАТ

Политики применяются предсказуемо: после MS16-072 пользовательские GPO читаются в контексте учётной записи компьютера, поэтому «почищенные» ради безопасности права больше не выключают политику молча. Логон перестаёт зависеть от инвентаризационных WQL-запросов.

КЛЮЧЕВОЙ НЮАНС

На каждой GPO держим минимум две записи: Authenticated Users с Read и целевую группу с Apply Group Policy. Ошибка в WQL не даёт события об отказе — фильтр считается несовпавшим, и политика тихо пропускается.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Профилактика: Central Store, loopback и контроль дрейфа

Что настраиваем

Домен целиком: SYSVOL с PolicyDefinitions, OU терминальных серверов, регламент бэкапа и сверки GPO

Как мы это делаем

1. Разворачиваем Central Store строго по пути SYSVOL\домен\Policies\PolicyDefinitions — имя папки менять нельзя, копию прошлой версии держим рядом как PolicyDefinition...
2. Убираем Extra Registry Settings в отчётах: они значат, что настройка есть в Registry.pol, а ADMX-описания в хранилище нет
3. Для RDS и переговорных — отдельная OU и Configure user Group Policy loopback processing mode в режиме Replace
4. Отключаем неиспользуемую половину каждой GPO (GPO Status: Computer или User configuration settings disabled) и заполняем вкладку Comment
5. Backup-GPO -All по расписанию плюс сверка Get-GPOReport с эталоном через Policy Analyzer из Security Compliance Toolkit

РЕЗУЛЬТАТ

Консоль показывает настройки человекочитаемо на любой машине с RSAT, число GPO не растёт бесконтрольно, а откат неудачного изменения занимает минуты: есть и копия объекта, и понятный diff против прошлого отчёта.

КЛЮЧЕВОЙ НЮАНС

Central Store читается из SYSVOL, поэтому его состояние зависит от здоровья DFSR. Перед вводом DC на Windows Server 2025 проверяем dfsrmig /getglobalstate: бинарников FRS в этой версии нет, реплику в FRS-домен...

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Удалили Authenticated Users из фильтра**
  После MS16-072 user-политики читаются в контексте компьютера: оставляем Read у Authenticated Users, а применение ограничиваем через GpoApply
- ✕ **WMI-фильтр на классе Win32_Product**
  Класс не оптимизирован под WQL и запускает проверку целостности всех MSI-пакетов — логон растягивается на десятки секунд. Заменяем на Win32_Operating…
- ✕ **Block Inheritance против Enforced**
  Блокировка наследования не отменяет ссылку с Enforced, а Enforced на домене перебивает всё ниже. Рисуем фактическую цепочку LSDOU, а не ожидаемую
- ✕ **Диагностика без ActivityID**
  В Operational-логе одновременно идут несколько экземпляров обработки, особенно на RDSH. Без фильтра по Correlation ActivityID события перемешиваются
- ✕ **Расхождение версий GPC и GPT**
  Атрибут versionNumber в AD и Version= в gpt.ini расходятся при сбое DFSR: клиент считает политику неизменной и не применяет новую редакцию
- ✕ **Отчёты с Extra Registry Settings**
  Нет ADMX в Central Store — консоль и gpresult показывают сырые ключи реестра. Кладём PolicyDefinitions под версию ОС и обновляем вместе с парком
- ✕ **Тяжёлый Software Installation в GPO**
  MSI в сотни мегабайт по ссылке на удалённый DC тянется при каждом синхронном логоне. Переносим на DFS-namespace ближайшей площадки
- ✕ **Логон стартует до готовности сети**
  Событие 1129 — NLA не отдала связность с DC вовремя. Лечим политиками Specify startup policy processing wait time и Always wait for the network, плюс…

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Authenticated Users с Read на каждой GPO, Apply Group Policy — только целевой группе
- Ни одного WMI-фильтра с обращением к Win32_Product в домене
- Ежемесячный Backup-GPO -All на ресурс вне контроллеров домена
- Проверка dcdiag /test:sysvolcheck и repadmin /replsummary раз в неделю

НОРМАЛЬНО

- Central Store SYSVOL\Policies\PolicyDefinitions обновляется под текущую сборку Windo…
- Тестовая OU: новая GPO живёт там не меньше недели до продакшена
- Отключены пустые половины GPO, заполнены Comment и единый шаблон имени
- Loopback Replace на отдельной OU терминальных серверов и киосков

ХОРОШО

- Мониторинг событий 8000-8007: алерт при обработке дольше 30 000 мс
- Сверка Get-GPOReport с эталоном через Policy Analyzer при каждом изменении
- SYSVOL на DFSR в состоянии Eliminated (dfsrmig State 3), DFL и FFL не ниже Server 20…
- Выгрузки GPO в git с обязательным ревью перед привязкой к боевой OU

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] У каждой GPO есть Read для Authenticated Users и явная группа с Apply Group Policy?
- [ ] Известно, сколько GPO применяется к типовому ПК и сколько мс занимает обработка по событиям 8000-8007?
- [ ] Есть ли в домене WMI-фильтры, обращающиеся к Win32_Product или другим тяжёлым классам?
- [ ] Проверены ли Block Inheritance и Enforced по всей цепочке от домена до конечной OU?
- [ ] Репликация SYSVOL здорова: dcdiag /test:sysvolcheck и repadmin /replsummary без ошибок?
- [ ] Развёрнут Central Store и в отчётах gpresult отсутствуют Extra Registry Settings?
- [ ] Для терминальных серверов включён loopback в режиме Replace на собственной OU?
- [ ] Делается ли Backup-GPO по расписанию и проверялось ли восстановление из копии?
- [ ] Отключены ли неиспользуемые половины GPO и заполнены ли комментарии с назначением?
- [ ] Домен переведён на DFSR (dfsrmig /getglobalstate возвращает Eliminated) до ввода DC на Server 2025?

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 всех GPO домена: права, WMI-фильтры, дубли, конфликты — отчёт с приоритетами
- Разгон логона: замер по событиям 8000-8007 и gpsvc.log, устранение медленных CSE
- Проектирование OU-структуры и именования GPO, перевод RDS на loopback Replace
- Развёртывание Central Store, регламент бэкапа GPO и сверки с эталонным baseline
- Разбор инцидентов 1030, 1058, 1097, 1129 — от кода ошибки до устранения причины

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 Applying Group Policy troubleshooting guidance (learn.microsoft.com — 2025)

02 Group Policy processing for Windows (AD DS) (learn.microsoft.com — 2025)

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

04 Windows Installer reconfigured all applications (Win32_Product) (learn.microsoft.com — 2025)

05 Create and manage Central Store for Administrative Templates (learn.microsoft.com — 2025)

06 SYSVOL Replication Migration Guide: FRS to DFS Replication (learn.microsoft.com — 2025)

07 Microsoft Security Compliance Toolkit Guide (Policy Analyzer) (learn.microsoft.com — 2025)

08 Наш шаблон аудита GPO и регламент бэкапа политик (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.