

AD/LDAP/ALD Pro

Интеграции с различными службами каталогов

- Интеграция KUMA с Active Directory (AD)
- Интеграция KUMA с ALD Pro
- Выгрузка LDAP информации в словарь KUMA

Интеграция KUMA с Active Directory (AD)

При интеграции с AD/ADFS важно иметь единое время на системах, настоятельно рекомендуется настроить NTP

<https://www.youtube.com/embed/1Rw6qOWF7jc?si=vOId0Aj4wFH-Vr47>

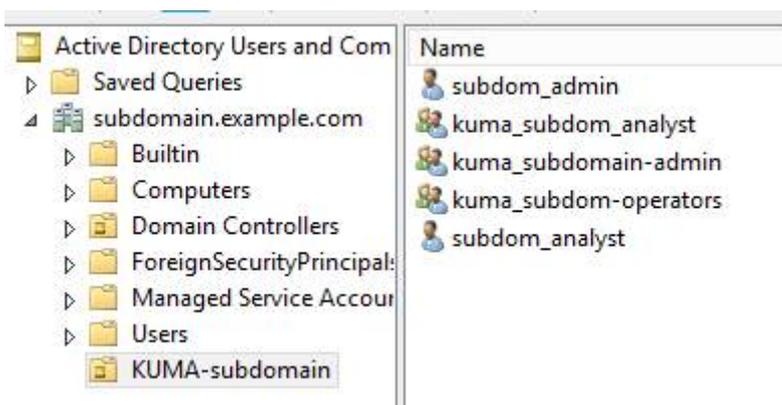
Аутентификация работает только для одного домена. Поэтому все группы должны быть созданы в корневом домене.

Пример инфраструктуры AD:

- корневой домен леса - example.com
- контроллер домена - dc-01.example.com
- дочерний домен - subdomain.example.com

В дочернем домене созданы:

- OU «KUMA subdomain»
- Universal группы безопасности: «kuma_subdomain_analyst», «kuma_subdomain_admin», «kuma_subdomain_operators»
- Пользователи: subdom_admin, subdom_analyst



Пользователи являются членами соответствующих групп:

```
PS C:\Users\Administrator> get-aduser -identity subdom_analyst -properties CN,memberOf,UserPrincipalName

CN                : subdom_analyst
DistinguishedName : CN=subdom_analyst,OU=KUMA-subdomain,DC=subdomain,DC=example,DC=com
Enabled           : True
GivenName        : subdom_analyst
MemberOf         : {CN=kuma_subdom_analyst,OU=KUMA-subdomain,DC=subdomain,DC=example,DC=com}
Name             : subdom_analyst
ObjectClass      : user
ObjectGUID       : 8eaf5558-0966-4de0-a957-5e0cefcb461d
SamAccountName   : subdom_analyst
SID              : S-1-5-21-1445412355-99643495-187345912-1112
Surname          :
UserPrincipalName : subdom_analyst@subdomain.example.com
```

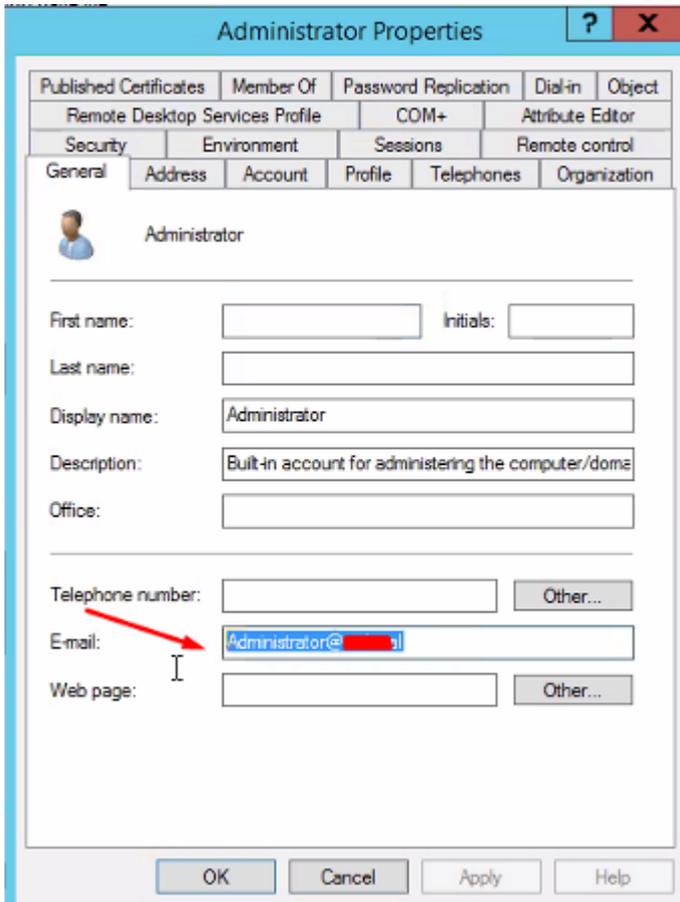
Настройки KUMA

Base DN - корневой домен (**не обязательно весь корневой домен**, зависит от вашего AD)

URL - контроллеры корневого домена, порт глобального каталога (**обязательно**)

Важно:

- Все группы доступа должны быть UNIVERSAL
- У пользователей в AD должно быть заполнен атрибут **email**



The screenshot shows the 'Administrator Properties' dialog box with the 'General' tab selected. The 'E-mail' field is highlighted with a red arrow and contains the text 'Administrator@' followed by a redacted domain name. The 'Display name' field contains 'Administrator' and the 'Description' field contains 'Built-in account for administering the computer/dome'.

Далее – для каждого тенанта указываете DistinguishedName групп, соответствующих правам доступа.

Connection

*Base DN	<input type="text" value="DC=example,DC=com"/>
*URL	<input type="text" value="dc-01.example.com:3268"/> <small>Use comma as a delimiter to enter multiple URLs</small>
Secret	<input type="text" value=""/> <small>+ [edit icon]</small>
TLS mode	<input type="text" value="Disabled"/>
Timeout in seconds	<input type="text" value="0"/>
General administrator	<input type="text" value="CN=kuma_example-admin,OU=KUMA,DC=example,DC=com"/>

Role filters

*Tenant	<input type="text" value="Main"/>
Operator	<input type="text" value="CN=kuma_subdom_operators,OU=KUMA-subdomain,DC=subdomain,DC=example,DC=com"/>
Analyst	<input type="text" value="CN=kuma_subdom_analyst,OU=KUMA-subdomain,DC=subdomain,DC=example,DC=com"/>

Информация по ролям и их возможностям: <https://support.kaspersky.com/help/KUMA/2.1/ru-RU/218031.htm>

Важный момент:

- Предоставление доступа происходит по принципу «**наименьших прав**». Если учетка пользователя одновременно состоит нескольких в группах одного тенанта.
- Например: kuma-analysts и kuma-admins, то пользователь получит права аналитика. Поэтому, при переводе работников из операторов в аналитики или аналитиков в админы, необходимо не только добавить пользователя в соответствующую новую группы, но еще и удалить из старой группы.

Результат

Для доменной аутентификации, как таковой учетки в KUMA не требуется. Когда все настроено, вводится доменный логин и пароль и в этот момент KUMA биндится к LDAP.

При аутентификации, пользователь вводит в консоль свою доменную учетку в формате UPN (user@example.com) и, на основании членства этой учетки в той или иной группе, пользователю предоставляется доступ к разным тенантам с указанными правами.

- Залогинившись под доменной учеткой subdom_analyst@subdomain.example.com
- Получаем права роли analyst в тенанте Main

The screenshot displays the KUMA interface. The browser's address bar is at the top, showing the URL 'kuma.example.com:7220/dashboard'. The dashboard header includes the Kaspersky logo and the text 'Kaspersky Unified Monitoring and Analysis Platform'. A sidebar on the left lists various navigation options: Dashboard, Alerts, Incidents, Events, Assets, Reports, Resources, and Task manager. The main dashboard area is titled 'Dashboard' and shows a timestamp 'Updated 10/25/21, 6:21 PM'. Below this, there are two panels: 'Alerts by Priority' and 'Alerts by Assign', both for the 'Main' tenant, which currently show 'No records'. On the right side, a 'User' profile is displayed, with a red vertical line highlighting the 'Name', 'Login', and 'Email' fields. The 'Name' field contains 'Subdom_analyst', the 'Login' field contains 'subdom_analyst@subdomain.example.com', and the 'Email' field contains 'subdom_analyst@subdomain.example.com'. Below these fields, the 'Tenants for roles' section is visible, with the 'analyst role' highlighted in yellow. Underneath, the 'Main' tenant is listed with a small gear icon.

Пример входа в KUMA с доменной учетной записью (kuma-admin@sales.lab):



Kaspersky

Unified Monitoring and Analysis Platform



Войти

Права API можно выдавать только для внутренних пользователей, не из AD

Порты AD

- Порт **3268**. Этот порт используется для запросов, специально предназначенных для глобального каталога. Запросы LDAP, отправленные на порт 3268, можно использовать для поиска объектов во всем лесу. Однако могут быть возвращены только атрибуты, помеченные для репликации в глобальный каталог. Например, отдел пользователя не может быть возвращен через порт 3268, так как этот атрибут не реплицируется в глобальный каталог.
- Порт **389**. Этот порт используется для запроса информации с локального контроллера домена. Запросы LDAP, отправленные на порт 389, можно использовать для поиска объектов только в домашнем домене глобального каталога. Однако запрашивающее приложение может получить все атрибуты этих объектов. Например, запрос на порт 389 может быть использован для получения отдела пользователя.
- При интеграции с SSL необходимо использовать сертификат Active Directory. В KUMA поддерживаются открытые ключи сертификата X.509 в Base64. Стандартный порт LDAPS - **636**.

Полезные команды

```
PS C:\Users\osepov> Get-ADUser -Identity kuma-admin
```

```
DistinguishedName : CN=kuma-admin,OU=admins,OU=Users,OU=MSK,DC=sales,DC=lab
Enabled           : True
GivenName        : kuma-admin
Name             : kuma-admin
ObjectClass      : user
ObjectGUID       : 0d81928e-e8db-48bb-84b9-d00ad552bdd9
SamAccountName   : kuma-admin
SID              : S-1-5-21-781213047-594974509-2262175553-1700
Surname          :
UserPrincipalName : kuma-admin@sales.lab
```

Интеграция KUMA с ALD Pro

Интеграция является не официальной

Документация по службе каталогов для Linux Astra ALD Pro: <https://astra.ru/software-services/application-software-astra-group/ald-pro/#docs>

Настройки выполняются по аналогии со статьей: <https://kb.kuma-community.ru/books/integracii/page/integraciia-kuma-s-active-directory-ad>

При интеграции с ALD Pro важно иметь единое время на системах, настоятельно рекомендуется настроить NTP

Выберите тип интеграции FreeIPA и группы для учетных записей заводите в таком виде:

```
uid=is.ldap.usr,cn=users,cn=accounts,dc=company,dc=com
```

Пример настроенной интеграции:

Доменная аутентификация

Пользователи

Группы

Доменная аутентификация

Угрозы

sky Threat Lookup

sky CyberTrace

Центры

sky Security Center

sky Industrial
Security for Networks

sky Automated
Security Awareness
Management

sky Endpoint
Protection and Response

Сервер

САР

1

И

Подключение установлено.

Подключение установлено.

Активов

Тип аутентификации

FreeIPA

FreeIPA

Выключено

*База поиска (Base DN)

cn=users,cn=accounts,dc=company

*URL

10.10.10.10:389

Используйте запятую в качестве разделителя

*Режим TLS

незащищенный

Секрет

Время ожидания в секундах

0

Секрет пользовательской
интеграции

ALD Pro

Данные аутентификации

ALD Pro

Тест

Группы администрирования

Группа администраторов

CN=Domain Admins,CN=Users,DC=company

В итоге доменная аутентификация работает и пользователи появлялись с заданными правами.

Выгрузка LDAP информации в словарь KUMA

Предварительно нужно выполнить настройку обогащение по этой статье <https://kb.kuma-community.ru/books/integracii/page/ldap-obogashhenie>

Шаг 1.

Нам нужно выгрузить сопоставление, например login(sAMAccountName)-mail. Создаете словарь типа таблица (важно), ключ login, колонка mail. Добавляете одну запись любую, чтобы сохранить словарь можно было.

[Словари](#) >
Изменить словарь

*Название

*Тенант

Описание

*Тип

*Значения Всего: 1

Если нужно выгрузить другое поле, посмотрите его название по примеру вывода одной записи из обогащения:

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

Шаг 2.

Выбираете пользователя в KUMA, даете ему права на запрос POST /dictionaries/update, генерируете токен и записываете себе куда-нибудь (например в блокнот).

Шаг 3.

На коре выполняете скрипт (нужно поставить утилиту jq):

```
echo 'login,mail' > /tmp/accounts.csv; /opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --eval
'DBQuery.shellBatchSize=<SIZE>; db.accounts.find({"archived":false}, {"displayName":1,
"sAMAccountName":1, "_id":0})' | grep -E '^{' | jq '.sAMAccountName,.displayName' | sed 'N;s\n/,/' | sed 's/"/g'
>> /tmp/accounts.csv; curl -k --request POST
'https://<KUMA_IP>:7223/api/v1/dictionaries/update?dictionaryID=<DICTIONARY_ID>' --header 'Content-Type:
multipart/form-data' --header 'Authorization: Bearer <TOKEN>' --form 'file=@"/tmp/accounts.csv"; rm -rf
/tmp/accounts.csv
```

- где **<SIZE>** - число записей в выводе, нужно ставить значение кол-во пользователей*1.1
/opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --quiet --eval
"db.accounts.find({"archived":false}, {"displayName":1, "sAMAccountName":1, "_id":0}).count()" полученное число умножить на 1.1 Или сразу посчитать с помощью: perl -w -e "use POSIX; print ceil(\$(/opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --quiet --eval "db.accounts.find({"archived":false}, {"displayName":1, "sAMAccountName":1, "_id":0}).count()")*1.1), qq{\n}"
- **<KUMA_IP>** - ip-адрес ядра KUMA
- **<DICTIONARY_ID>** - id словаря, можно скопировать из строки браузера, если зайти в словарь
- **<TOKEN>** - токен для доступа к API, скопированный на Шаге 2.

После выполнения скрипта, в словарь запишутся логины и их электронная почта, импортированные из AD.

Более продвинутый заполненный запрос с автоподсчетом **<SIZE>**:

```
SIZE=$(perl -w -e "use POSIX; print ceil($(/opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --quiet --eval "db.accounts.find({"archived":false},{\"sAMAccountName\":1, \"mail\":1, \"_id\":0}).count())*1.1), qq{\\n}");
echo 'login,mail' > /tmp/accounts.csv; /opt/kaspersky/kuma/mongodb/bin/mongo localhost/kuma --eval
'DBQuery.shellBatchSize='$SIZE'; db.accounts.find({"archived":false},{\"sAMAccountName\":1, \"mail\":1,
\"_id\":0})' | grep -E '^{' | jq '.sAMAccountName,.mail' | sed 'N;s\\n/,/' | sed 's/^//g' >> /tmp/accounts.csv; curl -k --
request POST 'https://10.68.85.125:7223/api/v1/dictionaries/update?dictionaryID=72323930-c4fb-43c7-9360-
5f8d5d929bbb' --header 'Content-Type: multipart/form-data' --header 'Authorization: Bearer
29ed4e42e25f7877c5ceb435736f860f' --form 'file=@"/tmp/accounts.csv"; rm -rf /tmp/accounts.csv
```