Подготовка инфраструктуры для развертывания KUMA

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

> Официальная документация по данному разделу приведена в онлайн-справке на продукт: https://support.kaspersky.ru/kuma/4.2/231034

Системные требования

Компоненты KUMA поддерживают развертывание как в виртуальной среде, так и на физическом оборудовании. За счет микросервисной архитектуры все компоненты системы могут сосуществовать на одном сервере или быть разнесены, в зависимости от инфраструктуры и планируемой нагрузки, на разных серверных мощностях. Более того, каждый компонент может быть развернут в виде множественных инсталляций для поддержки различных сценариев распределенной инфраструктуры, при этом, дублирование сервисов не требует наличия какой-либо дополнительной лицензии на продукт.

Доступны следующие варианты установки KUMA:

- **Установка на одном сервере (All-in-One).**
  Все компоненты KUMA разворачиваются на одном сервере.
- **Распределенная установка (Distributed).**
  Компоненты KUMA разворачиваются на разных серверах.
- **Распределенная установка в отказоустойчивой конфигурации.**
  Поддерживается 2 (два) варианта установки:
  - Ядро KUMA разворачивается в кластере Kubernetes для обеспечения отказоустойчивости.
  - Разворачивается несколько Ядер KUMA в кластере Raft (минимум 3 экземпляра, количество должно быть нечетным) для репликации данных и обеспечения отказоустойчивости.

>

> Вариант распределенной установки KUMA с несколькими сервисами Ядра KUMA в кластере Raft доступен, начиная с версии 4.0:
>
> https://support.kaspersky.ru/kuma/4.0/220925

> Статья онлайн-справки «Установка и удаление KUMA»:
>
> https://support.kaspersky.ru/kuma/4.0/217904

Требования к аппаратному обеспечению напрямую зависят от обрабатываемого количества событий в секунду (events per second), а также срока хранения событий. Для расчета аппаратных ресурсов требуется заполнить опросный лист и передать сотрудникам Лаборатории Касперского или представителям партнера Лаборатории Касперского.

> Статья онлайн-справки «Аппаратные и программные требования»:
>
> https://support.kaspersky.ru/kuma/4.0/217889

В рамках пилотного стенда – минимальные требования KUMA для варианта установки All-in-one:

- vCPU 16;
- RAM 32 GB;
- 500 GB в каталоге /opt.
- Частота процессора от 1.5 ГГц, CPU должен поддерживать набор инструкций SSE4.2 и AVX.
- Disk: SSD или HDD SAS 15k RAID10

Подготовительные действия

Перед установкой KUMA, убедитесь, что сервер, на котором будут установлены компоненты KUMA соответствует аппаратным и программным требованиям.

> Статья онлайн-справки «Аппаратные и программные требования»:
>
> https://support.kaspersky.ru/kuma/4.0/217889

Выполните обязательные шаги по подготовке ОС к установке KUMA:

Номер п/п	Наименование шага по подготовке ОС к установке KUMA	Статус выполнения

1	На этапе разбивки диска при установке ОС сделайте **/opt** отдельным разделом и выделите под него все дисковое пространство, за исключением 16 ГБ для операционной системы и 5 ГБ для журналов. Это необходимо в связи с тем, что KUMA размещает свои файлы в папке /opt. Итоговая рекомендуемая разбивка диска: • `/` и другие системные разделы - суммарно 16Гб • `/opt` - все остальное место • `/var/log` - 5Гб (не обязательно, но рекомендуется)	☐
2	В качестве файловой системы рекомендуется использовать ext4	☐
3	Убедитесь, что порты, которые KUMA займет при установке, доступны на сервере: https://support.kaspersky.ru/kuma/4.0/217770	☐

4	Настройте временную зону и синхронизацию системного времени с NTP-сервером
	
	Пример команды для настройки NTP
	
	Первый вариант (через chrony):
	
	`sudo apt install chrony`
	`sudo systemctl enable --now chronyd`
	`sudo timedatectl | grep 'System clock synchronized'`
	
	Если на сервере KUMA отсутствует доступ в Интернет, то после установки chrony отредактируйте файл **/etc/chrony.conf**, заменив в нем 2.pool.ntp.org на адрес NTP-сервера Вашей организации.
	
	Второй вариант (через systemd-timesyncd):
	
	`timedatectl set-timezone Europe/Moscow`
	`echo -e "[Time]\nServers=2.pool.ntp.org 1.pool.ntp.org" >> /etc/systemd/timesyncd.conf`
	`timedatectl set-ntp true`
	`timedatectl status`
		☐

5	Задайте имя сервера с помощью команды:
	
	`hostnamectl set-hostname kuma-1.mydomain.local`
	
	Обязательно используйте полное доменное имя (FQDN), например, kuma-1.mydomain.com.
	
	Проверьте, что возвращается правильное полное доменное имя сервера:
	
	`hostnamectl status`
	
	> Имя сервера должно ОБЯЗАТЕЛЬНО содержать минимум одну точку, например, kuma.local или kuma.demo.lab.
	
	> Имя сервера, на котором будет установлено Ядро KUMA, не должно начинаться с цифры.
	
	Компоненты KUMA взаимодействуют между собой, используя полное доменное имя (FQDN) сервера (например, kuma-1.mydomain.com).
	
	> Настоятельно не рекомендуется изменять FQDN серверов после установки KUMA, особенно на сервере с компонентом Core! Это приведет к невозможности проверки подлинности сертификатов и нарушит сетевое взаимодействие между компонентами KUMA. Для восстановления работоспособности потребуется перевыпуск сертификатов всех сервисов, а также изменение их конфигурации!
		☐

6	Задайте пароль пользователю root (можно сделать до установки ОС) > Не создавайте на сервере/серверах, где планируется установка компонентов KUMA, пользователя kuma. Данный пользователь создается автоматически при установке продукта и наличие в системе пользователя с таким же именем может сделать вход в систему невозможным (используйте другое имя).	☐
7	Укажите в файле **/etc/hosts** сервера KUMA его доменное имя и IP-адрес или создайте A-запись сервера KUMA на DNS-сервере организации (рекомендуется для продуктивной инсталляции).	☐

8	При использовании ОС Oracle или Ubuntu:
	Проверьте статус модуля SELinux с помощью команды:
	
	`sestatus`
	
	Если модуль SELinux включен, выключите модуль:
	• Выполните команду:
	
	`sudo setenforce 0`
	
	• Отредактируйте файл /etc/selinux/config, установив для параметра SELINUX= disabled
	• Сохраните внесенные изменения и перезагрузите сервер.
		☐

9	На серверах с компонентом Хранилище (Storage) включите использование ipv6. Если используется вариант установки All-in-one на сервере также требуется включить использование ipv6. > Для включения IPv6 можно воспользоваться статьей. > Либо используйте конфигурацию хранилища без использования IPv6. Для проверки, что ipv6 включен, используйте команду: `ip a | grep inet6`	☐
10	Установите необходимые пакеты в ОС: https://support.kaspersky.ru/kuma/4.0/231034 > Убедитесь, что в рамках одной инсталляции KUMA на разных хостах не используются одновременно Python версии 3.6 и Python версии 3.10 и выше. Данное ограничение также распространяется на контрольный хост. > Пример **НЕкорректной** конфигурации: > *Контрольный хост — Python 3.11.13* > *Целевые хосты — Python 3.6.8*	☐

11	**При использовании ОС Astra:** Проверьте наличие в ОС сервиса ufw (обычно устанавливается по умолчанию, но встречаются инсталляции, в которых сервис отсутствует): `systemctl status ufw` Если сервис отсутствует, выполните установку (рекомендуемый вариант). Нерекомендуемый вариант: в файле инвентаря измените значение параметра **no_firewall_actions** с **false** на **true** (см. Раздел **Установка KUMA**)	☐
12	При использовании ОС Astra: Присвойте необходимый уровень прав пользователю, под которым вы собираетесь устанавливать KUMA, с помощью команды: `sudo pdpl-user -i 63 <имя пользователя, под которым вы собираетесь устанавливать программу>`	☐

Доступ к внешним ресурсам

В процессе установки KUMA не подключается к внешним ресурсам, за исключением случая, когда для активации решения используется лицензионный код (см. Раздел Пошаговая установка KUMA). Для активации с помощью лицензионного кода серверу с установленным Ядром KUMA требуется доступ к следующему серверу ЛК: **https://activation-v2.kaspersky.com**

> В случае закрытой инфраструктуры вы можете указать прокси-сервер.

В процессе работы KUMA может подключаться к внешним ресурсам в следующих случаях:

- обновление контента (загрузка правил корреляции, нормализаторов и т.п.). Необходимо предоставить доступ к следующим серверам. В качестве альтернативы, можно использовать Kaspersky Update Utility (KUU).

- обращение к Kaspersky Security Network (KSN) при наличии интеграции с KIRA или правил обогащения для обнаружения DLL-Hijacking (требуется лицензия на модуль AI). Необходимо предоставить доступ к следующим серверам: **https://llm-gateway.ksn.kaspersky-labs.com** и **https://dc1-file.ksn.kaspersky-labs.com**. (см. Статью Настройка интеграции с KIRA и примеры использования и статью Настройка обнаружения DLL Hijacking).
- обращение к TIP (Threat Intelligence Portal) порталу для обогащения карточки события данными об индикаторах компрометации (требуется лицензия на TIP портал, отдельный продукт). Необходимо предоставить доступ к https://wlinfo.kaspersky.com (см. статью Интеграция с Kaspersky Threat Intelligence Portal)
- Также во всех перечисленных случаях необходим доступ до серверов инфраструктуры публичных ключей: **http://crl.kaspersky.com** и **http://ocsp.kaspersky.com.**

Revision #5
Created 2026-06-09 10:02:15 UTC by Dmitry Borisov
Updated 2026-08-18 15:05:44 UTC by Dmitry Borisov