KILDNS

# Руководство по использованию и администрированию

Версия 2.0.6

# Оглавление

# О решении

KvilDNS помогает просматривать все входящие DNS-запросы к DNS-серверам и анализировать их, чтобы облегчить обнаружение заражённых устройств. Он предлагает множество функций, которые повышают эффективность средств мониторинга и защиты, например: обнаружить домены, которые были посещены впервые в вашей сети, проаудировать эффективность других решений, занимающихся фильтрацией трафика, а расширенный интерфейс отчётности помогает идентифицировать скомпрометированные системы. Внедрение KvilDNS позволяет выявлять IP-адреса, имена хостов и пользователей, отправляющих запросы к вредоносным доменам, в том числе то, что попадает в слепую зону для МЭ нового поколения или других традиционных решений сетевой безопасности, с архитектурой основанной на сигнатурах, списках репутаций и CTI.

**Что такое DNSWatch?**

DNSWatch – это виртуальная машина, устанавливаемая на вашем гипервизоре во внутренней сети компании и отвечающая за сбор и локальную корреляцию анализ журналов событий. После установки будет необходимо указать корпоративные DNS-серверы в качестве источников журналов событий и/или перенаправлять такие журналы любым решением, поддерживающим отправку данных в формате Syslog. Обнаруженные в этих журналах доменные имена будут категоризированны движком KvilDNS, а полученный результат будет учтён в рамках анализа и корреляции.

**Как работает KvilDNS?**

KvilDNS анализирует каждую запись журнала событий сервиса DNS с учётом исходного IP-адреса, запрашиваемого домена и временной метки. Домен будет проанализирован и отнесён к определённой категории. Если функция “Обогащение” включена, в журнал будет добавлена информация об исходном пользователе, имени хоста и прочие детали вплоть до имени процесса, инициировавшего запрос. Журналы DNS-серверов Microsoft, могут быть импортированы с помощью протоколов SMB или WMI. Для получения журналов с прочих DNS серверов, KvilDNS может получать и анализировать журналы в формате Syslog.

# Типовые решаемые задачи

## Повышение уровня защищённости сети и защита от 0-day атак

KvilDNS обеспечивает:

- комплементарную защиту к существующим решениям NTA, NGFW, NAD/IPS;
- полную видимость DNS-трафика, включая DNS-over-TLS и DNS-over-HTTPS, что позволяет контролировать все запросы к DNS-серверам;
- роль межсетевого экрана уровня приложений, который блокирует угрозы в DNS-трафике;
- отслеживание и анализ исходящих DNS-запросов, для выявления подозрительной активности и предотвращения атак, связанные с использованием DNS протокола;
- детектирование и блокировку любых DNS-туннелей (не только широко известных средств, типа iodin, но и совершенно произвольных, самописных, включая сверхмедленные реализации туннелей).

### Устранение слепой зоны средств сетевой защиты

Решение будет полезно для усиления средств обеспечения безопасности сети и защиты от киберугроз нулевого дня для обеспечения непрерывности функционирования бизнес-процессов

## Реализация функционала DNS-фильтрации

KvilDNS обеспечивает:

- блокировку вредоносных ресурсов: KvilDNS блокирует доступ к ресурсам с вредоносным ПО, что предотвращает заражение устройств сотрудников и защищает от возможных кибератак, обеспечивает непрерывность работы сотрудников;
- защита от фишинговых атак: KvilDNS предотвращает переход сотрудников по фишинговым ссылкам, которые могут привести к краже личных данных или установке вредоносного ПО на устройства. Это нивелирует эффективность техник социальной инженерии, снижает риск финансовых потерь и обеспечивает безопасность корпоративной информации;
- соблюдение корпоративных политик доступа в интернет: KvilDNS позволяет настроить политики доступа в интернет, чтобы сотрудники могли получать доступ только к разрешённым сайтам и сервисам. Это помогает поддерживать корпоративную культуру и обеспечивать соблюдение внутренних правил и норм.

### Обеспечение непрерывной и безопасной работы сотрудников

Решение будет полезно для обеспечения непрерывной работы сотрудников, повышения дисциплины использования интернет-ресурсов и уменьшения числа обращений в службу технической поддержки

## Оптимизация работы SOC и обогащение SIEM

KvilDNS обеспечивает:

- оптимизацию работы SOC: благодаря предварительной фильтрации и корреляции DNS-событий, значительно сокращается объём событий связанных с DNS протоколом, требующих анализа в системе SOC (уменьшение от 98%). Это позволяет снизить нагрузку на специалистов и повысить эффективность их работы;
- улучшение качества мониторинга: Сотрудник SOC или SIEM аналитик фокусируется только на действительно важных событиях, связанных с потенциальными угрозами безопасности. Это позволяет оперативно реагировать на инциденты и предотвращать возможные атаки;
- повышение эффективности SIEM: Система SIEM теперь получает уже скоррелированные и обогащённые из журналов DHCP, AD, XDR данные об инцидентах связанных с DNS протоколом. Это упрощает процесс анализа данных и принятия решений, а также сокращает время, затрачиваемое на обработку информации;
- экономическая выгода: Сокращение нагрузки на SOC и оптимизация процессов позволяют сэкономить ресурсы компании, такие как время и человеческие усилия. Это может привести к снижению затрат на обеспечение безопасности и повышению общей эффективности работы организации.

Повышение функциональной и экономической эффективности SOC

Решение будет полезно для получения готовой аналитики по инцидентам, связанным с распространением вредоносного ПО, использования ботнетов, руткитов и т.п.

# Готовимся к установке

## Системные требования

Для использования продукта DNSWatch необходимо скачать образ виртуальной машины. Получить актуальный образ виртуальной машины можно обратившись в службу технической поддержки по адресу support@kvildns.ru

Минимальные необходимые ресурсы для импорта виртуальной машины DNSWatch:

- 8 CPU
- 32 GB RAM
- 500GB SSD/HDD

Виртуальная машина с данными параметрами рекомендована для обслуживания инфраструктуры до 5000 хостов.

Для интерфейса управления необходимо зарезервировать 1 статический адрес в корпоративной сети. С этого адреса для DNSWatch должны быть доступны следующие ресурсы в Интернет по TCP-портам 80(http) и 443(https):

- reputation.kvildns.ru
- registry.kvildns.ru
- securitygap.klivdns.ru
- portal.kvildns.ru
- sgap.kvildns.ru
- xray.kvildns.ru

При использовании в корпоративной сети прокси-сервера, аутентификация для управляющего IP-адреса DNSWatch должна быть отключена.

Если журналы DNS и/или DHCP собираются с серверов Microsoft, следует включить ведение журнала отладки (для DNS серверов, см. далее), и обеспечить доступ с управляющего адреса DNSWatch по TCP-порту 445 (SMB) до этих серверов. В сценарии с серверами Microsoft, также потребуется локальный или доменный пользователь, от имени которого DNSWatch будет подключаться и забирать журналы.

В случае не Microsoft инфраструктуры, DNS и/или DHCP журналы направляются на с управляющий адреса DNSWatch по Syslog, соответствующий трафик должен быть разрешён на уровне сети.

## Масштабирование

Указанных выше минимальных требований будет достаточно для инсталляции в инфраструктуре, содержащей до 5 тыс. хостов. Хост – это любое устройство, которое отправляет DNS-запросы: рабочая станция, сервер, сетевое оборудование, IoT, CCTV и т.п.

В случае большего количества ресурсов вам следует обратиться в службу поддержки для оптимизации вашего KvilDNS.

## Лицензирование

Лицензия KvilDNS рассчитывается на основе количества ресурсов, отправляющих запросы DNS. Среднее количество ресурсов можно увидеть на вкладке “Лицензии”. Это число рассчитывается ежедневно.

# Архитектура решения

**DNSWatch** – это виртуальная машина, устанавливаемая на гипервизоре во внутренней сети компании и отвечающая за сбор и локальную корреляцию анализ журналов событий. После установки использует корпоративные DNS-серверы в качестве источников журналов событий и/или перенаправлять такие журналы любым решением, поддерживающим отправку данных в формате Syslog. Обнаруженные в этих журналах доменные имена будут категоризированны движком DNSLab, а полученный результат будет учтён в рамках анализа и корреляции.

**DNSCube** – публичная сеть DNS серверов, обеспечивающих высокую доступность сервиса, быстрый отклик и фильтрацию исходящих из DNS запросов в зависимости от применённой пользователем политики.

**DNSLab** – движок категоризации, встроенный в инфраструктуру серверов DNSCube и отвечающий за принятие решения по категоризации каждого отдельного домена.


- **Облачная защита (РФ)**
- **Защита от DNS-туннелирования на основе искусственного интеллекта**
- **Защита от вредоносных программ, программ-вымогателей, фишинга и прочей заразы**
- **Наличие клиентов для мобильных пользователей**
- **Интеграция с XDR через DNSWatch**
- **Интеграция с SOAR/SIEM**

Обеспечивает расширенный уровень защиты от известных и неизвестных угроз.

DNSCube

- **Эффективное обнаружение аномалий в трафике**
- **Автоматизированное реагирование на инциденты**
- **Ускорение расследований инцидентов**
- **Автоматическое обогащение данных**
- **Интеграция с EDR/XDR**
- **Снижение ложных сигналов тревоги**
- **Идентификация слепых зон защиты**

Позволяет разобраться в журналах DNS и усилить аналитикой команду SOC

DNSWatch

- **Классификация доменов на основе искусственного интеллекта**
- **100% автоматизация**
- **Результат за 2 секунды, без участия человека**
- **Аналитика киберугроз**
- **Отслеживание и анализ всего Интернета**

Уникальная эффективность классификации за счёт использования ИИ и машинного обучения.

DNSLab

# Сценарии внедрения

## Сценарий "Аналитика"

В данном сценарии не используется компонент DNSCube, как следствие активная защита и блокировка подозрительной активности невозможна. Данный сценарий может являться как первым этапом полноценного разворачивания системы KvilDNS, так и использование системы KvilDNS с целью усиления SIEM и SOC. Данный сценарий позволяет получить полную картину всей сетевой активности с внешними адресатами и информацию о потенциальном горизонтальном распространении заражения вредоносным ПО. В рамках данного сценария DNSWatch может быть интегрирован с DNS, DHCP, AD и XDR для сбора и обогащения логов, а также SIEM для передачи итогов работы аналитики. При этом DNSWatch не влияет на прохождение трафика, а лишь читает журналы событий и/или получает из по Syslog

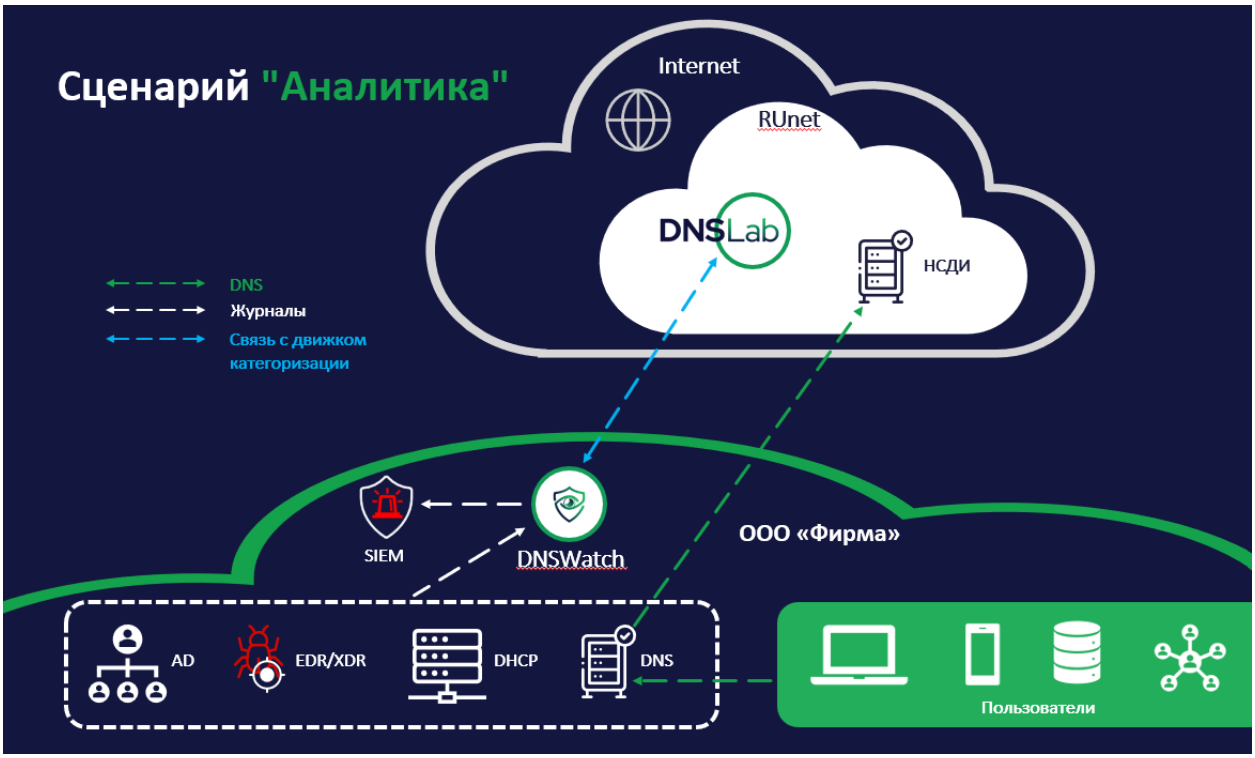


*Рисунок 1 – Сценарий "Аналитика"*

## Сценарий "Аналитика и Защита"

Данный сценарий полностью аналогичен описанному выше, но добавляется компонент активной защиты – DNSCube. Для реализации данного сценария, потребуется внесение изменений в конфигурацию корпоративных DNS серверов компании в части изменения, используемого ими вышестоящего DNS. Все исходящие DNS запросы должны адресоваться на сервера DNSCube. Это позволит реализовать активную защиты, появится возможность фильтрации днс запросов как по назначаемым пользователем критериям, так и на основе внутренних алгоритмов выявления манипуляций и атак с использованием DNS протокола (например, выявление и блокировка DNS-туннелирования, DGA доменов и т.п.).

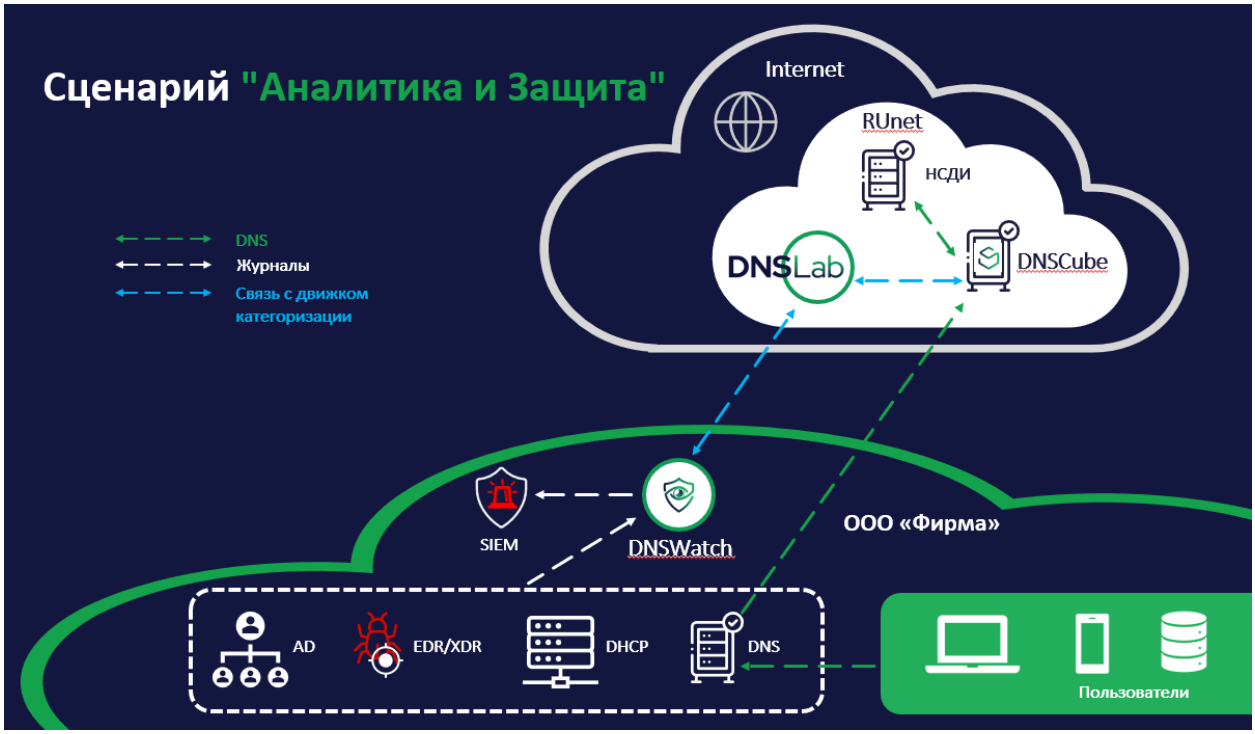


*Рисунок 2 – Сценарий "Аналитика и Защита"*

# Инициализация DNSWatch

Перед началом первого использования DNSWatch, необходимо провести ряд действий по его инициализации и первичной настройки. Подробные инструкции даны в руководстве администратора KvilDNS. Данный список действий включает:

- первичную инициализацию и назначение новых паролей от системных учётных записей;
- установку лицензии;
- обновление ПО до последней актуальной версии.

По завершению первичной настройки системы можно перейти к настройке источников журналов (как минимум с DNS и DHCP сервисов) и эксплуатации.

## Первый запуск

Импортируйте образ виртуальной машины в среду виртуализации. По завершению импорта необходимо провести инициализацию её сетевых настроек. Для этого пройдите на локальную консоль виртуальной машины, аутентифицируйтесь (admin/dnswatch, рекомендуется сменить данный пароль после первого использования) и следуйте мастеру настройки. Минимально необходимая конфигурация: назначить адрес и сетевые параметры на интерфейс управления, указать часовой пояс и время. После завершения конфигурирования и автоматического перезапуска служб, станет доступна WEB-консоль на назначенном адресе интерфейса управления. Аутентифицируйтесь в ней (admin/admin), установите новый пароль администратора и можно приступать к настройкам системы.

В последствии, при необходимости изменить сетевые настройки или пароли, это можно сделать в локальной консоле или подключившись по SSH и повторно пройдя визард.

## Установка лицензии

Перед конфигурацией DNSWatch, необходимо импортировать лицензионный ключ. Ключ можно скачать из кабинета пользователя на https://portal.kvildns.ru. Для этого аутентифицируетесь на https://portal.kvildns.ru и следуйте инструкции ниже.

Если вы ещё не зарегистрированы на портале KvilDNS, то перейдите на страницу https://portal.kvildns.ru/#/register и пройдите регистрацию. После подтверждения почтового адреса (он должен принадлежать корпоративной почте) появится возможность сгенерировать API ключ, выполняющий роль лицензии для DNSWatch.

Генерация лицензионного ключа:

1. Нажмите кнопку «Меню» ( ≡ )
2. Выберите раздел «Настройки»
3. Выберите раздел «Ключи API»
4. Нажмите кнопку «Создать новый API ключ» и выберете тип ключа «reputation»

Импорт ключа в DNSWatch:

1. Нажмите кнопку «Меню» ( ≡ )

2. Выберите раздел «Система»
3. Выберите раздел «Лицензия»
4. Нажмите кнопку «Добавить лицензионный ключ»
5. Вставmте ключ типа «Reputation» в поле Репутация и сохраните
6. Вы должны увидеть статус лицензионного ключа, отмеченный зелёным индикатором

## Обновление ПО

После ввода лицензионного ключа рекомендуется обновиться до последней актуальной версии.

**Порядок действий**

1. Нажмите кнопку «Меню» (  )
2. Выберите раздел «Система»
3. Выберите раздел «Обновление ПО»
4. Выберете последнюю доступную версию и нажмите кнопку «Установить»
5. После загрузки обновлений и их установки система самостоятельно перезагрузится.
6. По окончанию загрузки система готова к конфигурированию

# Конфигурирование DNSWatch

Для начала использования DNSWatch необходимо произвести настройки источников журналов. Подключить все источники и произвести их настройку можно в «Меню», в разделе «Настройки». Здесь вы также можете настроить отправку данных на сервер Syslog или в SIEM.

## Настройки источников журналов DNS

Для старта работы системы необходимо добавить, как минимум один источник журналов DNS. Корректная работа системы возможна только при получении журналов со всех DNS-серверов компании. На выбор доступно несколько вариантов подключения источников.

**Порядок действий**

1. Нажмите кнопку «Меню» ( )
2. Выберите раздел «Источник журналов DNS»
3. (Опционально) Нажмите кнопку «Настройки»

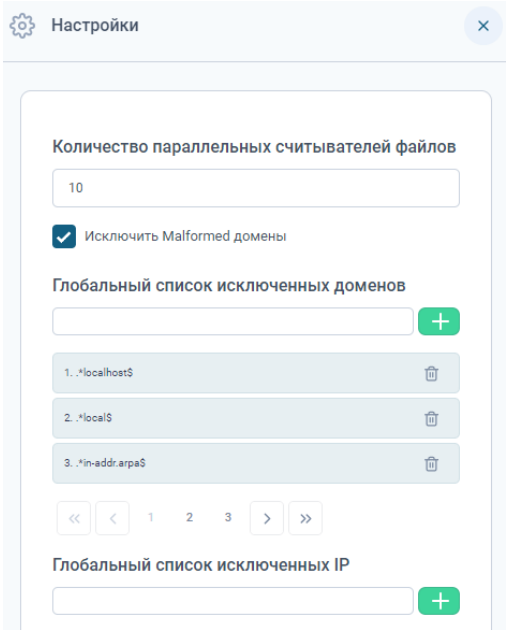


*Рисунок 3 – Глобальные настройки DNS журналов*

Параметр «Количество параллельных считывателей файлов»: это количество источников, которые будут опрашиваться одновременно. В случае возникновения каких-либо задержек вы можете увеличить это число. Обратите внимание, что при увеличении этого числа будет использоваться больше ресурсов процессора и памяти. Если вам необходимо изменить это значение, рекомендуется сначала обратиться в службу поддержки.

Поле «Глобальный список исключённых доменов»: список доменов, которые будут исключены из анализа, информация по ним не будет собираться, они не попадут в отчёты и движок корреляции. Рекомендуется добавить сюда ваши безопасные внутренние домены, например, локальные домены.

Поле «Глобальный список исключённых IP»: указанные здесь адреса будут игнорироваться при чтении журналов, они будут исключены из анализа, информация по ним не будет собираться, они не попадут в отчёты и движок корреляции. Рекомендуется добавить сюда адреса устройств DNS-запросы, которых не представляют интереса для

анализа и/или могут искажать накапливаемые данные, например песочницы, Wi-Fi точки с гостевыми сегментами, неумеющие доступа к внутренней сети.
Сохраните изменения, нажав «Сохранить».

4. Нажмите кнопку «Добавить источник», чтобы добавить источники журналов DNS. Дальнейшие шаги зависят от типа используемого DNS сервера, ниже рассмотрим два варианта Microsoft и произвольный *nix-based. Все остальные опции, такие как F5, Infoblox, NetScaler и Bind, будут использовать Syslog с преднастроенными параметрами, такие DNS-сервера должны отправлять Syslog на IP-адрес управления DNSWatch.

**Конфигурация источника на базе DNS-сервера Microsoft**

Если вы используете DNS-сервер Microsoft, предварительно необходимо активировать журнал отладки, как представлено на рисунке ниже.

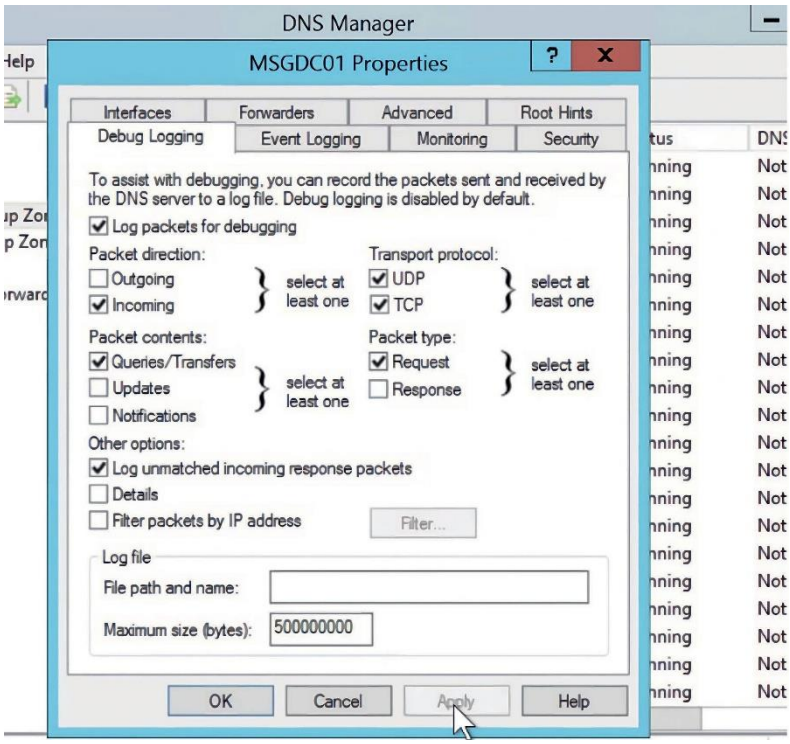


*Рисунок 4 – Включение журнал отладки Microsoft DNS сервера*

Журналы отладки Windows хранятся в c:\windows\system32\dns. Если вы хотите изменить этот каталог, вам необходимо ввести новое имя журнала и путь к нему в поле “Путь к файлу и имя” (например, c:\dnslog\dns.log). Журналы могут быть импортированы через SMB (File Share) или WMI протоколы.

**Порядок действий**

1. «Имя»: указать название вашего источника. Это то, как он будет отображаться в интерфейсе.
2. Источник DNS журналов– Microsoft DNS: уже будет выбран по умолчанию. Microsoft DNS может быть интегрирован по SMB (является рекомендованным способом) или по WMI. WMI следует использовать только в случае отсутствия возможности подключиться по SMB, т.к. его использование требует существенных ресурсов (одно ядро CPU может обрабатывать до 350 QPS).
3. При конфигурировании SMB:

- предоставьте общий доступ к папке с журналами DNS выделенному под эту задачу пользователю (доменному или локальному). Папка может быть доступна только для чтения. Пример конфигурации на рисунке ниже.

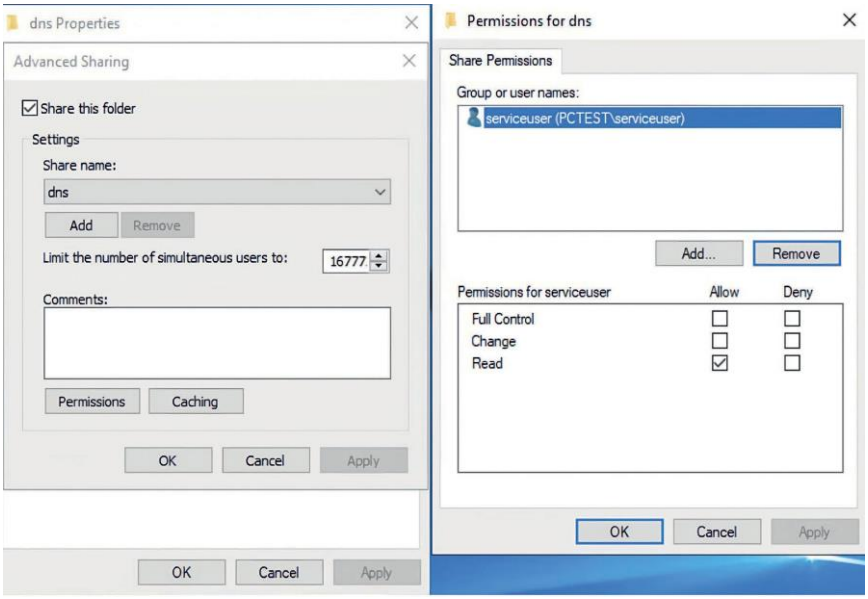


*Рисунок 5 – Предоставление доступа к журналам отладки Microsoft DNS сервера*

- в поле «hostname or IP/share name» необходимо указать имя хоста или IP и имя папки общего доступа. Обратите внимание на знак разделителя «/»
- выбрать «Учётные данные». Если учётных данных не было заведено ранее, необходимо их добавить, нажав «Добавить учётные данные»
- выбрать формат даты для журналов DNS-сервера. Формат даты, можно заранее посмотреть на DNS-сервере или сделать это в интерфейсе DNSWatch (для этого необходимо завершить настройку и нажать на значок в виде глаза. вы увидите сырые журналы, как их прочитала система).
- выбрать часовой пояс
- выбрать способ работы с файлом журнала.
  Truncate: файл журнала отладки Microsoft DNS сокращается до заданного предела, и журналы записываются в тот же файл.
  Rotate: когда файл журнала отладки Microsoft DNS достигает предела, создаётся новый файл, и журналы продолжают записываться в этот новый файл. Рекомендуется использовать «Truncate» с буфером 480 МБ.

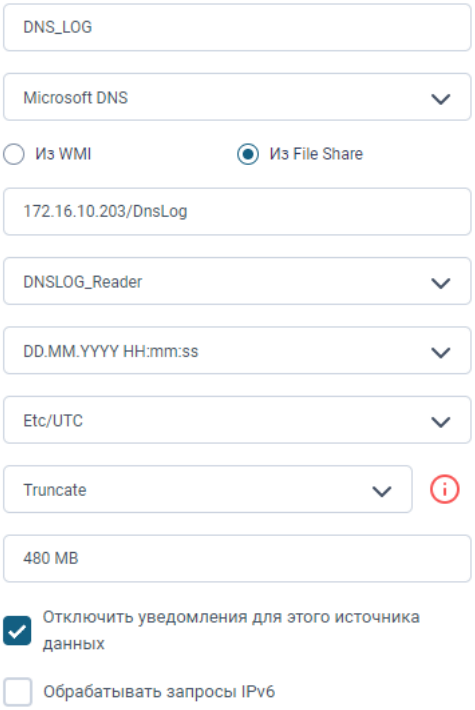


*Рисунок 6 – Настройки SMB*

4. При конфигурировании WMI:
   - указать имя хоста WMI или IP
   - выбрать «Учётные данные». Если учётных данных не было заведено ранее, необходимо их добавить, нажав «Добавить учётные данные»

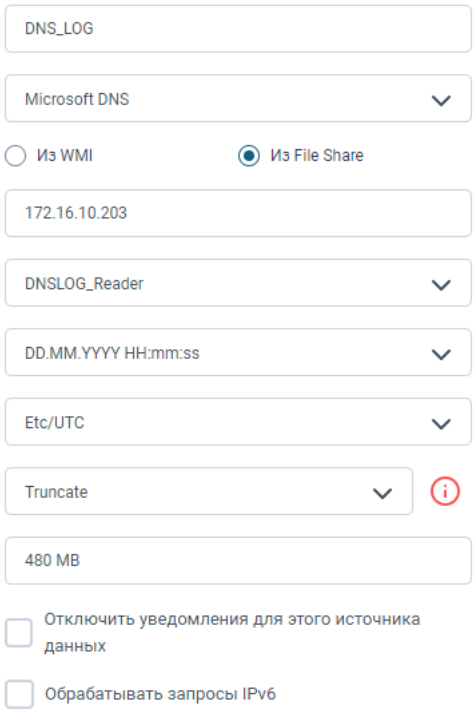


*Рисунок 7 – Настройки WMI*

5. Опция «Отключить уведомления для этого источника данных» отключит получение уведомлений об отсутствии журналов от источника за последний час.

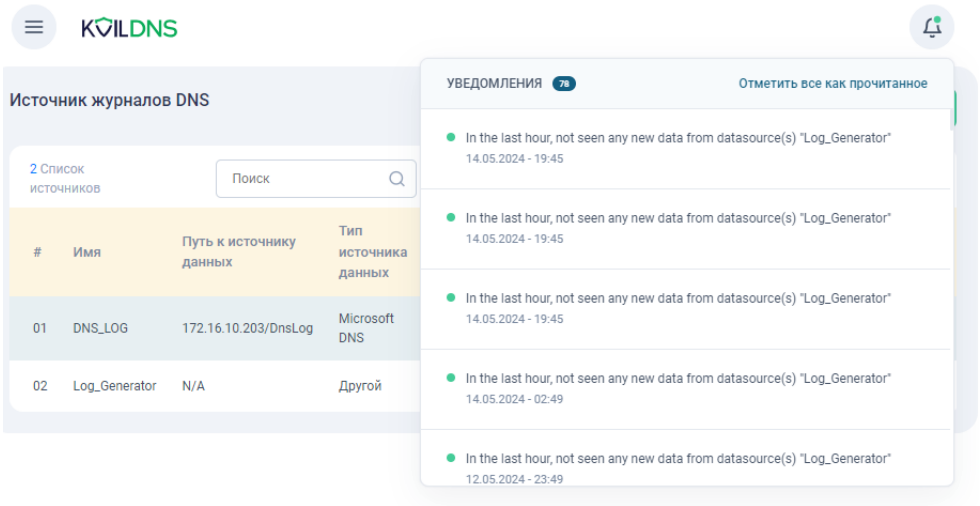


*Рисунок 8 – Пример уведомлений об отсутствии новых сообщений в журналах источника*

**Конфигурация для источника на базе *nix DNS-сервера**

Все остальные DNS-сервера, отличных от Microsoft, могут использовать Syslog для отправки журналов DNS в DNSWatch.

1. «Имя»: указать название вашего источника. Это то, как он будет отображаться в интерфейсе.
2. Источник DNS журналов выбрать вариант «Другой» и указать параметры получаемого Syslog. При возникновении трудностей с подключением DNS-серверов, отличных от Microsoft, пожалуйста, свяжитесь со службой поддержки.

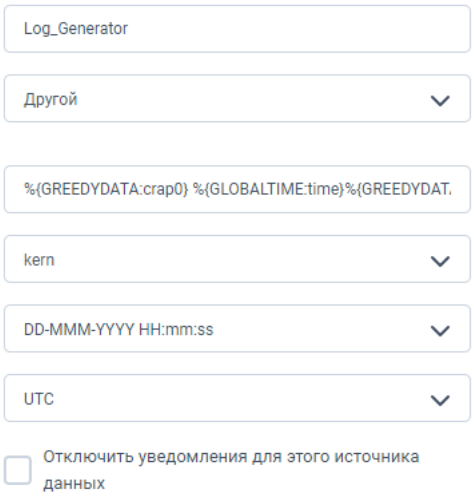


*Рисунок 9 – Настройки Syslog*

***Примеры GROK выражений***

| ***Для Syslog*** | |
|---|---|
| *Образец журнала* | *<141>**02-Aug-2024 09:31:40 Ebuber_Generator** CEF:0\| 02-Aug-2024 09:31:40 client 192.168.120.44 \| query www.msftncsi.com.edgesuite.net IN A response: NOERROR*<br>*<141>**02-Aug-2024 09:31:40 Ebuber_Generator** CEF:0\| 02-Aug-2024 09:31:40 client 192.168.105.165 \| query gvt1.com IN A response: NOERROR* |

| | |
|---|---|
| *GROK выражение* | *%{GREEDYDATA:crap0} %{GLOBALTIME:time}%{GREEDYDATA:crap1} client %{DATA:ip} %{GREEDYDATA:crap2} query %{DATA:domain} IN %{DATA:type} response* |
| *Формат даты* | *DD-MMM-YYYY HH:mm:ss* |

3. Опция «Отключить уведомления для этого источника данных» отключит получение уведомлений об отсутствии журналов от источника за последний час.

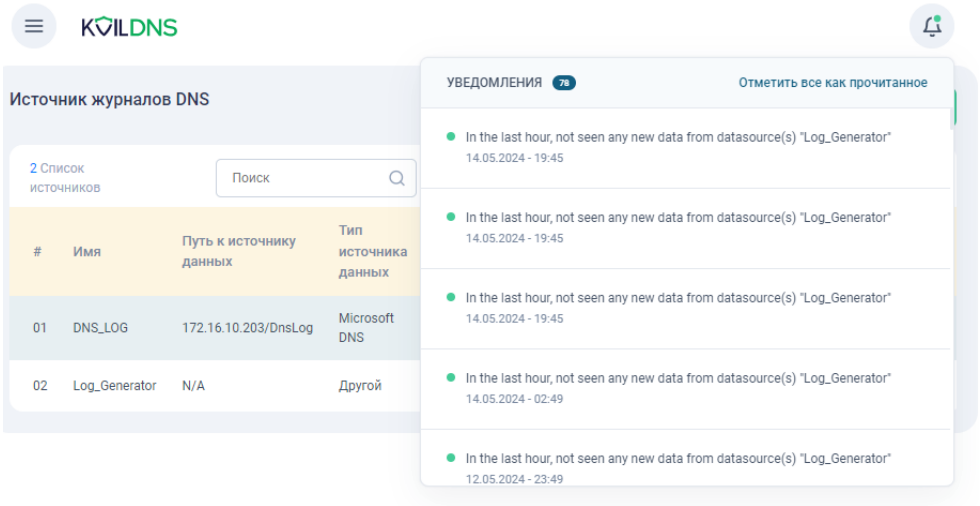


*Рисунок 10 – Пример уведомлений об отсутствии новых сообщений в журналах источника*

**Завершение конфигурации источников DNS журналов**

1. После успешного добавления источника любого типа нужно убедиться, что DNSWatch может получать данные от источника. Нажмите на значок в форме глаза, чтобы увидеть полученные события из журнала источника. Для всех сконфигурированных источников проверьте соответствие формата даты/времени в наблюдаемом тексте с параметрами, указанными в конфигурации источника. Нажмите на значок в виде пера, при необходимости внести изменения.

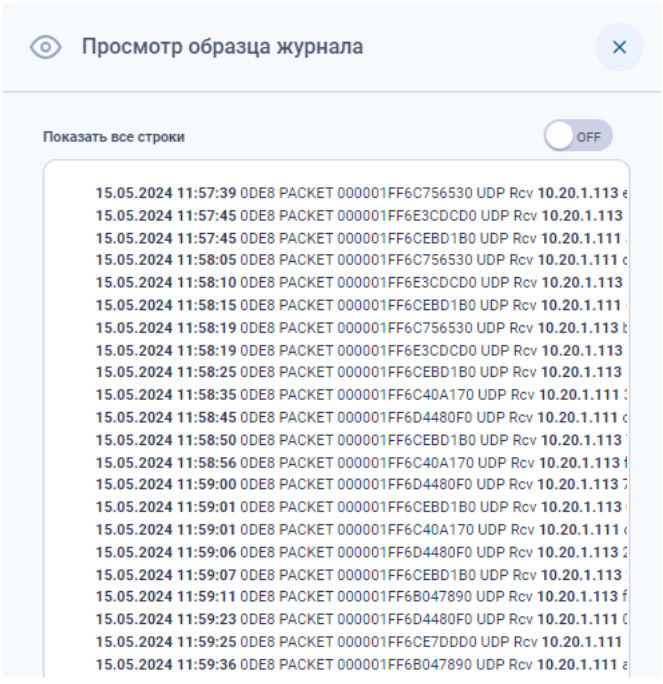


*Рисунок 11 – Пример успешного получения журналов событий*

2. Переведите тумблер «Активировать», в состояние «On»

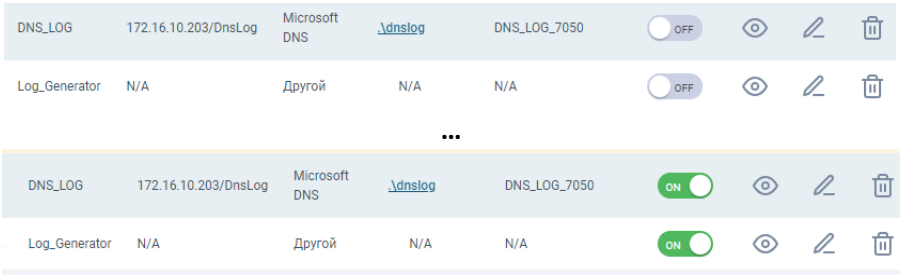


*Рисунок 12 – Подключение источников журналов*

3. В течении 5 минут на стартовой вкладке «Статистика» должны появиться первые данные.

## Настройка источников журналов DHCP

Получение журналов DHCP позволяет однозначно идентифицировать хост, даже при использовании динамический адресации. Это позволит вам увидеть имя хоста и MAC-адрес в журналах мониторинга.

**Порядок действий**

1. Нажмите кнопку «Меню» ( ≡ )
2. Выберите раздел «Источник журналов DHCP»
3. Нажмите на кнопку «Добавить источник журнала DHCP». Есть два варианта получения журналов DHCP.
4. Если используется DHCP-сервер на базе Windows, то журналы отладки на нём включены по умолчанию, и следует использовать общий доступ по протоколу SMB (вариант SMB Sharing), чтобы забрать эти журналы. Предварительно предоставьте общий доступ к папке с журналами DHCP (system32/dhcp) выделенному под эту задачу пользователю (доменному или локальному). Папка может быть доступна только для чтения. Настройки:
    - «Имя»: указать название вашего источника. Это то, как он будет отображаться в интерфейсе.
    - выбрать «Учётные данные». Если учётных данных не было заведено ранее, необходимо их добавить, нажав «Добавить учётные данные».
    - в поле «hostname or IP/share name» необходимо указать имя хоста или IP и имя папки общего доступа. Обратите внимание на знак разделителя «/»
    - выбрать формат даты для журналов DHCP-сервера. Формат даты, можно заранее посмотреть на DHCP-сервере или сделать это в интерфейсе DNSWatch (для этого необходимо завершить настройку и нажать на значок в виде глаза. вы увидите сырые журналы, как их прочитала система)
5. Если используемый DHCP-сервер способен отправлять свой журнал DHCP по Syslog, то следует выбрать вариант «Syslog». Настройки:
    - «Имя»: указать название вашего источника. Это то, как он будет отображаться в интерфейсе.
    - «Сервер»: указать адрес DHCP сервера
    - указать остальные параметры получаемого Syslog. Для удобства конфигурирования и отладки, можно воспользоваться кнопкой «Посмотреть журнал», она отобразит сырые данные журналов, как их видит система. Данный

инструмент позволит убедиться, что Syslog доходит до системы и упростит задачу по написанию GROK выражения для парсинга журнала.

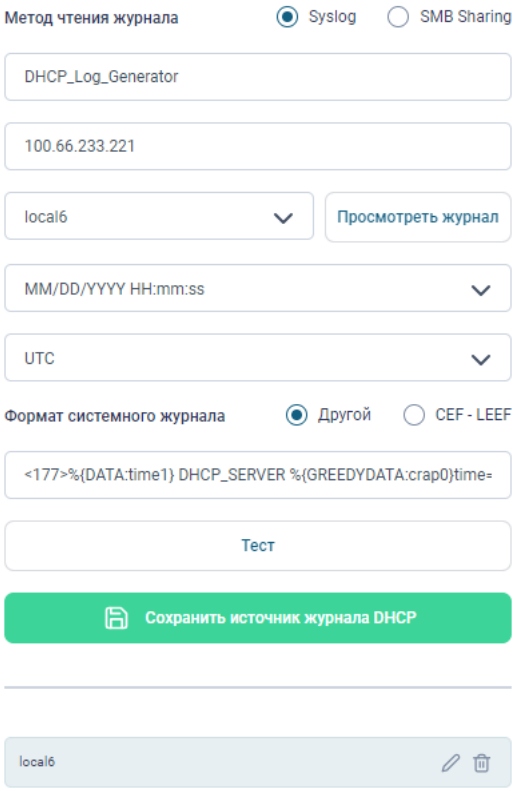


*Рисунок 13 – Пример настройки получения журналов DHCP по Syslog*

***Примеры GROK выражений***

| | |
|---|---|
| ***Для CentOS*** | |
| *Образец журнала* | *Jan 22 15:02:55 dhcp-primary dhcpd[830102]: DHCPACK on 10.246.1.37 to f8:4d:89:68:65:19 (Nosir-MBP) via 10.246.1.1* |
| *GROK выражение* | *%{SYSLOGTIMESTAMP:timestamp} %{DATA:host} %{WORD:dhcp_action} on %{IP:clientIp} to %{MAC:mac} \(%{DATA:hostname}\) via %{IP:server_ip}* |
| *Формат даты* | *MMM DD YYYY HH:mm:ss* |
| ***Для Checkpoint*** | |
| *Образец журнала* | *<190>Feb 21 14:31:36 CP-1800-node-1 dhcpd: [Local Network: DHCP] DHCPACK on 10.30.50.75 to 8c:04:ba:a4:9d:42 (DESKTOP-FVBFLBK) via LAN4.50* |
| *GROK выражение* | *<%{NUMBER:number}>%{DATA:time} CP%{GREEDYDATA:crap0} on %{DATA:clientIp} to %{DATA:mac} \(%{DATA:host}\) %{GREEDYDATA:crap1}* |
| *Формат даты* | *MMM dd HH:mm:ss* |
| ***Для CentOS*** | |
| *Образец журнала* | *<190>Apr 12 11:38:32 dhcp-primary dhcpd[2728370]: DHCPACK on 10.247.3.142 to 00:e9:3a:bb:ff:61 (NB-SAP-1043) via 10.247.3.1* |
| *GROK выражение* | *<%{NUMBER:number}>%{DATA:time} dhcp%{GREEDYDATA:crap0} on %{DATA:clientIp} to %{DATA:mac} \(%{DATA:host}\) %{GREEDYDATA:crap1}* |
| *Формат даты* | *MMM dd HH:mm:ss* |

При возникновении трудностей с подключением DHCP-серверов, отличных от Microsoft, пожалуйста, свяжитесь со службой поддержки.

6. После выбора всех параметров формата нажмите нужно протестировать конфигурацию, нажав “Тест” и убедиться, что данные распознаются корректно.
7. После успешной проверки работоспособности переведите тумблер «Активировать», в состояние «On»

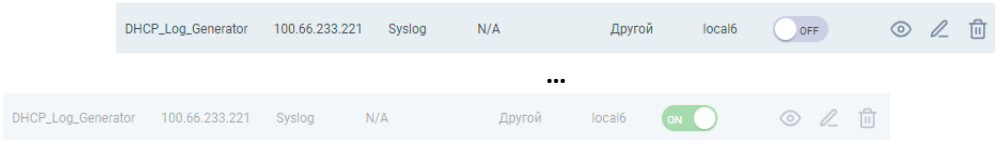


*Рисунок 14 – Подключение интеграции с DHCP*

## Идентификация пользователя в Active Directory

DNSWatch может отображать имя пользователя в дополнении к IP-адресу, если оно зарегистрировано в журнале событий Windows. Для этой конфигурации требуется пользователь службы с дополнительными правами доменного администратора.

**Порядок действий**

1. Нажмите кнопку «Меню» ( ≡ )
2. Выберите раздел «Идентификация пользователя в Active Directory»
3. Нажмите «Добавить сервер Active Directory»
4. Поле «Имя» предназначена только для идентификации сервера внутри интерфейса
5. В разделе «Учётные данные» выберете (или создайте) пользователя, у которого есть право доменного администратора
6. Добавьте IP-адрес или имя хоста сервера AD и нажмите "+ Добавить сервер Active Directory "

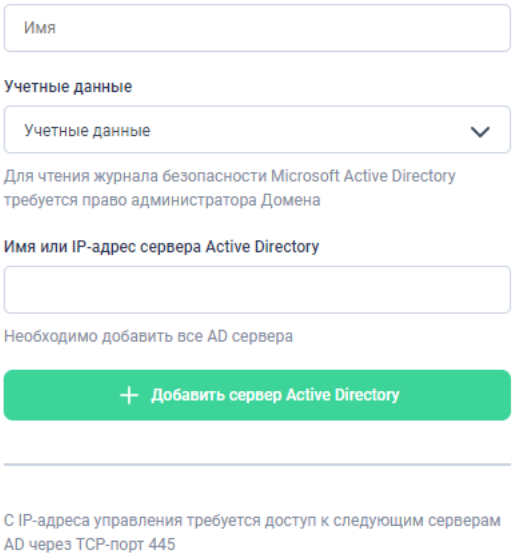


*Рисунок 15 – Интеграция с АД*

7. Проверьте наличие доступ: нажмите на «Проверить доступ» и убедитесь, что можете получить доступ к журналам AD.
8. Переведите тумблер «Активировать», в состояние «On»

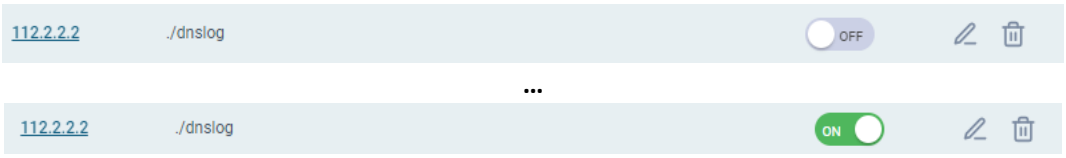


*Рисунок 16 – Подключение интеграции с AD*

# Интеграция с SIEM

**Порядок действий**

1. Нажмите кнопку «Меню» ( ≡ )
2. Выберите раздел «Интеграция с SIEM»
3. Нажмите «Добавить SIEM»
4. Введите IP-адрес и порт вашего SIEM
5. Выберите протокол и формат передачи данных
6. Поле «Название приложения» несёт дополнительную информацию и не влияет на функционирование
7. Выберите часовой пояс и сохраните конфигурацию
8. При необходимости возможно добавить дополнительный сервер SIEM, если данные нужно отправить более чем на один сервер
9. Выбрать пользовательский или системный шаблон отчёта. Все соответствующие выбранному отчёту события будут отправляться на выбранный SIEM

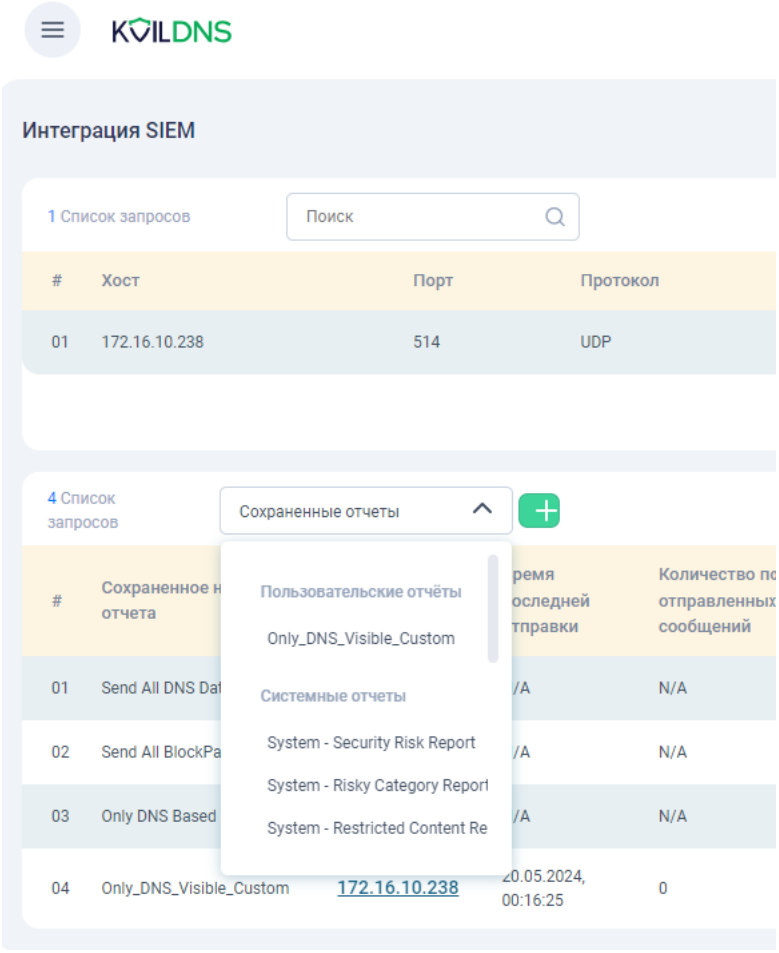


*Рисунок 17 – Выбор данных для отправки в SIEM*

10. После выполнения вышеуказанных действий включите значки в разделе “Включить/выключить”, чтобы начать отправку журналов

## Отчёт «Аудит периметра»

Эта функция поможет проаудировать эффективность работы других решений по фильтрации URL-адресов (NGFW), прокси-серверов или DNS фильтров используя KvilDNS с демонстрацией «слепых зон», используемых средств.

Вы также можете активировать отчёт «Аудит периметра» избирательно, только для категорий по вашему выбору. Логика работы данного функционала максимально проста: если среди запросов пользователей обнаруживается запрос, соответствующий определённой категории, DNSWatch с эмулирует запрос по данному URL-адресу и определит, может ли стороннее решение заблокировать запрос. В конце он выдаст отчёт о результате запроса как «Передан» или «Заблокирован» (“Passed” или “Blocked”).

**Конфигурация**

1. Нажмите кнопку «Меню» ( ≡ )
2. Выберите раздел «Аудит периметра» и нажмите кнопку «Настройки»
3. Раздел «**Контрольный список категорий**»
   Сначала определите список категорий, запросы к которым будут проверяться. Назначение конкретных категорий вредоносных доменов имеет важное значение и обеспечит большую точность при сравнении результатов. Рекомендуется выбирать категории, отличные от “Безопасных”.
4. Раздел «**DNS-сервер**».
   Выберите «Безопасный DNS», если вы используете DNS сервис с функцией фильтрации, отличный от KvilDNS (DNSCube), и вы хотите сравнить их. при выборе «Безопасный DNS», станет доступно поле «Блокирующее действие». В этом поле необходимо указать Sinkhole IP, используемый для блокировки DNS-запросов запрещённых доменов. Этот IP-адрес можно взять из вашего стороннего решения для фильтрации DNS-запросов. Поле «Описание защищённого DNS» может содержать комментарий и не влияет на работу системы.
5. Раздел «**DNS фильтрация KVILDNS**»
   Если вы используете DNSCube, необходимо указать используемый (сконфигурированный в DNSCube) Sinkhole IP, используемый для блокировки DNS-запросов запрещённых доменов.
6. Раздел «**Тестирование фильтрации на Web-шлюзе**»
   Выберите этот параметр, если вы хотите сравнить KvilDNS со сторонним решением по фильтрации на базе NGAF и/или прокси-сервера.
   Если решение является МЭ с функцией WEB фильтрации, то следует выбрать «Прямой HTTP-тест (через UTM/NGFW)». Вкладка “Марка/модель” содержит дополнительную информацию и не повлияет на процедуру тестирования.
   Если решение является прокси-сервером, вам следует выбрать «Прокси-тест». Необходимо добавить IP-адрес и порт прокси-сервера в поле «Выбрать прокси» кнопка «Добавить новый прокси».
   Поле «Заблокированный URL» предназначена только для тестирования. Вы можете ввести вредоносный домен, который, гарантированно заблокирован на вашем прокси-сервере, и нажать на значок в виде глаза.
   Изучив страницу блокировки вашего прокси-сервера, скопируйте характерный текст со страницы блокировки, который поможет KvilDNS понять, что это страница блокировки прокси-сервера, и вставьте его в поле “Ожидаемый текс со страницы блокировки”.
   Вкладка “Марка/модель” содержит дополнительную информацию и не повлияет не повлияет на процедуру тестирования.

7. Раздел «**Количество строк**»
   По умолчанию количество результатов ограничено 5 миллионами строк. При необходимости это число можно отредактировать.

# Часты вопросы и типовые проблемы

**Проблема №1:** после настройки источников журналов DNS на стартовой странице «Статистика» нет данных по истечению 5 минут.

**Возможная причина 1:** забыли активировать источник.

**Решение**: в разделе «Источники журналов DNS» переведите тумблер «Активировать», в состояние «On».

**Возможная причина 2:** некорректно указан формат времени.

**Решение**: сравните используемый формат времени в получаемых от источника журналах с настройкой формата времени в параметрах источника и приведите настройки источника в соответствие формату получаемых данных.

**Проблема №2:** после завершения мастера инициализации не получается попасть на WEB интерфейс управления. WEB интерфейс: «то доступен, то недоступен», «доступен несколько секунд а потом отваливается», «выдаёт ошибку страница не найдена, но адрес пингуется»

**Возможная причина 1:** назначенный на интерфейс управления адрес уже существует в сети и произошёл конфликт адресов.

**Решение**: выключить виртуальную машину, убедиться, что назначенный ей адрес продолжает пинговаться. Назначить на интерфейс управления новый адрес, предварительно убедившись, что он свободен.

**Возможная причина 2:** в визарде инициализации адрес, предназначенный для интерфейса управления, был назначен на Sinkhole интерфейс или был назначен один и тот же адрес на интерфейс управления и Sinkhole интерфейс.

**Решение**: назначьте корректный адрес на интерфейс управления, а на Sinkhole интерфейс назначьте произвольный несуществующий адрес.

## По вопросам документации

Для получения последней версии данного документа, пожалуйста, свяжитесь со службой поддержки по адресу support@KvilDNS.ru
Вы можете отправить свои отзывы или вопросы по поводу этого документа по адресу documentation@KvilDNS.ru

Редакция от 26.10.2024