

# DNS-имя

Уникальное DNS-имя, которое вписывают в конфигурацию как адрес резервного или устаревшего сервера. Событие появляется, когда это имя кто-то разрешает: запускает скопированную конфигурацию, проверяет адрес командой или прогоняет файл через сканер.

---

| СОБЫТИЕ          | СРАБАТЫВАЕТ         | ЗАДЕРЖКА | НУЖНО                      |
|------------------|---------------------|----------|----------------------------|
| DNS-запрос имени | когда имя разрешают | секунды  | выход к внешним DNS-именам |

---

## 1 Как работает

Кабинет выдаёт имя вида `k3f9x2m7q1z8p4w6.c.deception-lite.ru`: шестнадцать случайных латинских букв и цифр и зона `c.deception-lite.ru`. Зона делегирована сервису, поэтому любой DNS-запрос этого имени — из вашей сети, от провайдера или из чужой инфраструктуры — доходит до него. Свой DNS-сервер поднимать не нужно.

Сервис отвечает адресом своего сервера и записывает событие. Строка с именем в файле ничего не сообщает: событие создаёт только запрос имени.

Запрос сервису отправляет не компьютер, на котором открыли файл, а DNS-сервер, через который тот работает: корпоративный, провайдера или публичный. Поэтому в событии указан адрес DNS-сервера. Сам компьютер находят по журналу этого DNS-сервера (раздел 8).

### Приставка

Слева от имени можно дописать своё слово: `ansible.k3f9x2m7q1z8p4w6.c.deception-lite.ru`. Запрос такого имени тоже создаёт событие этой ловушки, а приставка видна в нём. Так одно имя можно разложить в несколько мест и различать их. В приставке — латинские буквы, цифры, дефис и точки, всего не больше 80 символов. Обращения с разными приставками не объединяются в одно событие.

---

## 2 Что понадобится

- Доступ к файлу или системе, куда вы впишете имя.
- Компьютеры и серверы, которые будут читать файл, должны разрешать внешние DNS-имена — напрямую или через ваш DNS-сервер. Если наружу DNS закрыт, запрос не дойдёт до сервиса.
- Агентов, своего DNS-сервера и доступа сервиса в вашу сеть не нужно.

---

## 3 Где разместить

### Подходит

- inventory Ansible и плейбуки выведенных стендов;
- docker-compose и файлы окружения старого стенда;
- переменные CI и шаблоны развёртывания;
- резервный профиль подключения к базе данных, строка `HostName` в `~/.ssh/config`;
- инструкция по развёртыванию в вики.

### Не подходит

- файлы, которые запускают задания по расписанию или читают мониторинг;
- репозитории и почта, которые проверяют сканеры секретов и фильтры ссылок: каждая проверка создаст событие;
- рабочие конфигурации, которые применяются при каждой выкладке.

---

## 4 Как разместить

1. В кабинете, в «Генераторе ловушек», нажмите «Сгенерировать» на карточке «DNS-имя». В поле «Где разместить» запишите файл и ресурс, например «inventory/legacy.ini в репозитории infra».
2. Скопируйте имя из карточки ловушки.
3. Впишите его туда, где в этом файле указан адрес сервера, под правдоподобным ключом:

```
[backup_db]
backup-db-01 ansible_host=k3f9x2m7q1z8p4w6.c.deception-lite.ru
```

или

```
BACKUP_DB_HOST=k3f9x2m7q1z8p4w6.c.deception-lite.ru
```

4. Не оставляйте рядом комментариев о ловушке и не упоминайте сервис в названиях переменных.
5. Убедитесь, что файл не используют задания по расписанию и мониторинг.

---

## 5 Как проверить

На любой рабочей станции выполните:

```
nslookup k3f9x2m7q1z8p4w6.c.deception-lite.ru
```

Команда вернёт адрес сервера сервиса. Через несколько секунд в разделе «Срабатывания» появится событие «DNS-запрос имени». Запишите время проверки, чтобы потом не разбирать собственное событие.

Повторная проверка через тот же DNS-сервер в течение часа нового события не создаст: одинаковые обращения объединяются. Чтобы проверить ещё раз, добавьте приставку: `nslookup test2.k3f9x2m7q1z8p4w6.c.deception-lite.ru`.

---

## 6 Что будет в событии

| Поле          | Что в нём                                                                                                                                                                                   |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Действие      | «DNS-запрос имени», в webhook — <code>dns_lookup</code> .                                                                                                                                   |
| IP            | Адрес DNS-сервера, который задал вопрос.                                                                                                                                                    |
| DNS-имя       | Запрошенное имя целиком, вместе с приставкой. В webhook — <code>details.hostname</code> , приставка отдельно в <code>details.dns_prefix</code> , тип запроса в <code>details.qtype</code> . |
| Где размещена | Запись из поля «Где разместили».                                                                                                                                                            |

---

## 7 Ложные срабатывания

- Ваша проверка.
  - Сканеры секретов в репозиториях и CI, которые проверяют найденные адреса.
  - Почтовые и веб-фильтры, которые открывают адреса из писем и документов.
  - Задания и мониторинг, которым достался этот файл.
- 

## 8 Если ловушка сработала

1. Исключите себя: сверьте время события с проверками и работами в этом месте.
2. По записи «Где разместили» определите файл и ресурс.
3. Если IP в событии — ваш DNS-сервер, найдите в его журнале запрос этого имени в то же время: там будет адрес компьютера.
4. Проверьте журналы доступа к ресурсу с файлом: кто читал или копировал его в последние дни.
5. Если IP внешний и не принадлежит вашей сети, файл, вероятно, вынесен за её пределы: проверьте, где ещё хранилась эта конфигурация.
6. Считайте прочитанным всё, что лежало рядом: смените настоящие пароли и ключи из того же места.
7. После разбора перевыпустите ловушку и разместите новое имя: прежнее уже известно тому, кто его нашёл.

### Чтобы не повторилось

- Ограничьте доступ к каталогам и репозиториям с конфигурациями.
- Храните настоящие учётные данные в хранилище секретов, а не в файлах конфигурации.

---

## 9 Как снять или заменить

Кнопка в «Ловушках организации»

Что происходит

|               |                                                                                    |
|---------------|------------------------------------------------------------------------------------|
| Выкл          | Имя перестаёт разрешаться, события не записываются. Строку в файле можно оставить. |
| Перевыпустить | Ловушка получает новое имя, прежнее перестаёт работать. Замените имя в файле.      |
| Удалить       | Ловушка исчезает, её события остаются в журнале. Уберите имя из файла.             |

---

## 10 Если события нет

Что происходит

Что проверить

|                                                  |                                                                                                                               |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| nslookup не отвечает или пишет об ошибке сервера | Компьютер или сеть не выпускают DNS-запросы наружу. Проверьте из другой сети или настройте пересылку запросов на внешний DNS. |
| Ответ «не существует»                            | Ловушка выключена или имя скопировано не полностью.                                                                           |
| Адрес вернулся, события нет                      | Такая же проверка через тот же DNS-сервер уже была в этот час. Проверьте с приставкой.                                        |
| Событие есть, уведомления нет                    | Канал включён и проходит «Тест» в разделе «Уведомления».                                                                      |

---