



Система защиты ИТ-  
инфраструктуры от кибератак на  
базе технологии Deception

---

Руководство по  
развертыванию

## **Контактная информация**

127106, г. Москва, ул. Гостиничная, д.5

Тел.: +7 (495) 988-92-25

E-mail: [office@avsw.ru](mailto:office@avsw.ru)

[www.avsw.ru/about/contacts](http://www.avsw.ru/about/contacts)

## **Авторское право**

ООО «АВ Софт»

[www.avsw.ru](http://www.avsw.ru)

© 2010-2023 ООО «АВ Софт»

## **Версия документа**

Руководство по развертыванию v5.0

Май 25, 2023.

Настоящий документ является собственностью ООО «АВ Софт» (далее — «АВ Софт») и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения «АВ Софт».

Документ может быть изменен без предварительного уведомления.

## СОДЕРЖАНИЕ

|          |                                                           |           |
|----------|-----------------------------------------------------------|-----------|
| <b>1</b> | <b>Термины и определения .....</b>                        | <b>4</b>  |
| <b>2</b> | <b>Описание поставки .....</b>                            | <b>5</b>  |
| 2.1      | Сетевые настройки.....                                    | 6         |
| 2.2      | Технические требования .....                              | 6         |
| <b>3</b> | <b>Описание развертывания на VMware ESXI Server .....</b> | <b>8</b>  |
| 3.1      | VMware ESXI Server .....                                  | 8         |
| 3.2      | Настройка сервиса менеджмента .....                       | 15        |
| 3.3      | Настройка сенсора.....                                    | 16        |
| <b>4</b> | <b>Описание развертывания на Microsoft Hyper-V.....</b>   | <b>17</b> |
| 4.1      | loki-server.....                                          | 17        |
| 4.2      | loki-sensor.....                                          | 22        |
| <b>5</b> | <b>Настройки в веб-интерфейсе .....</b>                   | <b>26</b> |
| 5.1      | Добавление сенсора .....                                  | 26        |

## 1 Термины и определения

В настоящем документе используются термины и определения, представленные в таблице 1.

Таблица 1. Термины и определения

| №  | Термин            | Определение                                                           |
|----|-------------------|-----------------------------------------------------------------------|
| 1. | Ловушка           | Контейнер сенсора имитирующий узел в сети.                            |
| 2. | Приманка          | Значимые для кибератаки данные, ведущие на ловушку.                   |
| 3. | Primary interface | Основной интерфейс для общения между сенсором и сервисом менеджмента. |

В настоящем документе используется перечень сокращений, представленный в таблице 2.

Таблица 2. Перечень сокращений

| №  | Сокращение | Значение                         |
|----|------------|----------------------------------|
| 1. | АРМ        | Автоматизированное рабочее место |
| 2. | ВМ         | Виртуальная машина               |
| 3. | ПО         | Программное обеспечение          |
| 4. | СУБД       | Система управления базами данных |
| 5. | VLAN       | Virtual Local Area Network       |

## 2 Описание поставки

Система реализована на едином программном обеспечении (платформе). Программное обеспечение (далее – ПО) системы LOKI состоит из программных модулей, описанных в таблице 3.

Таблица 3. Описание модулей ПО

| №  | Описание модуля      | Описание                                   | Формат файлов |
|----|----------------------|--------------------------------------------|---------------|
| 1. | Модуль управления    | Управление комплексом                      | server.ova    |
| 2. | Сенсоры сканирования | Сканирование подсетей и размещение ловушек | sensor.ova    |

Сервис менеджмента подключается к сенсору иницируя SSH сессию. Сенсор может подключиться к менеджменту, если он предварительно будет добавлен в сервис менеджмента.

Каждый распределенный модуль размещения ловушек (сенсор) обеспечивает возможность функционирования множества ловушек (эмулируемых устройств) одновременно в множестве VLAN. Сетевое взаимодействие таких ловушек (эмулированных устройств) может быть обеспечено на этапе развертывания сенсора как за счет подключения дополнительных сетевых интерфейсов, так и через единый сетевой интерфейс (TRUNK).

Модули системы взаимодействуют между собой с использованием TLS шифрования версии 1.3.

Система LOKI имеет возможность масштабирования по производительности путем подключения дополнительных компонентов (модулей размещения ловушек – сенсоров) без изменения архитектуры (горизонтальное масштабирование). При этом единый централизованный модуль управления имеет возможность осуществлять управления не менее, чем 150 модулями размещения ловушек.

Единый централизованный модуль управления предоставляет возможность масштабирования для обеспечения функционирования приманок на 80 000 APM и серверов, а также интеграции для этих целей со 120 доменами Active Directory без изменения архитектуры решения.

Все компоненты системы LOKI после установки располагаются в инфраструктуре Заказчика (on-premise). Обрабатываемая в системе

информация не передается за пределы инфраструктуры Заказчика.

Подключение к сети Интернет требуется на этапе установки системы LOKI, а также во время эксплуатации – для обновления базы данных уязвимостей.

Операционным ядром системы LOKI выступает ОС Debian. Альтернативный способ сборки системы может быть осуществлен на базе ОС Astra Linux (версии не ниже 1.7, Орел и Воронеж). В качестве СУБД системы LOKI выступает система MySQL.

## 2.1 Сетевые настройки

Необходимые сетевые доступы описаны в таблице 4.

Таблица 4. Сетевые доступы

| №         | Источник                                                         | Назначение       | Порт/Протокол |
|-----------|------------------------------------------------------------------|------------------|---------------|
| <b>1.</b> | <b>Сервис менеджмента</b>                                        |                  |               |
| 1.1.      | Доступ до машины                                                 | SSH              | 22/TCP        |
| 1.2.      | Интерфейс                                                        | HTTP             | 80/TCP        |
| 1.3.      | Интерфейс                                                        | HTTPS            | 443/TCP       |
| 1.4.      | Zabbix                                                           | Zabbix           | 10050/TCP     |
| 1.5.      | VPN                                                              | VPN              | 52302/UDP     |
| <b>2.</b> | <b>Сенсор</b>                                                    |                  |               |
| 2.1.      | RabbitMQ                                                         | RabbitMQ         | 5672/TCP      |
| 2.2.      | Общение с менеджментом                                           | -                | 32000-63000   |
| <b>3.</b> | <b>Агент на рабочее место</b> (у агента нет портов на прослушку) | Доступ к сенсору | 5672/TCP      |

## 2.2 Технические требования

Для развертывания модуля управления системы LOKI необходимо использовать серверное оборудование с минимальными характеристиками, указанными в таблице 5.

**Таблица 5. Технические характеристики (модуль управления)**

| <b>№</b>                 | <b>Параметры</b>           | <b>Минимальные требования</b> |
|--------------------------|----------------------------|-------------------------------|
| <b>Модуль управления</b> |                            |                               |
| 1.                       | Количество ядер процессора | 2                             |
| 2.                       | Оперативная память         | 32 GB                         |
| 3.                       | Диск                       | SSD 1 TB x 2 (RAID 1)         |
| 4.                       | Сеть                       | 10/100/1000 Мбит/с (2шт.)     |

Для развертывания сенсора системы LOKI необходимо использовать серверное оборудование с минимальными характеристиками, указанными в таблице 6.

**Таблица 6. Технические характеристики (сенсор)**

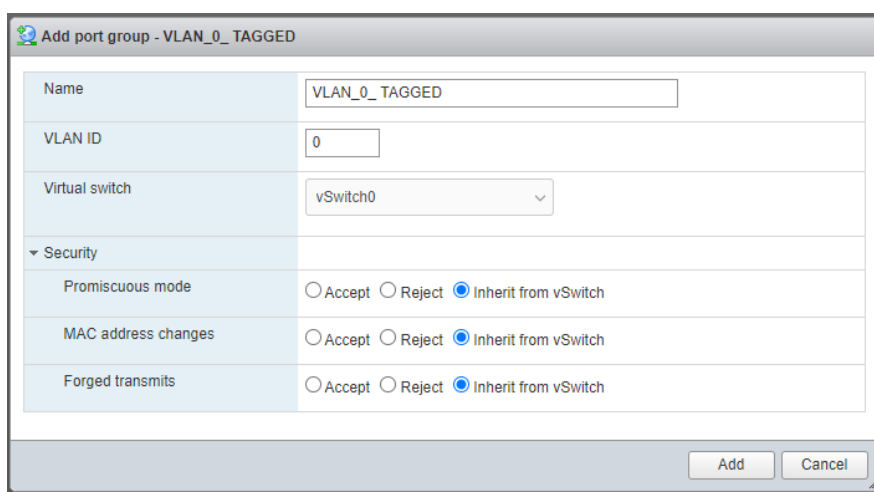
| <b>№</b>                   | <b>Параметры</b>           | <b>Минимальные требования</b> |
|----------------------------|----------------------------|-------------------------------|
| <b>Сенсор (10 ловушек)</b> |                            |                               |
| 1.                         | Количество ядер процессора | 2                             |
| 2.                         | Оперативная память         | 6 GB                          |
| 3.                         | Диск                       | SSD 256 GB x 2 (RAID 1)       |
| 4.                         | Сеть                       | 10/100/1000 Мбит/с (2шт.)     |

Система LOKI позволяет осуществлять управление не менее, чем 50 модулями размещения ловушек (сенсорами), а также обеспечивать функционирование приманок не менее, чем на 10000 АРМ и серверов.

## 3 Описание разворачивания на VMware ESXI Server

### 3.1 VMware ESXI Server

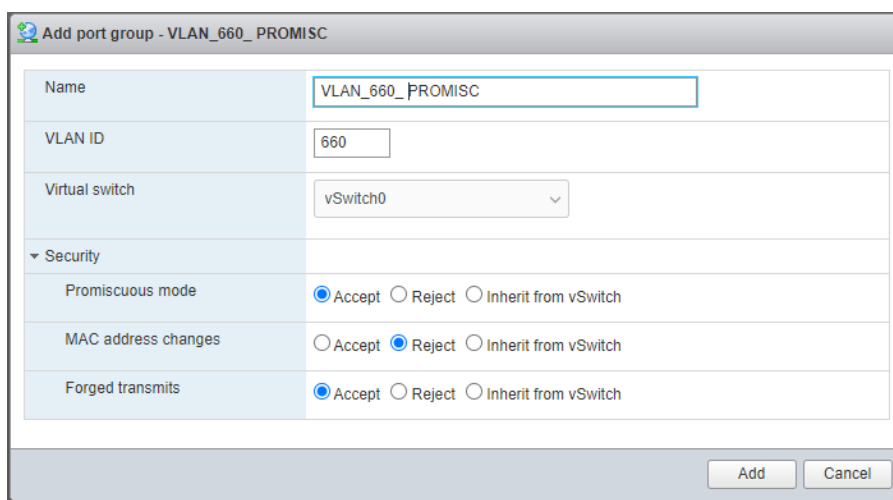
Система LOKI поддерживается установку на VMware ESX Server (далее – ESXI) от 5.5 версии. Для установки системы LOKI в среде виртуализации ESXi необходимо выделить минимум два сетевых интерфейса со свободным ID (выбранный ID необходимо будет вписать в настройки разворачиваемой виртуальной машины LOKI). Для этого в интерфейсе ESXi в разделе «**Networking > Port groups**» необходимо создаем VLAN\_(выбранный ID)\_TAGGED, «**Add port group**», со следующими настройками безопасности, как показано на рисунке 1, по завершении ввода данных необходимо нажать «**Add**».



| Add port group - VLAN_0_TAGGED |                                                                                                                 |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Name                           | VLAN_0_TAGGED                                                                                                   |
| VLAN ID                        | 0                                                                                                               |
| Virtual switch                 | vSwitch0                                                                                                        |
| ▼ Security                     |                                                                                                                 |
| Promiscuous mode               | <input type="radio"/> Accept <input type="radio"/> Reject <input checked="" type="radio"/> Inherit from vSwitch |
| MAC address changes            | <input type="radio"/> Accept <input type="radio"/> Reject <input checked="" type="radio"/> Inherit from vSwitch |
| Forged transmits               | <input type="radio"/> Accept <input type="radio"/> Reject <input checked="" type="radio"/> Inherit from vSwitch |
| <div>Add Cancel</div>          |                                                                                                                 |

Рисунок 1. Настройка сетевого интерфейса модуля управления

В данном VLAN будет располагаться модуль управления системой LOKI. Вторую Port Group по аналогии нужно сделать, как показано на рисунке 2.



| Add port group - VLAN_660_PROMISC |                                                                                                                 |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------|
| Name                              | VLAN_660_PROMISC                                                                                                |
| VLAN ID                           | 660                                                                                                             |
| Virtual switch                    | vSwitch0                                                                                                        |
| ▼ Security                        |                                                                                                                 |
| Promiscuous mode                  | <input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Inherit from vSwitch |
| MAC address changes               | <input type="radio"/> Accept <input checked="" type="radio"/> Reject <input type="radio"/> Inherit from vSwitch |
| Forged transmits                  | <input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Inherit from vSwitch |
| <div>Add Cancel</div>             |                                                                                                                 |

Рисунок 2. Настройка сетевого интерфейса сенсора

В данном VLAN будут располагаться имитируемые устройства (ловушки), которые будут принимать входящие подключения атакующих.

Далее необходимо создать ещё одну выделенную PortGroup «VLAN\_(выбранный ID)\_PROMISC» чтобы было как минимум две PortGroup: например, «VLAN\_660\_PROMISC» и «VLAN\_0\_TAGGED». В данном случае «VLAN\_660\_PROMISC» будет использоваться для развёртывания устройств-ловушек.

Далее необходимо создать виртуальную машину для развёртывания образа дистрибутива сервиса менеджмента системы LOKI. Для этого нужно перейти в раздел «**Virtual Machines**», нажать «**Create / Register VM**», в пункте 1 «**Select creation type**» выбрать «**Deploy a virtual machine from an OVF or OVA file**», далее нажать кнопку «**Next**» (Рисунок 3).

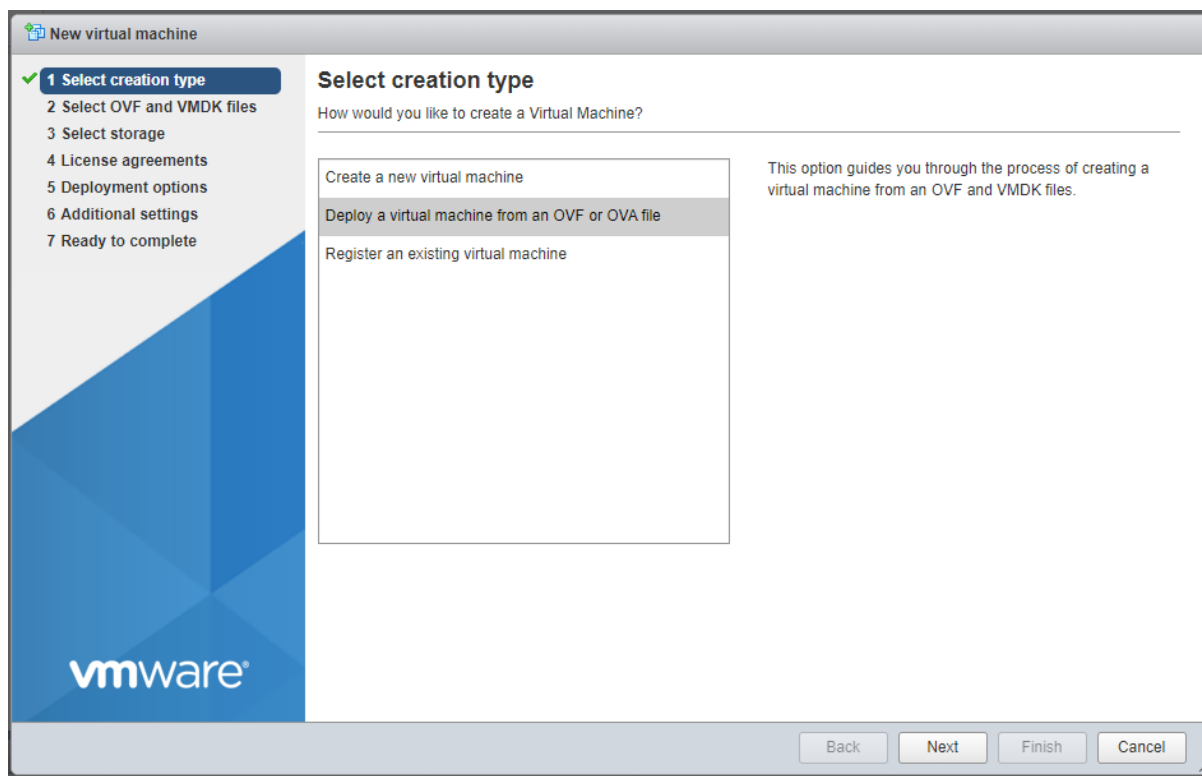


**Рисунок 3. Выбор типа файла для развёртывания**

Далее необходимо в пункте 2 «**Select OVF and VMDK files**» присвоить имя виртуальной машине и выбрать файл для загрузки (Рисунок 4).

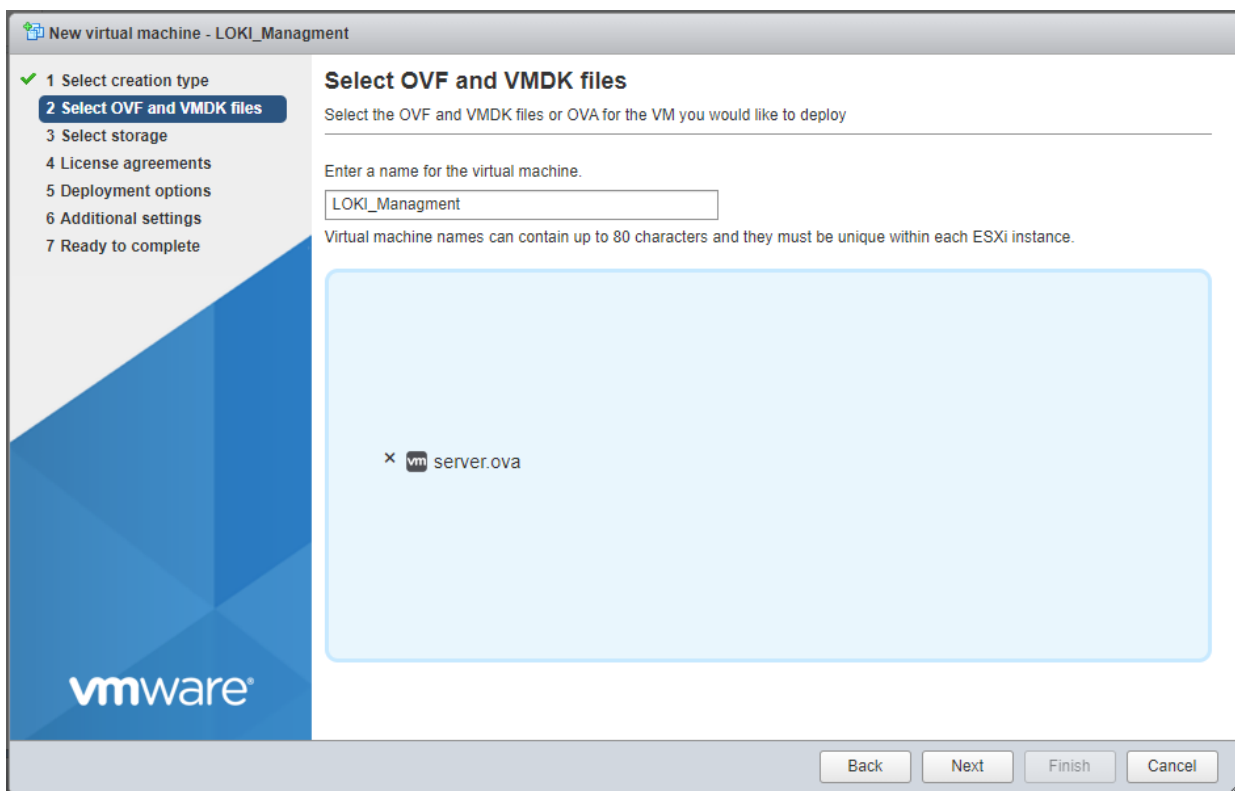


Рисунок 4. Импорт файла в виртуальную машину

Далее в пункте 3 «**Select storage**» необходимо выбрать хранилище, в котором будет размещен образ и нажать кнопку «**Next**» (Рисунок 5).

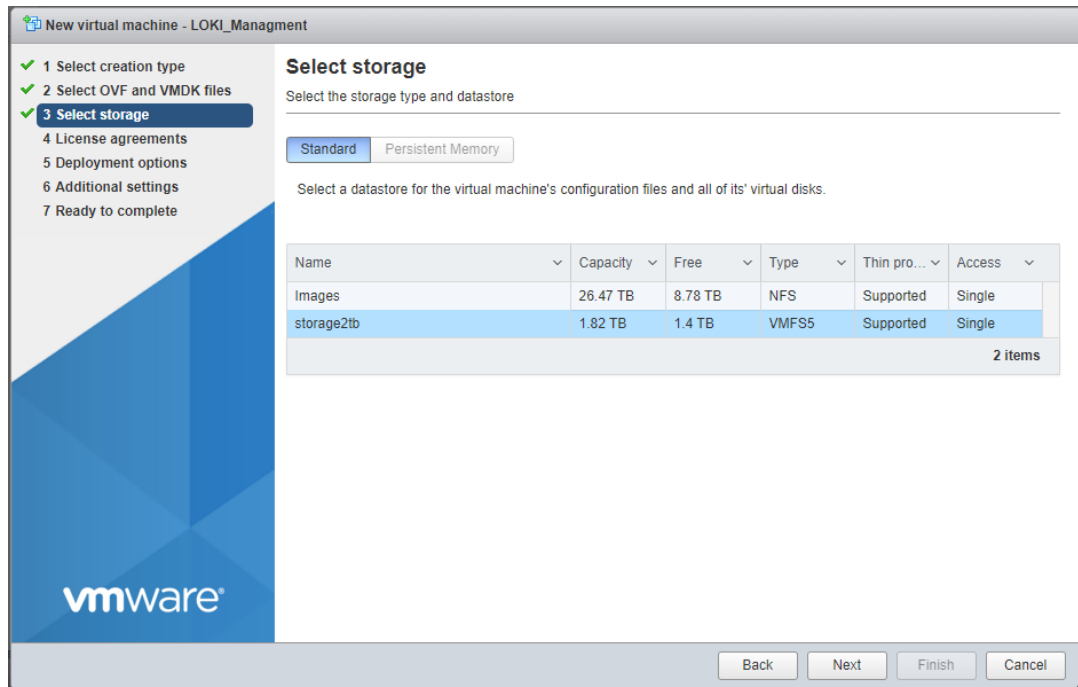


Рисунок 5. Выбор хранилища для размещения образа

Далее в пункте 4 «**Deployment options**» необходимо выбрать VLAN, способ размещения на диске (по умолчанию рекомендуется «тонкий», в случае необходимости — перезагрузите страницу) и автоматический способ запуска и нажать кнопку «**Next**» (Рисунок 6).

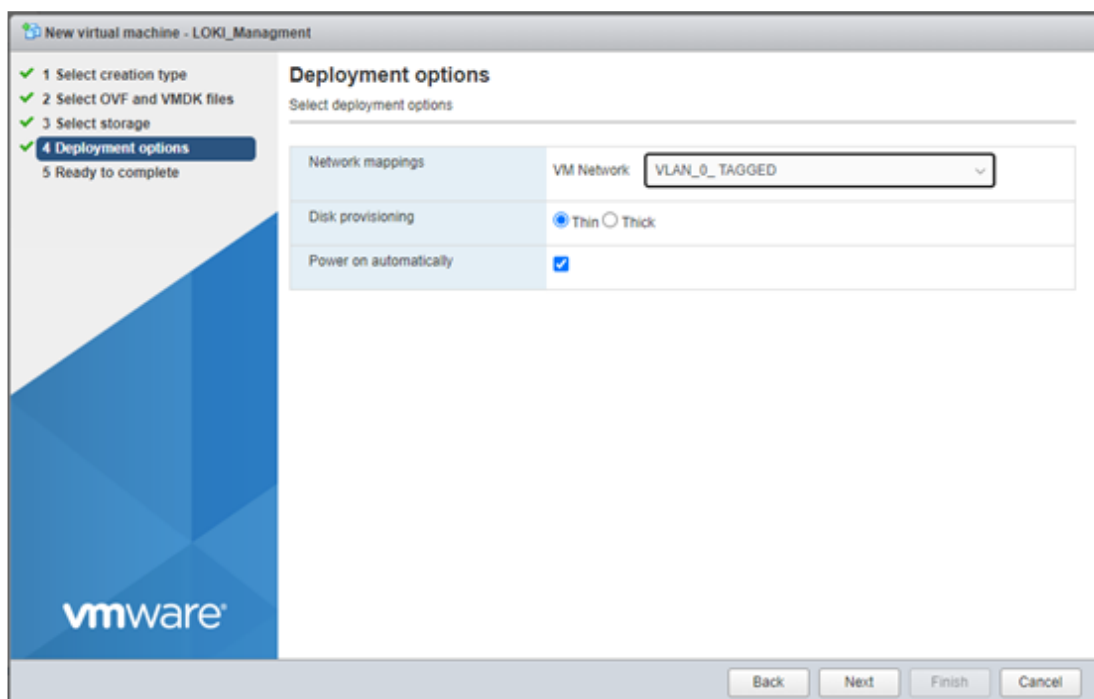


**Рисунок 6. Выбор настроек установки**

Далее в пункте 5 «**Ready to complete**» необходимо выполнить перепроверку настроек импорта и развертывания, если все корректно, то нажать кнопку «**Finish**» (Рисунок 7).

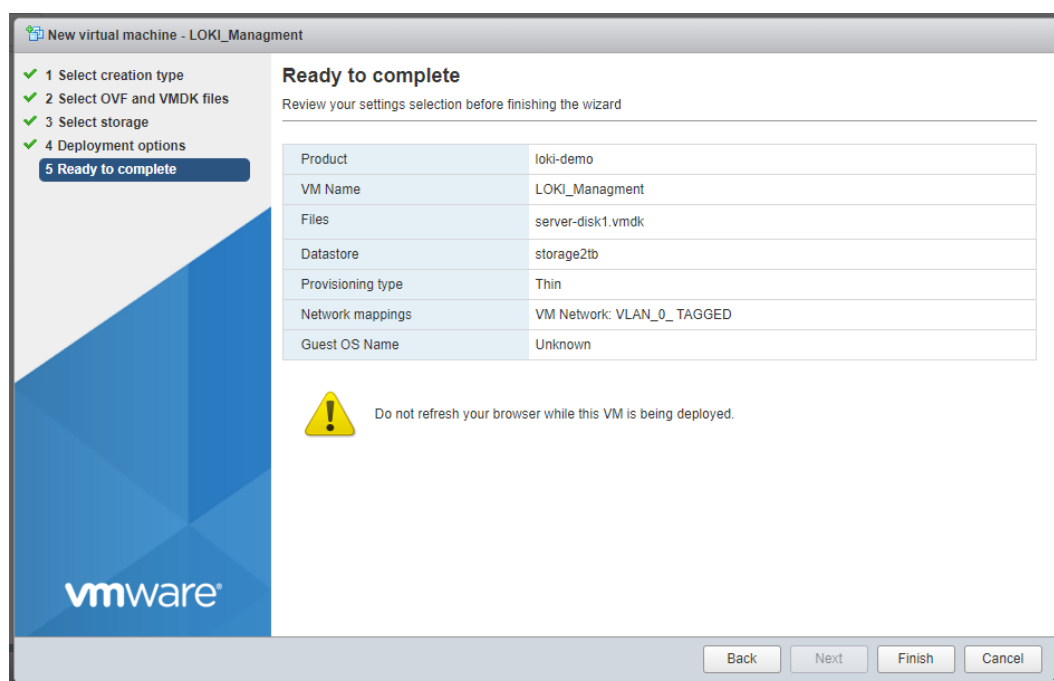


**Рисунок 7. Перепроверка настроек установки и ее запуск**

После завершения импорта в таблице заданий «**Recent tasks**» в столбце «**Result**» статус следующих заданий должен быть «Completed successfully»:

- Upload disk (Загрузка диска)
- Create VM (Создание виртуальной машины)

- Import VApp (Импорт образов)
- Power On VM (Запуск на виртуальной машине)

Далее необходимо создать виртуальную машину для развертывания образа дистрибутива сенсора, который будет осуществлять сканирование сети. Для этого нужно перейти в раздел «**Virtual Machines**», нажать «**Create / Register VM**», в пункте 1 «**Select creation type**» выбрать «**Deploy a virtual machine from an OVF or OVA file**», далее нажать кнопку «**Next**» (Рисунок 8).

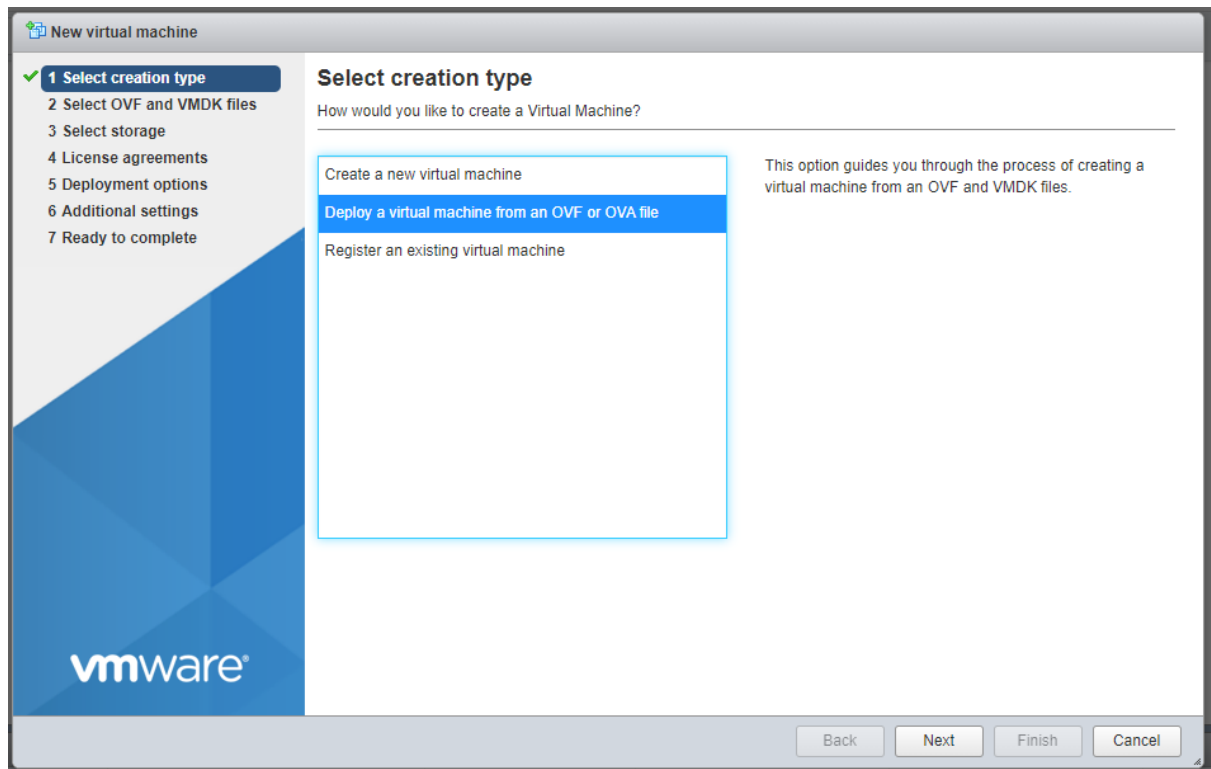


**Рисунок 8. Выбор типа файла для развертывания**

Далее необходимо в пункте 2 «**Select OVF and VMDK files**» присвоить имя виртуальной машине и выбрать файл для загрузки (Рисунок 9).

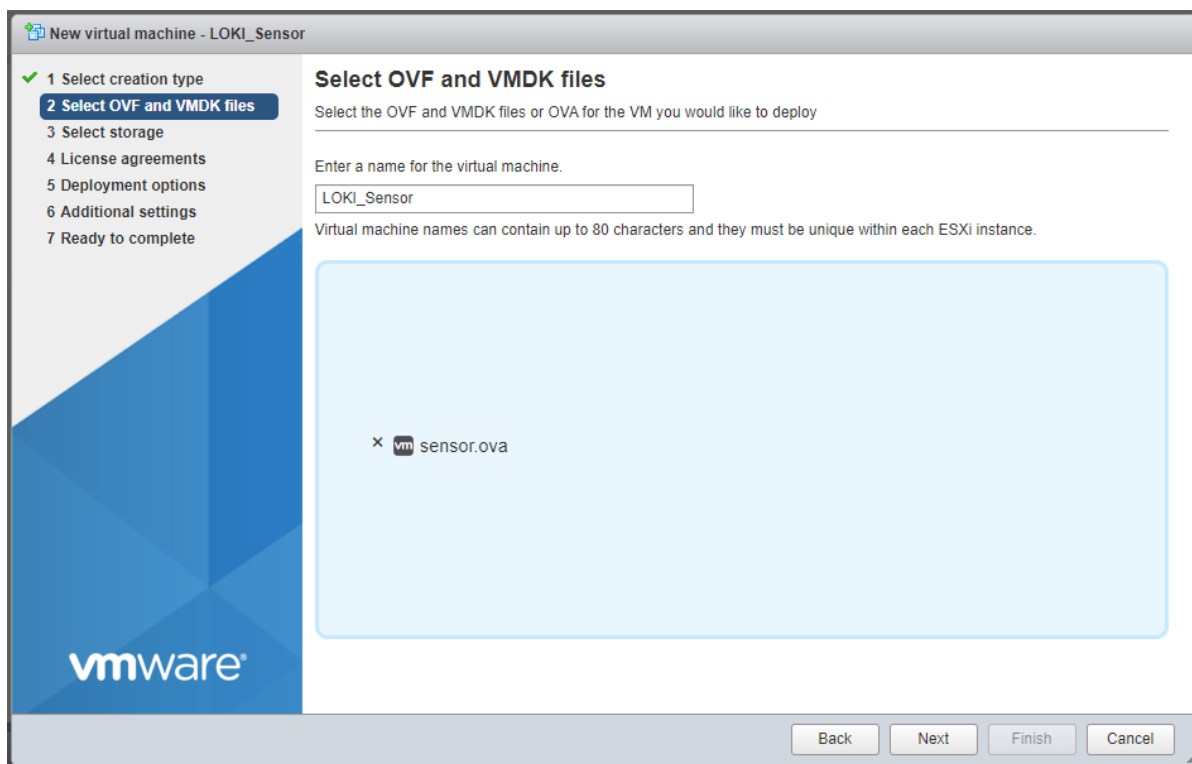


Рисунок 9. Импорт файла в виртуальную машину

Далее в пункте 3 «**Select storage**» необходимо выбрать хранилище, в котором будет размещен образ и нажать кнопку «**Next**» (Рисунок 10).

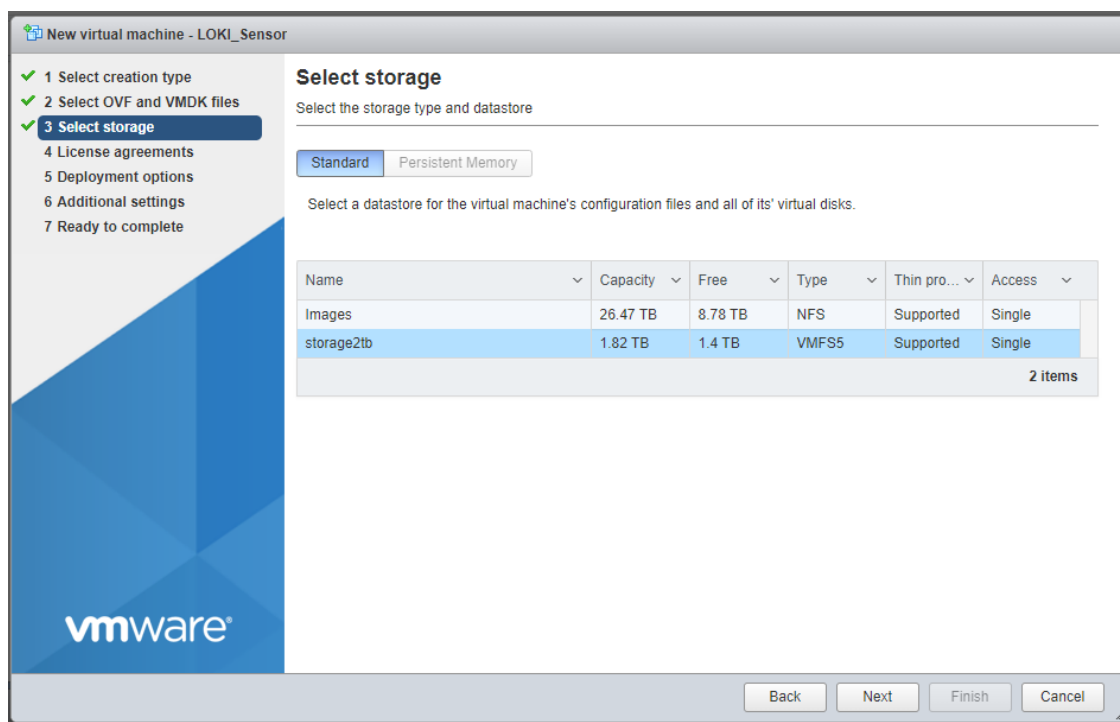


Рисунок 10. Выбор хранилища для размещения образа

Далее в пункте 4 «**Deployment options**» необходимо выбрать VLAN (один для сервиса менеджмента и один для ловушек), способ размещения на диске (по умолчанию рекомендуется «тонкий») и автоматический способ запуска и нажать кнопку «**Next**» (Рисунок 11).

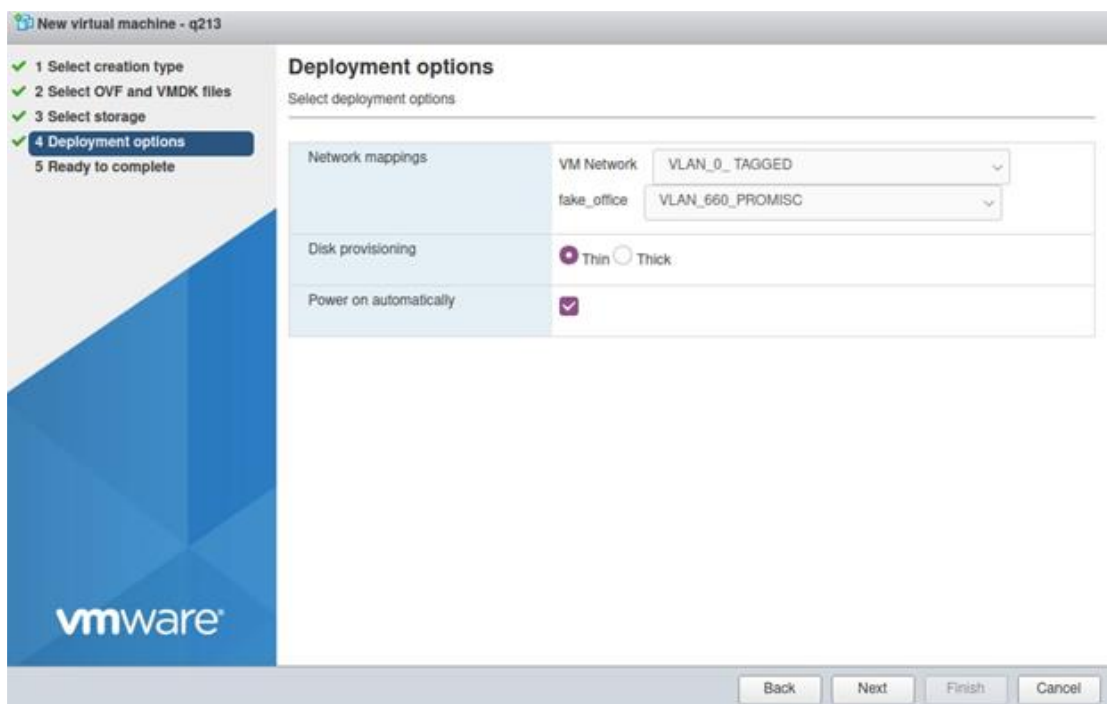


**Рисунок 11. Выбор настроек установки**

Далее в пункте 5 «**Ready to complete**» необходимо выполнить перепроверку настроек импорта и развертывания, если все корректно, то нажать кнопку «**Finish**» (Рисунок 12).

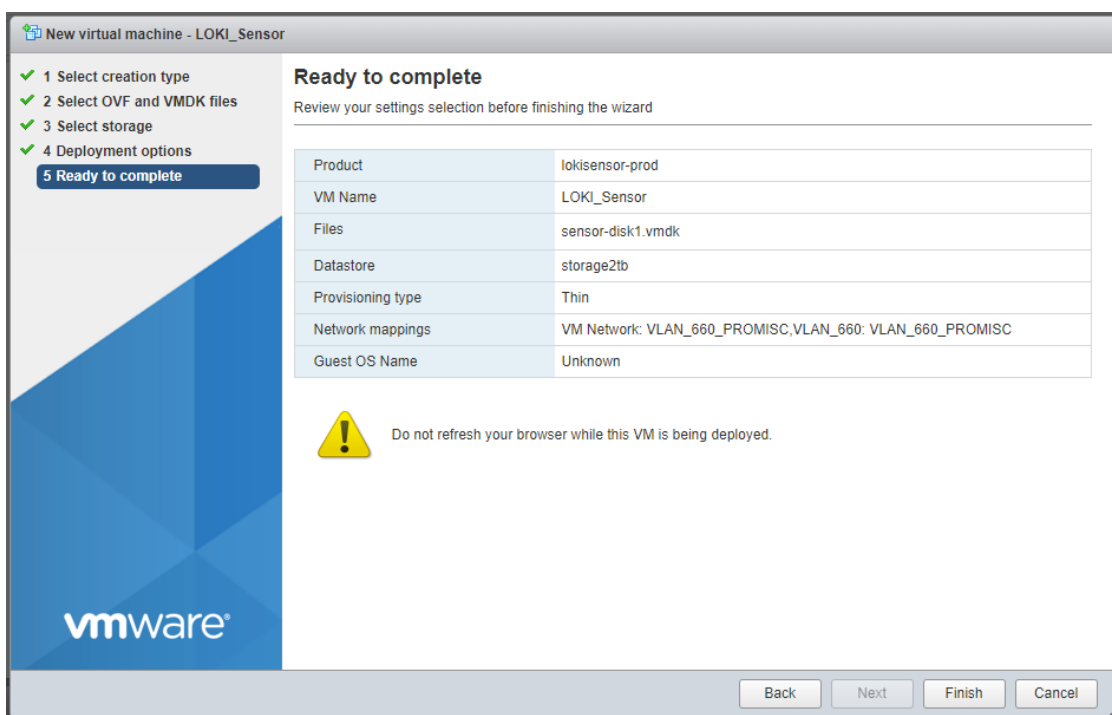


**Рисунок 12. Перепроверка настроек установки и ее запуск**

После завершения импорта в таблице заданий «**Recent tasks**» в столбце «**Result**» статус следующих заданий должен быть «Completed successfully»:

- Upload disk (Загрузка диска)

- Create VM (Создание виртуальной машины)
- Import VApp (Импорт образов)
- Power on VM (Запуск на виртуальной машине)

### 3.2 Настройка сервиса менеджмента

После успешного импортирования необходимо осуществить настройку сервера. Для этого необходимо перейти в консоль терминала (Рисунок 13).

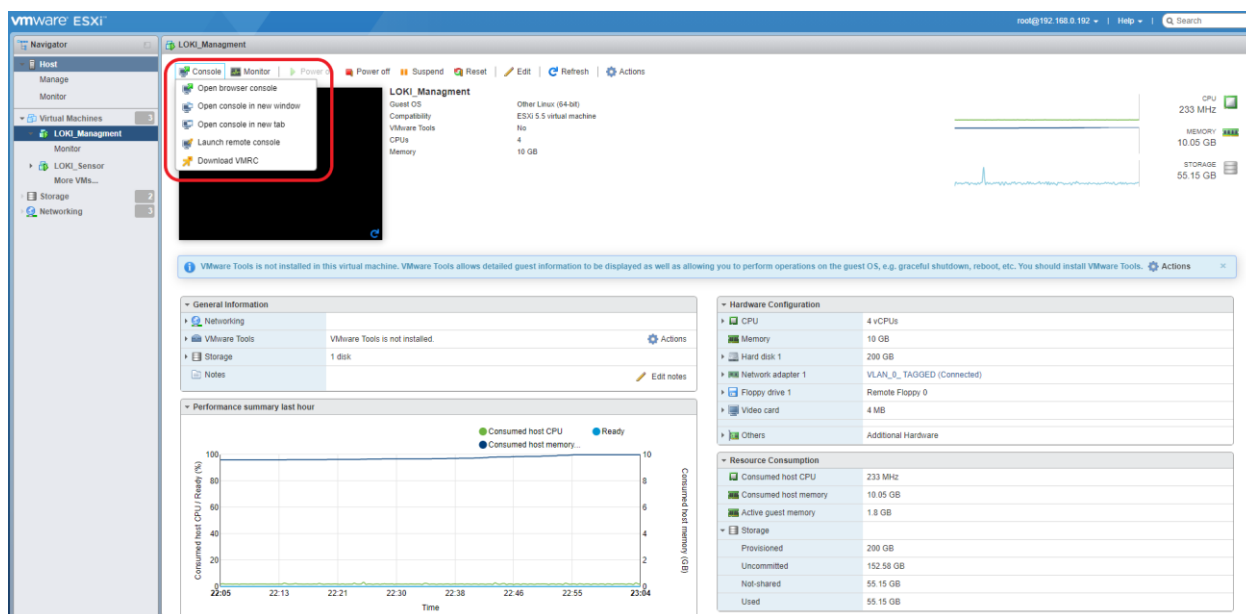


Рисунок 13. Переход в консоль терминала для настройки сервиса менеджмента

Далее необходимо авторизоваться под пользователем `avsoft_shell`, пароль от которого будет выдан вендором, после чего выполнить настройку сетевых интерфейсов. Выполнение команд описаны в таблице 7

Таблица 7. Команды настройки сетевых интерфейсов

| №  | Команда                                                                                                                                                                                 | Описание                                        | Использование                                                                                               |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| 1. | <code>&gt;&gt;&gt; interface info</code>                                                                                                                                                | отображает список доступных сетевых интерфейсов |                                                                                                             |
| 2. | <code>&gt;&gt;&gt; interface edit<br/>&lt;name&gt; static --ip<br/>&lt;ip&gt; --nm &lt;nm&gt; --gw<br/>&lt;gw&gt; --force&lt;force&gt;<br/>--ignore-errors &lt;ignore-errors&gt;</code> | задание статического адреса интерфейсу          | name(str) – название сетевого интерфейса<br>ip(str) – IP-адрес<br>nm(str) – сетевая маска<br>gw(str) – шлюз |

| №  | Команда                              | Описание                                       | Использование                                                                                                                                             |
|----|--------------------------------------|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                                      |                                                | force(bool)=false –<br>игнорирование<br>текущего состояния<br>сетевого интерфейса<br><br>- ignore-<br>errors(bool)=false –<br>игнорирование<br>исключений |
| 3. | >>> interface edit<br><name> dynamic | задание динамического адреса (dhcp) интерфейсу |                                                                                                                                                           |

При уведомлении в терминале о наличии конфигураций для недоступных интерфейсов - данные интерфейсы нужно удалить, чтобы применить настройки конфигурации текущих интерфейсов.

Дополнительные команды для настройки сети и команды, доступные в рамках терминала avsoft\_shell - описаны в документации ABCОФТ\_SHELL.

### 3.3 Настройка сенсора

После успешного импортирования необходимо осуществить настройку сенсора. Для этого необходимо перейти в консоль терминала (Рисунок 14).

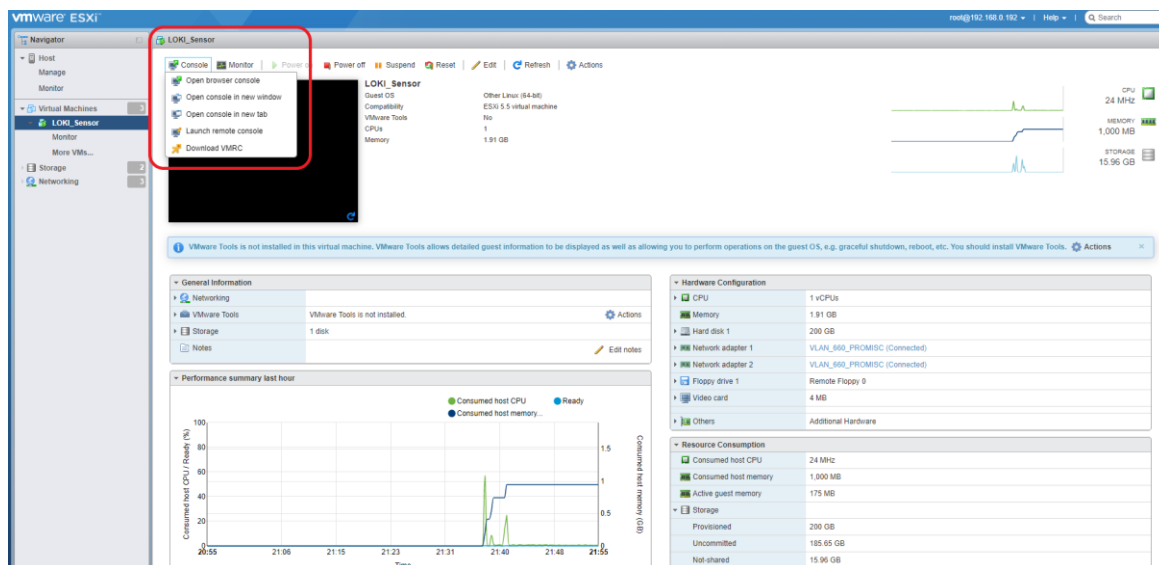


Рисунок 14. Переход в консоль терминала для настройки сенсора

Далее необходимо авторизоваться под пользователем avsoft\_shell, пароль от которого будет выдан вендором, после чего выполнить настройку

сетевых интерфейсов (повторить действия, описанные в разделе 3.2).

Зачастую это интерфейсы ens32 и ens34: ens32 используется для доступа к сенсору со стороны сервера менеджмента, ens34 - наблюдаемая сенсором подсеть с ловушками.

## 4 Описание разворачивания на Microsoft Hyper-V

Предоставляются два vhd образа диска, которых создается по отдельной виртуальной машине:

- loki-server.vhd
- loki-sensor.vhd

### 4.1 loki-server

В панели меню Диспетчера Hyper-V необходимо выбрать «Действие» → «Создать» → «Виртуальная машина» (Рисунок 15).

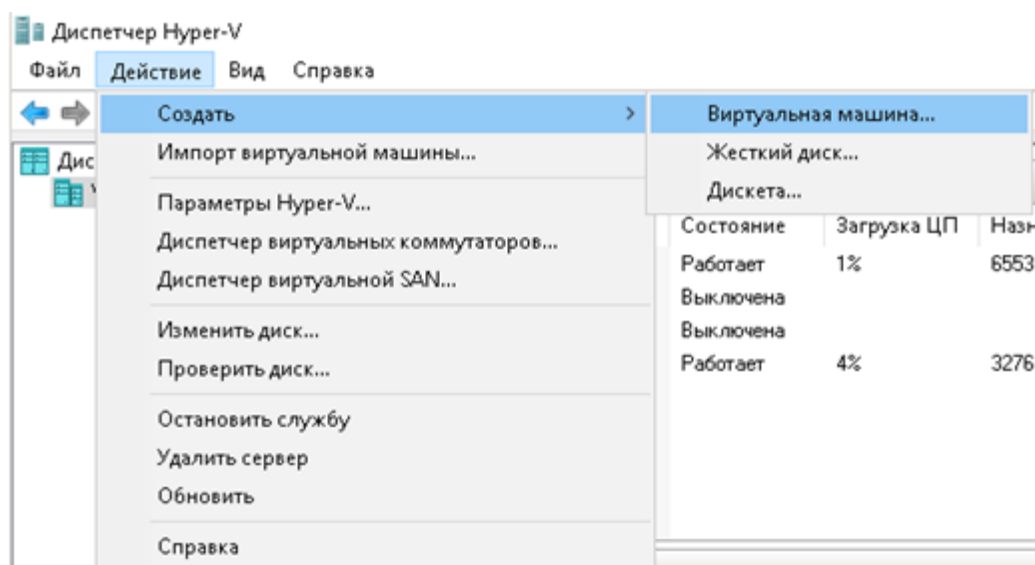


Рисунок 15. Создание виртуальной машины

Далее открывается «Мастер создания виртуальной машины», в котором необходимо нажать кнопку «Далее» (Рисунок 16).

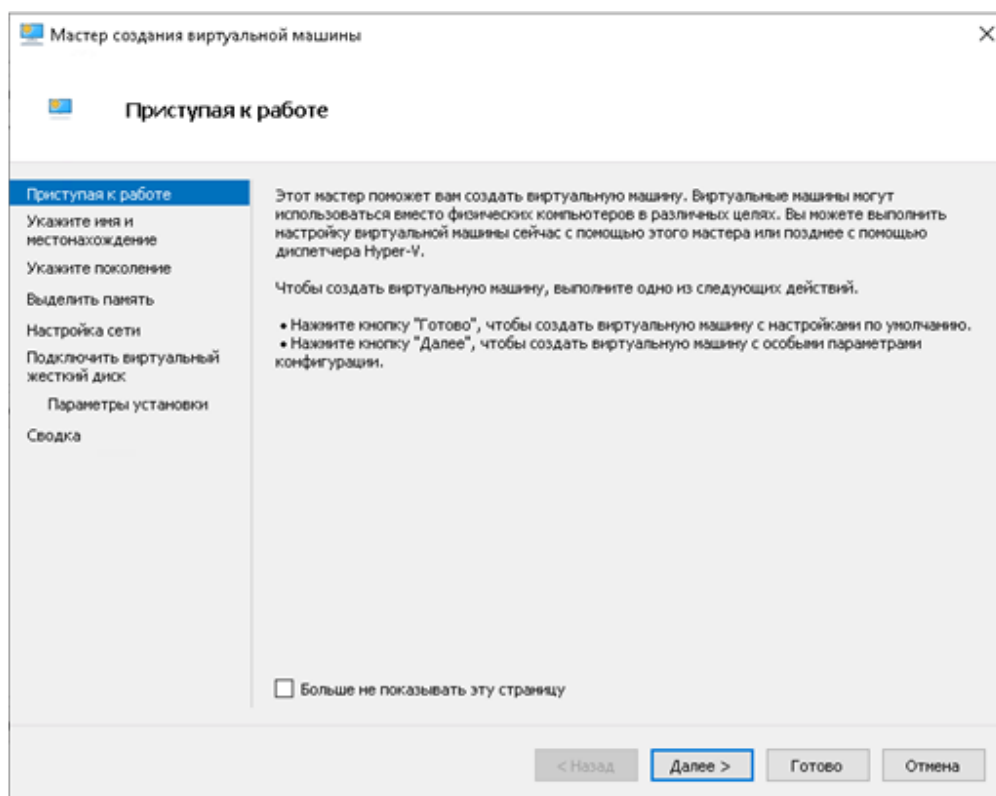


**Рисунок 16. Мастер создания виртуальных машин**

Затем необходимо задать виртуальной машине имя loki-server, расположить ее необходимо на диске с не менее чем 400 ГБ свободного пространства (Рисунок 17).

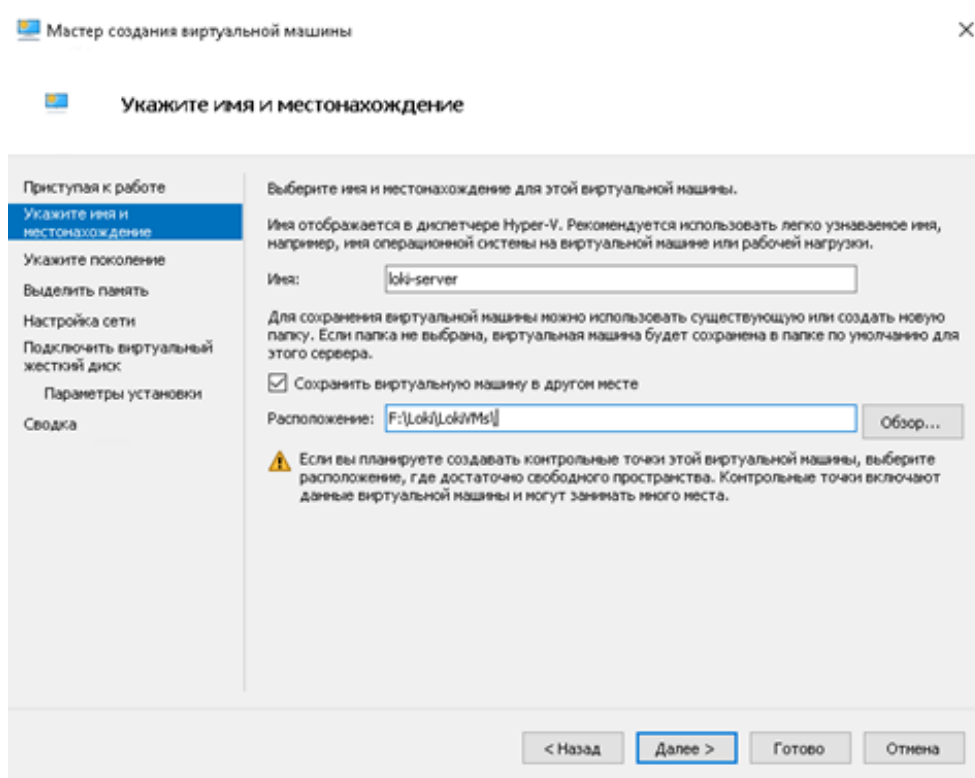


**Рисунок 17. Указание имени и местонахождения**

Далее необходимо выбрать «**Поколение 1 виртуальных машин**» (Рисунок 18).

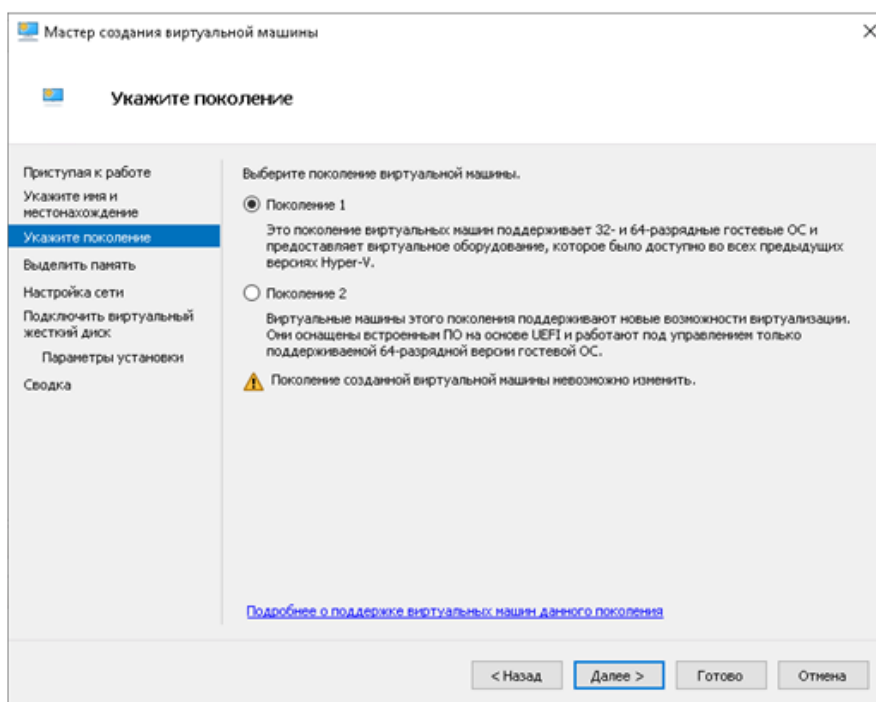


**Рисунок 18. Выбор поколения виртуальных машин**

Далее необходимо задать размер оперативной памяти виртуальной машины, минимальное рекомендуемое значение для работы – 8 ГБ (Рисунок 19).

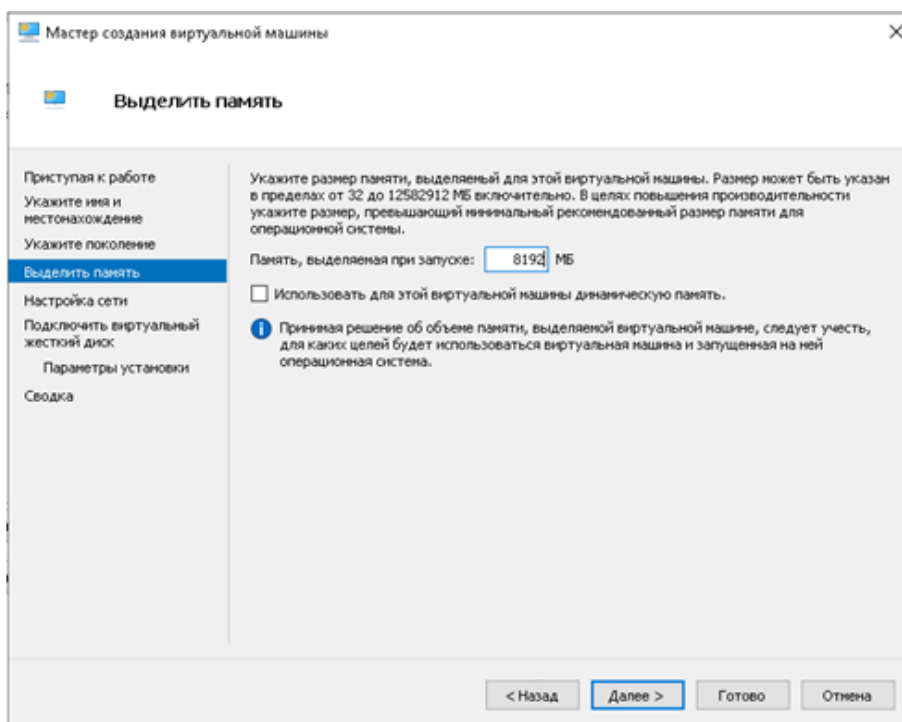


**Рисунок 19. Выделение памяти**

Для работы сети необходимо указать доступный виртуальный

коммутатор, если таковых не имеется, то его необходимо создать (Рисунок 20).

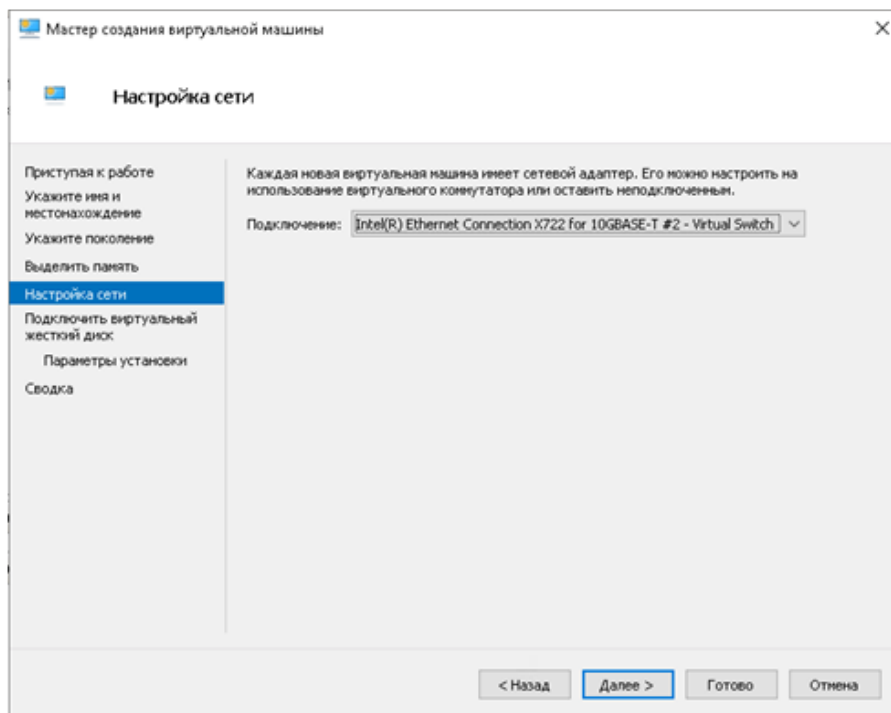


Рисунок 20. Настройка сети

В качестве виртуального хранилища подключаем образ диска дистрибутива Loki Server — **loki-server.vhd** (Рисунок 21).

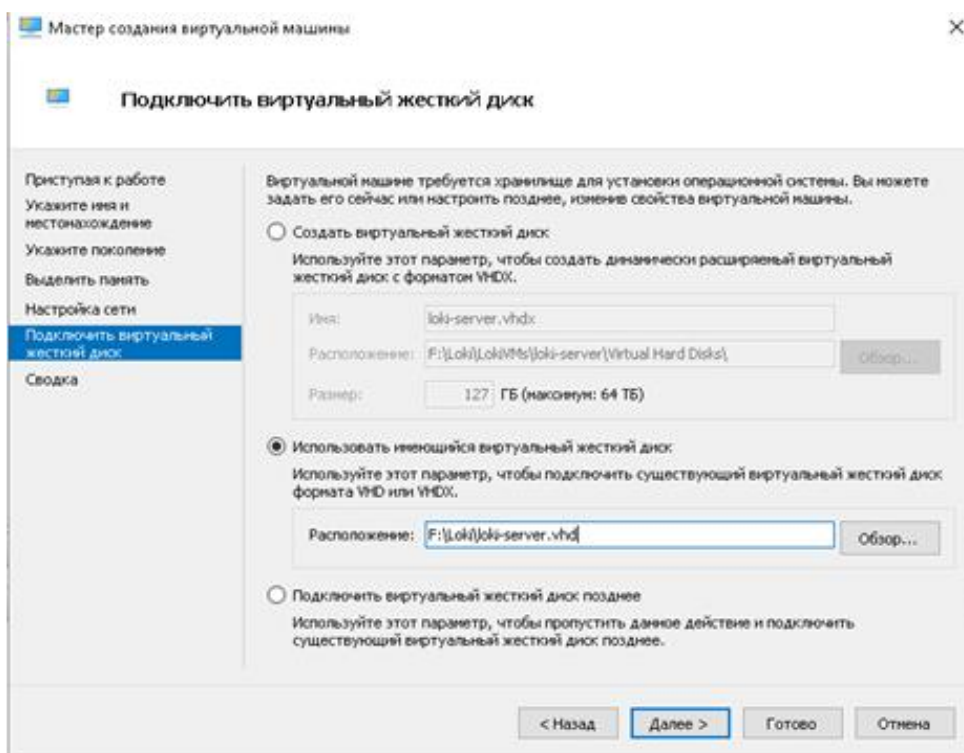


Рисунок 21. Подключение образа диска

Далее необходимо удостовериться в корректности указанных ранее данных и в соответствии с ними создать виртуальную машину **loki-server**

нажатием кнопки «Готово» (Рисунок 22).

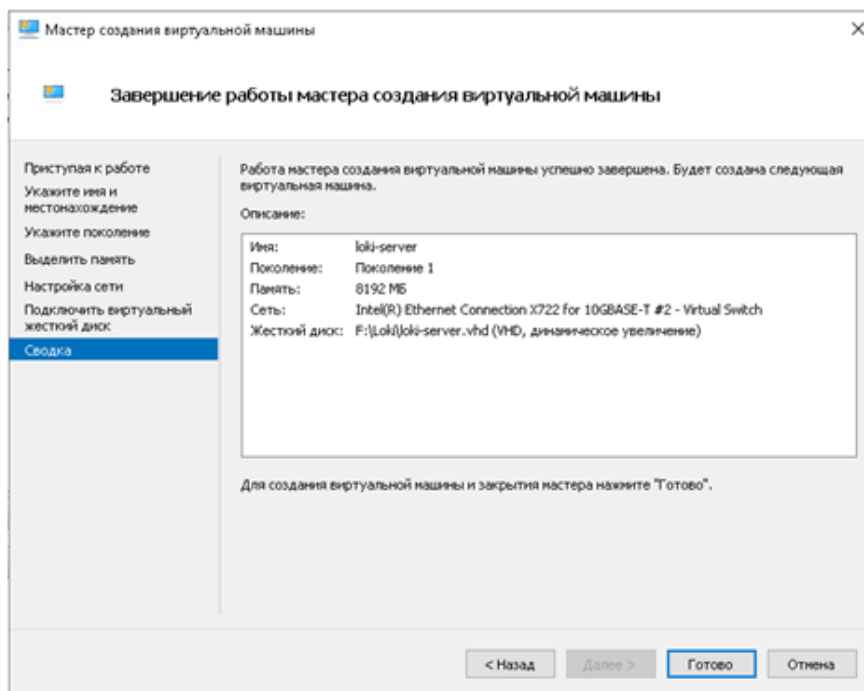


**Рисунок 22. Завершение создания виртуальной машины**

После создания машины необходимо нажать правой кнопкой мыши по ней в списке и зайти в меню «**Параметры**» (Рисунок 23).

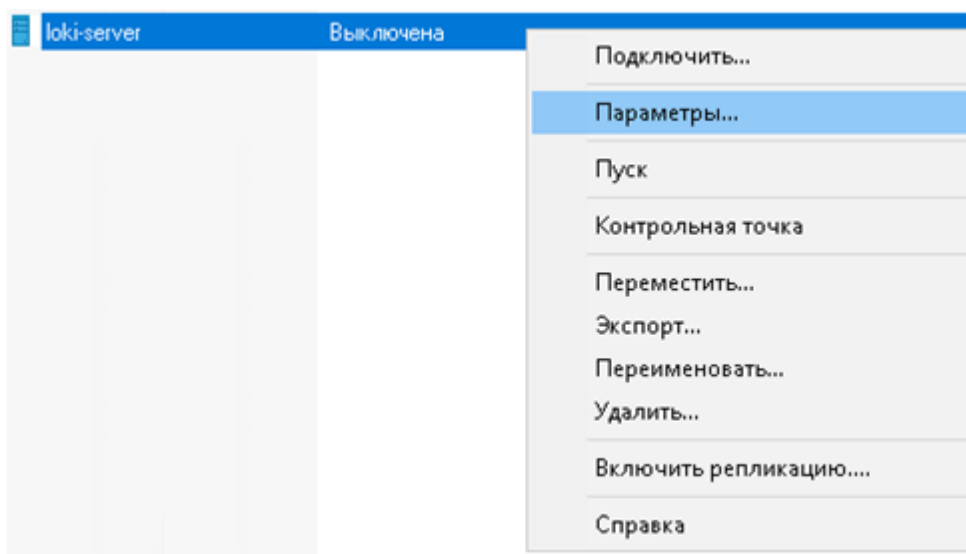


**Рисунок 23. Параметры виртуальной машины**

В параметрах необходимо выбрать пункт «**Процессор**» и задать число виртуальных процессоров машине, минимальное значение для работы — 4 виртуальных процессора, далее нажать кнопку «**ОК**» (Рисунок 24).

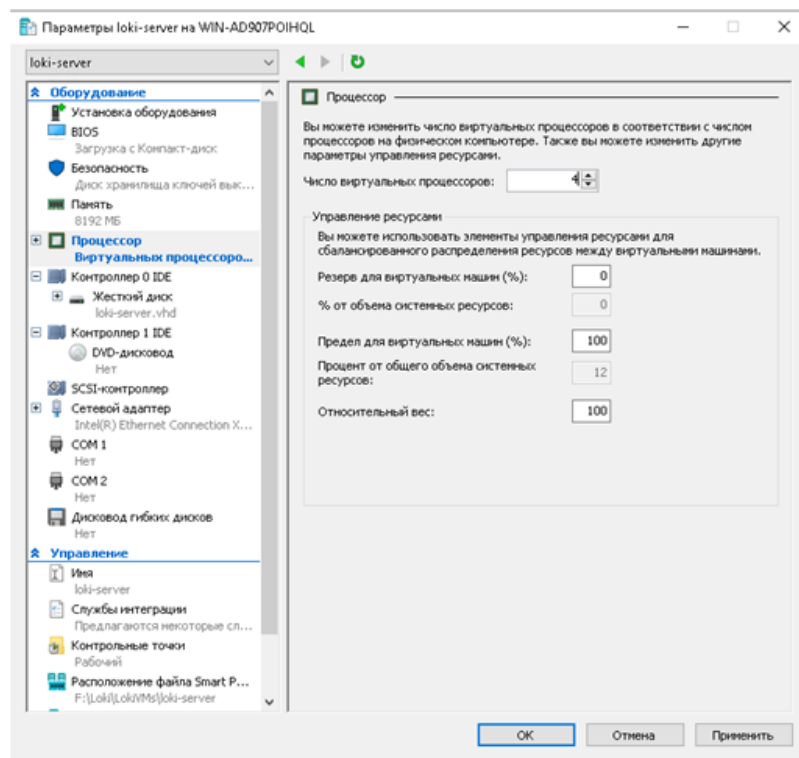


Рисунок 24. Процессор виртуальной машины

## 4.2 loki-sensor

Для настройки **loki-sensors** необходимо повторить создание виртуальной машины из инструкции **loki-server** выше. Задать новой виртуальной машине имя **loki-sensor**, расположить ее необходимо на том же диске с не менее чем 400 ГБ свободного пространства, как в инструкции loki-server выше (Рисунок 25).

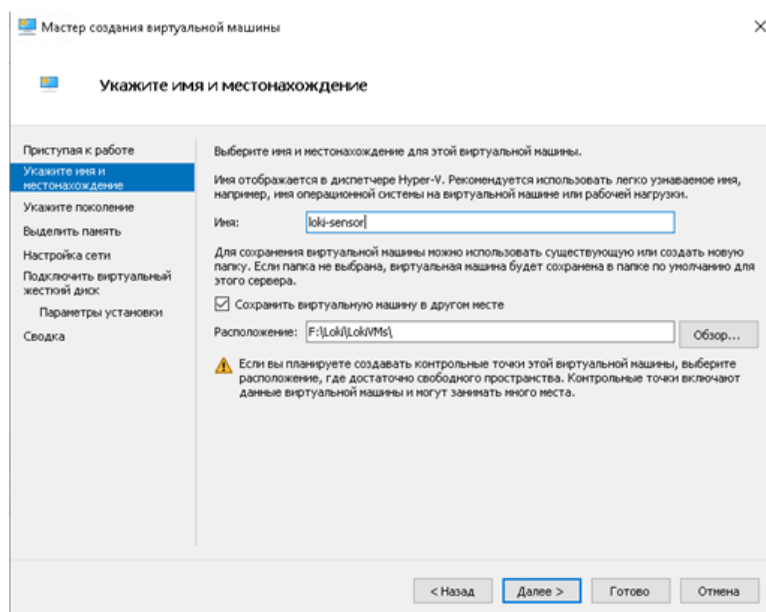


Рисунок 25. Указание имени и местонахождения

Выбрать «**Поколение 1 виртуальной машины**» (Рисунок 26).

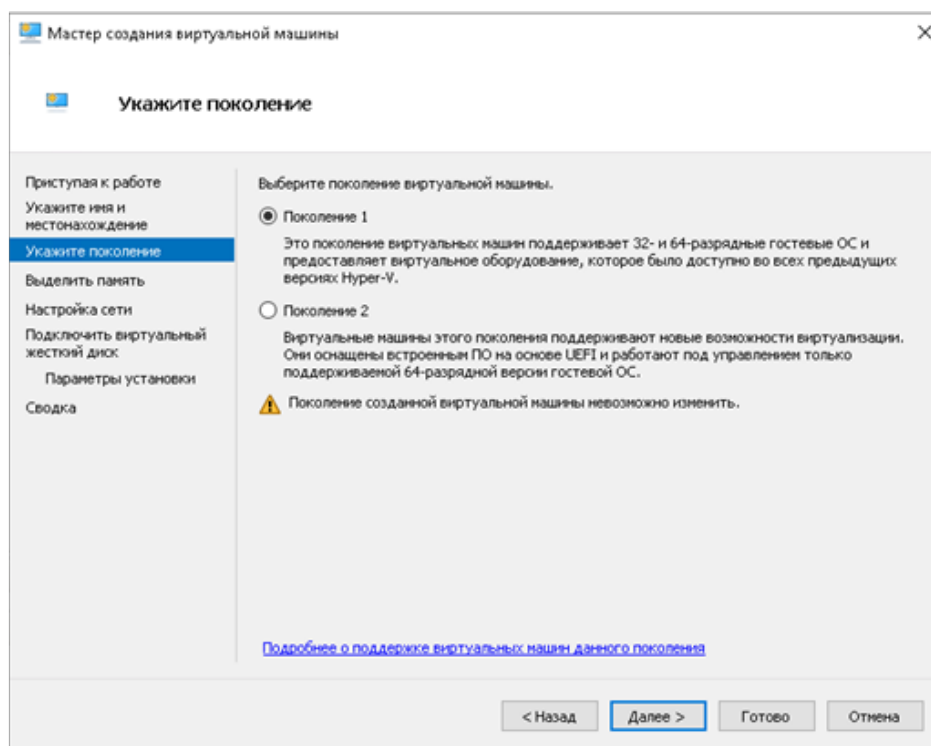


**Рисунок 26. Выбор поколения виртуальной машины**

Затем необходимо задать размер оперативной памяти виртуальной машины, минимальное значение для работы — 2 ГБ (Рисунок 27).

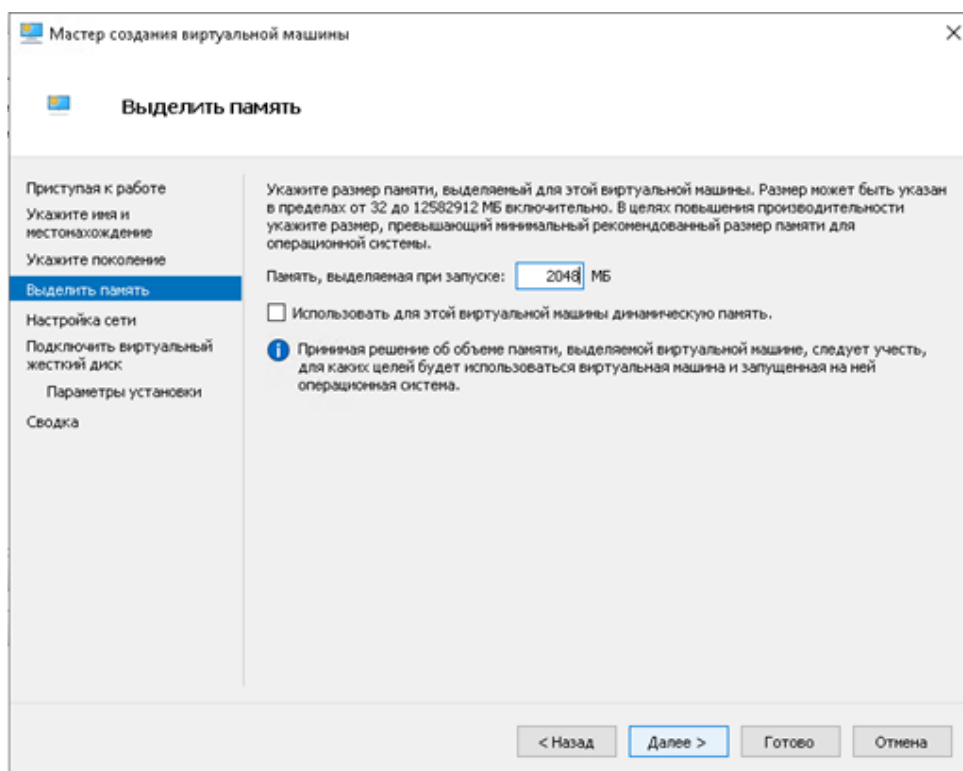


**Рисунок 27. Указание памяти виртуальной машине**

Для работы сети необходимо указать доступный виртуальный коммутатор, заданный ранее при создании виртуальной машины **loki-server** (Рисунок 28).

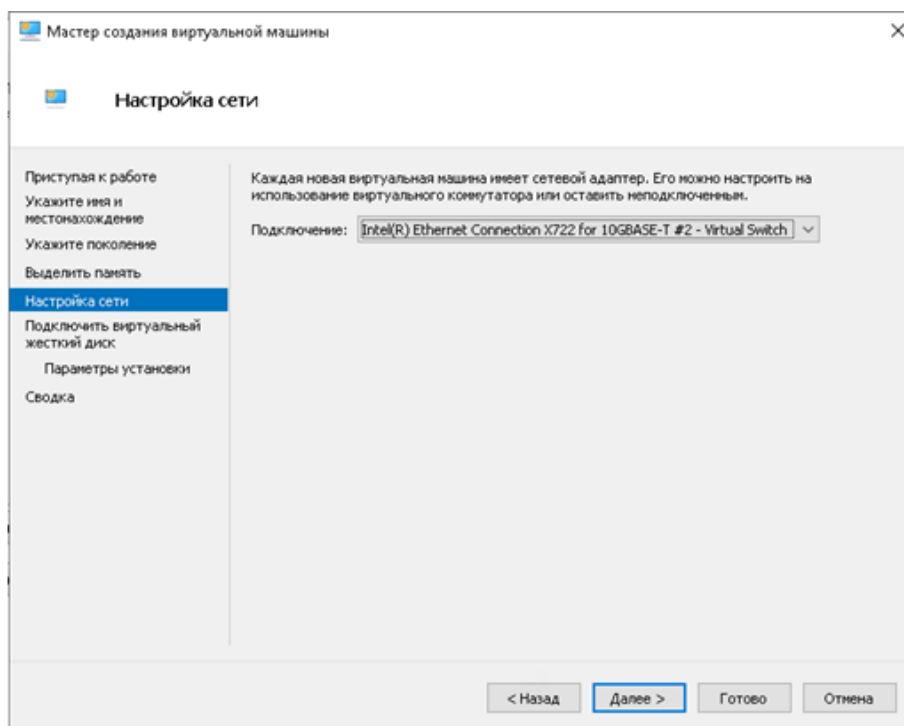


Рисунок 28. Настройка сети

В качестве виртуального хранилища подключается образ диска дистрибутива Loki Sensor — **loki-sensor.vhd** (Рисунок 29).

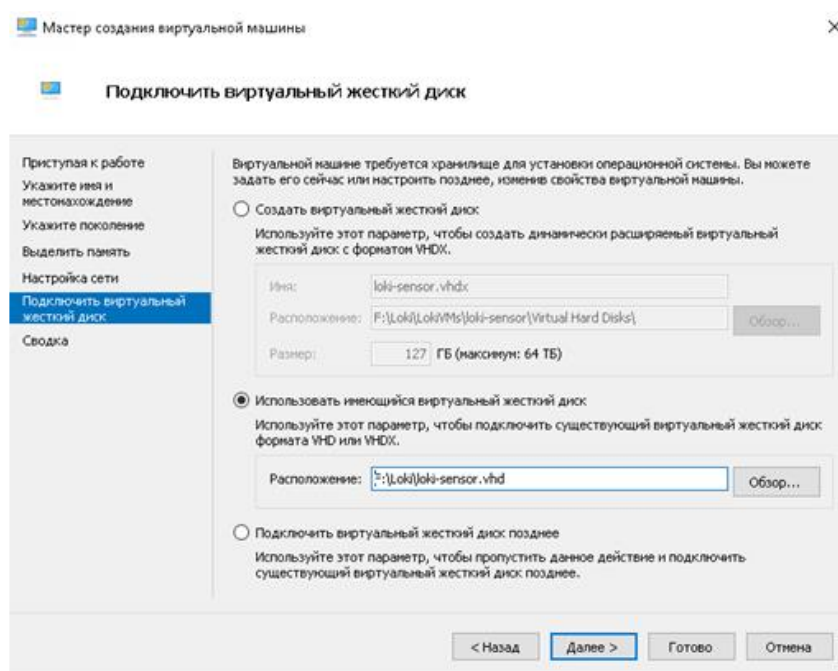


Рисунок 29. Подключение образа диска

Необходимо удостовериться в корректности указанных ранее данных и в соответствии с ними создать виртуальную машину **loki-sensor** нажатием кнопки «Готово» (Рисунок 30).

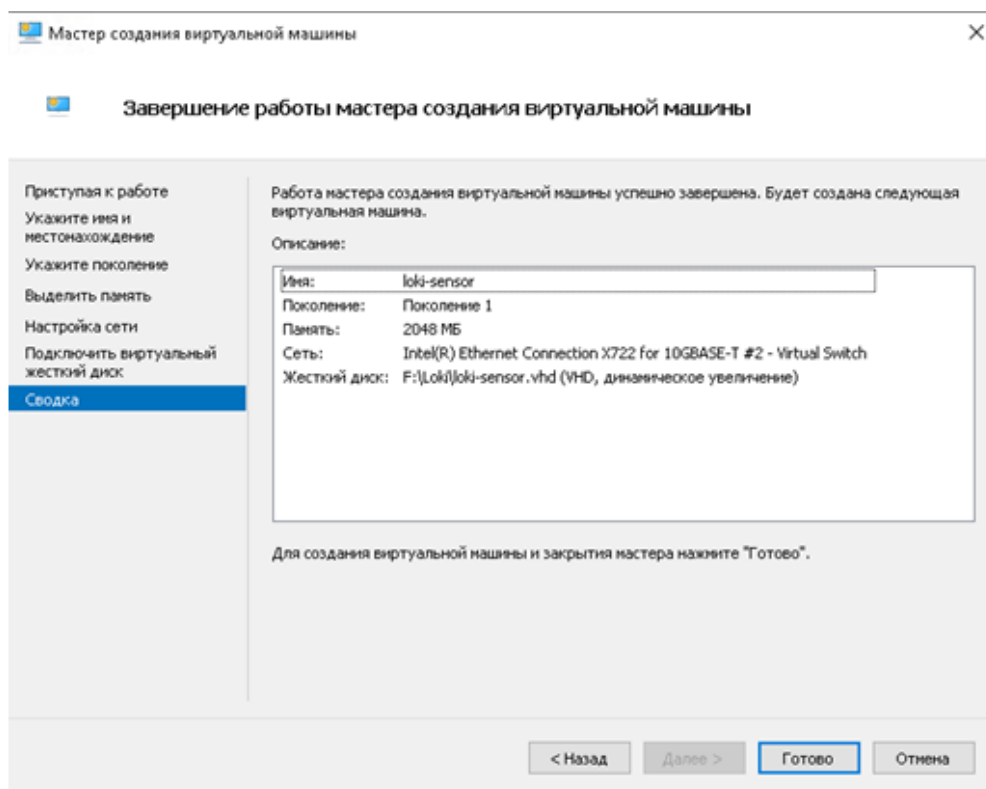


**Рисунок 30. Завершение создания виртуальной машины**

После создания машины необходимо нажать правой кнопкой мыши по ней в списке и зайти в меню «**Параметры**» (Рисунок 31).

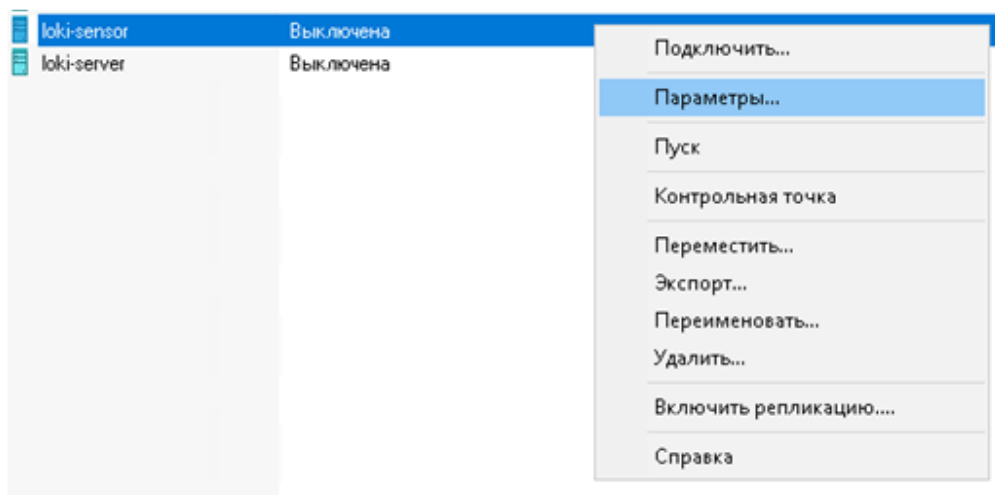


**Рисунок 31. Параметры виртуальной машины**

В параметрах необходимо выбрать пункт «**Процессор**» и задать число виртуальных процессоров машине, минимальное значение для работы — 2 виртуальных процессора, далее нажать кнопку «**ОК**» (Рисунок 32).

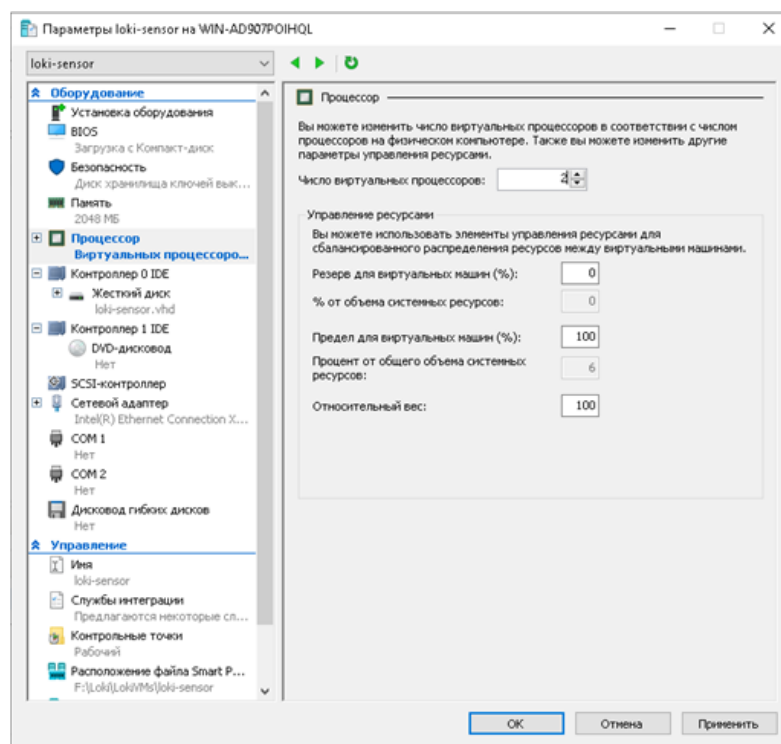


Рисунок 32. Процессор виртуальной машины

## 5 Настройки в веб-интерфейсе

Далее необходимо перейти в веб-интерфейс и выполнить авторизацию в нем, логин и пароль выдается вендором (Рисунок 33).

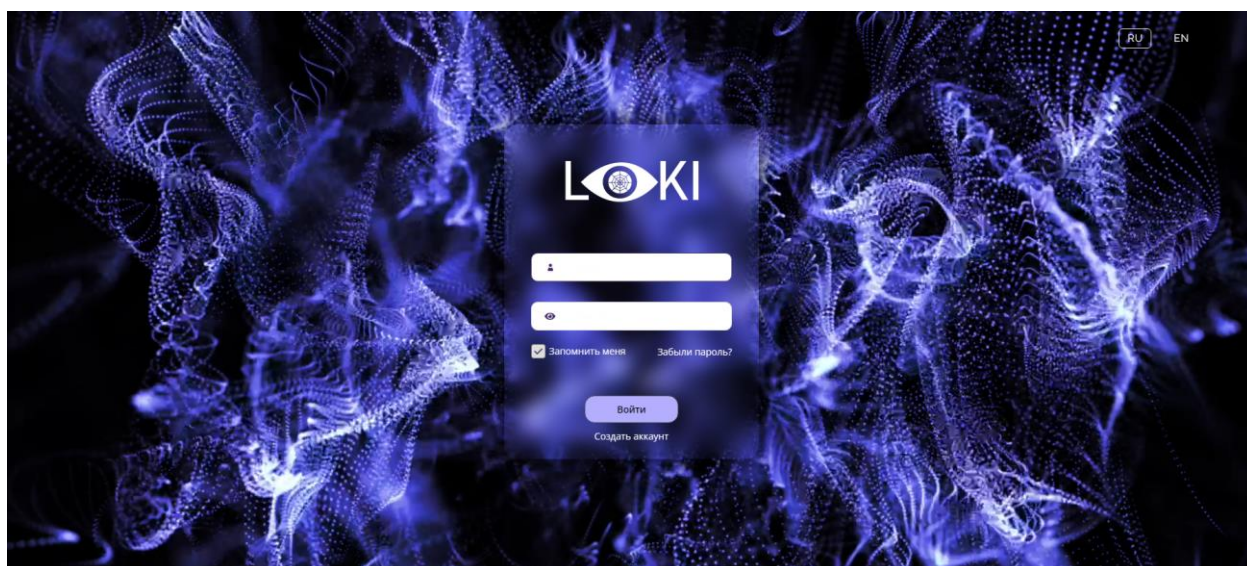


Рисунок 33. Авторизация в веб-интерфейсе

### 5.1 Добавление сенсора

Далее необходимо перейти в раздел «**Инфраструктура**» во вкладку «**Сенсоры**» и нажать на иконку «**Добавить**» (Рисунок 34).

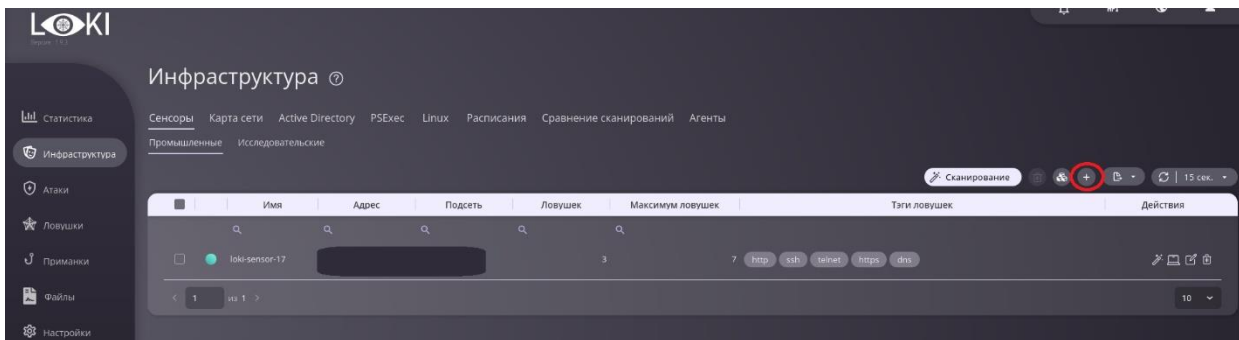


**Рисунок 34. Добавление сенсора для сканирования инфраструктуры**

Далее необходимо заполнить поля в окне «Сенсор» и по окончании ввода данных нажать кнопку «Сохранить» (Рисунок 35).

**Рисунок 35. Добавление сенсора в систему**

Рекомендации по заполнению полей формы представлены в таблице 8.

**Таблица 8. Рекомендации по заполнению полей в форме добавления сенсора**

| <b>№</b> | <b>Наименование поля</b> | <b>Рекомендации по заполнению</b>                                              |
|----------|--------------------------|--------------------------------------------------------------------------------|
| 1.       | Имя                      | Произвольное                                                                   |
| 2.       | Адрес                    | Доменное имя или IP адрес для SSH подключения                                  |
| 3.       | Интерфейс                | Интерфейс, к которому подключена наблюдаемая сеть (чаще всего ens34 или ens35) |
| 4.       | Адрес шлюза              | Адрес, через который будет происходить маршрутизация в наблюдаемой подсети.    |
| 5.       | Подсеть                  | Маска наблюдаемой подсети                                                      |
| 6.       | SSH порт                 | Порт для SSH подключения                                                       |
| 7.       | Логин                    | Имя пользователя для SSH сессии                                                |
| 8.       | Пароль                   | Пароль пользователя для SSH сессии                                             |