????????? ????????????? XML-?????? 1C ? ??????? Linux-??????

> Зачастую создание файловых информационных ресурсов на хостах компании недопустимо с точки зрения действующих требований департамента информационной безопасности. В связи с этим использование стандартного коллектора 1c-xml с возможностью вычитки события через примонтированную к серверу коллектора шару реализовать невозможно.

1. ????????? ?????????? ? ?????? KUMA ??? ???????????? ????????????? XML-?????? 1C

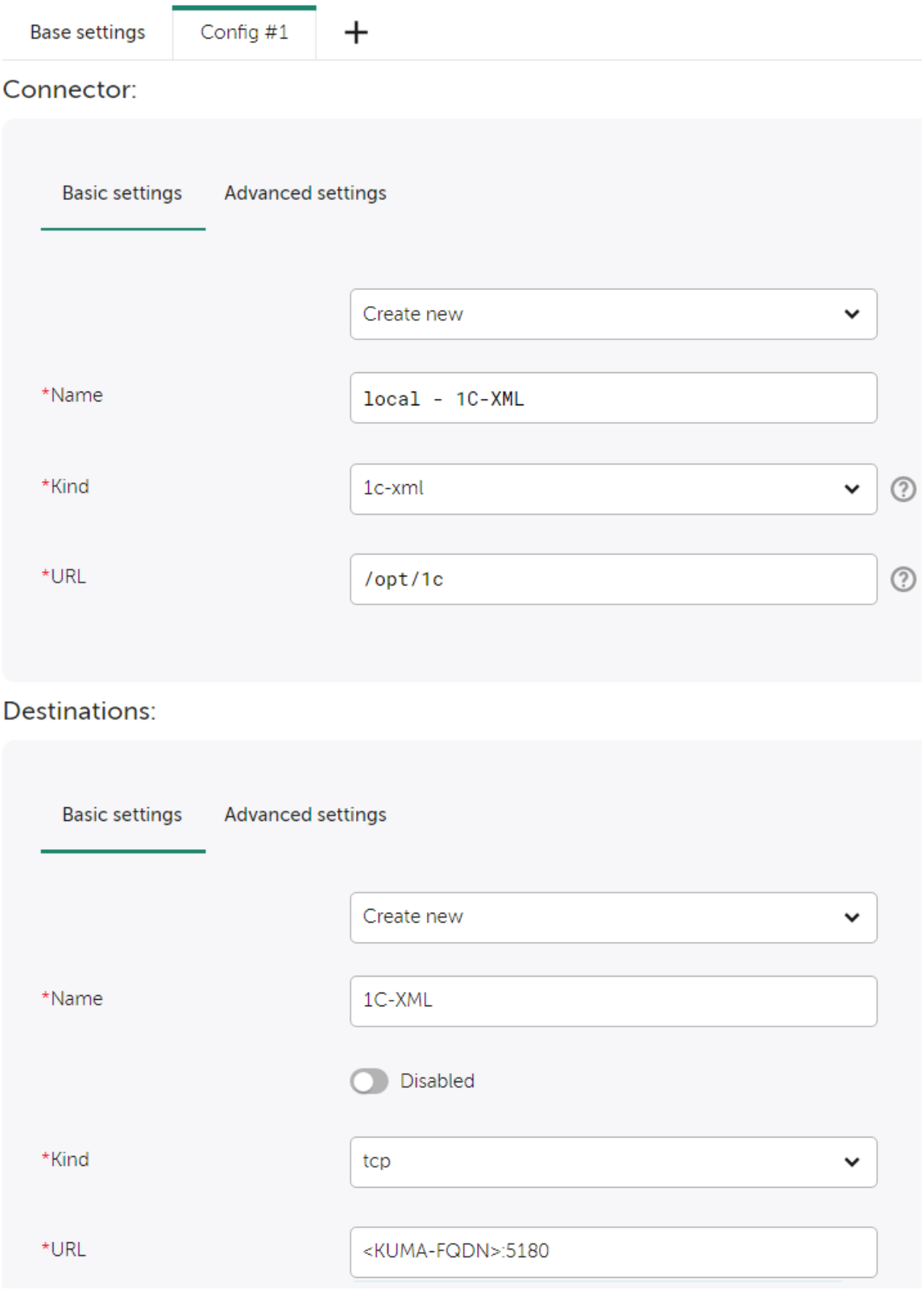
Конфигурация коллектора

Название поля	Значение поля	Описание
Collector name	[xml][1C] - Multiline	Название коллектора
Transport → Kind	tcp	Тип
Transport → URL	:5180	Локальный порт, который слушает коллектор
Event parsing → Name	[OOTB] 1C EventJournal Normalizer	Нормализатор для многострочных XML-файлов 1С

Конфигурация агента

Название поля	Значение поля	Описание
Agent name	[xml][1C] - Multiline	Название агента
Config → Connector → Name	local - 1C-XML	Название коннектора
Config → Connector → Kind	1c-xml	Тип
Config → Connector → URL	/opt/1c	Директория xml-файлов 1С
Config→ Destinations → Name	1C-XML	Название точки назначения
Config→ Destinations → Kind	tcp	Тип

Config→ Destinations → URL	<KUMA-FQDN>:5180	Сервер и порт коллектора для приема журналов 1C



2. ????????? Linux-?????? ?? ???? ??? ????? XML-???????? 1C

Для разового запуска Агента воспользуйтесь следующей командой:

```
sudo /opt/kaspersky/kuma/kuma agent --core https://<KUMA-FQDN>:7210 --id <ID> --wd
/opt/kaspersky/agent/<ID>
```

Для автоматизации процесса сбора событий установите агент в качестве службы.
Также можно воспользоваться утилитой **supervisor**. Для этого создайте конфигурационный файл (например, 1c.conf) в директории */etc/supervisor/conf.d/* со следующими настройками:

```
[program:agent_5f45aee7-655c-4014-aacd-07e4548de8ae]
command=sudo /opt/kaspersky/kuma/kuma agent --core https://<KUMA-FQDN>:7210 --id <ID> --wd
/opt/kaspersky/agent/<ID>
autostart=true
autorestart=true
```

Для применения конфигурации перезагрузите службу:

```
sudo systemctl restart supervisor
```

Для просмотра статуса и наличия ошибок воспользуйтесь следующей командой:

```
sudo supervisorctl status
```

3. ???????? ????????? ???????

В веб-интерфейсе KUMA выберите коллектор и перейдите к событиям (Resources → Collector → Go to events). На основном экране появятся нормализованные события 1С, полученные с Linux-агента.

```
SELECT * FROM `events` WHERE ServiceID = <ID> ORDER BY Timestamp DESC LIMIT 250
```

TenantID	Timestamp ↓	Name	DeviceProduct	DeviceVendor
Main	2023-08-23 19:23:11	Данные. Изменен...	Журнал событий	1С
Main	2023-08-23 19:23:11	Фоновое задание...	Журнал событий	1С
Main	2023-08-23 19:23:11	Сеанс. Начало	Журнал событий	1С
Main	2023-08-23 19:23:11	Фоновое задание...	Журнал событий	1С
Main	2023-08-23 19:23:11	Сеанс. Начало	Журнал событий	1С

Revision #23
Created 2023-08-23 16:01:22 UTC by Kirill German
Updated 2024-07-07 08:49:47 UTC by Koala