

DNS-обогащение

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

Официальная документация по данному разделу приведена в Онлайн-справке на продукт: <https://support.kaspersky.com/KUMA/2.1/ru-RU/217863.htm>

<https://www.youtube.com/embed/es0nC-YvZwc?si=4A7G3FrZtPNy91Ap>

Обогащение DNS

DNS обогащение позволяет преобразовывать доменные имена в адреса для следующих полей:

- DestinationHostName -> DestinationAddress
- DeviceHostName -> DeviceAddress
- SourceHostName -> SourceAddress

А также преобразовывать адреса в доменные имена для следующих полей:

- DestinationAddress -> DestinationHostName
- DeviceAddress -> DeviceHostName
- SourceAddress -> SourceHostName

Важный момент, DNS обогащение работает только для серых сетей

Обогащение происходит если: целевые поля пустые и если резолвится PTR из IP, то будут резолвиться только серые IP

"Cache TTL" в настройках DNS Обогащения (Дефолтовое значение 60 сек), работает следующим образом:

- KUMA резолвит server.example.com в 192.168.1.1 и получает TTL этой записи (от DNS сервера получает) 3600 сек например
- добавляет себе это в кеш

- как только время хранения записи в кеше достигает $TTL/2 = 1800$ сек, то KUMA сама идет в DNS сервер и обновляет закешированную запись
- те 60 сек которые мы выставяем - это время хранения записей, которые не обновлены с DNS - например `server.example.com` больше не существует

Поле настройки URL - не обязательно. Если оставить пустым, то при обогащении будут использоваться системные настройки сервера. Соответственно, если DNS в ОС серверов коллекторов разные - то и обогащение будет разное








Если событие с адресом 127.0.0.1, то можно перед DNS обогащением в коллекторе в парсинге добавить затирание `deviceAddress`, если оно равно 127.0.0.1, тогда обогащение DNS должно произойти

Настройка на стороне KUMA

Для повышения производительности, можно изменять число рабочих процессов коллектора (1 шаг настройки) / самого правила обогащения (для асинхронных задач эффективнее работа)

В разделе **Ресурсы - Правила Обогащения** создаем новое правило, ниже пример типового обогащения для DNS:

Редактирование правила обогащения

*Название	<input type="text" value="DNS"/>
*Тенант	Main 
*Тип источника данных	dns 
URL	<input type="text" value="10.68.85.2"/> <div> Добавить URL</div>
Запросов в секунду	<input type="text" value="5"/>
Рабочие процессы	<input type="text" value="2"/>
Количество задач	<input type="text" value="0"/> 
Срок жизни кеша	<input type="text" value="3600"/>
Кеш отключен	Включено 
*Отладка	Выключено 
Описание	<div>Описание</div>
Фильтр	Создать 

Сохранить

Далее созданное правило обогащения выше необходимо закрепить в коллекторе в части обогащения.

Revision #9

Created 15 August 2023 14:29:26 by Boris RZR

Updated 2 June 2025 07:41:34 by Boris RZR