



Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Принт-сервер и учёт печати: наводим порядок в парке МФУ офиса

Print Server на Windows Server 2022: раздача по GPO, учёт печати, SNMP-мониторинг расходников

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

Суть проблемы

В офисе 20–50 РМ печать чаще всего живёт хаосом: МФУ подключены по USB к чьим-то ПК, драйверы ставят вручную под правами админа, учёта страниц нет, тонер кончается в день сдачи отчётности. Мы переводим парк на принт-сервер Windows Server 2022: очереди централизованы, принтеры раздаются по GPO, каждое задание пишется в журнал, расходники мониторит Zabbix.

Почему это важно бизнесу

- Простой печати = простой бухгалтерии: счета, акты и ТОРГ-12 не уходят клиентам, отгрузка стоит
- Бесконтрольная печать — это 20–30% лишних страниц: личные распечатки и дубли никто не видит без учёта
- Открытый Point and Print — вектор повышения привилегий до SYSTEM на любом ПК офиса
- Внезапно кончившийся тонер — срочная закупка по розничной цене вместо плановой
- Каждый переезд сотрудника без GPO — заявка на ручную установку принтера, 30–60 минут инженера



Ключевые параметры реализации

=1

RestrictDriverInstallationToAdministrators
— установка драйверов печати
только админом

по докам Microsoft, KB5005652

307

Event ID в PrintService/Operational:
кто, что и сколько страниц
напечатал

Windows Server 2022, наш учёт печати

V4

Тип драйверов очередей: клиент не
скачивает драйвер с сервера —
очередь подключается без прав...

по докам Microsoft Print Services

15%

Порог остатка тонера в Zabbix
(prtMarkerSuppliesLevel) — покупаем
картридж до остановки печати

Printer-MIB RFC 3805 + Zabbix 7.0

5 мин

Интервал SNMP-опроса МФУ: уровни
расходников, счётчик страниц,
статус ошибок

наш стандарт мониторинга

7 дней

Период PrintBRM-экспорта
конфигурации (.printerExport) —
восстановление сервера за час

наш стандарт резервирования



Принт-сервер: консолидация очередей и драйверов

Что настраиваем

Роль Print and Document Services на Windows Server 2022; 20-50 РМ, 3-8 МФУ разных вендоров

Как мы это делаем

- 1 Ставим роль Print Server, всё управление — из printmanagement.msc: очереди, драйверы, порты и формы на одном экране
- 2 Снимаем очереди с рабочих станций, заводим порты Standard TCP/IP (RAW 9100) на статические IP МФУ из отдельной DHCP-резервации
- 3 Ставим пакетные V4-драйверы; где вендор даёт только V3 — включаем изоляцию (Set Driver Isolation → Isolated, процесс PrintIsolationHost.exe)
- 4 Переносим каталог спула с системного диска (Server Properties → Advanced → Spool Folder) и отключаем службу Spooler на контроллерах домена через GPO
- 5 Экспортируем конфигурацию PrintBrm.exe -b -f srv.printerExport по расписанию — восстановление или перенос одной командой -r

РЕЗУЛЬТАТ

Одна точка управления вместо десятка локальных установок: новая очередь появляется на всех РМ без обхода кабинетов, падение драйвера одного вендора не роняет печать всего офиса, а конфигурация сервера восстанавливается из .printerExport за час

КЛЮЧЕВОЙ НЮАНС

Смотрим в доке вендора наличие пакетного (package-aware) драйвера и заранее раскатываем его на клиентов (pnputil /add-driver или Add-PrinterDriver): при Restrict...=1 драйвер с сервера без прав админа не встанет...



Раздача по GPO и закрытие Point and Print

Что настраиваем

GPP Printers + политики Point and Print; все доменные РМ, группы доступа в AD

Как мы это делаем

- 1 Создаём группы вида PRN-Buh-Kyocera и раздаём очереди через GPP (User Configuration → Preferences → Printers) с item-level targeting по этим группам
- 2 Включаем Point and Print Restrictions: список разрешённых серверов = только наш принт-сервер, предупреждения при установке не отключаем
- 3 Держим RestrictDriverInstallationToAdministrators=1 (HKLM\...\Printers\PointAndPrint) — дефолт после KB5005652 не ослабляем
- 4 Включаем Package Point and Print — Approved servers, чтобы клиенты брали драйверы только с доверенного сервера
- 5 Для филиалов с медленным каналом включаем Branch Office Direct Printing: Set-Printer -RenderingMode BranchOffice — задания идут на МФУ напрямую

РЕЗУЛЬТАТ

Принтер «приезжает» сотруднику при входе по членству в группе AD: перевод в другой отдел = смена группы, ноль ручных установок; при этом ни один узел сети не может подсунуть рабочей станции вредоносный драйвер печати

КЛЮЧЕВОЙ НЮАНС

После KB5005652 ослабление RestrictDriverInstallationToAdministrators ради «удобства» возвращает вектор PrintNightmare; правильный путь — предустановка пакетных драйверов на клиентов + approved servers, а не о...



Учёт печати и мониторинг расходников

Что настраиваем

Журнал PrintService/Operational на сервере + Zabbix 7.0 LTS, SNMP v2c на всех МФУ

Как мы это делаем

- 1 Включаем журнал: wevtutil sl Microsoft-Windows-PrintService/Operational /e:true — по умолчанию он выключен, учёта нет
- 2 Включаем GPO «Allow job name in event logs», иначе в событии 307 не видно имени документа; увеличиваем размер журнала до 64 МБ
- 3 Скриптом собираем события 307 (пользователь, принтер, страницы) в ежемесячный отчёт по отделам
- 4 Заводим МФУ в Zabbix по SNMP: prtMarkerSuppliesLevel (OID 1.3.6.1.2.1.43.11.1.1.9) — тонер, prtMarkerLifeCount (1.3.6.1.2.1.43.10.2.1.4) — счётчик страниц
- 5 Триггеры: тонер <15% — задача на закупку, статус offline >10 мин — алерт инженеру в Telegram

РЕЗУЛЬТАТ

Руководитель видит реальные объёмы: страницы по отделам и пользователям за месяц, стоимость отпечатка по каждому МФУ; картриджи закупаются планово по алерту, а не срочно после остановки печати

КЛЮЧЕВОЙ НЮАНС

Событие 307 пишет число страниц задания, а prtMarkerLifeCount — жизненный счётчик механизма: сверяем их раз в месяц, расхождение = кто-то печатает мимо сервера, напрямую по IP



Подводные камни

✗ МФУ расшарено с ПК сотрудника

Выключил ПК — отдел без печати; очередь переезжает на сервер, МФУ получает статический IP и порт RAW 9100

✗ Зоопарк вендорских V3-драйверов

Один сбойный драйвер роняет spooler всего сервера; ставим V4/универсальные и включаем Driver Isolation (PrintIsolationHost.exe)

✗ Point and Print открыт всем серверам

Ослабление политик без списка серверов возвращает PrintNightmare; задаём approved servers и держим Restrict...=1

✗ Журнал печати выключен по умолчанию

PrintService/Operational не пишется, пока не включить wevtutil; без GPO «Allow job name in event logs» в 307 нет имени документа

✗ Spooler работает на контроллере домена

Служба печати на DC — классический вектор атаки на домен; отключаем Print Spooler на всех DC через GPO, очереди только на выделенном сервере

✗ О тонере узнаём от пользователей

Печать встаёт в день отчётности; SNMP-опрос prtMarkerSuppliesLevel каждые 5 минут и триггер 15% дают закупку заранее

✗ Спул на системном диске C:

Вал заданий забивает диск ОС и валит сервер; переносим Spool Folder на отдельный том, мониторим счётчик Print Queue\Jobs в Zabbix

✗ Нет экспорта конфигурации сервера

После сбоя очереди и драйверы восстанавливают вручную днями; еженедельный PrintBrm.exe -b даёт откат одной командой

Как правильно

МИНИМУМ

- Все очереди на принт-сервере, МФУ на статических IP, порты Standard TCP/IP
- Пакетные V4-драйверы, изоляция драйверов для остальных
- Журнал PrintService/Operational включён, размер 64 МБ
- Print Spooler отключён на контроллерах домена

НОРМАЛЬНО

- Раздача очередей через GPP по AD-группам с item-level targeting
- Point and Print: approved servers + RestrictDriverInstallation...=1
- Zabbix SNMP: тонер <15%, счётчики страниц, offline-алерты
- Еженедельный PrintBRM-экспорт .printerExport

ХОРОШО

- Ежемесячные отчёты печати по отделам из событий 307
- Branch Office Direct Printing для филиалов с тонким каналом
- Резервный принт-сервер с восстановлением из .printerExport
- Secure print на МФУ: выдача задания по PIN у аппарата

Чек-лист самопроверки

☐ Все МФУ подключены через принт-сервер, а не по USB или напрямую по IP с рабочих мест?

☐ Драйверы очередей пакетные (V4), изоляция драйверов включена для сторонних V3?

☐ RestrictDriverInstallationToAdministrators=1 и задан список approved servers?

☐ Служба Print Spooler отключена на контроллерах домена?

☐ Журнал PrintService/Operational включён и события 307 собираются в отчёт?

☐ Вы знаете, сколько страниц напечатал каждый отдел за прошлый месяц?

☐ Уровень тонера опрашивается по SNMP и алерт приходит до остановки печати?

☐ Есть свежий PrintBRM-экспорт конфигурации принт-сервера?

☐ Новому сотруднику принтеры назначаются автоматически по группе AD?

☐ Каталог спула вынесен с системного диска и очередь мониторится?

Если хотя бы на два вопроса ответ «нет» или «не знаю» — тема требует внимания.



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 парка печати за 1–2 дня: инвентаризация МФУ, счётчики, драйверы, карта очередей
- Принт-сервер под ключ: миграция очередей через PrintBRM, V4-драйверы, GPO-раздача по отделам
- Учёт печати: журнал событий 307 + ежемесячные отчёты по пользователям и отделам
- Мониторинг МФУ в Zabbix: тонер, счётчики, офлайн — алерты в Telegram
- Заккрытие PrintNightmare: политики Point and Print, изоляция драйверов, Spooler off на DC

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



Техническая база

- 01** KB5005652 — Point and Print driver installation behavior (support.microsoft.com — 2021)
- 02** Deploy printers by using Group Policy (learn.microsoft.com — WS2012R2+)
- 03** PrintBrm — резервное копирование и миграция принт-серверов (learn.microsoft.com — WS2012R2+)
- 04** Printer-MIB: prtMarkerSupplies, prtMarkerLifeCount (datatracker.ietf.org — RFC 3805)
- 05** Шаблоны SNMP-мониторинга принтеров (zabbix.com — 7.0 LTS)
- 06** Шаблон ITfresh: GPP-раздача принтеров и отчёт по событиям 307 (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.

