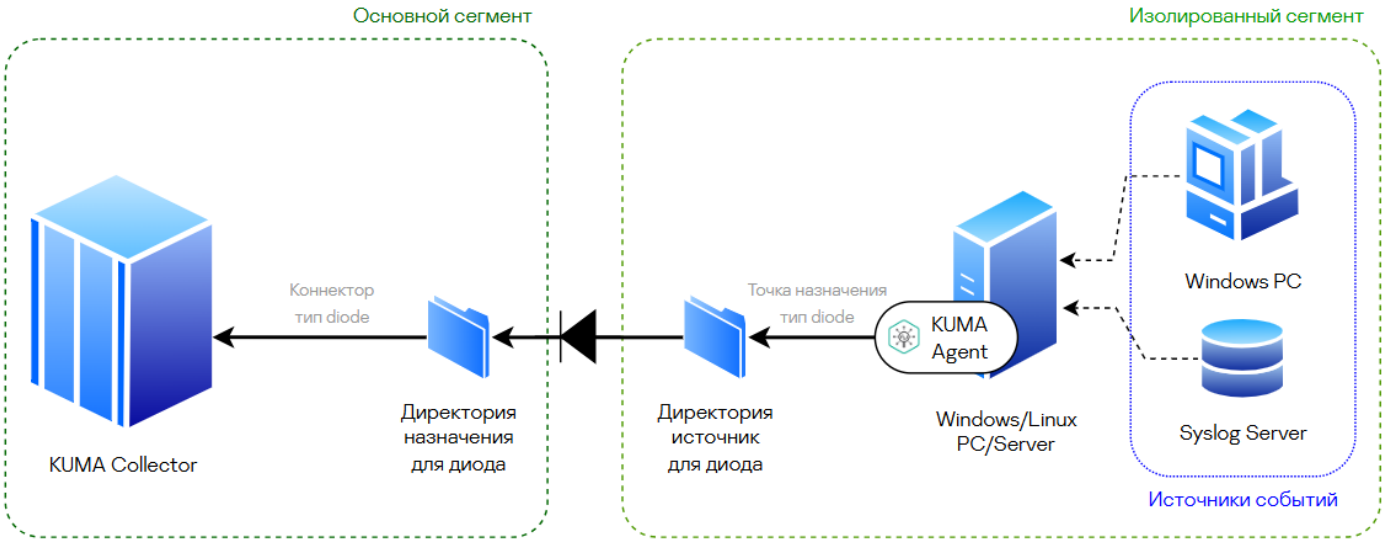
Установка агента в режиме диод (Diode)

Схема работы сбора в режиме diode



?????, ??????????? ? ????????????? ???????? ????, ???????? ??????? ? ?????????? ? ?????????? ?? ? ?????????? ????????, ?????? ?? ???????? ???? (????-????) *(????????? ?????????????, ??? ??????? KUMA)*. ???? ????????? ????? ? ?????????? ?????????? ???????? ????, ?????? ?? ?????????? ?????????. ?? ?????????? ?????????? ??????? ???????? ?????????, ?????? ?? ????? ??????????.

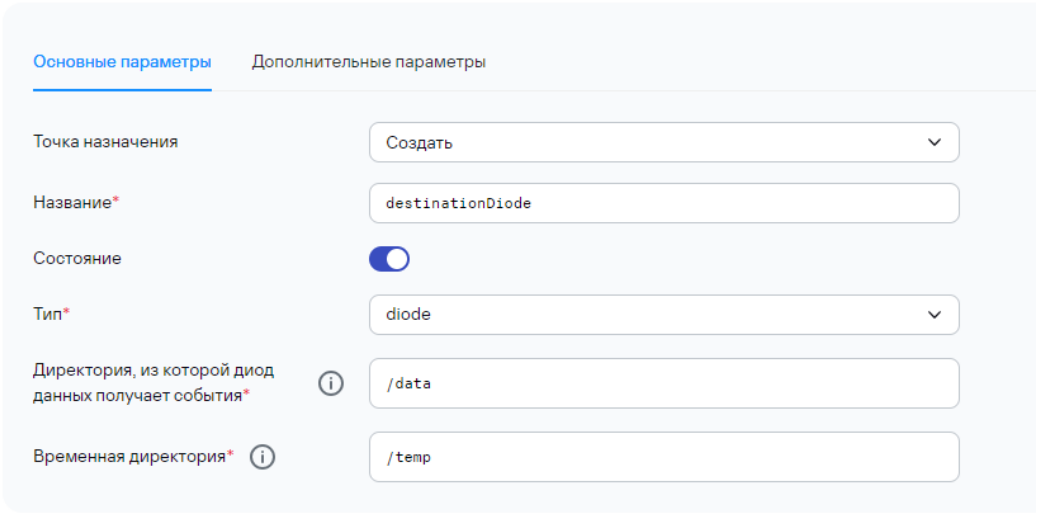
? KUMA ?????? ?? 4.2 ????????? ???????? ????? ?????????? ??????????? UDP

??? ????????????? ?????????? ??????? ???????? ??????? ????? ???? ??????????? ???? destination ? connector ???? diode, destination ?? ?????? ? connector ?? ??????????. ????? ????? ????? ????? ?? ????????? ????? connector, ? ????????? - ????? ?? ????????? destination.

????? ??? ?????? ??????????? ??????? ? ?????. ??? ?????? ????? ?????????? ???????? >=bufferSize (?? ????????? 64 ??), ??? ? ??????? ?????????? ?????? ?????? ? ???? ???????? > FlushInterval (?? ????????? 10 ???):

- ????? ?????????? ??????? ? ???? ?? ????????? ??????????, ????????? ????????????
- ????? ????????? ???? ?? ????????? ????? ? "??????????, ?? ??????? ???? ?????? ???????? ??????? (Data diode source directory)" , ??????? ????????????? ????. ???????? ????? ???????? sha256 ??? ??????????? ??? ??????????? ????????????? ???????? ???????????.

Точки назначения



?? ????????? ?????? ?????? ?? ??????????, ?? ??? ????? ????????????, ???? ??????? ? ?????????? destination ?????? ?????. ? ???? ?????? ??? ?????????? ?????? ??? ?? ???????? ?????? ???? ?????? ? ??????????????? diode connector.

??? ?????????? (diode connector) sha256 ??? ??????????? ????? ???????????? ? ????? ?? ????? ?????, ??? ????????????? ???? ????????? ? ????????? ??????? ??????.

> ?????? ????? ?????????? ? ?????? ?????? ????? ??? diode. ? ???? ??????? ?????????? ??????? ??????????, ?? ??????? ???? ?????? ????? ?????????? ????? ?? ??????? ??????? ????.

> ??? diode-?????? ?????????? ??????? ?????????? ???? sql ??? netflow.

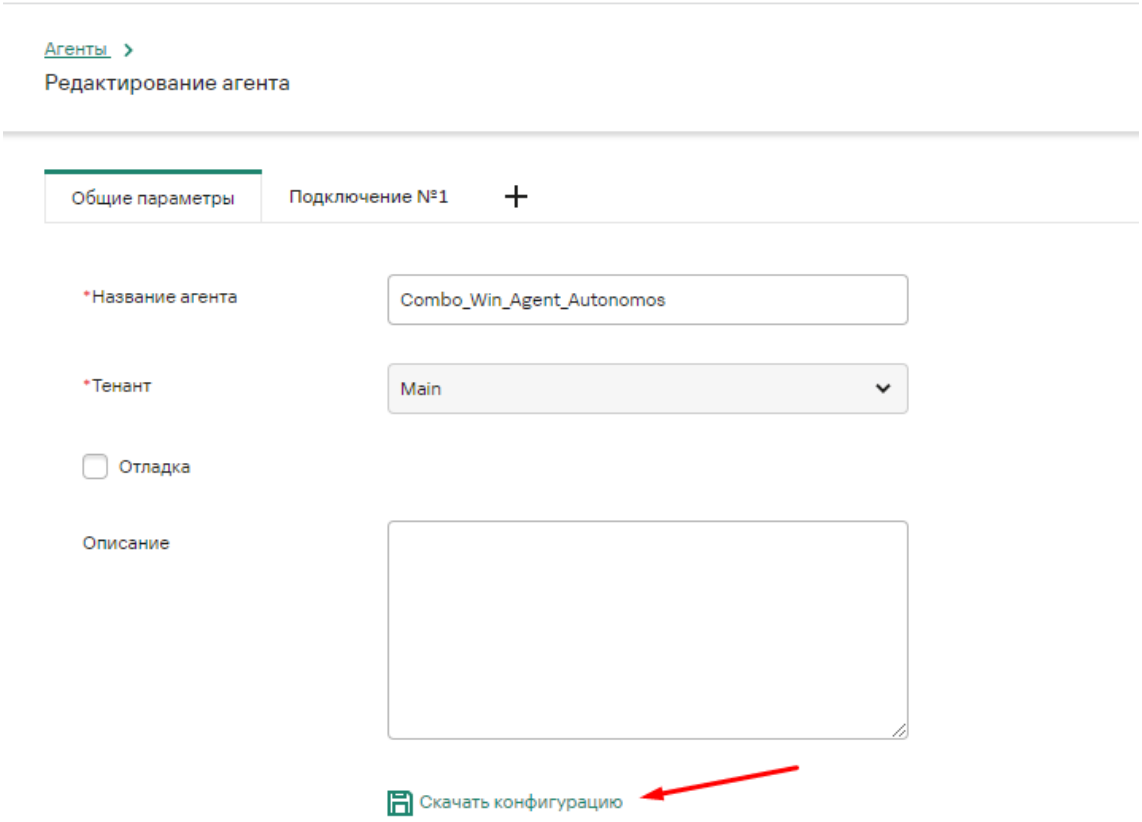
Конфигурационный файл

????????????? ???? ?????? ??????????? ? ?????????????? ???? ??? ??????????? ?????????? ???????? ???????. ??? ????????? ?????????? ???????? ? ???????? ????, ?????????? ???????? ???????? ?????????? ?? ??????? ?????????????? ???? ???????, ????? ? ?????????????? ????? ???????????? ??????? ? ??????, ??? ??? ???? ??????? (?? ?. ??????? ????????). ? ???????? ?????? ??????, ???????????? ??????? ?????? UUID ???????, ?????????? ???????? ????????? ???????? ? ???? secrets. ?????? ???????? ????? ????????? ??????? ? ?????????????? ?????, ??????? ???? ????????.

????? ? ??????? ??????? ???? ???????.

Имя поля	Тип	Описание
user	строка	Имя пользователя
password	строка	Пароль
token	строка	Токен
urls	массив строк	Список url
publicKey	строка	Публичный ключ (используется в PKI)
privateKey	строка	Приватный ключ (используется в PKI)
pfx	строка, содержащая base64 закодированное содержимое pfx	Содержимое pfx файла, закодированное в base64. На linux получить base64 кодировку файла можно при помощи команды base64 -w0 src > dst
pfxPassword	строка	Пароль от pfx
securityLevel	строка	Используется в snmp3. Возможные значения: NoAuthNoPriv, AuthNoPriv, AuthPriv
community	строка	Используется в snmp1
authProtocol	строка	Используется в snmp3. Возможные значения: MD5, SHA, SHA224, SHA256, SHA384, SHA512
privacyProtocol	строка	Используется в snmp3. Возможные значения: DES, AES
privacyPassword	строка	Используется в snmp3
certificate	строка, содержащая base64 закодированное содержимое pem	Содержимое pem файла, закодированное в base64. На linux получить base64 кодировку файла можно при помощи команды base64 -w0 src > dst

?????????????? ???? ??????????? ?? ???-?????????? ???? KUMA ? ????? ???????? ??????:



Запуск агента (автономный агент)

??? ????????? ?????? ??? ???????????????? ???? ?? ?????? ?????????? ? ??????????, ? ??????? ???????????????? ?????.

?????????? ??? ?????? ?????? ???????? ??????? (ACL) ????????? ????? ??????? ? ???????????????? ????? ???, ????? ?????? ?? ?????? ????? ??? ?????? ? ???????????, ??? ??????? ????? ???????? ?????.

TLS ?? ????????, ?? ????????? ??????????? ? ????.

?????????? ?????????? ?? ??????????? ???????? ?? ???????: `kuma.exe help agent`

Linux

??????? ???????????? ??????????: `/opt/kaspersky/kuma/kuma license`

??? ??????? ?????? ????????? ??????????? ???? /opt/kaspersky/kuma/kuma ? ??????, ??? ??????????? KUMA ?? ?????? ? linux, ??? ????? ??????? ????? ? ????????? ???: `./kuma agent --cfg <path to config file> --wd <path to working directory>`
????? ????? --wd ??????????? ???? ??? ???????? ?????? ??????, ?? ????????? ??? ????? ????????? ? ??????? ??????????.

???????????????? ???? ????? ????????? ???????, ??? ??????? ???????? ??? ?????? ACL, ??????????? ?????? ?????? ???????????? KUMA (600).

Windows

??????? ???????????? ??????????: `/opt/kaspersky/kuma/kuma.exe license`

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

```
kuma.exe agent --cfg <path to config file>
```

```
kuma.exe  agent --cfg <???? ? ???????????????? ????? ??????> --wd <???? ? ??????????, ??? ????? ??????????
????? ???????????????? ??????. ???? ?? ????????? ???? ????, ????? ????? ????????? ? ??????????, ??? ??????????
???? kuma>
```

? ??????????

```
kuma.exe agent --cfg <path to config file> --user <user to start service as> --install
```

??? ????????? ???????????? ???????????????? ???? ???????????? ? ??????? ?????????? (`ProgramData\Kaspersky Lab\KUMA\agent\<serviceID>\`) (ID ??????? ?? ??????? ?????? ? ???????????????? ?????), `kuma.exe` ???????????? ? ??????? ?????????? (`Program Files\Kaspersky Lab\KUMA`).

? ?????????? ???????????? ???????????? ???????????????? ????.

?????????????? ???? ????? ????????? ???????, ??? ??????? ???????? ??? ?????? ACL, ?????????? ?????? ?????? ???????????? ?? ????? ???? ??????????? KUMA.

Удаление

```
kuma.exe agent --cfg <path to config file> --uninstall
```

???

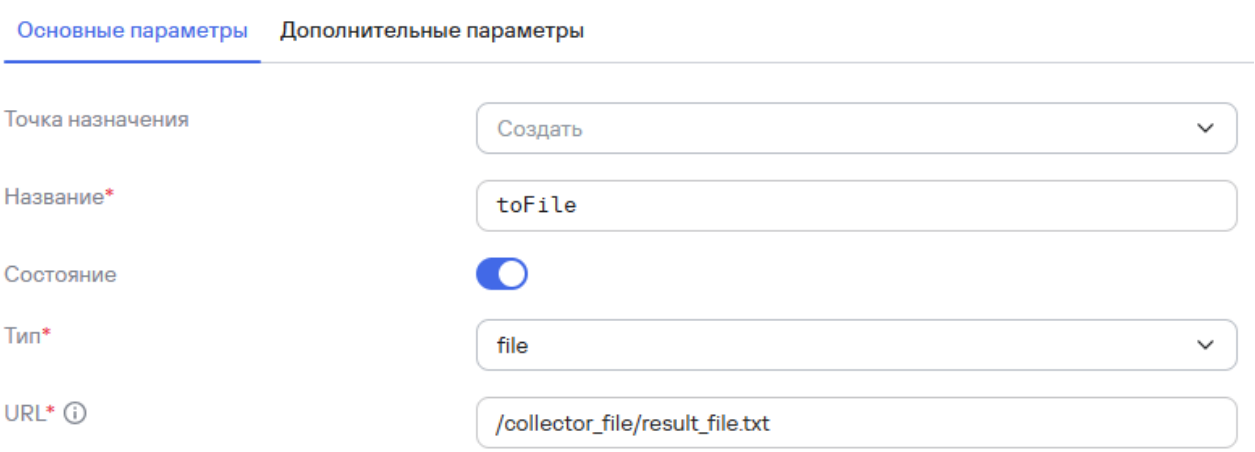
```
kuma.exe agent --id <????????????? ??????? ??????, ?????????? ? KUMA> --uninstall
```

Сбор коллектором из изолированного сегмента

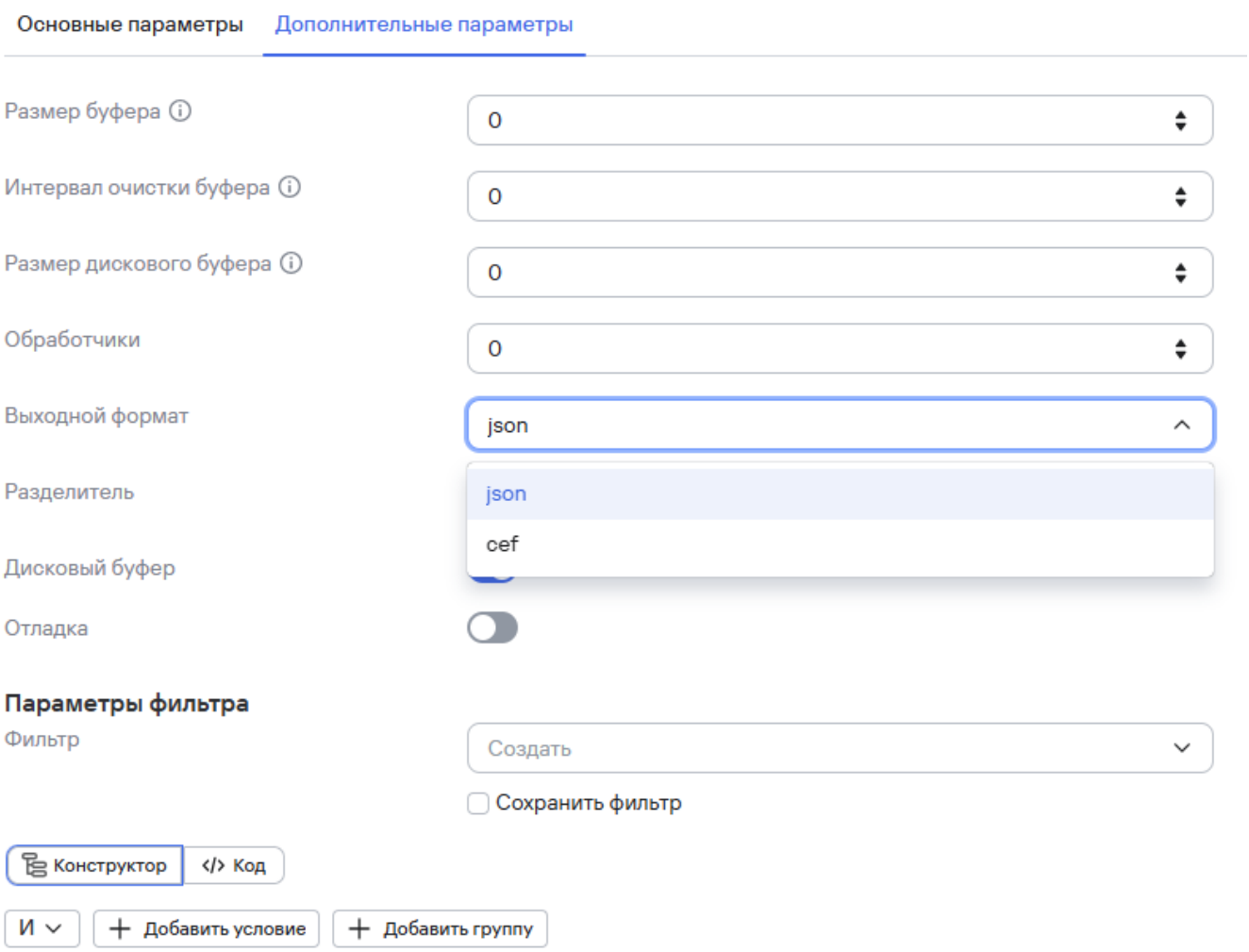
??? ????????? ?????????? (?.?. ????? ???????????? ?? ??? ???? ???????????) ?????????? ????? ? ?????, ??? ????? ?????? ????????????? ????????? ???? ? ????????????? ???????, ??????? ????? ????????? ???? ???????????. ????? ????????? ? ????????????? ????? ????????? ????????? ??????? ?? ? ?????????, ? ? ???? (????????: ????????????? ???? ?? ?????? ? ?? ??? JSON ?????? ??? CEF). ????????????? ?????????? ??????? ???? (?????) ? ???? ????? ??? ???????????? kuma:

```
chown -R kuma:kuma /collector_file/
chown -R kuma:kuma /collector_file/result_file.txt
```

Создание точки назначения



Создание точки назначения



????? ???? ???? ???????? ?????????? ????? ? ?????????? ?? ????? ? ???? ??????? ?? ????? ? ?????? ??????.

Revision #16
Created 2023-08-11 14:23:49 UTC by Boris Rzr
Updated 2025-12-10 10:43:50 UTC by Boris Rzr