Ай-ТИ Фреш

ТЕХНИЧЕСКИЙ РАЗБОР

Мониторинг Active Directory в Zabbix: DC и брутфорс раньше юзеров

Как мы ловим падение контроллера домена и подбор пароля учётки за минуты, а не по жалобе

Июль 2026

itfresh.ru · ИТ-аутсорсинг для юридических лиц

О ЧЁМ ЭТОТ РАЗБОР

Суть проблемы

У заказчика 1-2 контроллера домена держат вход в 1С, почту, файловые шары и VPN. Падение DC или подбор пароля админской учётки обычно вскрывается по звонку офиса «всё легло» или по факту блокировки бухгалтера в разгар отчётности. Мы разворачиваем Zabbix 7.0 LTS с шаблоном Windows by Zabbix agent + eventlog-мониторингом Security-журнала, чтобы алерт приходил раньше пользователя.

Почему это важно бизнесу

- Простой DC на 20-50 РМ = остановка 1С, почты и файловых шар одновременно
- Подбор пароля админской учётки обнаруживается постфактум, когда аккаунт уже скомпрометирован
- Массовые блокировки учёток в 9:00 воспринимаются как «сломался офис», а не как атака
- Аудит подрядчика/страховой требует доказуемого контроля инцидентов ИБ, а не «мы заметили сами»
- Ручной просмотр Event Viewer на 2-3 DC не масштабируется дальше 1 админа

ЧТО МЫ ЗАКЛАДЫВАЕМ

Ключевые параметры реализации

≤60 сек

интервал активных проверок eventlog на DC в нашей конфигурации

наш стандарт внедрения

4625/4771

порог: 5 событий 4625/4771 от одного источника за 10 минут = алерт

наш стандарт внедрения

2 канала

Telegram + email эскалация дежурному инженеру по одному триггеру

наш стандарт внедрения

4 ID

события 4625, 4740, 4771, 4768 — ядро нашего eventlog-мониторинга DC

learn.microsoft.com, 2026

30 дней

минимальный размер журнала Security на DC под наш ретеншн триггеров

наш стандарт внедрения

РЕАЛИЗАЦИЯ 1 ИЗ 3

Скрытый подбор пароля сервисной учётки 1С

Что настраиваем

Производственная компания, 45 рабочих мест, 2 DC на Windows Server 2019

Как мы это делаем

1. Развернули Zabbix agent2 на обоих DC, включили active checks на Security-журнал
2. Добавили item eventlog[Security,,,,4771,,skip] и триггер find() с порогом 5 событий за 10 минут
3. На 4-й день триггер сработал по сервисной учётке 1С-сервера с внешнего IP через VPN-шлюз
4. Сменили пароль учётки, включили Kerberos armoring, ограничили logon workstations
5. Настроили LLD-дискавери сервисов netlogon/kdc/ntds для авто-мониторинга после патчей

РЕЗУЛЬТАТ

Подбор пароля пойман на этапе перебора, до фактической компрометации; учётка не успела попасть в руки атакующего, простоя 1С не было

КЛЮЧЕВОЙ НЮАНС

Событие 4771 (Kerberos pre-auth failed) ловит перебор раньше, чем накопится порог блокировки в 4740 — при Kerberos-входе неудачные попытки видны сразу, ещё до лока

РЕАЛИЗАЦИЯ 2 ИЗ 3

Падение единственного DC в филиале

Что настраиваем

Торговая сеть, 30 PM в головном офисе + филиал на 8 PM

Как мы это делаем

1. Обнаружили единственный DC в филиале без мониторинга доступности служб
2. Добавили net.tcp.service[ldap,,389] и net.tcp.port[,88] с интервалом 30 сек
3. Настроили триггер nodata() на agent.ping и count() по недоступности LDAP 3 проверки подряд
4. DC завис из-за нехватки RAM под NTDS.dit кэш — алерт ушёл через 90 секунд после сбоя
5. Перезапустили DC удалённо до жалоб пользователей, добавили триггер на свободную RAM и рабочий набор lsass.exe

РЕЗУЛЬТАТ

Инцидент закрыт за 12 минут вместо обычных 40-60 минут при обращении по телефону, филиал не заметил простоя

КЛЮЧЕВОЙ НЮАНС

Для DC мало ping — нужен контроль конкретных служб (LDAP 389, Kerberos 88, DNS 53), потому что процесс может жить, а служба уже не отвечает

РЕАЛИЗАЦИЯ 3 ИЗ 3

Массовая блокировка учёток бухгалтерии перед сдачей отчётности

Что настраиваем

Логистическая компания, 38 PM, домен на 2 DC

Как мы это делаем

1. Клиент жаловался на регулярные блокировки 3-4 учёток бухгалтерии по утрам
2. Включили Advanced Audit Policy: Account Logon + Account Lockout на Default Domain Controllers Policy
3. Настроили eventlog[Security,,,,4740] и корреляцию с 4625 по полю Caller Computer Name
4. Нашли источник: старый терминал с сохранённым старым паролем к общей учётке в планировщике
5. Настроили LLD по discovery учётных записей с интервалом обновления списка раз в сутки

РЕЗУЛЬТАТ

Источник блокировок найден за один инцидент вместо недель гипотез, повторных блокировок не было

КЛЮЧЕВОЙ НЮАНС

Без Caller Computer Name в 4740 расследование зависает — событие часто приходит с DC, а не с источника, поэтому нужна корреляция с 4625

ЧТО МЫ ВЫУЧИЛИ НА ПРАКТИКЕ

Подводные камни

- ✕ **Мониторят только ping DC**
  ICMP жив, а LDAP/Kerberos/DNS уже не отвечают — нужны net.tcp.service[ldap] на 389 и net.tcp.port на 88/445 плюс net.dns на 53
- ✕ **Audit Policy не включена под Advanced**
  Legacy audit policy не пишет 4771/4768 в нужном разрезе — нужны Advanced Audit Policy Configuration подкатегории
- ✕ **Триггер на одно событие 4625**
  Один неверный пароль — это норма; триггер должен считать count() за окно, а не реагировать на первое совпадение
- ✕ **Нет skip в eventlog[]**
  Без параметра skip агент при рестарте перечитывает старые записи и шлёт ложные алерты по событиям недельной давности
- ✕ **Забыли про ротацию журнала Security**
  Маленький MaxSize журнала на DC с высокой нагрузкой перезаписывает события 4771/4768 быстрее интервала опроса Zabbix
- ✕ **Один DC без резервного мониторинга**
  Если Zabbix proxy стоит на том же DC, что и мониторится, падение DC гасит и сам алерт
- ✕ **Нет эскалации по каналам**
  Алерт только в веб-интерфейс Zabbix никто не видит ночью — нужна связка Telegram/email с action-эскалацией
- ✕ **Игнорируют 4776 при NTLM-переборе**
  Легаси-клиенты используют NTLM вместо Kerberos, и без 4776 (проверка учётных данных NTLM) перебор через NTLM останется невидимым

УРОВНИ РЕАЛИЗАЦИИ

Как правильно

МИНИМУМ

- agent.ping + net.tcp.service[ldap] на каждый DC с интервалом 30-60 сек
- eventlog[Security,,,,4625,,skip] с триггером count() >=5 за 10 минут
- Telegram-уведомление дежурному по триггеру severity High и выше
- Включить Advanced Audit Policy: Account Logon, Account Lockout, Kerberos Auth Service

НОРМАЛЬНО

- Добавить 4740, 4771, 4768 с корреляцией по Caller Computer Name/IP
- LLD-дискавери служб netlogon, kdc, dns, ntds с авто-триггерами по состоянию
- Раздельные проверки net.tcp.service[ldap,,389] и net.tcp.port[,88] для Kerberos отде…
- Ретеншн истории 90 дней и трендов 365 дней для расследования инцидентов задним числом

ХОРОШО

- Zabbix proxy в каждой изолированной локации, DC вне зоны его же мониторинга
- SIEM-выгрузка событий 4625/4740/4771/4768 в дополнение к Zabbix для форензики
- Дашборд по topology: DC, FSMO-роли, DFS-репликация, DHCP на одном экране NOC
- Плейбук авто-реакции: блокировка внешнего IP при триггере брутфорса через API

ПРОВЕРЬТЕ У СЕБЯ

Чек-лист самопроверки

- [ ] Zabbix agent2 установлен и активные проверки включены на всех DC
- [ ] net.tcp.service[ldap] на 389 и net.tcp.port[,88] на Kerberos настроены отдельно
- [ ] Advanced Audit Policy Configuration включена на Default Domain Controllers Policy
- [ ] eventlog[] items используют параметр skip для исключения исторических записей
- [ ] Триггеры считают count()/find() за окно, а не по единичному событию
- [ ] 4625/4740/4771/4768 покрыты отдельными item и триггерами с разными порогами
- [ ] Каналы эскалации Telegram/email проверены реальным тестовым триггером
- [ ] Zabbix proxy или сервер не совмещён физически с единственным DC
- [ ] Ретеншн истории и журнала Security достаточен для расследования постфактум
- [ ] LLD для служб netlogon/kdc/dns/ntds настроен и не шумит после патчей

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).

- Разворачиваем Zabbix 7.0 LTS и шаблон Windows by Zabbix agent под контроллеры домена клиента
- Настраиваем Advanced Audit Policy и eventlog-мониторинг Security-журнала под 4625/4740/4771/4768
- Считаем и калибруем пороги триггеров под реальную нагрузку конкретного домена без ложных алертов
- Подключаем эскалацию в Telegram/email с дежурством инженера ITfresh на инциденты ИБ
- Ведём инцидент от алерта до отчёта: кто, с какого IP и по какой учётке пытался подобрать пароль

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 Monitor Windows event log using active checks (zabbix.com — 2026)

02 Windows-specific item keys (eventlog, net.tcp.service, net.tcp.port) (zabbix.com — 2026)

03 Windows by Zabbix agent / agent2 templates (git.zabbix.com — 2026)

04 4740(S) A user account was locked out (learn.microsoft.com — 2026)

05 4771(F) Kerberos pre-authentication failed (learn.microsoft.com — 2026)

06 4625(F) An account failed to log on (learn.microsoft.com — 2026)

07 Advanced Security Audit Policy Settings (learn.microsoft.com — 2026)

Основано на официальной документации продуктов и нашей практике внедрения.