

Подготовка ОС перед установкой и Требования

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.com/help/KUMA/3.4/ru-RU/231034.htm>

Актуальные для развёртывания системы пакеты KUMA запросите у сотрудника Лаборатории Касперского.

Наборы правил корреляции и их описание доступно по ссылке - https://support.kaspersky.com/help/KUMA/3.4/ru-RU/SOC_correlation_rules_description.zip

Порядок обновления с предыдущих версий KUMA - <https://support.kaspersky.com/help/KUMA/3.4/ru-RU/222156.htm>

Карта доступов для KUMA <https://support.kaspersky.com/help/KUMA/3.2/ru-RU/217770.htm>

Дополнение: Между шардами кластера хранилища необходимо также открывать порт **9000**, несмотря на то, что это не указано в таблице документации

Подготовка целевой машины

Дистрибутивы

Oracle Linux 9.4: https://yum.oracle.com/ISOS/OracleLinux/OL9/u4/x86_64/OracleLinux-R9-U4-x86_64-dvd.iso

Ubuntu LTS 22.04 (система работает наиболее производительно):

<https://releases.ubuntu.com/jammy/> (скачайте iso `...live-server-amd64.iso`)

Astra Linux SE 1.7.5: Приобретается отдельно. Сайт производителя: <https://astralinux.ru/>

Разбивка диска

- `/` и другие системные разделы - суммарно 16Гб
- `/opt` - все остальное место
- `/var/log` - 5Гб (не обязательно, но рекомендуется)

Общие требования

Процессор

Набор инструкций SSE4.2 (для работы ClickHouse)

Инструкция AVX (для KUMA 3.2 для MongoDB)

Имя хоста

В качестве имени хоста **ОБЯЗАТЕЛЬНО** использовать FQDN (полное доменное имя, в котором есть хотя бы 1 точка), например, `kuma-1.mydomain.local`.

```
hostnamectl set-hostname kuma-1.mydomain.local
```

При установке / обновлении на версию 3.2.x имя хоста НЕ должно начинаться с цифры

Имя хоста можно задать во время установки (зависит от инсталлятора ОС), либо после.

Настоятельно не рекомендуется изменять FQDN машин 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 потребуются перевыпуск сертификатов всех сервисов, а также изменение их конфигурации!

Зарегистрируйте целевые машины в DNS-зоне вашей организации. Для пилотных инсталляций, как альтернативу, можно использовать файл `hosts`. Для этого на каждой целевой машине укажите в файле `hosts` имена всех машин и их `ip`-адреса (включая адрес машины, на которой происходит настройка).

Синхронизация времени

Настройте временную зону и синхронизацию системного времени с NTP-сервером на всех серверах KUMA. Это можно сделать во время установки ОС.

Пример команды для настройки NTP

```
sudo apt install chrony
sudo systemctl enable --now chronyd
sudo timedatectl | grep 'System clock synchronized'
```

Если доступ в Интернет отсутствует, то после установки chrony отредактируйте файл `/etc/chrony.conf`, заменив в нем `2.pool.ntp.org` на адрес NTP сервера вашей организации.

Либо:

```
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
```

Прочее

Задайте пароль пользователю root. Это можно сделать во время установки ОС.

Не создавайте на целевых машинах пользователя **kuma**! Он создается автоматически при установке продукта и наличие в системе пользователя с таким же именем может сделать вход в систему невозможным (придумайте другое имя).

Отключите SELinux на тех ОС, для которых это применимо (Oracle, Ubuntu).

Отключение SELinux

1. Выполните команду:

```
sudo setenforce 0
```

2. Откройте на редактирование файл `/etc/selinux/config` и установите в нем параметру `SELINUX=` значение `disabled`

3. Сохраните внесенные изменения и перезагрузите машину

```
sudo reboot
```

На серверах хранилищ включите использование ipv6. Если установка All-in-one, на целевой машине также требуется включить использование ipv6. Для проверки, что ipv6 включен, можно использовать команду:

```
ping ::1
```

Для включения ipv6 воспользуйтесь инструкцией из [статьи](#).

Установка пакетов

Требования к установке на различных ОС приведены в официальной документации: <https://support.kaspersky.com/help/KUMA/3.2/ru-RU/231034.htm>

Oracle Linux

Основные пакеты:

- python3 (python 3.6 - 3.11)
- netaddr
- firewalld

```
sudo yum install -y python3.6 python3-netaddr
```

Только для Oracle 9.x:

- compat-openssl11

```
sudo yum install -y compat-openssl11
```

Только для сервера Ядра (как правило, не требуются, если сервер установлен с GUI):

- nss
- gtk2
- atk
- libnss3.so
- libatk-1.0.so.0
- libxkbcommon
- libdrm
- at-spi2-atk

- mesa-libgbm
- alsa-lib
- cups-libs
- libXcomposite
- libXdamage
- libXrandr

```
sudo yum install -y nss gtk2 atk libnss3.so libatk-1.0.so.0 libxkbcommon libdrm atspi2-atk mesa-libgbm alsa-lib cups-libs libXcomposite libXdamage libXrandr
```

Astra Linux

Основные пакеты:

- python3 (python 3.6 - 3.11)
- python3-apt
- curl
- libcurl4
- netaddr
- python3-cffi-backend

```
sudo apt install -y python3 python3-apt curl libcurl4 python3-netaddr python3-cffi-backend
```

Перед установкой KUMA рекомендуется проверить наличие в ОС сервиса ufw (обычно устанавливается по умолчанию, но встречаются инсталляции, в которых сервис отсутствует):

```
systemctl status ufw
```

Если сервис отсутствует, выполнить установку (рекомендуемый вариант).

Нерекомендуемый вариант: в файле инвентаря изменить значение параметра `no_firewall_actions` с **false** на **true**

Только для сервера Ядра (как правило, не требуются, если сервер установлен с GUI):

- libgtk2.0.0
- libnss3
- libatk-adaptor
- libatk1.0-0
- libdrm-common
- libgbm1
- libxkbcommon0
- libasound2

```
sudo apt install -y libgtk2.0.0 libnss3 libatk-adaptor libatk1.0-0 libdrm-common libgbm1 libxkbcommon0 libasound2
```

Дополнительно требуется присвоить пользователю, под которым вы собираетесь установить KUMA необходимый уровень прав с помощью команды ниже

```
sudo pdpl-user -i 63 <имя пользователя>
```

Ubuntu

Основные пакеты:

- python3 (python 3.6 - 3.11)
- python3-apt
- curl
- libcurl4
- openssl 1.1.1
- acl

```
sudo apt install python3-apt curl libcurl4 acl
```

Для установки openssl 1.1.1 необходимо скачать пакет [libssl1.1_1.1.1f-1ubuntu2_amd64.deb](#) и установить его:

```
sudo dpkg -i libssl1.1_1.1.1f-1ubuntu2_amd64.deb
```

Только для сервера Ядра (как правило, не требуются, если сервер установлен с GUI):

- libatk1.0-0
- libgtk2.0-0
- libatk-bridge2.0-0
- libcups2
- libxcomposite-dev
- libxdamage1
- libxrandr2
- libgbm-dev
- libxkbcommon-x11-0
- libpangocairo-1.0-0
- libasound2

```
sudo apt install libatk1.0-0 libgtk2.0-0 libatk-bridge2.0-0 libcups2 libxcomposite-dev libxdamage1 libxrandr2  
libgbm-dev libxkbcommon-x11-0 libpangocairo-1.0-0 libasound2
```

Требования для Хранилища и Keeper

Процессор

- с частотой от 2 ГГц;
- с архитектурой x86_64 и **поддержкой инструкций SSE 4.2**;
- Рекомендуется использовать технологии Turbo Boost и Hyper-Threading (при наличии);

ClickHouse работает более эффективно в конфигурациях с большим количеством ядер, но с более низкой тактовой частотой, чем в конфигурациях с меньшим количеством ядер и более высокой тактовой частотой. Например, 16 ядер с 2600 MHz предпочтительнее, чем 8 ядер с 3600 MHz.

ОЗУ

Необходимый объём RAM зависит от Сложности запросов и Объёма данных, обрабатываемых в запросах.

- Рекомендуемый объём оперативной памяти от 16 Гб (для объемов данных ~ 16 - 32 ТБ [горячее хранение]);
- Рекомендуемый объём оперативной памяти от 32 Гб (для объемов данных ~ 32 - 48 ТБ);
- Рекомендуемый объём оперативной памяти от 48 Гб (для объемов данных ~ 48 - 64 ТБ);
- Рекомендуемый объём оперативной памяти от 64 Гб (для объемов данных ~ 64 - 80 ТБ);
- Рекомендуемый объём оперативной памяти от 128 Гб (для объемов данных > 80 ТБ);

В идеальном случае: Количество Гб ОЗУ примерно равно количеству ТБ хранилища.

Диск

Отключайте файл подкачки (swap) в продуктовых средах.

Настоятельно рекомендуется использовать SSD (обычно ~ > 15k EPS) или HDD-рейд (SAS 10-15k RPM) в зависимости от нагрузки (до 15-25k EPS).

Пропускная способность диска является более важным фактором по сравнению с IOPS.

В случае использования хранилищ в виде виртуальных машин на гипервизоре то необходимо использовать отдельные дисковые массивы для каждого из хранилищ. Также не желательно нахождение вместе с хранилищем других высоконагруженных

сервисов на одном гипервизоре.

Файловая система **ext4** — самый надежный вариант. XFS тоже работает хорошо. Большинство других файловых систем также должны работать нормально. FAT-32 и exFAT не поддерживаются из-за отсутствия жестких ссылок. Работа на NFS, тоже не лучшая идея.

Размер блока 64 КБ достаточен для большинства конфигураций RAID. Средний размер записи на сервере Clickhouse составляет примерно 1 МБ (1024 КБ), поэтому рекомендуемый размер страйпа (stripe) также составляет 1 МБ.

При необходимости размер блока можно оптимизировать, установив его равным 1 МБ, разделенному на количество дисков без четности в RAID-массиве, так что каждая запись распараллеливается на всех доступных дисках без четности. Никогда не устанавливайте размер блока слишком маленьким или слишком большим.

Кеерер более критичен к диску и требует от 1000 IOPS, в зависимости от нагрузки, идеально использовать тип носителя NVMe

Сеть

- Кеерер нужен IPv6, включите его в ОС, если он отключен;
- По возможности, используйте сети 10G и более высокого класса, минимально подойдет 1G.
- Пропускная способность сети критически важна для обработки распределенных запросов с большим количеством промежуточных данных. Также, скорость сети влияет на задержки в процессах репликации.

Кеерер рекомендуется устанавливать на отдельные сервера, отдельно от ClickHouse (при возможности, обычно это $\sim > 50k$ EPS), т.к. Кеерер менее производителен при установке на одном узле с ClickHouse. Процессор и ОЗУ - по сайзингу.

Требования для Core / Collector / Correlator

Требования к процессору (для KUMA от версии 3.2 для работы MongoDB требуется **наличие инструкций процессора AVX**) и ОЗУ по сайзингу, диски можно использовать любые HDD от 7,5k RPM от 0,5 ТБ.

Любое новое обогащение или агрегация на коллекторе это ~+ 100-200 Мб к ОЗУ
(учитывайте это при расчете)

Объем диска на ядре зависит от количества создаваемых алертов, рекомендуется от 1 ТБ

Требования к отказоустойчивому ядру в кластере Kubernetes

Требования к процессору и ОЗУ по сайзингу.

Диск

Быстрые диски являются наиболее важным фактором производительности и стабильности развертывания.

По возможности используйте диски SSD, в крайнем случае подойдет HDD RAID 10 (SAS 10-15k RPM);

Сеть

- Обычно 1GbE достаточно для обычных развертываний. Но если есть возможность, то 10GbE более предпочтительно;
- Сетевые задержки не должны превышать 100 мс.

Revision #37

Created 10 August 2023 13:26:08 by Boris RZR

Updated 28 February 2025 07:10:52 by Boris RZR