??????????? ?? ??? ?????????????? KICS for Networks

> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или ICS community и **НЕ** является официальной рекомендацией вендора

> Официальная документация по данному разделу приведена в Онлайн-справке на продукт: https://support.kaspersky.com/help/KICSforNetworks/4.3/ru-RU/83112.htm

> Актуальные пакеты для развёртывания запросите у сотрудников Лаборатории Касперского

????????? ??

????????? CentOS 9 Stream

KICS for Networks 4.2 работает под управлением CentOS Stream 9. Рекомендуется использовать образ ОС, расположенный по данной ссылке.

Скачанный образ необходимо записать на USB-носитель (например, Win32 Disk Imager или Rufus).

Для выполнения установки ОС CentOS Stream 9 выполнить следующие шаги.

Подключить загрузочный USB-носитель к серверу KICS for Networks и загрузиться с USB-носителя, затем выбрать “Install CentOS Stream 9”.

image.png

Подключить загрузочный USB-носитель к серверу KICS for Networks и загрузиться с USB-носителя, затем выбрать “Install CentOS Stream 9”.
image.png

Выбрать язык интерфейса установки ОС CentOS Stream 9, который вам удобен. Например, Russian (по умолчанию выбран English).

image.png

Нажать кнопку «Продолжить».

Для продолжения установки необходимо провести дополнительные настройки. Далее будут проведены поочередная настройка клавиатуры, часового пояса и раздела HDD, учетной записи для root и добавление нового пользователя (например, kics).

image.png

Выбрать основную раскладку клавиатуры (рекомендуется выбрать «English». С помощью клавиш управления перемещаем выбранный язык на верхнюю строку списка. Если ранее при выборе языка ОС был выбран «English», добавить «Russian» раскладку при необходимости с помощью «+». Выбирать удобные «горячие клавиши» для переключения раскладки с помощью кнопки «Параметры». Нажать кнопку «Готово».

image.png

Проверить и при необходимости скорректировать часовой пояс (рекомендуется выбирать пояс, соответствующий месту нахождения севера, на сенсорах должно быть идентичные временные настройки независимости от места их установки). Нажать кнопку «Готово».

image.png

Выбрать «Место установки», выбрать диск, выбрать параметр «По-своему». Нажать кнопку «Готово».

image.png

В окне «Разметка вручную» выбрать «Создать их автоматически», нажать кнопку «Готово».

image.png

При необходимости, допускается выделить необходимое место на диске под пользовательский каталог «/home». Оставшееся место выделить под корневой каталог «/» (вся информация хранится в корневом каталоге). Нажать кнопку «Готово».

image.png

Нажать кнопку «Принять изменения».

image.png

Важно!!! Если предполагается одновременное развертывание «Серверной» и «Сенсорной» части KICS for Networks с помощью «deploy script», то Логин/Пароль root пользователя на машинах, под которым запускает установка KICS for Networks, должны быть одинаковыми. Позже их можно будет изменить.

Задать пароль для пользователя «root». Отметить чекбокс «Разрешить вход пользователем root». Нажать «Готово».

image.png

Добавить нового пользователя (например: kics). Отметить чекбокс «Сделать этого пользователя администратором». Задать пароль для создаваемого пользователя. Нажать «Готово».

image.png

Остальные параметры можно оставить без изменений. Нажать «Начать установку».

image.png

Дождаться завершения установки. Нажать «Перезагрузить» для завершения установки.

image.png

Пройти авторизацию.

Нажать кнопку «Нет спасибо».

image.png

ОС CentOS Stream 9 готова к установке KICS for Networks 4.2.

????????? Astra Linux 1.8

Подключить загрузочный USB-носитель к серверу KICS for Networks и загрузиться с USB-носителя, затем выбрать “Установить Astra Linux"

image.png

Выбрать часовой пояс, если у сервера есть доступ к интернету, то можно выбрать NTP сервер.

image.png

Далее необходимо выбрать ручную разметку диска

image.png

в ручной разметке диска рекомендуется выполнять такое разбиение:

1. Раздел /home 10 ГБ.
2. Раздел /boot/efi 600 МБ.
3. раздел /boot 1024 МБ.
4. раздел / все остальное место на диске.

Далее необходимо выполнить шаги как на скринах ниже.

image.png

image.png

image.png

{1521B275-69D5-4E59-AADB-60B445A6623D}.png

image.png

image.png

image.png

image.png

image.png

image.png

Далее необходимо выбрать дополнительные пакеты, которые будут установлены. Рекомендуется добавить пакет SSH

image.png

Далее необходимо создать пользователя, который будет локальным администратором ОС.

image.png

На последнем шаге приводится сводка по установке ОС, можно поставить галку на чекбокс "Перезагрузить после завершения установки"

image.png

На этом процесс установки ОС будет завершен.

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

Настройка интерфейсов для Astra Linux отличается только интерфейсом ОС. Ниже приведен процесс настройки сетевых интерфейсов для ОС CentOS Stream 9.

Для работы KICS for Networks необходимо как минимум 2 сетевых интерфейса:

- MGMT – менеджмент интерфейс необходим для подключения к Web интерфейсу решения, поэтому IP-адрес выбирается исходя из карты IP-адресов конкретной площадки с учетом, чтобы все заинтересованные пользователи могли иметь к нему доступ. Данный порт так же может быть задействован для связи с сенсорами на удаленных площадках (для этого все сенсоры должны быть доступны для этой сети), но Вы так же можете выделить взаимодействие с сенсорами в отдельную подсеть;

- SPAN – интерфейс на который подается копия трафика с коммутаторов. Для каждой точки мониторинга на сервере и сенсоре должен быть сконфигурирован аналогичный сетевой интерфейс.

Для конфигурации сетевых интерфейсов перейти в сетевые настройки CentOS Stream 9.

image.png

Настроить сетевые интерфейсы для MGMT и SPAN (количество сетевых интерфейсов SPAN зависит от количества точек съема трафика).

image.png

????????? MGMT

Установить чек-бокс «Подключаться автоматически».

image.png

Настроить имя интерфейса (например, «MGMT»), выбрать MAC-адрес, соответствующий интерфейсу.

image.png

Выбрать метод IPv4 – «Вручную». Настроить IP-адрес для MGMT интерфейса.

image.png

Отключить IPv6. Нажать кнопку «Применить».

image.png

????????? SPAN

Установить чек-бокс «Подключаться автоматически».

image.png

Настроить имя интерфейса (например, «SPAN»), выбирать MAC, соответствующий интерфейсу.

image.png

Отключить IPv4.

image.png

Отключить IPv6. Нажать «Применить».

image.png

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

????????? ??????? ??? CentOS 9 Stream

Для начала необходимо воспользоваться подготовительным скриптом установки и сформировать zip архив с необходимыми пакетами. Для этого нужно воспользоваться опцией 4 подготовительного скрипта kics4net-preptool-2.3.sh.

> В случае если у вас нет доступа к интернету, то скачайте уже готовый zip архив с облака и перенесите его на сервер.

```
sudo sh ./kics4net-preptool-2.3.sh


1. Prepare host for deployment
2. Disable GUI (recommended for sensor nodes)
3. Enable GUI
4. Download/update required packages
```

После этого можно выполнять опцию 1 подготовительного скрипта для установки пакетов из архива.

>

> Подготовительный скрипт kics4net-preptool-2.3.sh должен лежать в той жедиректории что и zip архив.

> После выполнения опции 1 подготовительного скрипта все репозитории заблокируются!

```
sudo sh ./kics4net-preptool-2.3.sh


(+) 1. Prepare host for deployment
2. Disable GUI (recommended for sensor nodes)
3. Enable GUI
4. Download/update required packages
```

После выполнения скрипта будет предложено перезагрузить сервер. На этом подготовка сервера к установке KICS for Networks 4.2.x будет завершена.

????????? ??????? ??? Astra Linux 1.8

Необходимо выполнить следующие команды для скачивания требуемых пакетов:

```
sudo apt-cdrom add (если на сервере нет интернета, то вставьте диск, который вы хотите
использовать для подключения репозитория.)
sudo apt update

sudo apt install chrony -y
sudo systemctl enable chrony
sudo systemctl start chrony

sudo apt install rsync -y

sudo apt install libcap2-bin -y

sudo apt install python3-apt -y

sudo apt install ssh -y
sudo systemctl enable ssh
sudo systemctl start ssh

sudo apt install postgresql-15 -y
```

```
sudo systemctl enable postgresql-15
sudo systemctl start postgresql-15

sudo apt install python3-psycopg2 python3-cryptography python3-paramiko python3-requests -y

sudo apt install perl -y (версии 5.10 и выше, если устанавливается Агент администрирования Kaspersky Security Center).

sudo apt install exim4 -y
```

Необходимо включить локаль en_US.utf8 командой:

```
sudo localedef -i en_US -f UTF-8 en_US.utf8
```

Чтобы настроить почтовый сервер и включить автозапуск сервиса Exim перейдите в консоль операционной системы и выполните следующие шаги:

1. Откройте окно конфигурирования Exim. Для этого введите команду:

```
sudo dpkg-reconfigure exim4-config
```

2. В меню выбора типа почтовой конфигурации выберите пункт отправка почты через smarthost; прием по SMTP или через fetchmail.

3. На следующем шаге укажите имя отправителя писем в поле Почтовое имя системы (например, serverkics).

4. На следующем шаге не изменяйте значение по умолчанию 127.0.0.1 в поле IP-адреса, с которых следует ожидать входящие соединения SMTP.

5. На следующем шаге не изменяйте значение по умолчанию в поле Другие места назначения, для которых должна приниматься почта.

6. На следующем шаге оставьте незаполненным поле Машины, для которых доступна релейная передача почты.

7. На следующем шаге укажите IP-адрес или сетевое имя компьютера, который является SMTP-сервером в сети вашей организации (например, mail.example.com).

8. На следующем шаге при необходимости вы можете включить перезапись заголовков исходящей почты.

9. На следующем шаге в запросе Сокращать количество DNS-запросов до минимума (дозвон по требованию) выберите вариант Нет.

10. На следующем шаге в меню выбора метода доставки локальной почты выберите пункт mbox формат в /var/mail/.

11. На последнем шаге откажитесь от разделения конфигурации на отдельные файлы (размещение конфигурации должно быть в одном файле).

12. После закрытия окна конфигурирования откройте файл шаблона exim4.conf.template. Для этого введите команду:

```
sudo mcedit /etc/exim4/exim4.conf.template
```

13. Перейдите к концу раздела параметров remote_smtp или remote_smtp_smarthost и добавьте строку:

`message_linelength_limit = 10000000`

14. Сохраните и закройте файл шаблона.

15. Активируйте сервис Exim и включите его автозапуск. Для этого введите команды

```
sudo systemctl enable exim4.service
sudo systemctl start exim4.service
```

16. Предоставьте необходимые права доступа для директории /var/mail/. Для этого введите команду:

```
chmod 3775 /var/mail/
```

На этом подготовка сервера к установке KICS for Networks 4.3 будет завершена.

Revision #14
Created 24 July 2025 11:31:56
Updated 17 November 2025 09:11:31 by Sergey Malyugin