

Установка KOMRAD ENTERPRISE SIEM

Предварительные условия

Проверить запущен ли Apache сервер:

```
systemctl status httpd2.service
```

Если запущен - то остановить, так как для работы необходим 443 порт.

```
systemctl stop httpd2.service
```

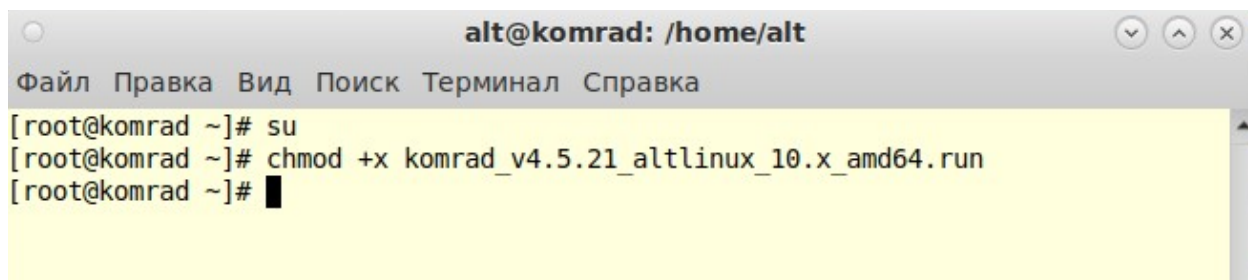
```
systemctl disable httpd2.service
```

Установка выполняется только под учетной записью супер-пользователя:

```
su
```

```
chmod +x komrad_v4.5.x_altlinux_10.x_amd64.run
```

где x – минорная версия программного обеспечения



The screenshot shows a terminal window titled 'alt@komrad: /home/alt'. The menu bar includes 'Файл', 'Правка', 'Вид', 'Поиск', 'Терминал', and 'Справка'. The terminal output shows the user switching to root with 'su' and then running 'chmod +x komrad_v4.5.21_altlinux_10.x_amd64.run'.

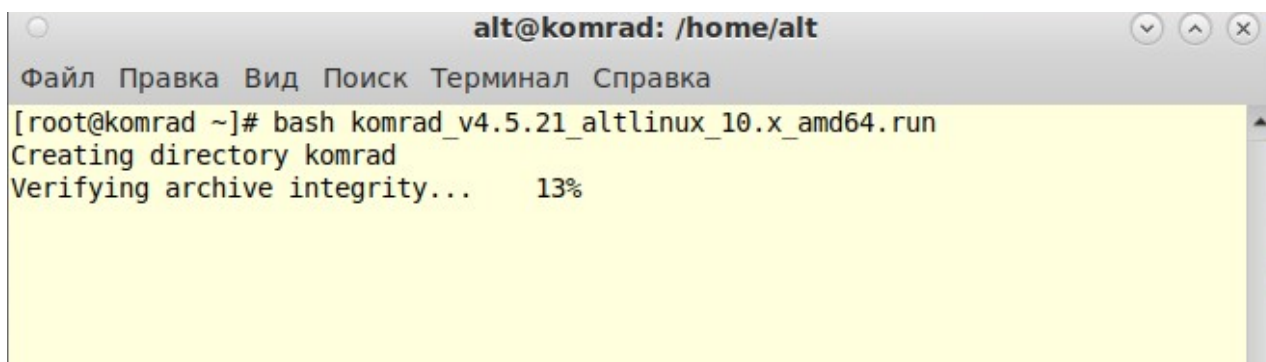
```
alt@komrad: /home/alt
[root@komrad ~]# su
[root@komrad ~]# chmod +x komrad_v4.5.21_altlinux_10.x_amd64.run
[root@komrad ~]#
```

Установка KOMRAD ENTERPRISE SIEM

Установка с помощью инсталлятора в автоматическом режиме.

(дополнительно: [Документация KOMRAD](#))

```
bash komrad_v4.5.x_altlinux_10.x_amd64.run
```



The screenshot shows a terminal window titled 'alt@komrad: /home/alt'. The menu bar is the same as in the previous screenshot. The terminal output shows the execution of 'bash komrad_v4.5.21_altlinux_10.x_amd64.run', which results in 'Creating directory komrad' and 'Verifying archive integrity... 13%'.

```
alt@komrad: /home/alt
[root@komrad ~]# bash komrad_v4.5.21_altlinux_10.x_amd64.run
Creating directory komrad
Verifying archive integrity... 13%
```

Процесс распаковки дистрибутива KOMRAD и запуск установщика.

Начало установки

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка
Uncompressing komrad SIEM v4.5.21 Installer 100%
+ rpm -i komrad-cli v4.5.21_altlinux_10.x_amd64.rpm
+ komrad-cli install singlenode
=== Установка KOMRAD SIEM ===

  KOMRAD - CLI
komrad-cli

GitVersion:      v4.5.21
GitCommit:       7a4dfab3d08c361b76aef97d7077ecd985185d40
GitTreeState:    clean
BuildDate:       2024-12-20T13:20:47
GoVersion:       go1.23.4
CGO:             false
Compiler:        gc
Platform:        linux/amd64

Определена ОС: altlinux 10.0

=====
      Установить Komrad SIEM с настройками по умолчанию?
=====

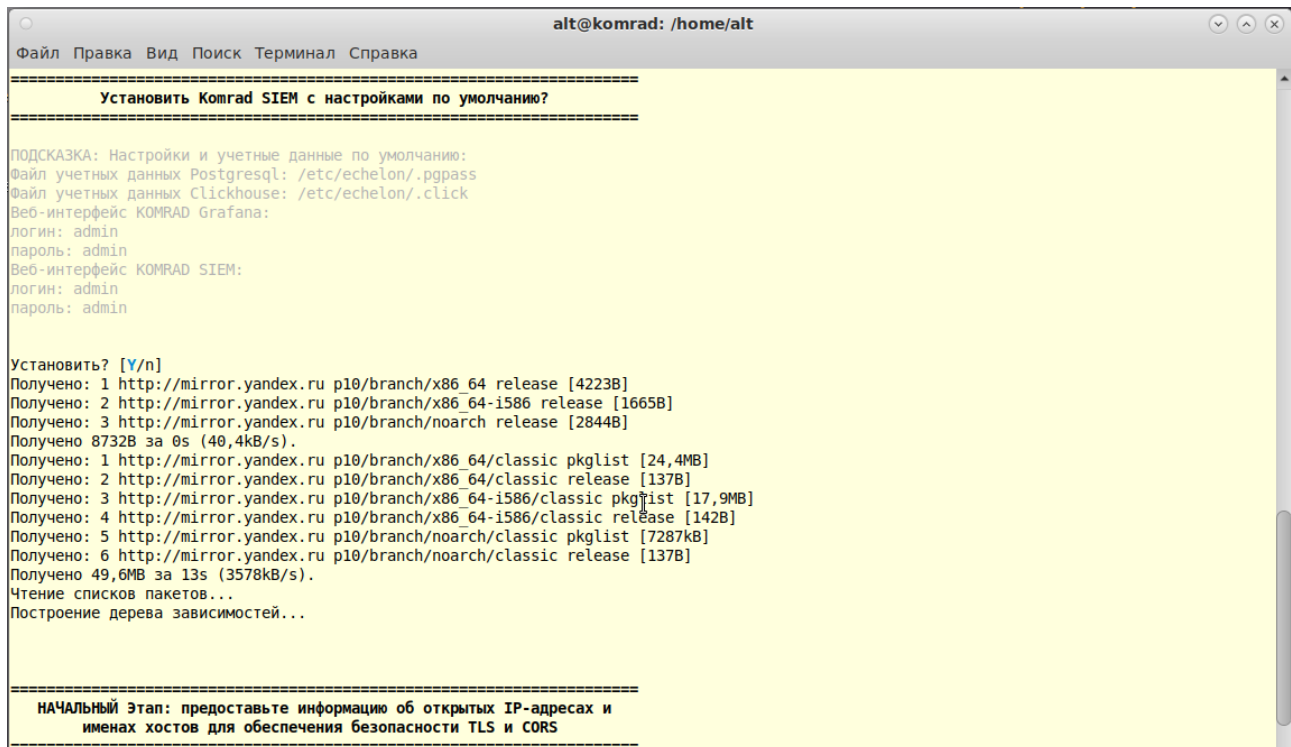
ПОДСКАЗКА: Настройки и учетные данные по умолчанию:
Файл учетных данных Postgresql: /etc/echelon/.pgpass
Файл учетных данных Clickhouse: /etc/echelon/.click
Веб-интерфейс KOMRAD Grafana:
логин: admin
пароль: admin
Веб-интерфейс KOMRAD SIEM:
логин: admin
пароль: admin

Установить? [Y/n]
```

Диалоговое окно выбора установки KOMRAD с настройками по умолчанию.

Нажмите Enter (или Y), чтобы произвести полную установку KOMRAD со всеми пакетами. Файлы подключений и данные для входа в административную панель отображаются на экране.

Обновление системы



```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
Установить Komrad SIEM с настройками по умолчанию?
=====

ПОДСКАЗКА: Настройки и учетные данные по умолчанию:
Файл учетных данных PostgreSQL: /etc/echelon/.pgpass
Файл учетных данных Clickhouse: /etc/echelon/.click
Веб-интерфейс KOMRAD Grafana:
логин: admin
пароль: admin
Веб-интерфейс KOMRAD SIEM:
логин: admin
пароль: admin

Установить? [Y/n]
Получено: 1 http://mirror.yandex.ru p10/branch/x86_64 release [4223B]
Получено: 2 http://mirror.yandex.ru p10/branch/x86_64-i586 release [1665B]
Получено: 3 http://mirror.yandex.ru p10/branch/noarch release [2844B]
Получено 8732B за 0s (40,4kB/s).
Получено: 1 http://mirror.yandex.ru p10/branch/x86_64/classic pkglist [24,4MB]
Получено: 2 http://mirror.yandex.ru p10/branch/x86_64/classic release [137B]
Получено: 3 http://mirror.yandex.ru p10/branch/x86_64-i586/classic pkglist [17,9MB]
Получено: 4 http://mirror.yandex.ru p10/branch/x86_64-i586/classic release [142B]
Получено: 5 http://mirror.yandex.ru p10/branch/noarch/classic pkglist [7287kB]
Получено: 6 http://mirror.yandex.ru p10/branch/noarch/classic release [137B]
Получено 49,6MB за 13s (3578kB/s).
Чтение списков пакетов...
Построение дерева зависимостей...

=====
НАЧАЛЬНЫЙ Этап: предоставьте информацию об открытых IP-адресах и
именах хостов для обеспечения безопасности TLS и CORS
=====
```

Указание информации об открытых IP-адресах и именах хостов для обеспечения безопасности TLS и CORS

Следуйте инструкции по установке. Установщик попытается определить IP-адрес и имя хоста самостоятельно. Нажмите Enter, чтобы продолжить с выбранными данными, либо введите свои. Далее укажите имя организации, местонахождение (по умолчанию – Moscow), страну (по умолчанию – RU), провинцию (по умолчанию – RU) и название центра сертификации.

Укажите пароль для сертификатов, которые в дальнейшем будут использоваться в браузере. Запомните или запишите этот пароль, он потребуется при импорте сертификатов в браузер.

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
именах хостов для обеспечения безопасности TLS и CORS
=====

Настройка внешнего IP-адреса и/или имени хоста
=====

ПОДСКАЗКА: На каком интерфейсе будет доступен HTTP-порт веб-интерфейса KOMRAD. Установщик попытается определить IP-адрес и имя хоста.

Используйте клавиши со стрелками для навигации: ↑ ↓ → ←
Пожалуйста, выберите IP-адрес с внешнего сетевого интерфейсом:

Текущий выбранный: [ens18] 10.0.5.77

ПОДСКАЗКА: Вы выбрали 10.0.5.77, чтобы веб-интерфейс HTTP был доступен. Рекомендуется, чтобы вы указали этот адрес, вы можете дополнительно указать другие IP-адреса если предполагается, что доступ осуществляется через прокси-сервера, вы также должны указать доменные адреса если предполагается, что доступ осуществляется по имени (например, siem.some-corp.ru)

ПОДСКАЗКА: Какие дополнительные адреса указывать в CORS, AllowedHosts, и самоподписанном автоматически сгенерированном сертификате?

? IP-адреса и имена хостов для TLS 10.0.5.77,localhost,127.0.0.1,::1,komrad
Сервер будет настроен для внешнего подключения через 10.0.5.77,127.0.0.1,::1,komrad,localhost
записанные открытые хосты в /etc/echelon/.exposed_hosts

=====
ЗАВЕРШЕННЫЙ этап: предоставьте информацию об открытых IP-адресах и
именах хостов для обеспечения безопасности TLS и CORS
=====
```

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====

НАЧАЛЬНЫЙ Этап: создание сертификатов TLS для защиты веб-интерфейса
и/или межсервисного взаимодействия (mTLS)
=====

? Организация Customer LLC
? Местонахождение Moscow
? Страна RU
? Провинция RU
? Название центра сертификации (CA) KOMRAD-CA-Customer LLC
Выдача сертификата корневого центра сертификации...
running: komrad-cli [certificates create ca --cert-dir /var/lib/echelon/komrad/certs --ca /var/lib/echelon/komrad/certs/ca.pem --ca-key /var/lib/echelon/komrad/certs/ca-key.pem --organization Customer LLC --locality Moscow --country RU --province RU --common-name KOMRAD-CA-Customer LLC --expire 25y]
Создание и ключ...
ВАЖНО! Рекомендуется хранить файл закрытого ключа корневого сертификата отдельно.
OK. ca key=/var/lib/echelon/komrad/certs/ca-key.pem, ca certificate=/var/lib/echelon/komrad/certs/ca.pem

Выдача сертификатов сервера...ПРИМЕЧАНИЕ: вы можете выдать дополнительные серверные и клиентские TLS-сертификаты используя команду 'komrad-cli certs create [client|server] ...'
Создание сертификат сервера и ключ...
OK. server key=/var/lib/echelon/komrad/certs/server-key.pem, server certificate=/var/lib/echelon/komrad/certs/server.pem
OK

Выдача клиентских сертификатов...Создание сертификат клиента и ключ...
OK. client key=/var/lib/echelon/komrad/certs/client-key.pem, client certificate=/var/lib/echelon/komrad/certs/client.pem
OK

Выпуск пакета browser .p12...
? Пожалуйста, введите пароль для шифрования файла .p12 ***
Ваш пакет .p12 был сохранен как /var/lib/echelon/komrad/certs/bundle.p12.
Файл с сертификатами для браузера: /var/lib/echelon/komrad/certs/bundle.p12

=====
ЗАВЕРШЕННЫЙ этап: создание сертификатов TLS для защиты веб-интерфейса
и/или межсервисного взаимодействия (mTLS)
=====
```

Примечание. Для поддержки шифрования в целях повышения безопасности необходимо импортировать сгенерированные в процессе установки сертификаты в ваш браузер.

Установка базы данных Clickhouse

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
НАЧАЛЬНЫЙ Этап: установка базы данных Clickhouse
=====
Cannot set 'net admin' or 'ipc lock' or 'sys nice' or 'net bind service' capability for clickhouse binary. This is optional. Taskstats accounting will be disabled. To enable taskstats accounting you may add the required capability later manually.
ClickHouse binary is already located at /usr/bin/clickhouse
Symlink /usr/bin/clickhouse-server already exists but it points to /clickhouse. Will replace the old symlink to /usr/bin/clickhouse.
Creating symlink /usr/bin/clickhouse-server to /usr/bin/clickhouse.
Symlink /usr/bin/clickhouse-client already exists but it points to /clickhouse. Will replace the old symlink to /usr/bin/clickhouse.
Creating symlink /usr/bin/clickhouse-client to /usr/bin/clickhouse.
Symlink /usr/bin/clickhouse-local already exists but it points to /clickhouse. Will replace the old symlink to /usr/bin/clickhouse.
Creating symlink /usr/bin/clickhouse-local to /usr/bin/clickhouse.
Symlink /usr/bin/clickhouse-benchmark already exists but it points to /clickhouse. Will replace the old symlink to /usr/bin/clickhouse.
Creating symlink /usr/bin/clickhouse-benchmark to /usr/bin/clickhouse.
Symlink /usr/bin/clickhouse-obfuscator already exists but it points to /clickhouse. Will replace the old symlink to /usr/bin/clickhouse.
Creating symlink /usr/bin/clickhouse-obfuscator to /usr/bin/clickhouse.
Creating symlink /usr/bin/clickhouse-git-import to /usr/bin/clickhouse.
Symlink /usr/bin/clickhouse-compressor already exists but it points to /clickhouse. Will replace the old symlink to /usr/bin/clickhouse.
Creating symlink /usr/bin/clickhouse-compressor to /usr/bin/clickhouse.
Symlink /usr/bin/clickhouse-format already exists but it points to /clickhouse. Will replace the old symlink to /usr/bin/clickhouse.
Creating symlink /usr/bin/clickhouse-format to /usr/bin/clickhouse.
Symlink /usr/bin/clickhouse-extract-from-config already exists but it points to /clickhouse. Will replace the old symlink to /usr/bin/clickhouse.
Creating symlink /usr/bin/clickhouse-extract-from-config to /usr/bin/clickhouse.
Symlink /usr/bin/clickhouse-keeper already exists but it points to /clickhouse. Will replace the old symlink to /usr/bin/clickhouse.
Creating symlink /usr/bin/clickhouse-keeper to /usr/bin/clickhouse.
Symlink /usr/bin/clickhouse-keeper-converter already exists but it points to /clickhouse. Will replace the old symlink to /usr/bin/clickhouse.
Creating symlink /usr/bin/clickhouse-keeper-converter to /usr/bin/clickhouse.
Creating symlink /usr/bin/clickhouse-disks to /usr/bin/clickhouse.
Symlink /usr/bin/ch already exists. Will keep it.
Symlink /usr/bin/chl already exists. Will keep it.
Symlink /usr/bin/chc already exists. Will keep it.
Creating clickhouse group if it does not exist.
groupadd -r clickhouse
Creating clickhouse user if it does not exist.
useradd -r --shell /bin/false --home-dir /nonexistent -g clickhouse clickhouse
Will set ulimits for clickhouse user in /etc/security/limits.d/clickhouse.conf.
```

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

Symlink /usr/bin/ch already exists. Will keep it.
Symlink /usr/bin/chl already exists. Will keep it.
Symlink /usr/bin/chc already exists. Will keep it.
Creating clickhouse group if it does not exist.
groupadd -r clickhouse
Creating clickhouse user if it does not exist.
useradd -r --shell /bin/false --home-dir /nonexistent -g clickhouse clickhouse
Will set ulimits for clickhouse user in /etc/security/limits.d/clickhouse.conf.
Creating config directory /etc/clickhouse-server/config.d that is used for tweaks of main server configuration.
Creating config directory /etc/clickhouse-server/users.d that is used for tweaks of users configuration.
Config file /etc/clickhouse-server/config.xml already exists, will keep it and extract path info from it.
/etc/clickhouse-server/config.xml has /var/lib/clickhouse/ as data path.
/etc/clickhouse-server/config.xml has /var/log/clickhouse-server/ as log path.
Users config file /etc/clickhouse-server/users.xml already exists, will keep it and extract users info from it.
Creating log directory /var/log/clickhouse-server/.
Creating data directory /var/lib/clickhouse/.
Creating pid directory /var/run/clickhouse-server.
chown -R clickhouse:clickhouse '/var/log/clickhouse-server/'
chown -R clickhouse:clickhouse '/var/run/clickhouse-server/'
chown clickhouse:clickhouse '/var/lib/clickhouse/'
Password for the default user is an empty string. See /etc/clickhouse-server/users.xml and /etc/clickhouse-server/users.d to change it.
Setting capabilities for clickhouse binary. This is optional.
chown -R clickhouse:clickhouse '/etc/clickhouse-server/'

ClickHouse has been successfully installed.

Start clickhouse-server with:
sudo clickhouse start

Start clickhouse-client with:
clickhouse-client

Synchronizing state of clickhouse-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable clickhouse-server
Created symlink /etc/systemd/system/multi-user.target.wants/clickhouse-server.service → /lib/systemd/system/clickhouse-server.service.
записана конфигурация Clickhouse в /etc/echelon/.click

=====
ЗАВЕРШЕННЫЙ этап: установка базы данных Clickhouse
=====
```

Во время установки будут созданы бд komrad_pg и komrad_events.

Установка базы данных PostgreSQL из репозитория пакетов операционной системы

При необходимости может потребоваться вставить установочный диск.

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
НАЧАЛЬНЫЙ Этап: установка базы данных PostgreSQL из репозитория
пакетов операционной системы
=====

Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие дополнительные пакеты будут установлены:
  libossp-uuid16 libpq5 monit-base postgresql-common postgresql16-server
Следующие пакеты будут ОБНОВЛЕНЫ:
  ca-certificates libpq5
Следующие НОВЫЕ пакеты будут установлены:
  libossp-uuid16 monit-base postgresql-common postgresql16 postgresql16-contrib postgresql16-server
2 будет обновлено, 6 новых установлено, 0 пакетов будет удалено и 891 не будет обновлено.
Необходимо получить 9154kB архивов.
После распаковки потребуется дополнительно 42,3MB дискового пространства.
Получено: 1 http://mirror.yandex.ru p10/branch/noarch/classic ca-certificates 2022.09.15-alt1:p10+308004.100.2.1@1665748370 [367kB]
Получено: 2 http://mirror.yandex.ru p10/branch/x86_64/classic libossp-uuid16 1.6.2-alt2:sisyphus+279666.100.1.3@1626655767 [22,2kB]
Получено: 3 http://mirror.yandex.ru p10/branch/x86_64/classic libpq5 16.6-alt0.p10.1:p10+363004.100.1.1@1732112418 [227kB]
Получено: 4 http://mirror.yandex.ru p10/branch/noarch/classic monit-base 5.33.0-alt1:p10+326225.100.2.1@1691390973 [20,6kB]
Получено: 5 http://mirror.yandex.ru p10/branch/noarch/classic postgresql-common 1.0-alt8:sisyphus+277004.100.1.2@1625345331 [4598B]
Получено: 6 http://mirror.yandex.ru p10/branch/x86_64/classic postgresql16 16.6-alt0.p10.1:p10+363004.100.1.1@1732112418 [1833kB]
Получено: 7 http://mirror.yandex.ru p10/branch/x86_64/classic postgresql16-server 16.6-alt0.p10.1:p10+363004.100.1.1@1732112418 [6046kB]
Получено: 8 http://mirror.yandex.ru p10/branch/x86_64/classic postgresql16-contrib 16.6-alt0.p10.1:p10+363004.100.1.1@1732112418 [634kB]
Получено 9154kB за 1s (4784kB/s).
Совершаем изменения...
Подготовка... ##### [100%]
Обновление / установка...
1: monit-base-5.33.0-alt1 ##### [10%]
2: postgresql-common-1.0-alt8 ##### [20%]
3: libpq5-16.6-alt0.p10.1 ##### [30%]
4: postgresql16-16.6-alt0.p10.1 ##### [40%]
5: postgresql16-server-16.6-alt0.p10.1 ##### [50%]
6: libossp-uuid16-1.6.2-alt2 ##### [60%]
7: postgresql16-contrib-16.6-alt0.p10.1 ##### [70%]
8: ca-certificates-2022.09.15-alt1 ##### [80%]
Очистка / удаление...
9: libpq5-14.1-alt1 ##### [90%]
10: ca-certificates-2021.10.06-alt1 ##### [100%]
Завершено.
Чтение списков пакетов... Завершено
```

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

Очистка / удаление...
9: libpq5-14.1-alt1 ##### [90%]
10: ca-certificates-2021.10.06-alt1 ##### [100%]
Завершено.
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Последняя версия postgresql16-server уже установлена.
0 будет обновлено, 0 новых установлено, 0 пакетов будет удалено и 891 не будет обновлено.
Creating default database:
Файлы, относящиеся к этой СУБД, будут принадлежать пользователю "postgres".
От его имени также будет запускаться процесс сервера.

Кластер баз данных будет инициализирован с локалью "ru_RU.UTF-8".
Кодировка БД по умолчанию, выбранная в соответствии с настройками: "UTF8".
Выбрана конфигурация текстового поиска по умолчанию "russian".

Контроль целостности страниц данных отключён.

исправление прав для существующего каталога /var/lib/pgsql/data... ок
создание подкаталогов... ок
выбирается реализация динамической разделяемой памяти... posix
выбирается значение max_connections по умолчанию... 100
выбирается значение shared_buffers по умолчанию... 128MB
выбирается часовой пояс по умолчанию... Europe/Moscow
создание конфигурационных файлов... ок
выполняется подготовительный скрипт... ок
выполняется заключительная инициализация... ок
сохранение данных на диске... ок

initdb: предупреждение: включение метода аутентификации "trust" для локальных подключений
initdb: подсказка: Другой метод можно выбрать, отредактировав pg_hba.conf или ещё раз запустив initdb с ключом -A, --auth-local или --auth-host.

Success. You can now start the database server using:

    service postgresql start
or
    pg_ctl -D /var/lib/pgsql/data -l файл_журнала start

записанные сертификаты PostgreSQL в /etc/echelon/.pgpass
Обновление баз данных PostgreSQL
```

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка
контроль целостности страниц данных отключен.

исправление прав для существующего каталога /var/lib/pgsql/data... ок
создание подкаталогов... ок
выбирается реализация динамической разделяемой памяти... posix
выбирается значение max_connections по умолчанию... 100
выбирается значение shared_buffers по умолчанию... 128MB
выбирается часовой пояс по умолчанию... Europe/Moscow
создание конфигурационных файлов... ок
выполняется подготовительный скрипт... ок
выполняется заключительная инициализация... ок
сохранение данных на диске... ок

initdb: предупреждение: включение метода аутентификации "trust" для локальных подключений
initdb: подсказка: Другой метод можно выбрать, отредактировав pg_hba.conf или ещё раз запустив initdb с ключом -A, --auth-local или --auth-host.

Success. You can now start the database server using:

    service postgresql start
or
    pg_ctl -D /var/lib/pgsql/data -l файл_журнала start

записанные сертификаты PostgreSQL в /etc/echelon/.pgpass
Обновление пользователя postgres
ALTER ROLE
Создание расширения postgres
CREATE EXTENSION
Создание БД postgres komrad-preferences

Создание БД postgres komrad-grafana

Создание БД postgres pauth-preferences

Создание БД postgres scanner

=====
ЗАВЕРШЕННЫЙ этап: установка базы данных PostgreSQL из репозитория
пакетов операционной системы
=====
```

Во время установки будут созданы таблицы komrad-preferences, komrad-grafana, pauth-preferences, scanner.

Установка интеграционной шины (komrad-bus)

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
НАЧАЛЬНЫЙ Этап: установка интеграционной шины сообщений (komrad-bus)
=====
TUNER      APPLIED  ENABLED  SUPPORTED
ballast_file true     true     true
useradd: пользователь «komrad» уже существует
You may need to update the config at (/etc/echelon/komrad/komrad-bus.yaml). See the default config at /etc/echelon/komrad/komrad-bus.default.yaml.

=====
ЗАВЕРШЕННЫЙ этап: установка интеграционной шины сообщений (komrad-bus)
=====
```

Установка сервера аутентификации и управления пользователями (pauth-server)

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
НАЧАЛЬНЫЙ Этап: установка сервера аутентификации и управления
пользователями (pauth-server)
=====
useradd: пользователь «komrad» уже существует
You may need to update the config at (/etc/echelon/komrad/pauth-server.yaml). See the default config at /etc/echelon/komrad/pauth-server.default.yaml
Forcing database migration
2024-12-23T13:17:57.273+0300 INFO executing with PostgreSQL database {"pg_addr": "127.0.0.1:5432", "database": "pauth-preferences"}
}
2024-12-23T13:17:57.284+0300 INFO roles added {"role_names": ["admin"], "status": "success"}
2024-12-23T13:17:57.294+0300 INFO executing with PostgreSQL database {"pg_addr": "127.0.0.1:5432", "database": "pauth-preferences"}
}
2024-12-23T13:17:57.379+0300 INFO user added {"status": "success", "login": "admin", "roles": ["admin"]}
=====
ЗАВЕРШЕННЫЙ этап: установка сервера аутентификации и управления
пользователями (pauth-server)
=====
```

На этапе установки будут созданы роли `admin` и `user`. А также пользователь **admin** с паролем **admin**.

Установка API-шлюза для микросервисов KOMRAD (komrad-server)

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
НАЧАЛЬНЫЙ Этап: установка API-шлюза для микросервисов KOMRAD (komrad-server)
=====
useradd: пользователь «komrad» уже существует
You may need to update the config at (/etc/echelon/komrad/komrad-server.yaml). See the default config at /etc/echelon/komrad/komrad-server.default.yaml
Adding capabilities for binding ports <1024 to komrad-server...
copied file from komrad-ebpf-collector_v4.5.21_altlinux_10.x_amd64.rpm to /var/lib/echelon/komrad/packages/komrad-ebpf-collector_v4.5.21_altlinux_10.x_amd64.rpm
copied file from komrad-ebpf-collector_v4.5.21_altlinux_10.x_amd64.rpm.asc to /var/lib/echelon/komrad/packages/komrad-ebpf-collector_v4.5.21_altlinux_10.x_amd64.rpm.asc
copied file from komrad-ebpf-collector_v4.5.21_astra_1.8_amd64.deb to /var/lib/echelon/komrad/packages/komrad-ebpf-collector_v4.5.21_astra_1.8_amd64.deb
copied file from komrad-file-collector_v4.5.21_altlinux_10.x_amd64.rpm to /var/lib/echelon/komrad/packages/komrad-file-collector_v4.5.21_altlinux_10.x_amd64.rpm
copied file from komrad-file-collector_v4.5.21_altlinux_10.x_amd64.rpm.asc to /var/lib/echelon/komrad/packages/komrad-file-collector_v4.5.21_altlinux_10.x_amd64.rpm.asc
copied file from komrad-file-collector_v4.5.21_astra_1.8_amd64.deb to /var/lib/echelon/komrad/packages/komrad-file-collector_v4.5.21_astra_1.8_amd64.deb
copied file from komrad-http-collector_v4.5.21_altlinux_10.x_amd64.rpm to /var/lib/echelon/komrad/packages/komrad-http-collector_v4.5.21_altlinux_10.x_amd64.rpm
copied file from komrad-http-collector_v4.5.21_altlinux_10.x_amd64.rpm.asc to /var/lib/echelon/komrad/packages/komrad-http-collector_v4.5.21_altlinux_10.x_amd64.rpm.asc
copied file from komrad-http-collector_v4.5.21_astra_1.8_amd64.deb to /var/lib/echelon/komrad/packages/komrad-http-collector_v4.5.21_astra_1.8_amd64.deb
copied file from komrad-snmp-collector_v4.5.21_altlinux_10.x_amd64.rpm to /var/lib/echelon/komrad/packages/komrad-snmp-collector_v4.5.21_altlinux_10.x_amd64.rpm
copied file from komrad-snmp-collector_v4.5.21_altlinux_10.x_amd64.rpm.asc to /var/lib/echelon/komrad/packages/komrad-snmp-collector_v4.5.21_altlinux_10.x_amd64.rpm.asc
copied file from komrad-snmp-collector_v4.5.21_astra_1.8_amd64.deb to /var/lib/echelon/komrad/packages/komrad-snmp-collector_v4.5.21_astra_1.8_amd64.deb
copied file from komrad-sql-collector_v4.5.21_altlinux_10.x_amd64.rpm to /var/lib/echelon/komrad/packages/komrad-sql-collector_v4.5.21_altlinux_10.x_amd64.rpm
copied file from komrad-sql-collector_v4.5.21_altlinux_10.x_amd64.rpm.asc to /var/lib/echelon/komrad/packages/komrad-sql-collector_v4.5.21_altlinux_10.x_amd64.rpm.asc
copied file from komrad-sql-collector_v4.5.21_astra_1.8_amd64.deb to /var/lib/echelon/komrad/packages/komrad-sql-collector_v4.5.21_astra_1.8_amd64.deb
copied file from komrad-syslog-collector_v4.5.21_altlinux_10.x_amd64.rpm to /var/lib/echelon/komrad/packages/komrad-syslog-collector_v4.5.21_altlinux_10.x_amd64.rpm
copied file from komrad-xflow-collector_v4.5.21_altlinux_10.x_amd64.rpm to /var/lib/echelon/komrad/packages/komrad-xflow-collector_v4.5.21_altlinux_10.x_amd64.rpm
copied file from komrad-xflow-collector_v4.5.21_altlinux_10.x_amd64.rpm.asc to /var/lib/echelon/komrad/packages/komrad-xflow-collector_v4.5.21_altlinux_10.x_amd64.rpm.asc
copied file from komrad-xflow-collector_v4.5.21_astra_1.8_amd64.deb to /var/lib/echelon/komrad/packages/komrad-xflow-collector_v4.5.21_astra_1.8_amd64.deb
=====
ЗАВЕРШЕННЫЙ этап: установка API-шлюза для микросервисов KOMRAD
(komrad-server)
=====
```

Установка сервера обработки событий безопасности (komrad-processor)

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
НАЧАЛЬНЫЙ Этап: установка сервера обработки событий безопасности
(komrad-processor)
=====
useradd: пользователь «komrad» уже существует
You may need to update the config at (/etc/echelon/komrad/komrad-processor.yaml). See the default config at /etc/echelon/komrad/komrad-processor.default.yaml
Ожидается готовность komrad-server
Подключение к komrad-server успешно
=====
ЗАВЕРШЕННЫЙ этап: установка сервера обработки событий безопасности
(komrad-processor)
=====
```

Установка сканера сетевой безопасности (komrad-scanner)

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
НАЧАЛЬНЫЙ Этап: установка сканера сетевой безопасности (komrad-scanner)
=====
=== установка пмар. Начинаем. ===
=== установка пмар. Завершена. ===
useradd: пользователь «komrad» уже существует
You may need to update the config at (/etc/echelon/komrad/komrad-scanner.yaml). See the default config at /etc/echelon/komrad/komrad-scanner.default.yaml
=====
ЗАВЕРШЕННЫЙ этап: установка сканера сетевой безопасности (komrad-scanner)
=====
```

Установка сервера реагирования на инциденты (komrad-reactor)

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
НАЧАЛЬНЫЙ Этап: установка сервера реагирования на инциденты (komrad-reactor)
=====
You may need to update the config at (/etc/echelon/komrad/komrad-reactor.yaml). See the default config at /etc/echelon/komrad/komrad-reactor.default.yaml
=====
ЗАВЕРШЕННЫЙ этап: установка сервера реагирования на инциденты (komrad-reactor)
=====
```

Установка шины управляющих сообщений и передачи событий безопасности (komrad-correlation-dispatcher)

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
НАЧАЛЬНЫЙ Этап: установка шины управляющих сообщений и передачи
событий безопасности (komrad-correlation-dispatcher)
=====
useradd: пользователь «komrad» уже существует
You may need to update the config at (/etc/echelon/komrad/komrad-correlation-dispatcher.yaml). See the default config at /etc/echelon/komrad/komrad-correlation-dispatcher.default.yaml
=====
ЗАВЕРШЕННЫЙ этап: установка шины управляющих сообщений и передачи
событий безопасности (komrad-correlation-dispatcher)
=====
```

Установка сервера управления инцидентами (komrad-incident-manager)

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
НАЧАЛЬНЫЙ Этап: установка сервера управления инцидентами (komrad-incident-manager)
=====
useradd: пользователь «komrad» уже существует
You may need to update the config at (/etc/echelon/komrad/komrad-incident-manager.yaml). See the default config at /etc/echelon/komrad/komrad-incident-manager.default.yaml
=====
ЗАВЕРШЕННЫЙ этап: установка сервера управления инцидентами (komrad-incident-manager)
=====
```

Установка коллектора событий системного журнала (komrad-syslog-collector)

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
НАЧАЛЬНЫЙ Этап: установка коллектора событий системного журнала (komrad-syslog-collector)
=====
useradd: пользователь «root» уже существует
You may need to update the config at (/etc/echelon/komrad/komrad-syslog-collector.yaml). See the default config at /etc/echelon/komrad/komrad-syslog-collector.default.yaml
=====
ЗАВЕРШЕННЫЙ этап: установка коллектора событий системного журнала (komrad-syslog-collector)
=====
```

Установка локального и удаленного (SSH) коллектора файлов (komrad-file-collector)

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
НАЧАЛЬНЫЙ Этап: установка локального и удаленного (SSH) коллектора файлов (komrad-file-collector)
=====
useradd: пользователь «komrad» уже существует
You may need to update the config at (/etc/echelon/komrad/komrad-file-collector.yaml). See the default config at /etc/echelon/komrad/komrad-file-collector.default.yaml
=====
ЗАВЕРШЕННЫЙ этап: установка локального и удаленного (SSH) коллектора файлов (komrad-file-collector)
=====
```

Установка коллектора событий SNMP - trap и SNMP - агента (komrad-snmp-collector)

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
НАЧАЛЬНЫЙ Этап: установка коллектора событий SNMP-trap и SNMP-агента (komrad-snmp-collector)
=====
useradd: пользователь «komrad» уже существует
You may need to update the config at (/etc/echelon/komrad/komrad-snmp-collector.yaml). See the default config at /etc/echelon/komrad/komrad-snmp-collector.default.yaml
=====
ЗАВЕРШЕННЫЙ этап: установка коллектора событий SNMP-trap и SNMP-агента (komrad-snmp-collector)
=====
```

Установка коллектора базы данных (komrad-sql-collector)

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
НАЧАЛЬНЫЙ Этап: установка коллектора базы данных (komrad-sql-
collector)
=====
useradd: пользователь «komrad» уже существует
You may need to update the config at (/etc/echelon/komrad/komrad-sql-collector.yaml). See the default config at /etc/echelon/komrad/komrad-sql-collector.default.yaml
=====
ЗАВЕРШЕННЫЙ этап: установка коллектора базы данных (komrad-sql-
collector)
=====
```

Установка коллектора sFlow, NetFlow v5/v9, IPFIX (komrad-xflow-collector)

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
НАЧАЛЬНЫЙ Этап: установка коллектора sFlow, NetFlow v5/v9, IPFIX
(komrad-xflow-collector)
=====
useradd: пользователь «komrad» уже существует
You may need to update the config at (/etc/echelon/komrad/komrad-xflow-collector.yaml). See the default config at /etc/echelon/komrad/komrad-xflow-collector.default.yaml
=====
ЗАВЕРШЕННЫЙ этап: установка коллектора sFlow, NetFlow v5/v9, IPFIX
(komrad-xflow-collector)
=====
```

Установка HTTP(s) коллектора GET/POST (komrad-http-collector)

```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

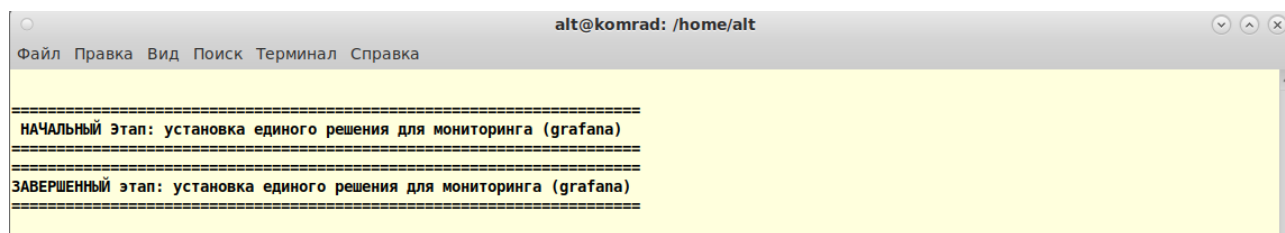
=====
НАЧАЛЬНЫЙ Этап: установка HTTP(s) коллектора GET/POST (komrad-http-
collector)
=====
useradd: пользователь «komrad» уже существует
You may need to update the config at (/etc/echelon/komrad/komrad-http-collector.yaml). See the default config at /etc/echelon/komrad/komrad-http-collector.default.yaml
=====
ЗАВЕРШЕННЫЙ этап: установка HTTP(s) коллектора GET/POST (komrad-http-
collector)
=====
```

Установка коллектора событий eBPF (komrad-ebpf-collector)

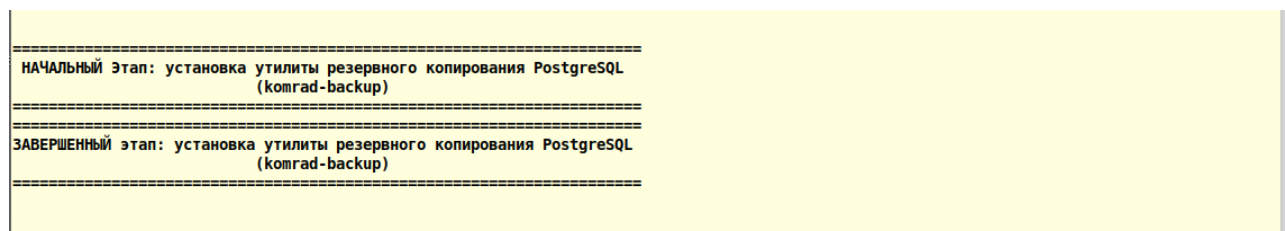
```
alt@komrad: /home/alt
Файл Правка Вид Поиск Терминал Справка

=====
НАЧАЛЬНЫЙ Этап: установка коллектора событий eBPF (komrad-ebpf-
collector)
=====
useradd: пользователь «root» уже существует
You may need to update the config at (/etc/echelon/komrad/komrad-ebpf-collector.yaml). See the default config at /etc/echelon/komrad/komrad-ebpf-collector.default.yaml
=====
ЗАВЕРШЕННЫЙ этап: установка коллектора событий eBPF (komrad-ebpf-
collector)
=====
```

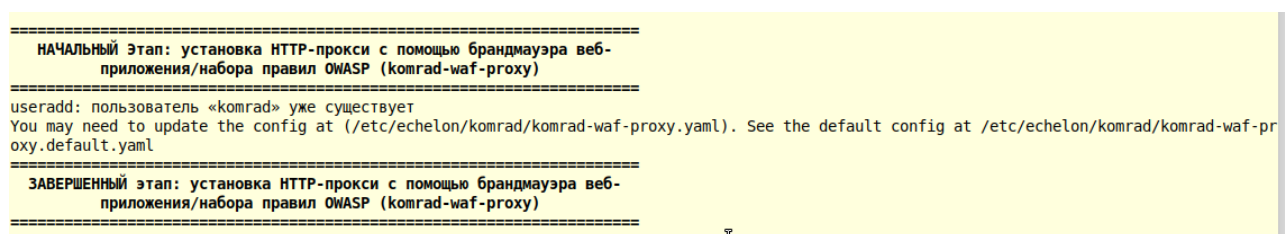
Установка единого решения для мониторинга (grafana)



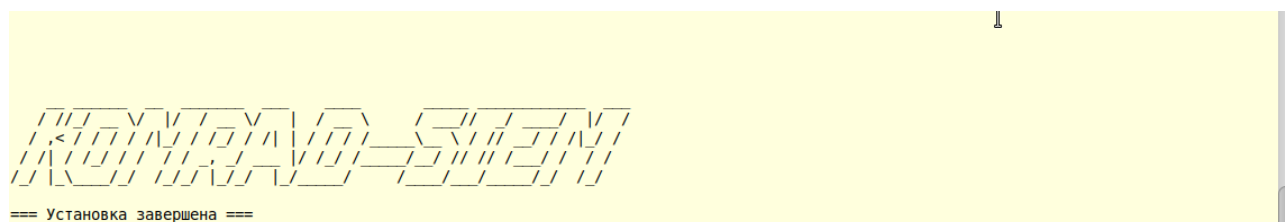
Установка утилиты резервного копирования PostgreSQL (komrad-backup)



Установка HTTP-прокси с помощью брандмауэра веб-приложения/набора правил OWASP (komrad-waf-proxy)



Установка завершена



Запуск

После установки KOMRAD – все сервисы автоматически запущены. В браузере Firefox вводим следующий адрес: **https://localhost**

Откроется окно входа в административную панель KOMRAD.

login: **admin**

password: **admin**

