Создание сервисов KUMA для SMP

Создание сервисов KUMA

? ??????? ??????? ???????? ????????? (Storage), ??????????? (Correlator) ? ?????????? (Collector) KUMA.

- ?????????, ??? ????, ?? ??????? ??????????? ????????? ??????? ???????? FQDN ???? KUMA, ???????? ??? ????????? SMP.

- ?????????, ??? ??????? SMP ???????? FQDN ?????, ?? ??????? ??????????? ????????? ??????? (FQDN ????? ?????? ??????????? ????? DNS-??????, ??????? ?????????? SMP).

- ? ?????? ??????? ?????????? ?? ?? ????? ? ????????? KUMA ?? ???????? ???????? ??????????? ??????? ??? ?????? ????????: API-?????, ????????? ? ??????? ???????? ???????? ? ????? ?????? ??????? ???????????, ???????? ? ?????????? ?????????? ?????????????? ???????????. ??????? ?????? ???????? **здесь**.

Подготовка целевого устройства для установки сервисов

???? ?????????? ??? ???????????? ? ????????? ???????? KUMA (??? ????????? SMP ??? ?????? ???? ????????? KUMA ? ??????? inventory) ?????????? ???? ?????? ? ?????????? ? ??????????.

???? ? ???????? ????????? SMP ?? ??? ?????? ???? ????????? KUMA ? ??????? inventory ? ?????????? ?? ???? ???????????? ??? ????????? ???????? - ?? ????? ??????????? ????? ????????? SMP ?? ?????????? ????.

1. ????????? **все** ???? ?????????? ?? ????????????? ??????? ? ???????? ?????????? ?????????? ? ?????????? ????????? ????? ????????? ??? ???????? KUMA.

- ???? ????? ???????? ????????? ??? ???????? KUMA ????????? ?? ?????!

2. ????????? ?? ???? ??????????????, ? ???????? ????? ??????????? ????????? SMP ? ?????????? ? ???????? KDT.

3. ????????? ???????:

```
./kdt invoke kuma --action addHosts --param host_inventory='<????_?_?????_?????????>'
```

4. ????????? ????????? ?????????, ????? ???? ?????????? ? ????????? ???????? ??? ????????? ????????.

Создание хранилища (Storage)

????????? ? **Мониторинг → Ресурсы и сервисы → Хранилища → Создать** ? ?????????? ????????? ?????? ?????????:

- ? ??????? **Основные параметры** ??????? ???????????? ??? ????????? ? ????????? ??????.
- ??????? **Варианты условий хранения** ? **Срок хранения событий аудита** (? ????).
- ? **Узлах кластера ClickHouse** ??????? FQDN ?????????, ? ????? ????????????? ?????, ??????? ? ??????.
- ? ????? ??????? **Создать**.

????????? ? **Мониторинг → Ресурсы и сервисы → Хранилища**, ??????? ??? ?? ?????? ??? ???????????? ????????? ? ???????? ????? **Копировать идентификатор** - ???? ???????? ?????????? ??? ????????? ???????.

????? ?????????? ?????? **Storage** ?? SSH-??????? ????????? ????????

```
/opt/kaspersky/kuma/kuma storage --core https://<kuma_core_FQDN>:7210 --id <service_id> --api.port 7230 --
install
```

????? `<kuma_core_FQDN>` - ???????? ??? ???? KUMA, ???????? ??? ????????? SMP. ??-????????? - kuma.<smp_domain>.

? `<service_id>` - ????????????? ???????, ????????????? ?????.

Создание точки назначения типа Хранилище

????? ????????? ?????????, ?????????? ??????? ????? ??????????, ??????? ????? ????????????? ?????????? ????????? ??? ???????? ??????? ? ?????????. ??? ???????? ????? ?????????? ????????? ?????????:

????????? ? **Мониторинг → Ресурсы и сервисы → Точки назначения → Создать.**

???????? **Тип** ????? ?????????? **storage.**

??????? ?? ???? **URL** - ? ?????????? ?????? ???????? ????????? ?????? ?????????, ???????? ????? ?????? ??? ?????????? ?????????.

Название ????? ?????????? ?????????? ?????????????.

Создание коррелятора (Correlator)

????????? ? **Мониторинг → Ресурсы и сервисы → Корреляторы → Создать** ? ?????????? ????????? ?????? ?????????:

- ? ??????? **Общие** ??????? ??????????? ??? ?????????? ? ????????? ??????.
- ? ??????? **Корреляция** ????????? ??? ?????????? ??????? ?????????.
- ? ??????? **Маршрутизация** ??????? **Добавить** ? ???????? ????? ????????? ????? ?????????? ?????????.
- ? ??????? **Проверка параметров** ???????? **Сохранить и создать сервис**.

? ?????????? KUMA ????????? ??????? ??? ????????? ?????????? ? ??. ?????????? ??, ??????? ?????? **Сохранить** ? ???????? ??????? ? SSH-???????.

Создание точки назначения типа Коррелятор

????? ????????? ??????????, ?????????? ??????? ????? ??????????, ??????? ????? ????????????? ??????????? ??? ???????? ??????? ? ????????? ??? ???????????? ? ????????? ?????????? ?? ?????? ? ??????????? ????????? ??????? ? ??????????. ??? ???????? ????? ?????????? ????????? ?????????:

????????? ? **Мониторинг → Ресурсы и сервисы → Точки назначения → Создать.**

???????? **Тип** ????? ?????????? **correlator.**

??????? ?? ???? **URL** - ? ?????????? ?????? ???????? ????????? ?????? ???????????, ???????? ????? ?????? ??? ?????????? ???????????.

Название ????? ?????????? ?????????? ?????????????.

Создание коллектора (Collector)

> ????? ????????? ?????????? ?? ???????? ?????????? ? ?????????? ????????? ?????????? ????? ????? ? ?????????????? **разделе**.

????????? ? **Мониторинг → Ресурсы и сервисы → Коллекторы → Создать** ? ??????????? ????????? ?????? ?????????:

- ? ??????? **Подключение источников** ??????? ???????????? **Имя** ?????????? ? ????????? **Тенант**.
- ? ??????? **Транспорт** ??????? **Тип** (????????) ? **URL** (:???? ??? FQDN:????), ?? ??????? ????????? ????? ????????? ?????? ?? ?????????.
- ? ??????? **Парсинг событий** ???????? ????? ????????????. ??????????, ????????? ? ?????????? ??????? - ?????????????? ?????????.
- ? ??????? ???????????? ???????? ????? ????????? ????? ?????????? ?????????? ? ?????????.
- ? ??????? **Проверка параметров** ???????? **Сохранить и создать сервис**.

? ?????????? KUMA ????????? ??????? ??? ????????? ?????????? ? ??. ?????????? ??, ??????? ?????? **Сохранить** ? ???????? ??????? ? SSH-???????.

Проверка поступления событий

????????? ? **Мониторинг → Ресурсы и сервисы → Активные сервисы** ? ???????? ????? ????????? ????????? ????????.

? ??????? ???? ???????? **Перейти к событиям**.

????????? ???????? ???? **Поиск угроз** ? ??????? ?????? **Выполнить запрос**

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

Дополнительные материалы

???????? ? ????????? ???????? KUMA (????????)

Revision #1
Created 2026-08-19 07:29:22 UTC by Koala
Updated 2026-08-19 08:28:04 UTC by Koala