

????

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

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

Kaspersky Industrial CyberSecurity for Networks

В данном разделе собраны способы сбора диагностической информации по KICS for Networks

- [Работа с утилитой Health Check tool](#)

?????? ? ?????????? Health Check tool

Утилита Health Check tool предназначена для сбора диагностических данных и создания отчета о работоспособности узлов, где развернуты компоненты KICS for Networks, о нагрузке на сервер KICS for Networks, определяет статус служб (активны/неактивны). Если архитектура KICS for Networks распределенная (сервер и сенсор разделены), то данная утилита позволяет подключиться к сенсорам по SSH для сбора диагностической информации.

Утилита Health Check tool предоставляется по запросу. Утилита представляет собой архив, где расположен скрипт для диагностики узлов KICS for Networks. Скрипт поддерживает только CentOS 8 Stream и CentOS 9 Stream.

Подготовка к работе с утилитой Health Check tool

Перед запуском утилиты Health Check tool убедитесь, что:

- у вас есть доступ к узлам с KICS for Networks с правами root;
- установлены пакеты Python3;
- установлены библиотеки python3-pandas и python3-requests;
- для распределенной диагностики настроен SSH-доступ к сенсорам и вам известны root-пароли для аутентификации.

Запуск утилиты и генерация отчетов

1. Перейдите в директорию с утилитой и распакуйте архив.
2. В архиве содержится скрипт (утилита):

```
kics4net-health-check.sh
```

3. Необходимо присвоить права для запуска скрипта:

```
chmod +x kics4net-health-check.sh
```

4. Запускаем скрипт:
-

5. Затем выберите опцию в соответствии с описанием ниже:

Deployment report (опция 1):

Скрипт определяет параметры текущего развертывания KICS for Networks и выполняет сбор данных, связанных с настройками при установке, состояние узлов и состояние служб KICS for Networks. В случае когда сервер KICS for Networks и сенсоры установлены отдельно, скрипт будет пытаться подключиться к сенсорам по протоколу SSH для сбора данных. Будьте готовы предоставить пароль root для аутентификации. Выполнение скрипта можно в любой момент, используя сочетание клавиш CTRL+C.

Диагностический отчет сохраняется в директории скрипта, по одному файлу для каждого узла KICS for Networks.

Operational data report (опция 2):

Health Check tool, в случае выбора данной опции, пытается подключиться к серверу KICS for Networks с помощью API, для запроса и обработки операционные данные, собранных KICS for Networks.

Перед началом связи скрипт устанавливает необходимые пакеты Python, если они не были установлены ранее. Для подключения через API вам необходимо создать новый коннектор с веб-интерфейсе KICS for Networks:

- Откройте веб-интерфейс KICS for Networks и перейдите в раздел "Параметры" -> Коннекторы.
- Создайте новый коннектор типа "Generic", укажите IP-адрес в качестве адреса сервера и укажите тот же адрес для "Адреса узла подключения".
- Установите пароль доступа по сертификату, который будет использоваться для подключения к API KICS for Networks.
- Задайте произвольное имя коннектора, например, "healthcheck".
- Выберите тип "Generic".
- Нажмите "Сохранить", после чего будет загружен результирующий zip-файл.

Затем переместите полученный zip-файл в папку 'connector' на узле сервера KICS for Networks и запустите выполнение скрипта, выбрав опцию 2.

В случае если сервер занят обработкой большого объема данных, выполнение скрипта может занять достаточно большое количество времени. Вы можете прервать выполнение скрипта в любой момент, используя сочетание клавиш CTRL+C.

Результирующий файл журнала сохраняется в директории скрипта.