LDAP-??????????

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

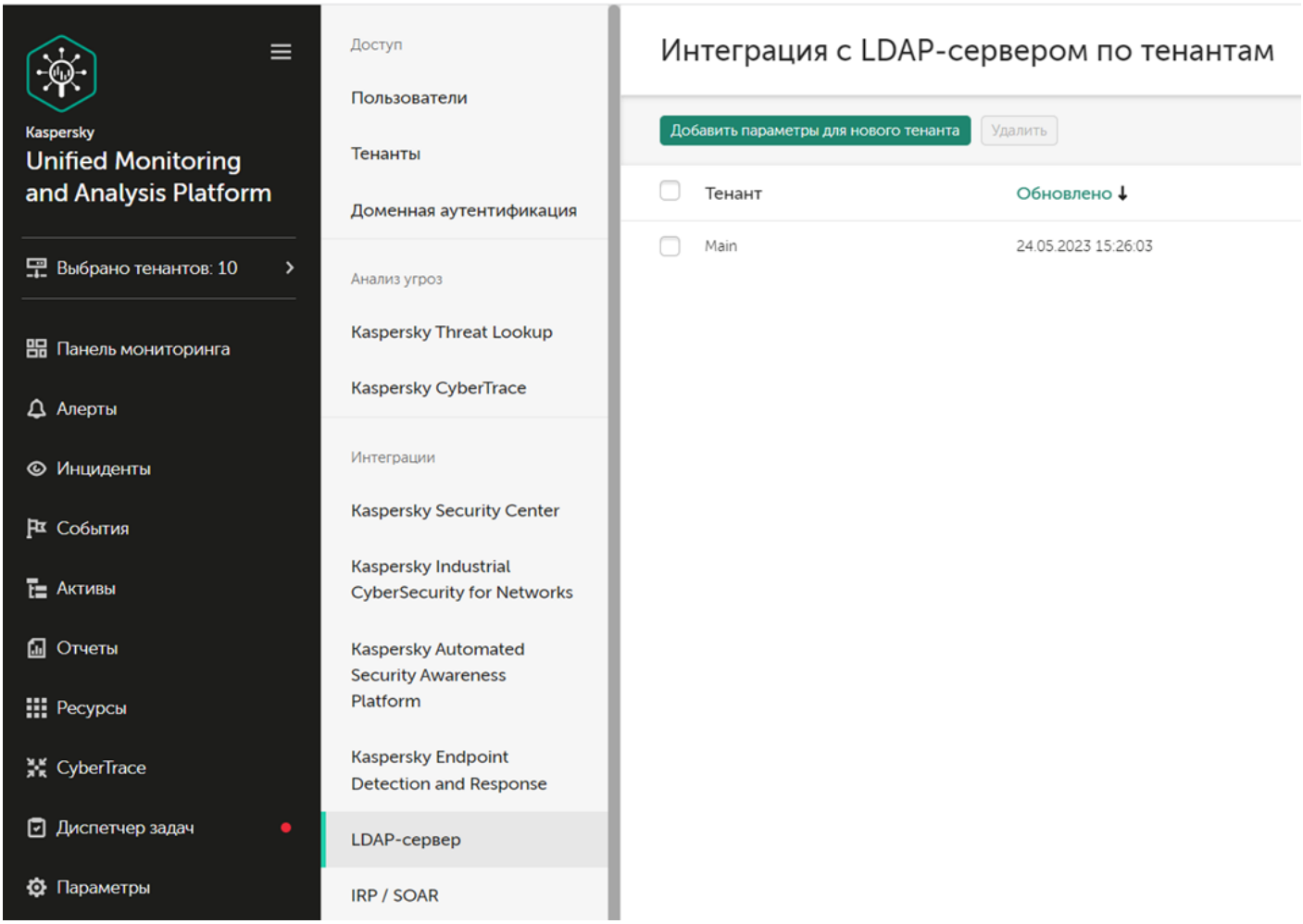
> Официальная документация по данному разделу приведена в Онлайн-справке на продукт: https://support.kaspersky.com/KUMA/3.2/ru-RU/217926.htm

https://www.youtube.com/embed/LX8-wcTzAqI?si=b4Vbszd2YtAtPyW6

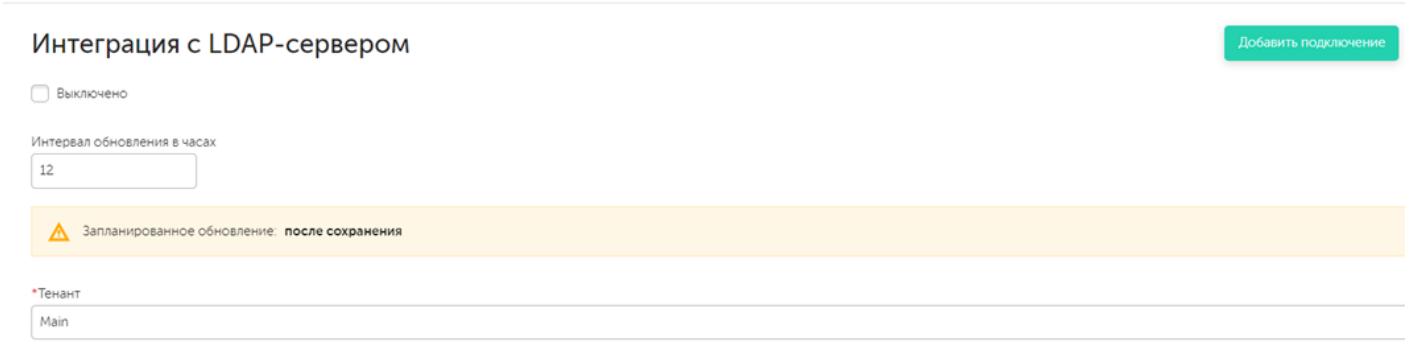
????????? ????????? ???????????? ? LDAP-??????? ??? ?????? < 4.0

Зайдите в веб-интерфейс KUMA с учетной записью Главного администратора или администратора тенанта, для которого необходимо настроить подключение к LDAP-серверу для последующего обогащения событий информацией об учетных записях.

Перейдите на вкладку **Параметры – LDAP-сервер** и нажмите на кнопку **Добавить параметры для нового тенанта**.



В открывшемся окне выберите **Тенант**, укажите **Интервал обновления в часах** и задайте **Время хранения данных**. Затем нажмите на кнопку **Добавить подключение**.

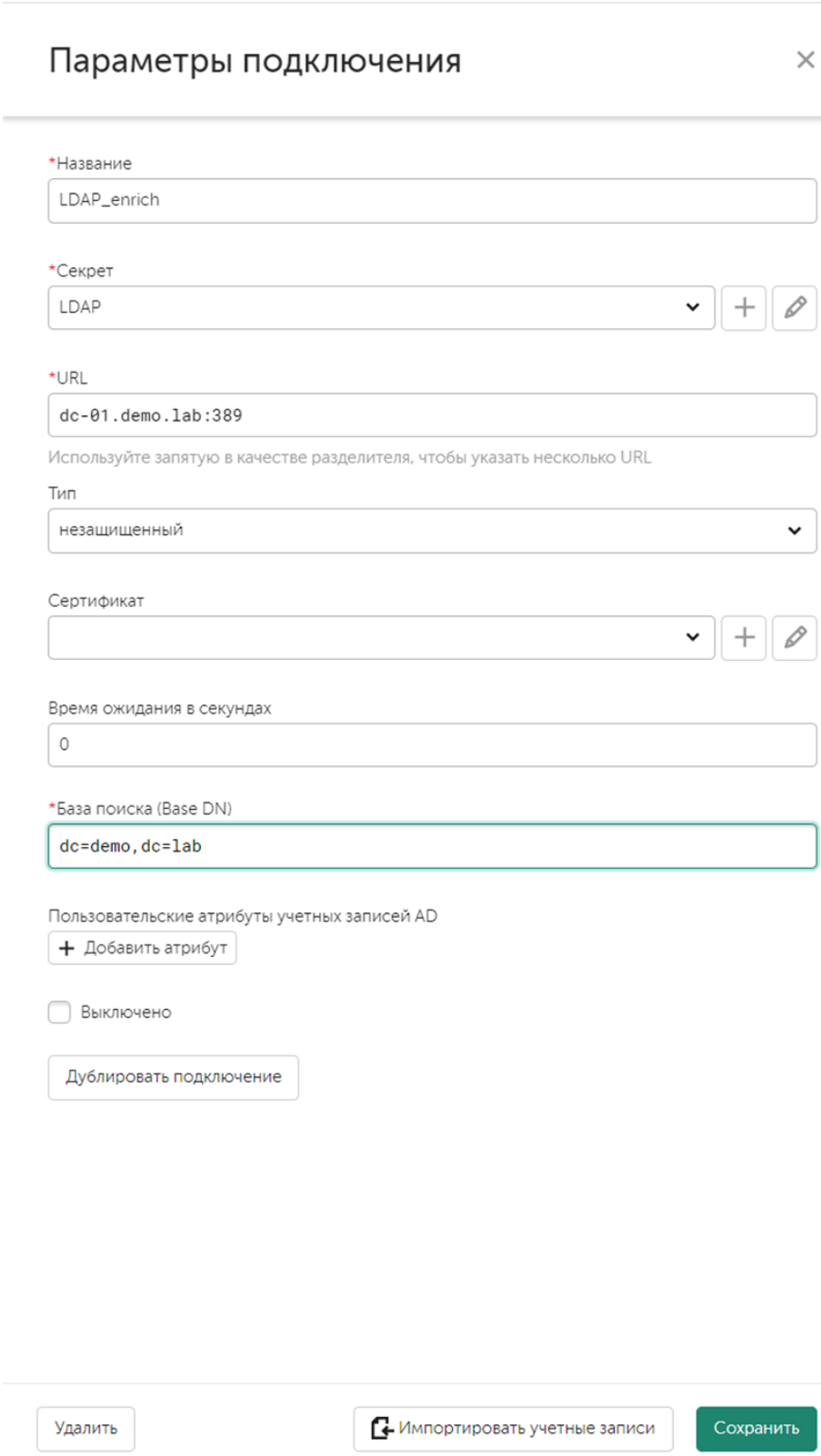


В открывшейся вкладке задайте параметры подключения к LDAP-серверу:

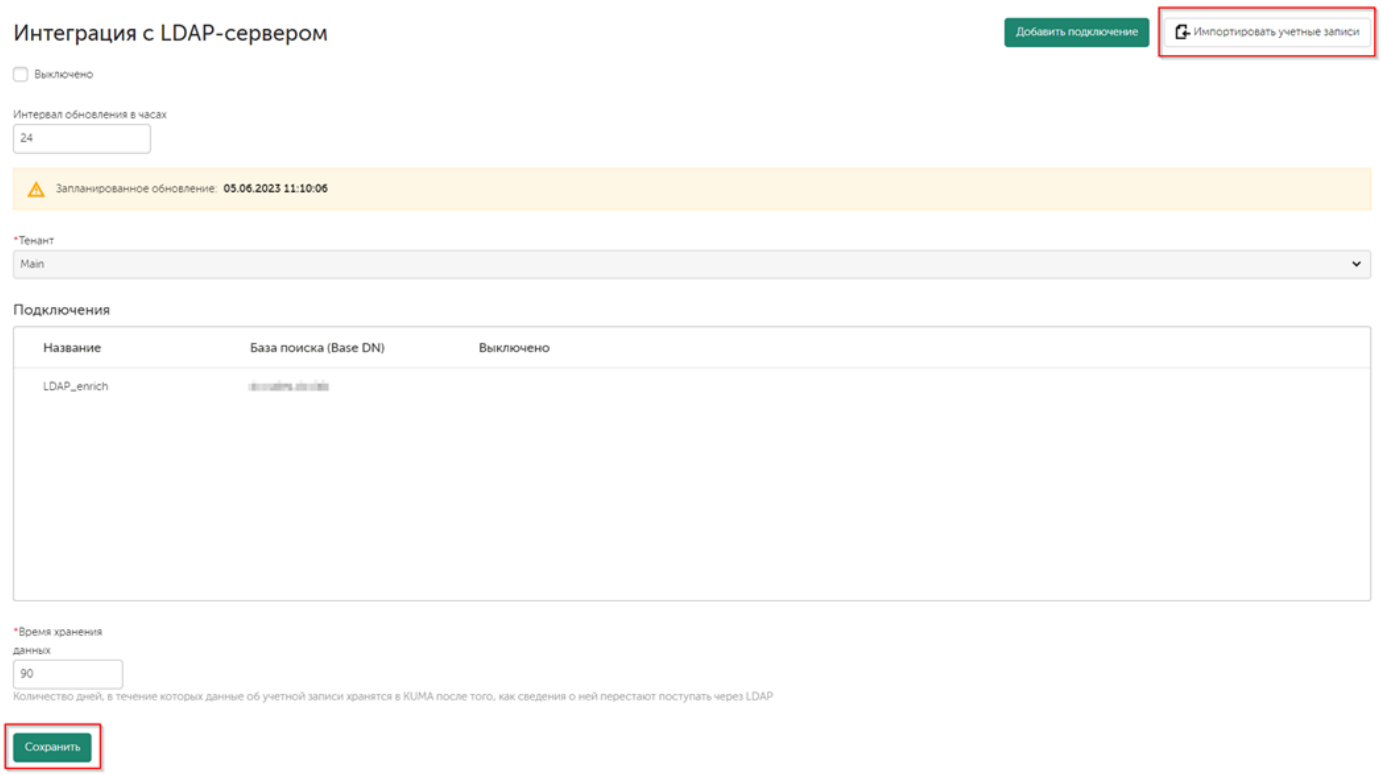
1. Укажите **Название** подключения
2. В поле **Секрет** добавьте учетную запись пользователя для подключения к серверу Active Directory. Имя пользователя может быть указано в одном из двух форматов: <user>@<domain> или <domain>\<user>
3. В поле **URL** укажите адрес одного или нескольких серверов LDAP (через запятую) в формате <hostname или IP-адрес сервера>:<порт>. Для незащищенного и startTLS подключения порт по умолчанию 389, для ssl – 636. В случае использования startTLS или ssl необходимо указывать hostname сервера, если сертификат сервера в поле

SAN не содержит IP-адреса сервера.

4. Выберите **Тип** подключения.
5. Если на прошлом шаге был выбран тип **ssl** или **startTLS**, добавьте сертификат для проверки подлинности сервера в поле **Сертификат**. В случае, если для DC используется не самоподписанный сертификат, необходимо импортировать сертификат корневого центра сертификации.
6. *Важно! Сертификат самого DC должен содержать параметр DNS Name в поле SAN, соответствующий доменному имени данного сервера (если в URL был указан hostname сервера) или параметр IP Address в поле SAN, соответствующий IP-адресу данного сервера (если в URL был указан IP-адрес сервера).*
7. Задайте **Время ожидания в секундах** – период, в течение которого KUMA будет ожидать ответа от сервера контроллера домена.
8. В поле **База поиска (Base DN)** укажите базовое отличительное имя каталога, в котором должен выполняться поисковой запрос. Можно посмотреть в Панель управления\Все элементы панели управления\Администрирование - Редактирование ADSI.
9. При необходимости укажите **Пользовательские атрибуты учетных записей AD**, на основе которых вы хотите обогащать события учетными записями.
10. Убедитесь, что галочка для пункта **Выключено** снята и нажмите на кнопку **Сохранить** для сохранения параметров подключения к LDAP-серверу.



Нажмите на кнопку **Сохранить**. При необходимости нажмите на кнопку **Импортировать учетные записи** для немедленного импорта информации об учетных записях в KUMA.

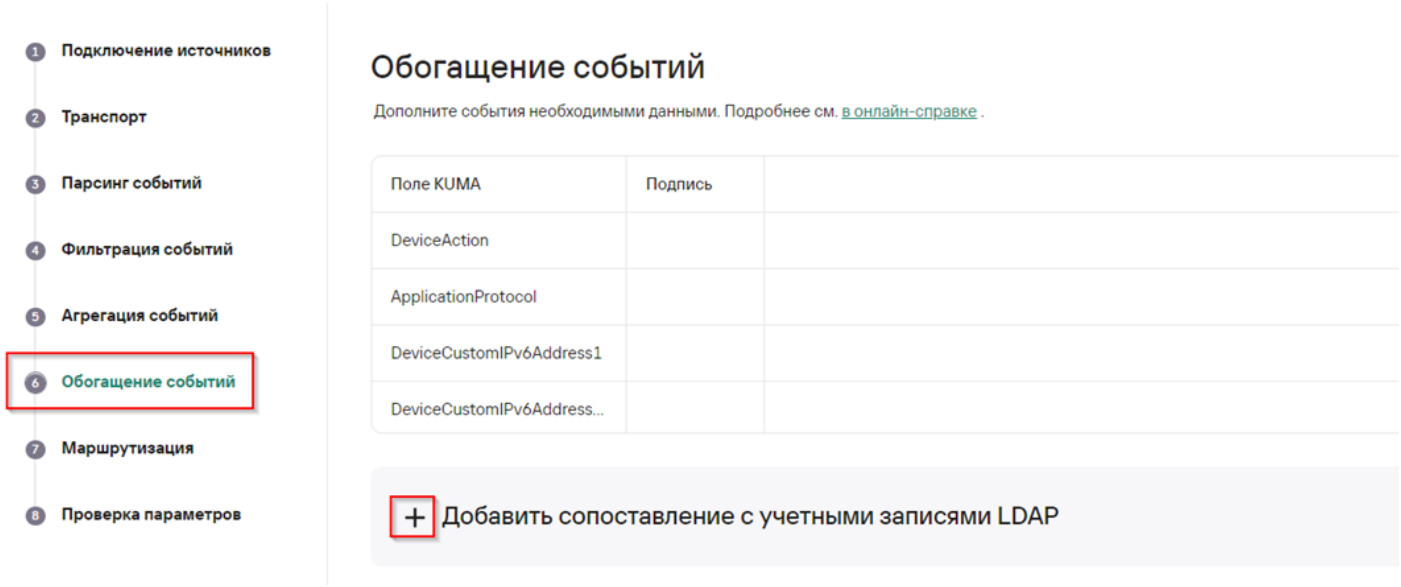


На данном этапе настройка импорта информации об учетных записях в KUMA завершена. Настройка обогащения событий информацией об учетных записях KUMA рассматривается в следующем разделе.

????????? LDAP-???????????

LDAP-обогащение настраивается на уровне коллектора и позволяет наполнить события информацией об учетных записях (атрибутах, импортированных из AD). На основе полученных атрибутов доступно выполнение реагирования AD и KASAP, а также написание правил корреляции по атрибуту memberOf. Остальные атрибуты, импортируемые из AD, служат справочной информацией и используются в расследовании алертов и инцидентов.

Для настройки обогащения, перейдите в коллектор, события с которого необходимо дополнять информацией об учетных записях и перейдите на вкладку **Обогащение событий** и нажмите на кнопку **Добавить сопоставление с учетными записями LDAP**.



Нажмите на кнопку **Добавить домен** и введите полное наименование домена в верхнем регистре. В случае, если обогащение было настроено для нескольких доменов, повторите процедуру необходимое количество раз.
В случае, если вы не знаете полного наименования домена для импортированных учетных записей, подключитесь к компоненту Core KUMA по ssh и выполните команду:

```
/opt/kaspersky/kuma/mongodb/bin/mongo kuma --eval 'accounts.findOne({},{_id:0, domain:1});'
```

Либо:

```
/opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --quiet --eval
"db.accounts.findOne({"archived":false},{"domain":1})"
```

В результате выполнения команды будет выведен домен:

```
[root@test-kuma ~]# /opt/kaspersky/kuma/mongodb/bin/mongo kuma --eval 'db.accounts.findOne({},{_id:0, domain:1});'
MongoDB shell version v4.4.16
connecting to: mongodb://127.0.0.1:27017/kuma?compressors=disabled&gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("3de79c8d-8913-4b67-83d1-e72aaa443c63") }
MongoDB server version: 4.4.16
{ "domain" : "SALES.LAB" }
```

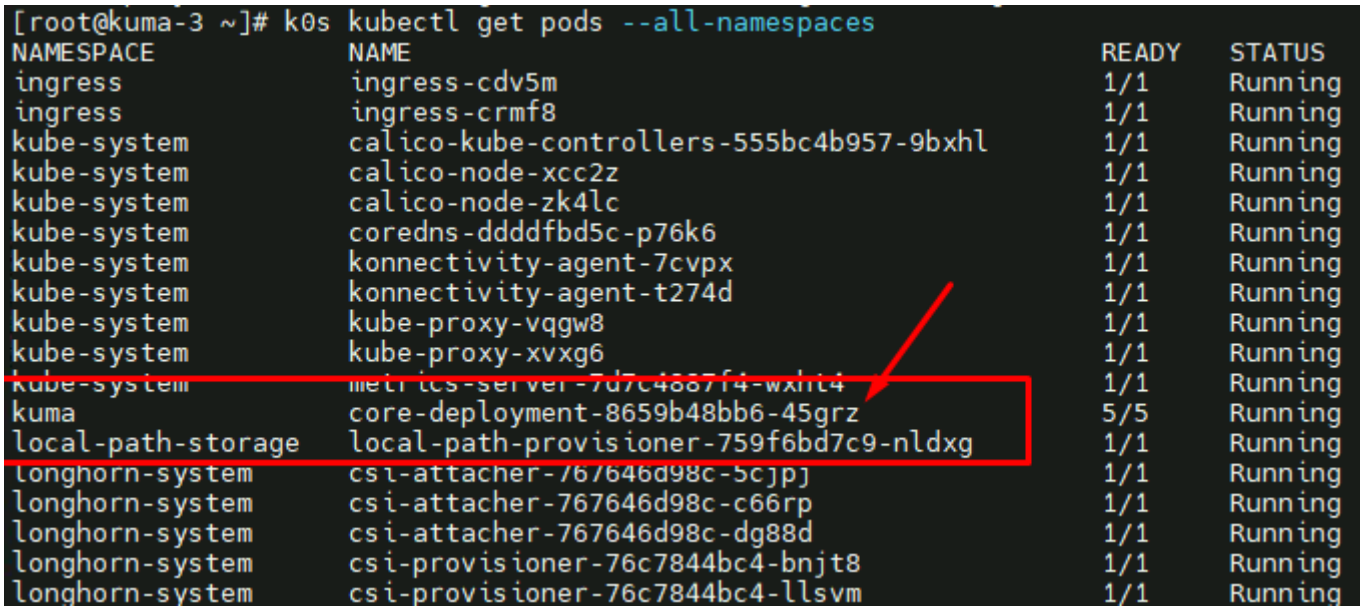
> Для версий от 4.0 изучите https://kb.kuma-community.ru/link/57#bkmrk-%D0%9F%D0%BE%D0%B4%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%BD%D0%B8%D0%B5-%D0%BA-%D0%B1%D0%B0%D0%B7%D0%B5-%D0%B4

Команда для ядра в кластере

Выполните команду на CP (Control Plane) для получения полного наименование деплоймента:

```
k0s kubectl get pods --all-namespaces
```

Получим следующий вывод:



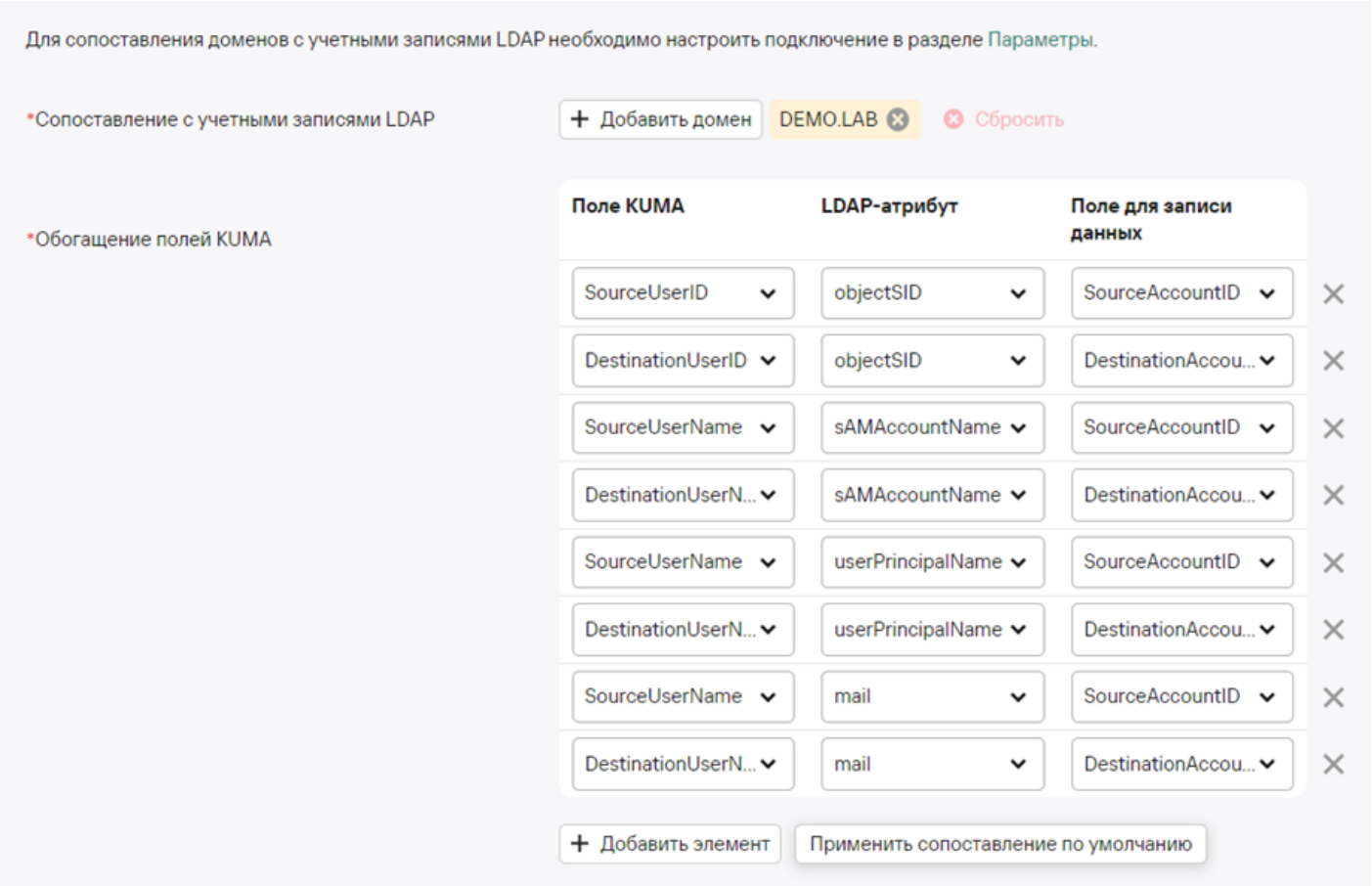
Далее выполняем команду для монго в контейнере:

```
k0s kubectl exec --stdin --tty core-deployment-8659b48bb6-45grz -n kuma -c mongodb --
/bin/sh -c '/bin/mongo localhost/kuma --quiet --eval "db.accounts.findOne({},{_id:0,
domain:1});"'
```

Если используется несколько доменов, то можно воспользоваться следующим запросом (выведет список всех доменов):

```
/opt/kaspersky/kuma/mongodb/bin/mongo kuma --eval 'db.accounts.distinct("domain");'
```

Настройте Обогащение полей KUMA на основе атрибутов AD. Для этого выберите **Применить сопоставление по умолчанию**, либо через кнопку **Добавить элемент** укажите атрибуты и поля KUMA.



Перейдите на вкладку коллектора **Проверка параметров** и нажмите на кнопку **Сохранить и перезапустить сервисы** для применения всех настроек.

На этом настройка обогащения LDAP завершена. В следующем разделе будут рассмотрены известные проблемы и пути их решения.

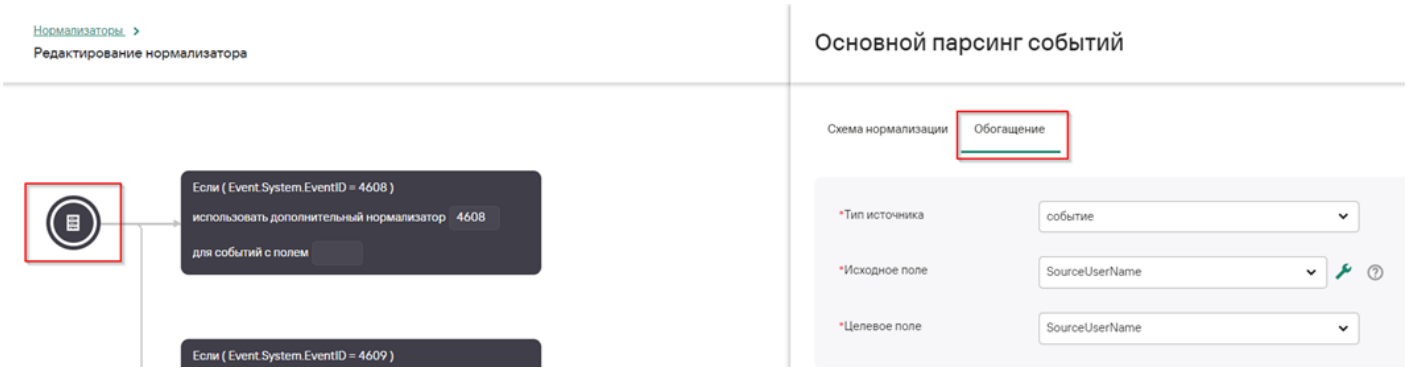
????????? ????????

> С версии KUMA 2.1.3, LDAP идет после других обогащений. Править нормалайзер (что неудобно) не нужно, а достаточно сделать правило обогащения, которое будет заменять EXAMPLE на EXAMPLE.LOCAL (если много разных доменов - можно сделать обогащение через словарь), чтобы все NetBIOS названия менялись на DNS названия доменов.

В некоторых событиях журналов Windows вместо DNS-имени домена может присутствовать NetBIOS-имя домена, которое не будет совпадать с DNS-именем домена, импортированных в KUMA учетных записей. Например, DEMO вместо DEMO.LAB.

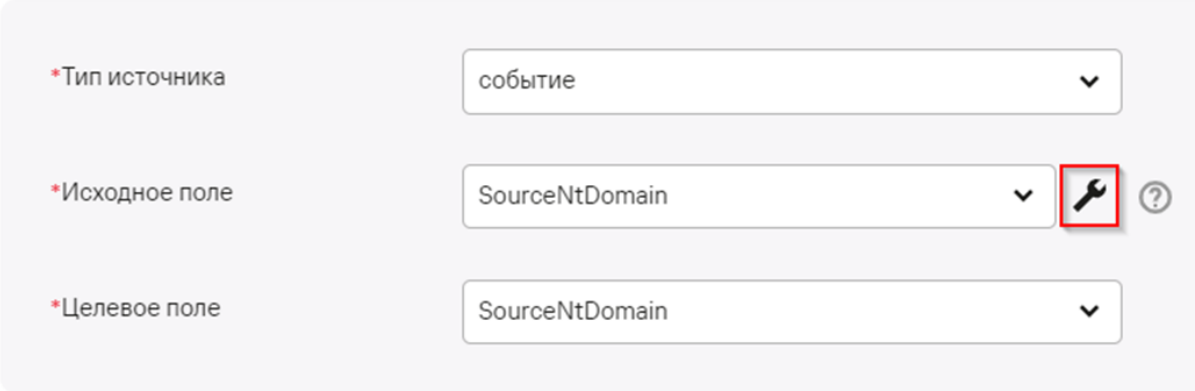
Данная проблема решается доработкой нормализатора Windows.

Для этого откройте на редактирование используемый нормализатор Windows и перейдите в **Основной парсинг событий – Обогащение**.

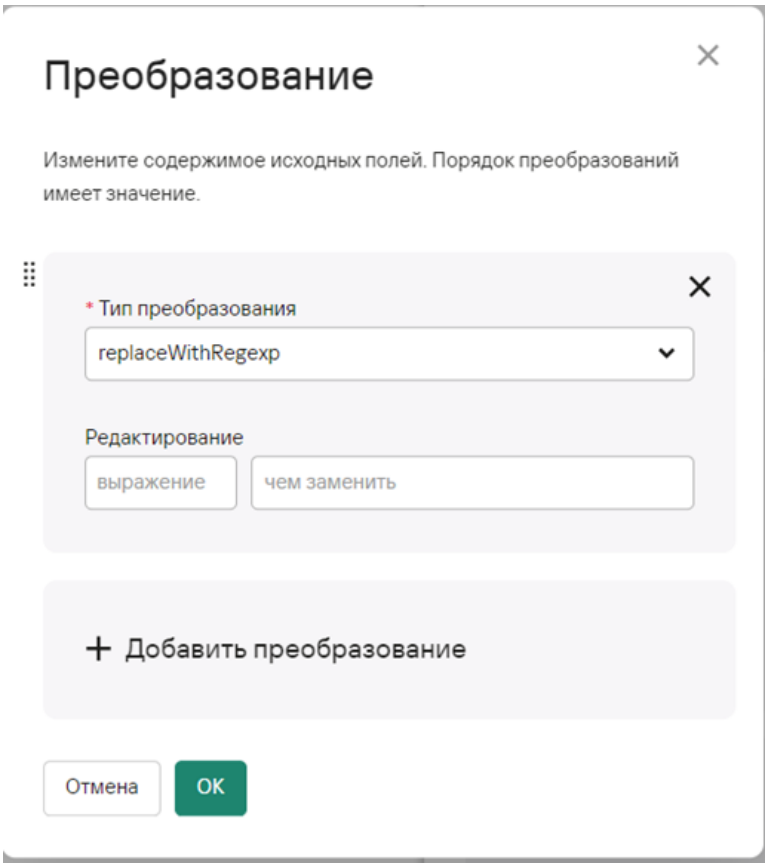


Пролистайте раздел до кнопки Добавить обогащение и нажмите ее.

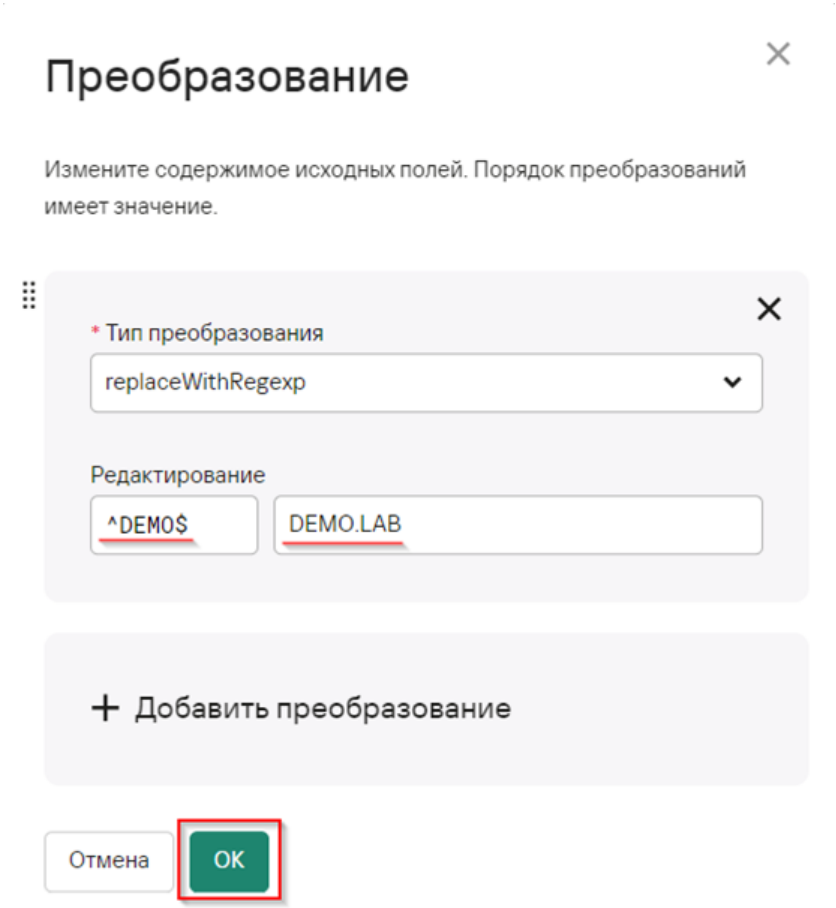
Задайте **Тип источника – событие, Исходное поле – SourceNtDomain**, Целевое поле – SourceNtDomain и нажмите на значок гаечного ключа рядом с исходным полем.



Нажмите кнопку Добавить преобразование. Выберите Тип преобразования replaceWithRegexp.



В левой части, в графе **выражение** укажите NetBIOS-имя домена в формате ^<NetBIOS-имя>$. В правой части, в графе **чем заменить** укажите DNS-имя домена. Нажмите кнопку **OK**.



Выполните аналогичные действия для поля **DestinationNtDomain**.

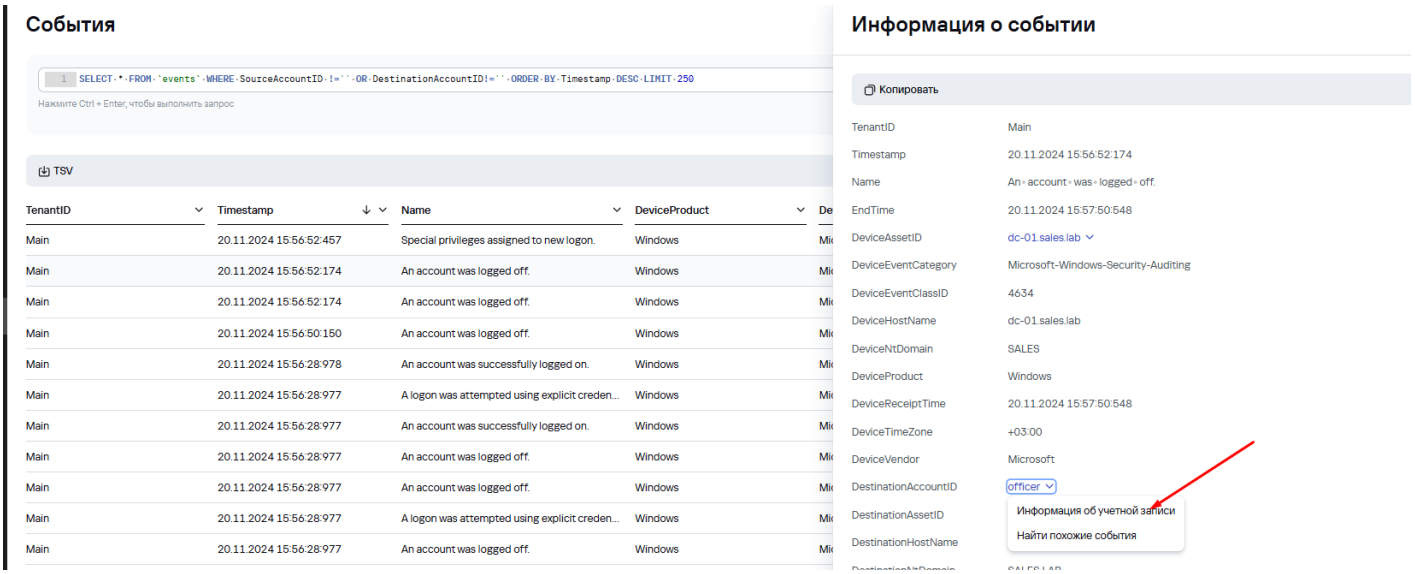
Сохраните нормализатор и выполните Обновление параметров сервиса для сервиса коллектора Windows.

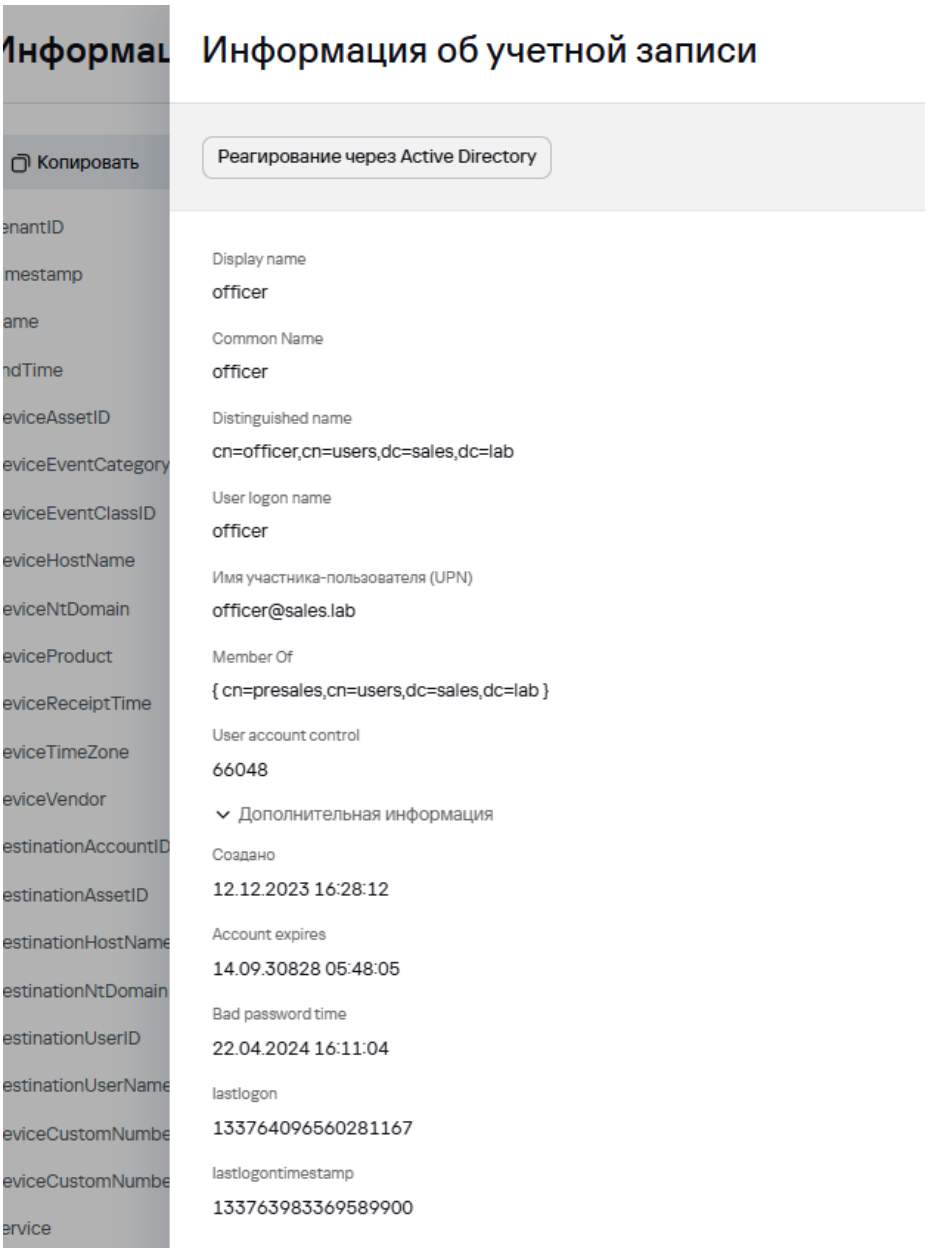
???????? ?????? LDAP-???????????

Для проверки работы обогащения перейдите на вкладку События и выполните поисковой запрос:

```
SELECT * FROM `events` WHERE SourceAccountID !='' OR DestinationAccountID!='' ORDER BY Timestamp DESC LIMIT 250
```

В результате будут выведены события, обогащенные информацией об учетных записях.


События
SELECT * FROM `events` WHERE SourceAccountID != '' OR DestinationAccountID!='' ORDER BY Timestamp DESC LIMIT 250
Нажмите Ctrl + Enter, чтобы выполнить запрос
TSV
TenantID
Timestamp
Name
DeviceProduct
Main 20.11.2024 15:56:52:457 Special privileges assigned to new logon. Windows
Main 20.11.2024 15:56:52:174 An account was logged off. Windows
Main 20.11.2024 15:56:52:174 An account was logged off. Windows
Main 20.11.2024 15:56:50:150 An account was logged off. Windows
Main 20.11.2024 15:56:28:978 An account was successfully logged on. Windows
Main 20.11.2024 15:56:28:977 A logon was attempted using explicit creden... Windows
Main 20.11.2024 15:56:28:977 An account was successfully logged on. Windows
Main 20.11.2024 15:56:28:977 An account was logged off. Windows
Main 20.11.2024 15:56:28:977 An account was logged off. Windows
Main 20.11.2024 15:56:28:977 A logon was attempted using explicit creden... Windows
Main 20.11.2024 15:56:28:977 An account was logged off. Windows
Информация о событии
Копировать
TenantID Main
Timestamp 20.11.2024 15:56:52:174
Name An account was logged off.
EndTime 20.11.2024 15:57:50:548
DeviceAssetID dc-01.sales.lab
DeviceEventCategory Microsoft-Windows-Security-Auditing
DeviceEventClassID 4634
DeviceHostName dc-01.sales.lab
DeviceNtDomain SALES
DeviceProduct Windows
DeviceReceiptTime 20.11.2024 15:57:50:548
DeviceTimeZone +03:00
DeviceVendor Microsoft
DestinationAccountID officer
DestinationAssetID
DestinationHostName
Информация об учетной записи
Найти похожие события


Информация об учетной записи
Копировать
Реагирование через Active Directory
Display name
officer
Common Name
officer
Distinguished name
cn=officer,cn=users,dc=sales,dc=lab
User logon name
officer
Имя участника-пользователя (UPN)
officer@sales.lab
Member Of
{ cn=presales,cn=users,dc=sales,dc=lab }
User account control
66048
Дополнительная информация
Создано
12.12.2023 16:28:12
Account expires
14.09.30828 05:48:05
Bad password time
22.04.2024 16:11:04
lastlogon
133764096560281167
lastlogontimestamp
133763983369589900

> В случае если проведенные выше действия не обогащают данные перезагрузите службу коллектора и снова проверьте обогащение

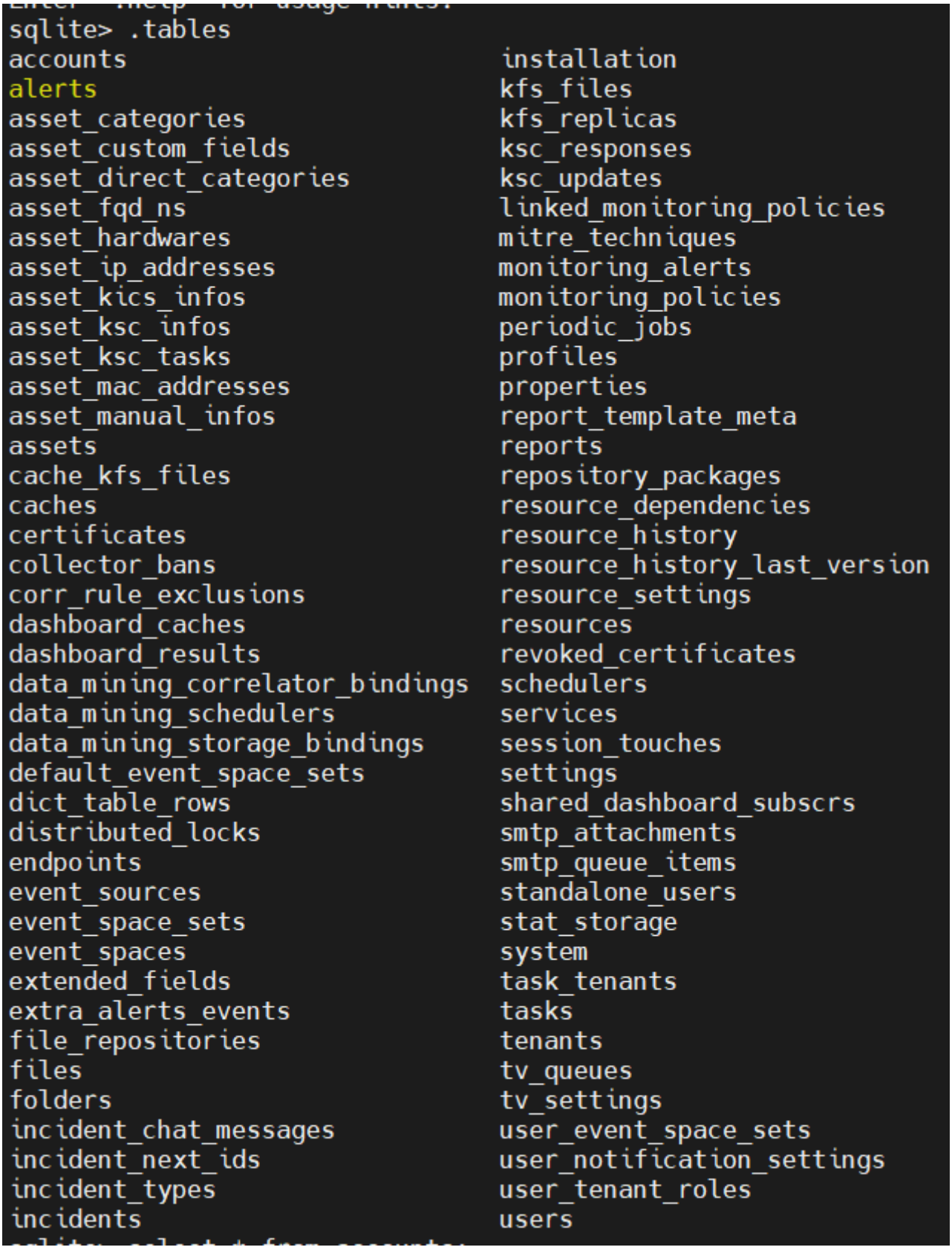
> Если рекомендация выше не помогла, попробуйте указать только те домены которые есть в базе, иначе (если не помогло) попробуйте сделать обогащения по одному домену

??????????? ? ???? ?????? ??? ?????? 4.0 ? ????

Чтобы подключиться к базе данных выполните команду:

```
sqlite3  /opt/kaspersky/kuma/core/00000000-0000-0000-0000-000000000000/raft/sm/db
```

чтобы просмотреть все таблицы выполните команду внутри СУБД `.tables`



Например, для просмотра учетных записей и соотношения их доменов в таблице аккаунтов, вы можете воспользоваться командой

```
select domain, cn from accounts where domain is not null;
```

```
sqlite> select domain, cn from accounts where domain is not null;
TRUECOMPANY.LOCAL|администратор
TRUECOMPANY.LOCAL|[redacted]
TRUECOMPANY.LOCAL|svc-kuma
TRUECOMPANY.LOCAL|[redacted]
TRUECOMPANY.LOCAL|[redacted]
TRUECOMPANY.LOCAL|svc-kuma-wec
TRUECOMPANY.LOCAL|[redacted]
TRUECOMPANY.LOCAL|svc-kuma-ldap
TRUECOMPANY.LOCAL|[redacted]
TRUECOMPANY.LOCAL|[redacted]
TRUECOMPANY.LOCAL|[redacted]
TRUECOMPANY.LOCAL|svc-kuma-agent
TRUECOMPANY.LOCAL|[redacted]
TRUECOMPANY.LOCAL|ivan ivanov
TRUECOMPANY.LOCAL|svc.kuma.ldap
TRUECOMPANY.LOCAL|svc.kuma.wmi
TRUECOMPANY.LOCAL|svc.kuma.wec
TRUECOMPANY.LOCAL|svc.kuma-test.wec
TRUECOMPANY.LOCAL|svc.kuma-test-ad
```

Для более подробной информации добавьте параметр, например, **member_of** `select domain, cn, member_of from accounts where domain is not null;`

```
TRUECOMPANY.LOCAL|ivan ivanov|{"cn=hr,cn=users,dc=truecompany,dc=local":true}
TRUECOMPANY.LOCAL|svc.kuma.ldap|{}
TRUECOMPANY.LOCAL|svc.kuma.wmi|{"cn=читатели журнала событий,cn=builtin,dc=truecompany,dc=local":true}
TRUECOMPANY.LOCAL|svc.kuma.wec|{}
TRUECOMPANY.LOCAL|svc.kuma-test.wec|{}
TRUECOMPANY.LOCAL|svc.kuma-test-ad|{}
```

Revision #20
Created 2023-08-11 14:33:12 UTC by Boris Rzr
Updated 2026-04-07 07:40:39 UTC by Boris Rzr