SQUADUS

# Руководство по развертыванию Virtual Appliance

**ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»**

# ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

# SQUADUS

# РУКОВОДСТВО ПО РАЗВЕРТЫВАНИЮ VIRTUAL APPLIANCE

**1.4**

**На 18 листах**

**Москва**
**2024**

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки и товарные знаки принадлежат их владельцам.

Товарные знаки «МойОфис» и «MyOffice» принадлежат ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ».

Ни при каких обстоятельствах нельзя истолковывать любое содержимое настоящего документа как прямое или косвенное предоставление лицензии или права на использование товарных знаков, логотипов или знаков обслуживания, приведенных в нем. Любое несанкционированное использование этих товарных знаков, логотипов или знаков обслуживания без письменного разрешения их правообладателя строго запрещено.

**СОДЕРЖАНИЕ**



 

## ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращения, которые используются в настоящем документе, приведены в таблице 1.

Таблица 1 — Сокращения и расшифровки

| Сокращение | Расшифровка |
|---|---|
| ВМ | Виртуальная машина |
| CA-сертификат | Корневой сертификат SSL (или CA certificate), это цифровой документ, с помощью которого центры сертификации заверяют SSL-сертификаты при выдаче |
| ОС | Операционная система |
| DHCP | Протокол прикладного уровня модели TCP/IP, предназначенный для автоматической выдачи IP-адресов сетевым устройствам |
| DNS | Domain Name System, компьютерная распределенная система для получения информации о доменах |
| KVM | Kernel-based Virtual Machine, программное решение, обеспечивающее виртуализацию в среде Linux на платформе x86 с поддержкой аппаратной виртуализации на базе Intel VT (Virtualization Technology) либо AMD SVM (Secure Virtual Machine) |
| OVF | Open Virtualization Format, открытый стандарт для хранения и распространения виртуальных машин |
| SSH | Secure Shell, сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений |
| SSL-сертификат | Цифровая подпись сайта, виртуальный документ, гарантирующий безопасный обмен данными на сайте |
| VA | Squadus Virtual Appliance, образ ВМ в формате OVF с предустановленной системой Squadus |
| vCPU | Виртуальный процессор |
| IOPS | Input/Output Operations Per Second, количество операций ввода/вывода |
| RAM | Random Access Memory, оперативная память |
| SAN | Subject Alternative Name, расширение X.509 позволяющее использовать один сертификат для множества доменов |

# 1 ОБЩИЕ СВЕДЕНИЯ

Squadus Virtual Appliance (далее — VA) — образ ВМ в формате OVF с предустановленной системой Squadus. В состав VA входит консольная утилита `va-squadus` для упрощения конфигурирования стенда и выполнения вспомогательных задач (см. раздел «Утилита va-squadus для настройки стенда»).

## 1.1 Поддерживаемые платформы

В данном руководстве приведен пример установки VA в системе VMware ESXi 6.5.0. VA может быть развернут на любой системе виртуализации с поддержкой формата OVF (Open Virtualization Format).

Для установки на других системах виртуализации может потребоваться конвертация образа ВМ (см. раздел «Конвертация образов ВМ для систем виртуализации KVM»).

## 1.2 Характеристики виртуальной машины

Характеристики виртуальной машины приведены в таблице 2.

Таблица 2 — Характеристики виртуальной машины

| Параметр | Значение |
|---|---|
| Количество ядер | 8 vCPUs |
| Оперативная память | 16 Гбайт |
| HDD | 50 Гбайт |
| ОС | Astra Linux 1.7 SE |

Приведенные в таблице параметры являются минимальными рекомендуемыми. При необходимости параметры могут быть увеличены в среде виртуализации (версия ОС должна оставаться неизменной).

– требуется частота RAM не менее 2133 Mhz;
– требуется CPU с производительностью не менее Intel Xeon E5-2650V4;
– требуется производительность дисковой подсистемы не менее 300 IOPS.

## 2 ПЕРВЫЙ ЗАПУСК

### 2.1 Развертывание стенда на примере импорта VA в среду виртуализации ESXi

Для импорта VA необходимо воспользоваться мастером создания/регистрации виртуальных машин в панели администрирования ESXi 6.5.0. После открытия мастера необходимо последовательно выбрать меню **Virtual Machines, Create/Register VM** (см. Рисунок 1).

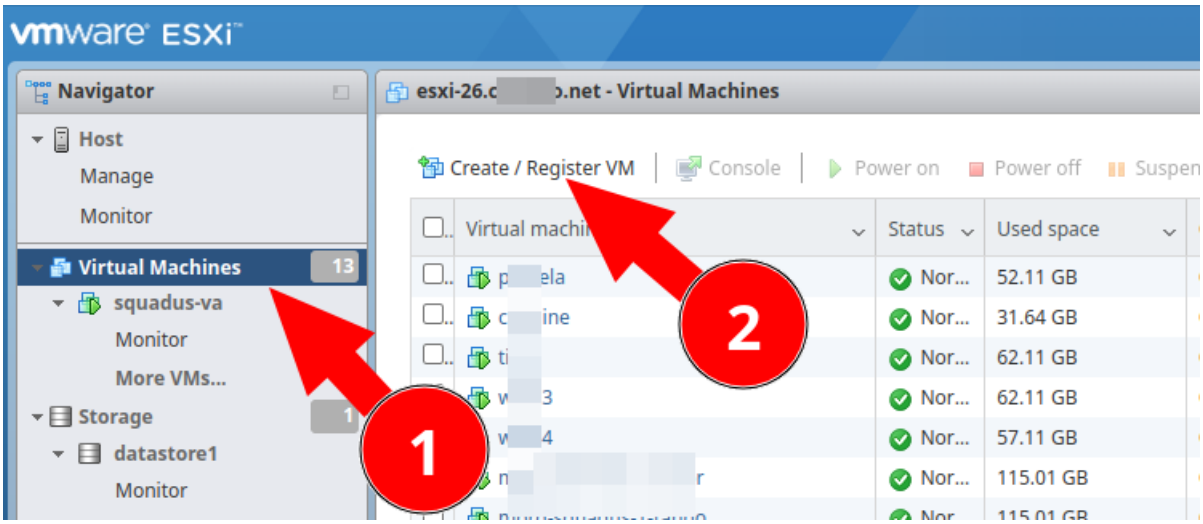


Рисунок 1 — Запуск мастера создания/регистрации виртуальных машин

В открывшемся списке следует выбрать пункт меню **Deploy a virtual machine from an OVF or OVA file** (см. Рисунок 2).

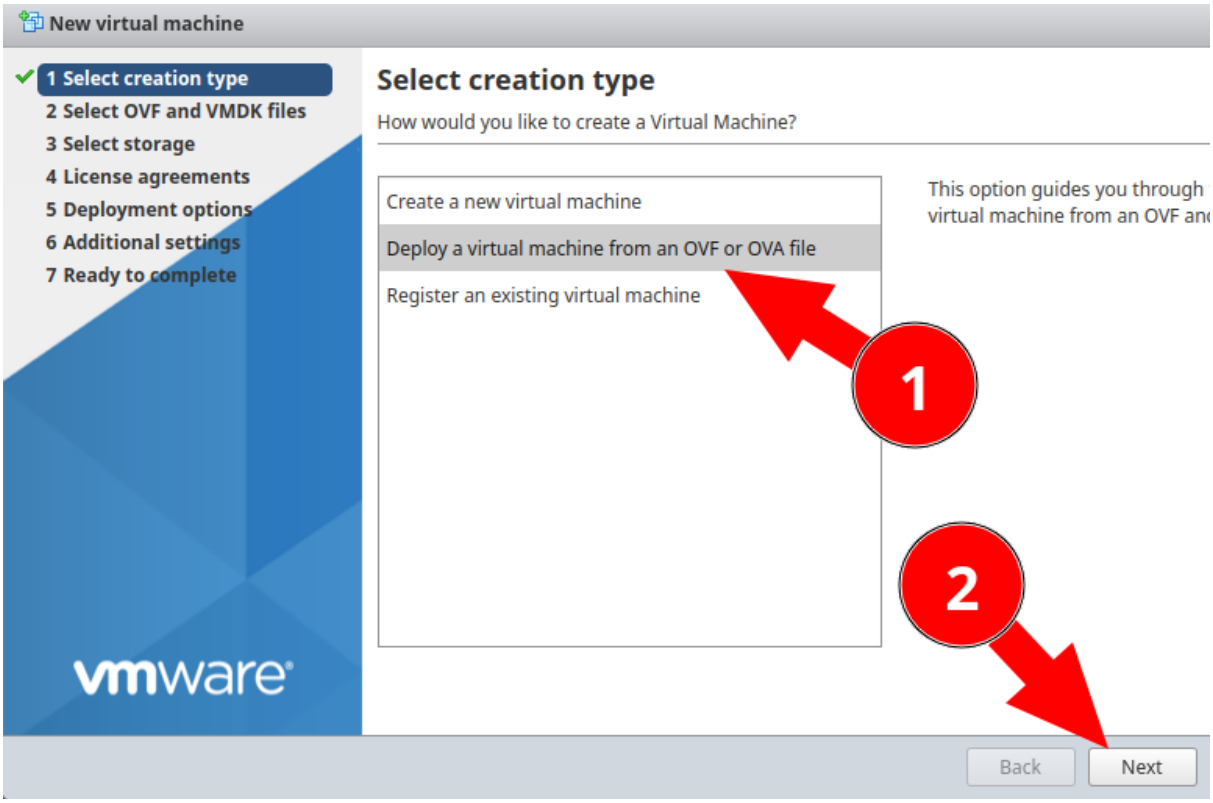


Рисунок 2 — Выбор варианта создания виртуальной машины

Необходимо ввести имя новой ВМ, затем выбрать или перетащить файл VA в окно **Click to select files or drag/drop** (см. Рисунок 3).

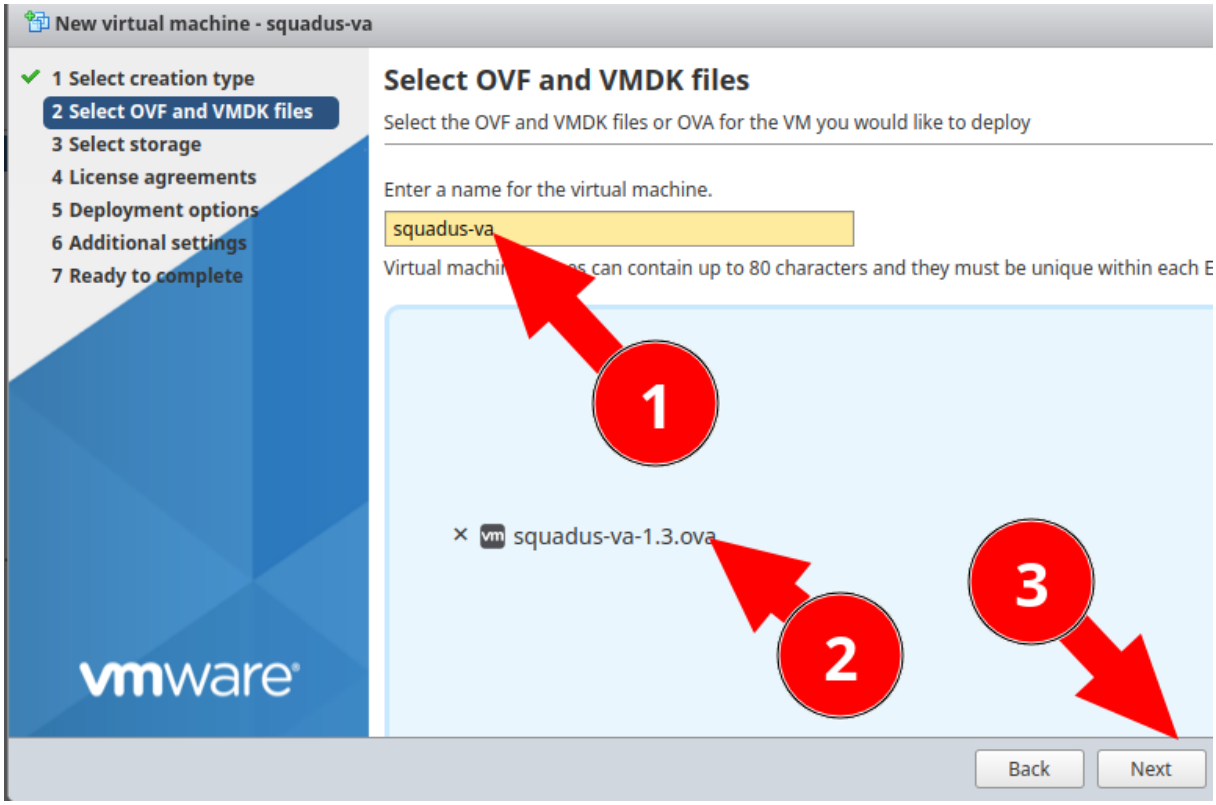


Рисунок 3 — Выбор имени и файла для создания виртуальной машины

Последующие пункты мастера создания/регистрации виртуальных машин содержат дополнительные настройки (параметры дискового хранилища и сетевых настроек), которые задаются согласно вашим требованиям.

После выбора дополнительных настроек необходимо запустить процесс импорта и дождаться его завершения (см. Рисунок 4).

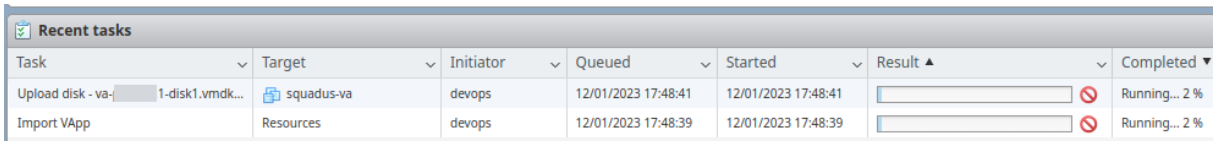


Рисунок 4 — Процесс установки

### 2.2 Настройка сети

По умолчанию сетевой интерфейс `eth0` в ВМ сконфигурирован на получение IP-адреса автоматически, по DHCP. Для доступа к ВМ следует использовать IP-адрес, выданный DHCP-сервером вашей инфраструктуры.

Необходимо убедиться, что IP-адрес, выданный по DHCP, закреплен за ВМ и будет выдаваться вашим DHCP-сервером на постоянной основе. При смене IP-адреса потребуется выполнение полной реконфигурации стенда (см. раздел «Полная реконфигурация стенда Squadus») и обновление DNS-записи.

Если инфраструктура не предусматривает использование DHCP-сервера, необходимо назначить статический IP-адрес для ВМ (см. раздел «Настройка статического IP-адреса»).

### 2.3 Административный доступ на ВМ

Для доступа по SSH необходимо использовать:

– имя пользователя «astra»;

– пароль «bt8btbGwEJg4awVU»;

– IP-адрес ВМ (см. раздел «Настройка сети»).

При отсутствии подключения по сети доступ осуществляется с помощью виртуальной консоли (TTY) в используемой системе виртуализации.

После успешной аутентификации в системе необходимо:

1. В целях безопасности сменить пароль по умолчанию с помощью команды:

```
passwd astra
```

2. Получить привилегии администратора системы с помощью команды:

```
sudo -i
```

3. Выполнять все операции от пользователя root.

### 2.4 Настройки межсетевого экранирования

Для корректной работы стенда необходимо обеспечить доступ клиентам по следующим портам:

– 80/tcp;

– 443/tcp;

– 10000/udp;

– 3478[tcp|udp];

– 5349[tcp|udp].

 

### 2.5 Выбор основного доменного имени

VA настроен по умолчанию для работы на домене example.net. При необходимости он может быть изменен с помощью утилиты `va-squadus` (см. раздел «Изменение основного домена для Squadus»).

### 2.6 Сертификаты SSL

VA поставляется с предустановленными самоподписанными wildcard SSL-сертификатами, которые подходят только для основного домена по умолчанию (*.example.net, example.net). Для корректной работы самоподписанного сертификата необходимо на всех клиентах, которые подключаются с серверу Squadus, установить корневой CA-сертификат в качестве доверенного.

Корневой CA-сертификат располагается на ВМ по следующему пути: `/root/install_squadus/certificates/ca.pem`.

Процедура добавления CA-сертификата зависит от используемой ОС, на которой будет работать клиент Squadus. Для установки следует обратиться к соответствующему руководству ОС.

В случае смены основного доменного имени необходимо установить подходящие SSL-сертификаты. SAN (Subject Alternative Name) устанавливаемого сертификата должен быть wildcard (*.new-domain.net, new-domain.net), либо содержать в себе все необходимые служебные поддомены:

– im.new-domain.net;

– go.new-domain.net;

– meet.new-domain.net;

– scc.new-domain.net;

– preview.new-domain.net;

– editor.new-domain.new;

– turn.new-domain.net.

Для установки нового сертификата следует воспользоваться утилитой `va-squadus` (см. раздел «Установка сертификата»), либо сгенерировать самоподписанный сертификат (см. раздел «Генерация самоподписанного сертификата»).

 

### 2.7 Необходимые внешние DNS-записи

Для подключения к стенду следует создать внешние DNS A-записи `im`, `go`, `meet`, `scc`, `preview`, `editor` и `turn` в DNS зоне основного домена (по умолчанию example.net), которые должны указывать на IP-адрес ВМ стенда.

### 2.8 Первичная настройка Squadus

После получения административного доступа и завершения настройки сети необходимо выполнить полную реконфигурацию стенда (см. раздел «Полная реконфигурация стенда Squadus»).

После завершения реконфигурации необходимо открыть адрес https://im.example.net с помощью браузера (значение example.net — домен по умолчанию, в случае изменения домена адрес будет отличаться). После перехода по адресу будет предложено создание первого пользователя в системе, обладающего правами администратора. Дополнительные настройки указываются согласно вашим требованиям.

Для полноценного функционирования Squadus необходимо указать лицензию в разделе **Администрирование -> Лицензии** (https://im.example.net/admin/licenses). Без ввода лицензии вся функциональность Squadus будет недоступна, а в приложении появится сообщение об ошибке **The application is blocked. License required** (см. Рисунок 5).

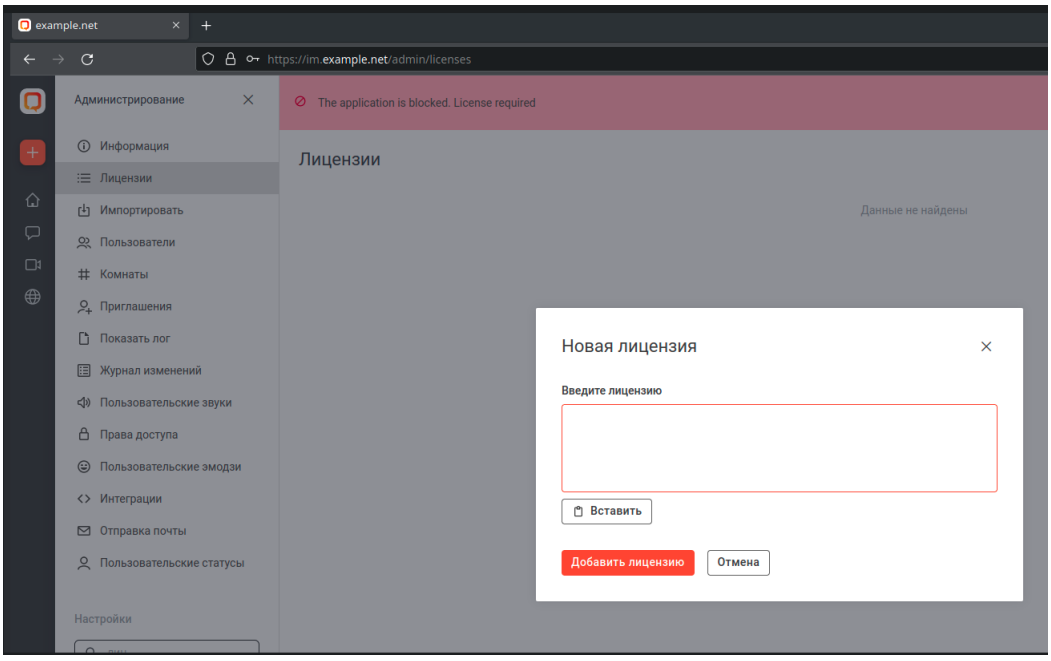


Рисунок 5 — Окно добавления лицензии

### 2.9 Настройка разрешения внешних доменных имен

Для разрешения сервисных доменных имен в VA используется внутренний DNS-сервер Unbound. Внешние доменные имена разрешаются с помощью перенаправления запросов на внешние DNS-серверы (по умолчанию 8.8.8.8, 8.8.4.4).

Если в инфраструктуре предусмотрены собственные DNS-серверы, их настройка выполняется с помощью утилиты `va-squadus`

(см. раздел «Настройка DNS серверов для разрешения доменных имен»).

# 3 УТИЛИТА VA-SQUADUS ДЛЯ НАСТРОЙКИ СТЕНДА

В состав VA входит консольная утилита `va-squadus`, предназначенная для настройки и обслуживания стенда. Для запуска утилиты необходимо переключиться на пользователя `root`.

Пример команды для запуска утилиты:

```
sudo -i va-squadus
```

После запуска откроется основное меню утилиты (см. Рисунок 6).

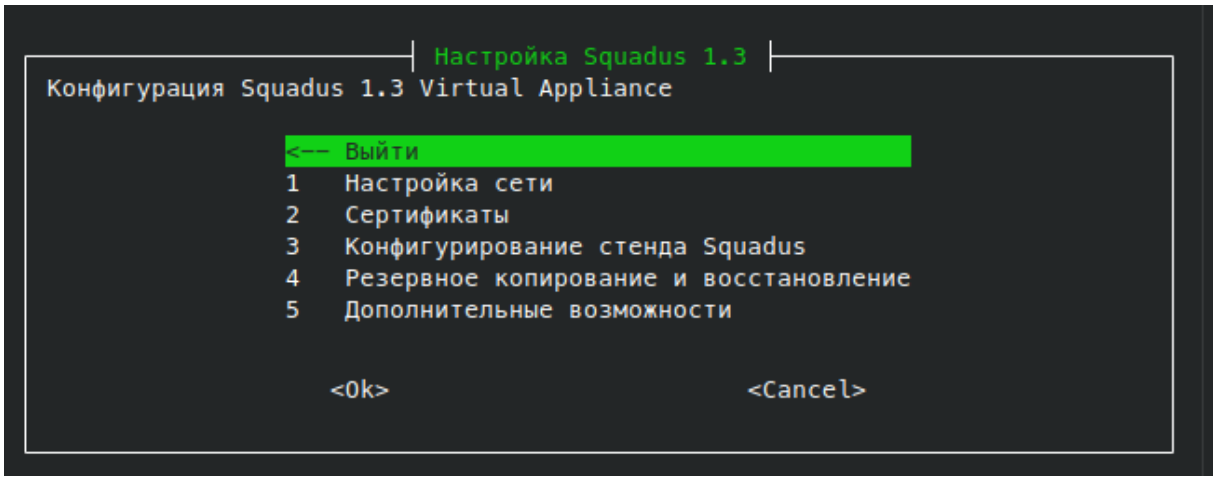


Рисунок 6 — Основное меню утилиты va-squadus

Навигация по пунктам меню осуществляется с помощью клавиш **Вверх**, **Вниз**, **Tab**. Активация выбранных пунктов выполняется клавишей **Enter**.

## 3.1 Настройка сети

### 3.1.1 Настройка статического IP-адреса

Пункт меню позволяет настроить статический IP-адрес для интерфейса `eth0`. Используется, если в инфраструктуре не предусмотрен DHCP-сервер для автоматического назначения IP-адресов или если автоматическая выдача адресов нежелательна. При активации необходимо ввести IP-адрес, маску подсети в формате «Dotted Decimal Notation» и основной шлюз. Новые настройки будут применены после ввода всех данных.

### 3.1.2 Настройка получения IP-адреса по DHCP

Пункт меню позволяет настроить получение IP-адреса автоматически, по DHCP. VA поставляется с этой настройкой по умолчанию.

### 3.1.3 Настройка DNS серверов для разрешения доменных имен

Для разрешения доменных имен в VA используется внутренний сервер Unbound, который обеспечивает работу служебных доменных имен, необходимых для корректного функционирования. Для разрешения остальных доменных имен запросы перенаправляются на внешние DNS-серверы (по умолчанию 8.8.8.8, 8.8.4.4).

Этот пункт меню позволяет настроить другие DNS-серверы для разрешения внешних доменных имен, сохраняя функциональность разрешения сервисных доменных имен, поддерживаемых сервером Unbound.

Другие способы настройки DNS могут нарушить работоспособность стенда (например, редактирование конфигурационного файла `/etc/resolv.conf`), поэтому их использование не допускается.

## 3.2 Сертификаты

### 3.2.1 Генерация самоподписанного сертификата

Позволяет сгенерировать самоподписанный (self-signed) wildcard сертификат и установить его на стенд. При активации необходимо ввести домен без «*.», например, example.net.

### 3.2.2 Установка сертификата

Пункт меню позволяет установить сертификаты двумя способами:

1. Выбрать в системе с помощью файлового менеджера сертификат, ключ сертификата, не защищенного паролем, а также корневой CA-сертификат.
2. Вставить текстовые значения из буфера обмена в текстовый редактор.

После установки сертификаты будут применены для стенда.

### 3.3 Конфигурирование стенда Squadus

#### 3.3.1 Полная реконфигурация стенда Squadus

Пункт меню позволяет привести Squadus в соответствие текущим параметрам ВМ и Ansible-конфигурации. Используется для восстановления работоспособности и сброса настроек после неудачной конфигурации.

#### 3.3.2 Изменение основного домена для Squadus

Изменение основного домена и применение конфигурации для стенда. По умолчанию стенд сконфигурирован на использование домена example.net, при необходимости может быть изменен.

#### 3.3.3 Изменение способа формирования доменного имени для Squadus

Позволяет изменить шаблон для формирования доменного имени по умолчанию `{service}.{domain}`. Шаблон предназначен для гибкого формирования доменного имени стенда в сочетании с основным доменом.

Пример:

При использовании шаблона `{service}-{domain}` и основного домена `squadus-va.example.net`, будут созданы доменные имена вида: `im-squadus-va.example.net`, `meet-squadus-va.example.net` и т.д.

Настройка используется при пересечении с существующими записями в зоне основного домена.

 

### 3.3.4 Резервное копирование и восстановление

Пункты меню позволяют выполнить резервное копирование базы данных Squadus, а также объектного хранилища (см. Рисунок 7). В базе данных хранятся сообщения и настройки стенда, а в объектном хранилище — файлы вложений.

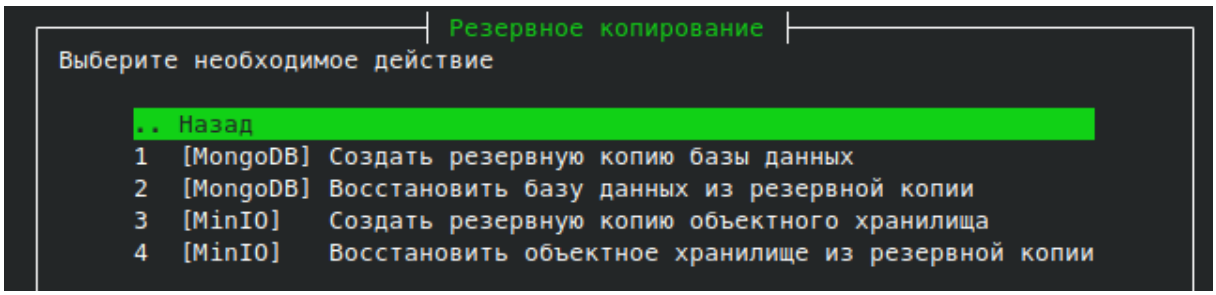


Рисунок 7 — Меню резервного копирования

### 3.4 Выбор текстового редактора по умолчанию

Этот пункт меню позволяет выбрать текстовый редактор по умолчанию (vim). Может быть полезным перед активацией вставки SSL-сертификатов из буфера обмена (см. раздел «Установка сертификата»).

## 4 КОНВЕРТАЦИЯ ОБРАЗОВ ВИРТУАЛЬНОЙ МАШИНЫ ДЛЯ СИСТЕМ ВИРТУАЛИЗАЦИИ KVM

Для конвертации образов используется команда `qemu-img`.

Для установки `qemu-img` необходимо использовать следующие команды:

1. Для ОС Red Hat Enterprise based linux:

```
yum install qemu-img
```

2. Для ОС Debian based linux:

```
apt-get install qemu-utils
```

Команда `qemu-img` использует параметры, приведенные в таблице 3.

Таблица 3 — Аргументы команды qemu-img

| Формат образа | Аргумент команды qemu-img |
|---|---|
| QCOW2 (KVM, Xen) | qcow2 |
| QED (KVM) | qed |
| VDI (VirtualBox) | vdi |
| VHD (Hyper-V) | vpc |
| VMDK (VMware) | vmdk |

Большинство систем виртуализации, основанных на KVM, поддерживают образы дисков типа `raw` или `qcow2`.

Пример использования `qemu-img`:

Распаковка файла виртуальной машины в формате `ova` и конвертация `vmdk` файла в `raw` образ выполняется с помощью команды:

```
$ tar xf va-squadus-1.4.ova
$ qemu-img convert -f vmdk -O raw va-squadus-disk1.vmdk va-squadus.img
```