KLMS

?????????, ??????????? ?? ?????? ????????, ???????? ??????????? ??????? pre-sales ?/??? community KUMA ? **HE** ???????? ??????????? ????????????? ???????.

??????????? ???????????? ?? ??????? ??????? ????????? ? ??????-??????? ?? ???????: https://support.kaspersky.com/help/KUMA/2.1/ru-RU/254786.htm

Настройка передачи событий KLMS в KUMA

????? ????????? ???????? ??????? KLMS ? KUMA:

1. ???????????? ? ??????? KLMS ?? ??????? SSH ??? ??????? ??????? ? ??????? ????????????? ????????? ? ???? Technical Support Mode.

2. ? ??????? ??????? `klms-control` ????????? ????????? ? ???? `settings.xml`:

```
sudo /opt/kaspersky/klms/bin/klms-control --get-settings EventLogger -n -f /tmp/settings.xml
```

3. ?????????, ??? ????????? ????? `/tmp/settings.xml` ????? ????????? ????????, ??? ????????????? ??????? ?????????:

```
<siemSettings>
<enabled>1</enabled>
<facility>Local1</facility>
```

4. ????????? ????????? ? ??????? ????????? ???????:

```
sudo /opt/kaspersky/klms/bin/klms-control --set-settings EventLogger -n -f /tmp/settings.xml
```

5. ??? ???????? ??????? ?? ????????? UDP ??????? ????????? ????????? ? ???????????????? ???? `/etc/rsyslog.conf`.

```
$WorkDirectory /var/lib/rsyslog
$ActionQueueFileName ForwardToSIEM
$ActionQueueMaxDiskSpace 1g
$ActionQueueSaveOnShutdown on
$ActionQueueType LinkedList
$ActionResumeRetryCount -1
local1.* @<IP-????? ?????????? KUMA>:<???? ??????????>
```

???? ?? ?????? ?????????? ??????? ?? ????????? TCP, ????????? ??????? ?????? ????????? ????????? ???????:

```
local1.* @@<IP-????? ?????????? KUMA>:<???? ??????????>
```

6. ????????? ????????? ?????????.

7. ????????????? ?????? rsyslog ? ??????? ????????? ???????:

```
sudo systemctl restart rsyslog.service
```

Настройка KUMA

????? ???? ??? ????????? ???????? ??????? ?????????, ????????? ??????? ????????? ? ???-?????????? KUMA ??? ??????? KLMS.

1. ?? ???? **Транспорт** ??????? ??? ? ???? ? ??????????? ? ??????????? ?? ??????? KLMS.

2. ?? ???? **Парсинг** ??????? ???????? ???????????? **[OOTB] KLMS syslog CEF**.

3. ?? ???? **Маршрутизация** ?????????, ??? ? ????? ???????? ?????????? ????????? ????????? ????? ???????????:

- Хранилище. ??? ???????? ???????????? ??????? ? ?????????.

- Коррелятор. ??? ???????? ???????????? ??????? ? ??????????.

???? ????? ?????????? **Хранилище** ? **Коррелятор** ?? ?????????, ???????? ??.

4. ?? ???? **Проверка параметров** ??????? **Сохранить и создать сервис**.

5. ?????????? ??????????? ??????? ??? ????????? ?????????? KUMA.

Полезные ссылки

????????? ????????? ??????? KLMS (??????-??????? KUMA):
https://support.kaspersky.com/help/KUMA/2.1/ru-RU/254786.htm

Revision #7
Created 2023-08-11 09:16:22 UTC by Koala
Updated 2024-11-26 12:49:49 UTC by Koala