# Содержание

# Установка и настройка VEOS

Если вы получили от нас уже готовую систему, то сразу обратитесь к разделу Инструкция по инсталляции.
В противном случае вам необходимо самостоятельно установить на ваш сервер операционную систему VEOS и предоставить нам удаленный доступ по SSH и права root для проведения работ по установке и начальной настройке платформы. После завершения работ удаленный доступ можно закрыть.

## Подготовка сервера и установка VEOS

1. Перед монтированием сервера в стойку убедитесь, что он соответствует необходимым требованиям. В случае выявления несоответствий на данном этапе обратитесь в техническую поддержку VAS Experts для оперативного решения вопроса.
2. Установите **VEOS по инструкции**

- Разметка диска:

```
~ 20 Гб для корневого раздела
остальное пространство можно отдать для директории  /var
SWAP  раздел CKAT не использует, но для системных задач может потребоваться, поэтому можно выделить 4ГБ
```

- Отключите Hyper-threading в BIOS

## Предварительная настройка VEOS

1. Создайте пользователя **vasexpertsmnt**:

   ```
   adduser -m -G wheel -u 3333 vasexpertsmnt
   ```

2. Задайте **сложный** пароль для пользователя **vasexpertsmnt**:

   ```
   passwd vasexpertsmnt
   ```

   Для удобства можете сгенерировать пароль с помощью openssl:

   ```
   openssl rand -base64 15
   ```

3. Сохраните пароль для **vasexpertsmnt**.
4. Установите разрешение пользователям группы wheel на использование всех команд от имени всех пользователей, для этого необходимо добавить в */etc/sudoers* строку:

   ```
   %wheel ALL=(ALL) NOPASSWD: ALL
   ```

5. Для предоставления удаленного доступа по SSH и установления ограничений на допустимые IP адреса из списка:

```
45.151.108.0/22, 94.140.198.64/27, 78.140.234.98, 193.218.143.187,
93.100.47.212, 93.100.73.160, 77.247.170.134, 91.197.172.2,
46.243.181.242, 93.159.236.11
```

```
    iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
    iptables -A INPUT -p tcp -s 45.151.108.0/22 -m tcp --dport 22 -j ACCEPT
    iptables -A INPUT -p tcp -s 94.140.198.64/27 -m tcp --dport 22 -j ACCEPT
    iptables -A INPUT -p tcp -s 78.140.234.98 -m tcp --dport 22 -j ACCEPT
    iptables -A INPUT -p tcp -s 193.218.143.187 -m tcp --dport 22 -j ACCEPT
    iptables -A INPUT -p tcp -s 93.100.47.212 -m tcp --dport 22 -j ACCEPT
    iptables -A INPUT -p tcp -s 93.100.73.160 -m tcp --dport 22 -j ACCEPT
    iptables -A INPUT -p tcp -s 77.247.170.134 -m tcp --dport 22 -j ACCEPT
    iptables -A INPUT -p tcp -s 91.197.172.2 -m tcp --dport 22 -j ACCEPT
    iptables -A INPUT -p tcp -s 46.243.181.242 -m tcp --dport 22 -j ACCEPT
    iptables -A INPUT -p tcp -s 93.159.236.11 -m tcp --dport 22 -j ACCEPT
    iptables -A INPUT -p tcp --dport 22 -j DROP
    service iptables save
```

Если вы используете firewalld:

```
    firewall-cmd --permanent --zone=public --add-rich-rule='rule
family="ipv4" source address="45.151.108.0/22" service name="ssh" accept'
firewall-cmd --permanent --zone=public --add-rich-rule='rule family="ipv4"
source address="94.140.198.64/27" service name="ssh" accept'
    firewall-cmd --permanent --zone=public --add-rich-rule='rule
family="ipv4" source address="78.140.234.98" service name="ssh" accept'
    firewall-cmd --permanent --zone=public --add-rich-rule='rule
family="ipv4" source address="193.218.143.187" service name="ssh" accept'
    firewall-cmd --permanent --zone=public --add-rich-rule='rule
family="ipv4" source address="93.100.47.212" service name="ssh" accept'
    firewall-cmd --permanent --zone=public --add-rich-rule='rule
family="ipv4" source address="93.100.73.160" service name="ssh" accept'
    firewall-cmd --permanent --zone=public --add-rich-rule='rule
family="ipv4" source address="77.247.170.134" service name="ssh" accept'
    firewall-cmd --permanent --zone=public --add-rich-rule='rule
family="ipv4" source address="91.197.172.2" service name="ssh" accept'
    firewall-cmd --permanent --zone=public --add-rich-rule='rule
family="ipv4" source address="46.243.181.242" service name="ssh" accept'
    firewall-cmd --permanent --zone=public --add-rich-rule='rule
family="ipv4" source address="93.159.236.11" service name="ssh" accept'
    firewall-cmd --reload
    firewall-cmd --zone=public --remove-service=ssh --permanent
```

**!Сохраните свои настройки, поскольку сервер в процессе инсталляции будет перезагружен!**

Убедившись в том что удаленный доступ по SSH обеспечен, пришлите в техподдержку компании VAS Experts (Service Desk) оформите заявку на установку лицензии CKAT с указанием пароля и имени пользователя для SSH доступа.

Установка ПО СКАТ осуществляется инженерами или самостоятельно по инструкции: instal_script.

Не обновляйте ядро операционной системы пока не активирована система обновлений, это может привести к отказу драйвера сетевой карты [1)]

Дальнейшие настройки производятся в зависимости от того, какие сценарии планируется использовать.

## Переход с CentOS на VEOS

В связи с тем, что Red Hat досрочно прекратила поддержку CentOS 8 в конце 2021 г. компания VAS Experts предлагает стратегию по дальнейшему использованию Red Hat в качестве Control Plane.
**Переход на новую редакцию ОС планируется в виде штатного обновления (без переустановки), в рамках активной технической поддержки.**

1)
Устранение отказа