Развертывание XDR на двух узлах (Ubuntu)

Развертывание Kaspersky XDR на двух узлах (Ubuntu Server 26.04 LTS): OSMP и сервисы KUMA

Раздел описывает развертывание экземпляра Kaspersky XDR Expert на двух машинах Ubuntu Server 26.04 LTS: узле OSMP и отдельном узле для сервисов KUMA. Установка выполняется с узла OSMP и разворачивает компоненты на оба узла.

Топология и легенда

Развертывание состоит из двух узлов:

- **Узел OSMP** — основной узел. На нём выполняется развертывание (утилитой KDT) и устанавливается PostgreSQL. IP-адрес: 10.0.0.100 (`<host_ip>`).
- **Узел сервисов KUMA** — отдельный сервер для компонентов KUMA (хранилище, коррелятор, коллектор). FQDN: `kuma-services.<домен>`, IP-адрес: 10.0.0.101 (`<kuma_ip>`).

В инструкции используются следующие обозначения:

- `10.0.0.100` — IP-адрес узла OSMP (`<host_ip>`);
- `10.0.0.101` — IP-адрес узла сервисов KUMA (`<kuma_ip>`);
- `10.0.0.200` — IP-адрес для записи A с подстановкой на этапе настройки DNS (`<ingress_ip>`);
- `kuma-services.<домен>` — FQDN узла сервисов KUMA;
- `user` — учетная запись пользователя для развертывания (`<user_name>`);
- `/home/user/.ssh/id_rsa` — путь к закрытой части SSH-ключа (`<ssh_key_path>`);
- `mydomain.local` — домен для входящего трафика (`<ingress_domain>`).

> **Порядок важен.** Установка (`kdt apply`) запускается с узла OSMP и разворачивает компоненты, в том числе на узел сервисов KUMA. Узел сервисов KUMA должен быть

полностью подготовлен (пакеты, отключение SELinux и swap, заданный FQDN, доступ по SSH-ключу с узла OSMP), а необходимые записи DNS — созданы, **до** запуска установки.

Узел OSMP — все команды этой части выполняются на узле OSMP

Аппаратные требования

- 16 vCPU;
- 32 ГБ оперативной памяти;
- 1 ТБ SSD или другое устройство с производительностью 8000 IOPS при произвольном доступе.

Итоговые требования к оборудованию рассчитайте в соответствии с руководством по масштабированию.

Проверка свободного места в каталогах /var, /opt и /tmp

Проверьте свободное место следующими командами:

- `df -h /var` — не менее 200 ГБ;
- `df -h /opt` — не менее 500 ГБ;
- `df -h /tmp` — не менее 50 ГБ.

Отключение SELinux и swap

Отключите swap (обязательное требование для узлов кластера Kubernetes):

```
sudo swapoff -a
```

Чтобы swap оставался отключённым после перезагрузки, закомментируйте строки со swap в файле `/etc/fstab`.

Проверьте статус SELinux:

```
sudo sestatus
```

Если SELinux включён, отключите его: задайте в файле `/etc/selinux/config` значение `SELINUX=disabled` и перезагрузите систему.

```
sudo sed -i 's/^SELINUX=.*/SELINUX=disabled/' /etc/selinux/config
```

Настройка учетной записи пользователя для развертывания

1. Откройте файл `/etc/sudoers`:

```
sudo visudo
```

2. Добавьте в конец файла строку (где `{user}` — учетная запись, используемая для развертывания):

```
{user} ALL=(ALL) NOPASSWD: ALL
```

> Если появляется ошибка `user is not in sudoers file`, переключитесь на пользователя с правами root и выполните команду:

```
echo "$USER ALL=(ALL) NOPASSWD: ALL" | sudo tee /etc/sudoers.d/$USER
```

3. Сохраните и закройте файл:

```
:wq
```

4. Создайте SSH-ключ:

```
ssh-keygen -t rsa -b 4096 -N ""
```

5. Скопируйте открытый ключ на целевой хост (для узла OSMP это тот же хост, с которого выполняется команда):

```
ssh-copy-id <host_ip>
```

Установка и настройка Docker

Установка Docker

Поддерживаются версии Docker 25 и выше. Используйте один из вариантов.

Вариант 1 — из репозитория Ubuntu:

```
sudo apt update && sudo apt install docker.io
```

Вариант 2 — из официального репозитория Docker. Установите необходимые пакеты:

```
sudo apt update && sudo apt install ca-certificates curl
```

Загрузите keyring Docker:

```
sudo curl -fsSL https://download.docker.com/linux/ubuntu/gpg -o /etc/apt/keyrings/docker.asc
&& sudo chmod 0755 /etc/apt/keyrings/docker.asc
```

Добавьте apt-репозиторий Docker:

```
sudo tee /etc/apt/sources.list.d/docker.sources <<EOF
Types: deb
URIs: https://download.docker.com/linux/ubuntu
Suites: $(. /etc/os-release && echo "${UBUNTU_CODENAME:-$VERSION_CODENAME}")
Components: stable
Architectures: $(dpkg --print-architecture)
Signed-By: /etc/apt/keyrings/docker.asc
EOF
```

Обновите кеш репозитория и установите пакеты Docker:

```
sudo apt update && sudo apt install docker-ce docker-ce-cli containerd.io docker-buildx-plugin
docker-compose-plugin
```

Настройка Docker

1. Добавьте текущего пользователя в группу `docker`:

```
sudo usermod -aG docker $USER
```

2. Примените членство в группе `docker` в текущей сессии:

```
newgrp docker
```

Установка и настройка PostgreSQL

Поддерживается PostgreSQL 18.4.

1. Установите PostgreSQL:

```
sudo apt install -y postgresql-18
```

> Если PostgreSQL 18 отсутствует в подключённом репозитории, добавьте репозиторий PostgreSQL (PGDG). Инструкции см. на сайте PostgreSQL.

2. Создайте отдельного суперпользователя PostgreSQL:

```
sudo -u postgres createuser --superuser xdr
```

3. Задайте пароль пользователя:

```
sudo -u postgres psql -c "ALTER USER xdr WITH PASSWORD 'ваш пароль';"
```

4. Создайте базу данных с тем же именем:

```
sudo -u postgres psql -c "CREATE DATABASE xdr OWNER xdr;"
```

5. Разрешите доступ к PostgreSQL с любого IP-адреса:

```
echo "host all all 0.0.0.0/0 scram-sha-256" | sudo tee -a /etc/postgresql/18/main/pg_hba.conf
```

6. Задайте параметры в конфигурационном файле `/etc/postgresql/18/main/postgresql.conf`. Закомментированные (#) строки раскомментируйте:

```
listen_addresses = '*'
shared_buffers = 8192MB
max_stack_depth = 7MB
temp_buffers = 24MB
work_mem = 16MB
max_connections = 512
max_parallel_workers_per_gather = 0
maintenance_work_mem = 128MB
standard_conforming_strings = on
```

7. Перезапустите PostgreSQL:

```
sudo systemctl restart postgresql
```

Распаковка утилиты KDT

Создайте директорию и распакуйте в неё утилиту KDT:

```
mkdir ./kdt && tar -xvf bin.tar.gz -C ./kdt
```

Синхронизация системного времени (NTP)

Настройте синхронизацию времени с NTP-сервером:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

В выводе должна присутствовать строка `System clock synchronized: yes`. Текущие дату и время можно проверить командой `date`.

> **Узел сервисов KUMA — все команды этой части выполняются на узле сервисов KUMA**

Аппаратные требования

Аппаратные требования к узлу сервисов KUMA совпадают с требованиями к узлу OSMP:

- 16 vCPU;
- 32 ГБ оперативной памяти;
- 1 ТБ SSD или другое устройство с производительностью 8000 IOPS при произвольном доступе.

Разметка диска

Основной объём диска выделите под каталог `/opt` — в него устанавливаются компоненты KUMA. Под системный раздел оставьте не менее 16 ГБ. Если установщик Ubuntu рекомендует для системных разделов больший размер, используйте рекомендованное значение.

Установка пакетов

Установите необходимые пакеты:

```
apt install python3-apt curl libcurl4 acl
apt install python3-netaddr python3-cffi-backend
```

Отключение SELinux и swap

Отключите swap (обязательное требование для узлов кластера Kubernetes):

```
sudo swapoff -a
```

Чтобы swap оставался отключённым после перезагрузки, закомментируйте строки со swap в файле `/etc/fstab`.

Проверьте статус SELinux:

```
sudo sestatus
```

Если SELinux включён, отключите его: задайте в файле `/etc/selinux/config` значение `SELINUX=disabled` и перезагрузите систему.

```
sudo sed -i 's/^SELINUX=.*/SELINUX=disabled/' /etc/selinux/config
```

Доменное имя (FQDN)

Задайте узлу сервисов KUMA полное доменное имя (FQDN) — обязательно с точкой, например `kuma-services.<домен>`. FQDN должен быть установлен как имя хоста системы.

> Не используйте для этого узла имя `kuma` — оно занято служебными адресами OSMP. Используйте отдельное имя, например `kuma-services`.

Запись A для этого имени создаётся на DNS-сервере — см. раздел «Настройка DNS».

Синхронизация системного времени (NTP)

Настройте синхронизацию времени с NTP-сервером:

```
sudo apt update
sudo apt install -y systemd-timesyncd
sudo timedatectl set-ntp true
sudo timedatectl set-timezone Europe/Moscow
sudo timedatectl set-local-rtc 0
timedatectl status
```

Доступ по SSH с узла OSMP

Установка подключается к узлу сервисов KUMA по SSH с узла OSMP. Скопируйте открытый SSH-ключ с узла OSMP на узел сервисов KUMA — команда выполняется **на узле OSMP**:

```
ssh-copy-id <kuma_ip>
```

Настройка DNS

> **Настройка DNS выполняется на DNS-сервере (общем для обоих узлов)**

Зарегистрируйте на DNS-сервере доменные имена служб OSMP и узла сервисов KUMA. DNS-сервер общий для обоих узлов, поэтому все записи задаются в одном месте.

Для служб OSMP добавьте запись A с подстановкой (wildcard), указывающую на свободный IP-адрес (`<ingress_ip>`) в той же подсети, что и кластер. Шлюз кластера Kubernetes прослушивает этот адрес и направляет трафик к соответствующим службам. По умолчанию службы OSMP доступны по следующим адресам:

```
<ingress_ip> - admsrv.<ingress_domain>
<ingress_ip> - api.<ingress_domain>
<ingress_ip> - console.<ingress_domain>
<ingress_ip> - kuma.<ingress_domain>
<ingress_ip> - *.kuma.<ingress_domain>
<ingress_ip> - monitoring.<ingress_domain>
<ingress_ip> - agentserver.<ingress_domain>
<ingress_ip> - updater.<ingress_domain>
```

Для узла сервисов KUMA добавьте отдельную запись A:

```
<kuma_ip> - kuma-services.<домен>
```

> Если DNS-сервер отсутствует или его нельзя использовать, разверните собственный DNS-сервер на BIND — см. статью Создание собственного DNS-сервера на BIND.

> **Далее все команды выполняются на узле OSMP**

Создание конфигурации для запуска установки

> Обратите внимание, что узлы, указанные в файле инвентаря будут подготовлены для установки сервисов KUMA. Однако, сами сервисы KUMA (коллектор, коррелятор, хранилище) на узле установлены не будут. Для развертывания непосредственно сервисов KUMA воспользуйтесь инструкцией в конце данной статьи.

Файл инвентаря KUMA

Создайте на узле OSMP файл инвентаря KUMA (например, `kuma-inventory.yml`, шаблон файла инвентаря находится в директории с распакованной утилитой kdt с названием `single.inventory.yml.template`) и разместите его рядом с остальными файлами установки. Во всех блоках `hosts` укажите FQDN и IP-адрес узла сервисов KUMA. Путь к этому файлу задаётся в параметре установки `inventory`.

```
all:
  vars:
    deploy_example_services: false
    ansible_connection: local # не изменять
    ansible_user: nonroot # не изменять
kuma:
  vars:
    ansible_connection: ssh
    ansible_user: root # укажите имя пользователя, от имени которого будет производиться
установка
# Если пользователь не root, раскомментируйте строки ниже
#    ansible_become: true
#    ansible_become_method: sudo
  children:
    kuma_utils:
      hosts:
        kuma-services.example.com: # FQDN узла сервисов KUMA
          ansible_host: 10.0.0.101 # IP-адрес узла сервисов KUMA
    kuma_collector:
      hosts:
        kuma-services.example.com: # FQDN узла сервисов KUMA
          ansible_host: 10.0.0.101 # IP-адрес узла сервисов KUMA
    kuma_correlator:
      hosts:
        kuma-services.example.com: # FQDN узла сервисов KUMA
          ansible_host: 10.0.0.101 # IP-адрес узла сервисов KUMA
    kuma_storage:
      hosts:
        kuma-services.example.com: # FQDN узла сервисов KUMA
          ansible_host: 10.0.0.101 # IP-адрес узла сервисов KUMA
          shard: 1
          replica: 1
          keeper: 1
```

> Ниже представлены инструкции по заполнению файла с параметрами установки.Файл с параметрами установки можно заполнить либо с помощью мастера, либо вручную.

> **Обратите внимание!** В инструкции далее для параметра `license` необходимо указать путь к файлу лицензии KUMA `license.key` (это лицензия KUMA, а не лицензия OSMP/XDR). Разместите `license.key` рядом с остальными файлами, необходимыми для установки.

Вариант 1 - Указание параметров установки с помощью мастера настройки

1. Запустите мастер настройки:

```
./bin/kdt wizard -k xdr-<версия_приложения>.tar -o params.yaml
```

Ответьте на вопросы мастера:

1. Введите количество primary_nodes (не менее 1): `1`
2. Введите IPv4-адрес первого управляющего узла: `10.0.0.100`
3. Введите имя пользователя для подключения к первому управляющему узлу: `user`
4. Введите путь к SSH-ключу для подключения к первому управляющему узлу: `/home/user/.ssh/id_rsa`
5. Введите количество worker_nodes (0 — развертывание OSMP на одном узле): `0`
6. Введите `1`, если требуется балансировщик нагрузки; иначе нажмите Enter: `Enter`
7. Введите строку подключения к СУБД (postgres://<dbms_username>:<password>@<fqdn>:<port>): `postgres://xdr:<your_password>@10.0.0.100:5432`

   > **Обратите внимание!** Если пароль для подключения к PostgreSQL содержит специальные символы, необходимо закодировать такие символы в URL.
   >
   > Например, тут: https://www.urlencoder.org/
8. Введите IP-адрес шлюза кластера Kubernetes. Шлюз обеспечивает подключение компонентов Kaspersky XDR Expert внутри кластера: `10.0.0.200`
9. Введите пароль учетной записи пользователя Kaspersky XDR Expert (8–256 символов; прописные и строчные буквы, цифры и специальные символы): `ваш_пароль`
10. Введите путь к файлу инвентаря KUMA: `./kuma-inventory.yaml`
11. Введите путь к SSH-ключу для подключения к узлам со службами KUMA: `/home/user/.ssh/id_rsa`
12. Введите путь к файлу лицензионного ключа KUMA (это лицензия именно KUMA): `./license.key`
13. Введите доменное имя для публичных служб Kaspersky XDR Expert (например, console.<domain name>): `mydomain.local`
14. Введите путь к файлу пользовательского сертификата и закрытому ключу для публичных сервисов (для самоподписанного сертификата нажмите Enter): `Enter`

15. Введите «Y», если в вашем регионе требуется расширенный жизненный цикл инцидентов: `N`
16. Введите имя учетной записи для просмотра метрик OSMP в Grafana (1–30 символов; начинается с буквы; строчные буквы a–z, цифры 0–9, символы _ -.): `xdr`
17. Введите пароль учетной записи для просмотра метрик OSMP в Grafana (8–256 символов; прописные и строчные буквы, цифры и специальные символы): `ваш_пароль`

Вариант 2 - Указание параметров установки с помощью конфигурационного файла

Шаблон конфигурационного файла (`singlenode.smp_param.yaml.template`) находится в дистрибутиве в архиве с утилитой KDT. Обратите внимание на параметры `inventory` (путь к файлу инвентаря KUMA) и `license` (путь к файлу лицензии KUMA `license.key`).

> **Обратите внимание!** Если пароль для подключения к PostgreSQL (`<ваш_пароль>` в параметре `psql_dsn`) содержит специальные символы, необходимо закодировать такие символы в URL. Например, тут: https://www.urlencoder.org/

```
schemaType: ParameterSet
schemaVersion: 1.0.1
namespace: ""
name: bootstrap
project: xdr
nodes:
  - desc: cdt-primary0
    type: primary-worker
    host: <host_ip> # адрес хоста для установки OSMP
    access:
      ssh:
        user: <user_name> # имя пользователя, под которым выполняется установка
        key: <ssh_key_path> # путь к файлу ключа пользователя
parameters:
  - name: psql_dsn
    source:
      value: postgres://xdr:<ваш_пароль>@<host_ip>:5432 # строка подключения к PostgreSQL
  - name: ingress_ip
    source:
      value: <ingress_ip> # адрес шлюза k8s
  - name: ssh_pk
    source:
      path: <ssh_key_path> # путь к файлу ключа пользователя
```

```
  - name: admin_password
    source:
      value: "ваш_пароль" # пароль для доступа к консоли, 8-256 символов, должен содержать буквы в обоих регистрах, цифры и спец. символы
  - name: low_resources
    source:
      value: "true"
  - name: openbao_ha_mode
    source:
      value: "false"
  - name: default_class_replica_count
    source:
      value: "1"
  - name: inventory
    source:
      value: ./kuma-inventory.yml # путь к файлу инвентаря KUMA
  - name: license
    source:
      value: ./license.key # путь к файлу лицензии KUMA
  - name: домен_smp
    source:
      value: "<ingress_domain>" # домен для OSMP
  - name: pki_host_list
    source:
      value: "admsrv api console kuma monitoring updater"
  - name: grafana_admin_user
    source:
      value: xdr # имя пользователя для доступа к разделу метрик
  - name: grafana_admin_password
    source:
      value: "ваш_пароль" # пароль для доступа к разделу метрик
```

> Если установка сервисов KUMA в кластере не требуется, добавьте строки ниже в конец файла конфигурации. В таком случае в кластере будут развернуты только сервисы Ядра и Метрик.

```
  - name: autodeploy_plan
    source:
      value: "none"
```

Установка Kaspersky XDR

Запустите установку:

```
./bin/kdt apply --accept-eula -k xdr-<версия_приложения>.tar -i params.yaml
```

При успешной установке в терминале отображается информация следующего вида:

```
INFO[0038] apply inventory ./conf.yaml
INFO[0039] preparing bootstrap_<версия>.tgz
INFO[0092] installing: bootstrap
INFO[0404] time: prepare 53.113895029s install 5m12.442326155s
INFO[0404] current installation is valid
INFO[0404] bundles will be published: 40
INFO[0536] bundles published 40
INFO[0536] bundles will be applied: 39
INFO[2450] apply done: 31m53.851140069s
INFO[2450] apply command completed successfully
INFO[2450] time: publish 2m11.679771805s install 31m53.930470045s
```

Чтобы проверить установку, откройте страницу авторизации в браузере:

```
https://console.<ingress_domain>
```

где `<ingress_domain>` — доменное имя для публичных служб, заданное в мастере настройки или файле конфигурации.

Включение отчетности KUMA (cnab)

После завершения установки включите отчетность KUMA (возможность сохранения отчетов в форматах PDF, HTML и др.). Архив `chrome_full.tar.gz` входит в поставку. Разместите его рядом с утилитой KDT и выполните команду:

```
./kdt invoke kuma --action=enableReporting --if reporting_archive=chrome_full.tar.gz
```

Действия после установки

Для базовой настройки системы после установки воспользуйтесь соответствующими инструкциями

1. Установка плагинов

2. Первый вход и 2FA

3. Добавление лицензии на функционал XDR

4. Установка сервисов KUMA

5. Настройка интеграций

6. Установка кастомного сертификата для доступа к веб-консоли

Revision #8
Created 2026-08-17 10:29:40 UTC by Koala
Updated 2026-08-18 12:55:57 UTC by Koala