

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

Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **HE** 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.

Параметры подключения



*Название

*Секрет

*URL

Используйте запятую в качестве разделителя, чтобы указать несколько URL

Тип

Сертификат

Время ожидания в секундах

*База поиска (Base DN)

Пользовательские атрибуты учетных записей AD

Добавить атрибут

Выключено

Дублировать подключение

Удалить

Импортировать учетные записи

Сохранить

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

Интеграция с LDAP-сервером

[Добавить подключение](#) [Импортировать учетные записи](#)

Выключено

Интервал обновления в часах

24

⚠ Запланированное обновление: 05.06.2023 11:10:06

*Тенант

Main

Подключения

Название	База поиска (Base DN)	Выключено
LDAP_enrich	dc=example,dc=org	

*Время хранения

данных

90

Количество дней, в течение которых данные об учетной записи хранятся в KUMA после того, как сведения о ней перестают поступать через LDAP

[Сохранить](#)

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**.

- 1 Подключение источников
- 2 Транспорт
- 3 Парсинг событий
- 4 Фильтрация событий
- 5 Агрегация событий
- 6 Обогащение событий**
- 7 Маршрутизация
- 8 Проверка параметров

Обогащение событий

Дополните события необходимыми данными. Подробнее см. [в онлайн-справке](#).

Поле KUMA	Подпись	
DeviceAction		
ApplicationProtocol		
DeviceCustomIPv6Address1		
DeviceCustomIPv6Address...		

+ 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 наименования деплоя:

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

Получим следующий вывод:

```
[root@kuma-3 ~]# k0s kubectl get pods --all-namespaces
```

NAMESPACE	NAME	READY	STATUS
ingress	ingress-cdv5m	1/1	Running
ingress	ingress-crmf8	1/1	Running
kube-system	calico-kube-controllers-555bc4b957-9bxhl	1/1	Running
kube-system	calico-node-xcc2z	1/1	Running
kube-system	calico-node-zk4lc	1/1	Running
kube-system	coredns-ddddfb5c-p76k6	1/1	Running
kube-system	konektivitiy-agent-7cvpx	1/1	Running
kube-system	konektivitiy-agent-t274d	1/1	Running
kube-system	kube-proxy-vqgw8	1/1	Running
kube-system	kube-proxy-xvvg6	1/1	Running
kube-system	metrics-server-7d7c4887f4-wxht4	1/1	Running
kuma	core-deployment-8659b48bb6-45grz	5/5	Running
local-path-storage	local-path-provisioner-759f6bd7c9-nldxg	1/1	Running
longhorn-system	csi-attacher-767646d98c-5cjpj	1/1	Running
longhorn-system	csi-attacher-767646d98c-c66rp	1/1	Running
longhorn-system	csi-attacher-767646d98c-dg88d	1/1	Running
longhorn-system	csi-provisioner-76c7844bc4-bnjt8	1/1	Running
longhorn-system	csi-provisioner-76c7844bc4-llsvm	1/1	Running

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.

Для сопоставления доменов с учетными записями LDAP необходимо настроить подключение в разделе [Параметры](#).

*Сопоставление с учетными записями LDAP

+ Добавить домен DEMO.LAB ✕ Сбросить

*Обогащение полей KUMA

Поле KUMA	LDAP-атрибут	Поле для записи данных	
SourceUserID	objectSID	SourceAccountID	✕
DestinationUserID	objectSID	DestinationAccou...	✕
SourceUserName	sAMAccountName	SourceAccountID	✕
DestinationUserN...	sAMAccountName	DestinationAccou...	✕
SourceUserName	userPrincipalName	SourceAccountID	✕
DestinationUserN...	userPrincipalName	DestinationAccou...	✕
SourceUserName	mail	SourceAccountID	✕
DestinationUserN...	mail	DestinationAccou...	✕

+ Добавить элемент Применить сопоставление по умолчанию

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.

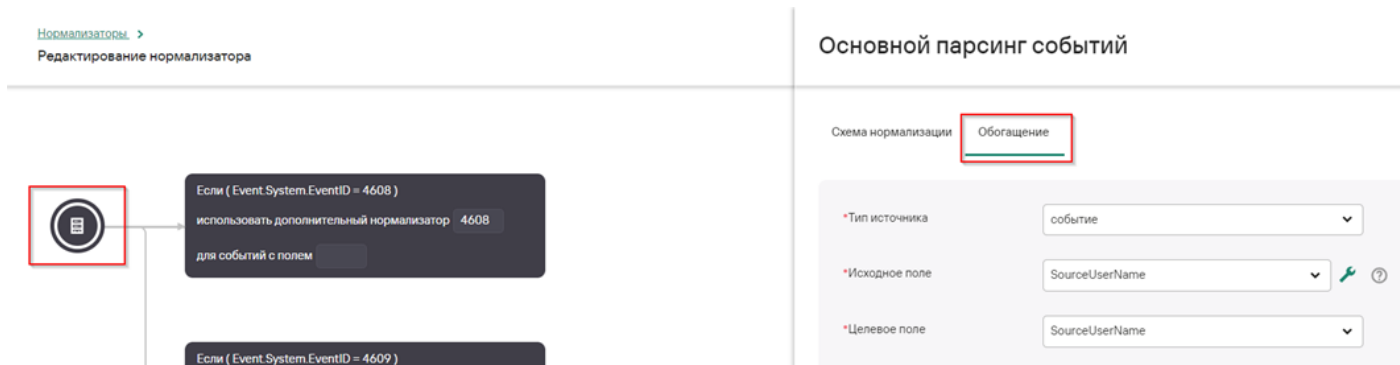
?????????? ??????????

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.

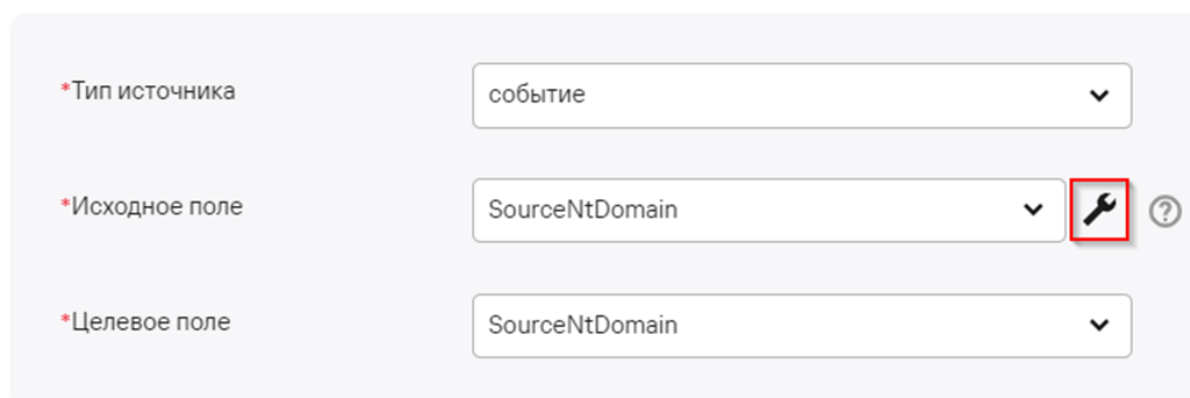
Данная проблема решается доработкой нормализатора Windows.

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



Прокрутите 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`.

Преобразование ✕

Измените содержимое исходных полей. Порядок преобразований имеет значение.

☰ ✕

* Тип преобразования

replaceWithRegex ▾

Редактирование

выражение чем заменить

+ Добавить преобразование

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**.

Преобразование ×

Измените содержимое исходных полей. Порядок преобразований имеет значение.

☰×

* Тип преобразования

replaceWithRegex▼

Редактирование

^DEMOS

DEMO.LAB

+ Добавить преобразование

Отмена

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.

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`

Enter 'help' for usage hints:

```
sqlite> .tables
accounts                               installation
alerts                                  kfs_files
asset_categories                        kfs_replicas
asset_custom_fields                    ksc_responses
asset_direct_categories                 ksc_updates
asset_fqd_ns                            linked_monitoring_policies
asset_hardwarees                       mitre_techniques
asset_ip_addresses                     monitoring_alerts
asset_kics_infos                       monitoring_policies
asset_ksc_infos                        periodic_jobs
asset_ksc_tasks                        profiles
asset_mac_addresses                   properties
asset_manual_infos                    report_template_meta
assets                                  reports
cache_kfs_files                       repository_packages
caches                                  resource_dependencies
certificates                           resource_history
collector_bans                         resource_history_last_version
corr_rule_exclusions                   resource_settings
dashboard_caches                      resources
dashboard_results                     revoked_certificates
data_mining_correlator_bindings       schedulers
data_mining_schedulers                 services
data_mining_storage_bindings          session_touches
default_event_space_sets              settings
dict_table_rows                       shared_dashboard_subscrs
distributed_locks                     smtp_attachments
endpoints                              smtp_queue_items
event_sources                          standalone_users
event_space_sets                      stat_storage
event_spaces                           system
extended_fields                       task_tenants
extra_alerts_events                   tasks
file_repositories                     tenants
files                                  tv_queues
folders                                tv_settings
incident_chat_messages                user_event_space_sets
incident_next_ids                     user_notification_settings
incident_types                        user_tenant_roles
incidents                             users
```

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 | valery karpin
TRUECOMPANY.LOCAL | svc-kuma
TRUECOMPANY.LOCAL | finbar sandan
TRUECOMPANY.LOCAL | lisa faga
TRUECOMPANY.LOCAL | svc-kuma-wec
TRUECOMPANY.LOCAL | alexander kabanov
TRUECOMPANY.LOCAL | svc-kuma-ldap
TRUECOMPANY.LOCAL | alexander galov
TRUECOMPANY.LOCAL | alexander karpin
TRUECOMPANY.LOCAL | alexander
TRUECOMPANY.LOCAL | svc-kuma-agent
TRUECOMPANY.LOCAL | valery karpin
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**

```
TRUECOMPANY.LOCAL | valery karpin | {"cn=valery karpin,dc=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