Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

DC виснет на логоне: переполнение Security Log на контроллере

Наш стандарт: канал журнала через GPO, чистка подкатегорий аудита, архив и мониторинг

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

Утренний пик логонов упирается в Security Log на DC: канал по умолчанию 20 МБ, в режиме Circular он перекрывается за час и аудит теряется, а в режиме Retain полный журнал даёт событие 1104 и отказ входа всем, кроме администраторов. Параллельно приходит 4612: очередь аудита LSASS исчерпана, часть событий не записана. Люди ждут вход по 3-5 минут. Мы приводим канал журнала, полит...

Почему это важно бизнесу

- Простой 40 человек по 5 минут утром — это больше 3 часов оплаченного рабочего времени в день, которых никто не планировал
- Отказ входа блокирует 1С, склад и кассу: отгрузки и приём заказов стоят до момента, пока инженер не разберёт журнал
- Потерянный аудит (событие 4612) обнуляет расследование: кто, когда и откуда заходил — восстановить уже неоткуда
- CrashOnAuditFail при невозможности записи аудита роняет DC в STOP 0xC0000244 — это не тормоза, а простой всего домена
- Без архива .evtx нечем закрыть требования по хранению журналов безопасности при проверке или при разборе инцидента

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

20 МБ

Размер Security Log по умолчанию, если политика Event Log Service не задана — наш первый чек н...

Event Log Service, политика размера канала

196608 КБ

Базовый размер канала Security по бейслайну для серверов; на DC мы поднимаем до 4194240 КБ

Security baseline Windows Server

64 КБ

Кратность MaxSize: wevtutil /ms округляет до кратного 64 КБ, минимум 1048576 байт

wevtutil, опция /ms

10 / 150

MaxConcurrentApi: дефолт на DC с WS2012 и потолок — проверяем до правок журнала

Netlogon, параметр MaxConcurrentApi

80 / 95 %

Пороги заполнения Security Log в Zabbix: warning и high с автоэкспортом .evtx

наш стандарт

60 с

Интервал съёма процента заполнения и числа событий за час агентом Zabbix

наш стандарт

Диагностика: канал журнала, источники шума, узкое место

Что настраиваем

Контроллер домена WS2019/WS2022, роль PDC-эмулятора, 40-60 учётных записей; работаем на живом DC без перезагрузки

Как мы это делаем

1. Снимаем факты: Get-WinEvent -ListLog Security → LogMode, FileSize, MaximumSizeInBytes, IsLogFull, OldestRecordNumber; события 1104, 1105, 4612, 4621 ищем в самом ка…
2. Считаем шум за час: Get-WinEvent -FilterHashtable @{LogName='Security'; StartTime=(Get-Date).AddHours(-1)} | Group-Object Id | Sort Count -Descending — топ обычно 4…
3. Разворачиваем топ-ID по учёткам: сервисные аккаунты мониторинга и WMI-опросов дают тысячи 4624 в сутки с одного источника
4. Проверяем LSA: HKLM\SYSTEM\CurrentControlSet\Control\Lsa\CrashOnAuditFail — значение 2 означает, что DC уже падал по STOP 0xC0000244
5. Снимаем счётчики Netlogon: Semaphore Waiters и Average Semaphore Hold Time — отделяем упор в журнал от упора в MaxConcurrentApi

РЕЗУЛЬТАТ

За 15-20 минут получаем цифры вместо догадок: сколько событий в час, какие ID и какие учётные записи их порождают, и упирается ли вход в ротацию журнала или в NTLM-семафор Netlogon. Дальше правим адресно, а не по принципу «увеличим лог и посмотрим».

КЛЮЧЕВОЙ НЮАНС

Пустой Security Log — не признак выключенного аудита, а следствие ротации: смотрим не содержимое, а свойства канала (LogMode, OldestRecordNumber) и события 1104/1105, которые пишутся в сам канал Security, а не…

РЕАЛИЗАЦИЯ 2 ИЗ 3

Приведение канала Security и подкатегорий аудита к стандарту

Что настраиваем

GPO Default Domain Controllers Policy на OU Domain Controllers плюс проверка канала на каждом DC домена

Как мы это делаем

1. Фиксируем точку отката: auditpol /backup /file:C:\Audit\dc-before.csv и wevtutil gl Security /f:xml до любых изменений
2. Через GPO: Event Log Service → Security → «Specify the maximum log file size (KB)» = 4194240 — это потолок политики (4 ГБ) и кратно 64
3. Там же «Control Event Log behavior when the log file reaches its maximum size» = Enabled: архив вместо перезаписи (Retention=1, AutoBackupLogFiles=1), локально — we…
4. Оставляем по бейслайну для DC: Credential Validation, User Account Management, Security Group Management, Directory Service Access и Changes, Logon, Logoff, Special…
5. Гасим шум: Filtering Platform Connection (5156) и Detailed File Share (5145) выключаем; объём 4662 режем не подкатегорией, а SACL на разделе домена; SCENoApplyLegac…

РЕЗУЛЬТАТ

Заполнение канала уходит с полутора часов на сутки и больше, файлы .evtx автоматически уезжают в архивный каталог, а не перетираются по кругу. Утренний вход в домен перестаёт зависеть от того, в какой момент LSA дошёл до конца файла журнала.

КЛЮЧЕВОЙ НЮАНС

Подкатегории работают только при включённой политике «Audit: Force audit policy subcategory settings» — иначе legacy-категории затирают тонкую настройку на следующем gpupdate.

РЕАЛИЗАЦИЯ 3 ИЗ 3

Мониторинг заполнения и вынос событий с DC

Что настраиваем

Zabbix 7.0 LTS agent на всех DC плюс коллектор WEF или нода Wazuh 4.14 на 2 vCPU / 4 ГБ RAM

Как мы это делаем

1. UserParameter на DC отдаёт процент заполнения (FileSize к MaximumSizeInBytes) и число событий за последний час, интервал 60 с
2. Триггеры: заполнение >80 % — warning, >95 % — high с автоэкспортом .evtx; отдельный триггер на всплеск свыше 50 тыс. событий в час
3. Ловим аварию: eventlog[Security,,,,4612,,skip], eventlog[Security,,,,4621,,skip], eventlog[Security,,,,1104,,skip] — все три события пишутся в канал Security
4. Выносим события с DC: подписка WEF (wecutil, режим Custom, MaxLatencyTime и HeartbeatInterval) либо агент Wazuh на контроллере
5. В Wazuh канал берём через localfile: log_format eventchannel, query с XPath Event/System[EventID != 5156 and EventID != 5145], only-future-events yes

РЕЗУЛЬТАТ

Проблема видна за дни до утреннего затыка: график заполнения канала и событий в час сразу показывает новый сервисный аккаунт или случайно включённую подкатегорию. Локальный журнал перестаёт быть единственной копией аудита — события живут и на коллекторе.

КЛЮЧЕВОЙ НЮАНС

Ключ eventlog[] работает только в активных проверках агента: при пассивном режиме элемент молча уходит в unsupported, и мониторинг журнала существует лишь на бумаге.

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **/ab:true без /rt:true**
  Автоархив требует retention=true. Иначе канал остаётся Circular и продолжает перетирать события, хотя команда отработала без ошибки.

- ✕ **MaxSize задан «красивым» числом**
  wevtutil округляет значение до кратного 64 КБ, минимум 1048576 байт, потолок политики — 4194240 КБ. Результат всегда сверяем через wevtutil gl Securi…

- ✕ **Retain без запаса на диске**
  Режим «не перезаписывать» плюс полный канал = событие 1104 и отказ входа всем, кроме администраторов. Архивный каталог кладём на отдельный том с конт…

- ✕ **CrashOnAuditFail оставлен включённым**
  При невозможности записи аудита DC уходит в STOP 0xC0000244, после восстановления ключ становится 2, пишется 4621 и вход остаётся только у администра…

- ✕ **Правка на узле вместо GPO**
  wevtutil на DC живёт до первого gpupdate: политика Event Log Service вернёт 20 МБ. Размер и режим фиксируем в GPO на OU Domain Controllers.

- ✕ **1104 ищут в журнале System**
  1104 и 1105 пишет провайдер Microsoft-Windows-Eventlog в канал Security. Фильтр по System не даёт ничего, и переполнение считают несуществующим.

- ✕ **Чистка журнала без экспорта**
  wevtutil cl без /bu уничтожает аудит безвозвратно и порождает 1102. Сначала epl в .evtx с датой в имени, только потом очистка канала.

- ✕ **Лечим журнал, а тормозит Netlogon**
  Если Semaphore Waiters стабильно больше нуля, вход упирается в MaxConcurrentApi, а не в аудит — увеличение размера канала тут не даст ничего.

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- Security Log на DC не меньше 1 ГБ, режим Circular, размер задан через GPO
- Ежедневный экспорт .evtx (wevtutil epl) в отдельный каталог с датой в имени файла
- Проверены CrashOnAuditFail и отсутствие событий 1104, 4612, 4621 в канале Security
- Топ-10 источников событий за час снят и записан в паспорт домена

НОРМАЛЬНО

- Канал 4194240 КБ, /rt:true /ab:true, AutoBackupLogFiles=1, архив на отдельном томе
- Advanced Audit Policy в GPO DC, 5156 и 5145 выключены, SACL на разделе домена сужен
- Zabbix-агент отдаёт заполнение и события в час, пороги 80 и 95 %
- Учтены сервисные аккаунты: кто и с какой частотой опрашивает DC

ХОРОШО

- WEF-подписка или агент Wazuh: события уезжают с DC в течение минуты
- Алерты на 4740, 4728, всплеск 4625 и на 1102/1104 с эскалацией дежурному
- Срок хранения архивов .evtx задан регламентом, чтение архива проверено
- Ежеквартальный пересмотр подкатегорий аудита и лимитов каналов

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Знаете ли вы размер и режим (Circular/AutoBackup/Retain) Security Log на каждом контроллере домена?
- [ ] Задан ли размер журнала политикой GPO, а не разовой командой на конкретном узле?
- [ ] Настроен ли автоархив .evtx и хватает ли места на томе под архивный каталог?
- [ ] Известен ли топ-5 учётных записей по числу событий 4624 за один час?
- [ ] Выключены ли шумные подкатегории 5156 и 5145 и сужен ли SACL, дающий поток 4662?
- [ ] Включена ли политика принудительного применения подкатегорий аудита на DC?
- [ ] Есть ли в мониторинге процент заполнения журнала с порогами 80 и 95 %?
- [ ] Проверялись ли CrashOnAuditFail и наличие 1104, 4612, 4621 именно в канале Security?
- [ ] Уезжают ли события безопасности с DC во внешний коллектор WEF или SIEM?
- [ ] Отделены ли тормоза журнала от узкого места Netlogon по Semaphore Waiters?

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 контроллеров домена: каналы, подкатегории, источники шума — письменный отчёт с планом правок
- Настройка каналов Security и System через GPO с автоархивом и контролем свободного места
- Мониторинг DC в Zabbix: заполнение журнала, события в час, отклик LSASS, алерты в Telegram
- Централизованный сбор событий: коллектор WEF или Wazuh на отдельной ноде под ключ
- Регламент хранения и проверки архивов .evtx под требования внутренних и внешних проверок

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 System Audit Policy recommendations (AD DS) (learn.microsoft.com — 2025)

02 wevtutil: set-log /ms /rt /ab, export-log, clear-log (learn.microsoft.com — 2026)

03 EventLogService Policy CSP: размер и поведение канала Security (learn.microsoft.com — 2025)

04 Audit: Shut down system immediately if unable to log security audits (learn.microsoft.com — 2025)

05 События 1102, 1104, 4612, 4621 — справочник аудита безопасности (learn.microsoft.com — 2025)

06 MaxConcurrentApi: identify and remediate MCA issues (learn.microsoft.com — 2025)

07 Zabbix agent, Windows-ключ eventlog[] (только активные проверки) (zabbix.com — 7.0 LTS)

08 Wazuh: localfile, log_format eventchannel, query и only-future-events (documentation.wazuh.com — 4.14)

09 Наш шаблон аудита DC: чек-лист каналов и подкатегорий (itfresh.ru — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.