Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

ПРИНЯТО

на заседании педагогического совета
Протокол № 2
«26» 12 2023 г.

УТВЕРЖДАЮ

Директор СПб ГБПОУ «АУГСГиП»
_____ А.М. Кривоносов
«26» 12 2023 г.

КОМПЛЕКТ КОНТРОЛЬНО-ОЦЕНОЧНЫХ СРЕДСТВ

по текущему контролю успеваемости
и промежуточной аттестации
по профессиональному модулю
ПМ.05 ЭКСПЛУАТАЦИЯ ОБЛАЧНЫХ СЕРВИСОВ

по специальности
09.02.06 Сетевое и системное администрирование

Квалификация
Системный администратор

Форма обучения
очная

Санкт-Петербург
2023 год

Комплект контрольно-оценочных средств по профессиональному модулю ПМ.05 Эксплуатация облачных сервисов разработан на основе Федерального государственного образовательного стандарта по специальности 09.02.06 Сетевое и системное администрирование, утвержденного приказом Министерства Просвещения РФ от 10 июля 2023 г. № 519.

СОГЛАСОВАНО
ООО «ДЖИ-ТИ ИНВЕСТ»
Генеральный директор
_____ П.С. Тюганов
«26» ____12____ 2023 г.

Комплект контрольно-оценочных средств по профессиональному модулю рассмотрен на заседании методического совета СПб ГБПОУ «АУГСГиП»

Протокол №2 от «29» ____11____ 2023 г.

Комплект контрольно-оценочных средств по профессиональному модулю рассмотрен на заседании цикловой комиссии общетехнических дисциплин и компьютерных технологий

Протокол № 4 от «21» ____11____ 2023 г.

Председатель цикловой комиссии: Караченцева М.С. _____

СОДЕРЖАНИЕ

1. Паспорт комплекта оценочных средств

Результатом освоения профессионального модуля является готовность обучающегося к выполнению вида профессиональной деятельности «Сопровождение модернизации сетевой инфраструктуры» и составляющих его профессиональных компетенций, а также общих компетенций, формирующихся в процессе освоения ППССЗ в целом.

Комплект контрольно-оценочных средств позволяет оценивать:

1. Освоение профессиональных компетенций (ПК), соответствующих виду профессиональной деятельности, и общих компетенций (ОК):

№ ПК и ОК	Содержание компетенции
ПК 5.1	Осуществлять развертывание облачной инфраструктуры
ПК 5.2	Проводить документирование требований и технических возможностей облачных инфраструктур
ПК 5.3	Проводить настройку виртуальных машин с использованием механизмов автоматического масштабирования и распределения нагрузки.
ПК 5.4	Производить хранение и анализ данных.
ПК 5.5	Обеспечивать информационную безопасность в облачной инфраструктуре с помощью различных инструментов.
ПК 5.6	Проводить мониторинг системы в облачных сервисах
ОК 1.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;
ОК 2.	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;
ОК 4.	Эффективно взаимодействовать и работать в коллективе и команде;
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;
ОК 9.	Пользоваться профессиональной документацией на государственном и иностранном языках.

2. Приобретение в ходе освоения профессионального модуля практического опыта:

Освоение практического опыта

Иметь практический опыт	Виды работ на учебной и/ или производственной практике и требования к их выполнению
– В развертывании облачной инфраструктуры; – Настройке балансировщиков нагрузки и проведения тестирования жизнеспособности облачных сервисов; – Реализации концепции декларативного управления инфраструктурой; – Организации документирования технических требований к облачным инфраструктурам; – Создания и поддержки планов автоматического масштабирования; – Создания образов виртуальных машин; – Управления образами виртуальных машин; – Организации распределения нагрузки внутри облачно инфраструктуры; – Организации хранения данных в облачной инфраструктуре; – проведения анализа данных; – Обеспечения безопасности в облачной инфраструктуре; – Организации функции управления учетными записями и доступом к облачной инфраструктуре; – Настройки службы защиты сетей от внешних атак; – Маркировки ресурсов для последующего мониторинга и оценки стоимости; – Сбора метрик и формирования журнала мониторинга; – Внедрения и осуществления мониторинга облачных сервисов;	1. Развертывание облачной инфраструктуры; 2. Настройке балансировщиков нагрузки и проведения тестирования жизнеспособности облачных сервисов; 3. Реализации концепции декларативного управления инфраструктурой; 4. Организации документирования технических требований к облачным инфраструктурам 5. Создания и поддержки планов автоматического масштабирования 6. Создание образов виртуальных машин; 7. Управление образами виртуальных машин 8. Организация распределения нагрузки внутри облачно инфраструктуры 9. Организация хранения данных в облачной инфраструктуре; 10. Проведение анализа данных; 11. Управление учетными записями и доступом к облачной инфраструктуре 12. Настройка службы защиты сетей от внешних атак 13. Маркировка ресурсов для последующего мониторинга и оценки стоимости; 14. Сбор метрик и формирования журнала мониторинга 15. Внедрение осуществление мониторинга облачных сервисов 16. Обеспечение безопасности в облачной инфраструктуре

3. Освоение умений и усвоение знаний:

№	Освоенные умения, усвоенные знания
З1	Различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами;
З2	Разграничение ответственности за безопасность между поставщиком облачных услуг и клиентом публичного облака;
З3	Показатели системы, сети и приложений, а также их влияние на надежность, доступность и производительность инфраструктуры;
З4	Требования к совместимости компонентов внутри облачной инфраструктуры;

№	Освоенные умения, усвоенные знания
З5	Сетевой поток данных и соответствующая зависимость доступности систем;
З6	Методы работы с заинтересованными сторонами бизнеса для решения задач, связанных с соответствием регламентирующим документам;
З7	Разграничение ответственности за безопасность между поставщиком облачных услуг и клиентом публичного облака;
З8	Различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками;
З9	Как взаимодействовать с бизнес-единицами для определения лучших практик развертывания и создания плана по миграции в облачную инфраструктуру;
З10	Важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений;
З11	Различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами;
З12	Основные потребности инфраструктурного дизайна для отдельных групп инженеров;
З13	Различные технологические решения для достижения бизнес-целей;
З14	Сетевой поток данных и соответствующая зависимость доступности систем;
З15	Требования к производительности и возможные узкие места при проектировании инфраструктуры;
З16	Важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений;
З17	Различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами;
З18	Показатели системы, сети и приложений, а также их влияние на надежность, доступность и производительность инфраструктуры;
З19	Методики и возможности автоматизации, широко используемые в техническом сообществе;
З20	Методы работы с заинтересованными сторонами бизнеса для решения задач, связанных с соответствием регламентирующим документам;
З21	Важность каждого уровня инфраструктуры, включая вычисление, хранение, сетевое взаимодействие, базы данных, использование кэша и приложений;
З22	Требования к совместимости компонентов внутри облачной инфраструктуры;
З23	Методики и возможности автоматизации, широко используемые в техническом сообществе;
З24	Сетевой поток данных и соответствующая зависимость доступности систем;
З25	Требования к производительности и возможные узкие места при проектировании инфраструктуры;
З26	Различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами;
З27	Важность и назначение сетевого траффика, а также изоляцию ресурсов;

№	Освоенные умения, усвоенные знания
З28	Различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками;
З29	Сетевой поток данных и соответствующая зависимость доступности систем;
З30	Как метрики приложения, системы и сети могут быть использованы для определения реализации доступных, масштабируемых и гибких архитектур;
З31	Требования к производительности и возможные узкие места при проектировании инфраструктуры
З32	Различные сетевые архитектуры для оптимального взаимодействия с существующими/доступными приложениями и средами;
З33	Разграничение ответственности за безопасность между поставщиком облачных услуг и клиентом публичного облака;
З34	Показатели системы, сети и приложений, а также их влияние на надежность, доступность и производительность инфраструктуры;
З35	Требования к совместимости компонентов внутри облачной инфраструктуры;
З36	Сетевой поток данных и соответствующая зависимость доступности систем;
З37	Методы работы с заинтересованными сторонами бизнеса для решения задач, связанных с соответствием регламентирующим документам;
З38	Разграничение ответственности за безопасность между поставщиком облачных услуг и клиентом публичного облака;
З39	Различные варианты производительности инфраструктуры, доступные благодаря таким решениям, как кэширование, правильный размер ресурсов и сервисы, предоставляемые поставщиками;
З40	Сетевой поток данных и соответствующая зависимость доступности систем;
З41	Как метрики приложения, системы и сети могут быть использованы для определения реализации доступных, масштабируемых и гибких архитектур;
З42	Требования к производительности и возможные узкие места при проектировании инфраструктуры
У1	Определять общие модели развертывания облачной инфраструктуры;
У2	Поддерживать облачные конфигурации в актуальном состоянии и вести учет контроля версий;
У3	Определять, насколько данные модели соответствуют требованиям, специфичным для организации;
У4	Пользоваться преимуществами облачной инфраструктуры для снижения операционных нагрузок при развертывании служб;
У5	Документировать ключевые требования бизнес-приложений и то, как они соотносятся миграцией в облачную инфраструктуру;
У6	Переводить бизнес-цели и задачи в спецификации, а также презентовать их заинтересованным сторонам;
У7	Проводить оценку, выбор и внедрение передовых облачных сервисов, таких как сервисы управления данными, сервисы кэширования и сервисы автоматического масштабирования и обеспечения доступности;
У8	Создавать внутренние руководящие документы и требования к

№	Освоенные умения, усвоенные знания
	процедурам, необходимым для создания, обновления, удаления и получения доступа к инфраструктуре и ресурсам общедоступного облака;
У9	Проводить оценку, выбирать и внедрять базовые облачные сервисы, таких как вычислительная среда, сеть и хранилище;
У10	Разрабатывать и внедрять процессы проверки подлинности на уровне подразделения и компании в целом, контролировать доступ к системе управления общедоступным облаком;
У11	Анализировать и интерпретировать показатели производительности вычислений, хранения данных, уровня сети и приложений для использования в дизайне общедоступной облачной инфраструктуре;
У12	Использовать методы и пакеты настройки производительности для обеспечения оптимального использования ресурсов;
У13	Реализовать стратегию микросервисов для получения выгоды от технологических достижений в таких областях, как технологии контейнеров;
У14	Внедрять базы данных и решения для хранения данных, которые наилучшим образом соответствуют потребностям конкретного приложения;
У15	Разрабатывать и внедрять процессы проверки подлинности на уровне подразделения и компании в целом, контролировать доступ к системе управления общедоступным облаком;
У16	Использовать общедоступные облачные службы и функции для поддержки разработки и внедрения решений в соответствии с требованиями доступности, надежности и масштабируемости;
У17	Проводить постоянные проверки отказоустойчивости и восстановления системы;
У18	Внедрение решений для мониторинга с целью формирования предупреждений и автоматизации реагирования на различные инциденты;
У19	Поддерживать облачные конфигурации в актуальном состоянии и вести учет контроля версий;
У20	Внедрять централизованный сбор и анализ метрик для системной, сетевой и прикладной информации
У21	Проводить постоянные проверки отказоустойчивости и восстановления системы;.

Формой аттестации по профессиональному модулю является экзамен. Итогом экзамена является однозначное решение: «вид профессиональной деятельности освоен/не освоен».

2. Система контроля и оценки освоения программы ПМ.05 Эксплуатация облачных сервисов

2.1. Формы промежуточной аттестации по ППССЗ при освоении профессионального модуля

Элементы модуля, профессиональный модуль	Формы промежуточной аттестации
МДК.05.01 Технологии виртуализации и автоматизации	Дифференцированный зачет
МДК.05.02 Безопасность облачных сервисов	Дифференцированный зачет
МДК.05.03Технологии хранения и анализа данных	Дифференцированный зачет
ПП	Дифференцированный зачет
ПМ	**Экзамен**

2.2. Организация контроля и оценки освоения программы ПМ

Итоговый контроль освоения вида профессиональной деятельности Эксплуатация облачных сервисов осуществляется на экзамене. Условием допуска к экзамену является положительная аттестация по МДК, учебной практике и производственной практике.

Экзамен проводится в виде выполнения практического экзаменационного задания.

Условием положительной аттестации (вид профессиональной деятельности освоен) на экзамене квалификационном является положительная оценка освоения всех профессиональных компетенций по всем контролируемым показателям. При отрицательном заключении хотя бы по одной из профессиональных компетенций принимается решение «вид профессиональной деятельности не освоен».

Промежуточный контроль освоения профессионального модуля осуществляется при проведении экзаменов по МДК, дифференцированного зачета по производственной практике. Предметом оценки освоения МДК являются умения и знания. Экзамен по МДК проводится по заранее подготовленным и утвержденным экзаменационным вопросам. Условием положительной аттестации является получение обучающимся на экзамене оценки «удовлетворительно», «хорошо», «отлично».

Предметом оценки по учебной и производственной практике является освоение общих и профессиональных компетенций, умений. Контроль и оценка по производственной практике проводится на основе Аттестационного листа обучающегося с места прохождения практики.

Текущий контроль по МДК осуществляется в форме выполнения практических проверочных заданий, устных зачетов.

3. Комплект материалов для освоения умений и усвоения знаний, оценки сформированности общих и профессиональных компетенций по виду профессиональной деятельности

3.1. Задания для оценки освоения теоретического курса профессионального модуля

3.1.1. Оценка освоения теоретического курса профессионального модуля по МДК.05.01

Дидактические единицы	Проверяемые ОК, ПК, У, З	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
Тема 1.1. Платформы виртуализации на основе кластерного подхода	ПК 5.1.- ПК 5.4. ОК1-9 З1-З17 У1-У8	Устный зачет по теме 1.1	Устные ответы на дифференцированном зачете
		Практическая работа № 2 Работа с Hypervisor: Установка и настройка нативного Hypervisor.	
		Практическая работа № 10 Работа с контейнерами Kubernetes в среде Proxmox VE	
		Практическая работа № 14 Настройка межплатформенный бесклиентский шлюз удаленного рабочего стола	

Устный зачет по теме 1.1

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 8 мини-вопросов.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Виртуализация ресурсов: compute, storage, network
2. Передача сетевого состояния, datapath, удаленного управления трафиком, виртуальный NAT. Сетевой мост
3. Кластер Proxmox VE: Узлы кластера. Отказоустойчивость. Репликация.
4. Кластеры Kubernetes в среде Proxmox VE: Мастер-ноды Kubernetes
5. Исполняемые среды контейнеров: Docker, containerd, CRI-O и Kubernetes CRI. Планирование, приоритизация и вытеснение
6. Пакетные операции в kubectl
7. Облачные бизнес-модели IaaS, PaaS и SaaS

Практическая работа № 2
Работа с Hypervisor: Установка и настройка нативного Hypervisor.

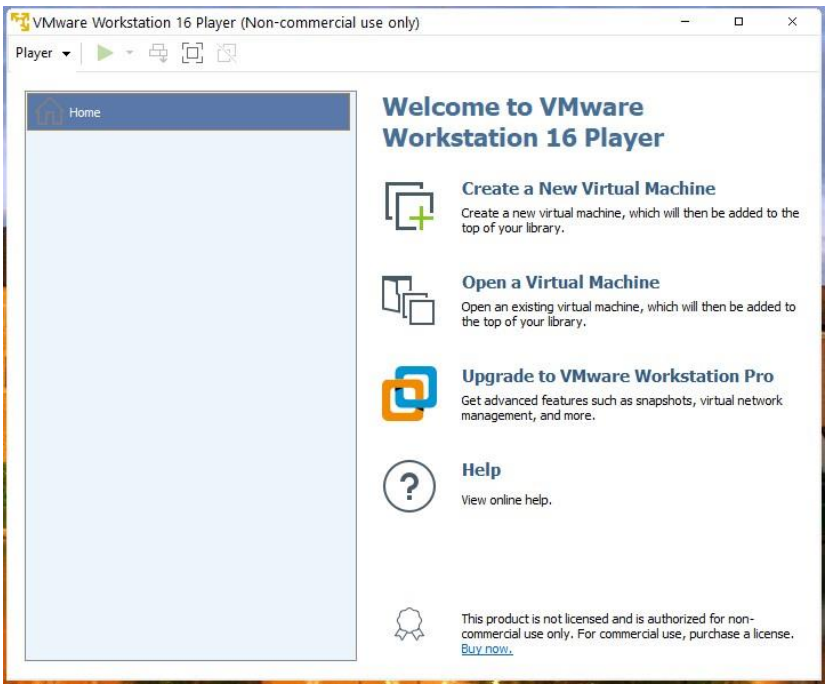
Инструкция для обучающихся

Внимательно прочитайте задание. Выполните все необходимые операции

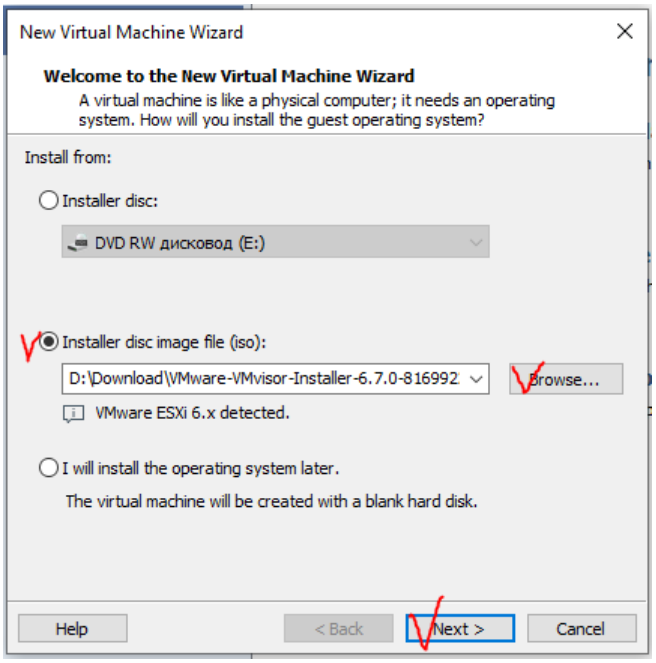
Время выполнения – 90 минут.

Задание

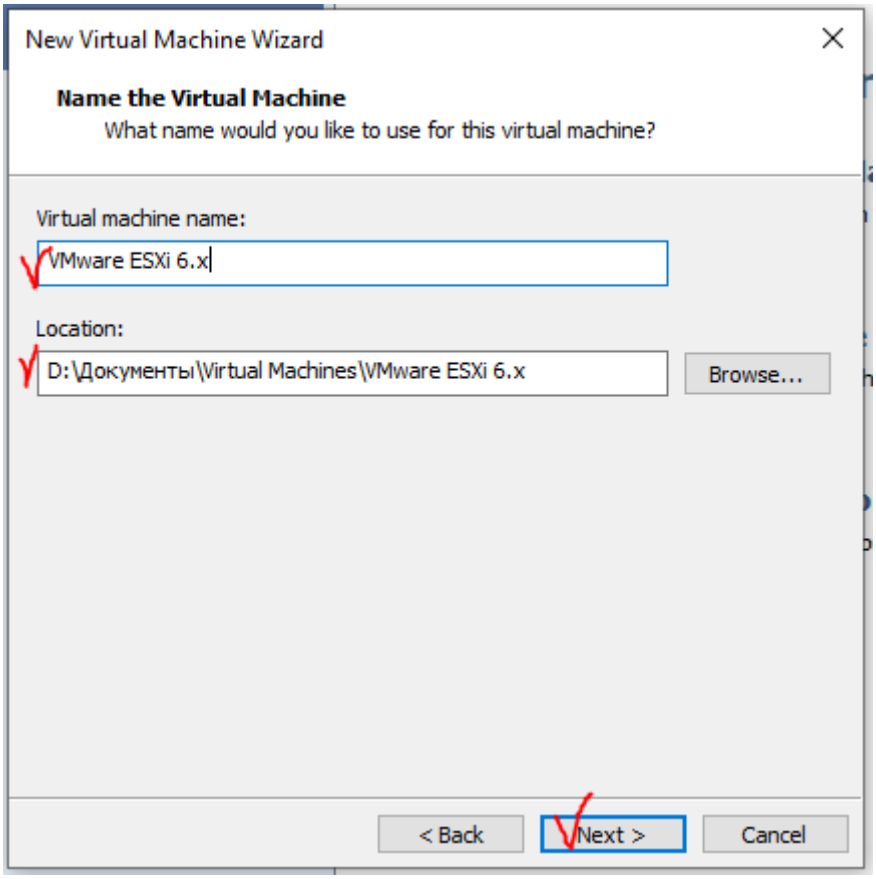
1. Установить гипервизор VMware Player 16. Скачать инсталляции можно по ссылке https://yadi.sk/d/J70iVaTwiPJJ1w



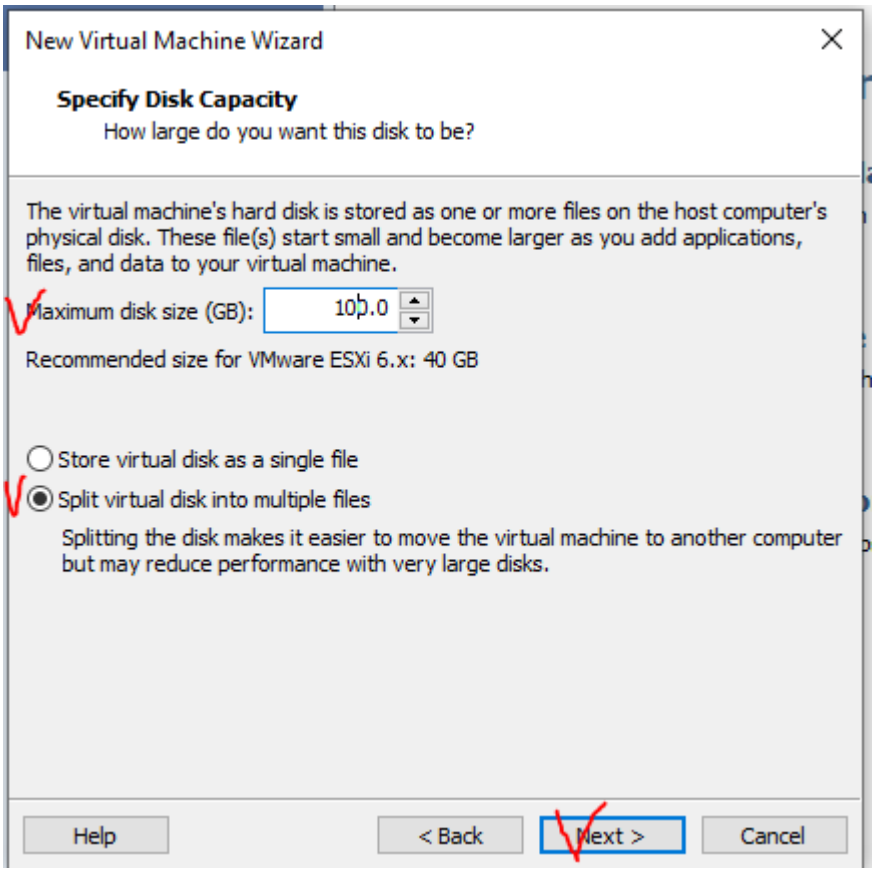
2. Установить систему виртуализации VMware ESXi 6.7. Скачать инсталляции можно по ссылке https://yadi.sk/d/1CqbT5_7m8g0pQ
    a. Выбрать пункт *Create a New Virtual Machine*
    b. Выбрать второй пункт *Installer disc image file (iso)*



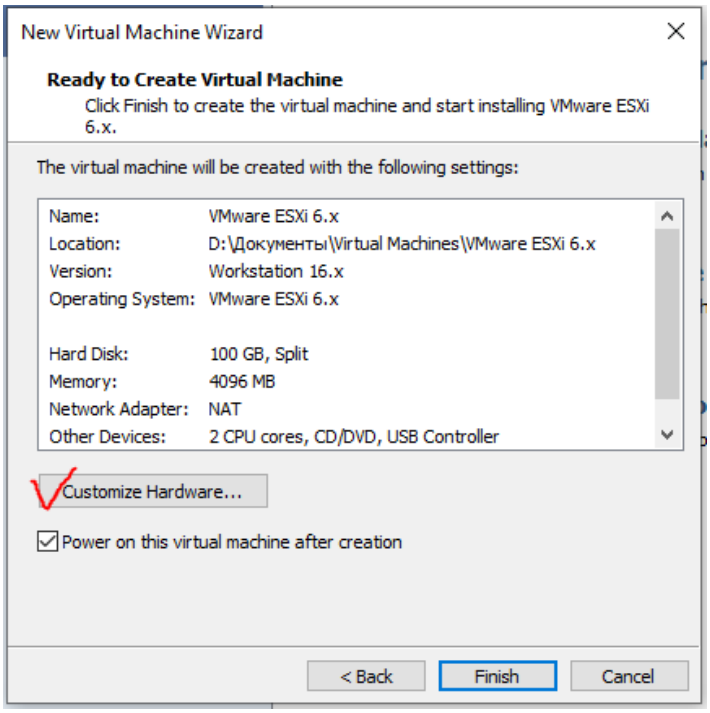
    c. Указать имя и место хранения файлов виртуальной машины или оставить по умолчанию.



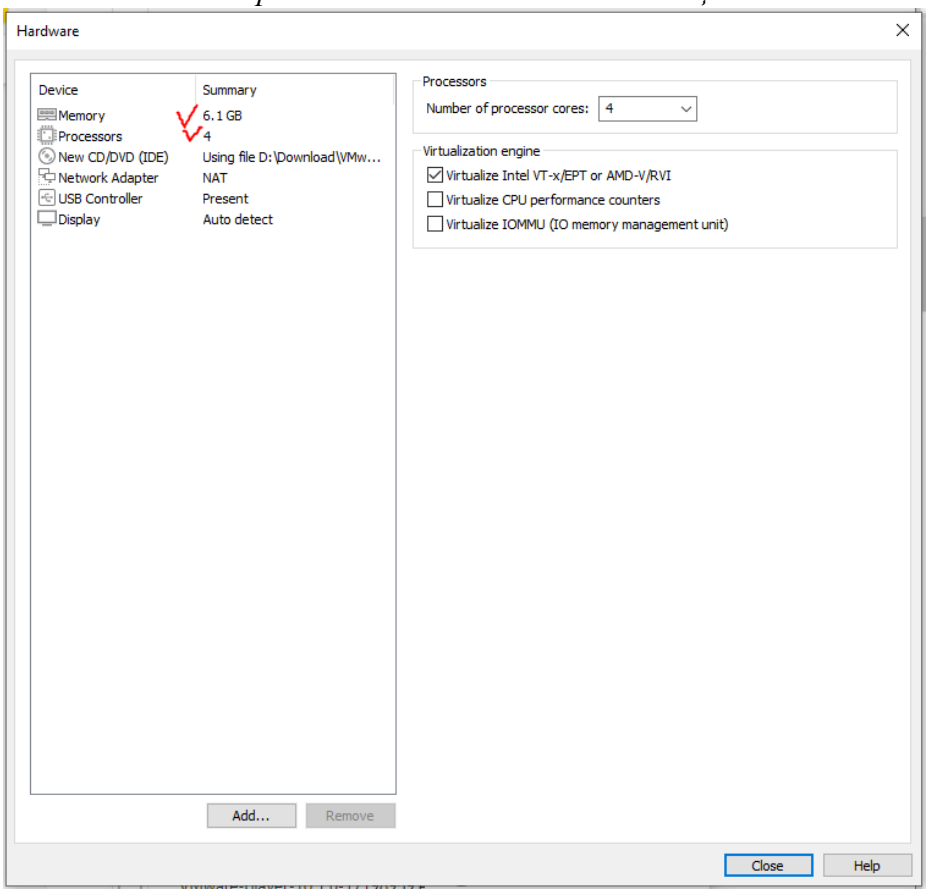
d. Указать размер диска для виртуальной машины. Здесь необходимо указать максимально возможный размер, который позволяет ваша система.



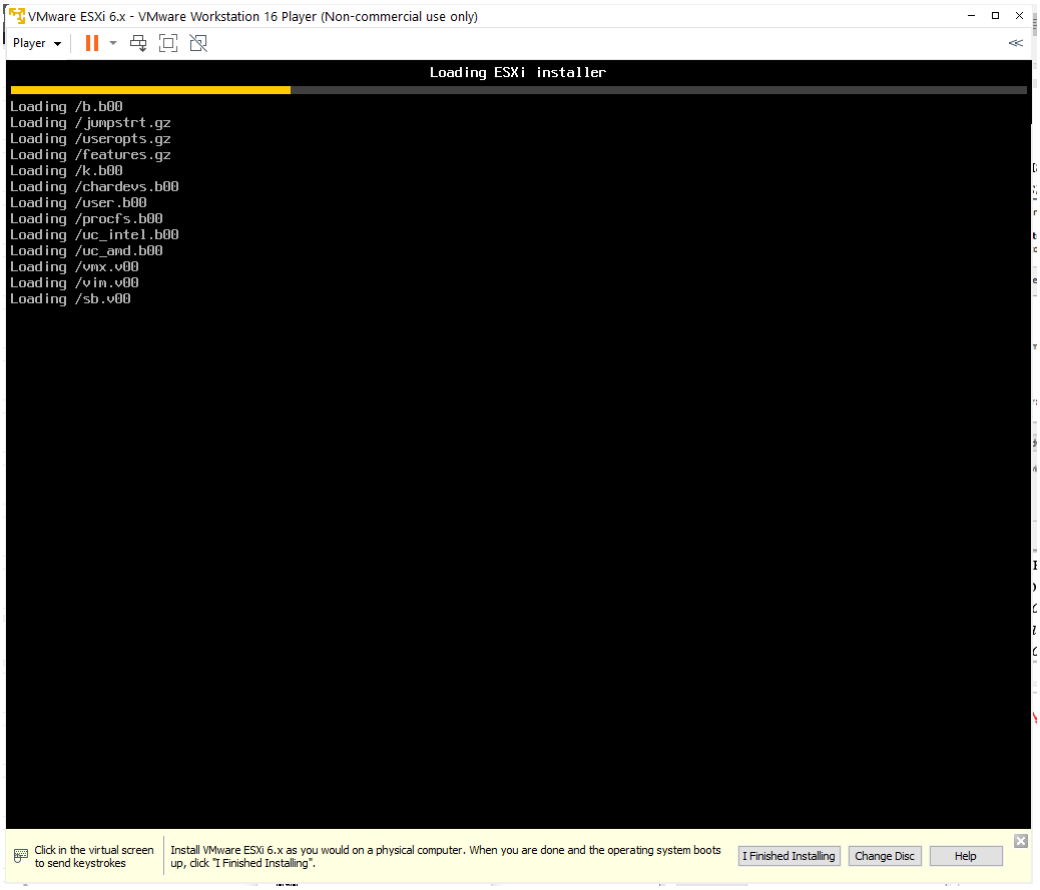
e. Провести настройку параметров виртуальной машины, нажав кнопку *Customize Hardware*

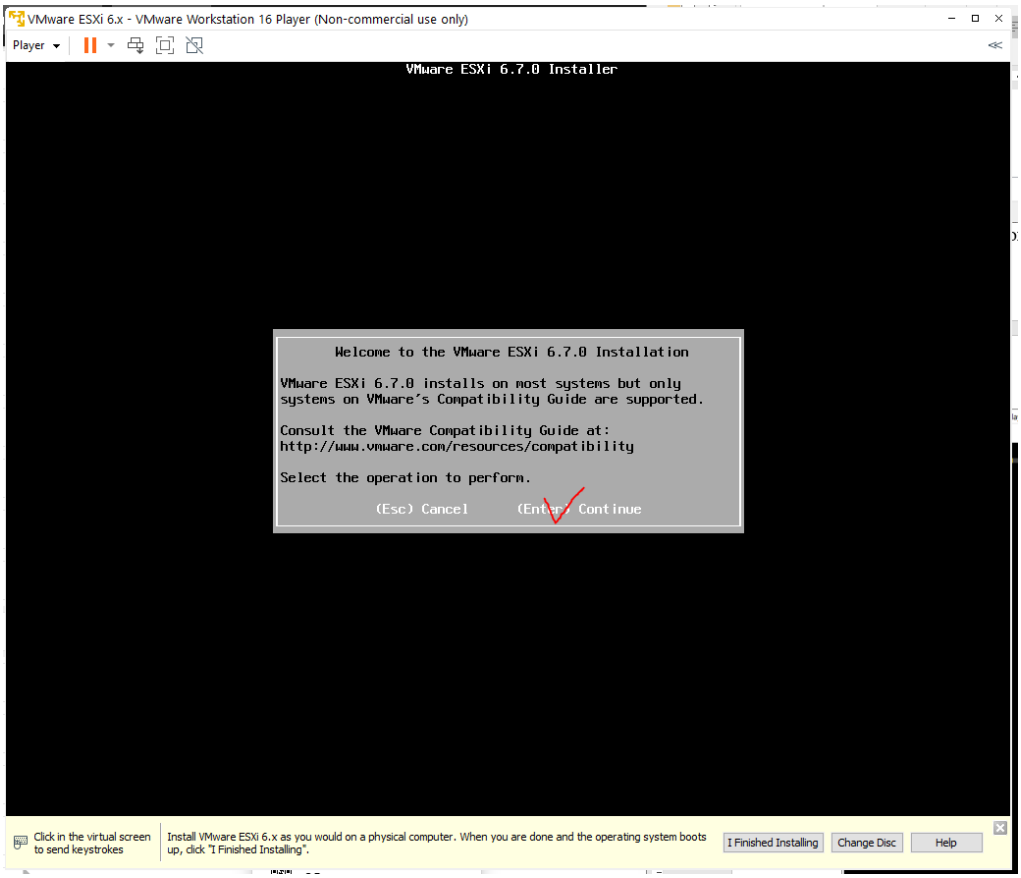


Указать максимально возможное количество ОЗУ и количество процессоров, которое позволяет выбрать ваша система. *Количество ОЗУ для виртуальной машины должно быть меньше имеющейся физической памяти в системе иначе произойдет падение производительности системы в целом*.

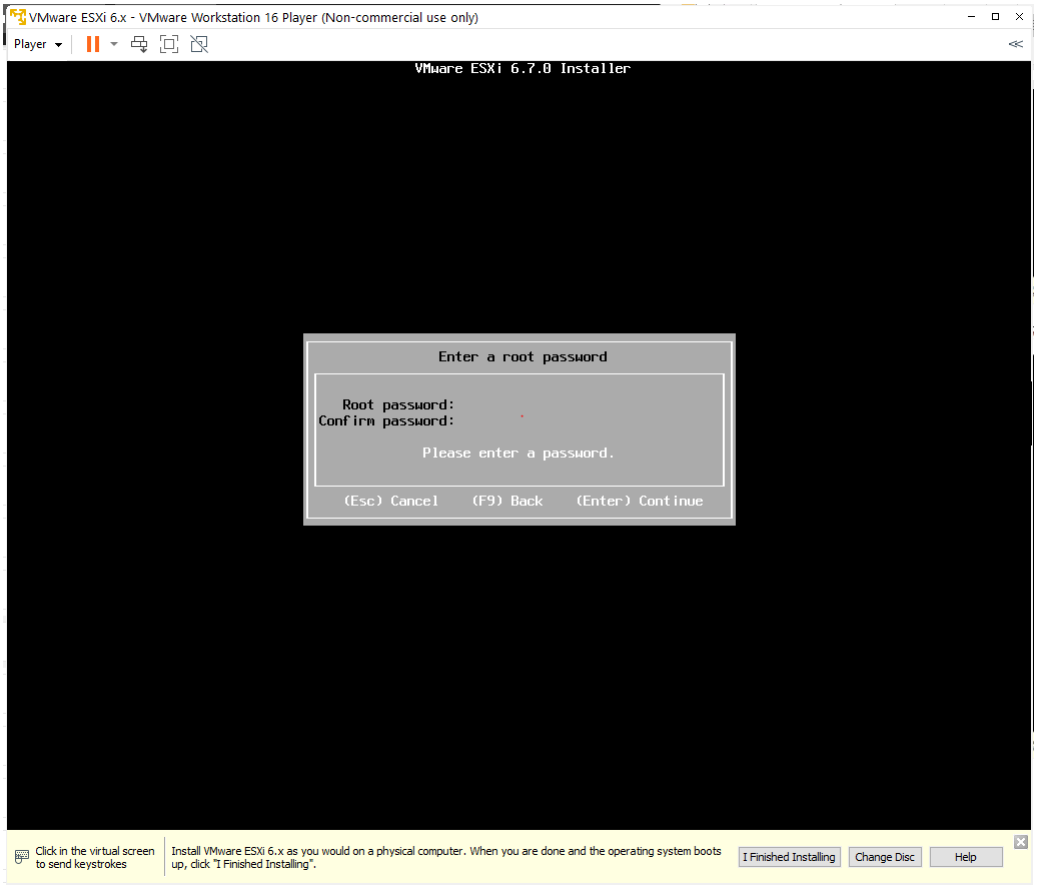


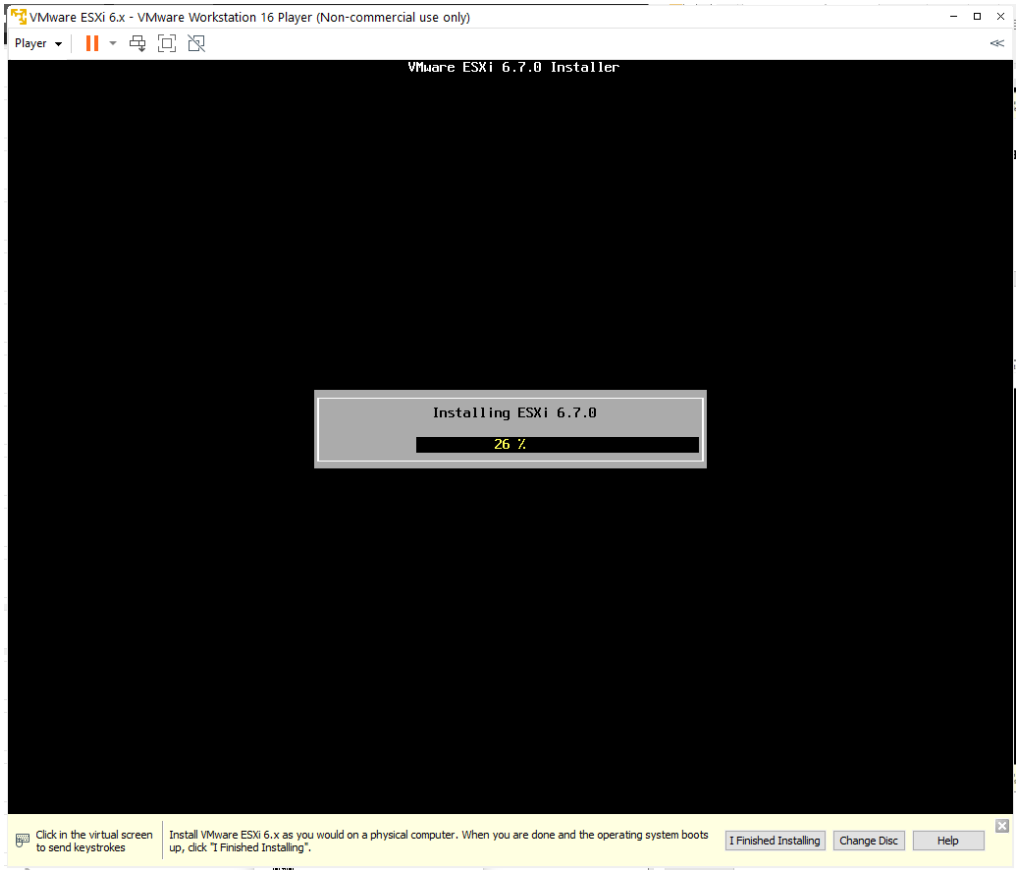
f. Нажать кнопку *Finish*. Запустится процесс установки



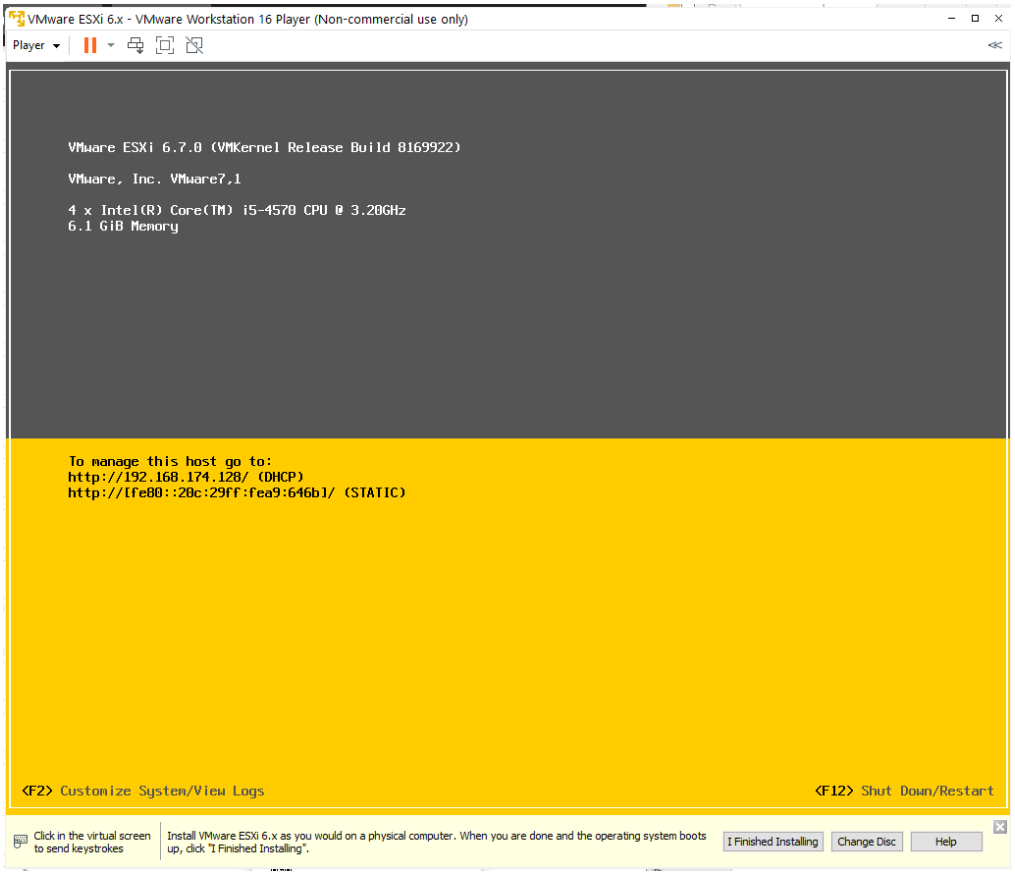


Указать пароль администратора

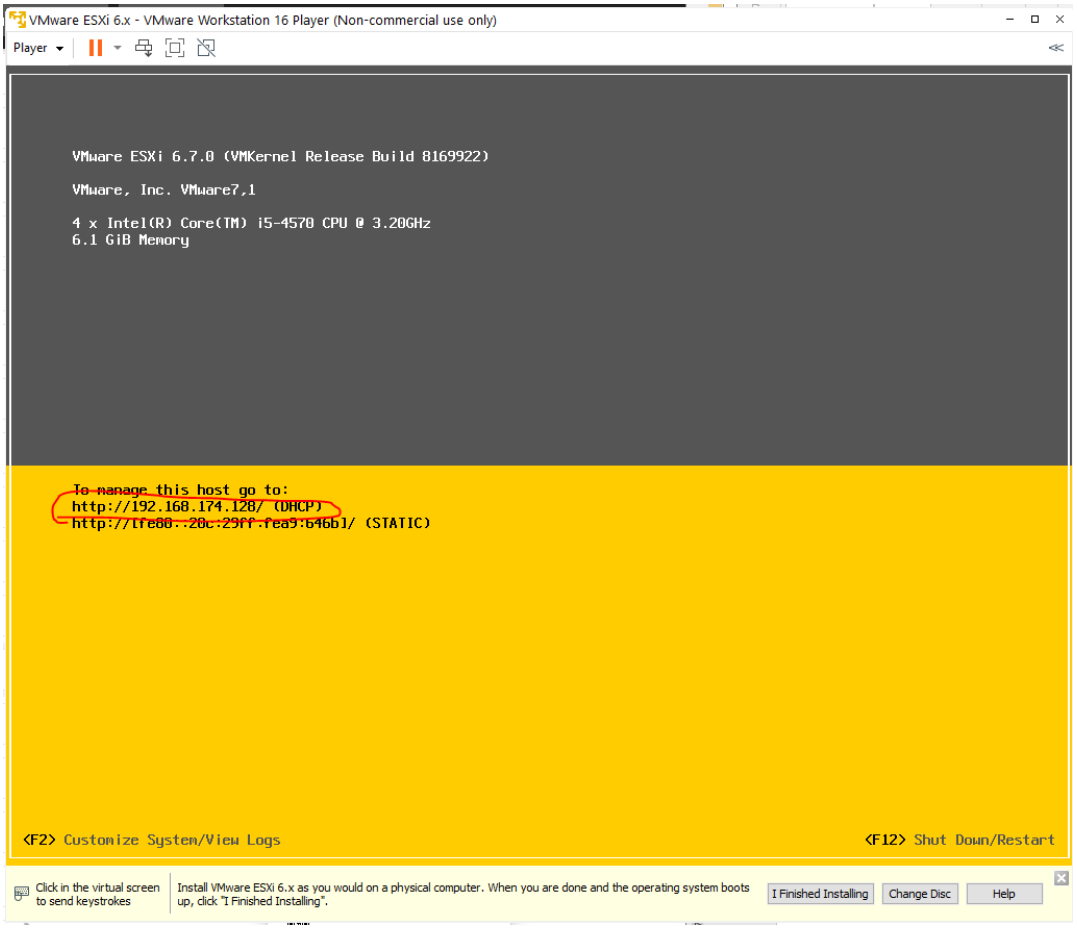




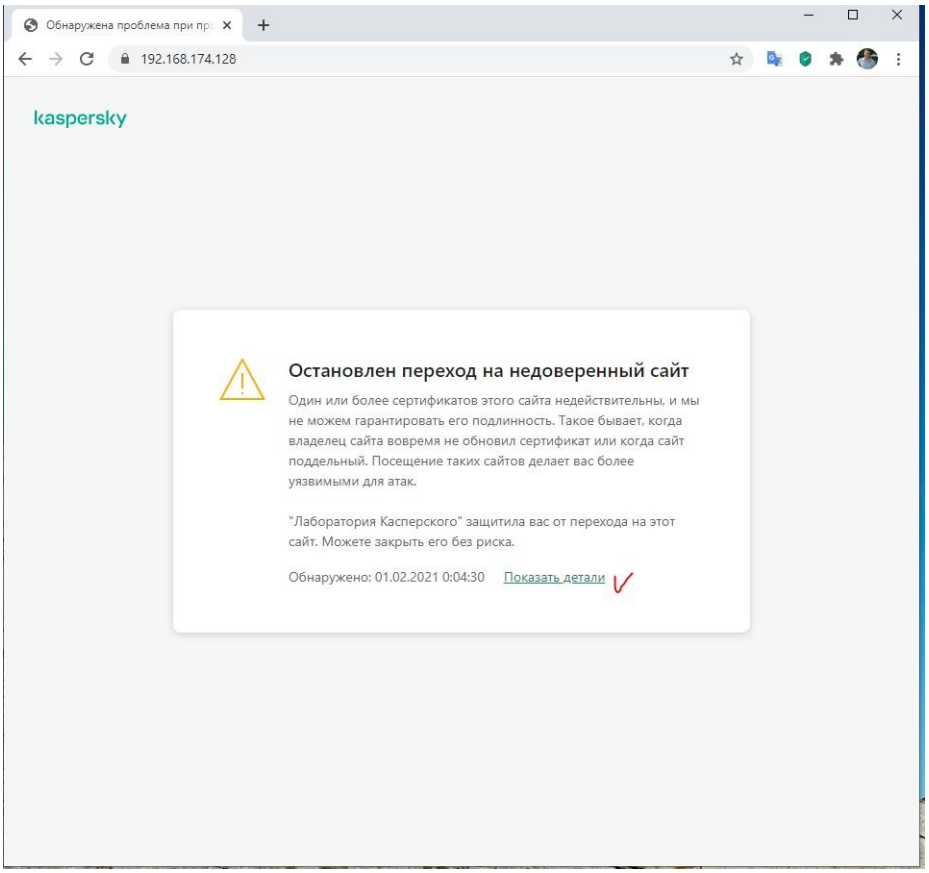
После перезагрузки система готова к работе

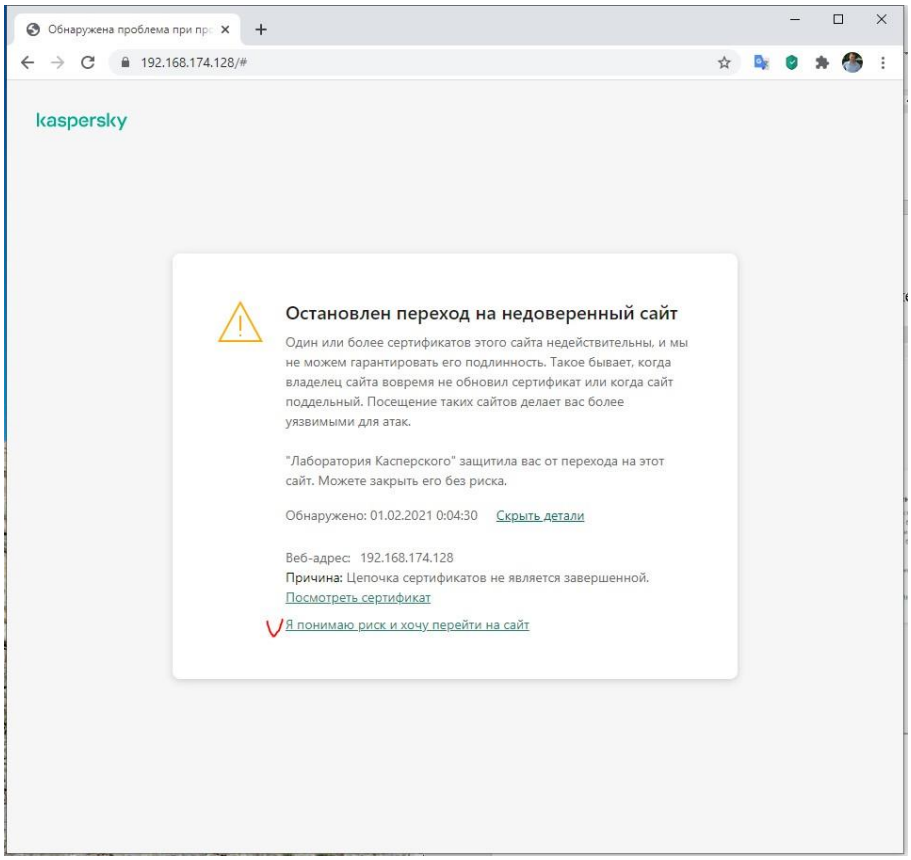


3. Доступ к системе осуществляется с помощью Web-браузера. В адресной сроке необходимо указать IP адрес, указанный на экране гипервизора

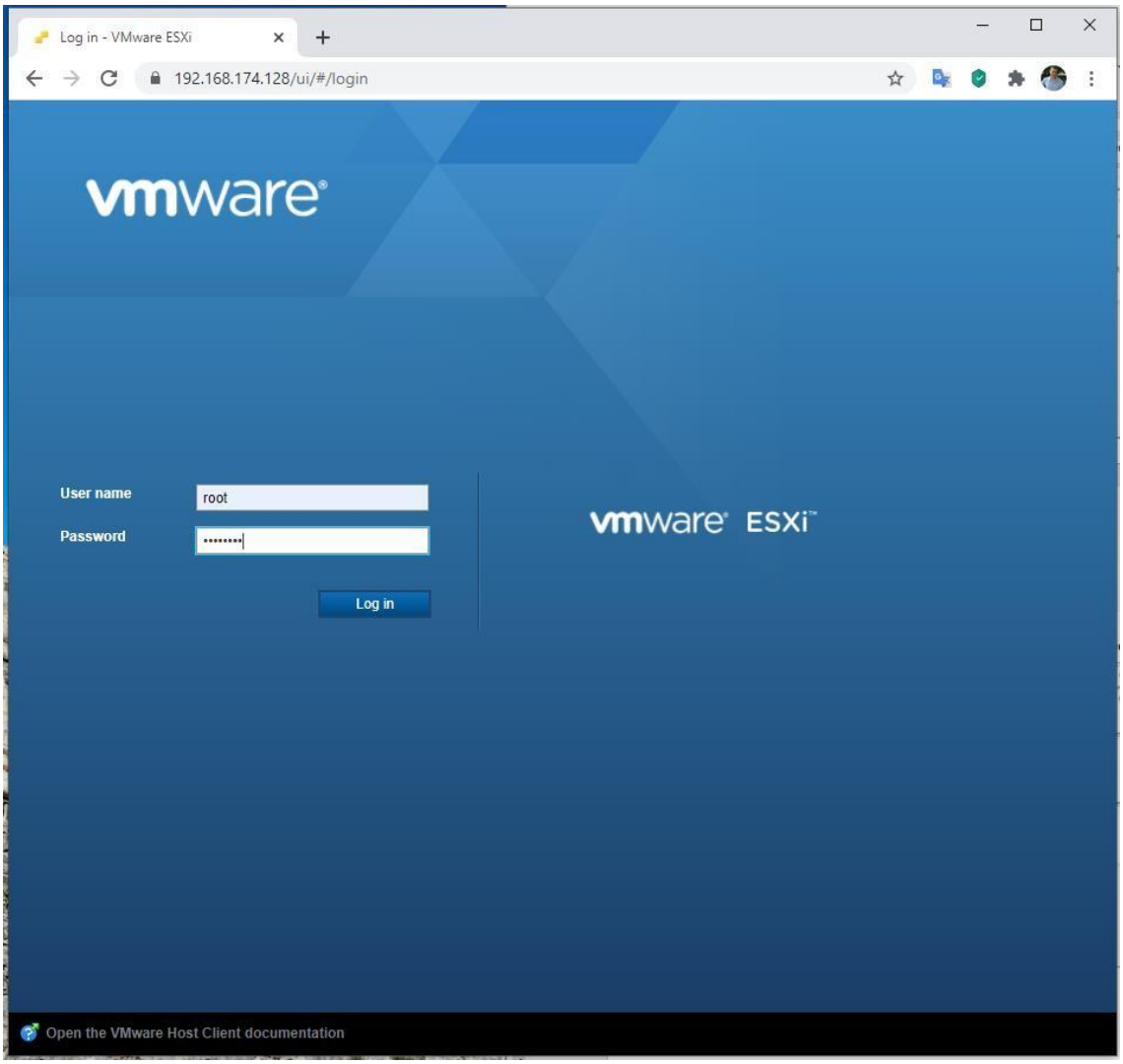


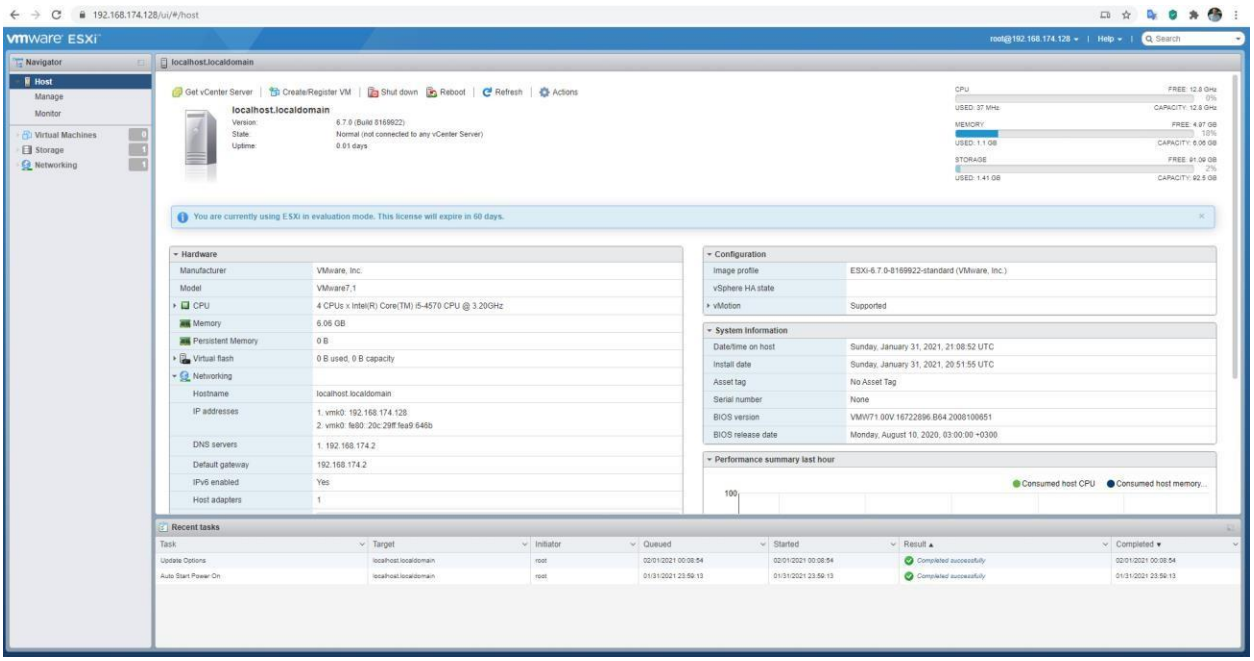
4. Возможно сообщение антивируса о небезопасном использовании этой веб страницы





5. Ввести логин и пароль





Создание сетевой инфраструктуры

Для проведения лабораторных работ будет использована схема сети, представленная на рисунке

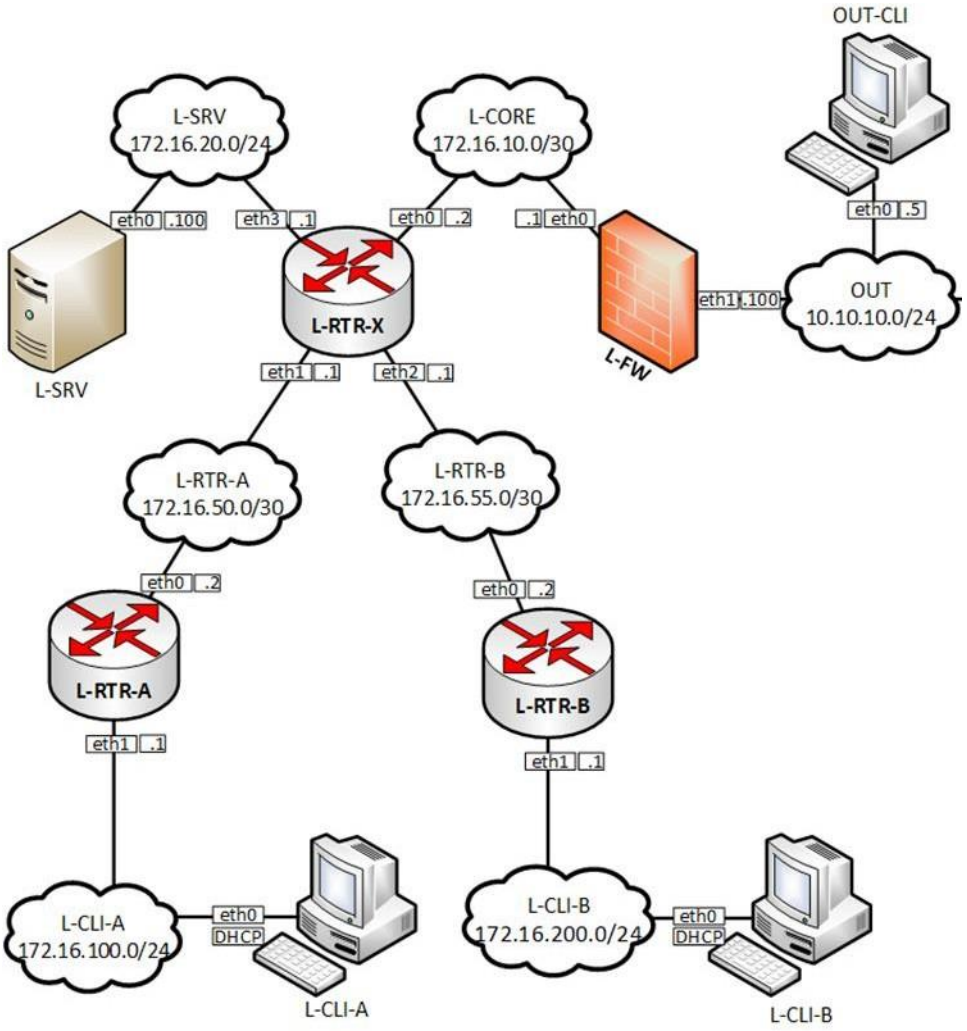
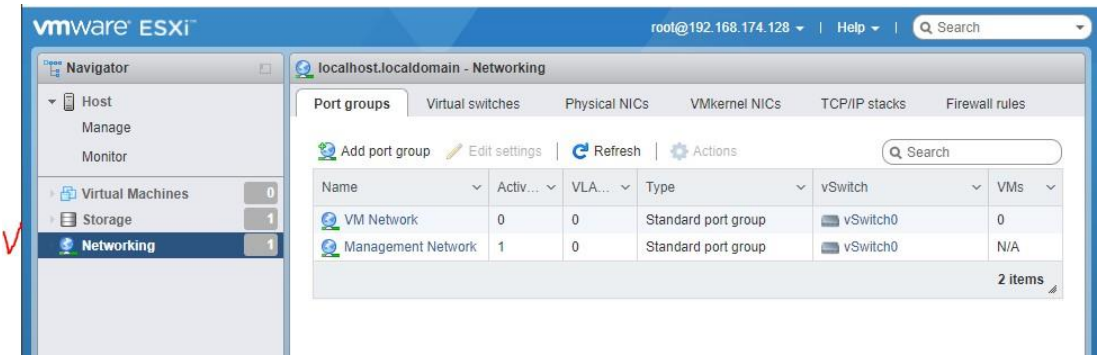


Рисунок 1. Топология сети

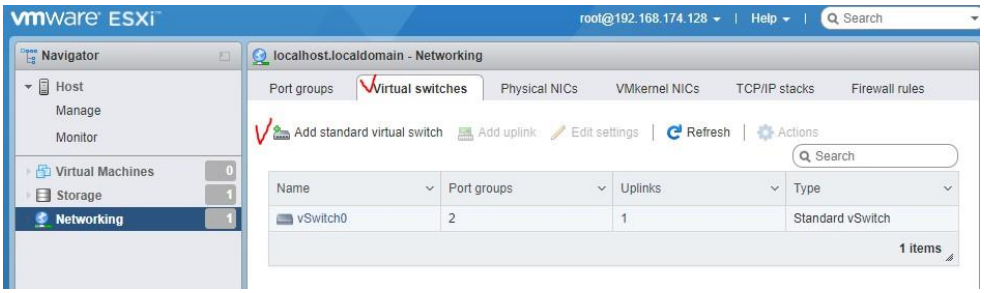
Каждое «облако» на схеме представляет собой отдельную подсеть со своим адресным пространством. В системе VMware ESXi реализовать такую топологию возможно с использованием механизма **Виртуальных коммутаторов** и **Групп портов**.

Для создания виртуального коммутатора и группы портов необходимо:

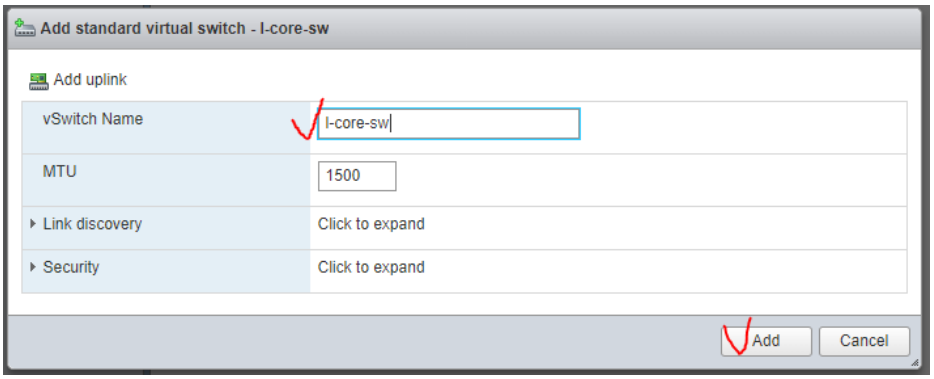
1. Нажать на пункт *Networking* в древовидном списке слева



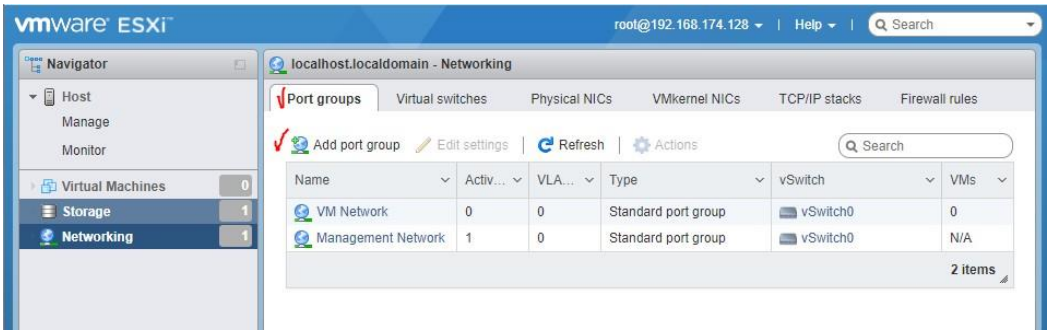
2. Открыть вкладку *Virtual switches* и нажать *Add standard virtual switch*



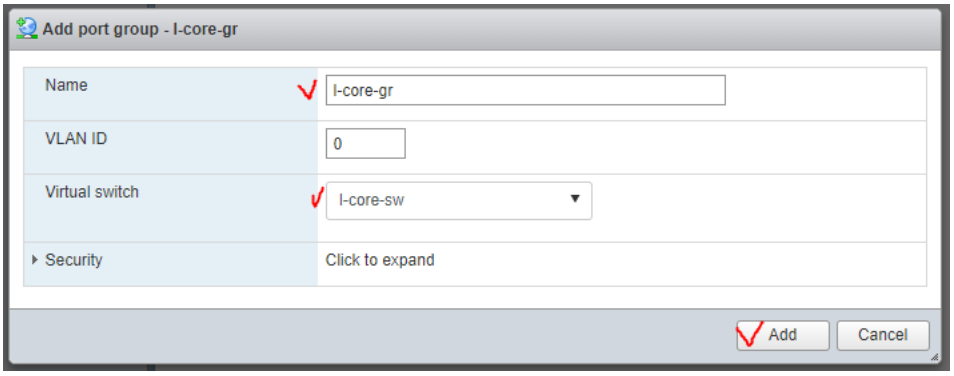
3. Указать имя нового коммутатора, например, *l-core-sw*, и нажать кнопку *Add*



4. Открыть вкладку *Port groups* и нажать *Add port group*

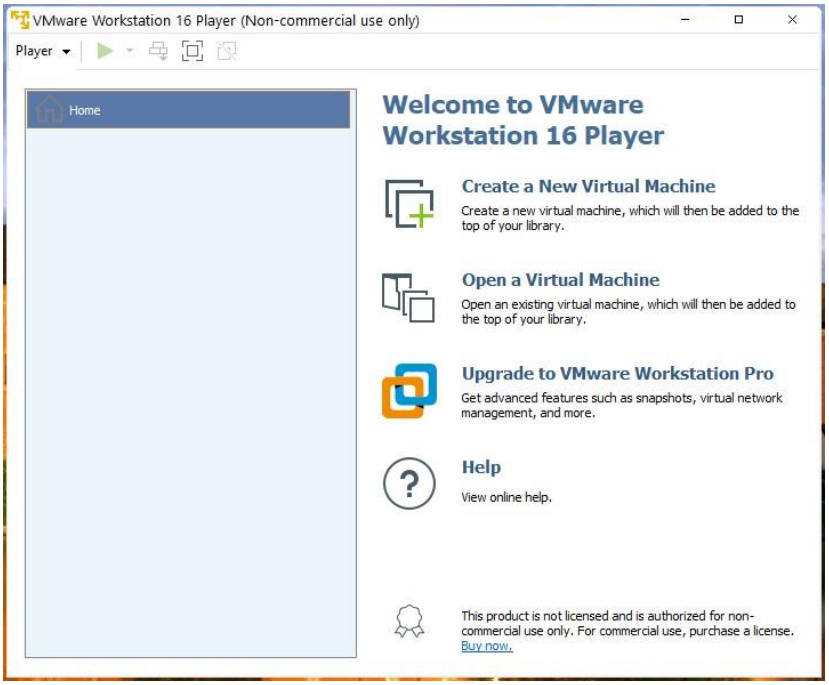


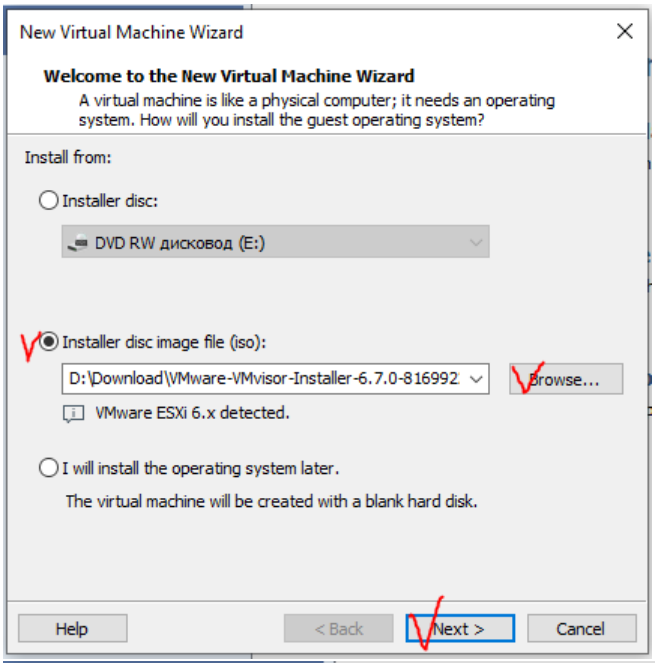
5. Указать имя новой группы портов, например, L-core-gr, и выбрать из списка виртуальных коммутаторов нужный, в нашем случае – это L- core-sw, и нажать кнопку *Add*

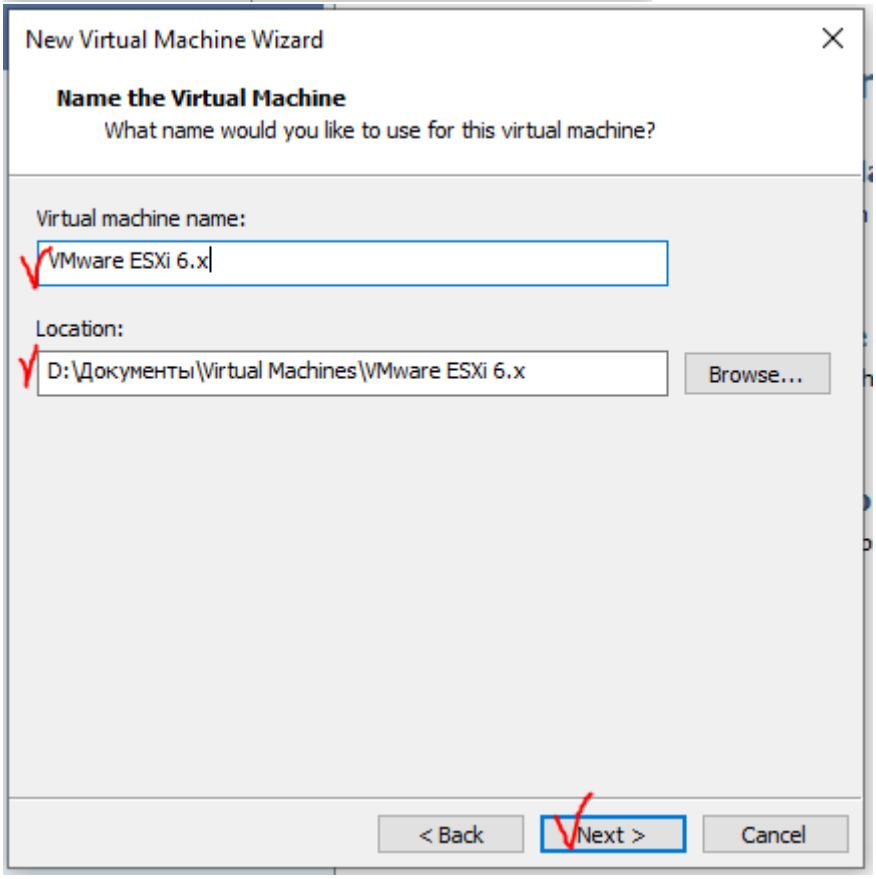


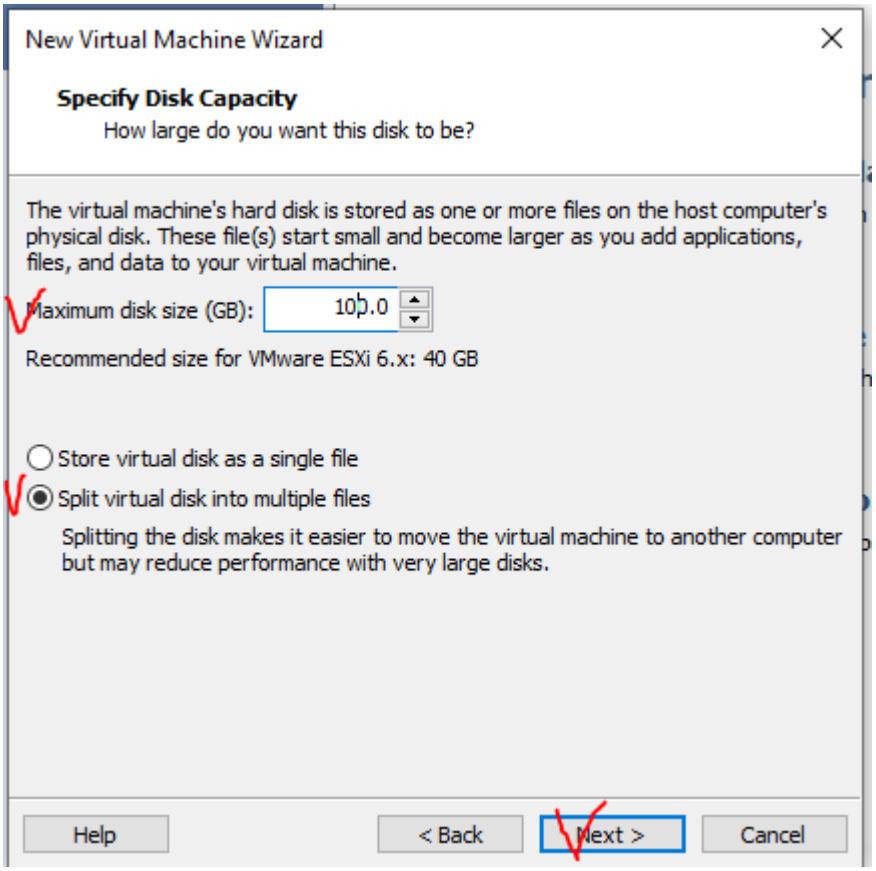
Таким образом, с помощью указанного механизма реализуется следующее правило: группа портов подключается только к одному виртуальному коммутатору, а один виртуальный коммутатор может содержать несколько групп портов. Подключение виртуальных машин к виртуальным коммутаторам, т.е. **создание подсетей**, осуществляется с помощью **присоединения сетевого адаптера виртуальной машины к нужной группе портов**.

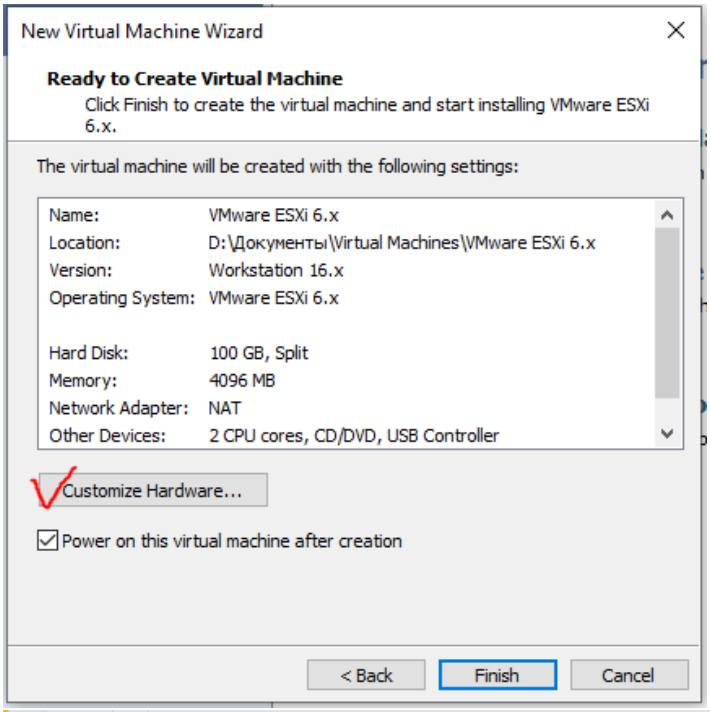
Эталон ответа

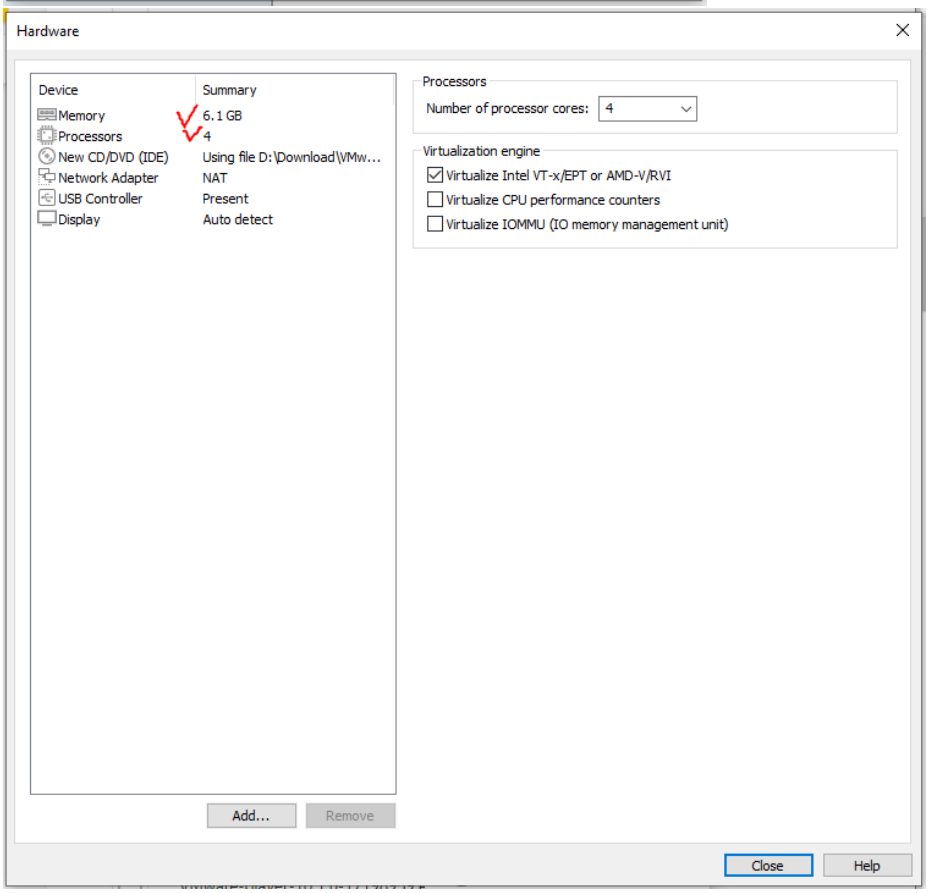


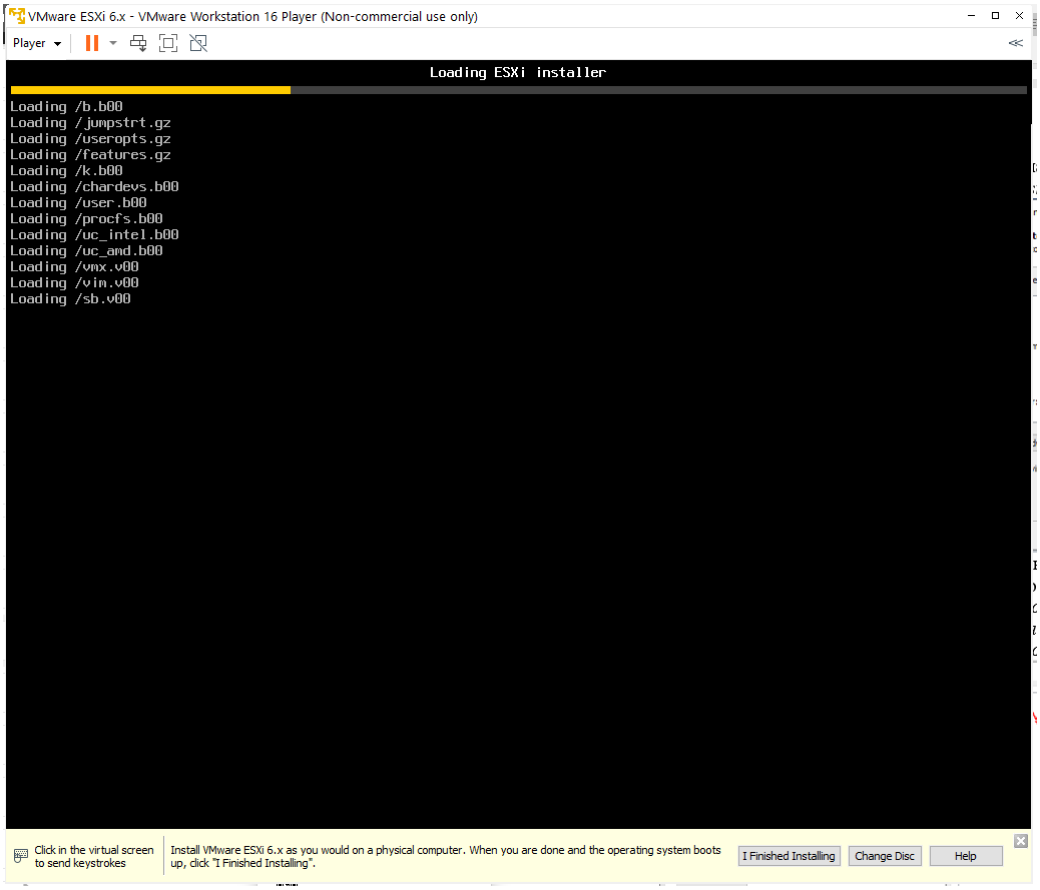

New Virtual Machine Wizard
Welcome to the New Virtual Machine Wizard
A virtual machine is like a physical computer; it needs an operating system. How will you install the guest operating system?
Install from:
Installer disc:
DVD RW дисковод (E:)
Installer disc image file (iso):
D:\Download\VMware-VMvisor-Installer-6.7.0-816992
Browse...
VMware ESXi 6.x detected.
I will install the operating system later.
The virtual machine will be created with a blank hard disk.
Help
< Back
Next >
Cancel

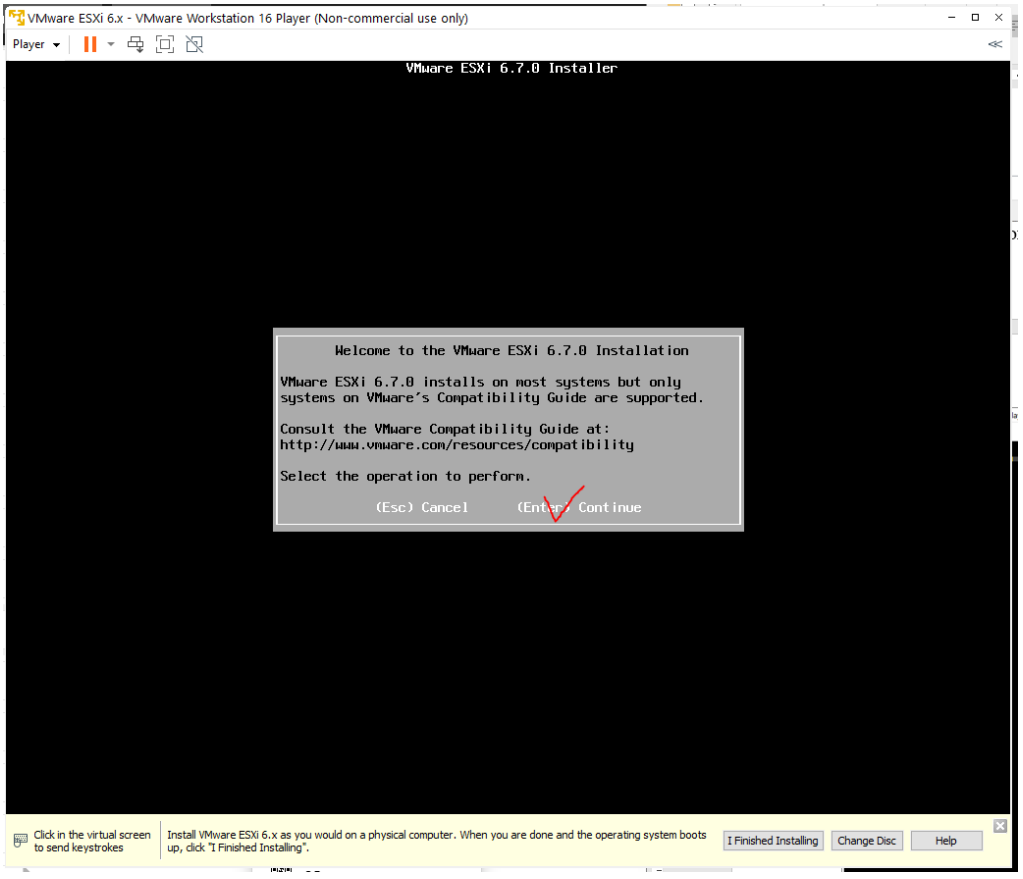

New Virtual Machine Wizard
Name the Virtual Machine
What name would you like to use for this virtual machine?
Virtual machine name:
VMware ESXi 6.x
Location:
D:\Документы\Virtual Machines\VMware ESXi 6.x
Browse...
< Back
Next >
Cancel

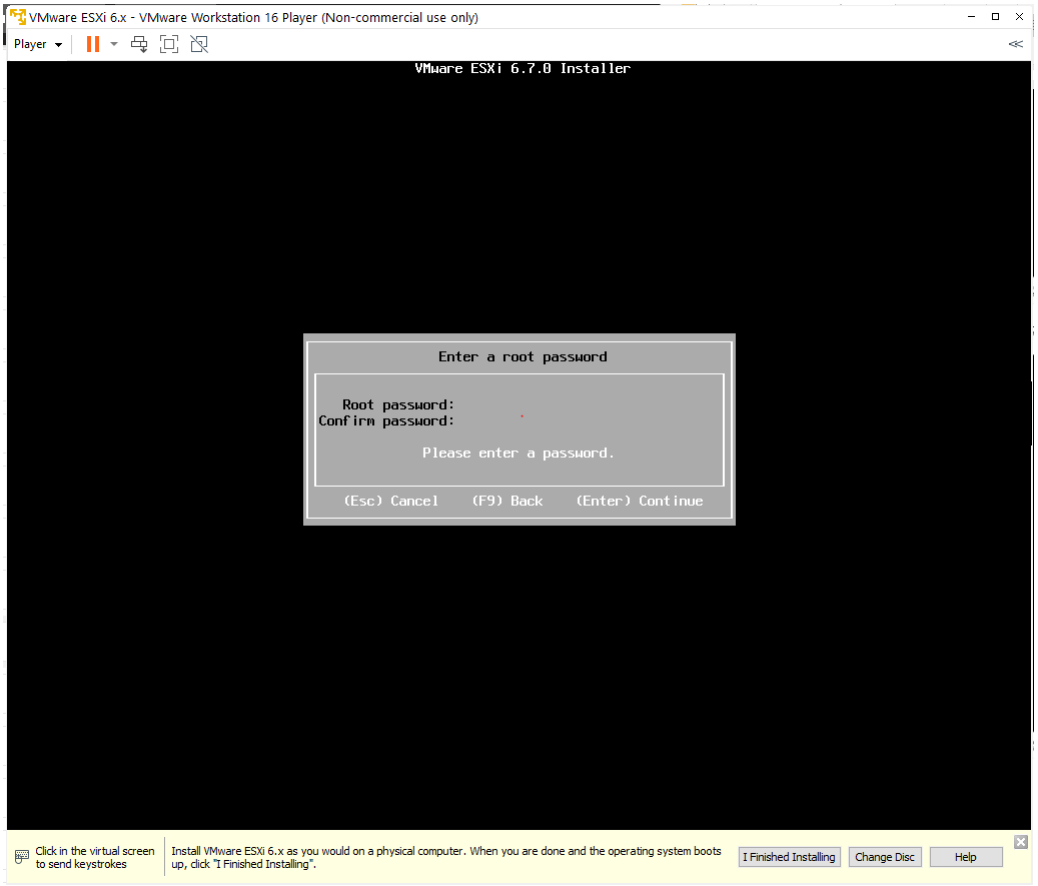

New Virtual Machine Wizard
Specify Disk Capacity
How large do you want this disk to be?
The virtual machine's hard disk is stored as one or more files on the host computer's physical disk. These file(s) start small and become larger as you add applications, files, and data to your virtual machine.
Maximum disk size (GB):
100.0
Recommended size for VMware ESXi 6.x: 40 GB
Store virtual disk as a single file
Split virtual disk into multiple files
Splitting the disk makes it easier to move the virtual machine to another computer but may reduce performance with very large disks.
Help
< Back
Next >
Cancel

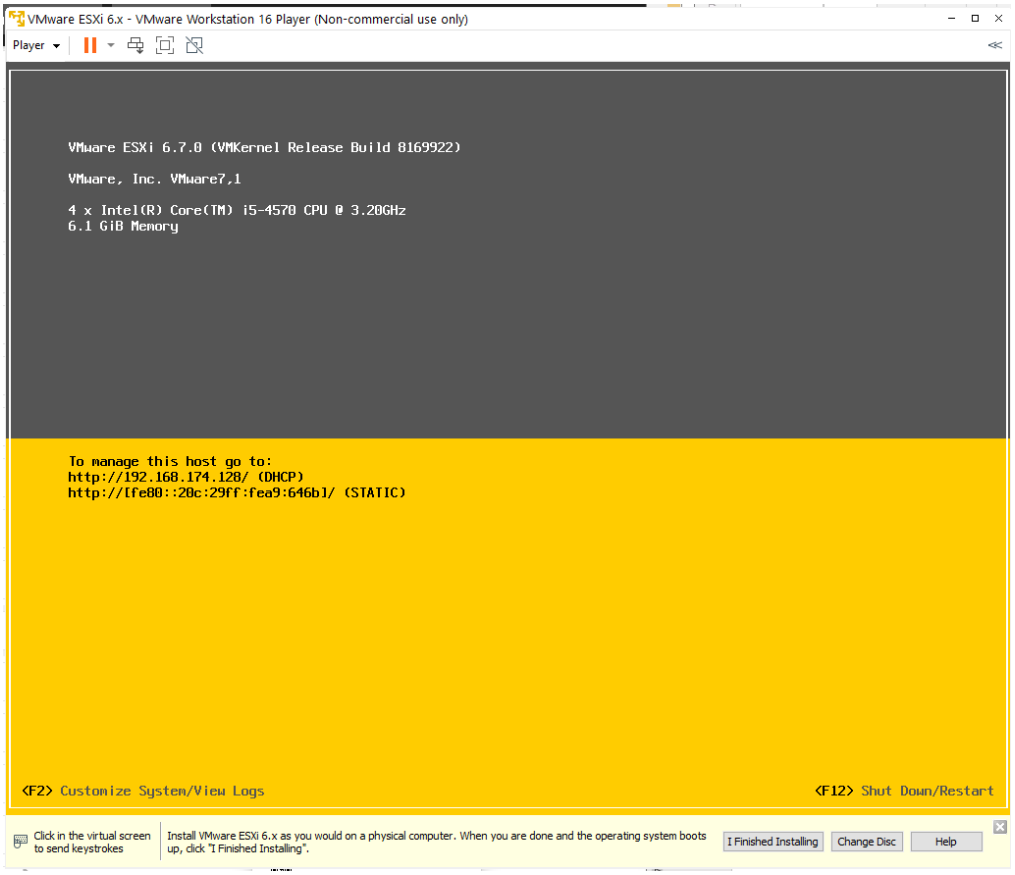

New Virtual Machine Wizard
Ready to Create Virtual Machine
Click Finish to create the virtual machine and start installing VMware ESXi 6.x.
The virtual machine will be created with the following settings:
Name: VMware ESXi 6.x
Location: D:\Документы\Virtual Machines\VMware ESXi 6.x
Version: Workstation 16.x
Operating System: VMware ESXi 6.x
Hard Disk: 100 GB, Split
Memory: 4096 MB
Network Adapter: NAT
Other Devices: 2 CPU cores, CD/DVD, USB Controller
Customize Hardware...
Power on this virtual machine after creation
< Back
Finish
Cancel

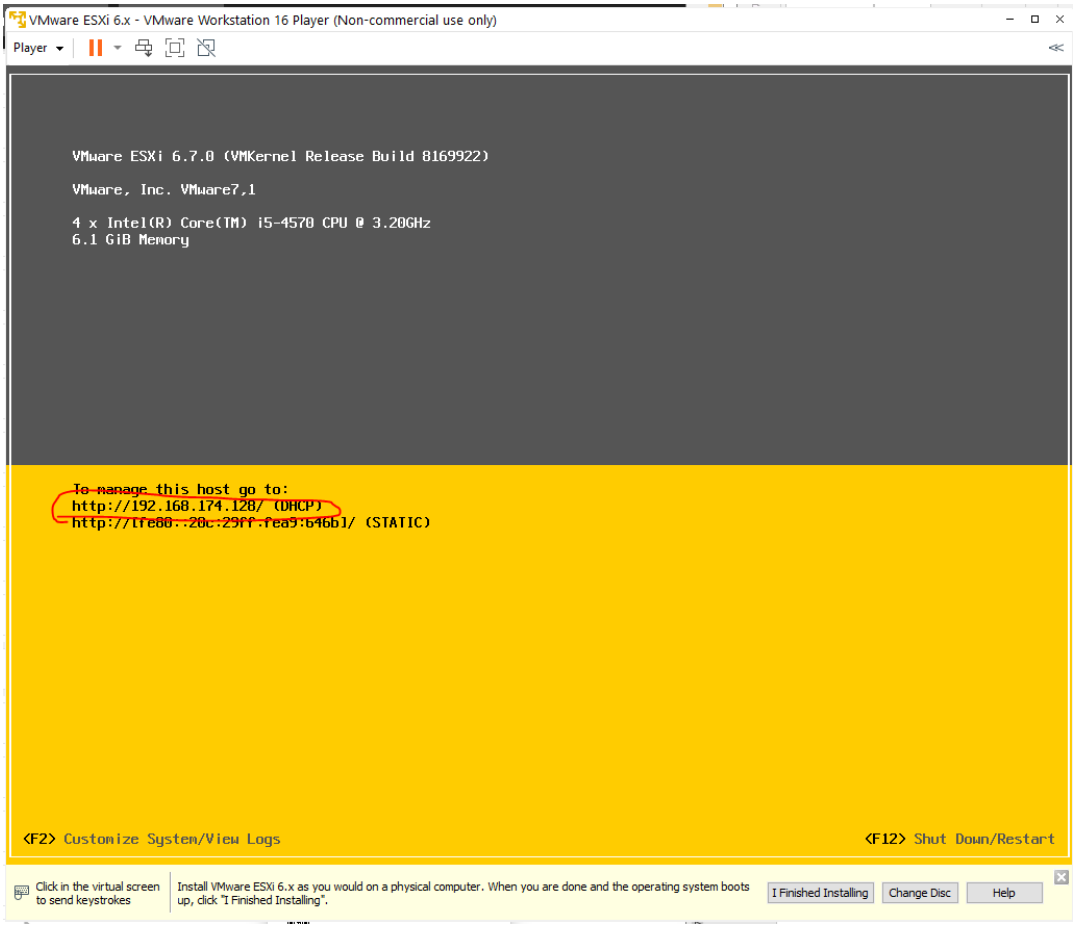

Hardware
Device
Summary
Memory
6.1 GB
Processors
4
New CD/DVD (IDE)
Using file D:\Download\VMw...
Network Adapter
NAT
USB Controller
Present
Display
Auto detect
Processors
Number of processor cores: 4
Virtualization engine
Virtualize Intel VT-x/EPT or AMD-V/RVI
Virtualize CPU performance counters
Virtualize IOMMU (IO memory management unit)
Add...
Remove
Close
Help

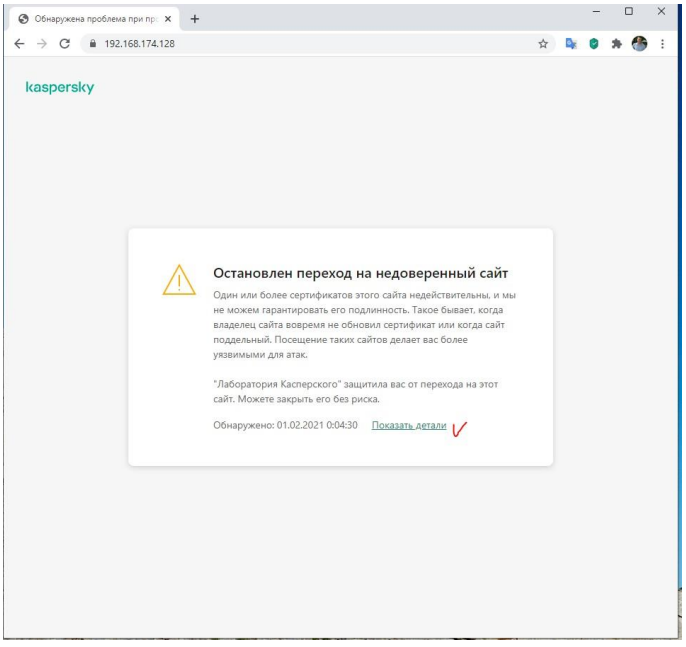

VMware ESXi 6.x - VMware Workstation 16 Player (Non-commercial use only)
Player
Loading ESXi installer
Loading /b.b00
Loading /jumpstrt.gz
Loading /useropts.gz
Loading /features.gz
Loading /k.b00
Loading /chardevs.b00
Loading /user.b00
Loading /procfs.b00
Loading /uc_intel.b00
Loading /uc_amd.b00
Loading /vmx.v00
Loading /vim.v00
Loading /sb.v00
Click in the virtual screen to send keystrokes
Install VMware ESXi 6.x as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Change Disc
Help

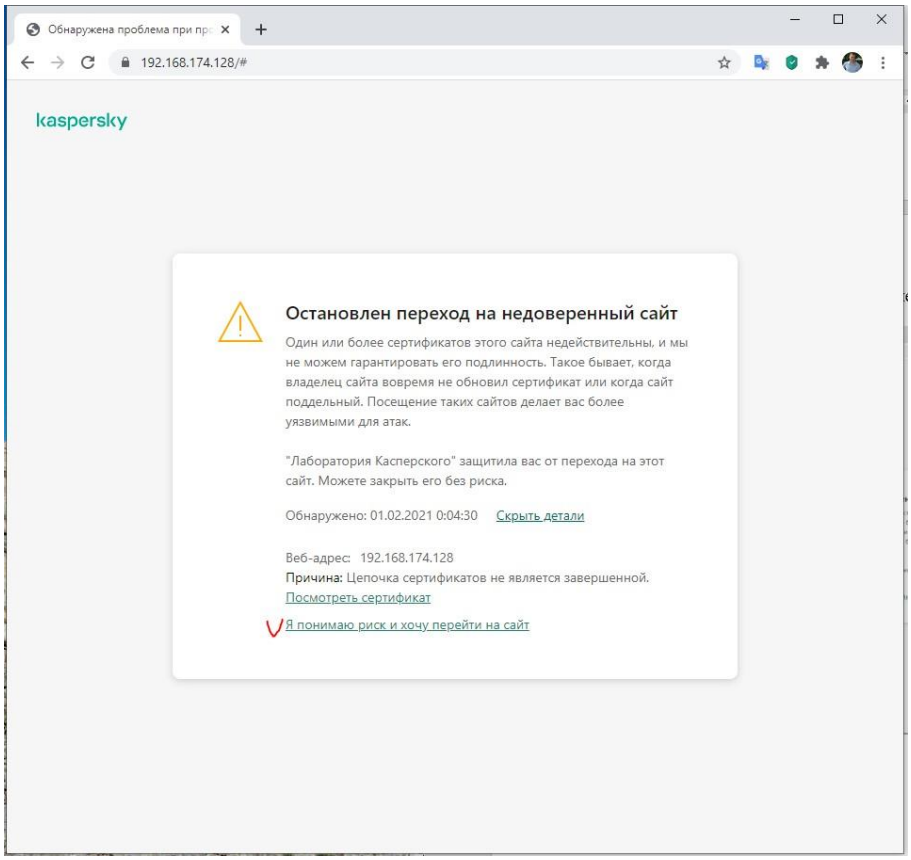

VMware ESXi 6.x - VMware Workstation 16 Player (Non-commercial use only)
Player
VMware ESXi 6.7.0 Installer
Welcome to the VMware ESXi 6.7.0 Installation
VMware ESXi 6.7.0 installs on most systems but only systems on VMware's Compatibility Guide are supported.
Consult the VMware Compatibility Guide at:
http://www.vmware.com/resources/compatibility
Select the operation to perform.
(Esc) Cancel
(Enter) Continue
Click in the virtual screen to send keystrokes
Install VMware ESXi 6.x as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Change Disc
Help

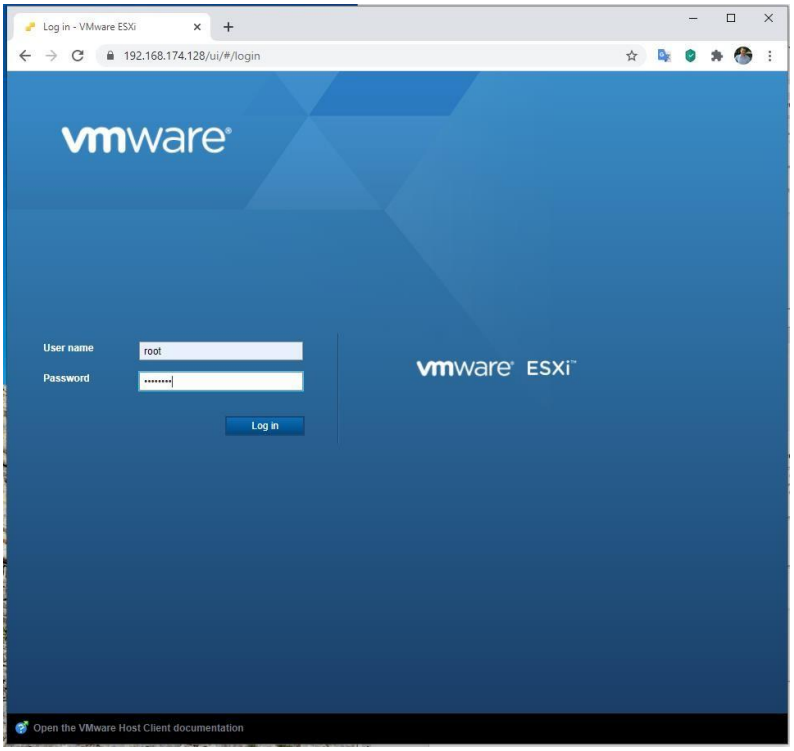

VMware ESXi 6.x - VMware Workstation 16 Player (Non-commercial use only)
Player
VMware ESXi 6.7.0 Installer
Enter a root password
Root password:
Confirm password:
Please enter a password.
(Esc) Cancel (F9) Back (Enter) Continue
Click in the virtual screen to send keystrokes
Install VMware ESXi 6.x as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Change Disc
Help

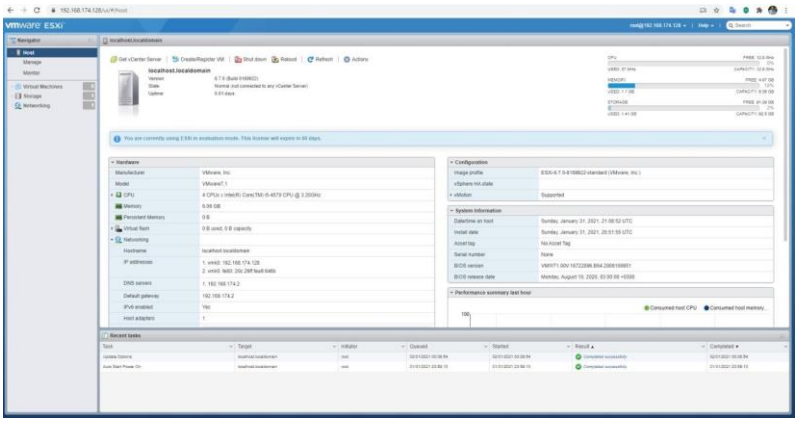

VMware ESXi 6.x - VMware Workstation 16 Player (Non-commercial use only)
Player
VMware ESXi 6.7.0 (VMkernel Release Build 8169922)
VMware, Inc. VMware7,1
4 x Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz
6.1 GiB Memory
To manage this host go to:
http://192.168.174.128/ (DHCP)
http://[fe80::20c:29ff:fea9:646b]/ (STATIC)
<F2> Customize System/View Logs
<F12> Shut Down/Restart
Click in the virtual screen to send keystrokes
Install VMware ESXi 6.x as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Change Disc
Help

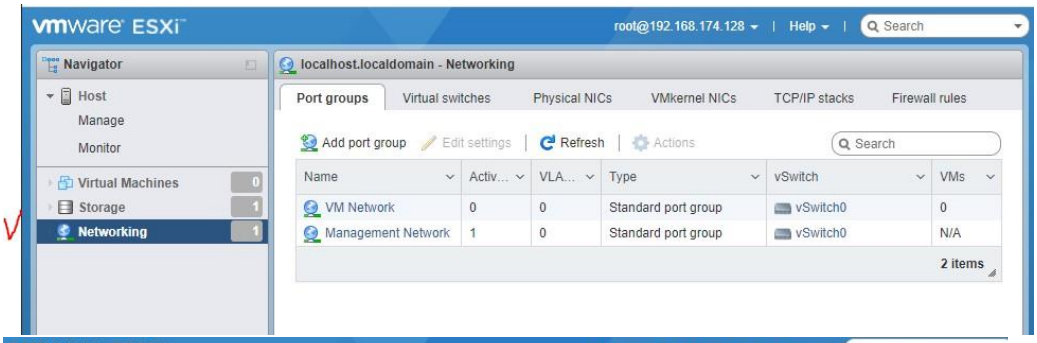

VMware ESXi 6.x - VMware Workstation 16 Player (Non-commercial use only)
Player
VMware ESXi 6.7.0 (VMKernel Release Build 8169922)
VMware, Inc. VMware7,1
4 x Intel(R) Core(TM) i5-4570 CPU @ 3.20GHz
6.1 GiB Memory
To manage this host go to:
http://192.168.174.128/ (DHCP)
http://[fe80::20c:29ff:fea9:646b]/ (STATIC)
<F2> Customize System/View Logs
<F12> Shut Down/Restart
Click in the virtual screen to send keystrokes
Install VMware ESXi 6.x as you would on a physical computer. When you are done and the operating system boots up, click "I Finished Installing".
I Finished Installing
Change Disc
Help

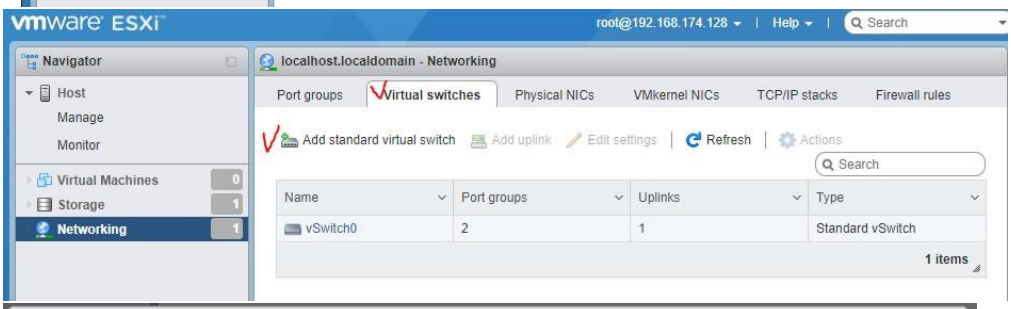

192.168.174.128
kaspersky
Остановлен переход на недоверенный сайт
Один или более сертификатов этого сайта недействительны, и мы не можем гарантировать его подлинность. Такое бывает, когда владелец сайта вовремя не обновил сертификат или когда сайт поддельный. Посещение таких сайтов делает вас более уязвимыми для атак.
"Лаборатория Касперского" защитила вас от перехода на этот сайт. Можете закрыть его без риска.
Обнаружено: 01.02.2021 0:04:30
Показать детали

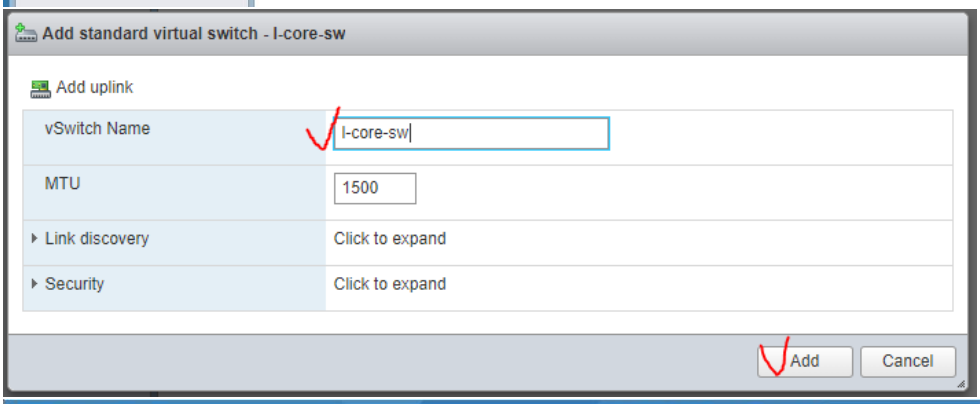

Обнаружена проблема при пр
192.168.174.128/#
kaspersky
Остановлен переход на недоверенный сайт
Один или более сертификатов этого сайта недействительны, и мы не можем гарантировать его подлинность. Такое бывает, когда владелец сайта вовремя не обновил сертификат или когда сайт поддельный. Посещение таких сайтов делает вас более уязвимыми для атак.
"Лаборатория Касперского" защитила вас от перехода на этот сайт. Можете закрыть его без риска.
Обнаружено: 01.02.2021 0:04:30
Скрыть детали
Веб-адрес: 192.168.174.128
Причина: Цепочка сертификатов не является завершенной.
Посмотреть сертификат
Я понимаю риск и хочу перейти на сайт


Log in - VMware ESXi
192.168.174.128/ui/#/login
vmware
User name
root
Password
Log in
vmware ESXi
Open the VMware Host Client documentation

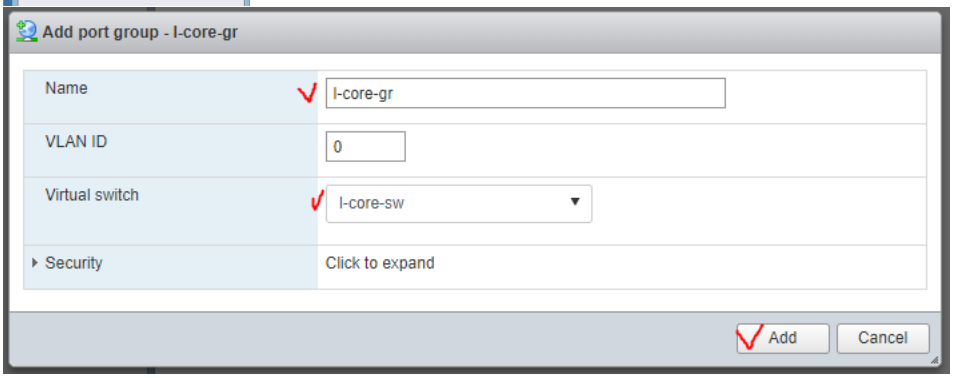

vmware ESXi
localhost.localdomain


vmware ESXi
root@192.168.174.128 | Help | Search
Navigator
Host
Manage
Monitor
Virtual Machines 0
Storage 1
Networking 1
localhost.localdomain - Networking
Port groups
Virtual switches
Physical NICs
VMkernel NICs
TCP/IP stacks
Firewall rules
Add port group
Edit settings
Refresh
Actions
Search
Name
Activ...
VLA...
Type
vSwitch
VMs
VM Network 0 0 Standard port group vSwitch0 0
Management Network 1 0 Standard port group vSwitch0 N/A
2 items


vmware ESXi
root@192.168.174.128 | Help | Search
Navigator
Host
Manage
Monitor
Virtual Machines 0
Storage 1
Networking 1
localhost.localdomain - Networking
Port groups
Virtual switches
Physical NICs
VMkernel NICs
TCP/IP stacks
Firewall rules
Add standard virtual switch
Add uplink
Edit settings
Refresh
Actions
Search
Name
Port groups
Uplinks
Type
vSwitch0 2 1 Standard vSwitch
1 items


Add standard virtual switch - l-core-sw
Add uplink
vSwitch Name
l-core-sw
MTU
1500
Link discovery
Click to expand
Security
Click to expand
Add
Cancel


vmware ESXi
root@192.168.174.128 | Help | Search
Navigator
Host
Manage
Monitor
Virtual Machines 0
Storage 1
Networking 1
localhost.localdomain - Networking
Port groups
Virtual switches
Physical NICs
VMkernel NICs
TCP/IP stacks
Firewall rules
Add port group
Edit settings
Refresh
Actions
Search
Name
Activ...
VLA...
Type
vSwitch
VMs
VM Network 0 0 Standard port group vSwitch0 0
Management Network 1 0 Standard port group vSwitch0 N/A
2 items


Add port group - l-core-gr
Name
l-core-gr
VLAN ID
0
Virtual switch
l-core-sw
Security
Click to expand
Add
Cancel

Практическая работа № 10 Работа с контейнерами Kubernetes в среде Proxmox VE

Инструкция для обучающихся

Внимательно прочитайте задание. Выполните все необходимые операции.

Время выполнения задания – 90 минут.

Задание

Задание:

Установка того, с каким Kubernetes-кластером взаимодействует kubectl и изменяет конфигурационную информацию. Подробную информацию о конфигурационном файле смотрите на странице Authenticating Across Clusters with kubeconfig.

kubectl config view # показать объединённые настройки kubeconfig

использовать несколько файлов kubeconfig одновременно и посмотреть объединённую конфигурацию из этих файлов

KUBECONFIG=~/.kube/config:~/.kube/kubconfig2

kubectl config view

получить пароль для пользователя e2e

kubectl config view -o jsonpath='{.users[?(@.name == "e2e")].user.password}'

показать первого пользователя

kubectl config view -o jsonpath='{.users[].name}'

получить список пользователей

kubectl config view -o jsonpath='{.users[*].name}'

показать список контекстов

kubectl config get-contexts

показать текущий контекст (current-context)

kubectl config current-context

установить my-cluster-name как контекст по умолчанию

kubectl config use-context my-cluster-name

добавить новую конфигурацию для кластера в kubeconf с базовой аутентификацией

kubectl config set-credentials kubeuser/foo.kubernetes.com --username=kubeuser --password=kubepassword

сохранить пространство имен для всех последующих команд kubectl в этом контексте.

kubectl config set-context --current --namespace=ggckad-s2

установить контекст, используя имя пользователя и пространство имен.

kubectl config set-context gce --user=cluster-admin --namespace=foo \

&& kubectl config use-context gce

удалить пользователя foo

kubectl config unset users.foo

Эталон ответа

Задание:

kubectl config view # показать объединённые настройки kubeconfig

использовать несколько файлов kubeconfig одновременно и посмотреть объединённую конфигурацию из этих файлов

KUBECONFIG=~/.kube/config:~/.kube/kubconfig2

kubectl config view

```
# получить пароль для пользователя e2e

kubectl config view -o jsonpath='{.users[?(@.name == "e2e")].user.password}'

# показать первого пользователя

kubectl config view -o jsonpath='{.users[].name}'

# получить список пользователей

kubectl config view -o jsonpath='{.users[*].name}'

# показать список контекстов

kubectl config get-contexts

# показать текущий контекст (current-context)

kubectl config current-context

# установить my-cluster-name как контекст по умолчанию

kubectl config use-context my-cluster-name

# добавить новую конфигурацию для кластера в kubeconf с базовой аутентификацией

kubectl config set-credentials kubeuser/foo.kubernetes.com --username=kubeuser --
password=kubepassword

# сохранить пространство имен для всех последующих команд kubectl в этом контек-
сте.

kubectl config set-context --current --namespace=ggckad-s2

# установить контекст, используя имя пользователя и пространство имен.

kubectl config set-context gce --user=cluster-admin --namespace=foo \

&& kubectl config use-context gce

# удалить пользователя foo

kubectl config unset users.foo
```

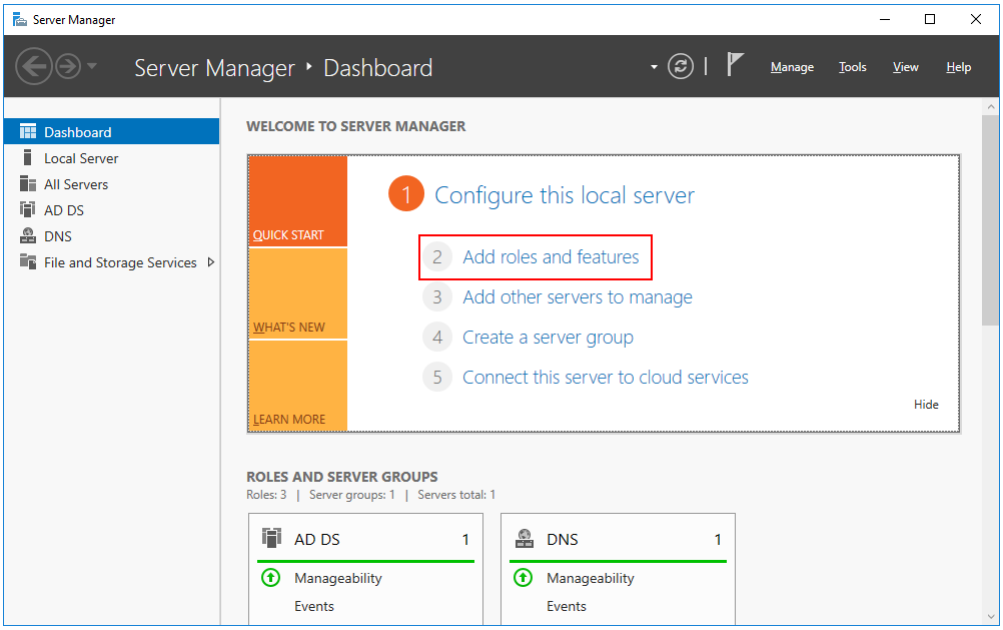
Практическая работа № 14 Настройка межплатформенный бесклиентский шлюз удаленного рабочего стола

Инструкция для обучающихся
Внимательно прочитайте задание. Выполните все необходимые операции.

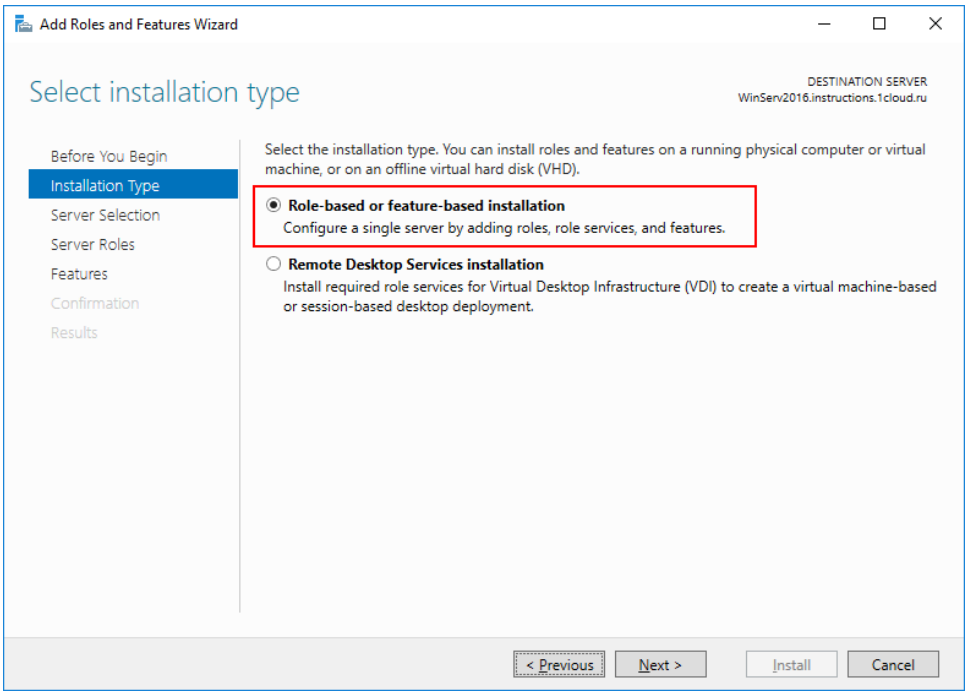
Время выполнения задания – 90 минут.

Задание:

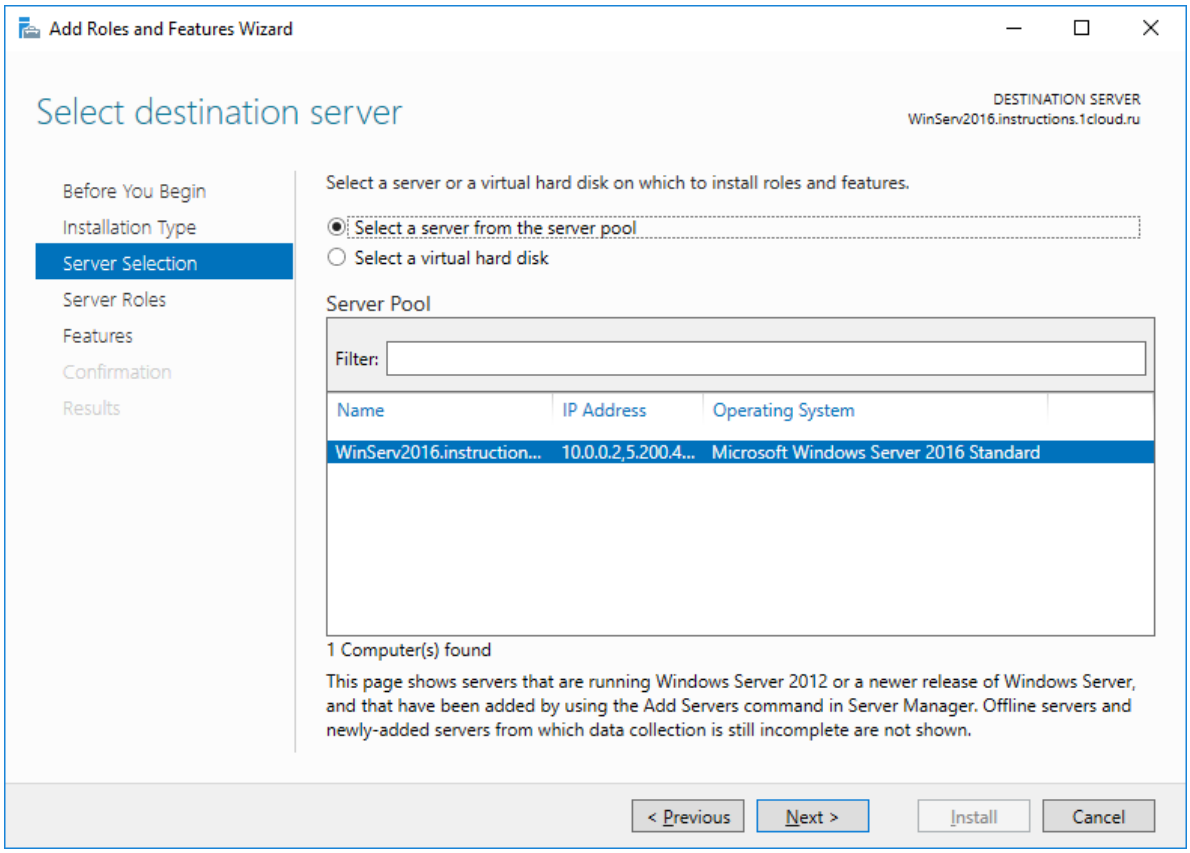
Откройте **Диспетчер серверов** и выберите пункт **Add roles and features**.



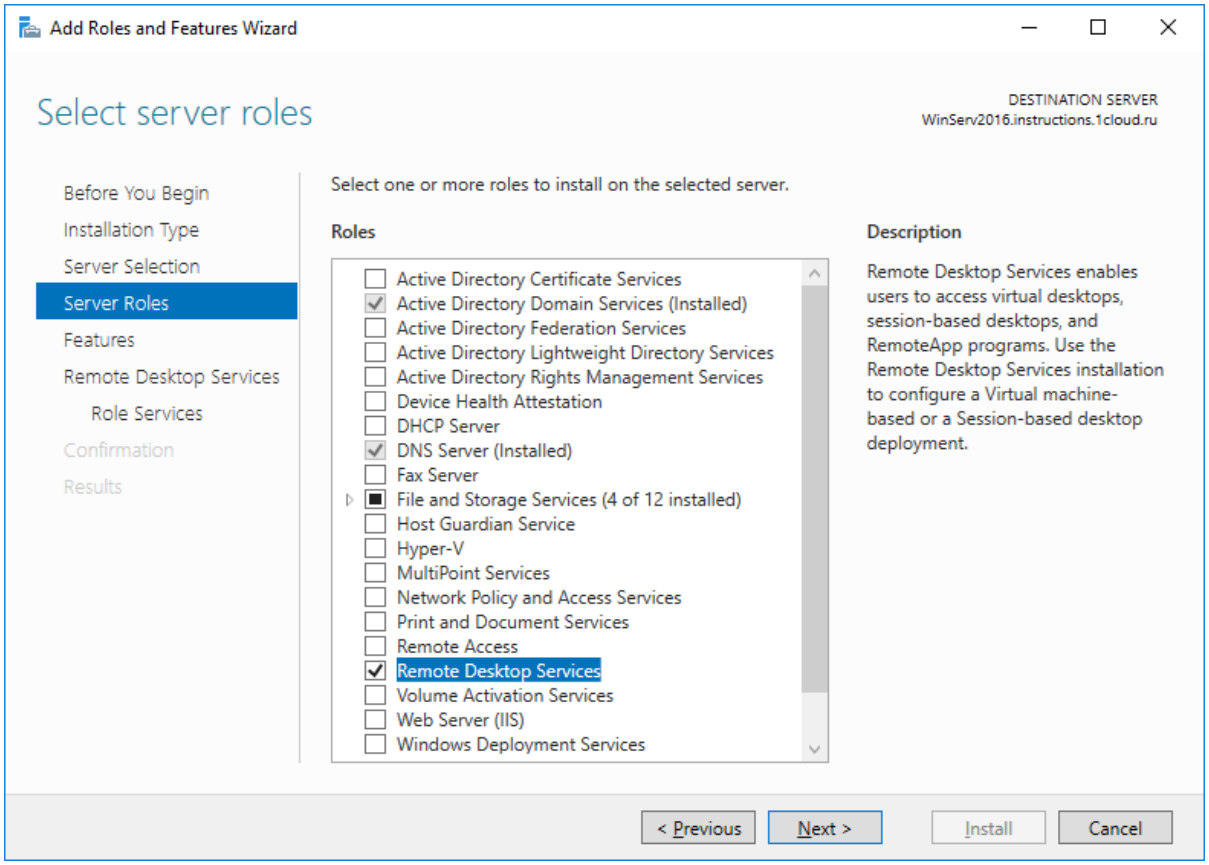
В качестве типа установки укажите **Role-based or feature-based installation**.



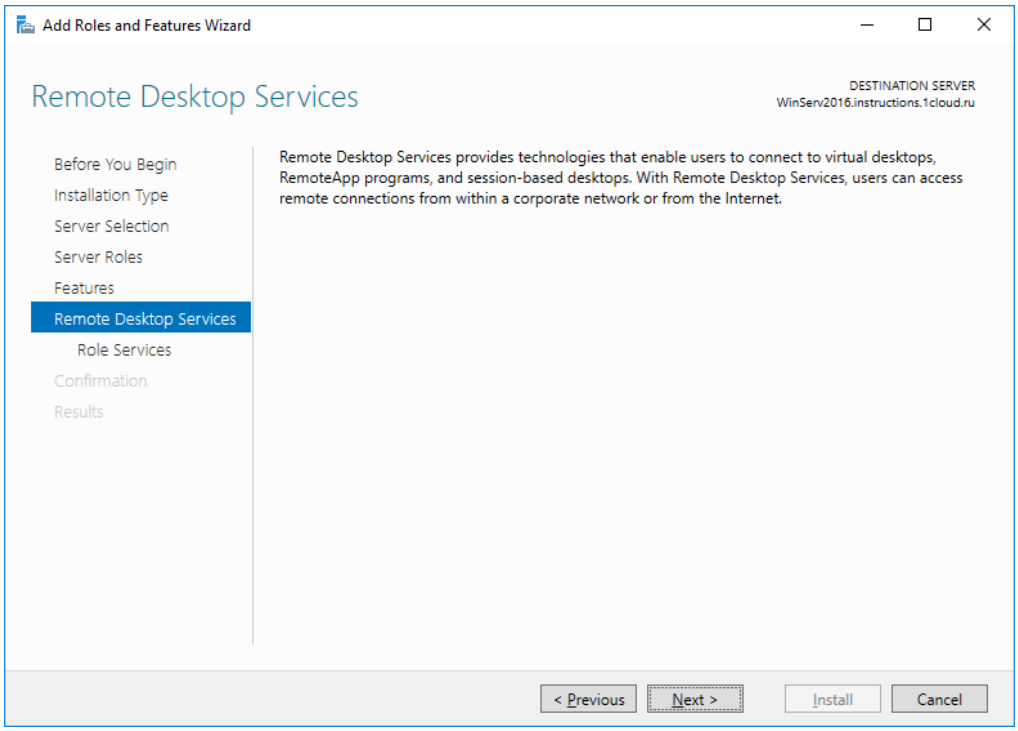
Выберите ваш сервер из пула.



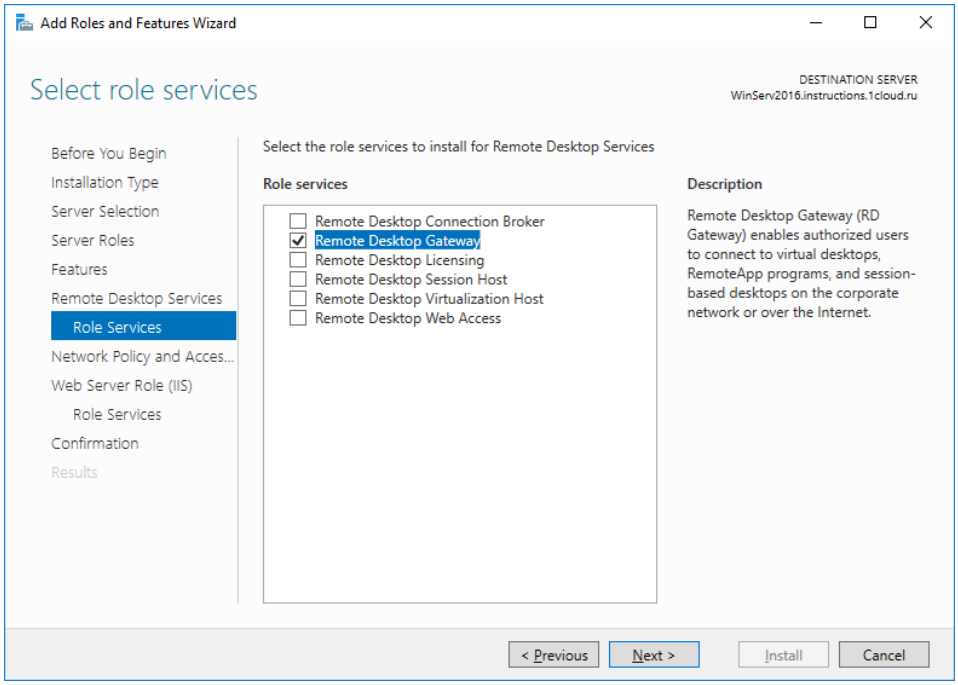
В следующем окне отметьте **Remote Desktop Services**.



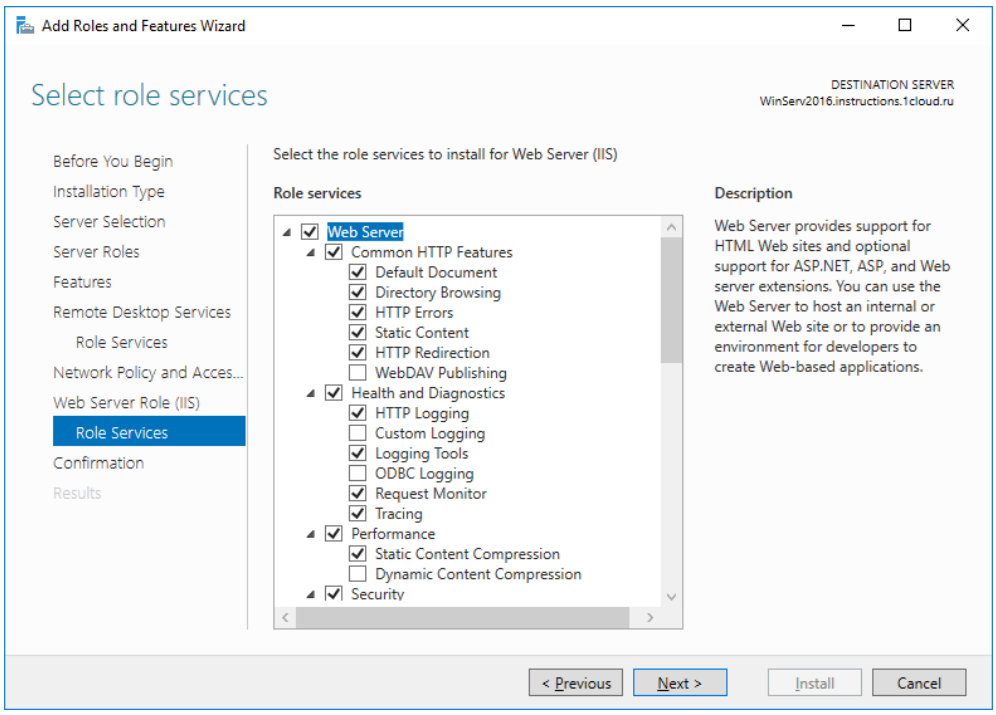
Далее вы увидите краткую информацию о роли.



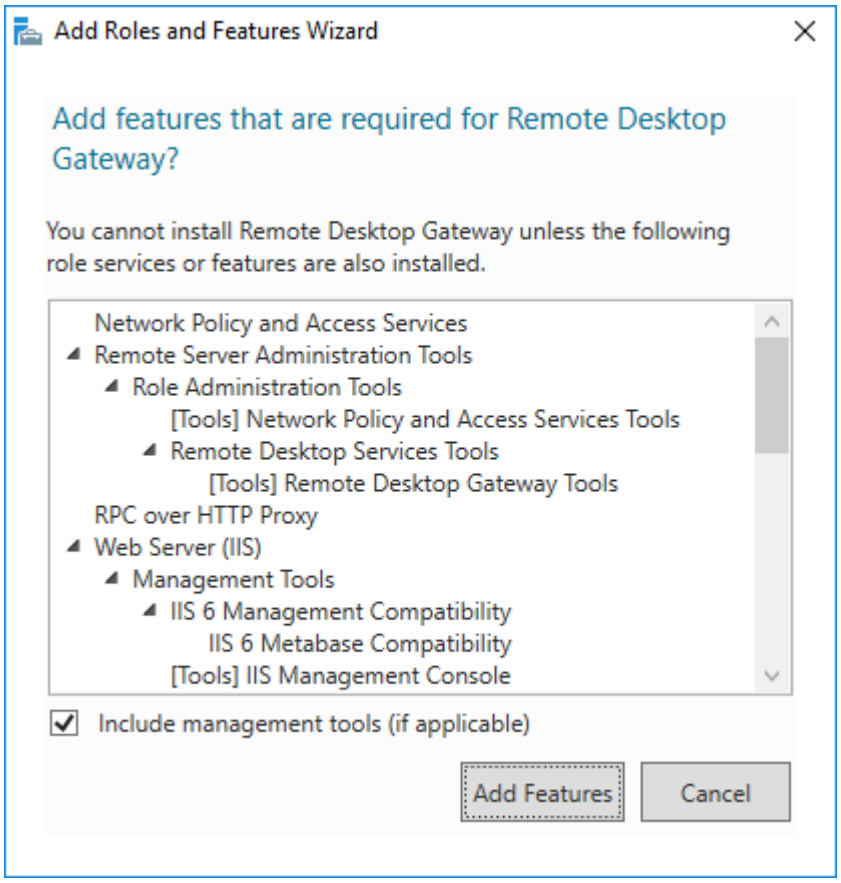
Далее добавьте сервис **Remote Desktop Gateway**.



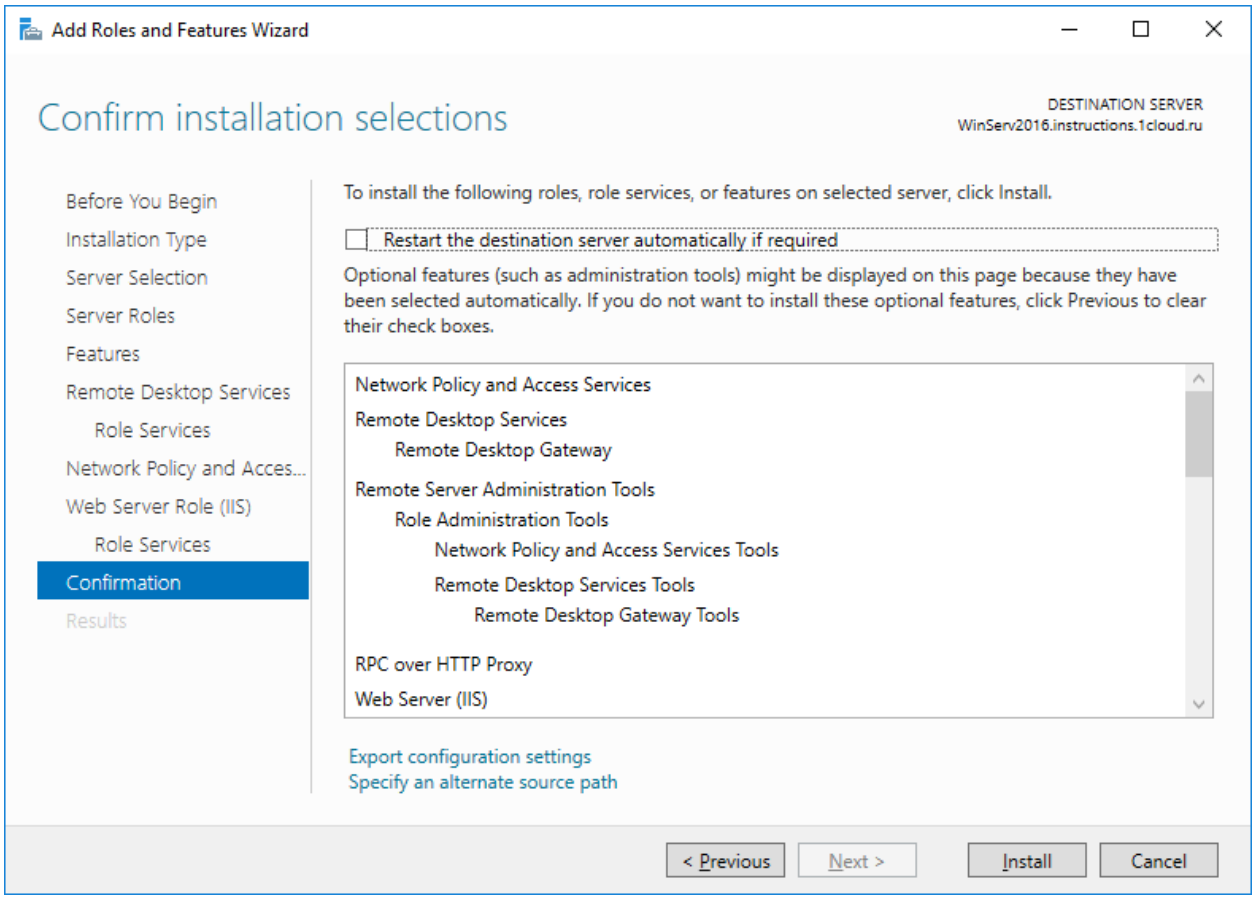
Для работы этого сервиса необходимо веб-сервер IIS и дополнительные административные инструменты, они будут предложены автоматически, если не были установлены ранее.



Добавьте данные функции.

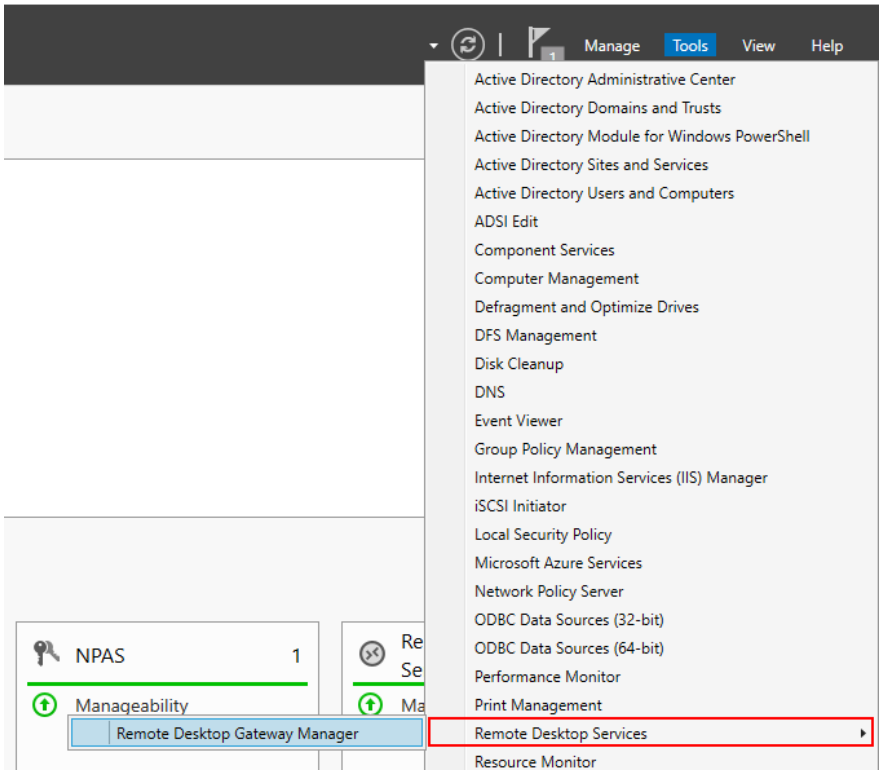


Установите все выбранные компоненты на VPS с помощью кнопки **Install**.

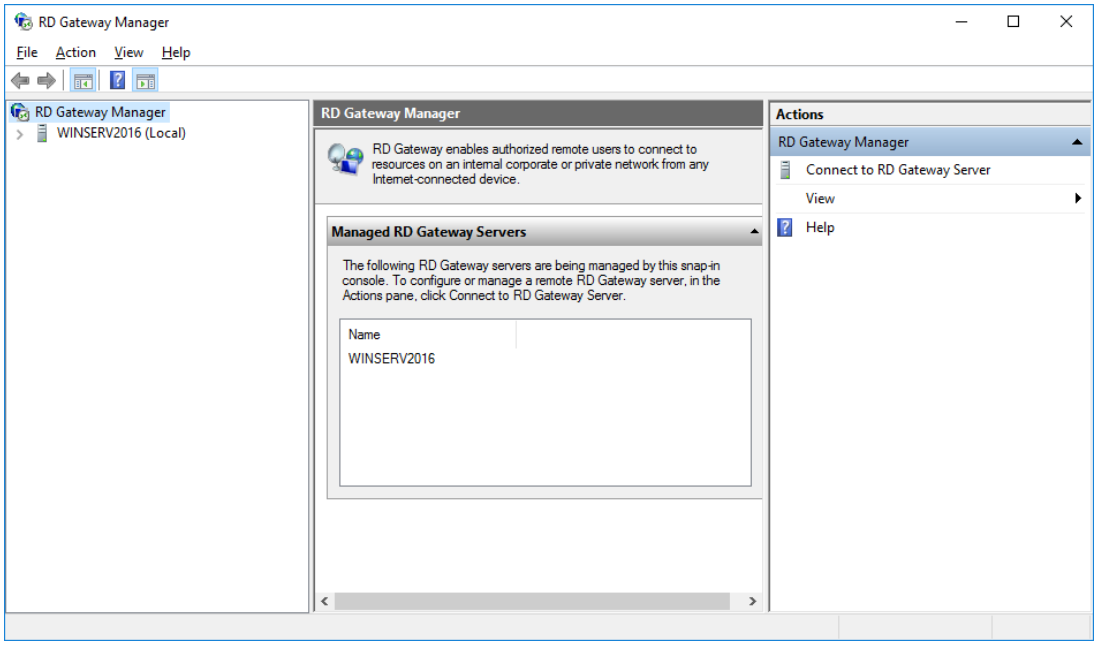


Создание политики авторизации подключения и ресурсов

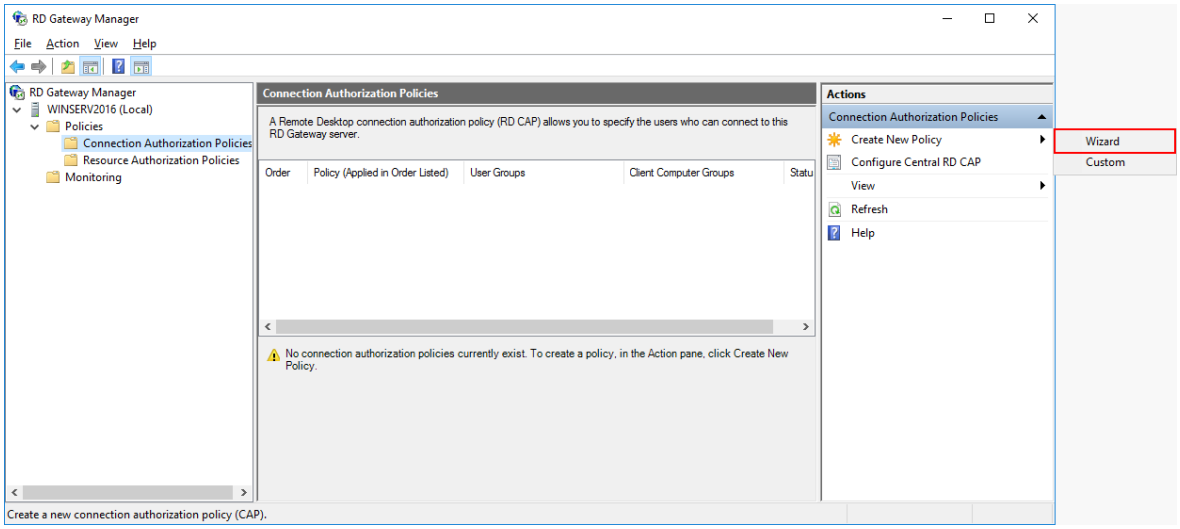
Чтобы открыть Remote Desktop Gateway Manager, в **Диспетчере серверов** выберите Tools и в открывшемся списке **Remote Desktop Services → Remote Desktop Gateway Manager**.



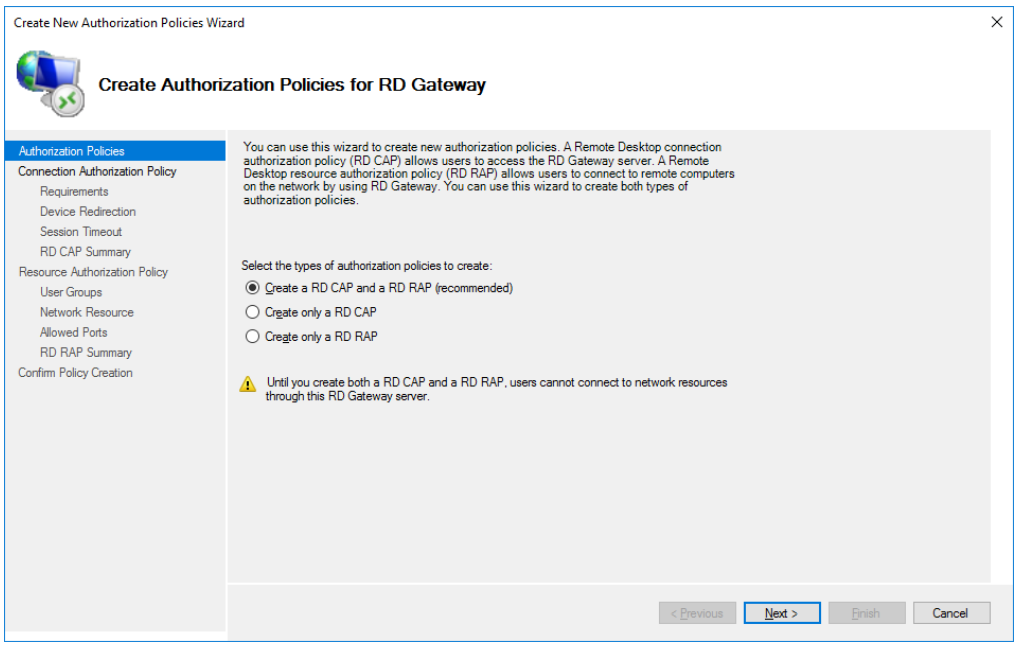
Перед вами откроется менеджер шлюза.



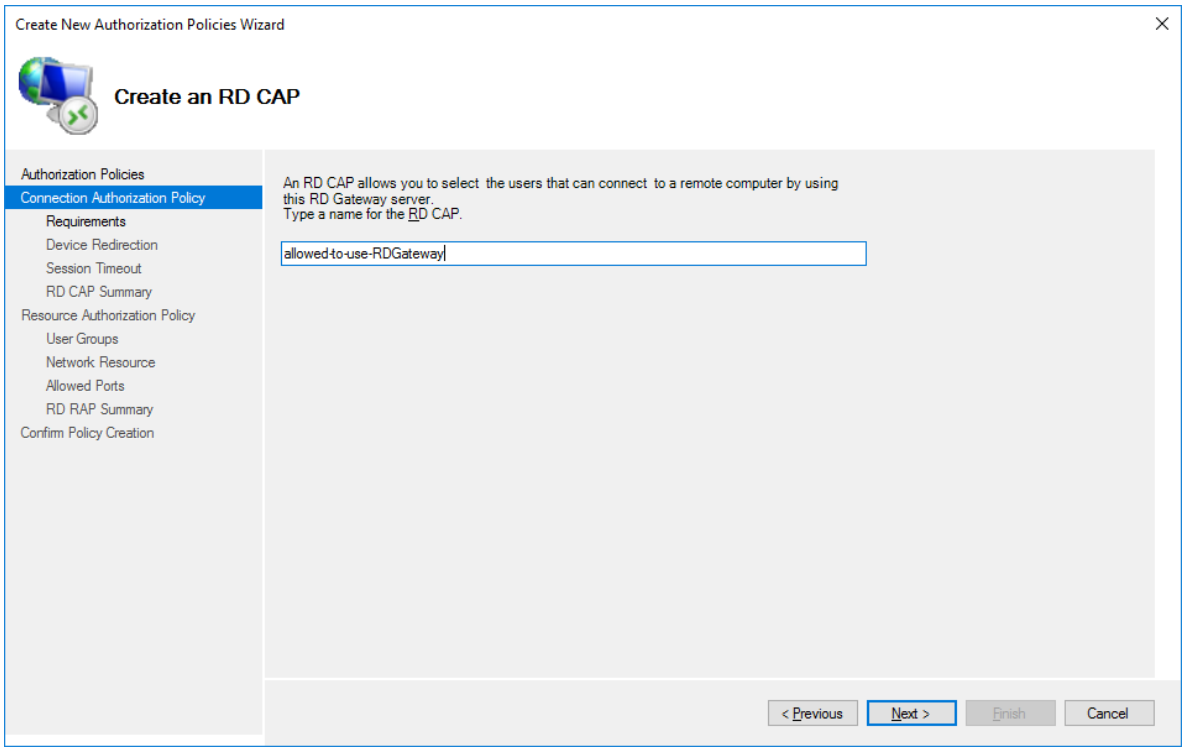
Для создания политик авторизации в древовидной структуре откройте **RD Gateway Manager → <Имя сервера> → Policies → Connection Authorization Policies**. В вертикальном меню Actions справа выберите **Create New Policy → Wizard**.



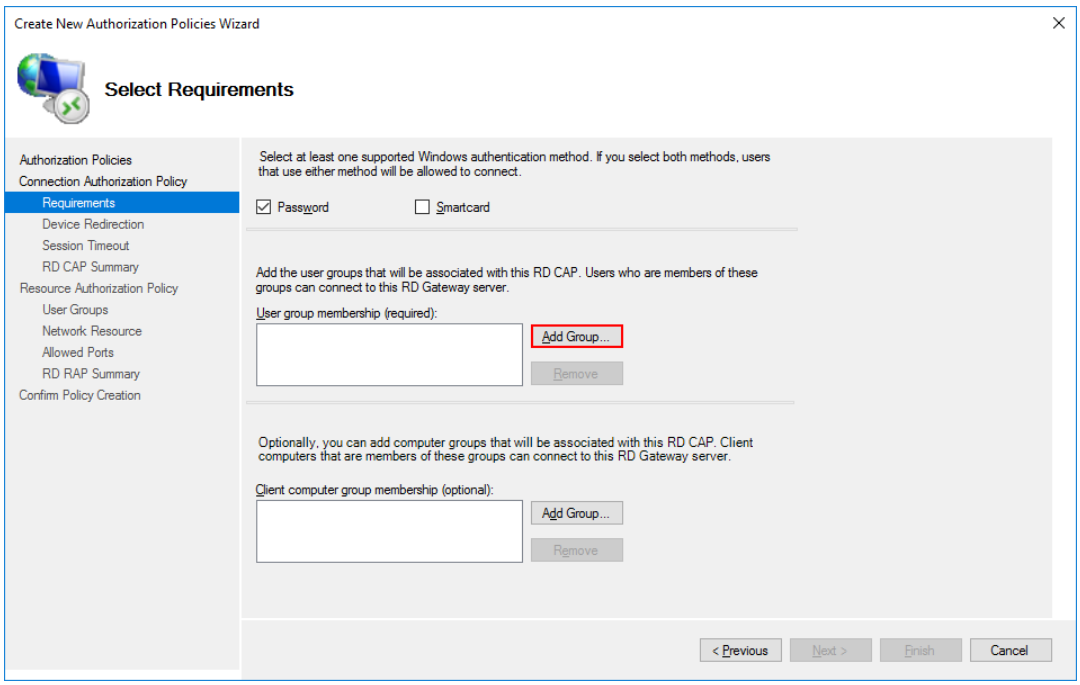
В открывшемся окне выберите Create RD CAP and RD RAP (recommended), чтобы с помощью одного процесса настроить обе политики.



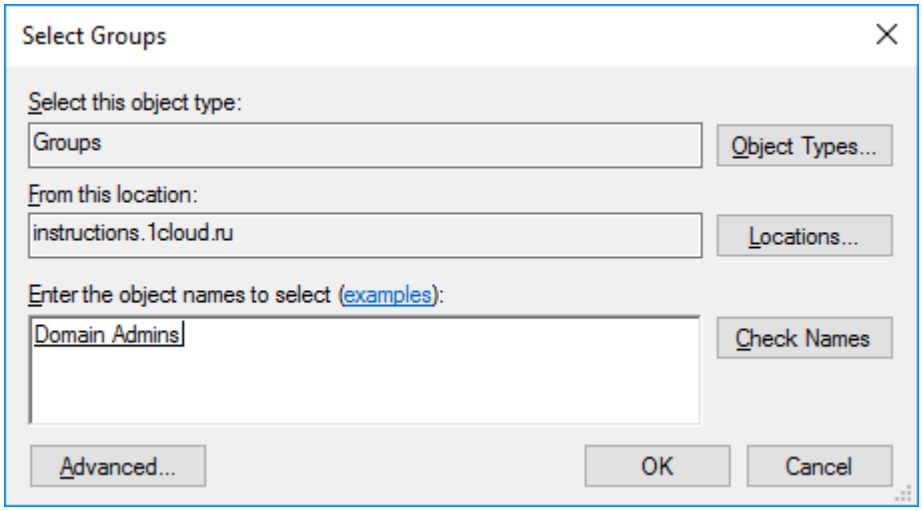
Введите удобное имя для политики авторизации подключения.



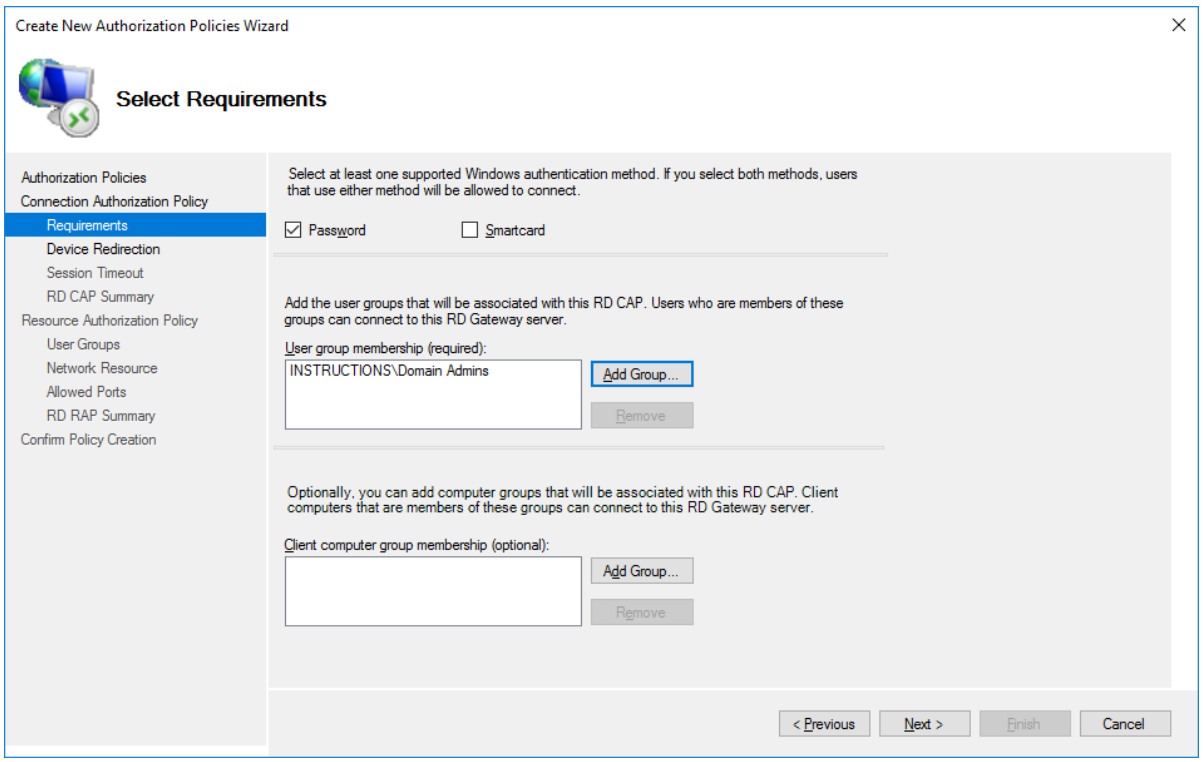
На следующем шаге выберите наиболее удобный метод аутентификации: пароль или smartcard. Далее добавьте группы пользователей которые смогут подключаться к этому RD Gateway серверу, для это нажмите **Add Group**.



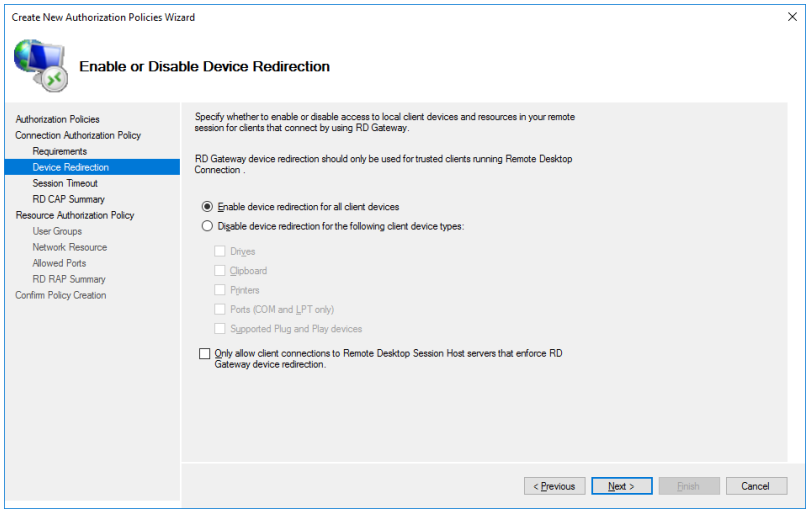
Выберите нужную группу, например администраторов домена или контроллеры домена. Выполнить поиск можно с помощью кнопки **Check Names**.



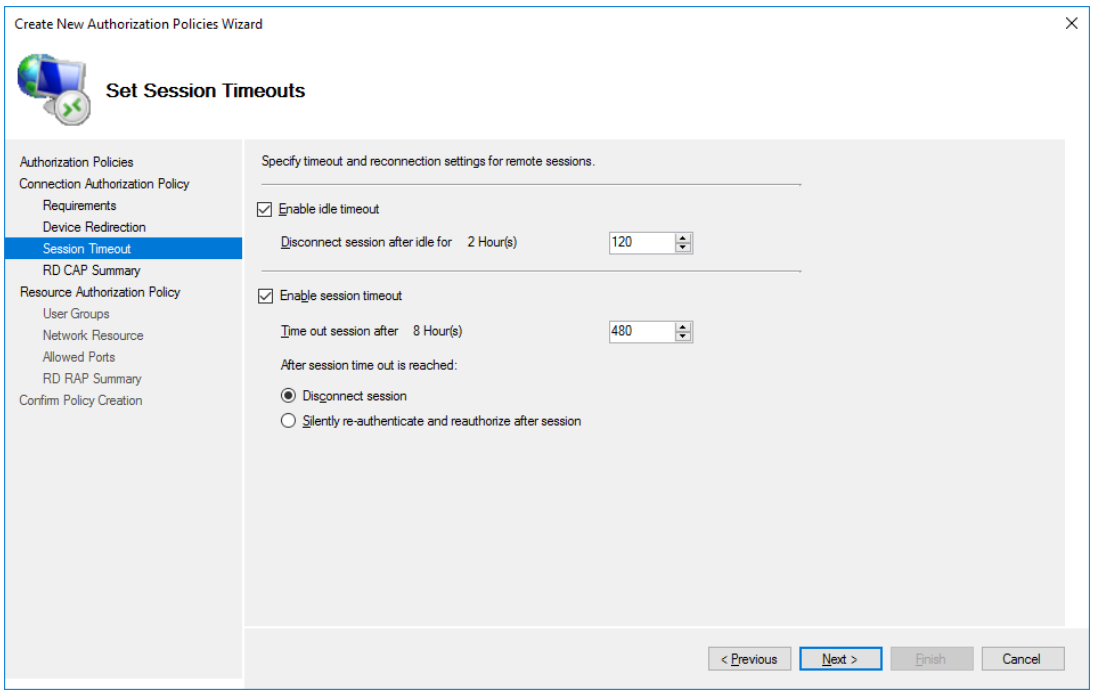
После добавления групп можно переходить к следующему действию.



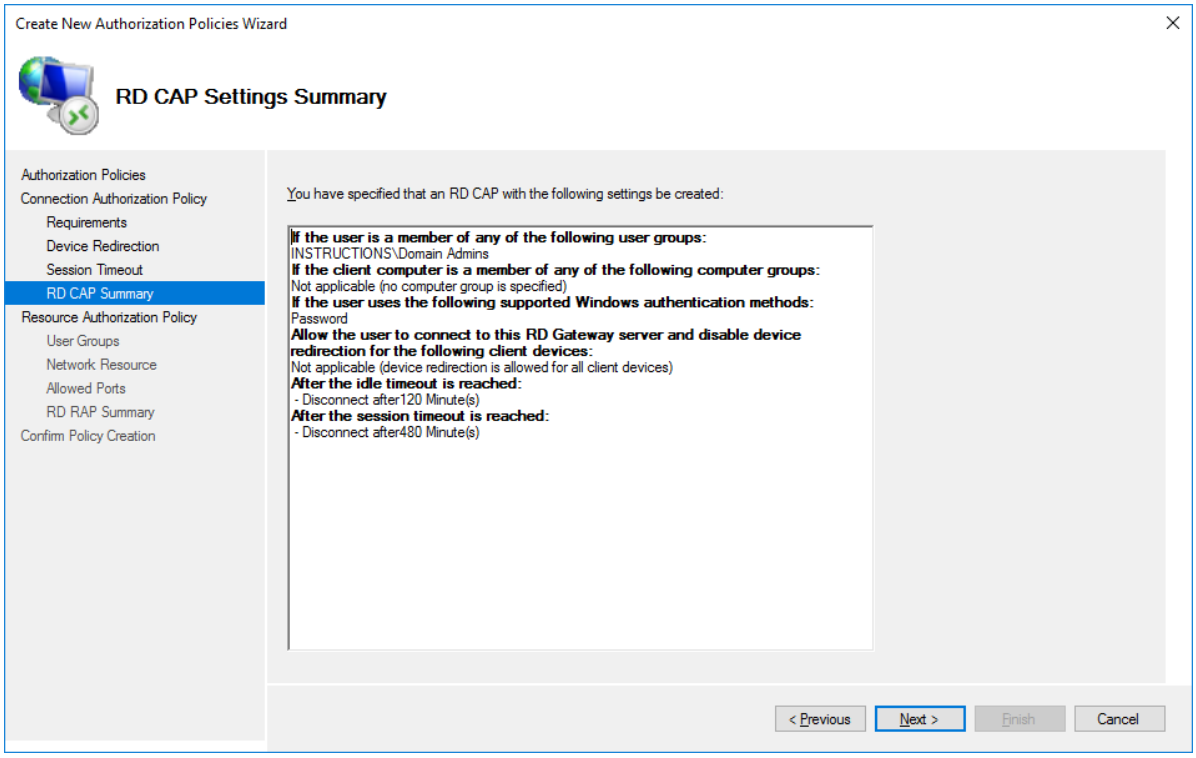
Выберите устройства и ресурсы удаленной сессии, которые будут доступны клиентам использующие шлюз.



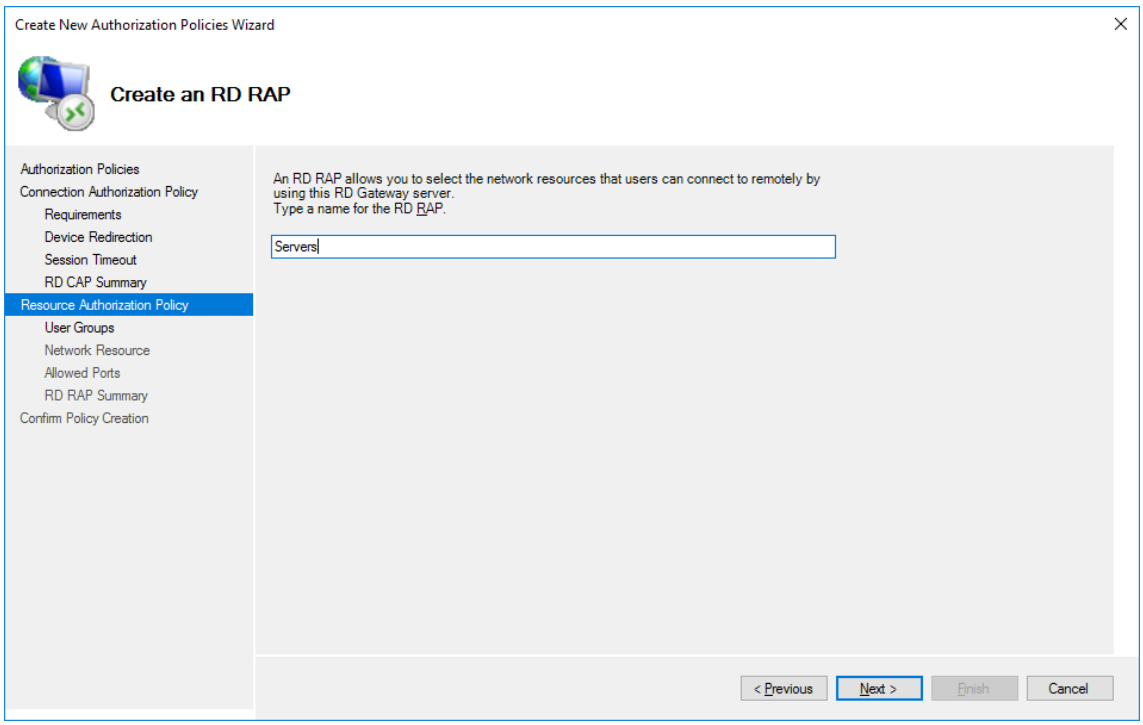
Выберите нужные для вас значения таймаутов: времени простоя и времени работы сессии.



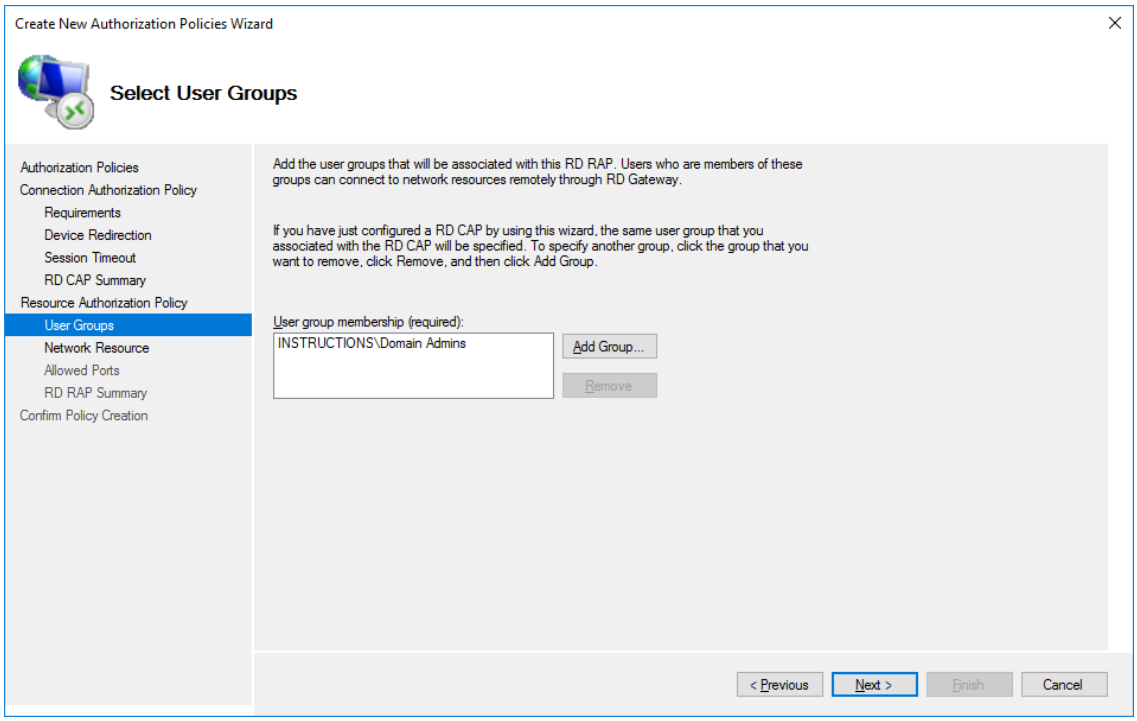
Перепроверьте выбранные настройки.



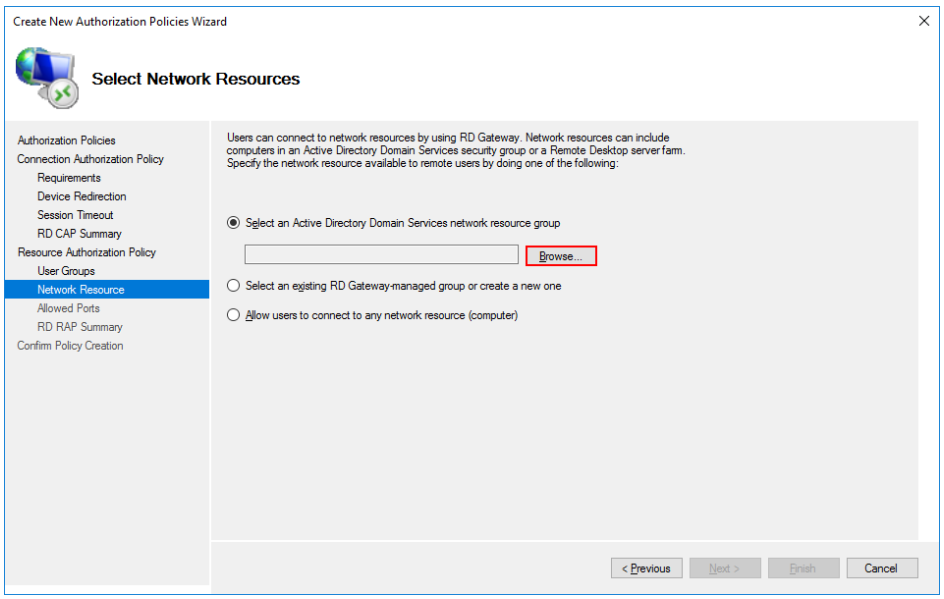
Далее вы перейдете к настройке политики авторизации ресурсов. Введите удобное имя политики.



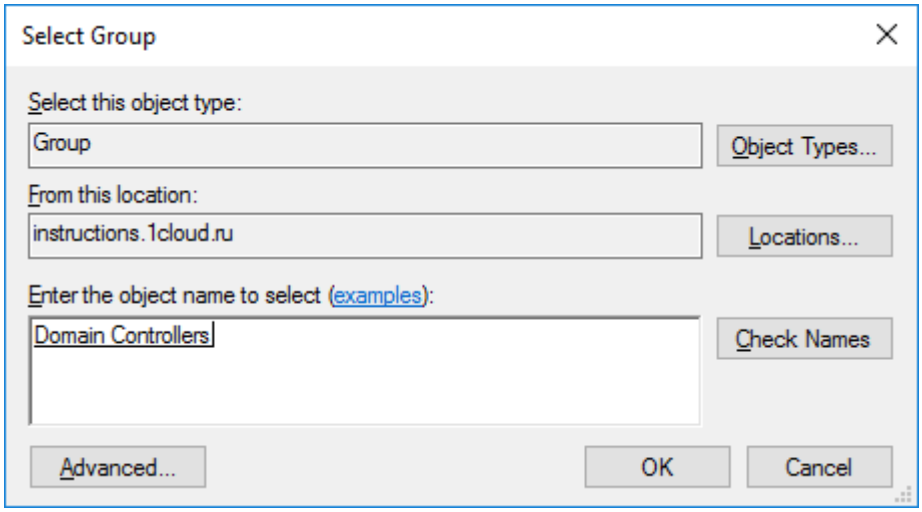
Также добавьте группы пользователей, которые смогут подключаться к сетевым ресурсам.



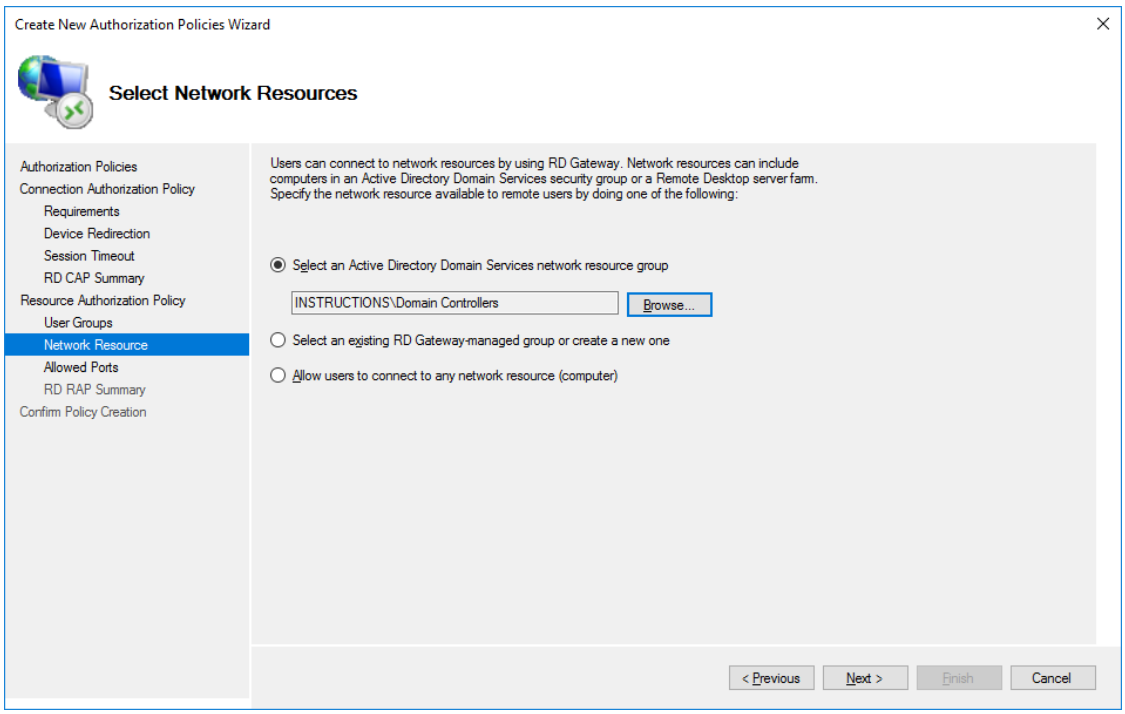
Выберите группу, содержащую серверы, на которых указанные группы пользователей могли бы работать с удаленным рабочим столом. Для этого нажмите **Browse**.



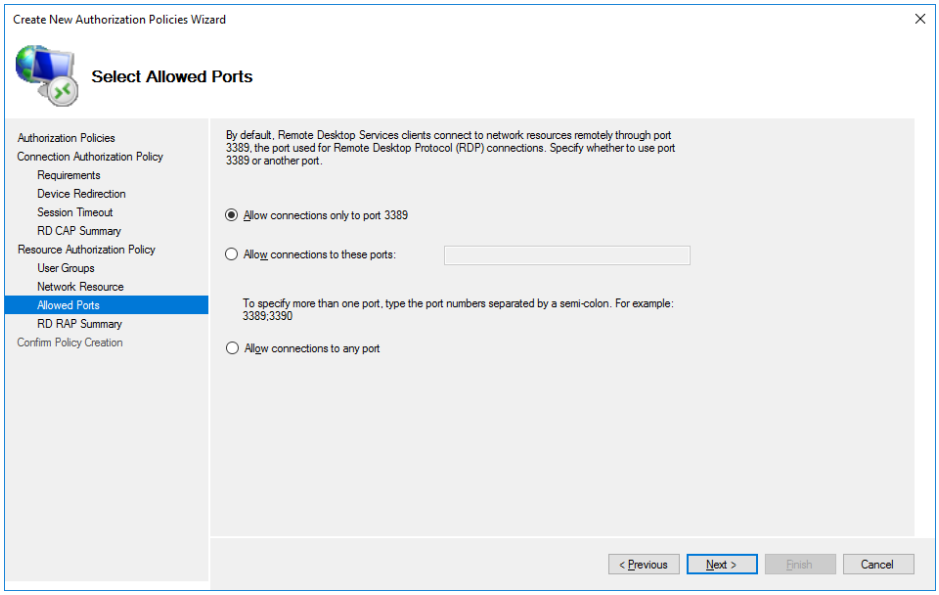
В этом примере используется встроенная группа под названием Domain Controllers. Вы можете создавать дополнительные группы, содержащие серверы, которые связаны или принадлежат к определенным отделам или сотрудникам. Таким образом, на предыдущих шагах вы можете назначать группы на основе потребностей пользователей и разрешать им доступ только к определенным серверам.



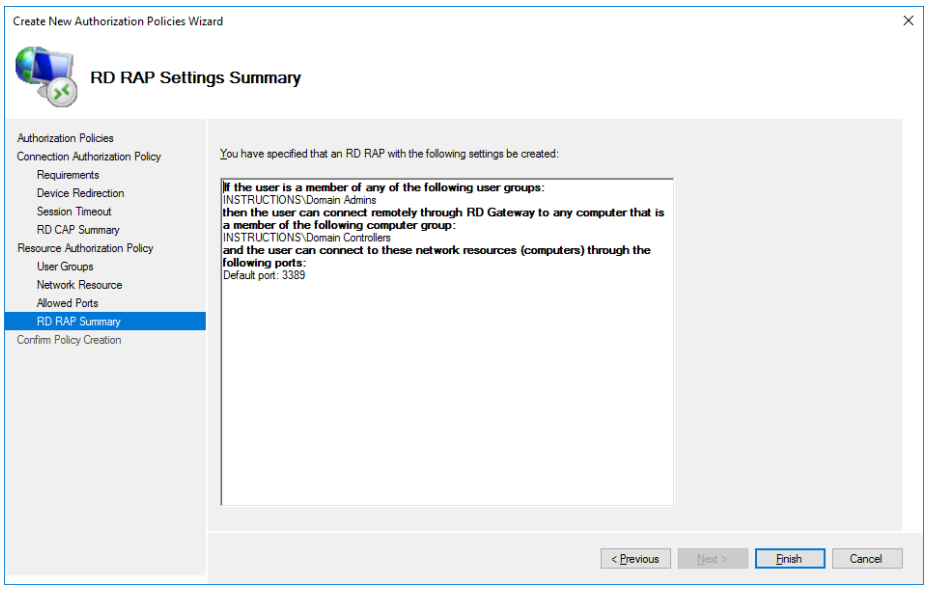
Убедитесь, что добавлена нужная группа.



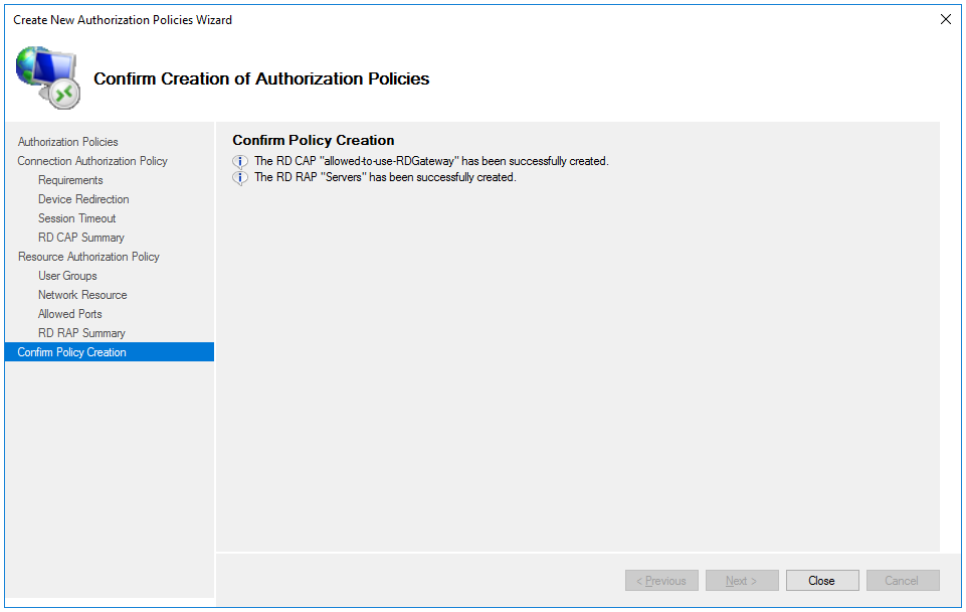
Если порт по умолчанию удаленного рабочего стола на серверах был изменен, используйте эту страницу для указания порта. В противном случае выберите разрешение подключения только к порту 3389.



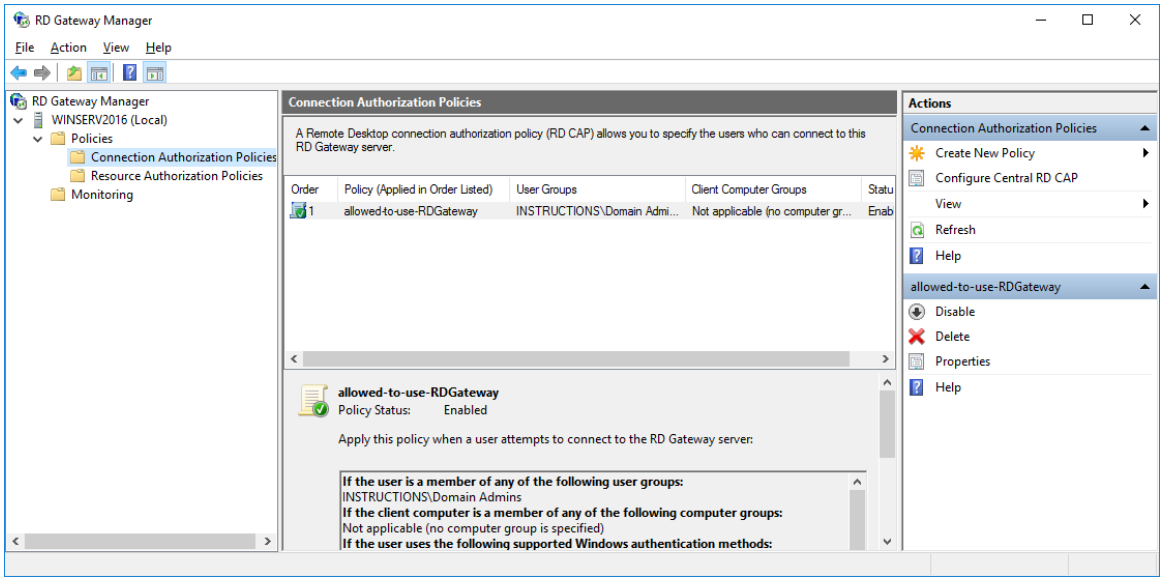
Проверьте указанные настройки для политики.



Далее отобразится результат создания политик.

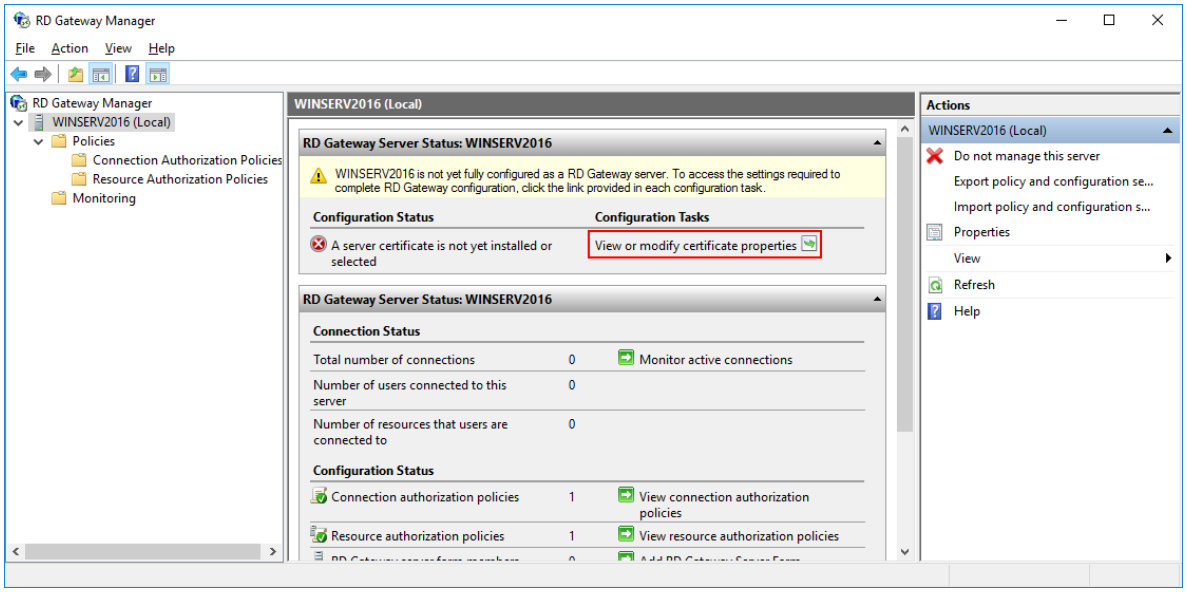


После создания политик менеджер будет выглядеть следующим образом.



Установка SSL-сертификата

Для шлюза удаленного рабочего стола должен быть установлен SSL-сертификат. Чтобы установить SSL-сертификат, щелкните имя сервера удаленного рабочего стола в консоли управления удаленным рабочим столом и выберите **View or modify certificate properties**.



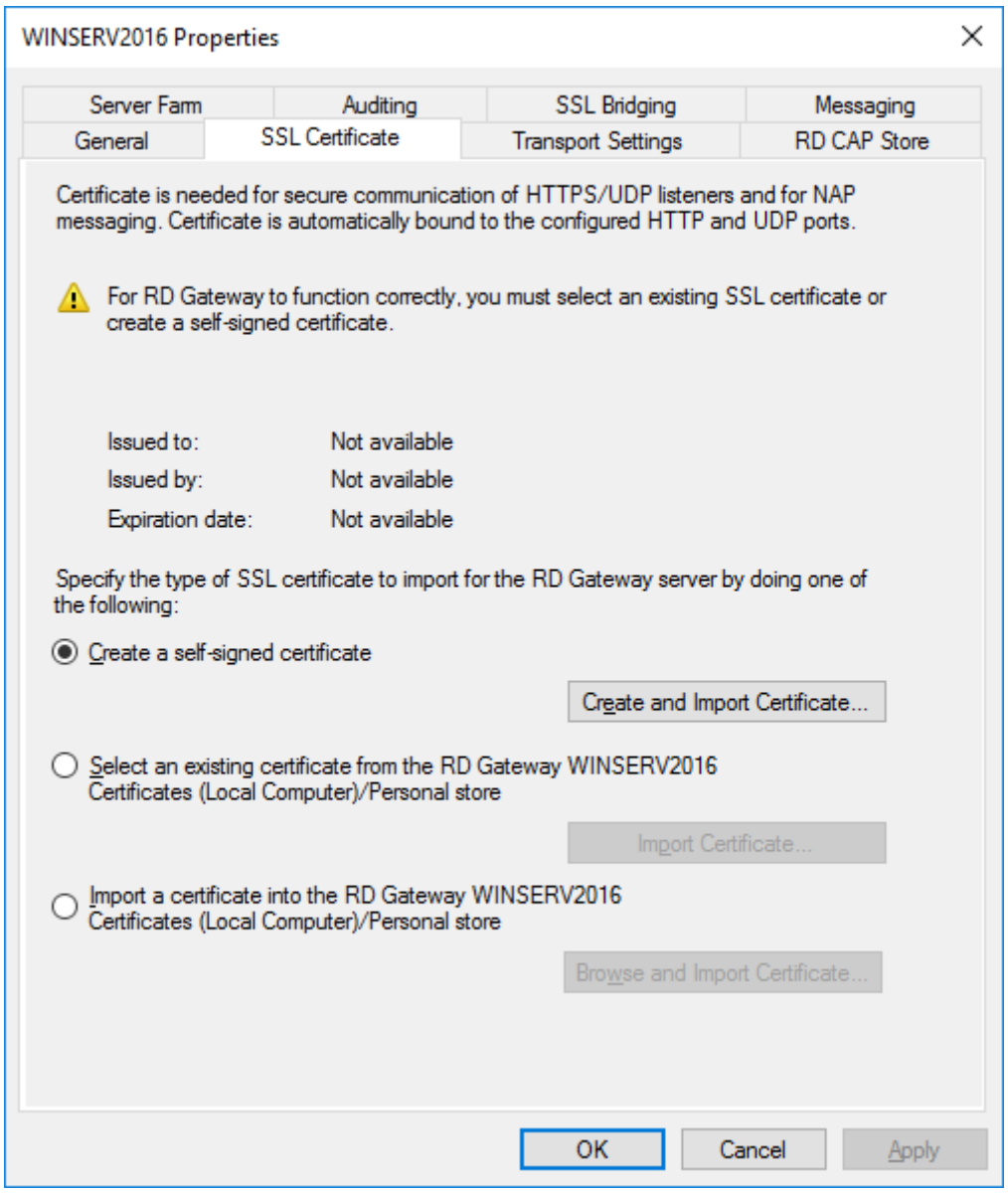
Возможно 3 способа импорта сертификатов:

создание самоподписанного сертификата и его импорт;

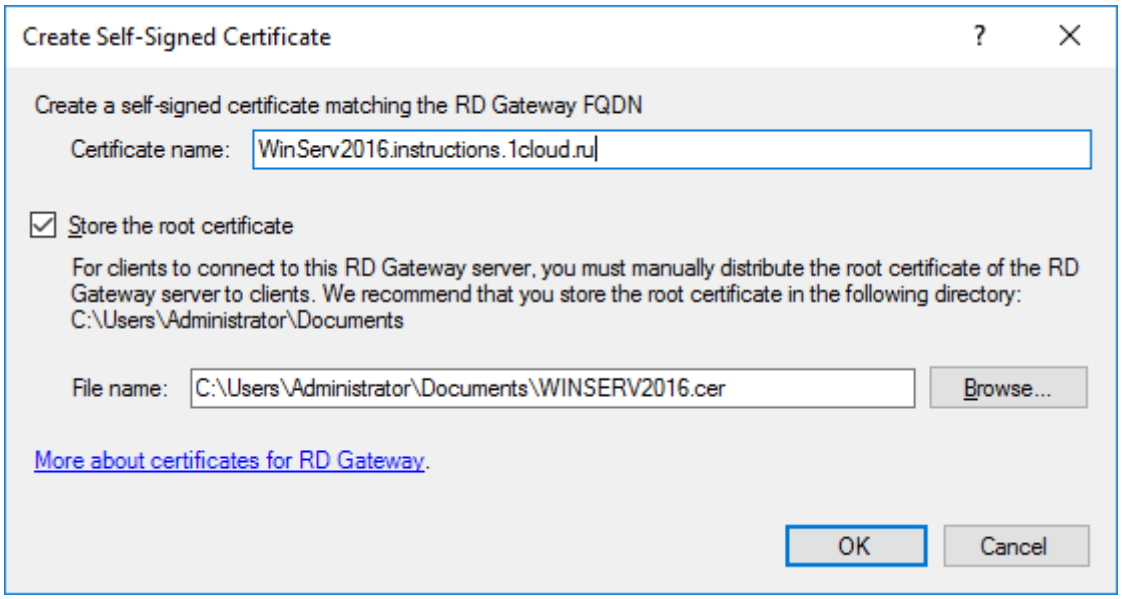
импорт ранее загруженного сертификата (самоподписанного или стороннего);

загрузка стороннего сертификата (например, Comodo) и его импорт;

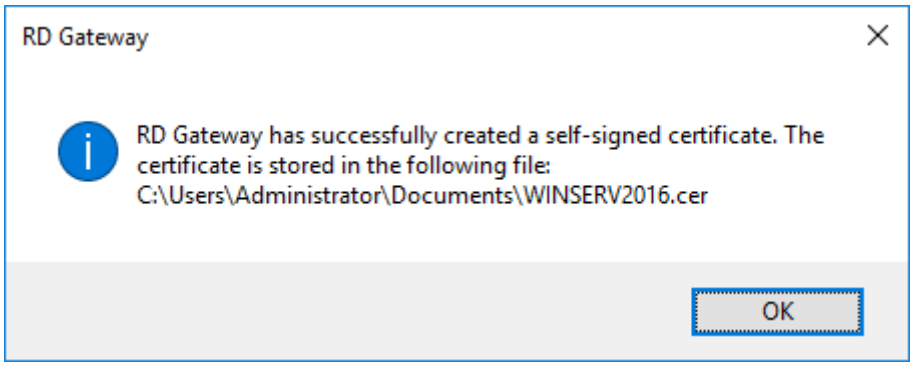
Выберите подходящий вам способ, в нашем примере мы рассмотрим первый случай с генерацией и импортом самоподписанного сертификата.



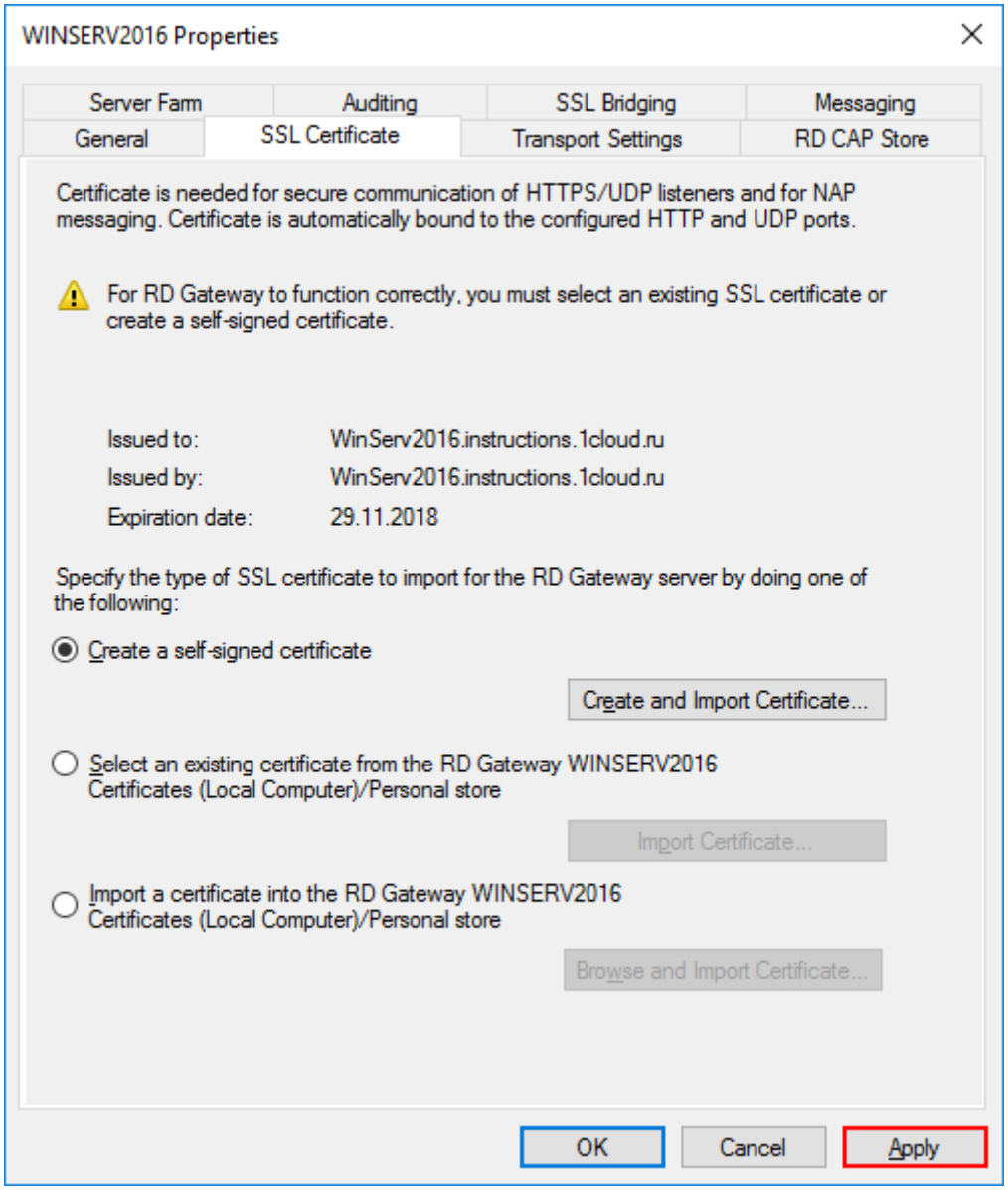
Введите имя сертификата и его расположение на сервере. Нажмите OK.



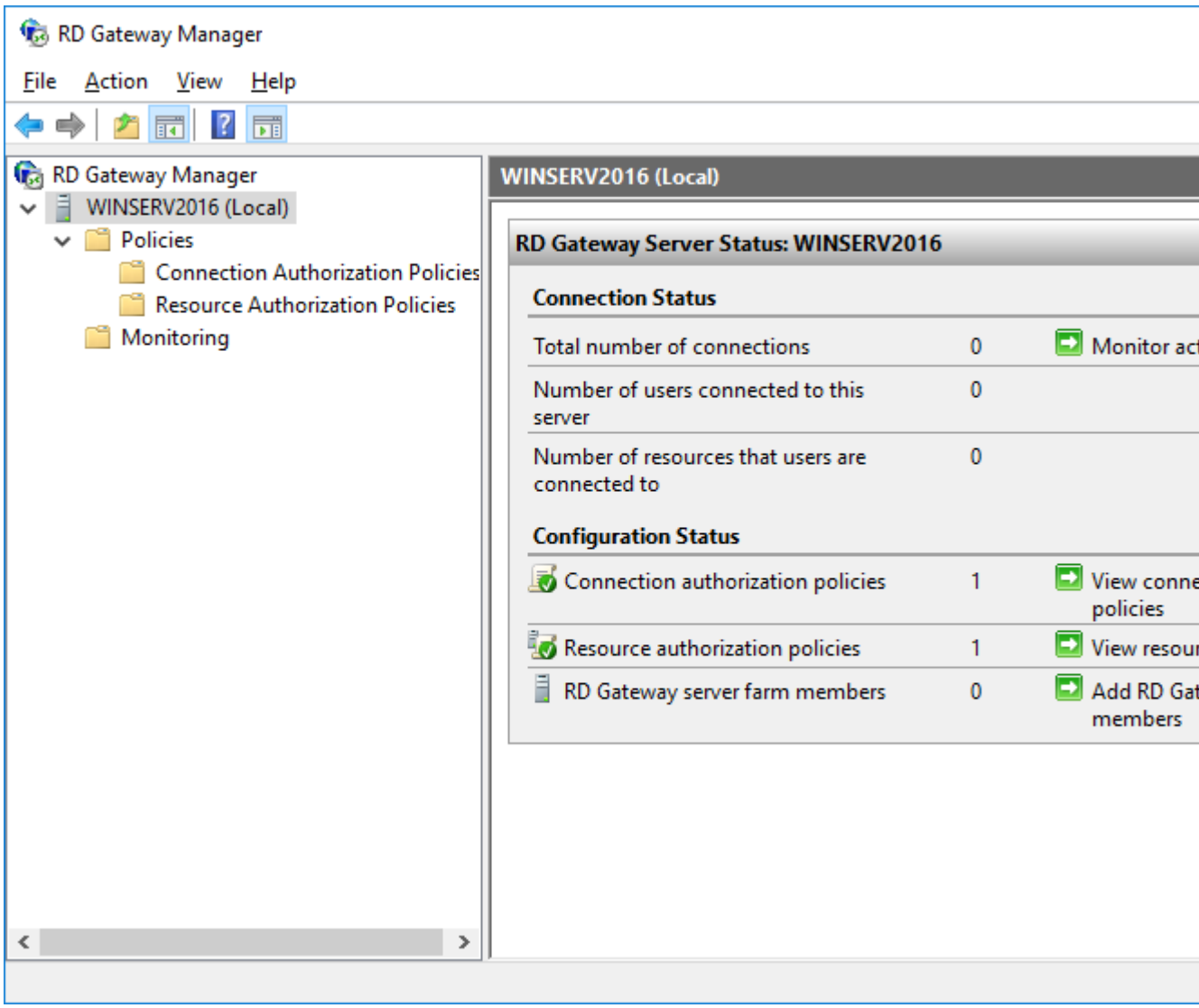
Сертификат будет сгенерирован.



В результате отобразится - кому, кем и до какого числа выдан ssl-сертификат. Нажмите Apply для сохранения изменений.

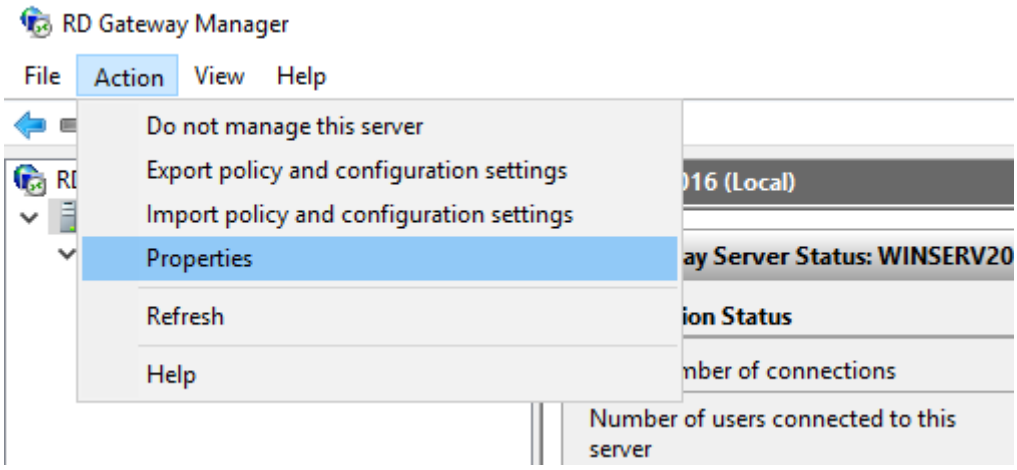


Теперь самоподписанный SSL-сертификат успешно установлен на TCP-порт 443 (порт SSL по умолчанию).

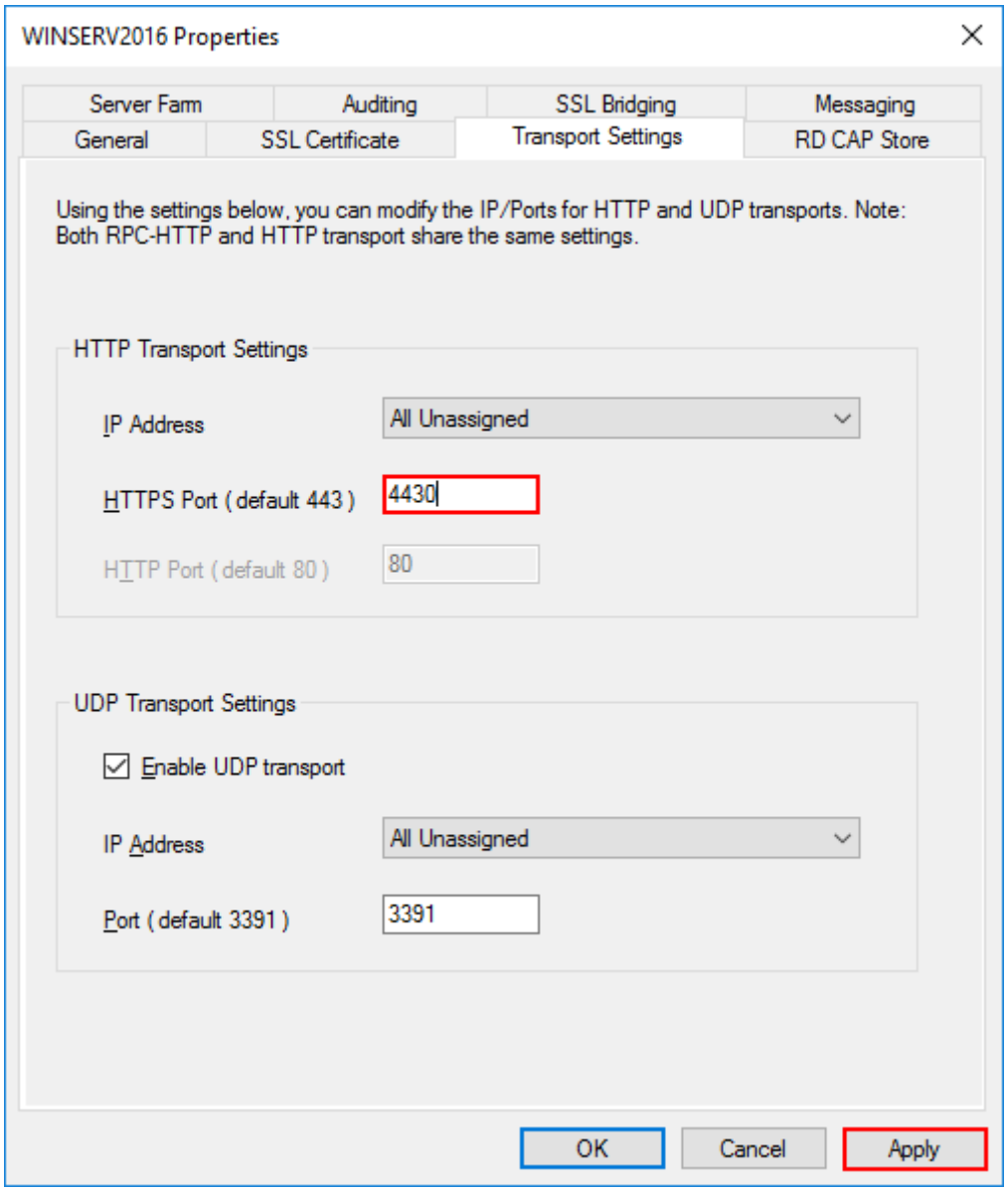


В целях безопасности рекомендуется изменить порт SSL для шлюза удаленных рабочих столов на другой номер. Обычно компании делают это, чтобы попытаться обмануть хакеров, которые могут ориентироваться на стандартный порт 443.

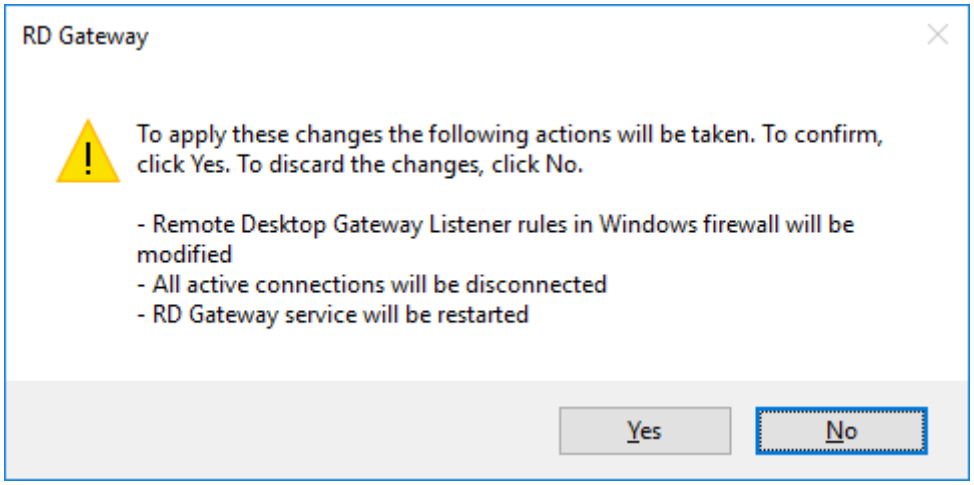
Чтобы изменить номер порта для шлюза RD, щелкните правой кнопкой мыши имя сервера и выберите свойства в консоли управления удаленным рабочим столом (Action →Properties).



Измените значение HTTP-порта на любое удобное значение и сохраните изменения.

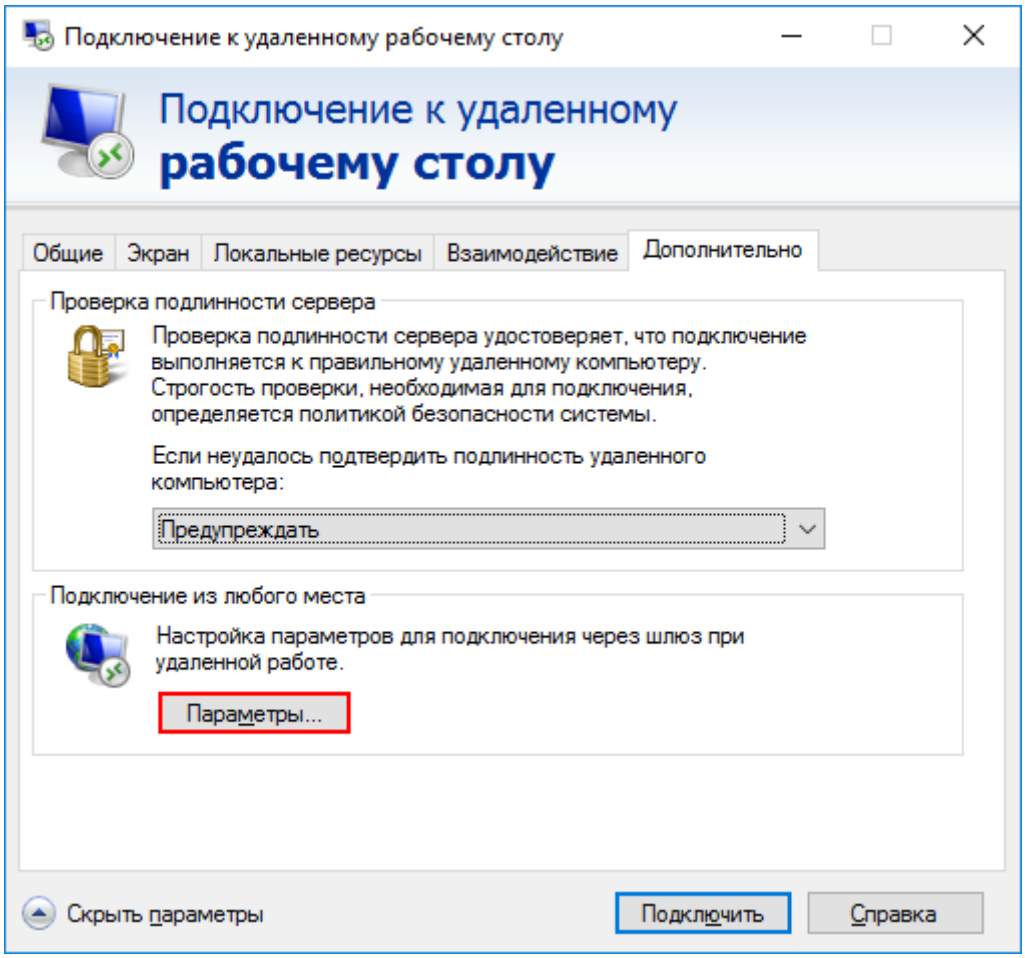


Подтвердите изменения, нажав **Yes**.

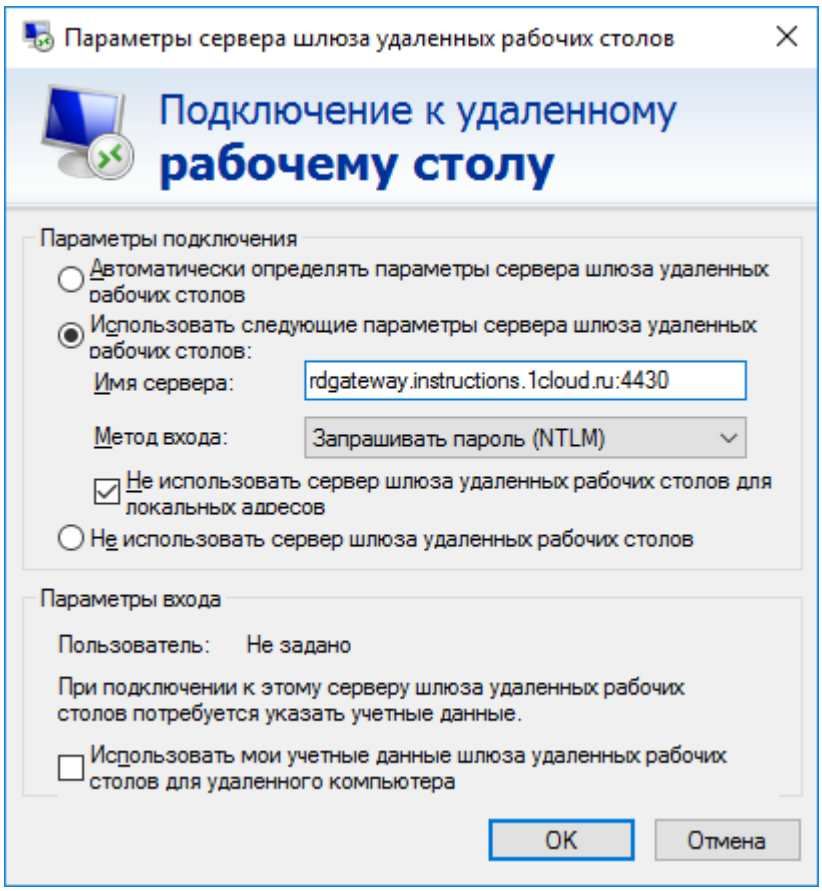


Подключение через шлюз

Для подключения откройте стандартное приложение Windows **Подключение к удаленному рабочему столу** (mstsc.exe). На вкладке **Дополнительно** нажмите на кнопку **Параметры**.

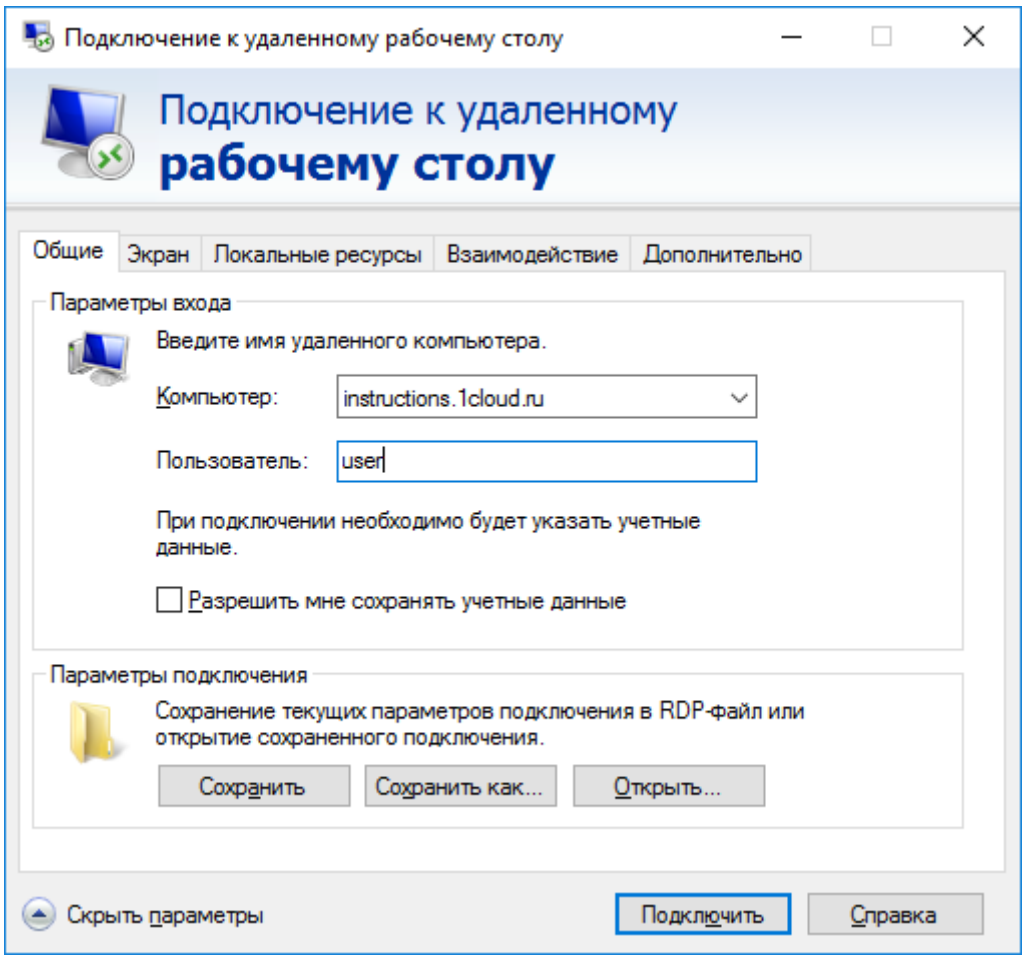


В открывшемся окне выберите Использовать следующие параметры сервера шлюза удаленных рабочих столов. Введите имя сервера в следующем формате и нажмите OK: rdgateway.<ваш домен>:<порт>

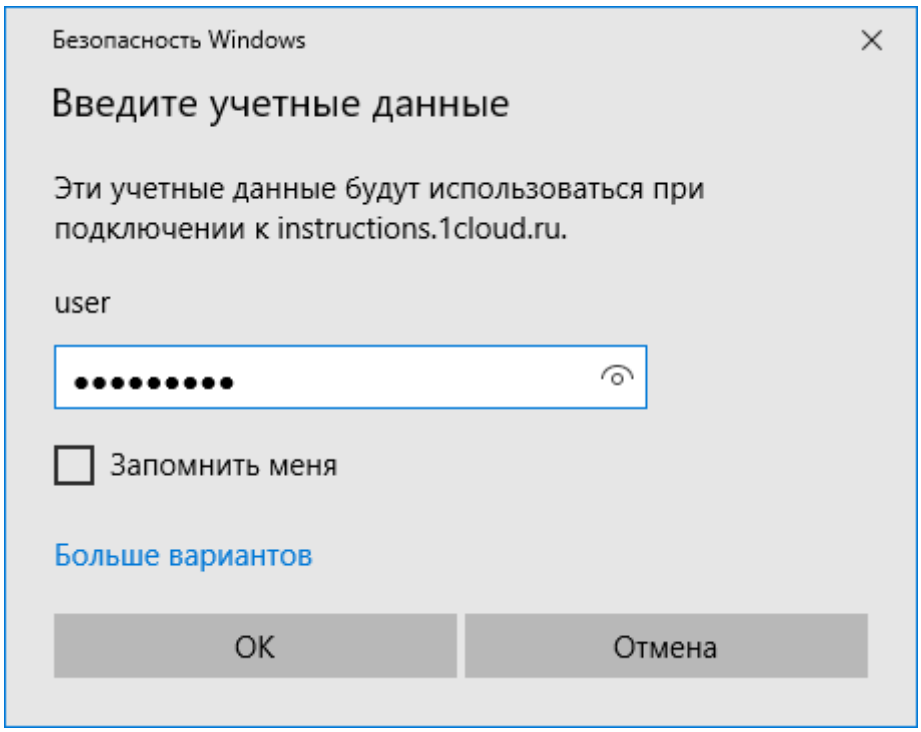


На вкладке **Общие** в поле **Компьютер** введите домен, в поле **Пользователь** имя пользователя и нажмите **Подключить**. При необходимости можете сохранить параметры входа.

Примечание: пользователь должен иметь права подключения через шлюз, которые были настроены ранее.



Введите пароль от учетной записи.



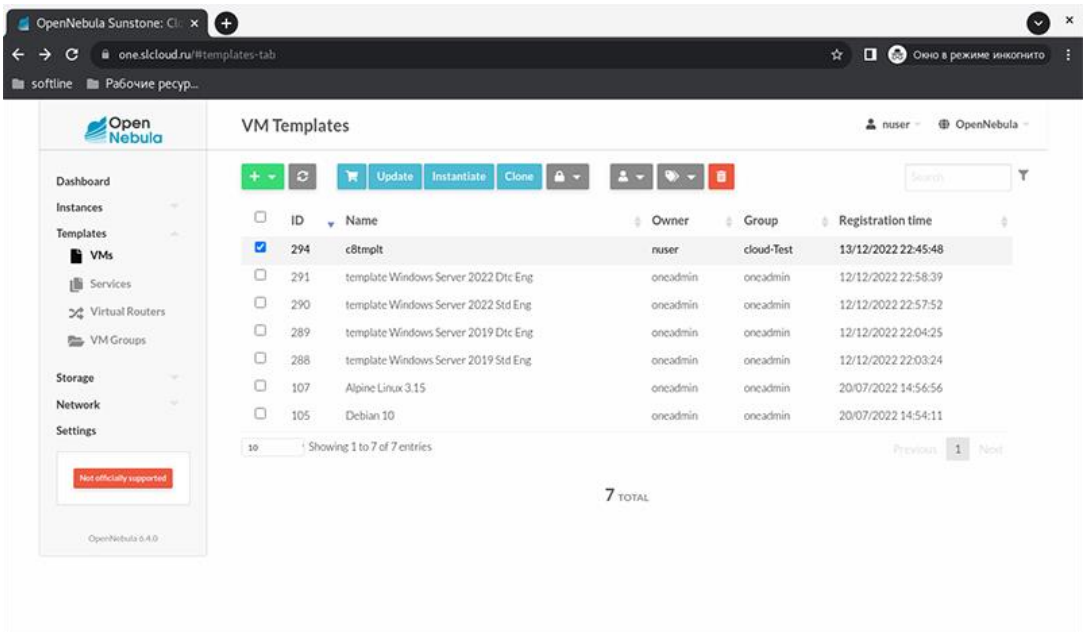
В результате будет произведено подключение к удаленному рабочему столу через шлюз RD Gateway. Это можно проверить с помощью команды tracert:

```
PS C:\Users\user> tracert 1cloud.ru

Tracing route to 1cloud.ru [5.200.50.90]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  5.200.47.1
  2     3 ms     2 ms     8 ms  5.200.46.254
  3    12 ms    <1 ms    <1 ms  fw-5-200-46-220.it-grad.ru [5.200.46.220]
  4     1 ms    <1 ms    <1 ms  5.200.50.90

Trace complete.
```

Практическая работа № 15 Работа с Облачными бизнес-моделями IaaS: Установка.

Задание:

На странице **Templates > VMs** в списке доступных шаблонов выберите созданный на предыдущем шаге и нажмите **Instantiate**.



Страница параметров ВМ

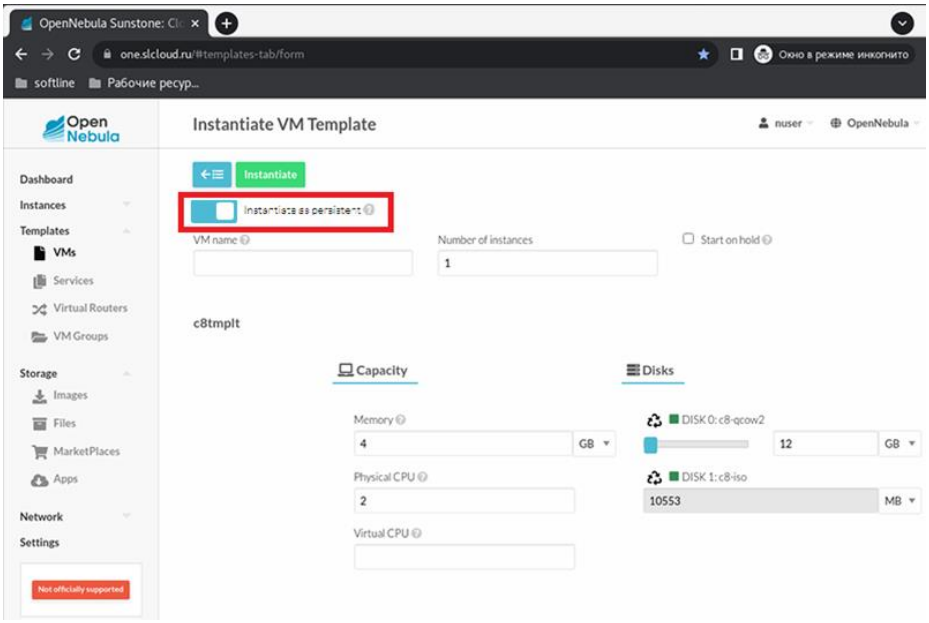
На странице создания ВМ **обязательно включите параметр «Instantiate as persistent».**

Заполните поля:

VM name – укажите имя ВМ.

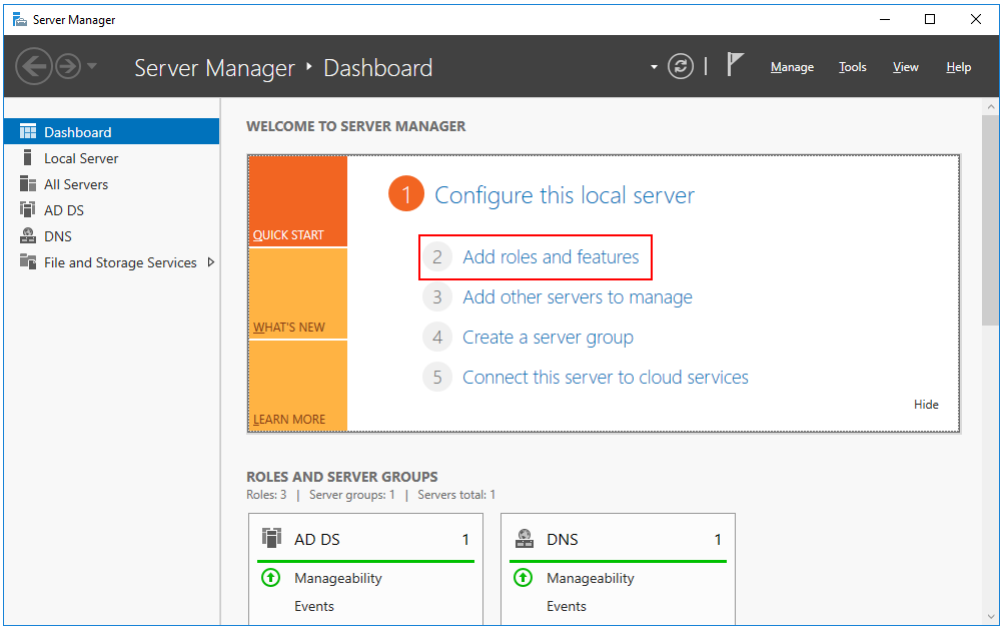
Memory – укажите объём RAM.

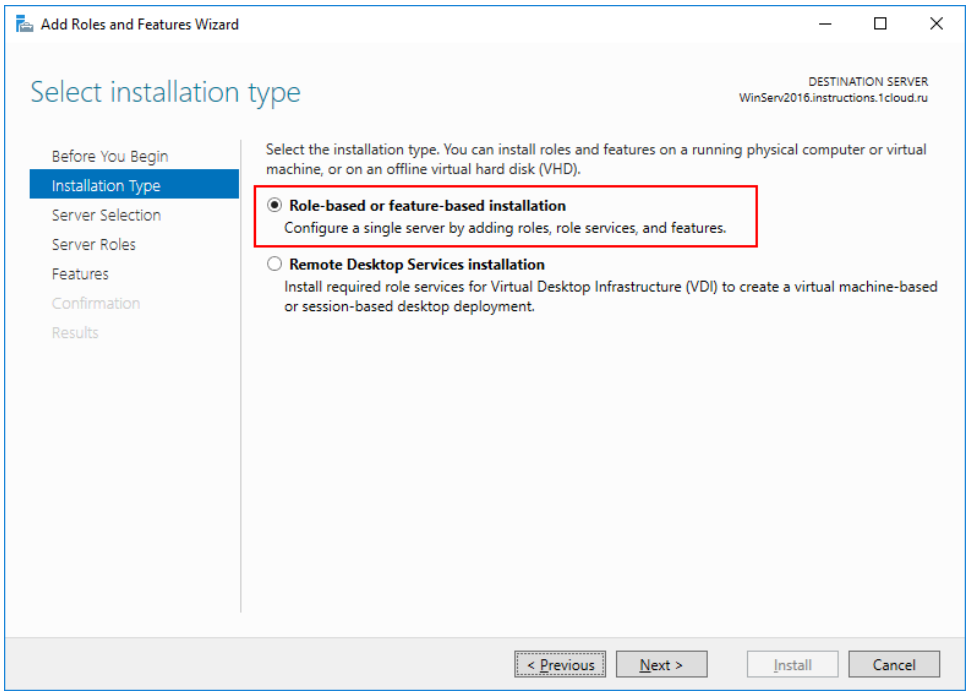
Physical CPU, Virtual CPU – укажите количество CPU. Рекомендуется указывать значение Physical CPU равное Virtual CPU. Если вы хотите сэкономить ресурсы, то для тестовых и маловажных ВМ можно указать значение Physical CPU меньше, чем Virtual CPU.

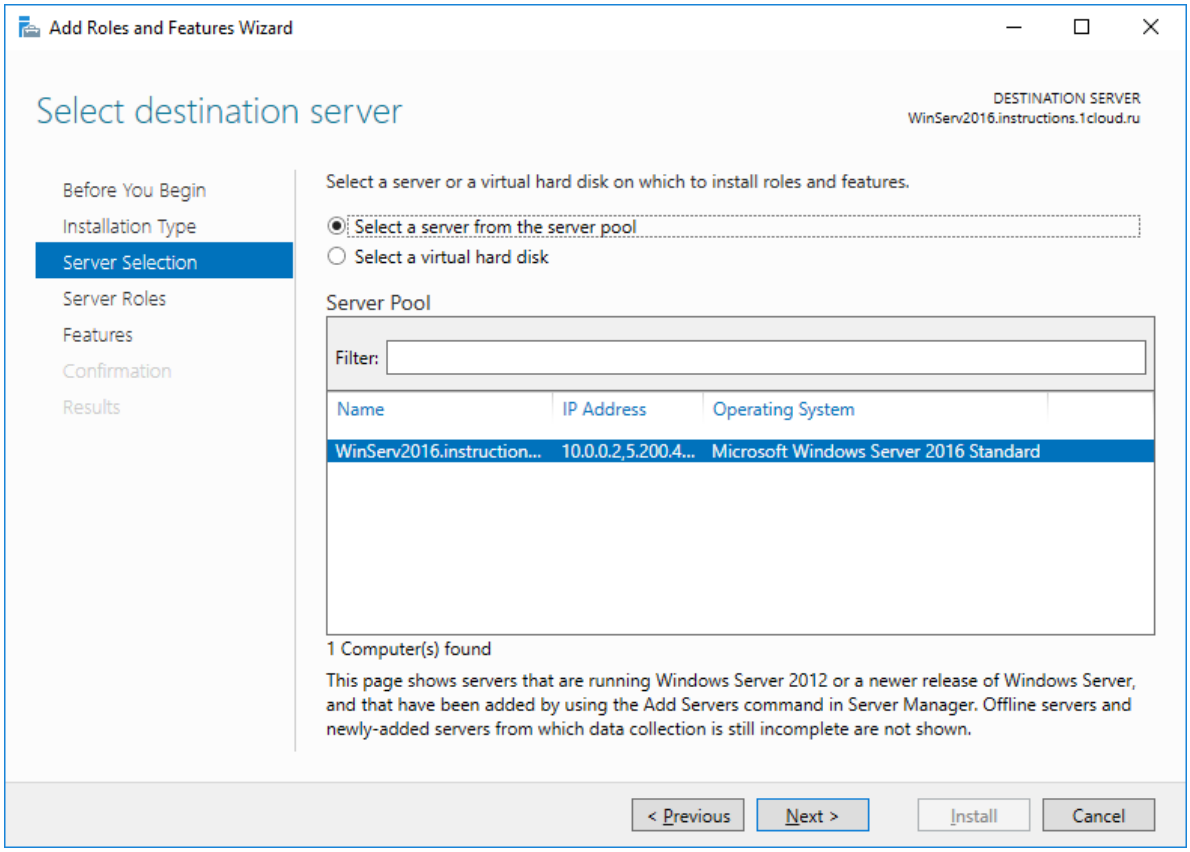


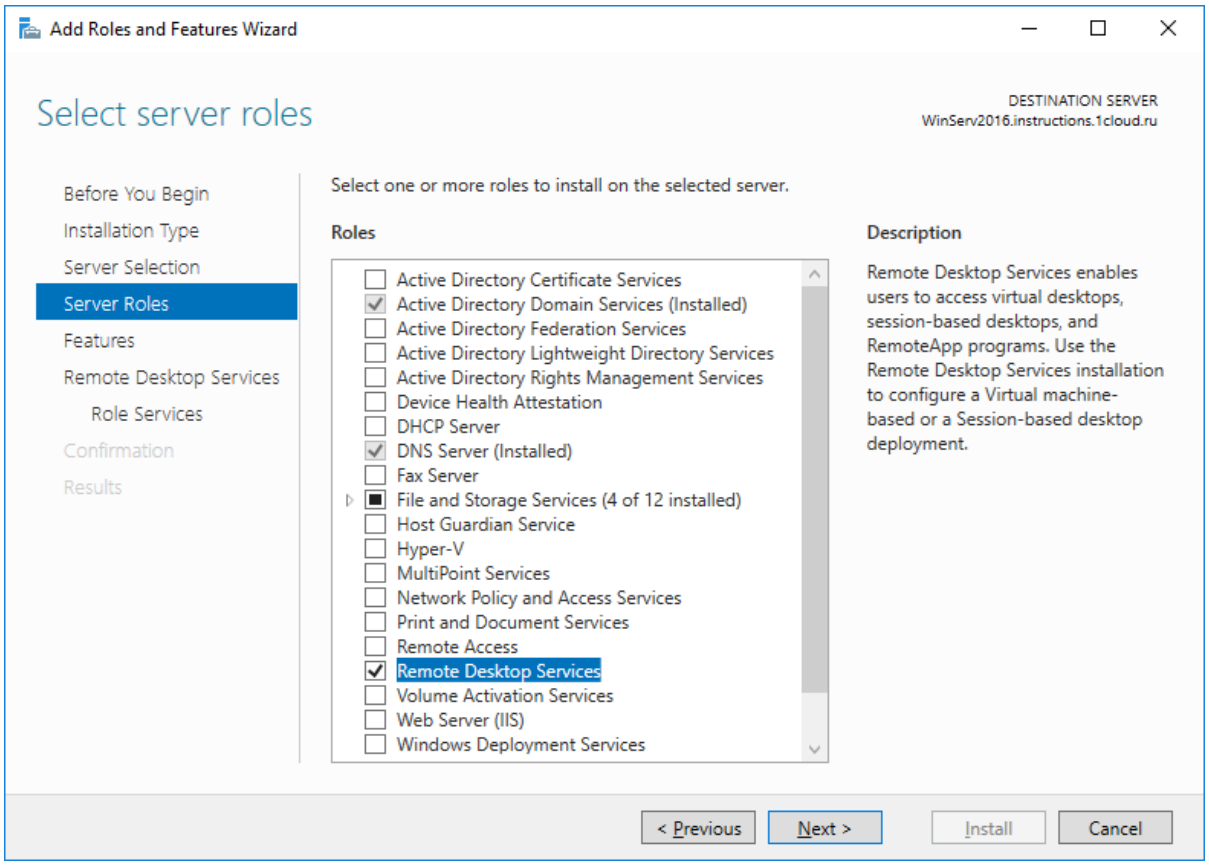
Нажмите Instantiate.

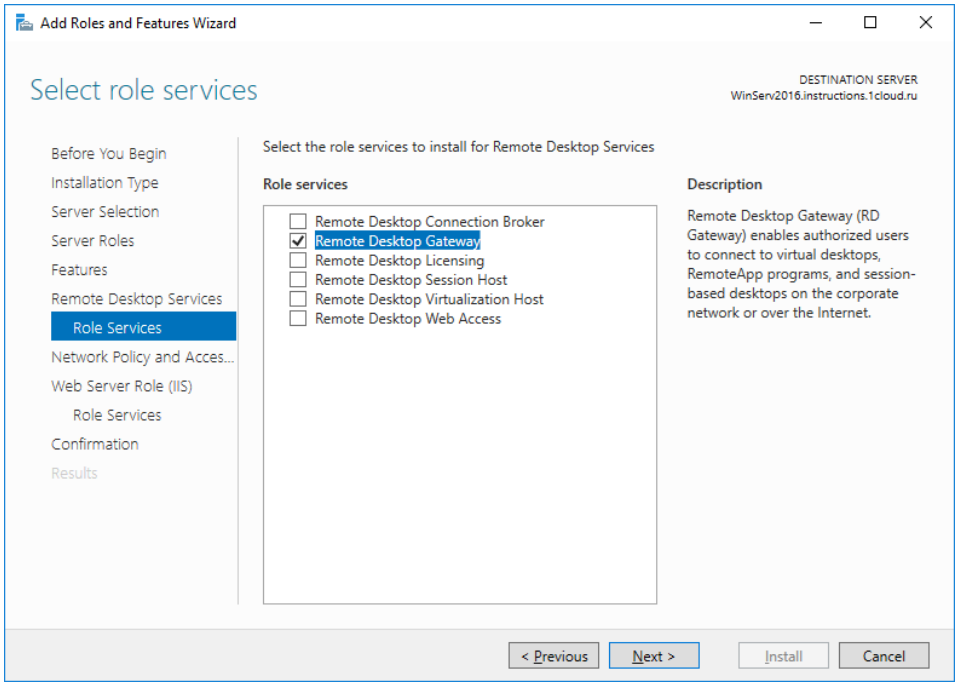
Эталон ответа

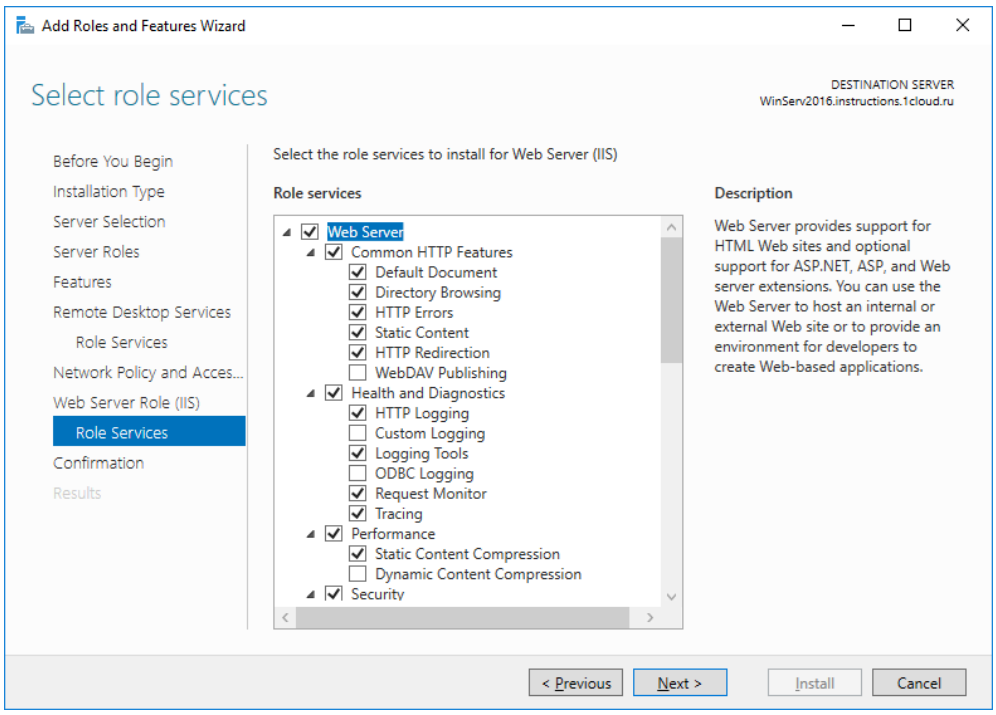


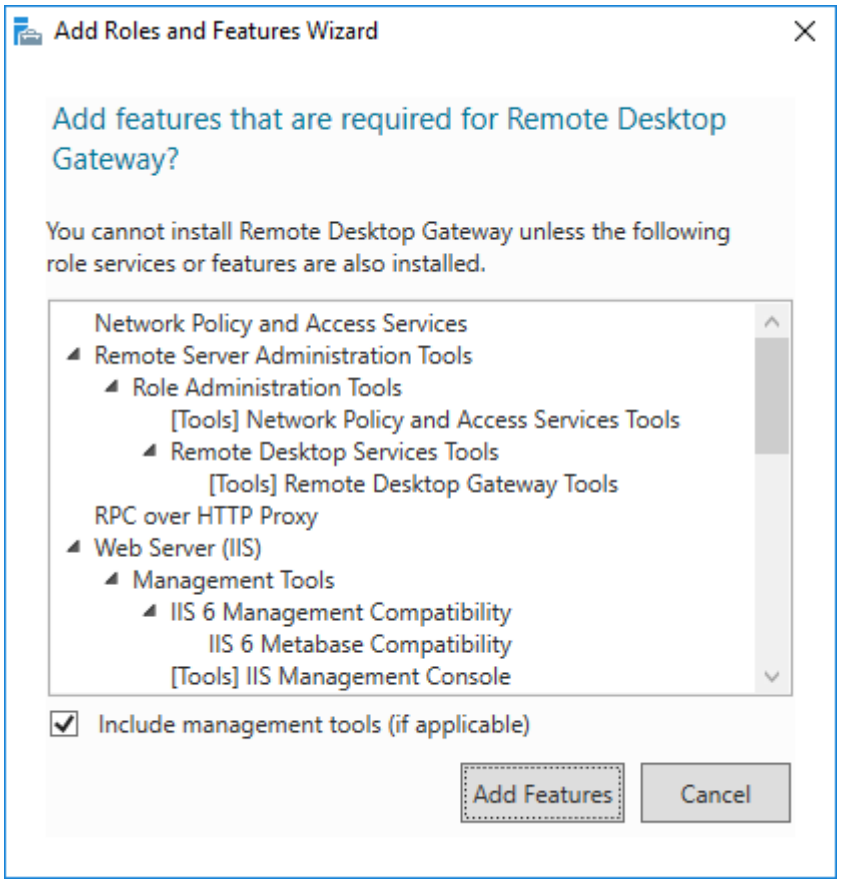

Add Roles and Features Wizard
Select installation type
DESTINATION SERVER
WinServ2016.instructions.1cloud.ru
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).
Role-based or feature-based installation
Configure a single server by adding roles, role services, and features.
Remote Desktop Services installation
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
< Previous
Next >
Install
Cancel

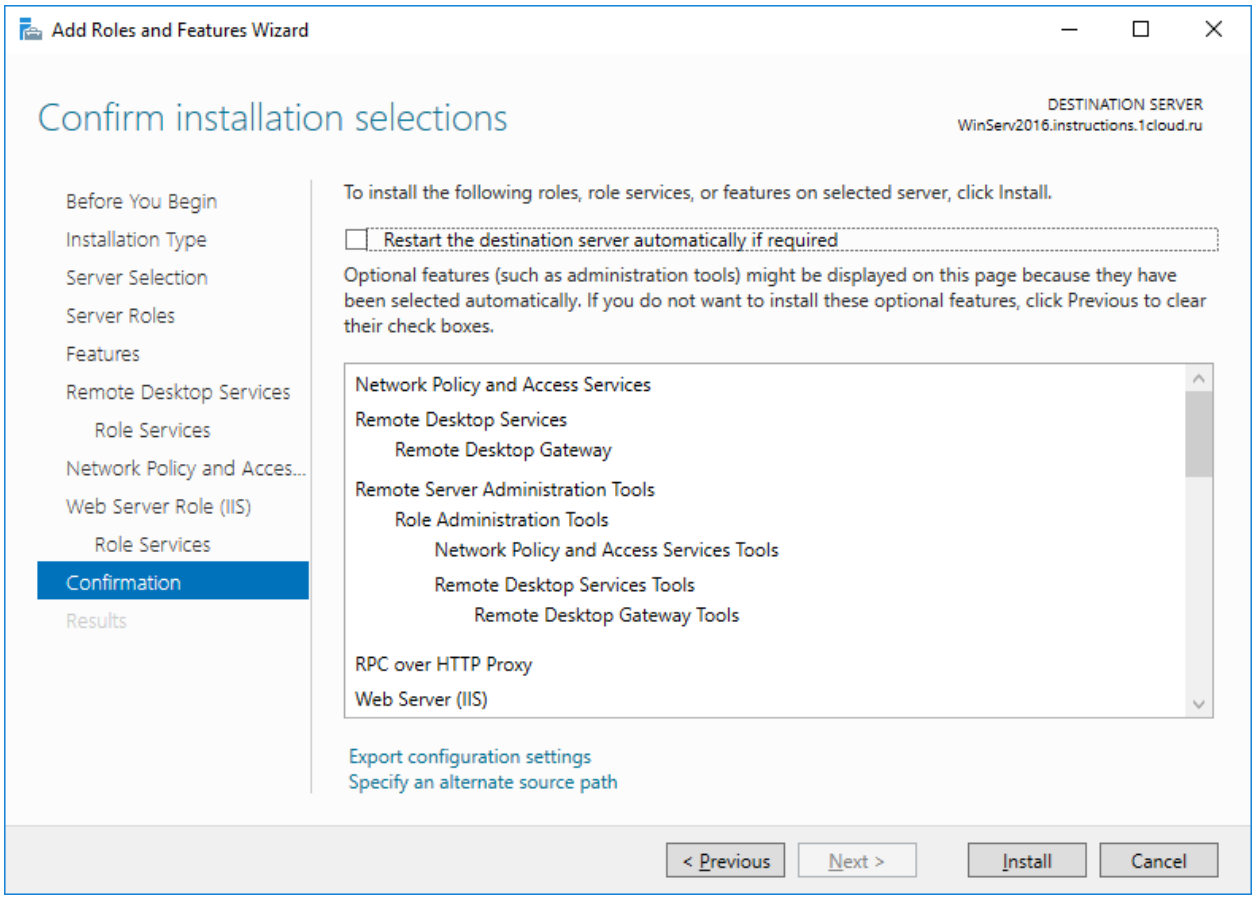

Add Roles and Features Wizard
Select destination server
DESTINATION SERVER
WinServ2016.instructions.1cloud.ru
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select a server or a virtual hard disk on which to install roles and features.
Select a server from the server pool
Select a virtual hard disk
Server Pool
Filter:
Name
IP Address
Operating System
WinServ2016.instruction...
10.0.0.2,5.200.4...
Microsoft Windows Server 2016 Standard
1 Computer(s) found
This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.
< Previous
Next >
Install
Cancel

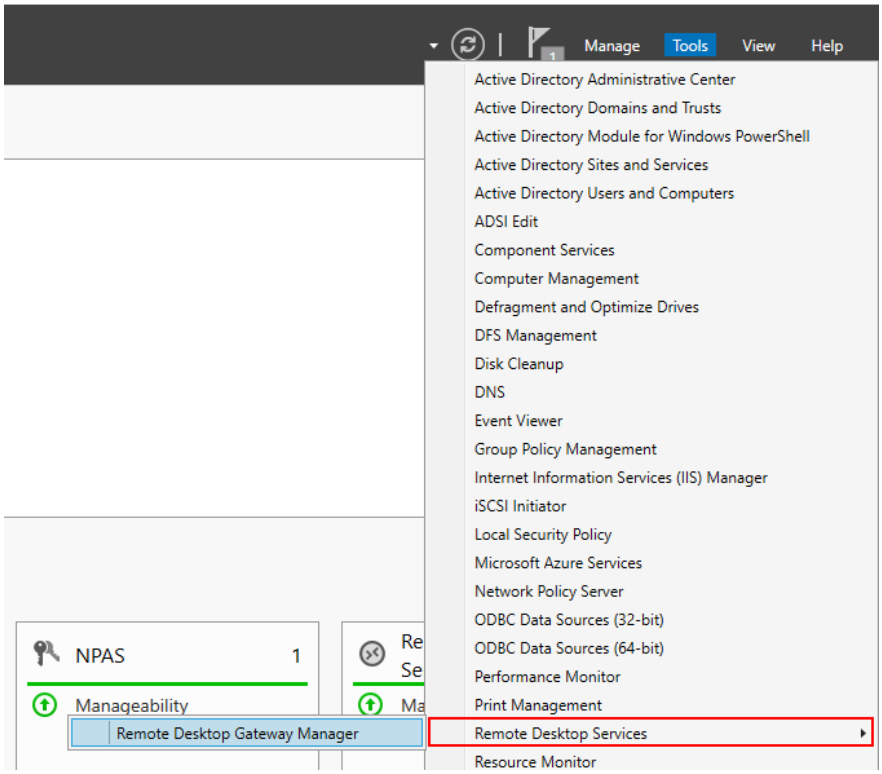

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
WinServ2016.instructions.1cloud.ru
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Desktop Services
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services (Installed)
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server (Installed)
Fax Server
File and Storage Services (4 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Description
Remote Desktop Services enables users to access virtual desktops, session-based desktops, and RemoteApp programs. Use the Remote Desktop Services installation to configure a Virtual machine-based or a Session-based desktop deployment.
< Previous
Next >
Install
Cancel

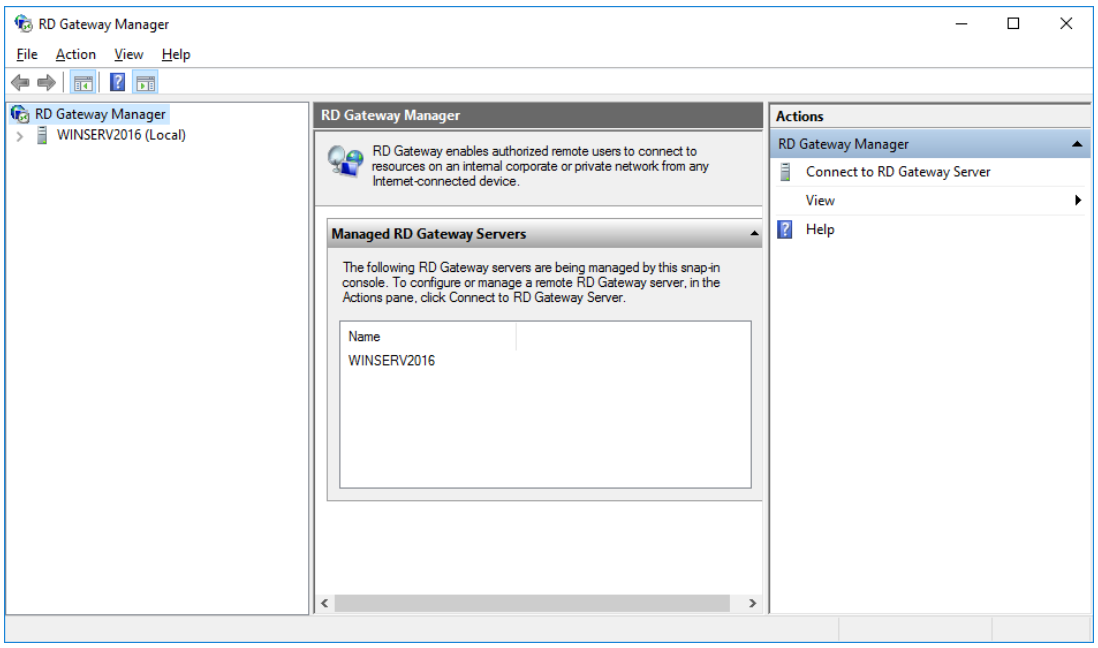

Add Roles and Features Wizard
Select role services
DESTINATION SERVER
WinServ2016.instructions.1cloud.ru
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Desktop Services
Role Services
Network Policy and Acces...
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Remote Desktop Services
Role services
Remote Desktop Connection Broker
Remote Desktop Gateway
Remote Desktop Licensing
Remote Desktop Session Host
Remote Desktop Virtualization Host
Remote Desktop Web Access
Description
Remote Desktop Gateway (RD Gateway) enables authorized users to connect to virtual desktops, RemoteApp programs, and session-based desktops on the corporate network or over the Internet.
< Previous
Next >
Install
Cancel

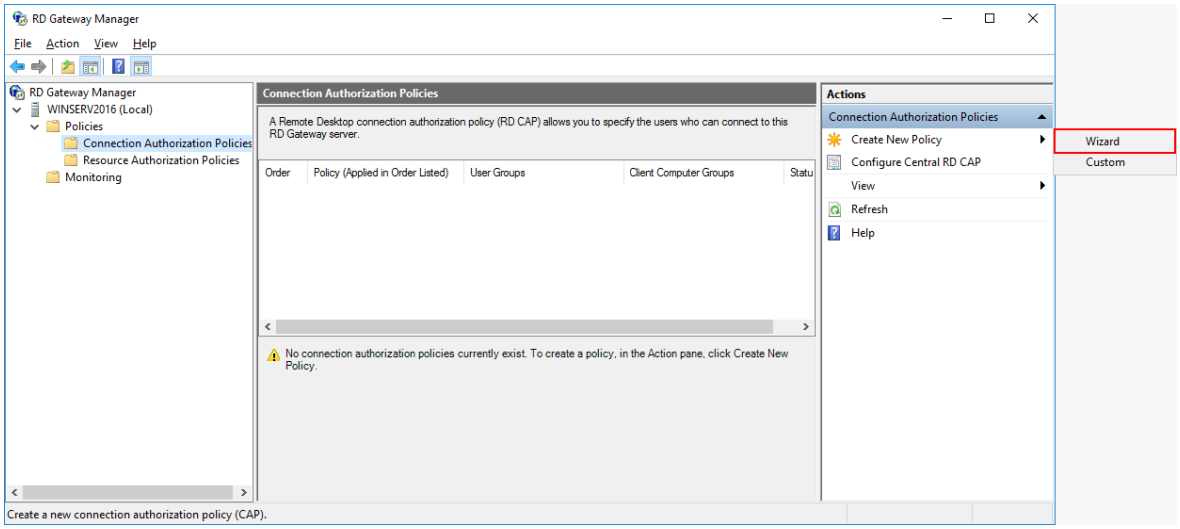

Add Roles and Features Wizard
Select role services
DESTINATION SERVER
WinServ2016.instructions.1cloud.ru
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Desktop Services
Role Services
Network Policy and Acces...
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Web Server (IIS)
Role services
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
HTTP Redirection
WebDAV Publishing
Health and Diagnostics
HTTP Logging
Custom Logging
Logging Tools
ODBC Logging
Request Monitor
Tracing
Performance
Static Content Compression
Dynamic Content Compression
Security
Description
Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
< Previous
Next >
Install
Cancel

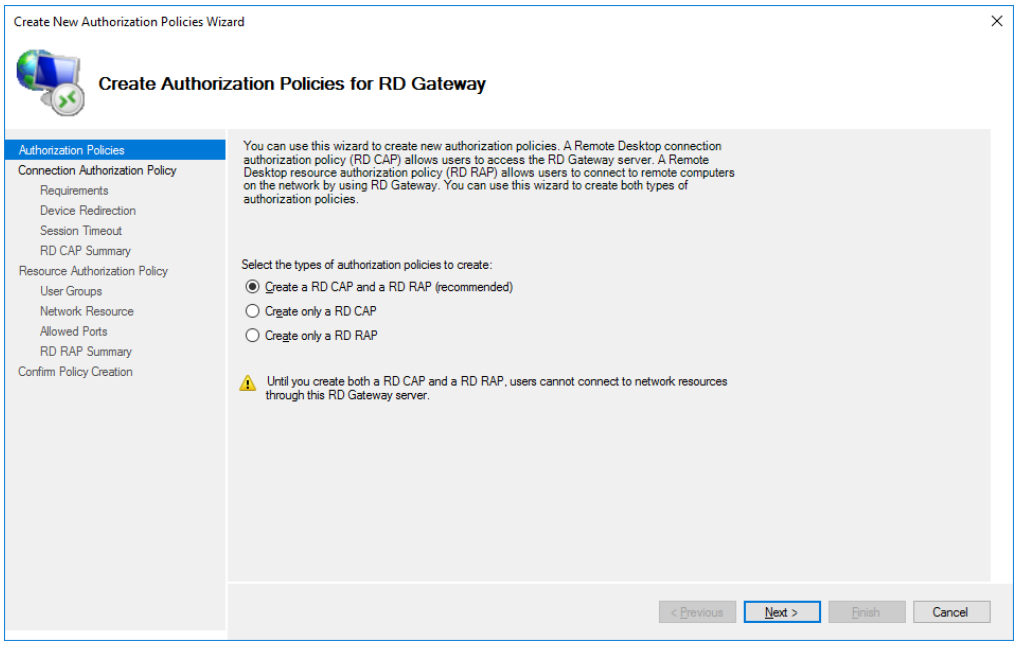

Add Roles and Features Wizard
Add features that are required for Remote Desktop Gateway?
You cannot install Remote Desktop Gateway unless the following role services or features are also installed.
Network Policy and Access Services
Remote Server Administration Tools
Role Administration Tools
[Tools] Network Policy and Access Services Tools
Remote Desktop Services Tools
[Tools] Remote Desktop Gateway Tools
RPC over HTTP Proxy
Web Server (IIS)
Management Tools
IIS 6 Management Compatibility
IIS 6 Metabase Compatibility
[Tools] IIS Management Console
Include management tools (if applicable)
Add Features
Cancel

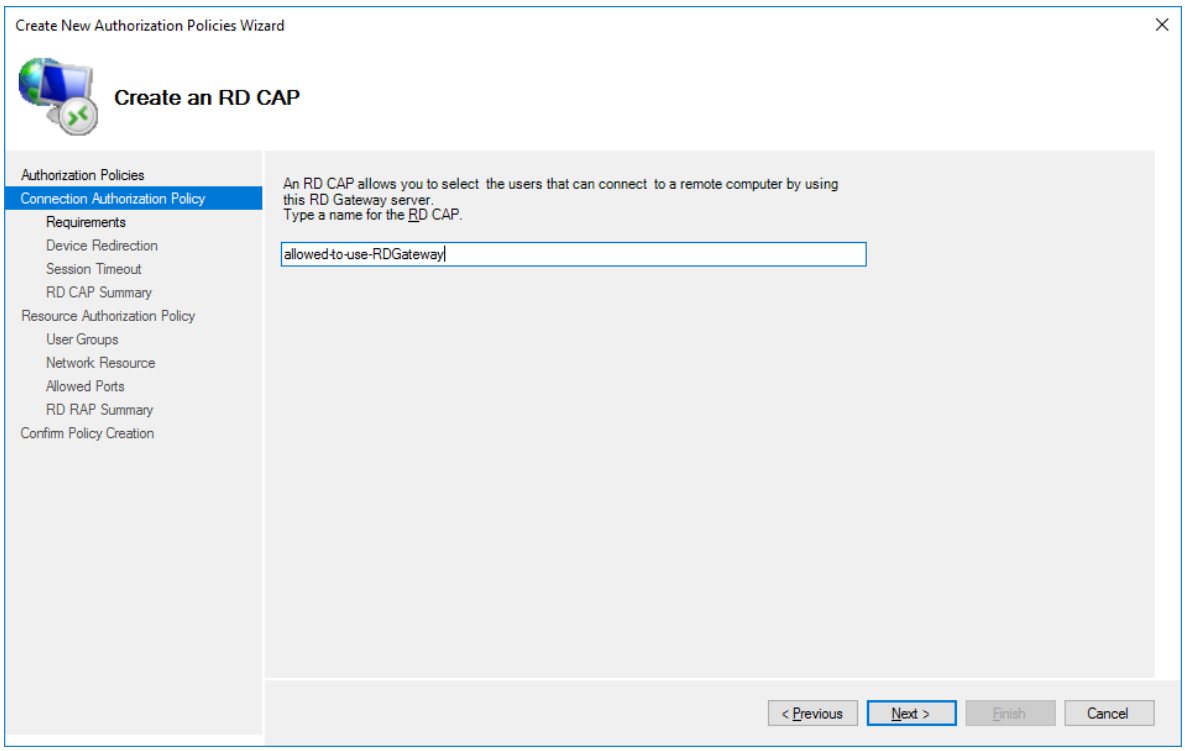

Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
WinServ2016.instructions.1cloud.ru
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Desktop Services
Role Services
Network Policy and Acces...
Web Server Role (IIS)
Role Services
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Network Policy and Access Services
Remote Desktop Services
Remote Desktop Gateway
Remote Server Administration Tools
Role Administration Tools
Network Policy and Access Services Tools
Remote Desktop Services Tools
Remote Desktop Gateway Tools
RPC over HTTP Proxy
Web Server (IIS)
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

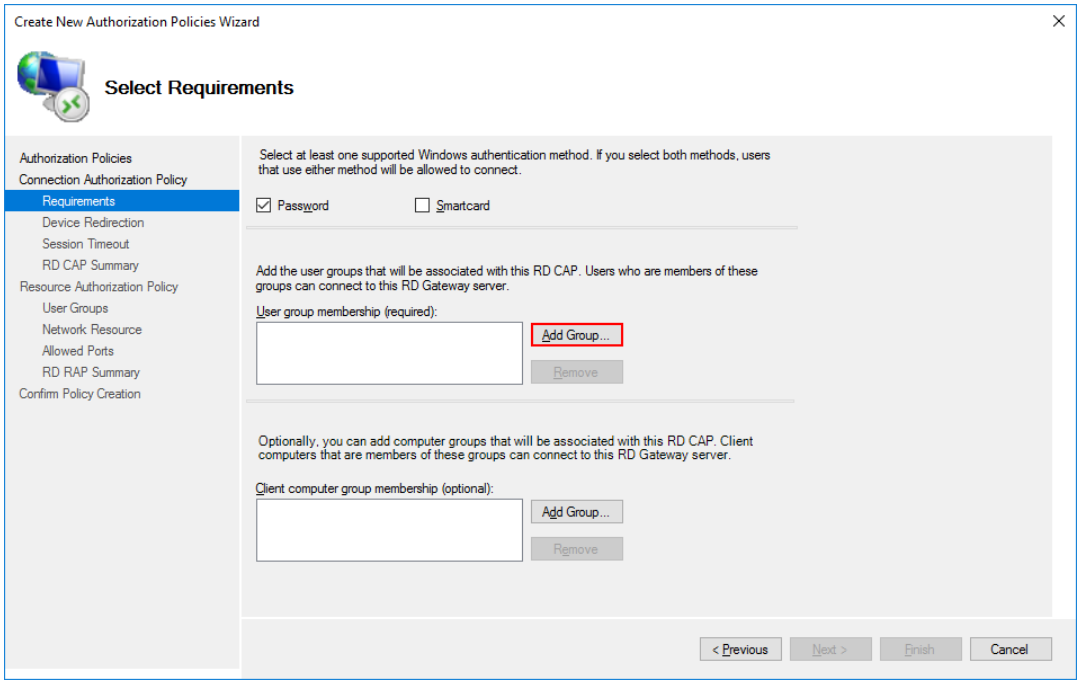

Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DFS Management
Disk Cleanup
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
Network Policy Server
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Remote Desktop Services
Resource Monitor
NPAS
1
Manageability
Remote Desktop Gateway Manager

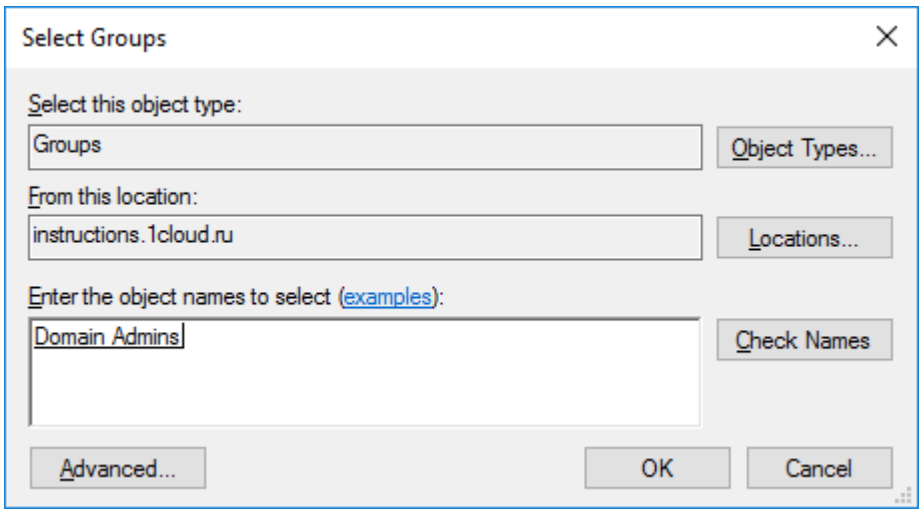

RD Gateway Manager
File Action View Help
RD Gateway Manager
WINSERV2016 (Local)
RD Gateway Manager
RD Gateway enables authorized remote users to connect to resources on an internal corporate or private network from any Internet-connected device.
Managed RD Gateway Servers
The following RD Gateway servers are being managed by this snap-in console. To configure or manage a remote RD Gateway server, in the Actions pane, click Connect to RD Gateway Server.
Name
WINSERV2016
Actions
RD Gateway Manager
Connect to RD Gateway Server
View
Help

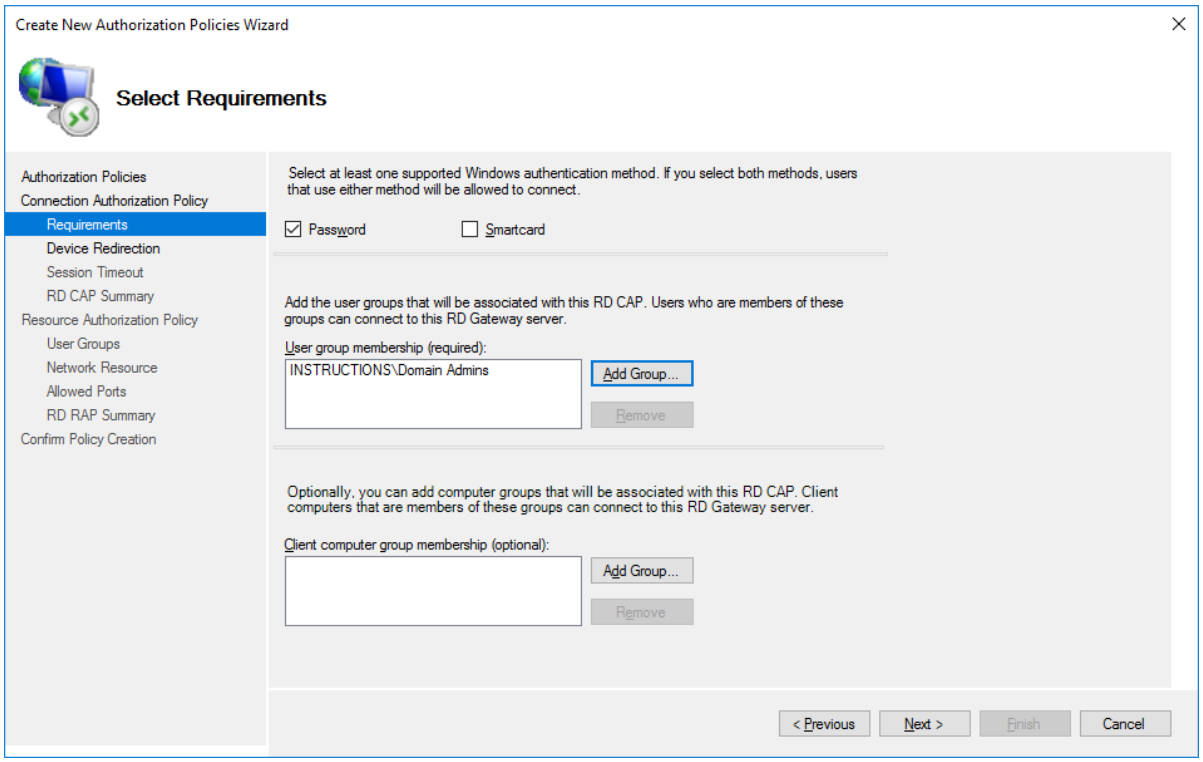

RD Gateway Manager
File Action View Help
RD Gateway Manager
WINSERV2016 (Local)
Policies
Connection Authorization Policies
Resource Authorization Policies
Monitoring
Connection Authorization Policies
A Remote Desktop connection authorization policy (RD CAP) allows you to specify the users who can connect to this RD Gateway server.
Order
Policy (Applied in Order Listed)
User Groups
Client Computer Groups
Statu
No connection authorization policies currently exist. To create a policy, in the Action pane, click Create New Policy.
Actions
Connection Authorization Policies
Create New Policy
Configure Central RD CAP
View
Refresh
Help
Wizard
Custom
Create a new connection authorization policy (CAP).

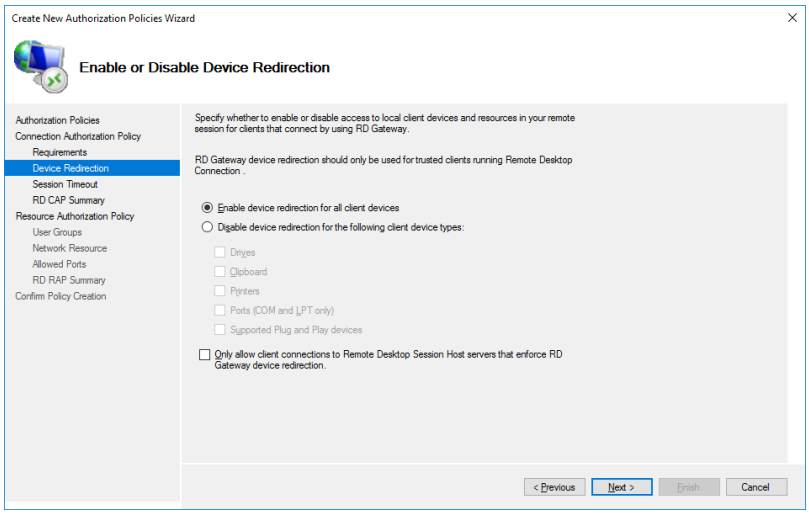

Create New Authorization Policies Wizard
Create Authorization Policies for RD Gateway
Authorization Policies
Connection Authorization Policy
Requirements
Device Redirection
Session Timeout
RD CAP Summary
Resource Authorization Policy
User Groups
Network Resource
Allowed Ports
RD RAP Summary
Confirm Policy Creation
You can use this wizard to create new authorization policies. A Remote Desktop connection authorization policy (RD CAP) allows users to access the RD Gateway server. A Remote Desktop resource authorization policy (RD RAP) allows users to connect to remote computers on the network by using RD Gateway. You can use this wizard to create both types of authorization policies.
Select the types of authorization policies to create:
Create a RD CAP and a RD RAP (recommended)
Create only a RD CAP
Create only a RD RAP
Until you create both a RD CAP and a RD RAP, users cannot connect to network resources through this RD Gateway server.
< Previous
Next >
Finish
Cancel

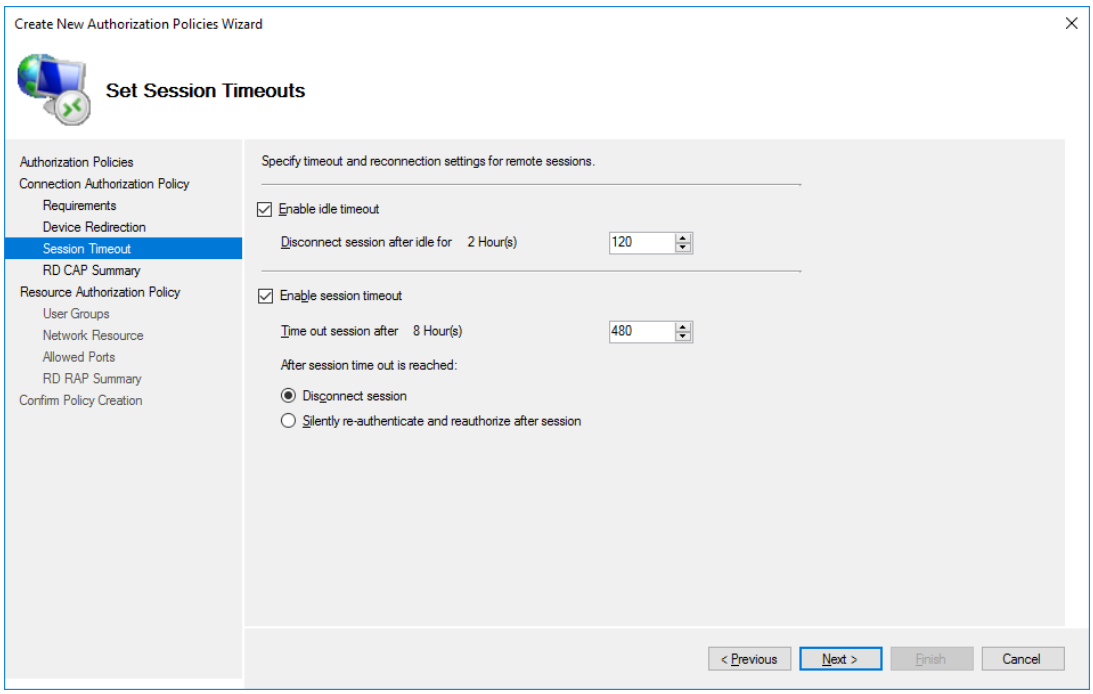

Create New Authorization Policies Wizard
Create an RD CAP
Authorization Policies
Connection Authorization Policy
Requirements
Device Redirection
Session Timeout
RD CAP Summary
Resource Authorization Policy
User Groups
Network Resource
Allowed Ports
RD RAP Summary
Confirm Policy Creation
An RD CAP allows you to select the users that can connect to a remote computer by using this RD Gateway server.
Type a name for the RD CAP.
allowed-to-use-RDGateway
< Previous
Next >
Finish
Cancel

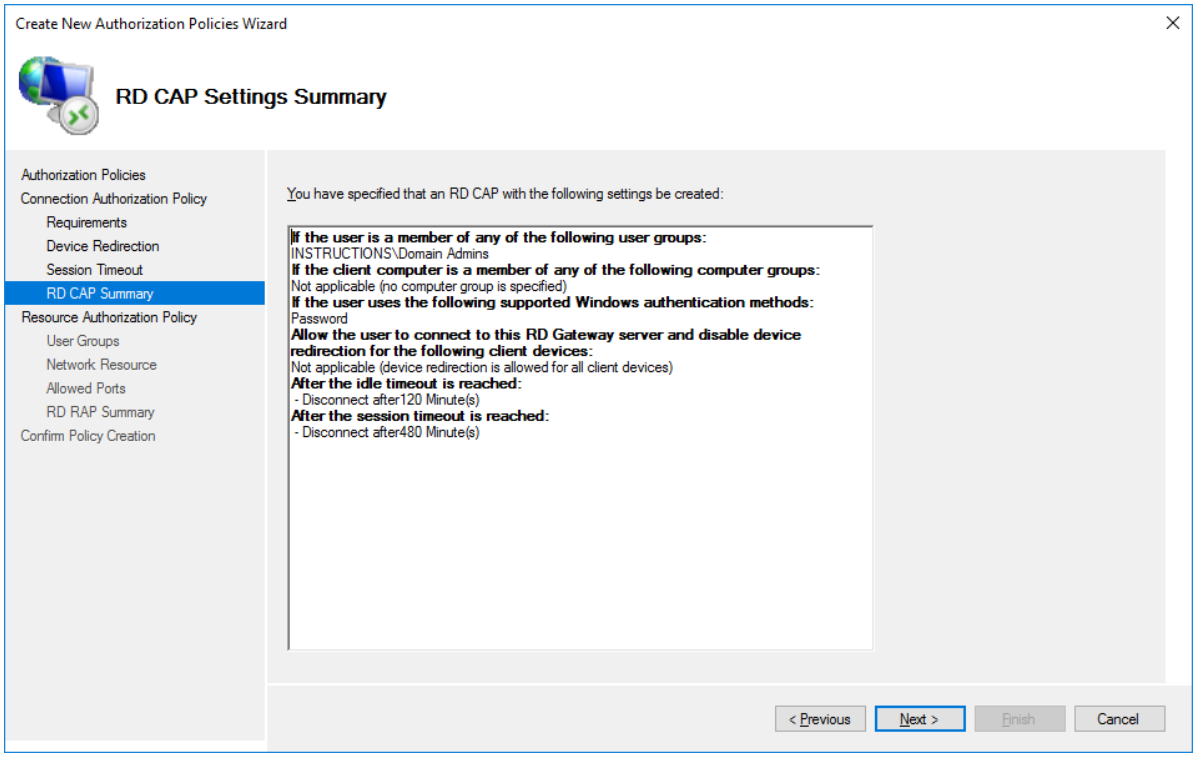

Create New Authorization Policies Wizard
Select Requirements
Authorization Policies
Connection Authorization Policy
Requirements
Device Redirection
Session Timeout
RD CAP Summary
Resource Authorization Policy
User Groups
Network Resource
Allowed Ports
RD RAP Summary
Confirm Policy Creation
Select at least one supported Windows authentication method. If you select both methods, users that use either method will be allowed to connect.
Password
Smartcard
Add the user groups that will be associated with this RD CAP. Users who are members of these groups can connect to this RD Gateway server.
User group membership (required):
Add Group...
Remove
Optionally, you can add computer groups that will be associated with this RD CAP. Client computers that are members of these groups can connect to this RD Gateway server.
Client computer group membership (optional):
Add Group...
Remove
< Previous
Next >
Finish
Cancel

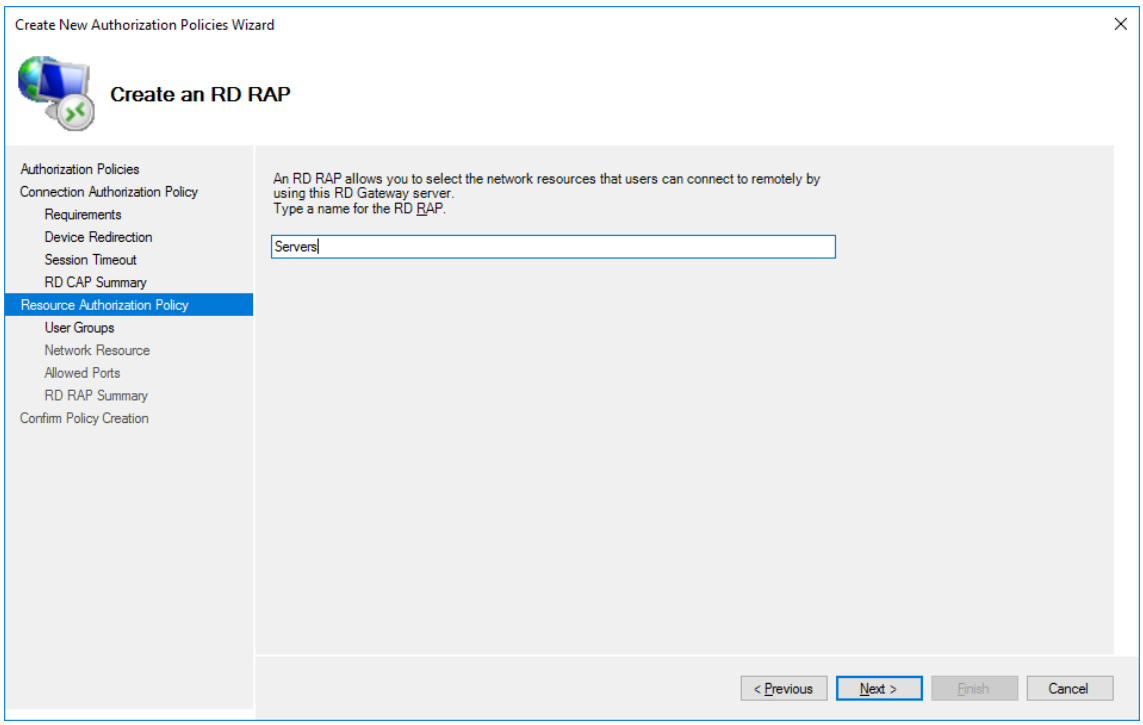

Select Groups
Select this object type:
Groups
Object Types...
From this location:
instructions.1cloud.ru
Locations...
Enter the object names to select (examples):
Domain Admins
Check Names
Advanced...
OK
Cancel

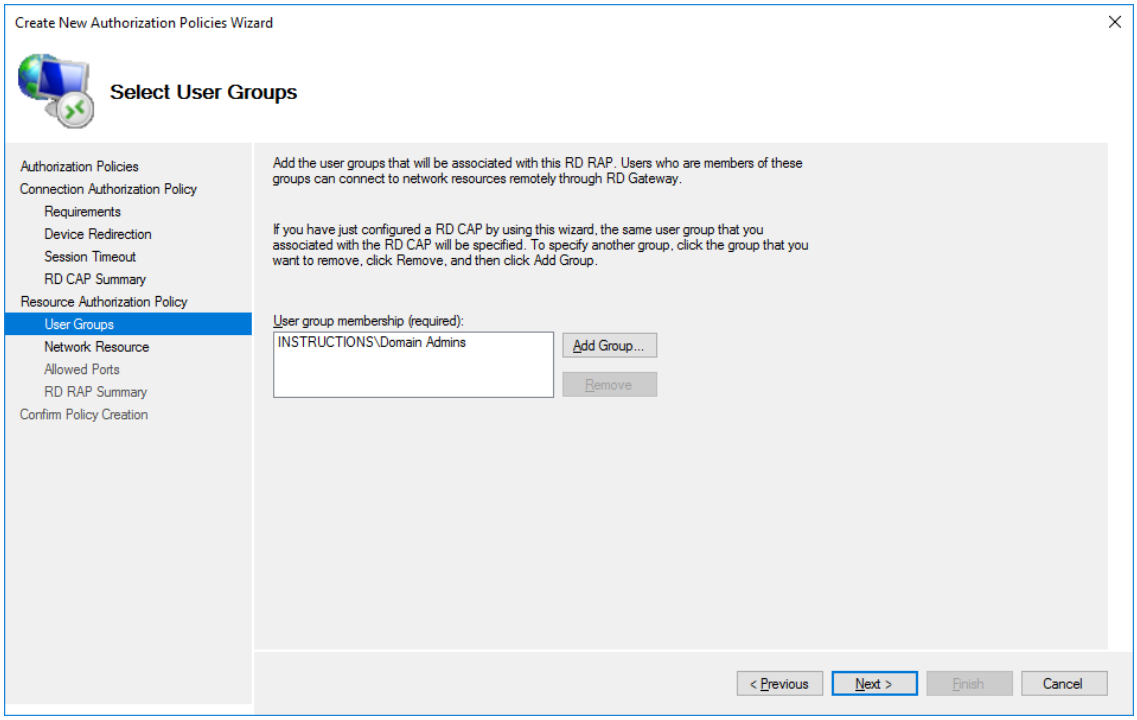

Create New Authorization Policies Wizard
Select Requirements
Authorization Policies
Connection Authorization Policy
Requirements
Device Redirection
Session Timeout
RD CAP Summary
Resource Authorization Policy
User Groups
Network Resource
Allowed Ports
RD RAP Summary
Confirm Policy Creation
Select at least one supported Windows authentication method. If you select both methods, users that use either method will be allowed to connect.
Password
Smartcard
Add the user groups that will be associated with this RD CAP. Users who are members of these groups can connect to this RD Gateway server.
User group membership (required):
INSTRUCTIONS\Domain Admins
Add Group...
Remove
Optionally, you can add computer groups that will be associated with this RD CAP. Client computers that are members of these groups can connect to this RD Gateway server.
Client computer group membership (optional):
Add Group...
Remove
< Previous
Next >
Finish
Cancel

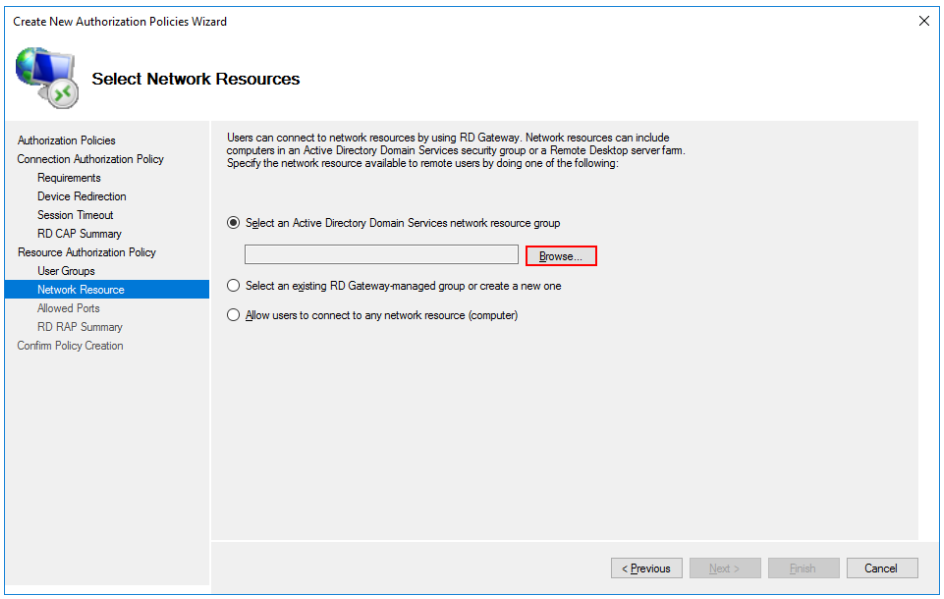

Create New Authorization Policies Wizard
Enable or Disable Device Redirection
Authorization Policies
Connection Authorization Policy
Requirements
Device Redirection
Session Timeout
RD CAP Summary
Resource Authorization Policy
User Groups
Network Resource
Allowed Ports
RD RAP Summary
Confirm Policy Creation
Specify whether to enable or disable access to local client devices and resources in your remote session for clients that connect by using RD Gateway.
RD Gateway device redirection should only be used for trusted clients running Remote Desktop Connection .
Enable device redirection for all client devices
Disable device redirection for the following client device types:
Drives
Clipboard
Printers
Ports (COM and LPT only)
Supported Plug and Play devices
Only allow client connections to Remote Desktop Session Host servers that enforce RD Gateway device redirection.
< Previous
Next >
Finish
Cancel

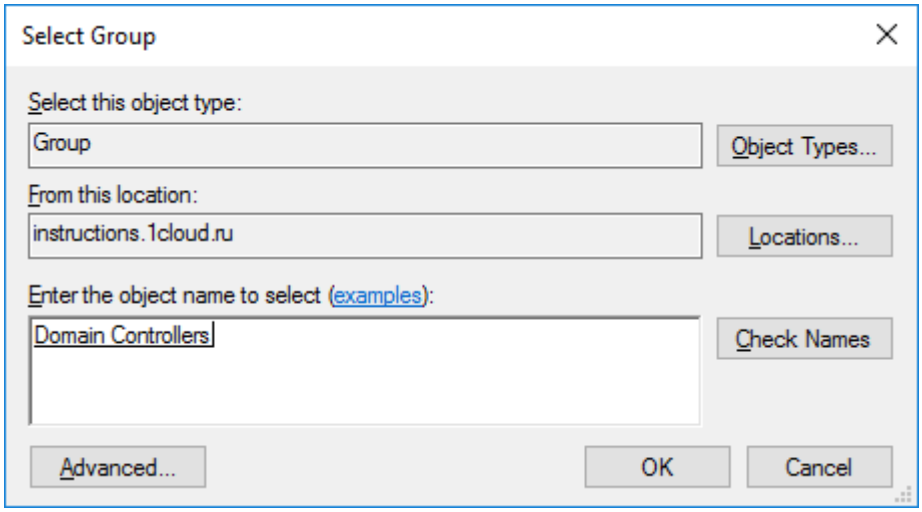

Create New Authorization Policies Wizard
Set Session Timeouts
Authorization Policies
Connection Authorization Policy
Requirements
Device Redirection
Session Timeout
RD CAP Summary
Resource Authorization Policy
User Groups
Network Resource
Allowed Ports
RD RAP Summary
Confirm Policy Creation
Specify timeout and reconnection settings for remote sessions.
Enable idle timeout
Disconnect session after idle for 2 Hour(s)
120
Enable session timeout
Time out session after 8 Hour(s)
480
After session time out is reached:
Disconnect session
Silently re-authenticate and reauthorize after session
< Previous
Next >
Finish
Cancel


Create New Authorization Policies Wizard
RD CAP Settings Summary
Authorization Policies
Connection Authorization Policy
Requirements
Device Redirection
Session Timeout
RD CAP Summary
Resource Authorization Policy
User Groups
Network Resource
Allowed Ports
RD RAP Summary
Confirm Policy Creation
You have specified that an RD CAP with the following settings be created:
If the user is a member of any of the following user groups:
INSTRUCTIONS\Domain Admins
If the client computer is a member of any of the following computer groups:
Not applicable (no computer group is specified)
If the user uses the following supported Windows authentication methods:
Password
Allow the user to connect to this RD Gateway server and disable device redirection for the following client devices:
Not applicable (device redirection is allowed for all client devices)
After the idle timeout is reached:
- Disconnect after120 Minute(s)
After the session timeout is reached:
- Disconnect after480 Minute(s)
< Previous
Next >
Finish
Cancel

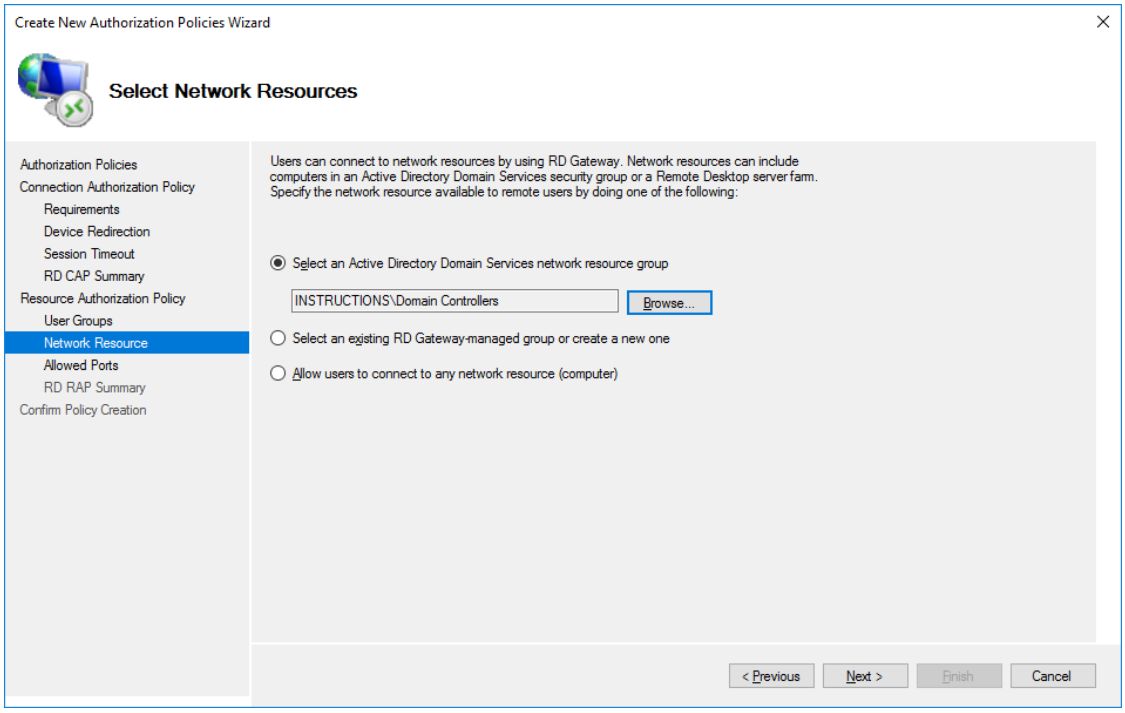

Create New Authorization Policies Wizard
Create an RD RAP
Authorization Policies
Connection Authorization Policy
Requirements
Device Redirection
Session Timeout
RD CAP Summary
Resource Authorization Policy
User Groups
Network Resource
Allowed Ports
RD RAP Summary
Confirm Policy Creation
An RD RAP allows you to select the network resources that users can connect to remotely by using this RD Gateway server.
Type a name for the RD RAP.
Servers
< Previous
Next >
Finish
Cancel

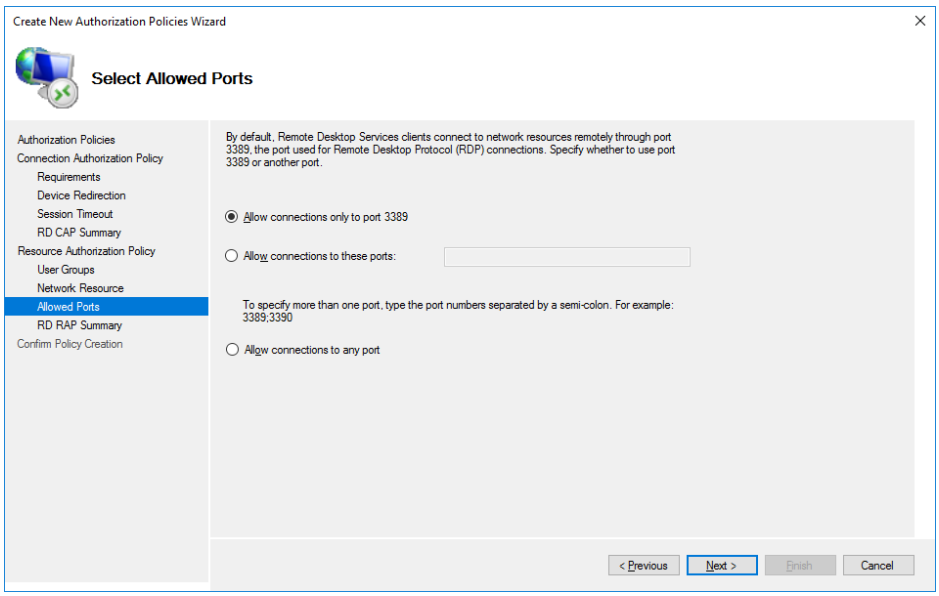

Create New Authorization Policies Wizard
Select User Groups
Authorization Policies
Connection Authorization Policy
Requirements
Device Redirection
Session Timeout
RD CAP Summary
Resource Authorization Policy
User Groups
Network Resource
Allowed Ports
RD RAP Summary
Confirm Policy Creation
Add the user groups that will be associated with this RD RAP. Users who are members of these groups can connect to network resources remotely through RD Gateway.
If you have just configured a RD CAP by using this wizard, the same user group that you associated with the RD CAP will be specified. To specify another group, click the group that you want to remove, click Remove, and then click Add Group.
User group membership (required):
INSTRUCTIONS\Domain Admins
Add Group...
Remove
< Previous
Next >
Finish
Cancel

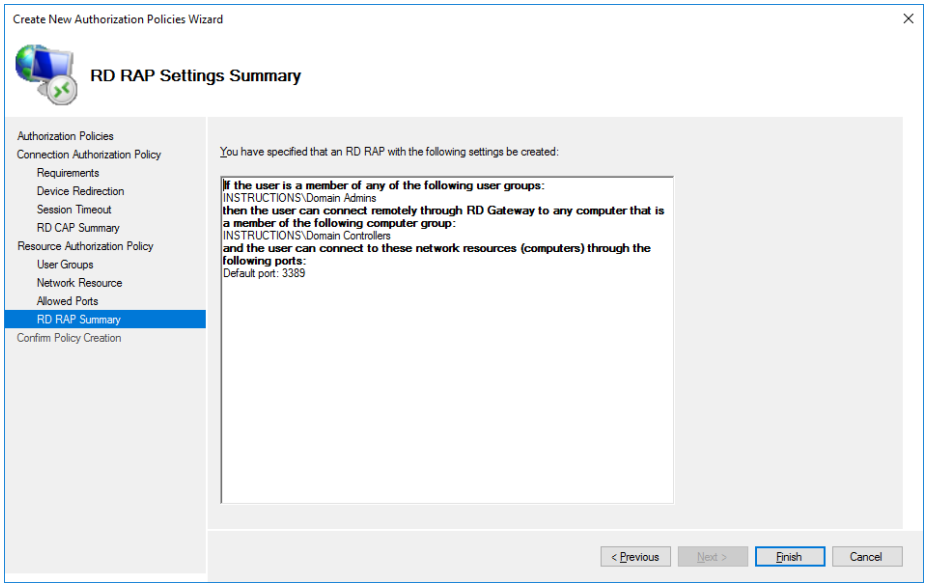


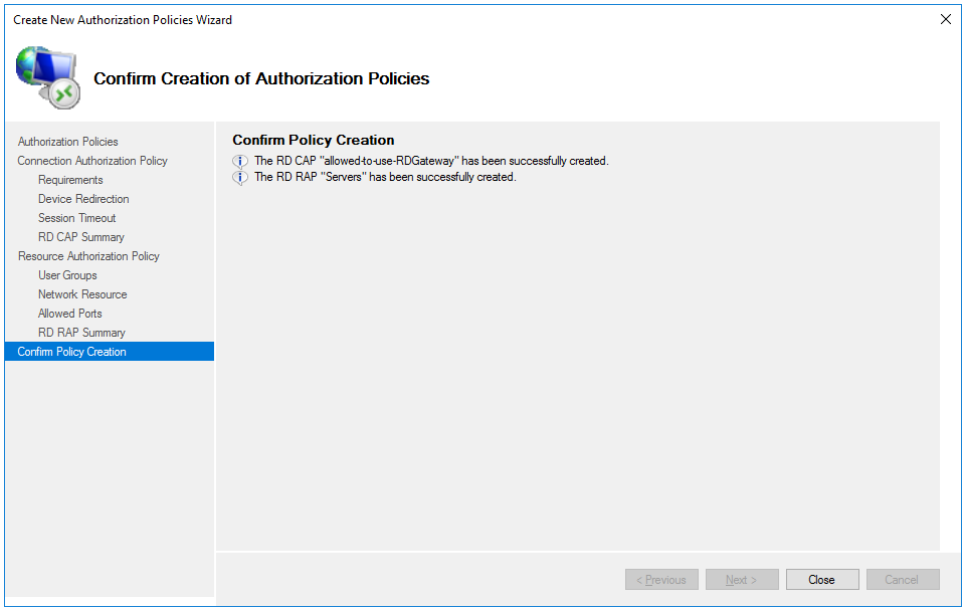


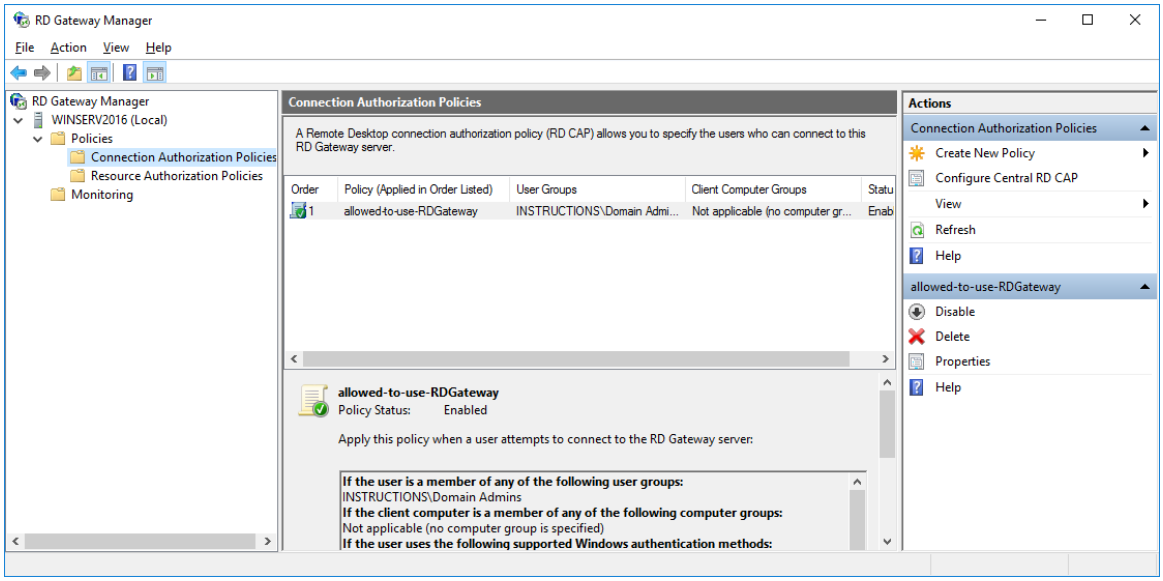
Убедитесь, что добавлена нужная группа.

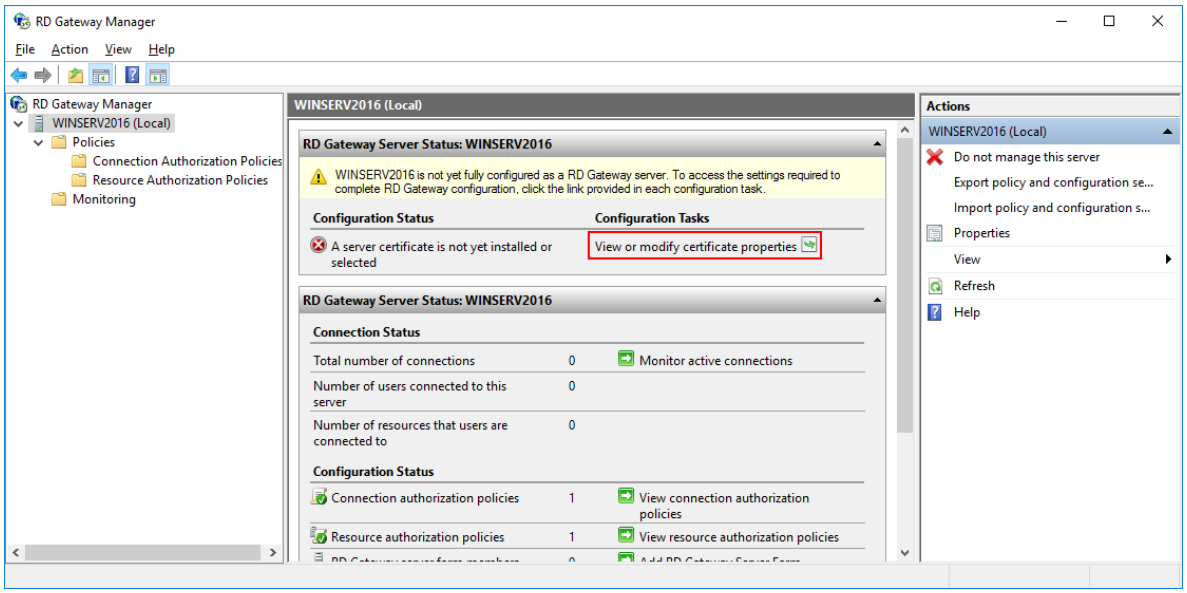


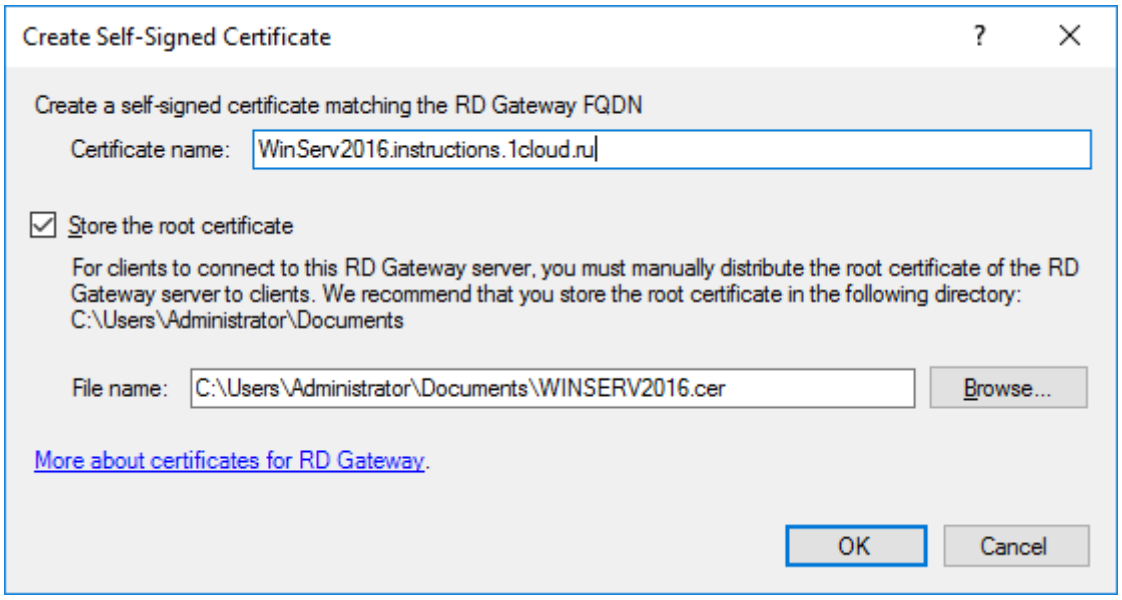

Create New Authorization Policies Wizard
Select Allowed Ports
Authorization Policies
Connection Authorization Policy
Requirements
Device Redirection
Session Timeout
RD CAP Summary
Resource Authorization Policy
User Groups
Network Resource
Allowed Ports
RD RAP Summary
Confirm Policy Creation
By default, Remote Desktop Services clients connect to network resources remotely through port 3389, the port used for Remote Desktop Protocol (RDP) connections. Specify whether to use port 3389 or another port.
Allow connections only to port 3389
Allow connections to these ports:
To specify more than one port, type the port numbers separated by a semi-colon. For example: 3389;3390
Allow connections to any port
< Previous
Next >
Finish
Cancel

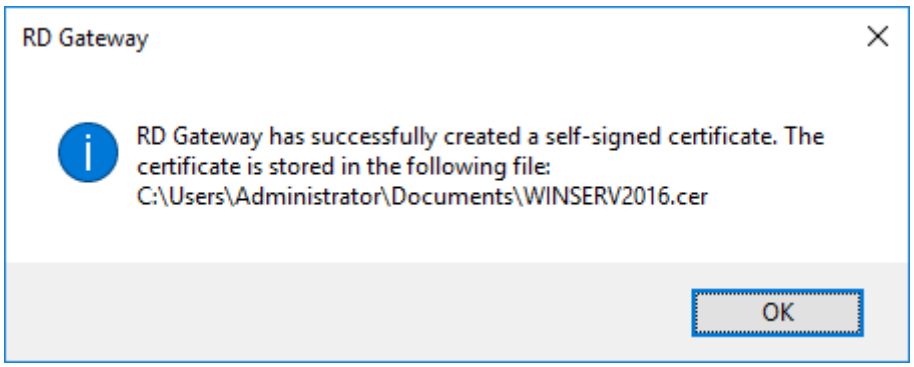

Create New Authorization Policies Wizard
RD RAP Settings Summary
Authorization Policies
Connection Authorization Policy
Requirements
Device Redirection
Session Timeout
RD CAP Summary
Resource Authorization Policy
User Groups
Network Resource
Allowed Ports
RD RAP Summary
Confirm Policy Creation
You have specified that an RD RAP with the following settings be created:
If the user is a member of any of the following user groups:
INSTRUCTIONS\Domain Admins
then the user can connect remotely through RD Gateway to any computer that is a member of the following computer group:
INSTRUCTIONS\Domain Controllers
and the user can connect to these network resources (computers) through the following ports:
Default port: 3389
< Previous
Next >
Finish
Cancel

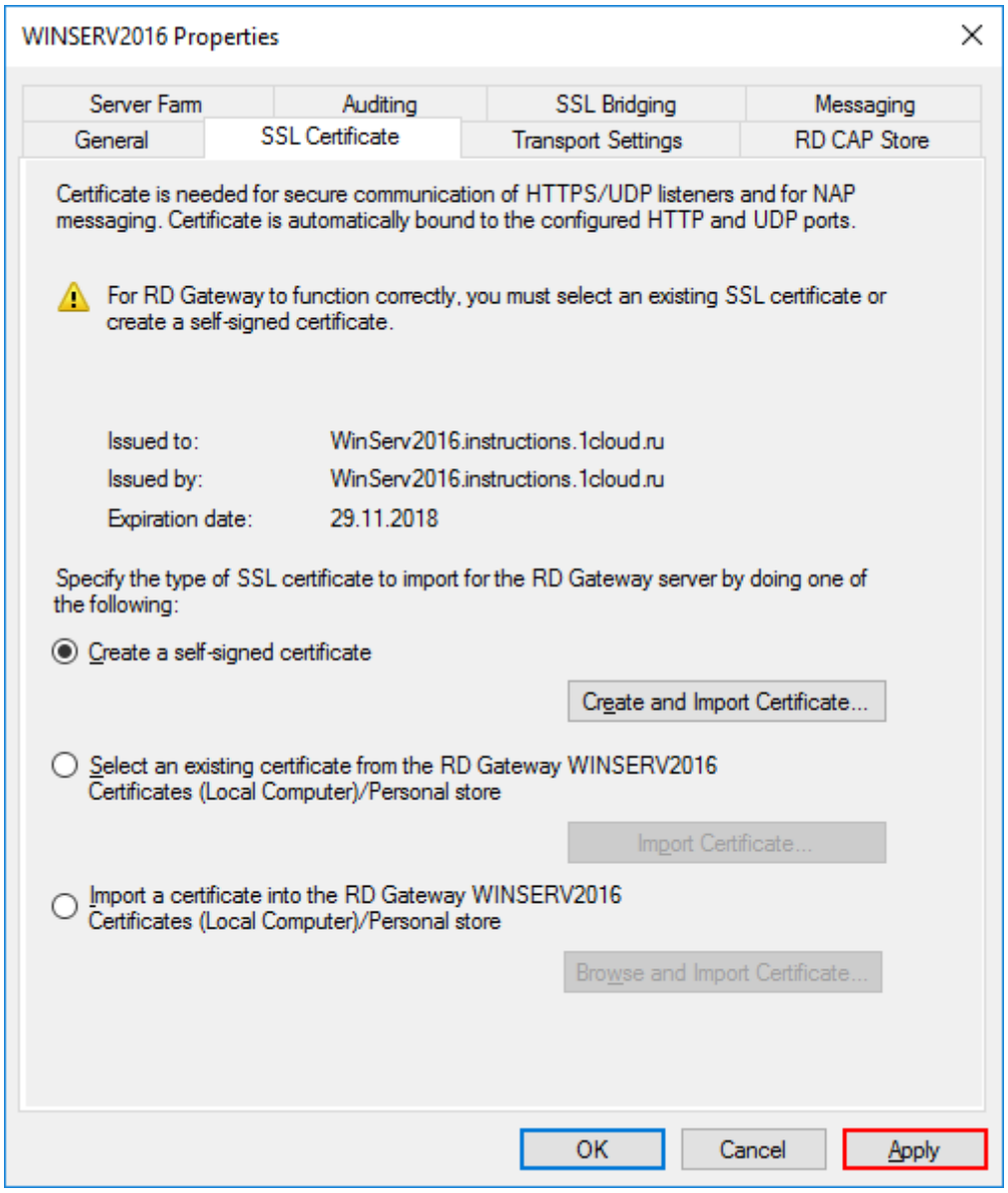

Create New Authorization Policies Wizard
Confirm Creation of Authorization Policies
Authorization Policies
Connection Authorization Policy
Requirements
Device Redirection
Session Timeout
RD CAP Summary
Resource Authorization Policy
User Groups
Network Resource
Allowed Ports
RD RAP Summary
Confirm Policy Creation
Confirm Policy Creation
The RD CAP "allowed-to-use-RDGateway" has been successfully created.
The RD RAP "Servers" has been successfully created.
< Previous
Next >
Close
Cancel

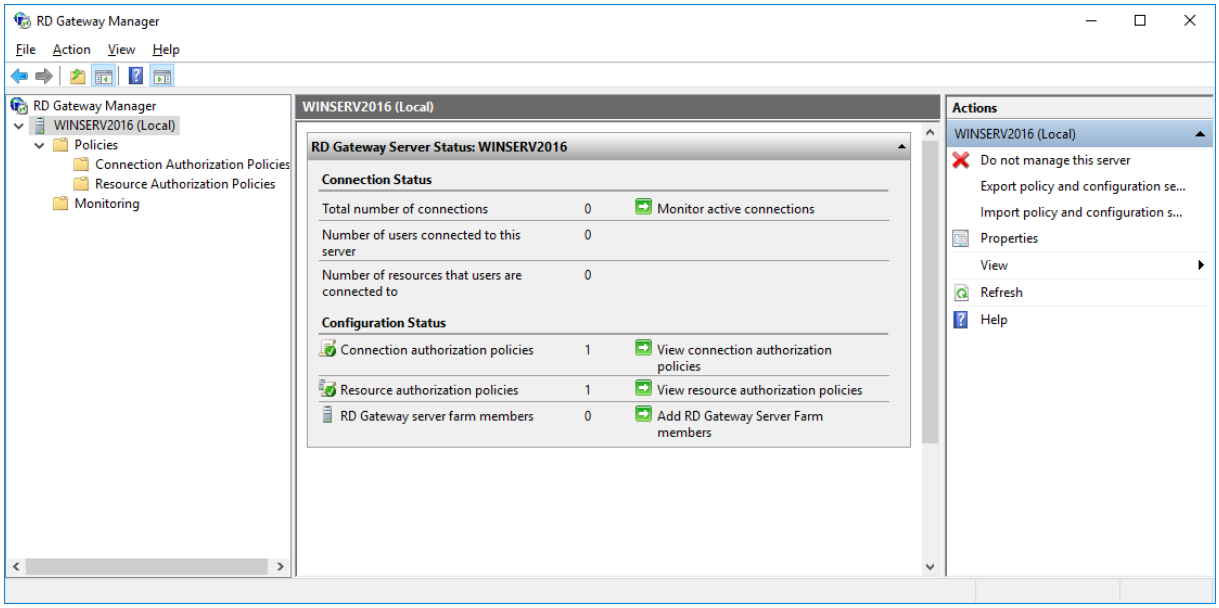

RD Gateway Manager
File Action View Help
RD Gateway Manager
WINSERV2016 (Local)
Policies
Connection Authorization Policies
Resource Authorization Policies
Monitoring
Connection Authorization Policies
A Remote Desktop connection authorization policy (RD CAP) allows you to specify the users who can connect to this RD Gateway server.
Order
Policy (Applied in Order Listed)
User Groups
Client Computer Groups
Statu
1
allowed-to-use-RDGateway
INSTRUCTIONS\Domain Admi...
Not applicable (no computer gr...
Enab
allowed-to-use-RDGateway
Policy Status: Enabled
Apply this policy when a user attempts to connect to the RD Gateway server:
If the user is a member of any of the following user groups:
INSTRUCTIONS\Domain Admins
If the client computer is a member of any of the following computer groups:
Not applicable (no computer group is specified)
If the user uses the following supported Windows authentication methods:
Actions
Connection Authorization Policies
Create New Policy
Configure Central RD CAP
View
Refresh
Help
allowed-to-use-RDGateway
Disable
Delete
Properties
Help

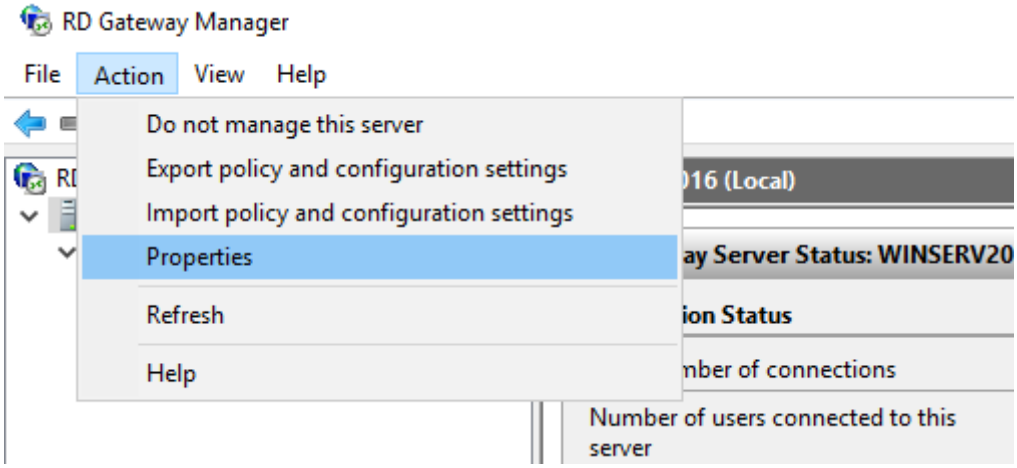

RD Gateway Manager
File Action View Help
RD Gateway Manager
WINSERV2016 (Local)
Policies
Connection Authorization Policies
Resource Authorization Policies
Monitoring
WINSERV2016 (Local)
RD Gateway Server Status: WINSERV2016
WINSERV2016 is not yet fully configured as a RD Gateway server. To access the settings required to complete RD Gateway configuration, click the link provided in each configuration task.
Configuration Status
Configuration Tasks
A server certificate is not yet installed or selected
View or modify certificate properties
RD Gateway Server Status: WINSERV2016
Connection Status
Total number of connections 0
Monitor active connections
Number of users connected to this server 0
Number of resources that users are connected to 0
Configuration Status
Connection authorization policies 1
View connection authorization policies
Resource authorization policies 1
View resource authorization policies
Actions
WINSERV2016 (Local)
Do not manage this server
Export policy and configuration se...
Import policy and configuration s...
Properties
View
Refresh
Help

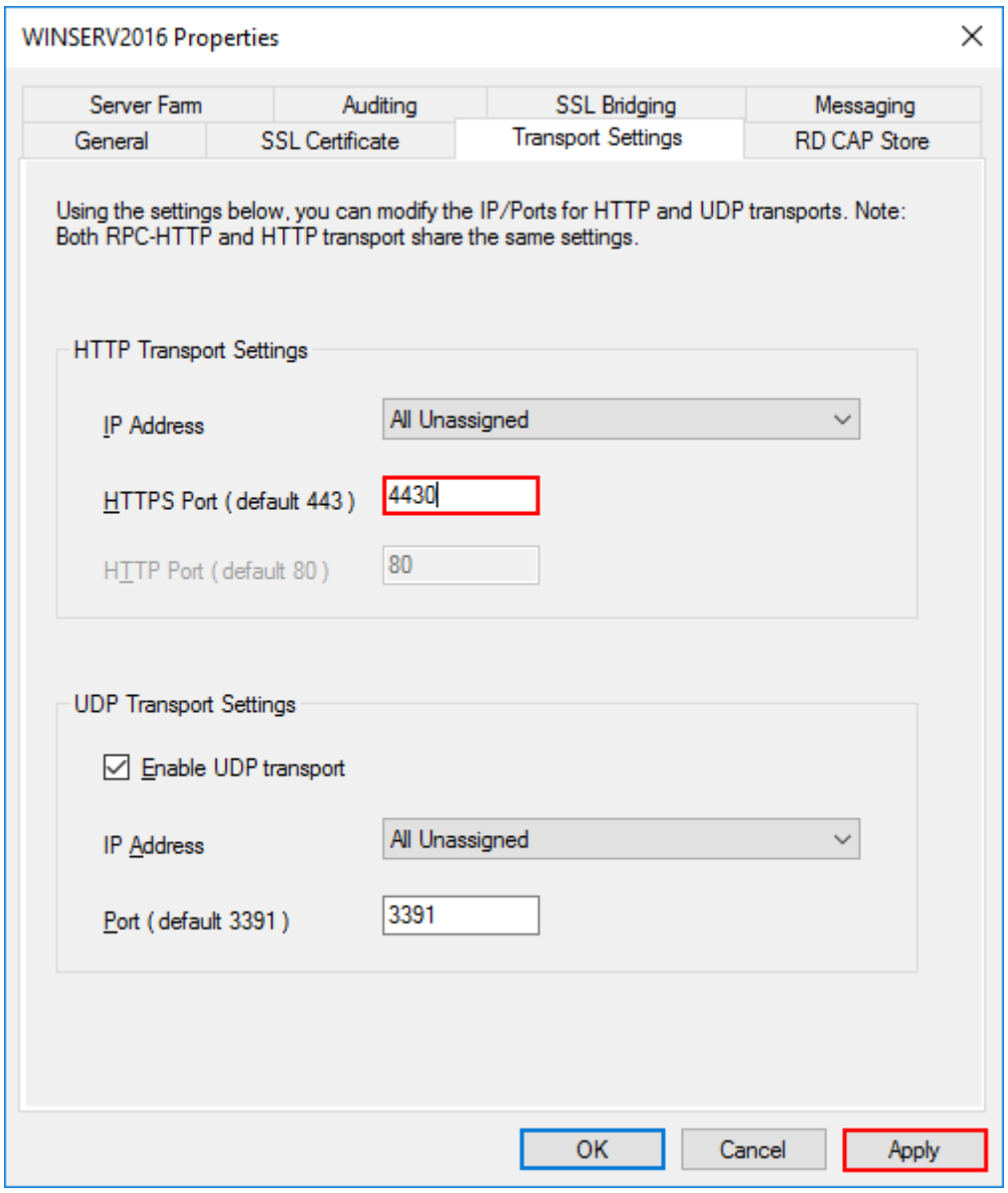

Create Self-Signed Certificate
Create a self-signed certificate matching the RD Gateway FQDN
Certificate name: WinServ2016.instructions.1cloud.ru
Store the root certificate
For clients to connect to this RD Gateway server, you must manually distribute the root certificate of the RD Gateway server to clients. We recommend that you store the root certificate in the following directory:
C:\Users\Administrator\Documents
File name: C:\Users\Administrator\Documents\WINSERV2016.cer
Browse...
More about certificates for RD Gateway.
OK
Cancel

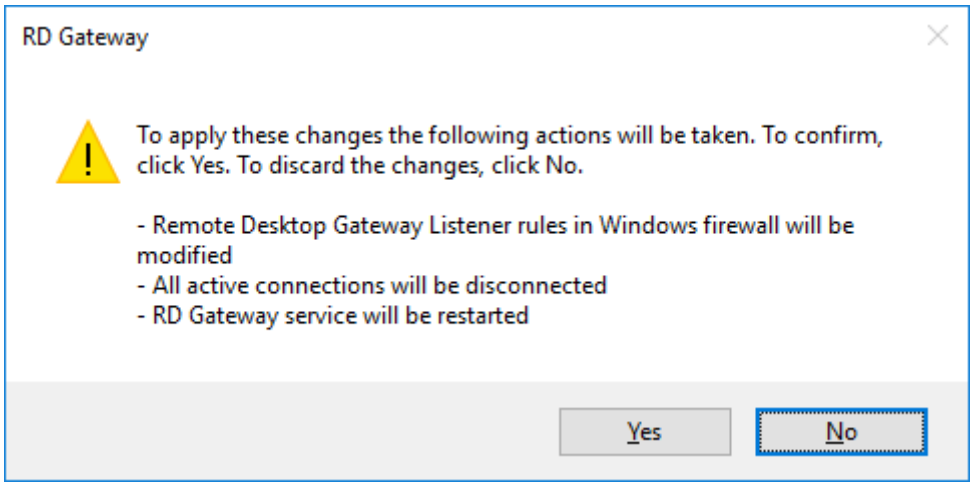

RD Gateway
RD Gateway has successfully created a self-signed certificate. The certificate is stored in the following file:
C:\Users\Administrator\Documents\WINSERV2016.cer
OK

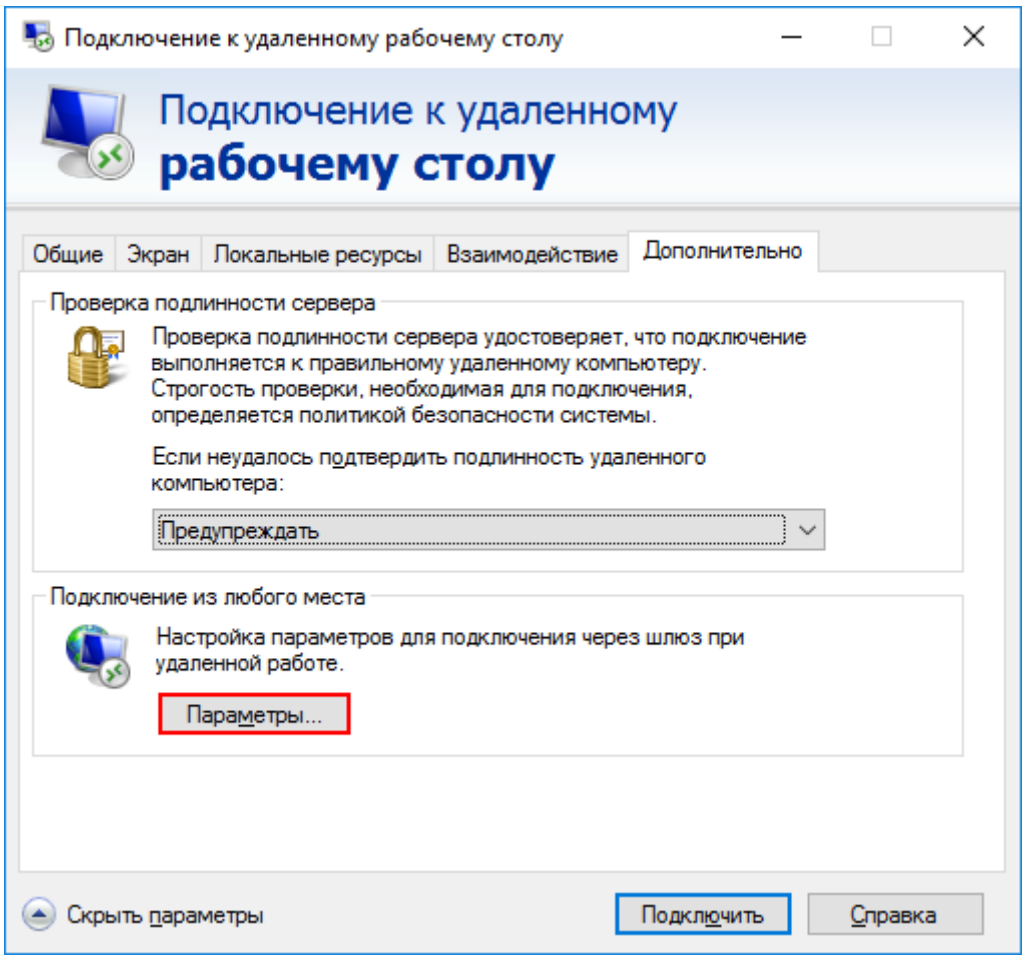

WINSERV2016 Properties
Server Farm
Auditing
SSL Bridging
Messaging
General
SSL Certificate
Transport Settings
RD CAP Store
Certificate is needed for secure communication of HTTPS/UDP listeners and for NAP messaging. Certificate is automatically bound to the configured HTTP and UDP ports.
For RD Gateway to function correctly, you must select an existing SSL certificate or create a self-signed certificate.
Issued to: WinServ2016.instructions.1cloud.ru
Issued by: WinServ2016.instructions.1cloud.ru
Expiration date: 29.11.2018
Specify the type of SSL certificate to import for the RD Gateway server by doing one of the following:
Create a self-signed certificate
Create and Import Certificate...
Select an existing certificate from the RD Gateway WINSERV2016 Certificates (Local Computer)/Personal store
Import Certificate...
Import a certificate into the RD Gateway WINSERV2016 Certificates (Local Computer)/Personal store
Browse and Import Certificate...
OK
Cancel
Apply

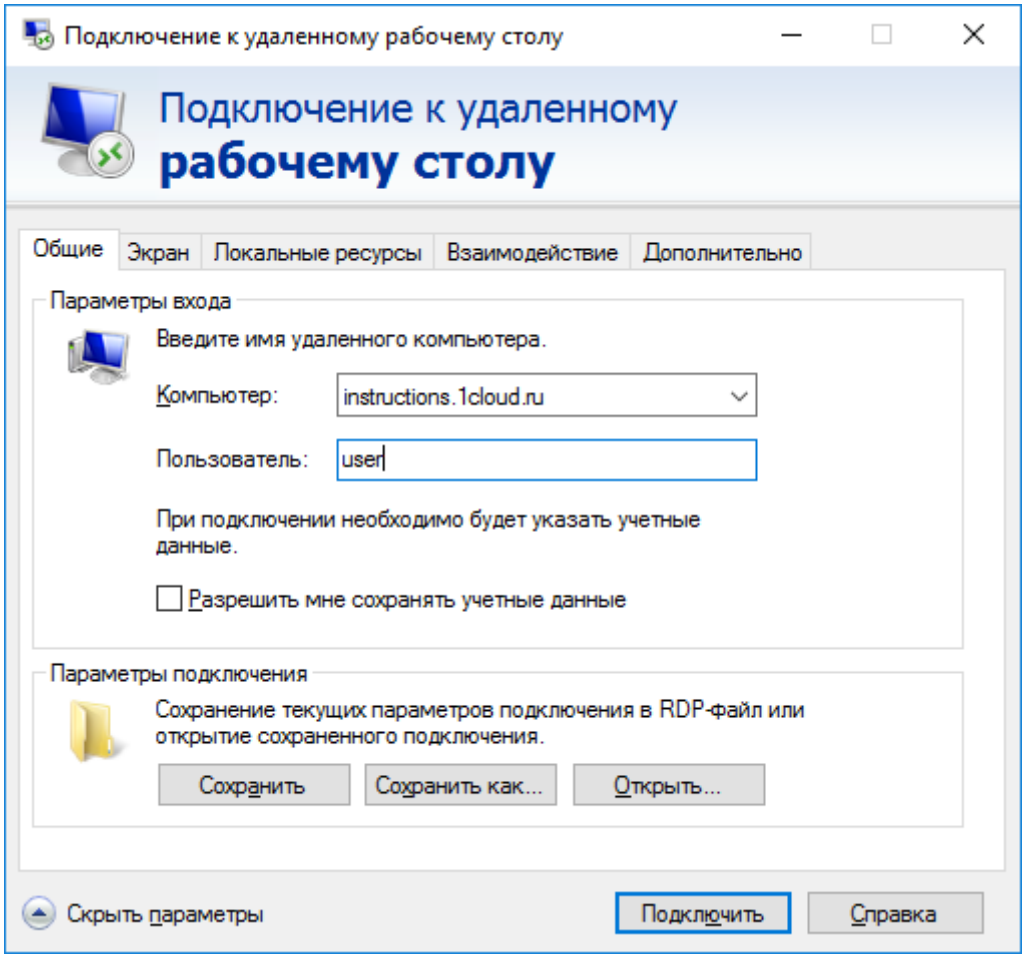

RD Gateway Manager
File Action View Help
RD Gateway Manager
WINSERV2016 (Local)
Policies
Connection Authorization Policies
Resource Authorization Policies
Monitoring
WINSERV2016 (Local)
RD Gateway Server Status: WINSERV2016
Connection Status
Total number of connections 0
Monitor active connections
Number of users connected to this server 0
Number of resources that users are connected to 0
Configuration Status
Connection authorization policies 1
View connection authorization policies
Resource authorization policies 1
View resource authorization policies
RD Gateway server farm members 0
Add RD Gateway Server Farm members
Actions
WINSERV2016 (Local)
Do not manage this server
Export policy and configuration se...
Import policy and configuration s...
Properties
View
Refresh
Help

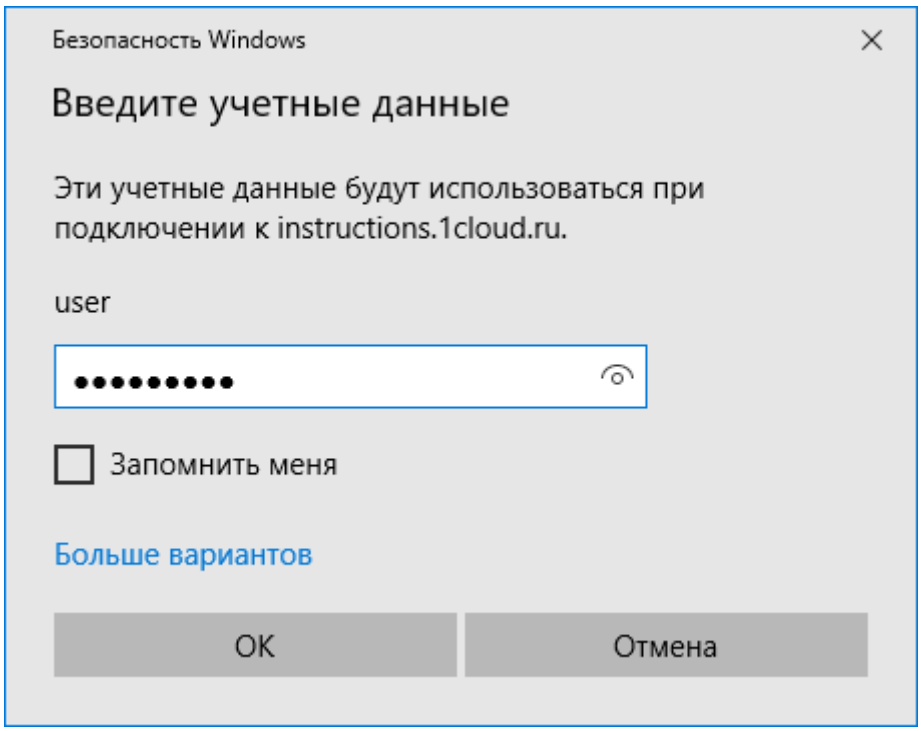

RD Gateway Manager
File
Action
View
Help
Do not manage this server
Export policy and configuration settings
Import policy and configuration settings
Properties
Refresh
Help
016 (Local)
ay Server Status: WINSERV20
ion Status
nber of connections
Number of users connected to this server


WINSERV2016 Properties
Server Farm
Auditing
SSL Bridging
Messaging
General
SSL Certificate
Transport Settings
RD CAP Store
Using the settings below, you can modify the IP/Ports for HTTP and UDP transports. Note: Both RPC-HTTP and HTTP transport share the same settings.
HTTP Transport Settings
IP Address
All Unassigned
HTTPS Port (default 443)
4430
HTTP Port (default 80)
80
UDP Transport Settings
Enable UDP transport
IP Address
All Unassigned
Port (default 3391)
3391
OK
Cancel
Apply


RD Gateway
To apply these changes the following actions will be taken. To confirm, click Yes. To discard the changes, click No.
- Remote Desktop Gateway Listener rules in Windows firewall will be modified
- All active connections will be disconnected
- RD Gateway service will be restarted
Yes
No


Подключение к удаленному рабочему столу
Подключение к удаленному
рабочему столу
Общие
Экран
Покальные ресурсы
Взаимодействие
Дополнительно
Проверка подлинности сервера
Проверка подлинности сервера удостоверяет, что подключение выполняется к правильному удаленному компьютеру. Строгость проверки, необходимая для подключения, определяется политикой безопасности системы.
Если неудалось подтвердить подлинность удаленного компьютера:
Предупреждать
Подключение из любого места
Настройка параметров для подключения через шлюз при удаленной работе.
Параметры...
Скрыть параметры
Подключить
Справка


Подключение к удаленному рабочему столу
Подключение к удаленному
рабочему столу
Общие
Экран
Покальные ресурсы
Взаимодействие
Дополнительно
Параметры входа
Введите имя удаленного компьютера.
Компьютер:
instructions.1cloud.ru
Пользователь:
user
При подключении необходимо будет указать учетные данные.
Разрешить мне сохранять учетные данные
Параметры подключения
Сохранение текущих параметров подключения в RDP-файл или открытие сохраненного подключения.
Сохранить
Сохранить как...
Открыть...
Скрыть параметры
Подключить
Справка




```
PS C:\Users\user> tracert 1cloud.ru

Tracing route to 1cloud.ru [5.200.50.90]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  5.200.47.1
  2     3 ms     2 ms     8 ms  5.200.46.254
  3    12 ms    <1 ms    <1 ms  fw-5-200-46-220.it-grad.ru [5.200.46.220]
  4     1 ms    <1 ms    <1 ms  5.200.50.90

Trace complete.
```

3.1.2 Оценка освоения теоретического курса профессионального модуля по МДК.05.02

Дидактические единицы	Проверяемые ОК, ПК, У, З	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
Тема 2.1. Безопасность облачных сервисов	ПК 5.5 ОК1-9 З17-35 У9-14	Устный зачет по теме 2.1	Теоретические вопросы на дифференцированном зачете
		Практическая работа №1 Настройка WAF (Web Application Firewall)	
		Практическая работа № 9 Развёртывание защиты от DDoS атак	

Устный зачет по теме 2.1

Инструкция для обучающихся

Зачет сдается в рамках учебного занятия. Каждый студент отвечает в устной форме на предложенные преподавателем 6 мини-вопросов.

Выполнение задания: одному студенту на ответ выделяется 3 мин., группа сдает зачет за одно учебное занятие.

Перечень вопросов:

1. Виды угроз безопасности для облачных сервисов.
2. Современные методики и технологии защиты облачных данных.
3. Шифрование данных в облаке
4. Использование сложных паролей и многофакторной аутентификации
5. Технология защиты: SSL
6. Методики мониторинга состояния сети
7. Стратегия защиты от DoS и DDoS атак
8. Технологии резервного копирования облака, общие правила хранения данных
9. Стратегии аварийного восстановления данных

Практическая работа №1 Настройка WAF (Web Application Firewall)

Инструкция для обучающихся

Внимательно прочитайте задание. Выполните все необходимые операции.

Время выполнения – 90 минут.

Задание

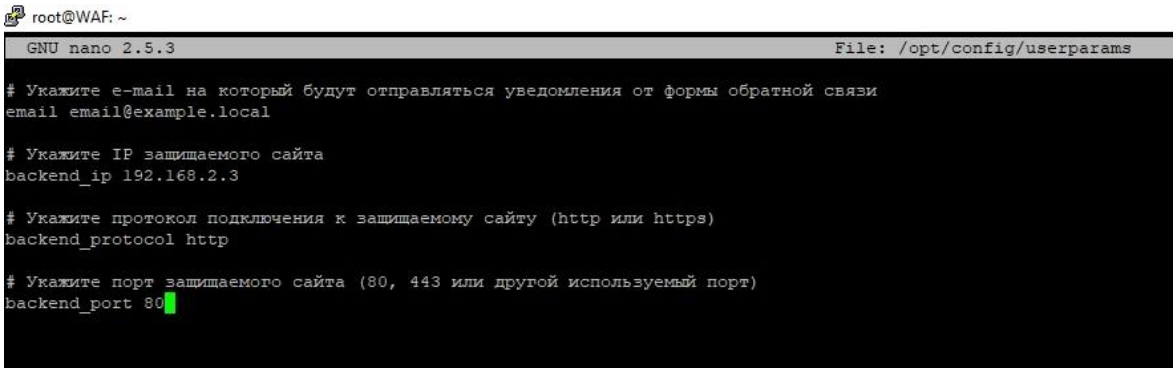
1. Для быстрого внедрения WAF клиентам в Public Catalogs доступен шаблон WAF-modsecurity.

   Шаблон на Ubuntu 16.04 LTS включает:
   - Nginx/1.13.12
   - ModSecurity for Nginx/3.0.0
   - OWASP ModSecurity Core Rule Set Version 3.0.0
   - Модуль Nginx Length Hiding Filter Module
   - Модуль Nginx Headers More Module
   - OpenSSL 1.0.2g
   - Fail2Ban
   - Форму обратной связи для оповещения о ложных срабатываниях WAF

Для первоначальной настройки необходимо:

1. Скопировать имеющиеся у Вас SSL сертификаты в папку **/opt/ssl,** переименовав их в ssl_certificate.crt и ssl_certificate.key (шаблон WAF подразумевает, что защищаемый сайт использует HTTPS);

2. Внести в файл **/opt/config/userparams** следующие данные:

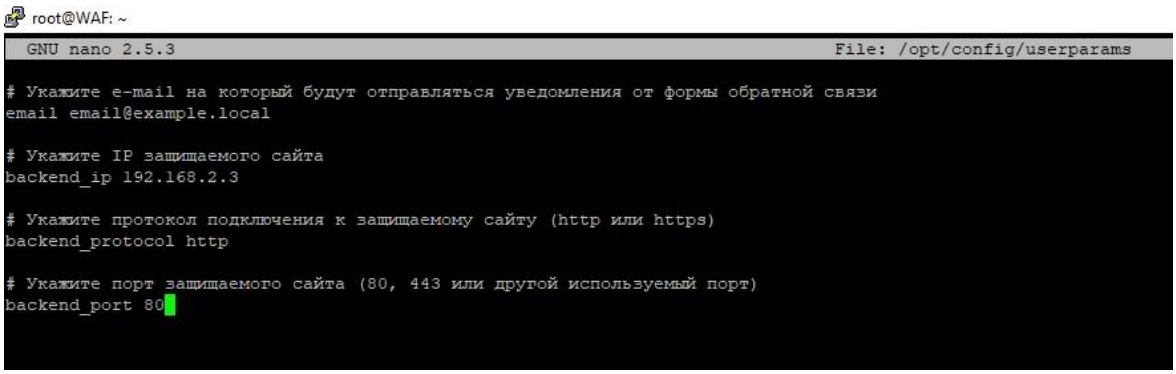


3. Выполнить скрипт **/opt/config/set_userparams.sh,** который перенесёт указанные параметры в конфигурацию Nginx и форму обратной связи.

После этого WAF готов к работе.

Для проверки WAF можно открыть сайт, добавив в адресную строку ?testparam=test
Например, https://Ваш IP/?testparam=test
Если все настроено правильно, откроется форма обратной связи с предложением отправить сообщение администратору о ложном срабатывании WAF.
При нажатии на кнопку "Unblock \\ Разблокировать" на указанный ранее E-mail будет отправлено письмо с техническими данными, данными из логов и текстом сообщения администратору.

Эталон ответа



Практическая работа № 9 Развёртывание защиты от DDoS атак

Инструкция для обучающихся

Внимательно прочитайте задание. Выполните все необходимые операции.

Время выполнения – 90 минут.

Задание

Стенд состоит из трёх основных частей:

1. Виртуальная среда на базе VMWare, имитирующая локальную сеть + ЦОД (слева на схеме)
2. Межсетевой экран HP NGFW
3. Виртуальная среда, имитирующая сегмент сети Интернет (справа на схеме)

Виртуальная среда, имитирующая локальную сеть, представляет собой развернутые на рабочей станции виртуальные машины на базе операционной системы Windows. Для имитации работы вредоносного ПО, на часть виртуальных машин установлен тестирующий агент, способный сгенерировать DDoS трафик.

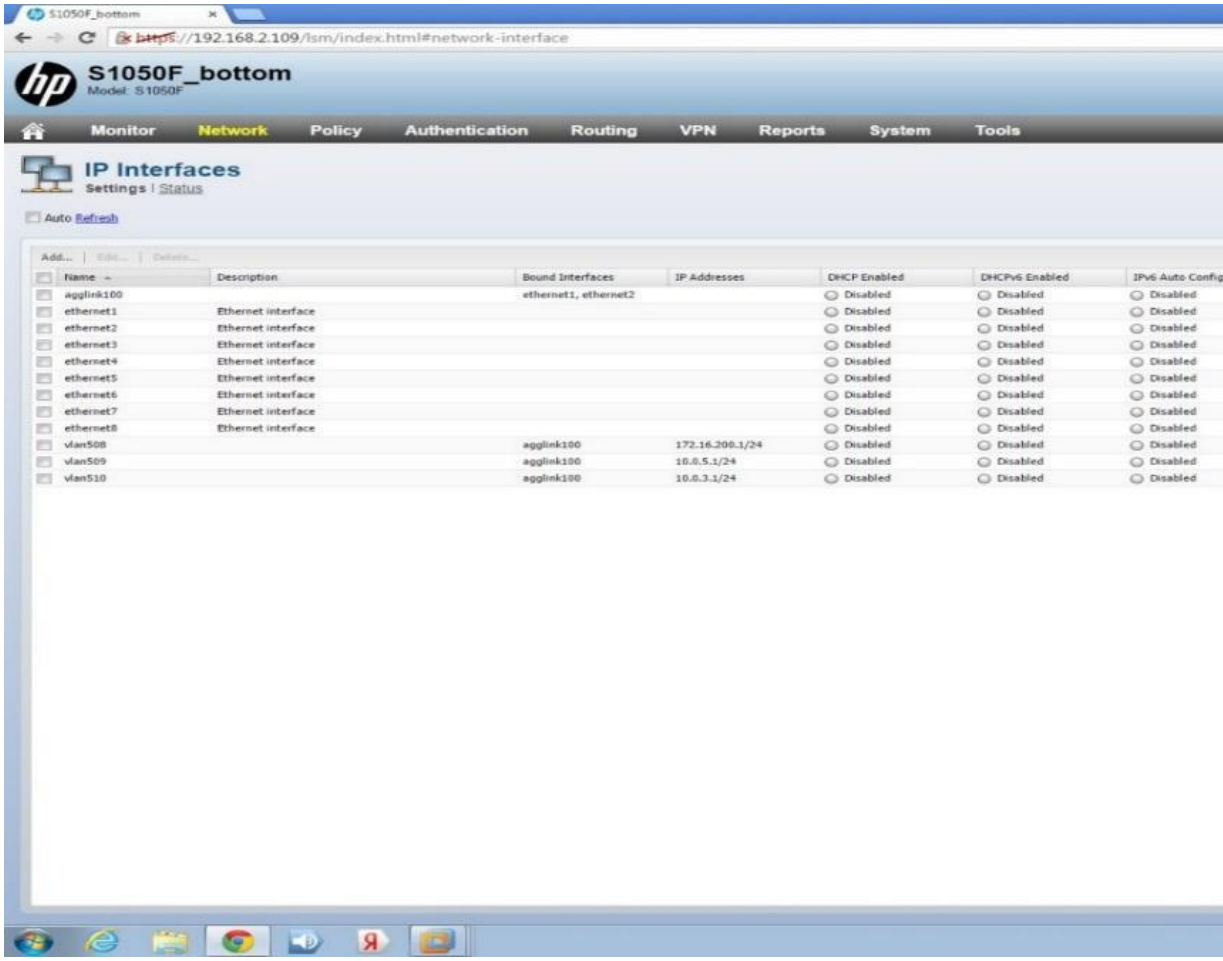
Межсетевой экран установлен в разрыв между сегментом Интернет и локальной сетью и в данном стенде представляет собой устройство третьего уровня, маршрутизирующее трафик между сегментами. Базовые правила и настройки межсетевого экрана показаны на схеме выше.

Виртуальная среда, имитирующая сегмент Интернет, представляет собой набор виртуальных машин на базе операционной системы Linux с установленном на них специализированным ПО – в числе прочего, веб-сервер Apache, сервер баз данных

MySQL, интерпретатор языка PHP версии 5, сканер безопасности Nessus, утилита сканирования сети nmap.

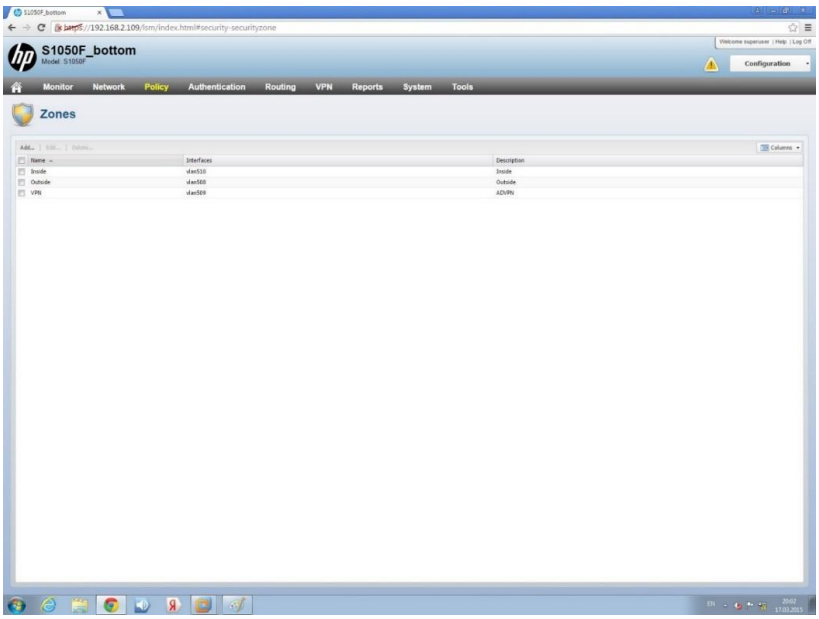
Базовая конфигурация межсетевого экрана

Ниже приведены базовые настройки NGFW в соответствии с разработанной схемой стенда, приведенной на рисунке 3. Все настройки показаны в собственном веб-интерфейсе NGFW. На рисунке 4 приведены настройки IP интерфейсов FW в соответствии со схемой приведенной выше.



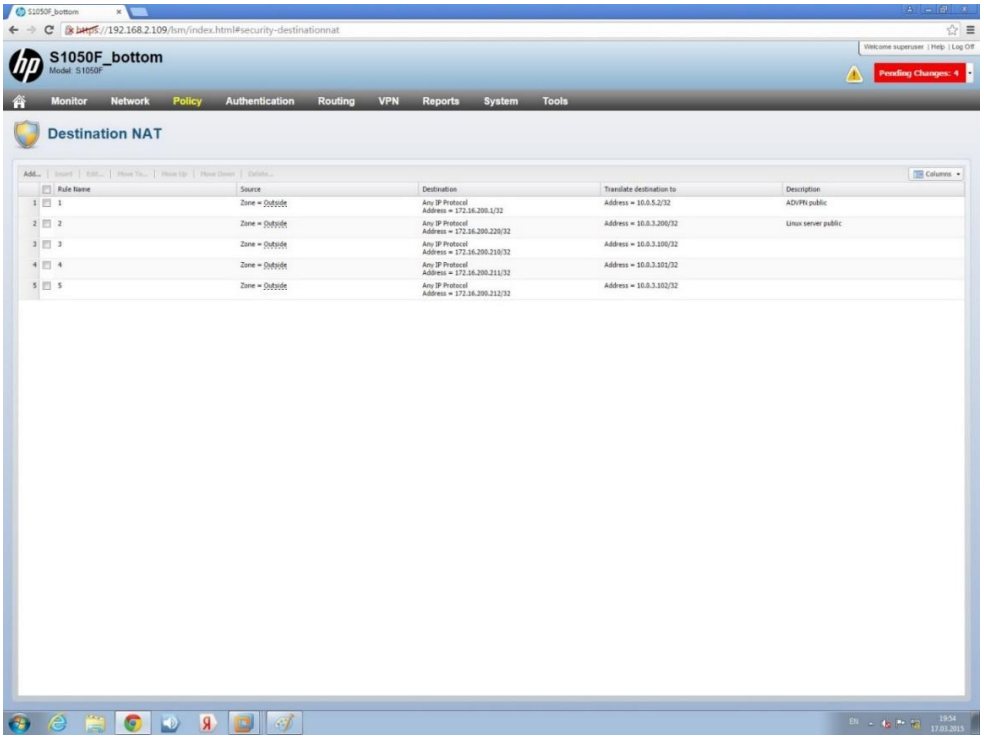
Настройки IP интерфейсов

Ниже показаны настройки зон безопасности. В стенде для простоты настроено три зоны безопасности – Inside, Outside и VPN.



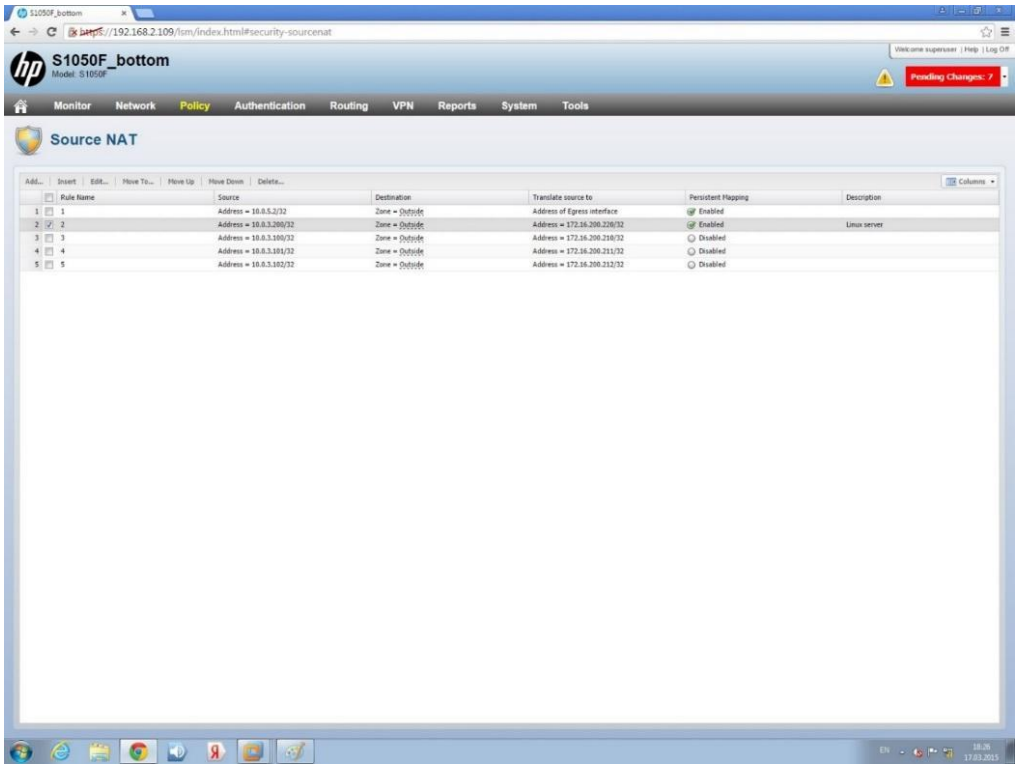
Настройки зон безопасности

На рисунке 6 показаны базовые настройки, сделанные для Destination NAT. Опубликовано несколько внутренних адресов виртуальных машин, на которых запущены различные сетевые сервисы (HTTP/HTTPS, FTP и т.д.).



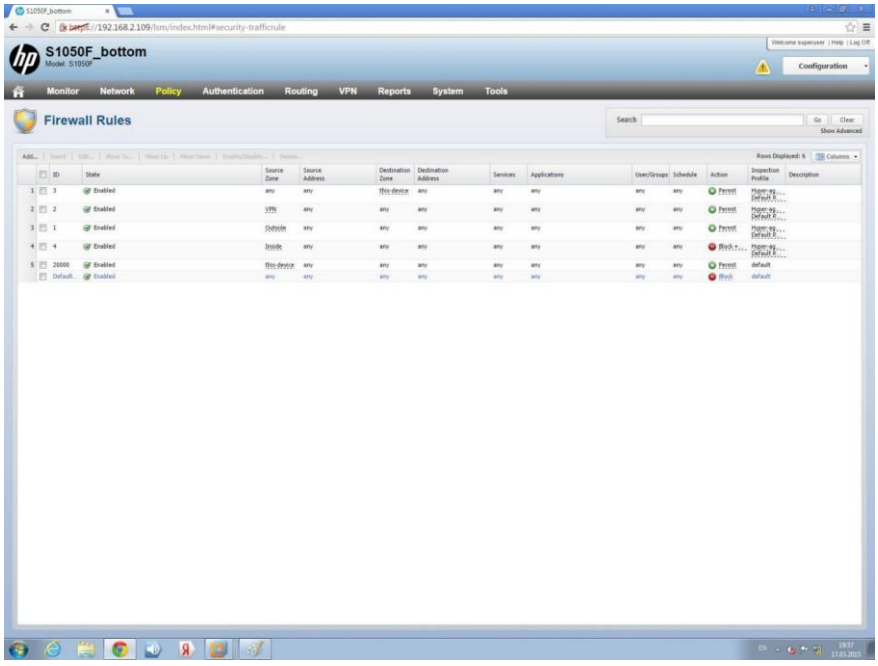
Настройки Destination NAT

Ниже показаны базовые настройки Source NAT. Несколько адресов виртуальных машин транслированы во внешние адреса, чтобы обеспечить их доступ к эмулированным сервисам с вредоносным ПО.



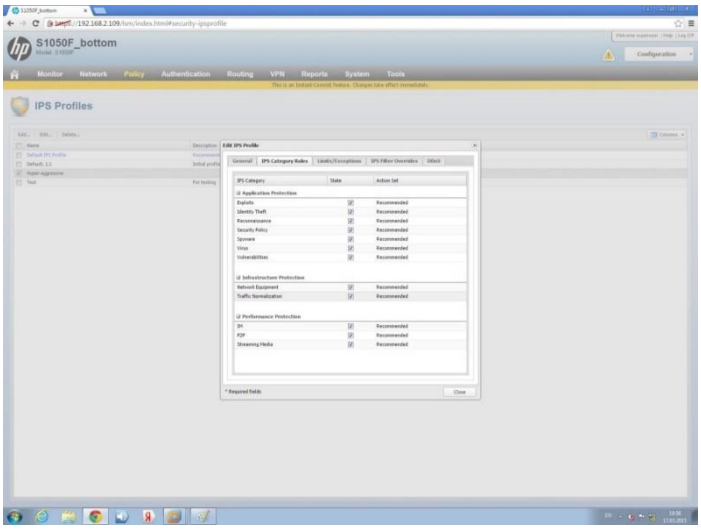
Source NAT

Базовые настройки FW Policy, в соответствии с которыми обрабатывается трафик, показаны на рисунке 8. Для того, чтобы проверить как отрабатывает политика IPS, настроенная по умолчанию, мы пропустим весь трафик через базовые фильтры Stateful FW прозрачно.



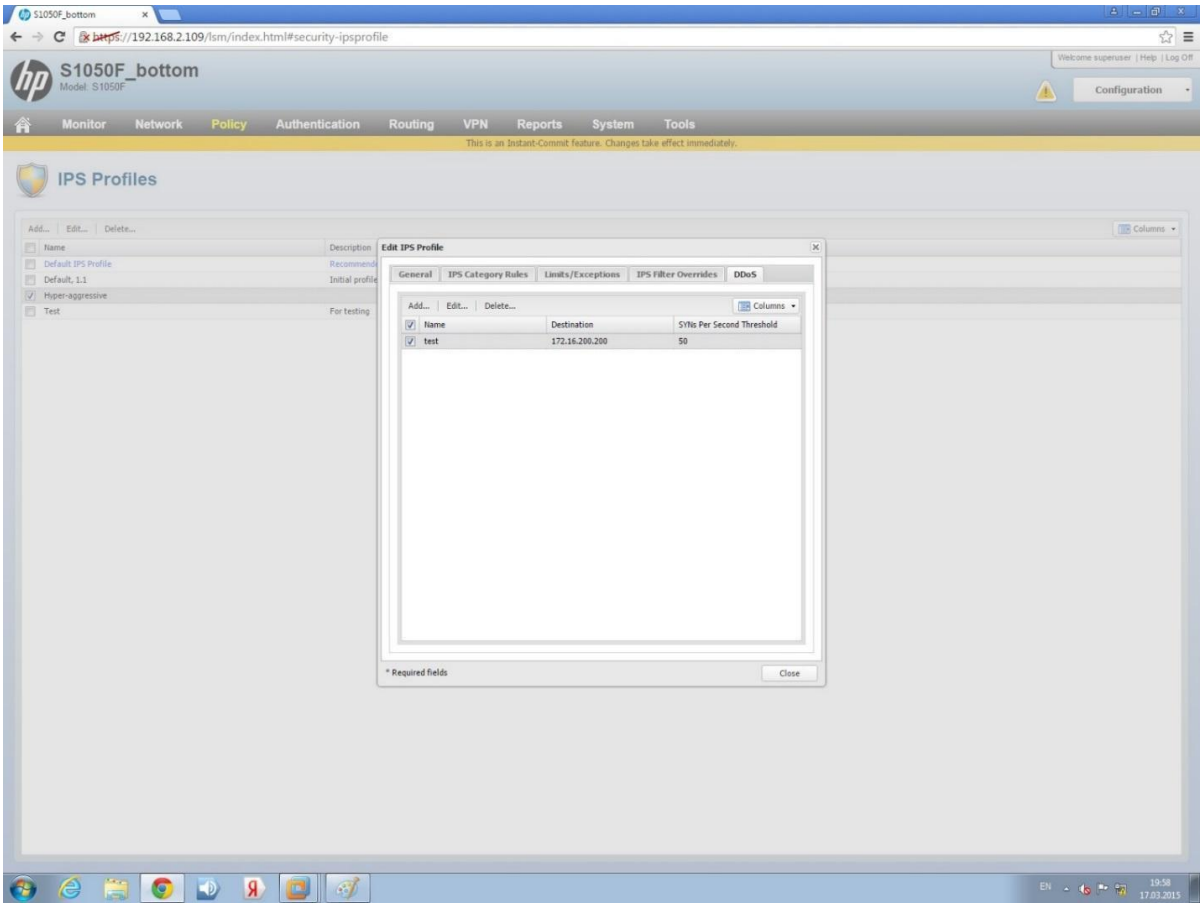
FW Policy

Базовые настройки системы противодействия вторжениям (IPS). Все рекомендованные категории фильтрации IPS включены в данном тесте.



Базовые настройки IPS

Настройка порогов для атак типа DDoS. Порог срабатывания IPS на DDoS атаку типа SYN FLOOD – 100 пакетов в секунду.

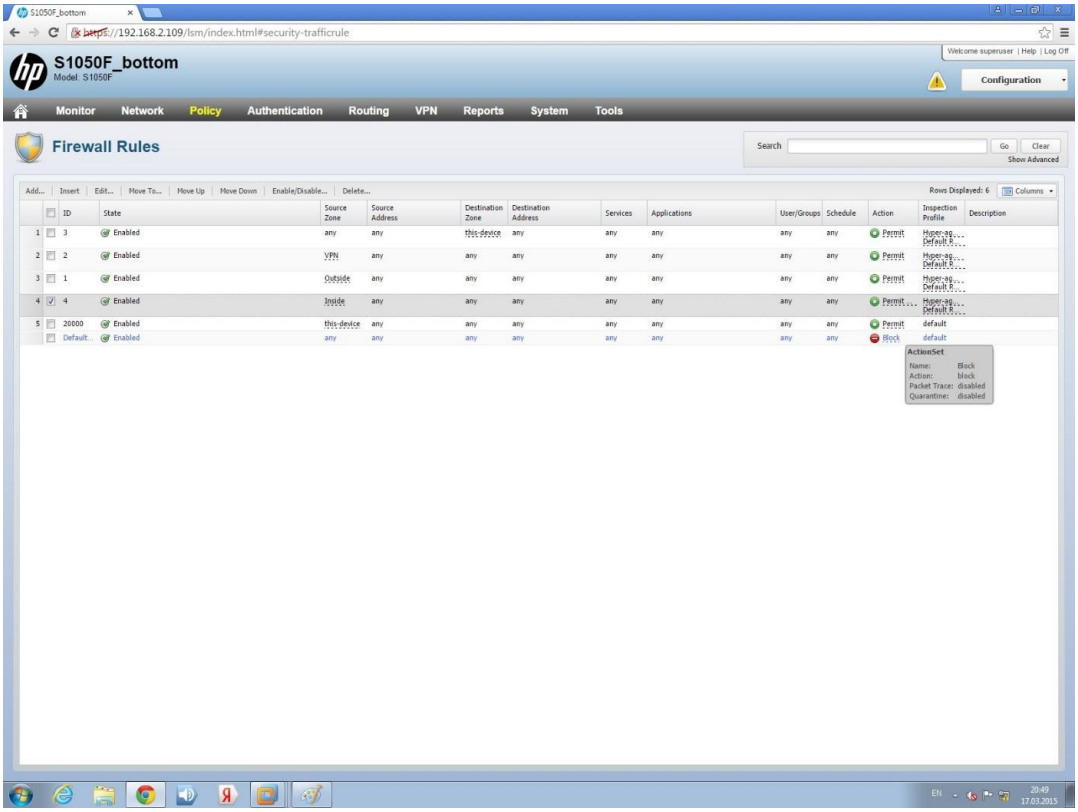


IPS DDoS

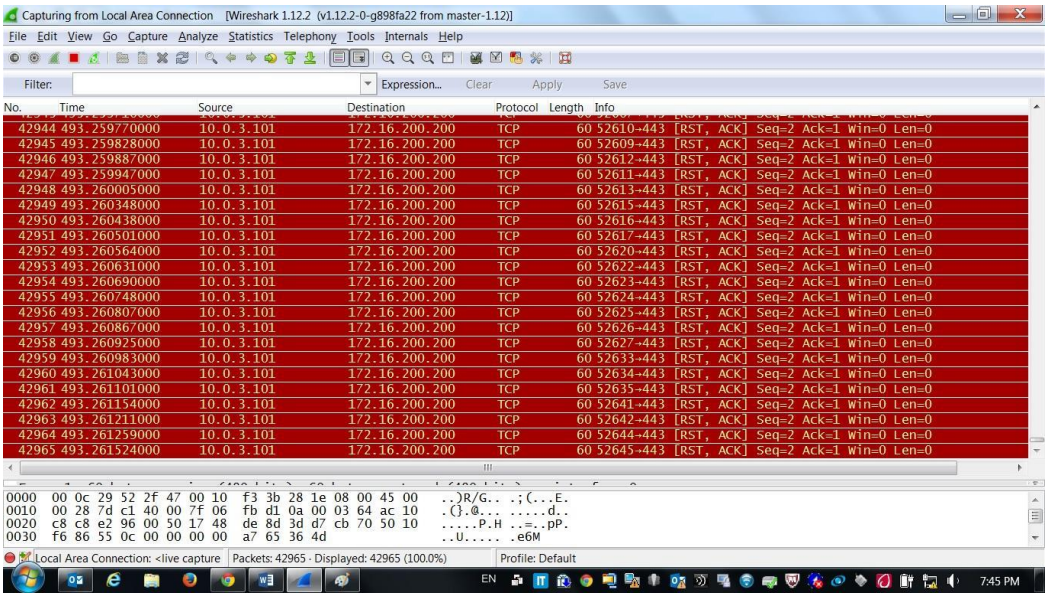
Эмулируем атаку согласно классической схеме, приведенной в части 2 серии и попытаемся защититься от атаки при помощи NGFW. При этом, в реальной DDoS атаке фильтровать по портам/адресам – подход неэффективный, так как заражённые машины разбросаны, как правило, по сети и имеют хаотически разбросанные адреса. Поэтому пропускаем весь трафик на IPS и, как показано выше, настраива-

ем в IPS правило защиты от DDoS:

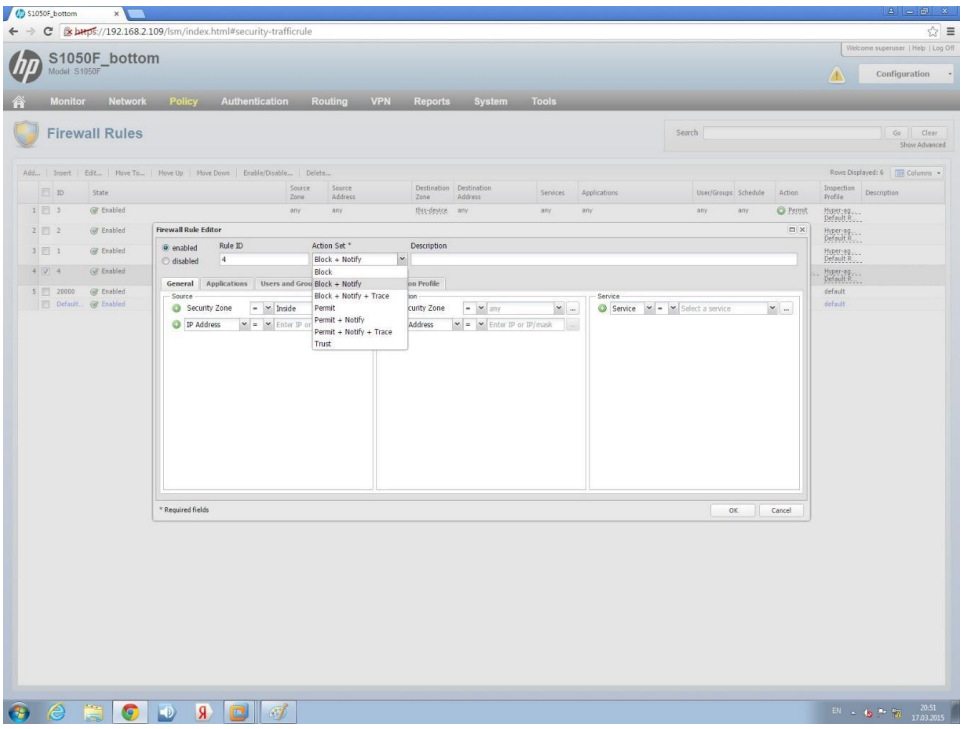
1. Чтобы убедиться, что работает именно IPS, выключаем на NGFW правило, по которому трафик хоста-источника сетевой атаки будет блокирован:



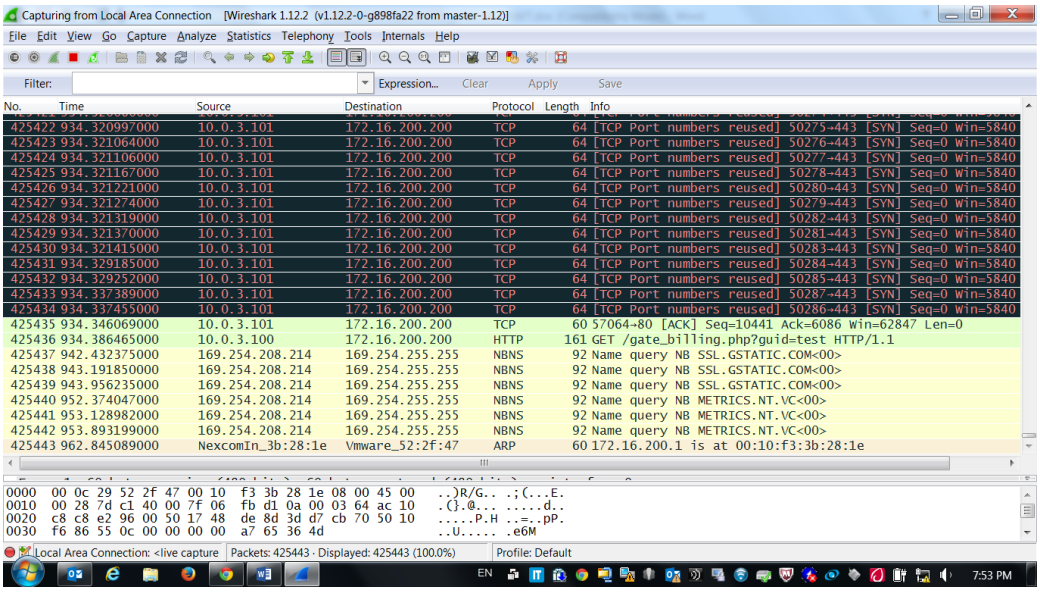
2. Запускаем сетевую атаку DDoS и смотрим в логи Wireshark и наблюдаем классическую DoS атаку с зараженной агентом виртуальной машины:



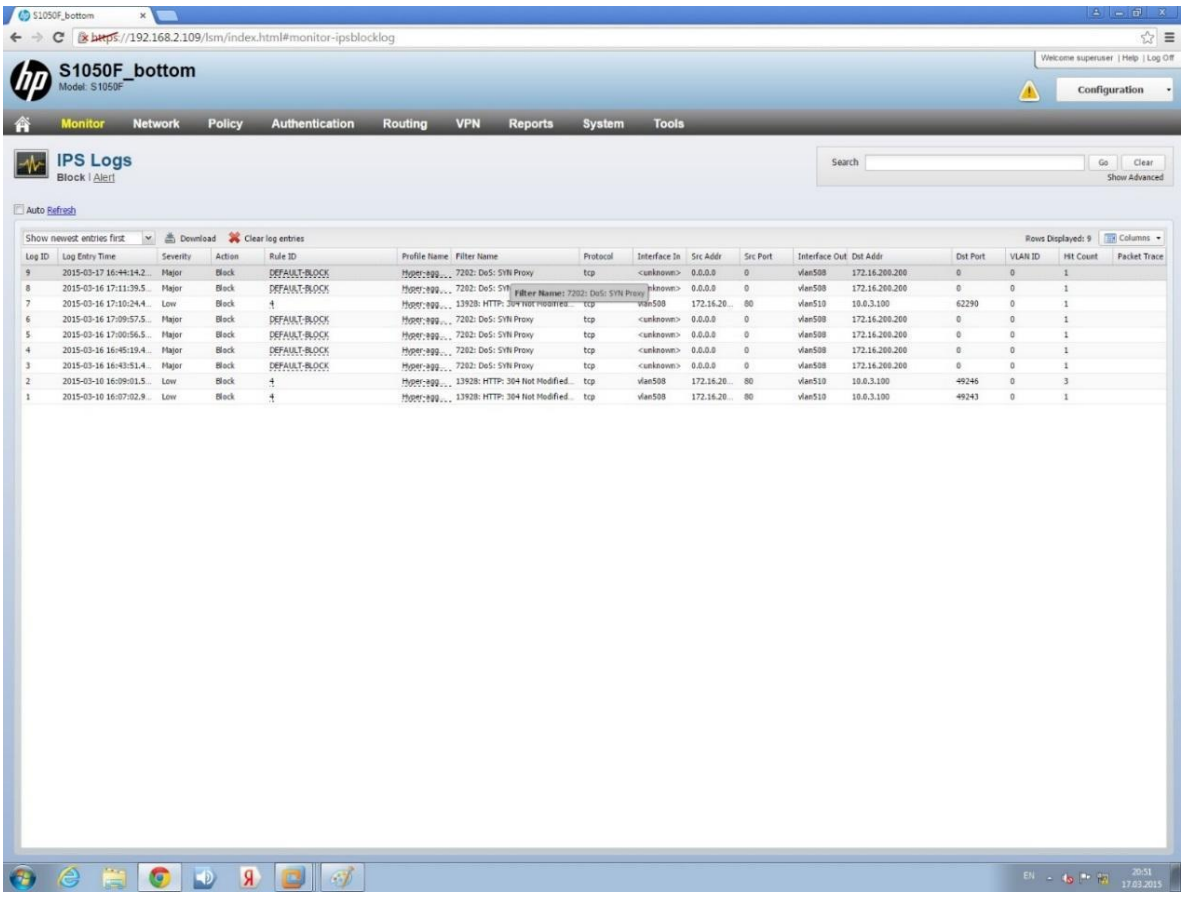
3. Включаем на NGFW IPS правило, блокирующее трафик хоста, с которого идет сетевая атака:



4. Убеждаемся в логах Wireshark, что правило сработало и DoS атака прекращена:

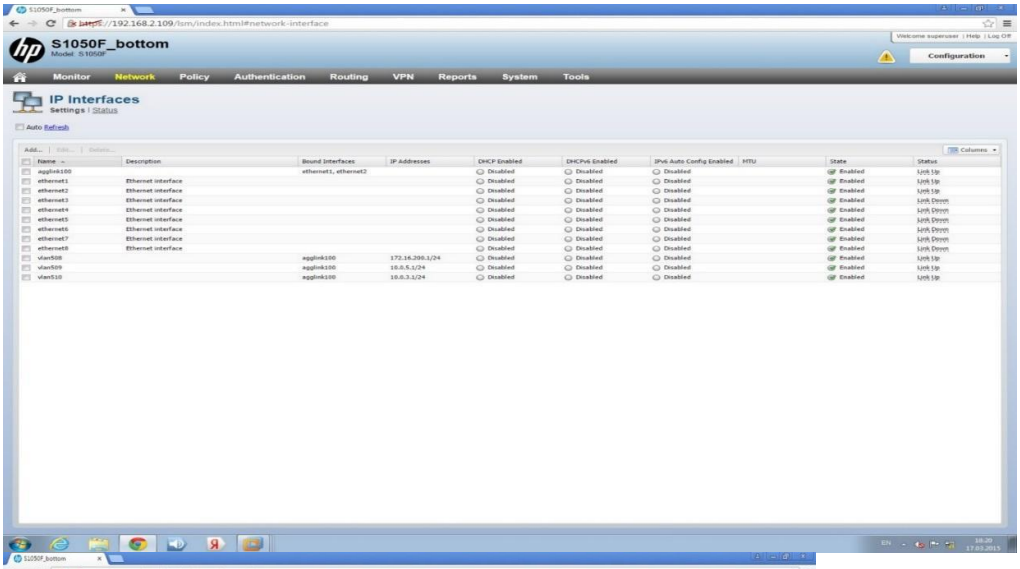


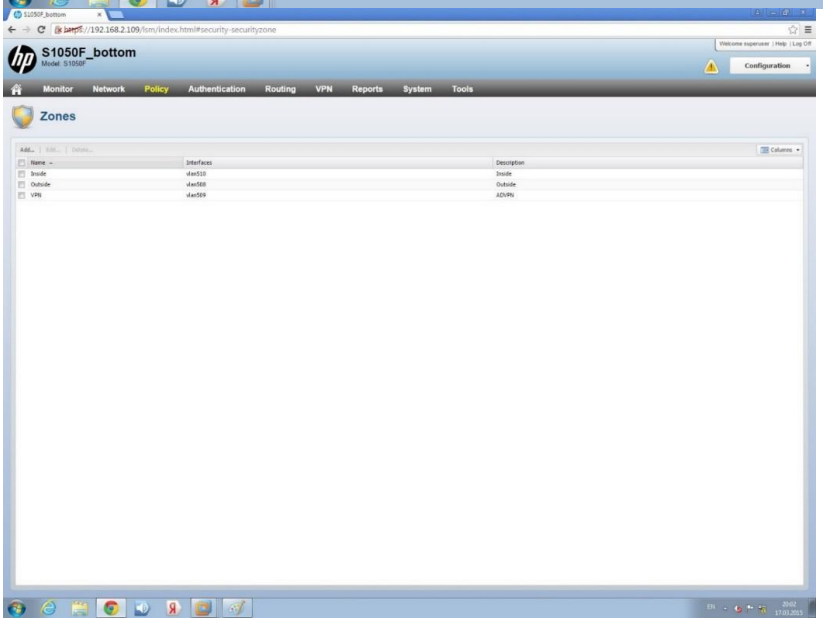
5. Смотрим в логи NGFW и отмечаем, что атака обнаружена и трафик с атакующего хоста закрыт:

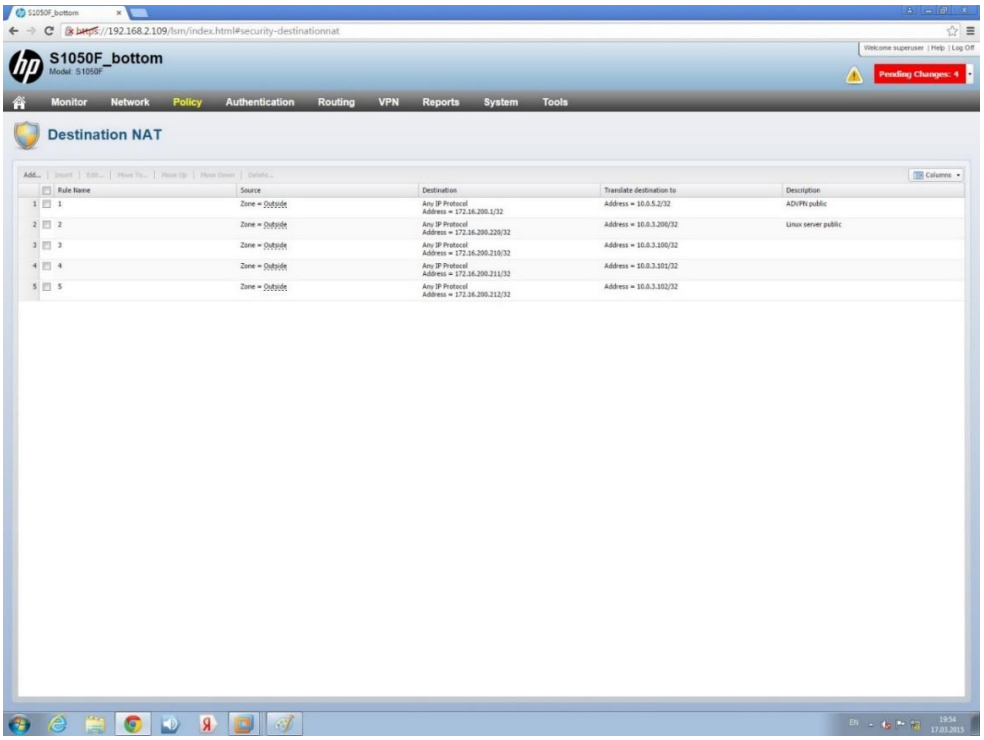


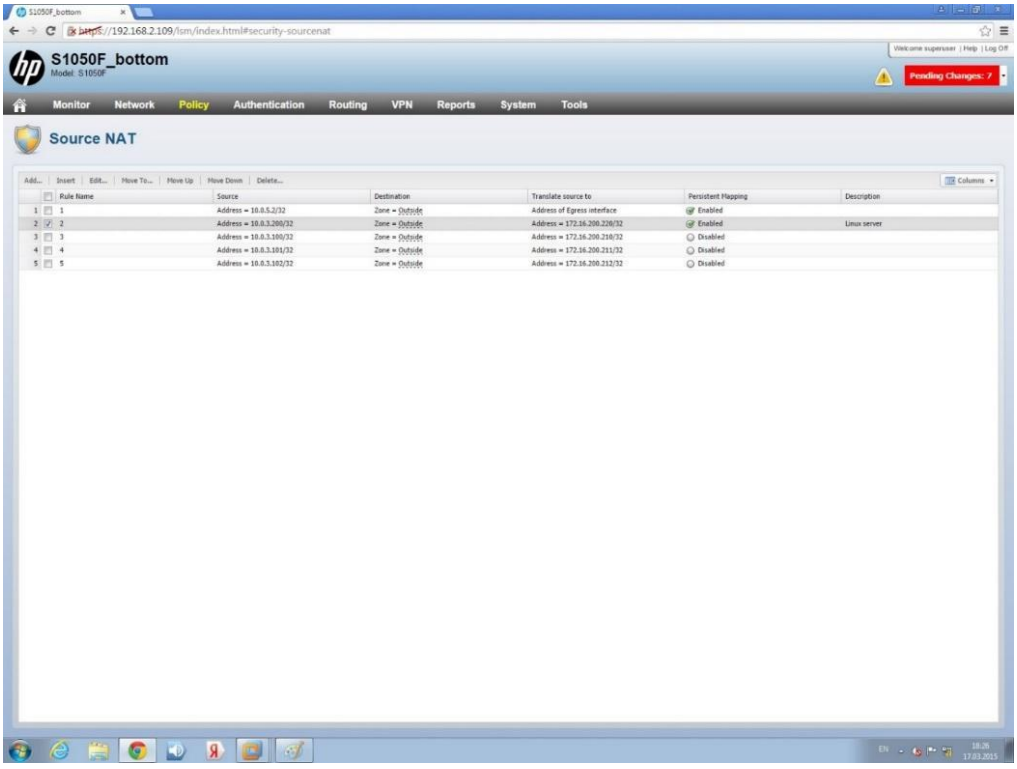
Данный пример показывает, как при помощи правил, преднастроенных в системе обнаружения вторжений NGFW, обнаруживаются и предотвращаются классические атаки типа DDoS.

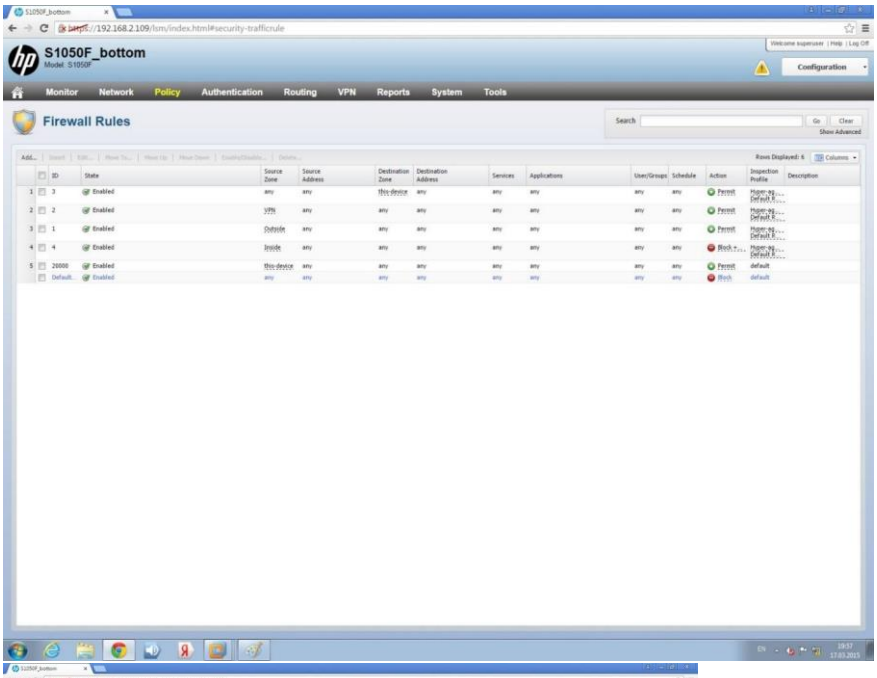
Эталон ответа:

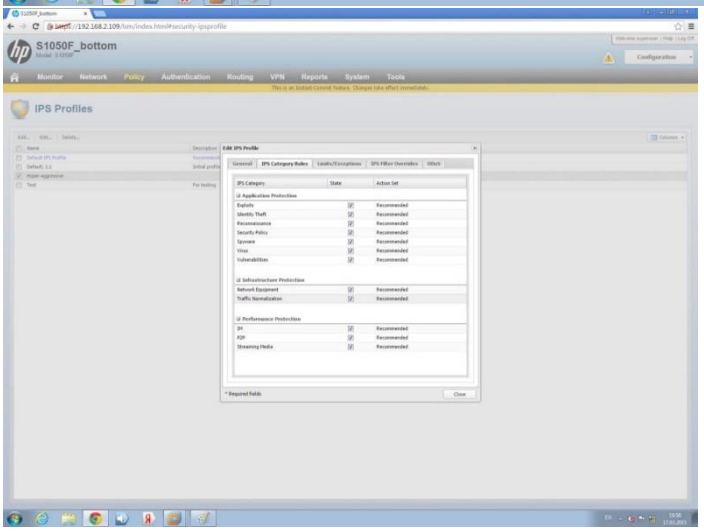


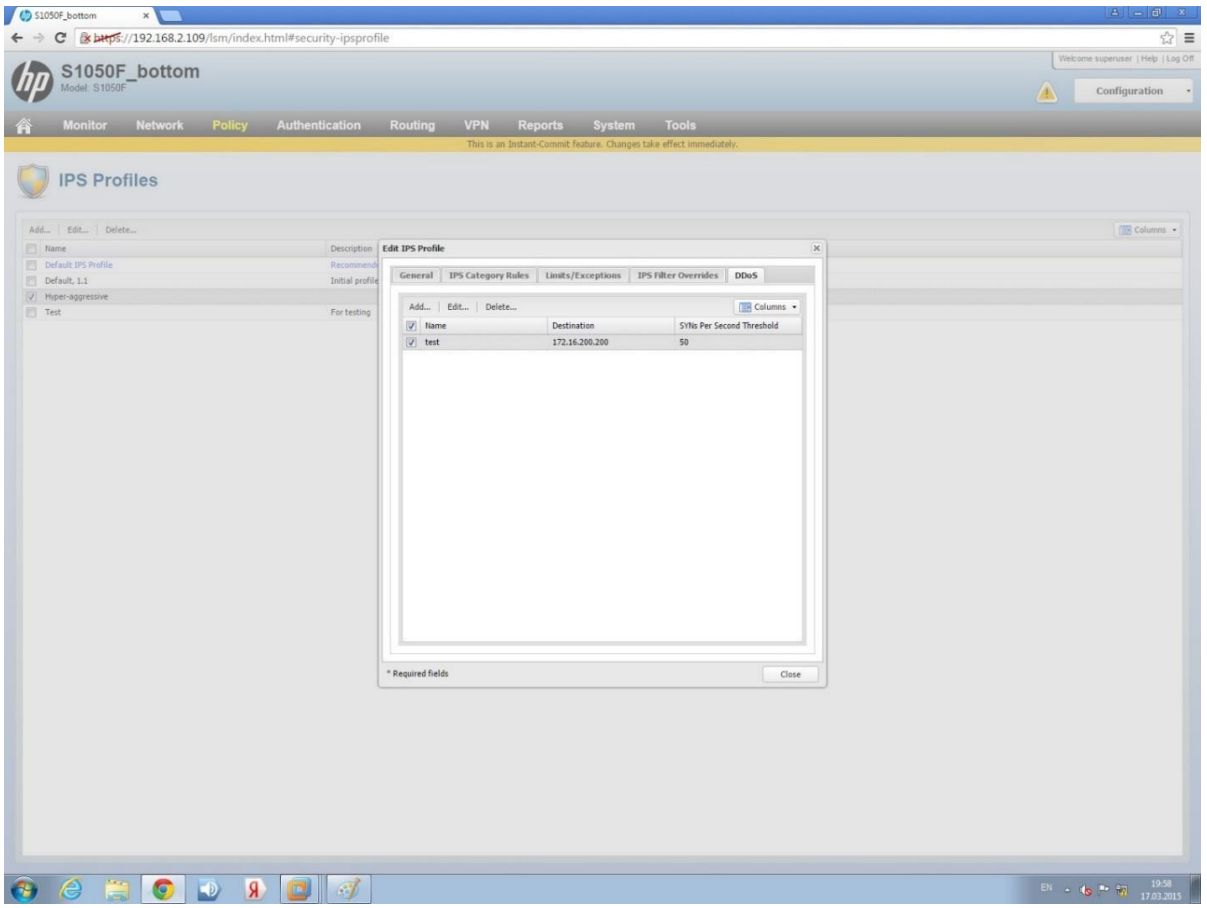


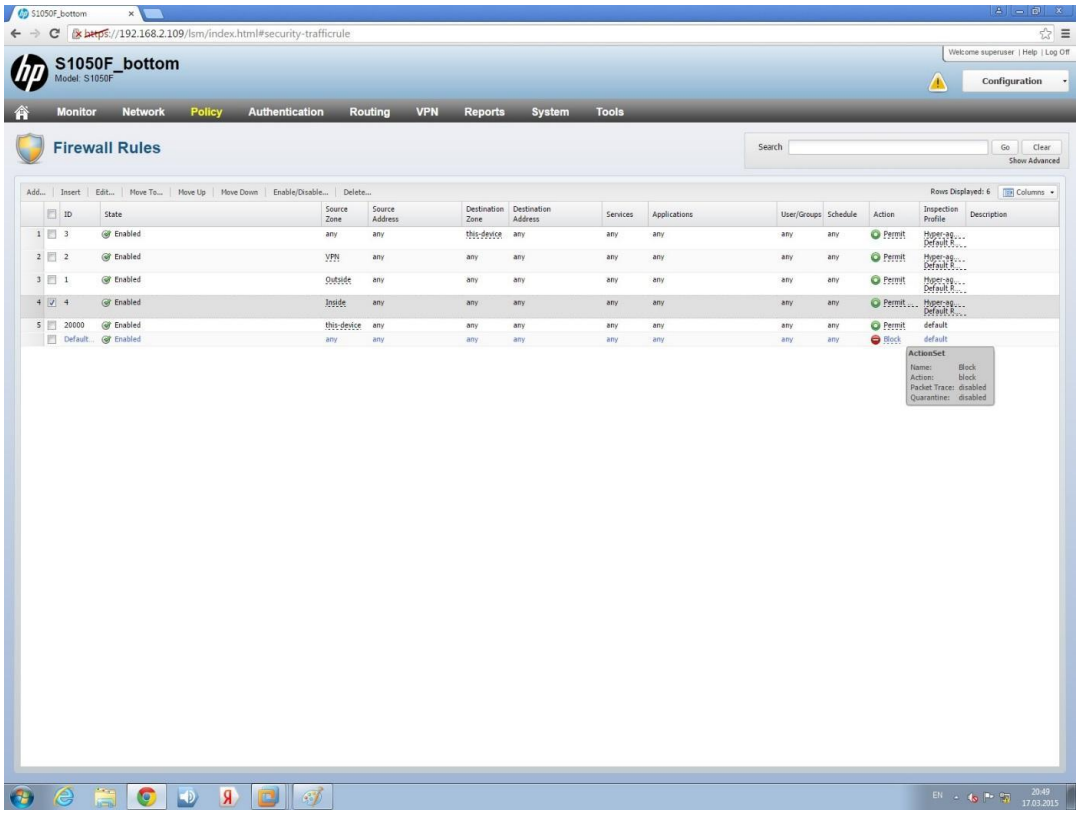

S1050F_bottom
https://192.168.2.109/lsm/index.html#security-destinationnat
S1050F_bottom
Model: S1050F
Pending Changes: 4
Monitor
Network
Policy
Authentication
Routing
VPN
Reports
System
Tools
Destination NAT
Rule Name
Source
Destination
Translate destination to
Description
1
Zone = Outside
Any IP Protocol
Address = 172.16.200.1/32
Address = 10.0.5.2/32
ADVPN public
2
Zone = Outside
Any IP Protocol
Address = 172.16.200.220/32
Address = 10.0.3.200/32
Linux server public
3
Zone = Outside
Any IP Protocol
Address = 172.16.200.210/32
Address = 10.0.3.100/32
4
Zone = Outside
Any IP Protocol
Address = 172.16.200.211/32
Address = 10.0.3.101/32
5
Zone = Outside
Any IP Protocol
Address = 172.16.200.212/32
Address = 10.0.3.102/32

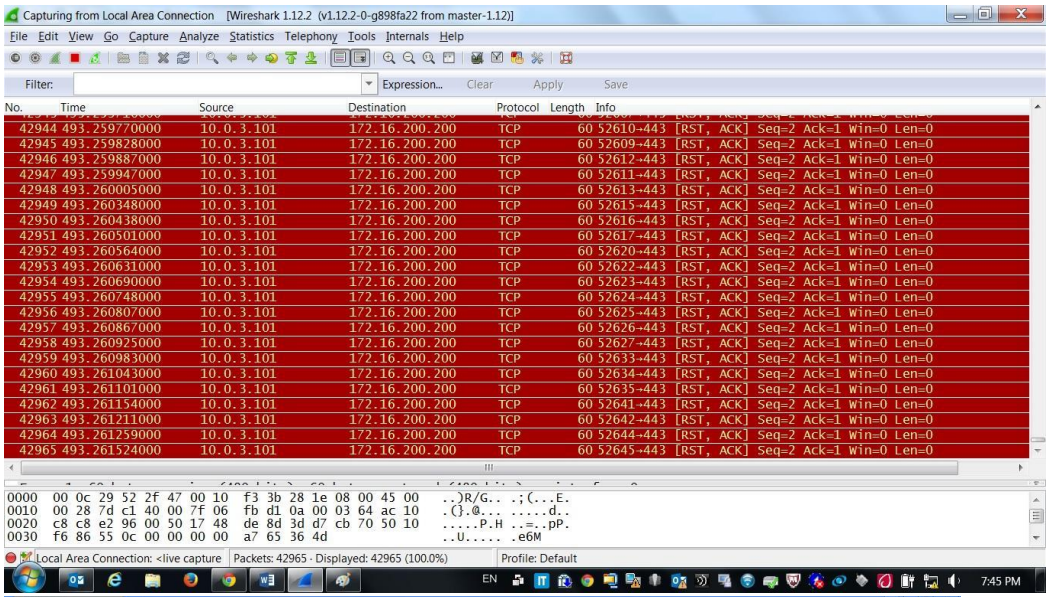

S1050F_bottom
https://192.168.2.109/lsm/index.html#security-sourcenat
S1050F_bottom
Model: S1050F
Pending Changes: 7
Monitor
Network
Policy
Authentication
Routing
VPN
Reports
System
Tools
Source NAT
Rule Name
Source
Destination
Translate source to
Persistent Mapping
Description
1
Address = 10.0.5.2/32
Zone = Outside
Address of Egress interface
Enabled
2
Address = 10.0.3.200/32
Zone = Outside
Address = 172.16.200.220/32
Enabled
Linux server
3
Address = 10.0.3.100/32
Zone = Outside
Address = 172.16.200.210/32
Disabled
4
Address = 10.0.3.101/32
Zone = Outside
Address = 172.16.200.211/32
Disabled
5
Address = 10.0.3.102/32
Zone = Outside
Address = 172.16.200.212/32
Disabled

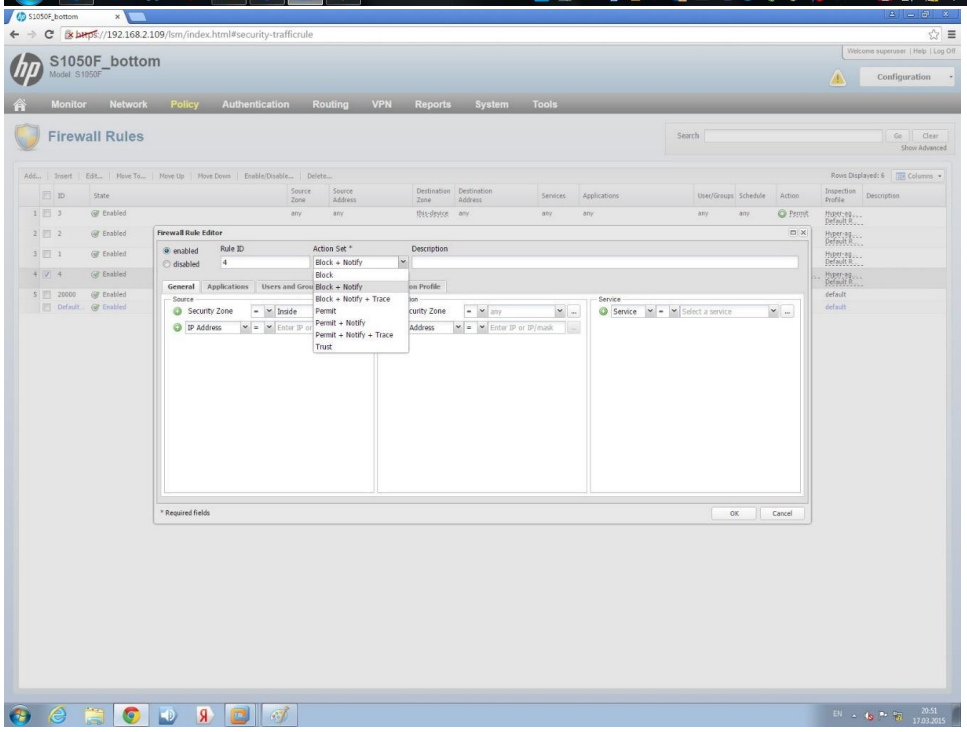

S1050F_bottom
Model: S1050F
Configuration
Monitor
Network
Policy
Authentication
Routing
VPN
Reports
System
Tools
Firewall Rules
Search
Go
Clear
Show Advanced

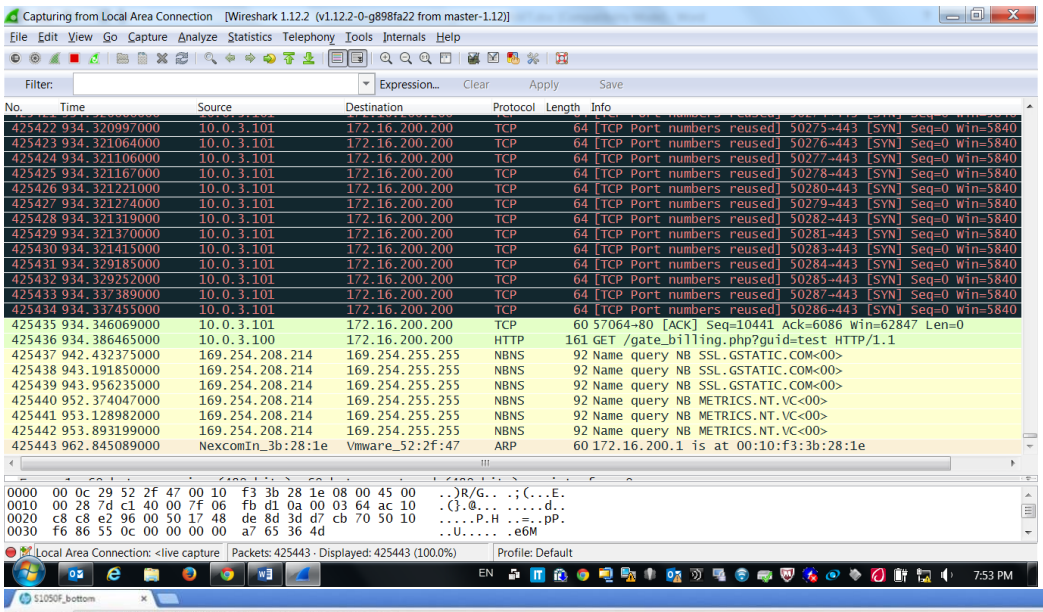

S1050F_bottom
Model: S1050F
Configuration
Monitor
Network
Policy
Authentication
Routing
VPN
Reports
System
Tools
IPS Profiles

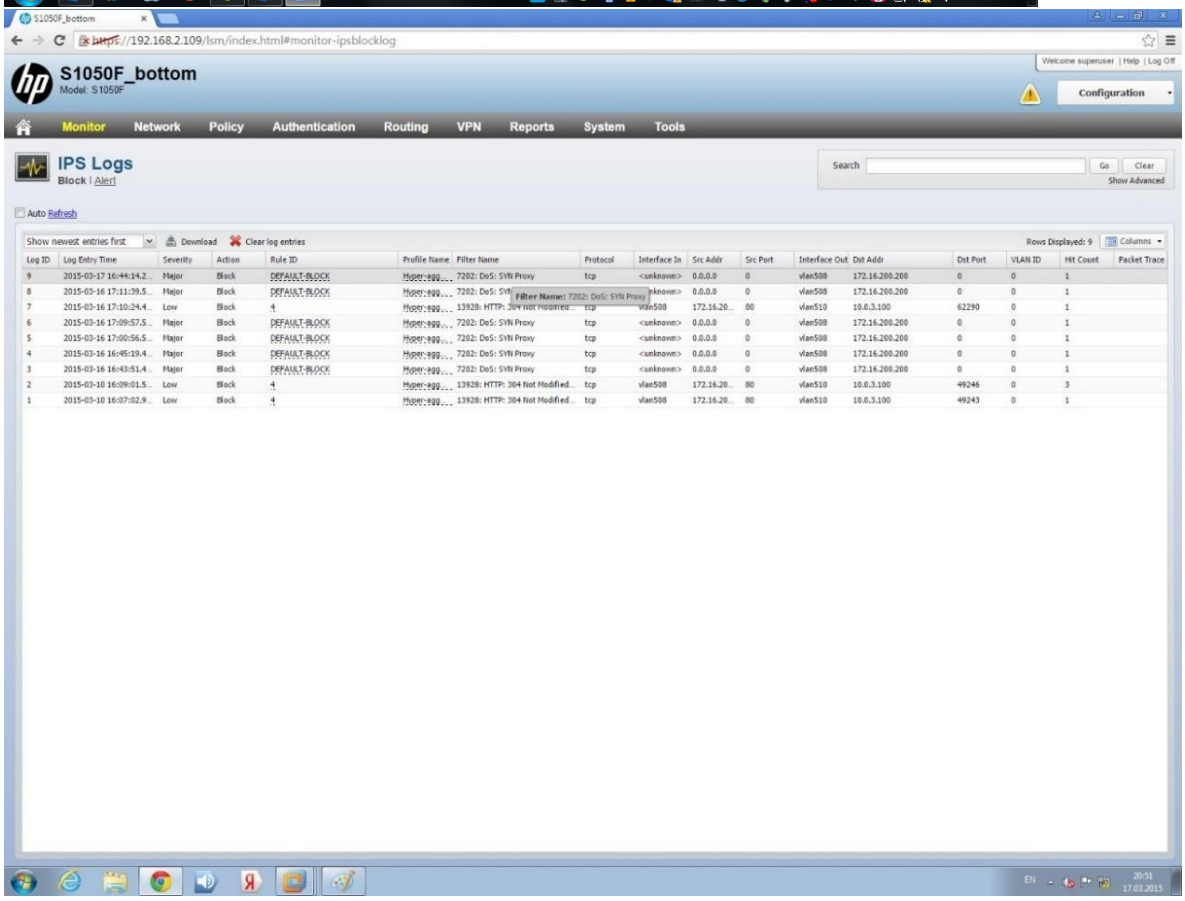

S1050F_bottom
https://192.168.2.109/lsm/index.html#security-ipsprofile
S1050F_bottom
Model: S1050F
Configuration
Monitor
Network
Policy
Authentication
Routing
VPN
Reports
System
Tools
This is an Instant-Commit feature. Changes take effect immediately.
IPS Profiles
Edit IPS Profile
General
IPS Category Rules
Limits/Exceptions
IPS Filter Overrides
DDoS
Name
Destination
SYNs Per Second Threshold
test
172.16.200.200
50
* Required fields
Close


S1050F_bottom
https://192.168.2.109/lsm/index.html#security-trafficrule
S1050F_bottom
Model: S1050F
Configuration
Monitor
Network
Policy
Authentication
Routing
VPN
Reports
System
Tools
Firewall Rules
Search
Go
Clear
Show Advanced
ID
State
Source Zone
Source Address
Destination Zone
Destination Address
Services
Applications
User/Groups
Schedule
Action
Inspection Profile
Description
ActionSet
Name: Block
Action: block
Packet Trace: disabled
Quarantine: disabled


Capturing from Local Area Connection [Wireshark 1.12.2 (v1.12.2-0-g898fa22 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
42944 493.259770000 10.0.3.101 172.16.200.200 TCP 60 52610→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42945 493.259828000 10.0.3.101 172.16.200.200 TCP 60 52609→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42946 493.259887000 10.0.3.101 172.16.200.200 TCP 60 52612→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42947 493.259947000 10.0.3.101 172.16.200.200 TCP 60 52611→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42948 493.260005000 10.0.3.101 172.16.200.200 TCP 60 52613→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42949 493.260348000 10.0.3.101 172.16.200.200 TCP 60 52615→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42950 493.260438000 10.0.3.101 172.16.200.200 TCP 60 52616→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42951 493.260501000 10.0.3.101 172.16.200.200 TCP 60 52617→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42952 493.260564000 10.0.3.101 172.16.200.200 TCP 60 52620→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42953 493.260631000 10.0.3.101 172.16.200.200 TCP 60 52622→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42954 493.260690000 10.0.3.101 172.16.200.200 TCP 60 52623→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42955 493.260748000 10.0.3.101 172.16.200.200 TCP 60 52624→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42956 493.260807000 10.0.3.101 172.16.200.200 TCP 60 52625→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42957 493.260867000 10.0.3.101 172.16.200.200 TCP 60 52626→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42958 493.260925000 10.0.3.101 172.16.200.200 TCP 60 52627→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42959 493.260983000 10.0.3.101 172.16.200.200 TCP 60 52633→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42960 493.261043000 10.0.3.101 172.16.200.200 TCP 60 52634→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42961 493.261101000 10.0.3.101 172.16.200.200 TCP 60 52635→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42962 493.261154000 10.0.3.101 172.16.200.200 TCP 60 52641→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42963 493.261211000 10.0.3.101 172.16.200.200 TCP 60 52642→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42964 493.261259000 10.0.3.101 172.16.200.200 TCP 60 52644→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
42965 493.261524000 10.0.3.101 172.16.200.200 TCP 60 52645→443 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
0000 00 0c 29 52 2f 47 00 10 f3 3b 28 1e 08 00 45 00 ..)R/G.. .;(...E.
0010 00 28 7d c1 40 00 7f 06 fb d1 0a 00 03 64 ac 10 .(}.@... .....d..
0020 c8 c8 e2 96 00 50 17 48 de 8d 3d d7 cb 70 50 10 .....P.H ..=..pP.
0030 f6 86 55 0c 00 00 00 00 a7 65 36 4d ..U..... .e6M
Local Area Connection: <live capture
Packets: 42965 · Displayed: 42965 (100.0%)
Profile: Default
7:45 PM


https://192.168.2.109/lsm/index.html#security-trafficrule
S1050F_bottom
Model: S1050F
Configuration
Monitor Network Policy Authentication Routing VPN Reports System Tools
Firewall Rules
Firewall Rule Editor
enabled
disabled
Rule ID
Action Set *
Block + Notify
Block
Block + Notify + Trace
Permit
Permit + Notify
Permit + Notify + Trace
Trust
Description
General
Applications
Source
Security Zone
Inside
IP Address
Service
Select a service
* Required fields
OK
Cancel


Capturing from Local Area Connection [Wireshark 1.12.2 (v1.12.2-0-g898fa22 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
425422 934.320997000 10.0.3.101 172.16.200.200 TCP 64 [TCP Port numbers reused] 50275→443 [SYN] Seq=0 Win=5840
425423 934.321064000 10.0.3.101 172.16.200.200 TCP 64 [TCP Port numbers reused] 50276→443 [SYN] Seq=0 Win=5840
425424 934.321106000 10.0.3.101 172.16.200.200 TCP 64 [TCP Port numbers reused] 50277→443 [SYN] Seq=0 Win=5840
425425 934.321167000 10.0.3.101 172.16.200.200 TCP 64 [TCP Port numbers reused] 50278→443 [SYN] Seq=0 Win=5840
425426 934.321221000 10.0.3.101 172.16.200.200 TCP 64 [TCP Port numbers reused] 50280→443 [SYN] Seq=0 Win=5840
425427 934.321274000 10.0.3.101 172.16.200.200 TCP 64 [TCP Port numbers reused] 50279→443 [SYN] Seq=0 Win=5840
425428 934.321319000 10.0.3.101 172.16.200.200 TCP 64 [TCP Port numbers reused] 50282→443 [SYN] Seq=0 Win=5840
425429 934.321370000 10.0.3.101 172.16.200.200 TCP 64 [TCP Port numbers reused] 50281→443 [SYN] Seq=0 Win=5840
425430 934.321415000 10.0.3.101 172.16.200.200 TCP 64 [TCP Port numbers reused] 50283→443 [SYN] Seq=0 Win=5840
425431 934.329185000 10.0.3.101 172.16.200.200 TCP 64 [TCP Port numbers reused] 50284→443 [SYN] Seq=0 Win=5840
425432 934.329252000 10.0.3.101 172.16.200.200 TCP 64 [TCP Port numbers reused] 50285→443 [SYN] Seq=0 Win=5840
425433 934.337389000 10.0.3.101 172.16.200.200 TCP 64 [TCP Port numbers reused] 50287→443 [SYN] Seq=0 Win=5840
425434 934.337455000 10.0.3.101 172.16.200.200 TCP 64 [TCP Port numbers reused] 50286→443 [SYN] Seq=0 Win=5840
425435 934.346069000 10.0.3.101 172.16.200.200 TCP 60 57064→80 [ACK] Seq=10441 Ack=6086 Win=62847 Len=0
425436 934.386465000 10.0.3.100 172.16.200.200 HTTP 161 GET /gate_billing.php?guid=test HTTP/1.1
425437 942.432375000 169.254.208.214 169.254.255.255 NBNS 92 Name query NB SSL.GSTATIC.COM<00>
425438 943.191850000 169.254.208.214 169.254.255.255 NBNS 92 Name query NB SSL.GSTATIC.COM<00>
425439 943.956235000 169.254.208.214 169.254.255.255 NBNS 92 Name query NB SSL.GSTATIC.COM<00>
425440 952.374047000 169.254.208.214 169.254.255.255 NBNS 92 Name query NB METRICS.NT.VC<00>
425441 953.128982000 169.254.208.214 169.254.255.255 NBNS 92 Name query NB METRICS.NT.VC<00>
425442 953.893199000 169.254.208.214 169.254.255.255 NBNS 92 Name query NB METRICS.NT.VC<00>
425443 962.845089000 NexcomIn_3b:28:1e Vmware_52:2f:47 ARP 60 172.16.200.1 is at 00:10:f3:3b:28:1e
0000 00 0c 29 52 2f 47 00 10 f3 3b 28 1e 08 00 45 00 ..)R/G.. .;(...E.
0010 00 28 7d c1 40 00 7f 06 fb d1 0a 00 03 64 ac 10 .(}.@... .....d..
0020 c8 c8 e2 96 00 50 17 48 de 8d 3d d7 cb 70 50 10 .....P.H ..=..pP.
0030 f6 86 55 0c 00 00 00 00 a7 65 36 4d ..U..... .e6M
Local Area Connection: <live capture Packets: 425443 · Displayed: 425443 (100.0%) Profile: Default
7:53 PM


https://192.168.2.109/lsm/index.html#monitor-ipsblocklog
S1050F_bottom
Model: S1050F
Configuration
Monitor Network Policy Authentication Routing VPN Reports System Tools
IPS Logs
Block | Alert
Search Go Clear Show Advanced
Auto Refresh
Show newest entries first Download Clear log entries Rows Displayed: 9 Columns
Log ID Log Entry Time Severity Action Rule ID Profile Name Filter Name Protocol Interface In Src Addr Src Port Interface Out Dst Addr Dst Port VLAN ID Hit Count Packet Trace
9 2015-03-17 16:44:14.2... Major Block DEFAULT-BLOCK Hyper-ggg... 7202: DoS: SYN Proxy tcp <unknown> 0.0.0.0 0 vlan508 172.16.200.200 0 0 1
8 2015-03-16 17:11:39.5... Major Block DEFAULT-BLOCK Hyper-ggg... 7202: DoS: SYN Proxy tcp <unknown> 0.0.0.0 0 vlan508 172.16.200.200 0 0 1
7 2015-03-16 17:10:24.4... Low Block 4 Hyper-ggg... 13928: HTTP: 304 Not Modified... tcp vlan508 172.16.20... 80 vlan510 10.0.3.100 62290 0 1
6 2015-03-16 17:09:57.5... Major Block DEFAULT-BLOCK Hyper-ggg... 7202: DoS: SYN Proxy tcp <unknown> 0.0.0.0 0 vlan508 172.16.200.200 0 0 1
5 2015-03-16 17:00:56.5... Major Block DEFAULT-BLOCK Hyper-ggg... 7202: DoS: SYN Proxy tcp <unknown> 0.0.0.0 0 vlan508 172.16.200.200 0 0 1
4 2015-03-16 16:45:19.4... Major Block DEFAULT-BLOCK Hyper-ggg... 7202: DoS: SYN Proxy tcp <unknown> 0.0.0.0 0 vlan508 172.16.200.200 0 0 1
3 2015-03-16 16:43:51.4... Major Block DEFAULT-BLOCK Hyper-ggg... 7202: DoS: SYN Proxy tcp <unknown> 0.0.0.0 0 vlan508 172.16.200.200 0 0 1
2 2015-03-10 16:09:01.5... Low Block 4 Hyper-ggg... 13928: HTTP: 304 Not Modified... tcp vlan508 172.16.20... 80 vlan510 10.0.3.100 49246 0 3
1 2015-03-10 16:07:02.9... Low Block 4 Hyper-ggg... 13928: HTTP: 304 Not Modified... tcp vlan508 172.16.20... 80 vlan510 10.0.3.100 49243 0 1
Filter Name: 7202: DoS: SYN Proxy

3.1.3 Оценка освоения теоретического курса профессионального модуля по МДК.04.03

Дидактические единицы	Проверяемые ОК, ПК, У, З	Формы контроля (наименование контрольной точки)	
		Текущая аттестация	Промежуточная аттестация
Тема 3.1. Технологии хранения и анализа данных	ОК1-9 З3-З24 ПК4.3. У15-У21	Устный зачет по Темам 3.1	Устные ответы на дифференцированном зачете
		Практическая работа №1 Создание RAID на Linux	
		Практическая работа № 5 Установка Zabbix-server на Linux	

1. Устный зачет по Темам 3.1

Инструкция для обучающихся: Зачет сдается в рамках учебного занятия. Каждому студенту по выбору преподавателя дается два вопроса, на которые он отвечает в устной форме.

Выполнение задания: одному студенту на ответ выделяется 3 мин, группа сдает зачет за одно учебное занятие.

Вопросы к зачету:

1. Понятие NFS
2. Понятие SMB
3. Понятие InfiniBand (IB)
4. Понятие Unified storage
5. Понятие SDS
6. Понятие пиперконвергентной системы
7. Понятие облака и эфемерного хранилища

Практическая работа № 2
Работа с Hypervisor: Установка и настройка нативного Hypervisor.

Инструкция для обучающихся

Внимательно прочитайте задание. Выполните все необходимые операции

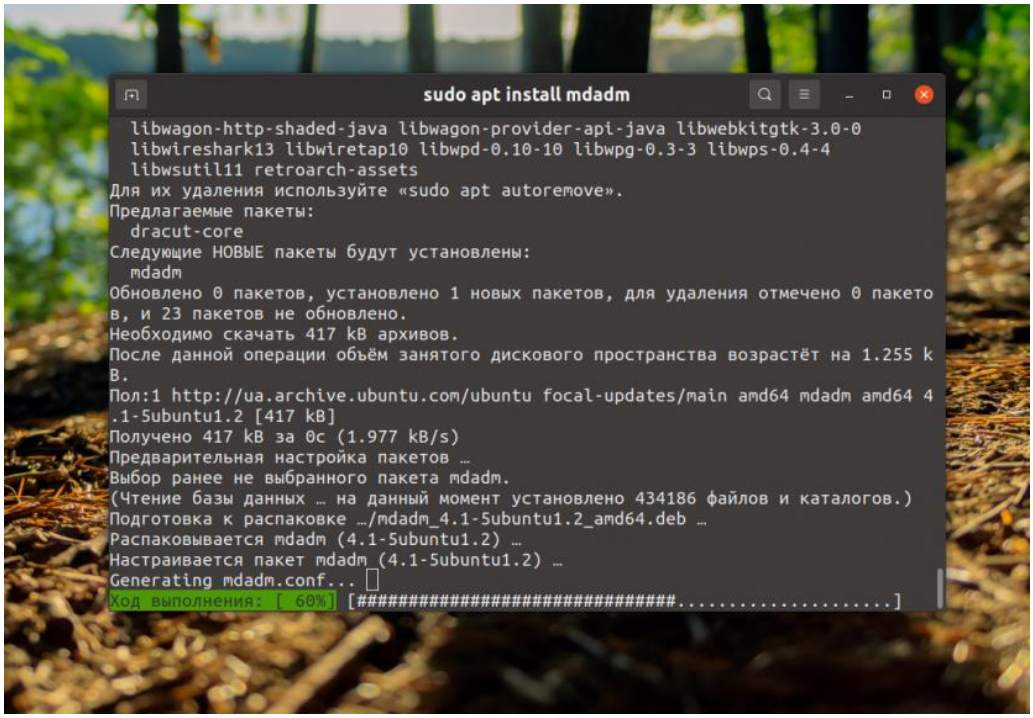
Время выполнения – 90 минут.

Задание

Шаг 1. Установка mdadm

Для управления программными RAID массивами в Linux используется утилита mdadm. Для того чтобы установить её в Ubuntu или Debian выполните такую команду:

sudo apt install mdadm



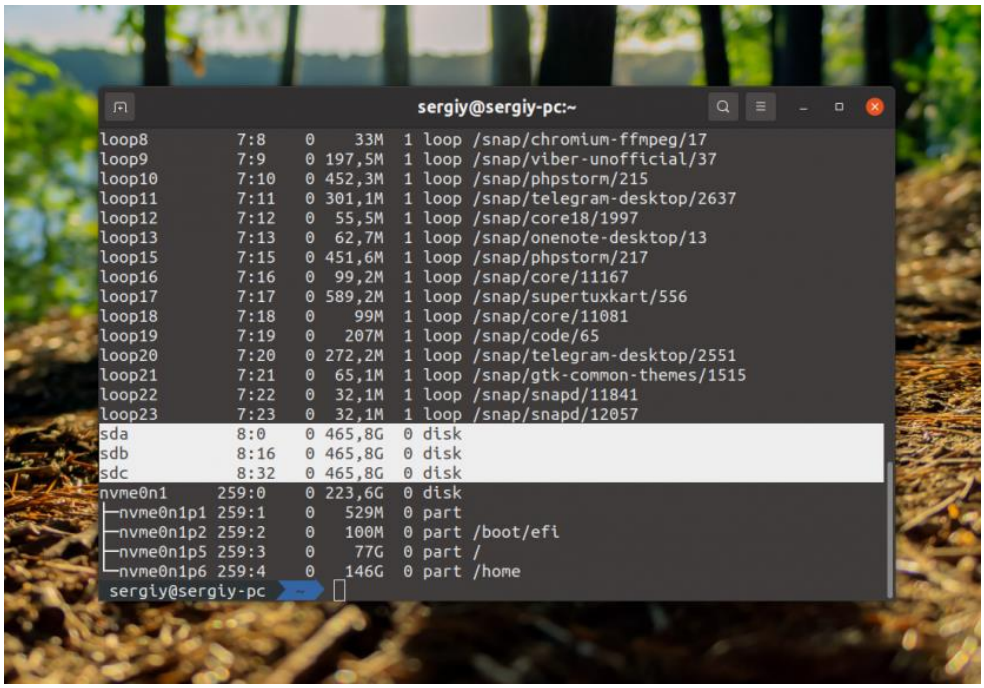
Для установки утилиты в CentOS/Fedora/RedHat необходимо выполнить:

sudo yum install mdadm

Шаг 2. Подготовка дисков

Посмотреть список дисков, подключённых к системе можно с помощью команды lsblk:

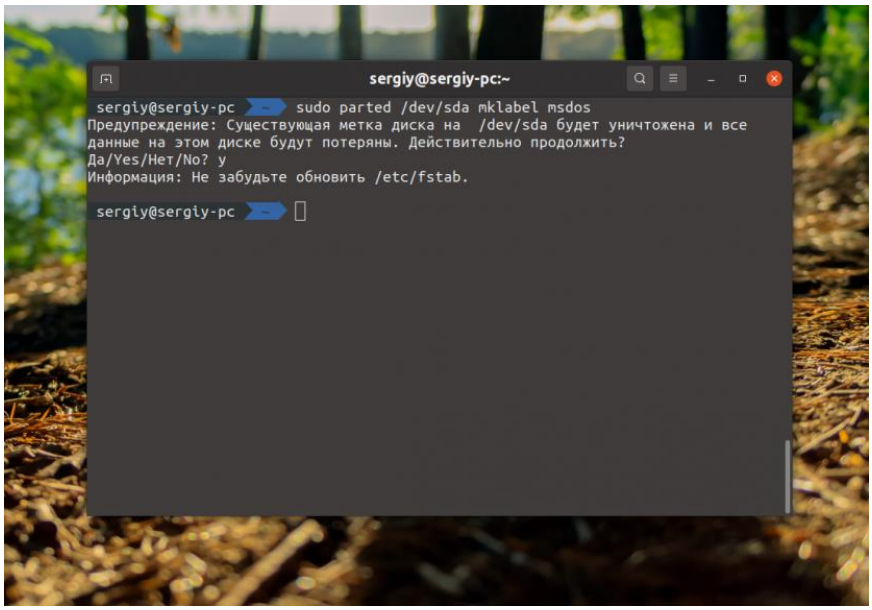
lsblk



В этой статье я покажу как объединить три диска в RAID на примере дисков **/dev/sda**, **/dev/sdb** и **/dev/sdc**. Сначала необходимо определиться стоит ли размещать RAID непосредственно на диски или на разделы. Лучше выбрать разделы, так как это дает больше гибкости и безопасности. Во первых, операционная система может перезаписать суперблок RAID если он размещён прямо на диске. Во вторых, если вы выделяете весь диск под RAID, то у вас могут возникнуть проблемы при замене диска. Диски одинакового объема, обычно, немного отличаются у разных производителей. Поэтому для замены вам придется искать точно такой же диск с точно таким же реальным объемом. Если же у вас будет раздел, вы просто сможете создать раздел нужного объема.

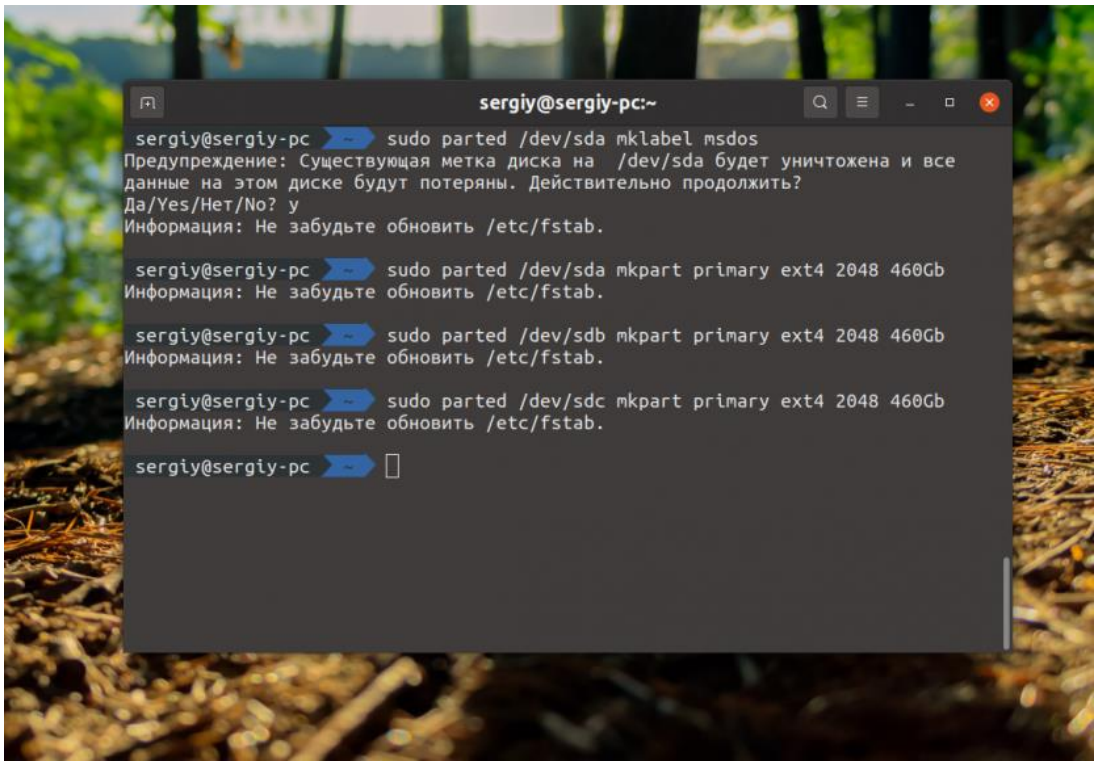
Сначала нужно создать таблицу разделов на всех выбранных дисках:

sudo parted /dev/sda mklabel msdos
sudo parted /dev/sdb mklabel msdos
sudo parted /dev/sdc mklabel msdos

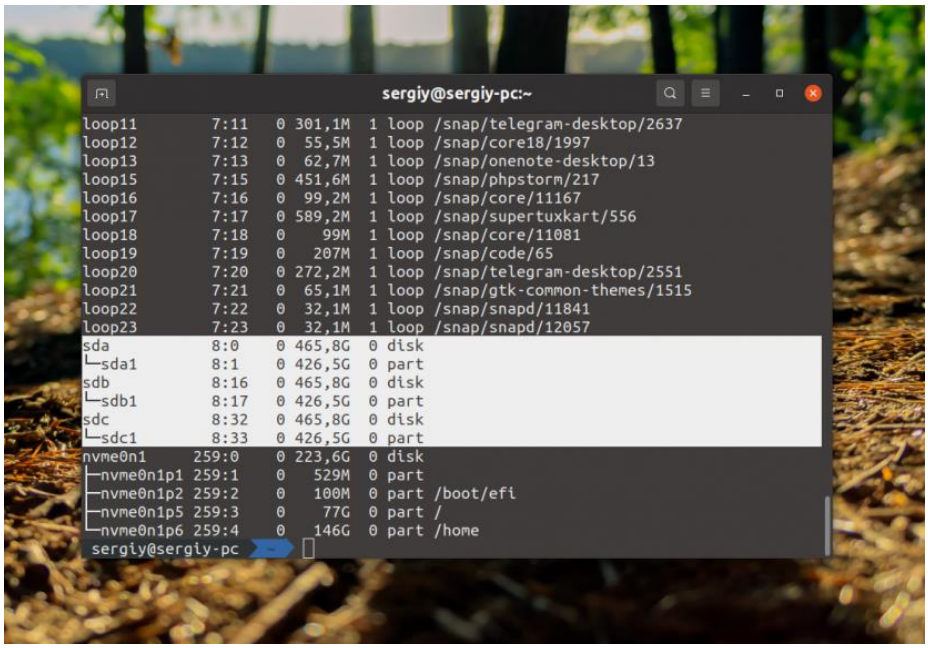


Если на диске уже существует таблица разделов программа предупредит о том, что создание новой сотрёт все данные с диска. После создания таблицы разделов следует создать по разделу на каждом диске. Например, создадим разделы размером 460 гигабайт. Для этого можно воспользоваться той же командой parted:

sudo parted /dev/sda mkpart primary ext4 2048 460Gb
sudo parted /dev/sdb mkpart primary ext4 2048 460Gb
sudo parted /dev/sdc mkpart primary ext4 2048 460Gb



Теперь диски готовы к размещению на них RAID:



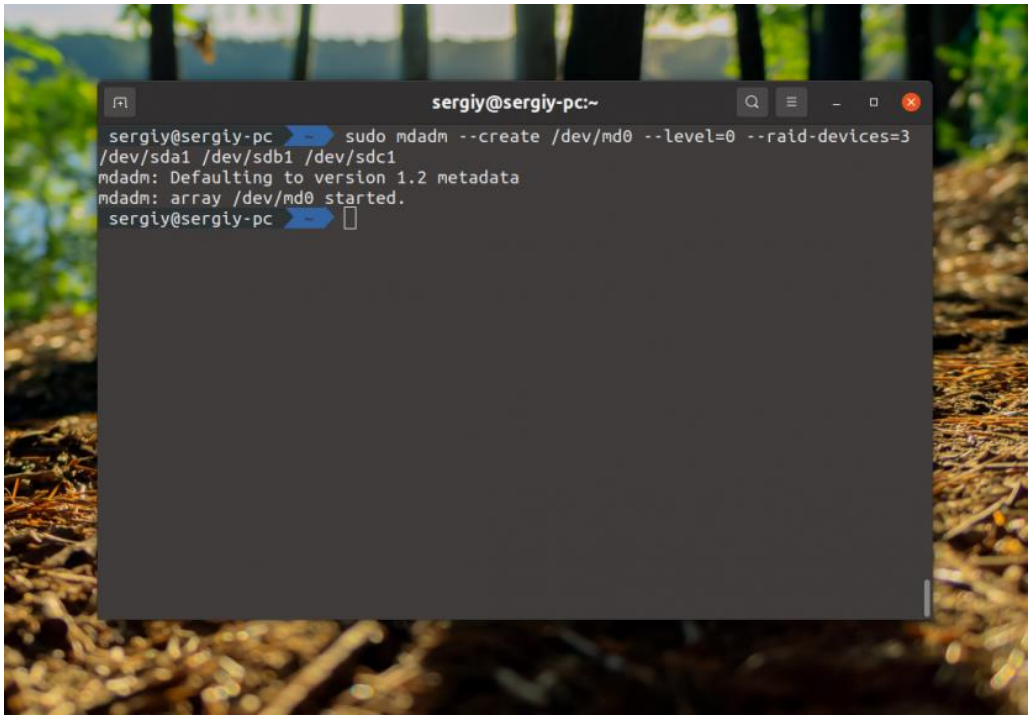
Шаг 3. Создание RAID 0

Для создания RAID массива надо выполнить команду mdadm с опцией --create, указать режим работы массива, количество дисков и сами диски. Синтаксис команды такой:

$ sudo mdadm --create /dev/имя_массива --level=режим_работы --raid-devices=количество_устройств список устройств

Например:

sudo mdadm --create /dev/md0 --level=0 --raid-devices=3 /dev/sda1 /dev/sdb1 /dev/sdc1



После выполнения этой команды вы увидите раздел raid в lsblk. С этим разделом можно работать как с любым обычным разделом в вашей системе.

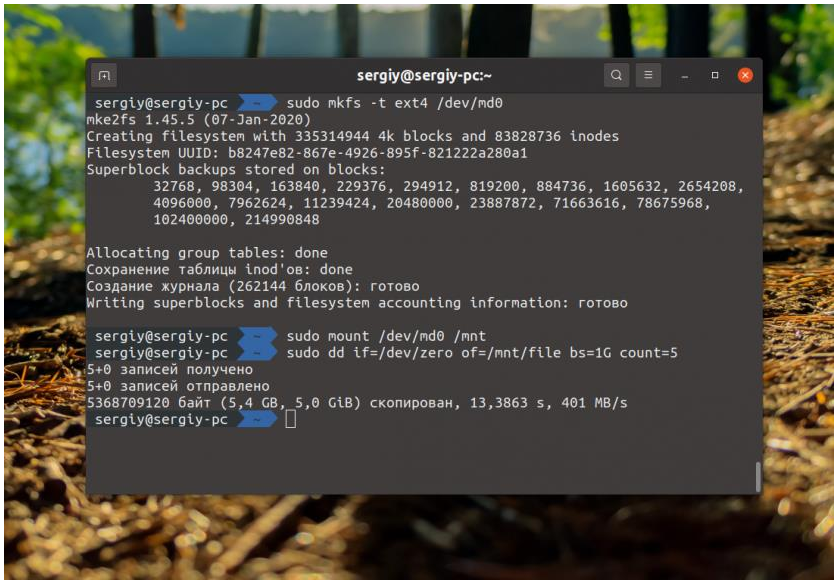
Шаг 4. Тестирование RAID 0

Давайте для примера отформатируем полученный раздел в файловую систему Ext4, смонтируем и попробуем записывать туда файлы:

sudo mkfs -t ext4 /dev/md0
sudo mount /dev/md0 /mnt

Затем можно тестировать скорость с помощью dd:

sudo dd if=/dev/zero of=/mnt/file bs=1G count=5

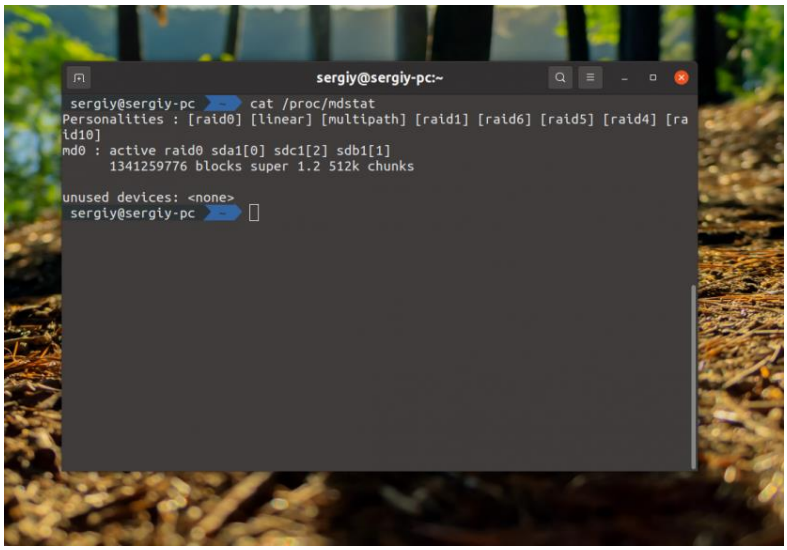


Как видите, при записи 5 Гб данных мы получаем скорость 400 Мб/сек, это уже на уровне обычного SSD.

Шаг 5. Информация о RAID

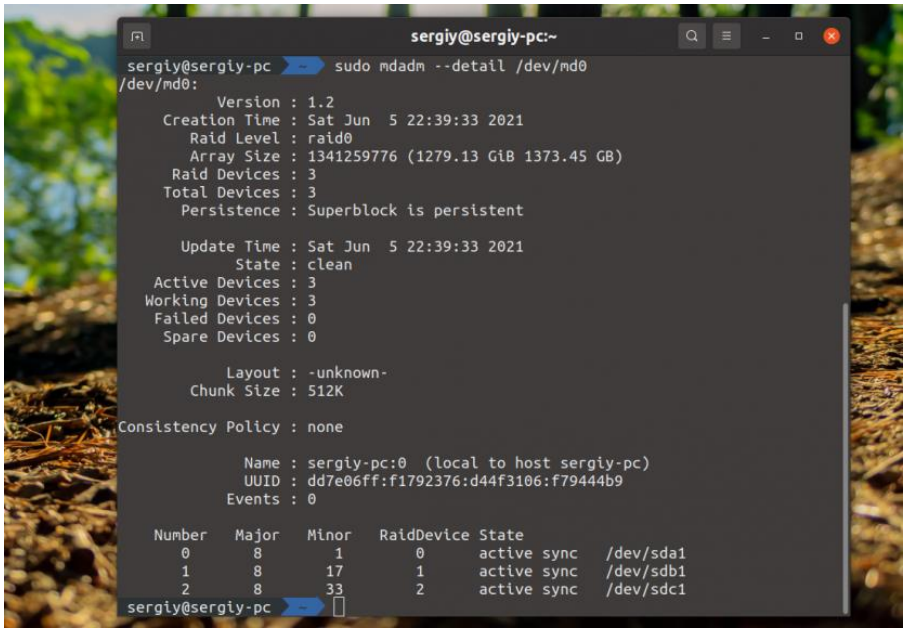
Найти информацию обо всех созданных в системе RAID массивах вы можете в файле **/proc/mdstat:**

cat /proc/mdstat



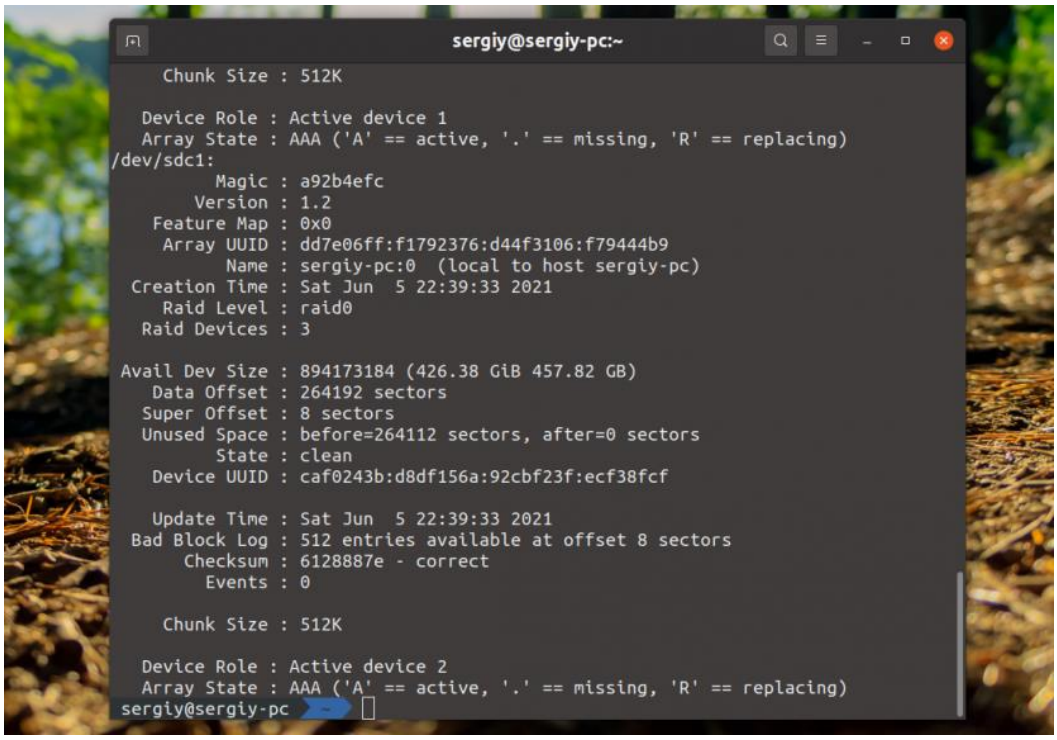
Именно так можно посмотреть RAID Linux. Посмотреть более детальную информацию о массиве /dev/md0 можно с помощью самой утилиты mdadm:

sudo mdadm --detail /dev/md0



Здесь в том числе отображается состояние RAID Linux. Посмотреть детальную информацию о каждом устройстве, которое входит в RAID можно с помощью опции --**examine**:

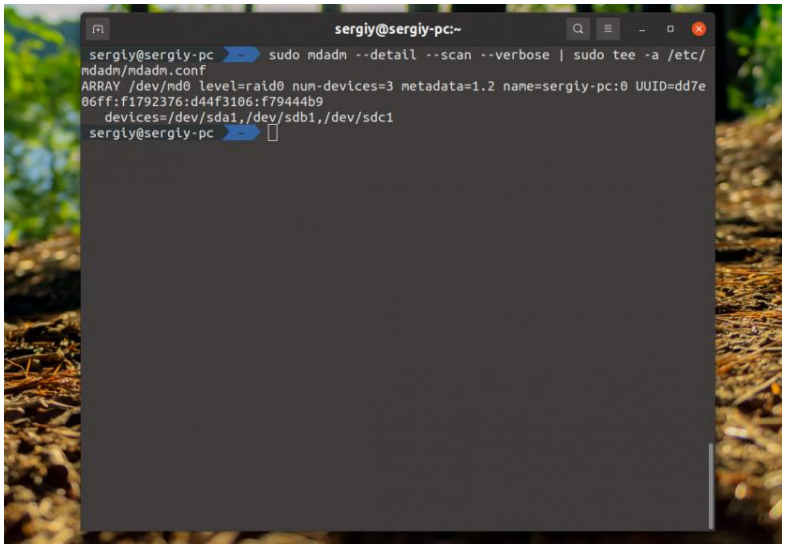
sudo mdadm --examine /dev/sda1 /dev/sdb1 /dev/sdc1



Шаг 6. Сохранение RAID массива

В принципе, уже сейчас RAID массив работает и продолжит работать после перезагрузки, потому что mdadm просканирует все диски, найдёт метаданные массива и построит его. Но неизвестно какое имя программа присвоит полученному массиву и неизвестно все ли параметры будут восстановлены верно. Поэтому конфигурацию массива лучше сохранить. Для этого используйте такую команду:

sudo mdadm --detail --scan --verbose | sudo tee -a /etc/mdadm/mdadm.conf



Затем нужно пересоздать initramfs с поддержкой этого массива:

sudo update-initramfs -u

С полученным массивом можно обращаться как с обычным разделом диска. Например, для того чтобы автоматически монтировать его в систему добавьте такую строчку в /etc/fstab:

sudo vi /etc/fstab

/dev/md0 /mnt/ ext4 defaults 0 0

На этом создание raid массива linux завершено.

Шаг 7. Переименование RAID массива

Если вы не выполните предыдущий пункт и перезагрузите компьютер, то можете получить RAID массив с именем md127 вместо md0, такое имя также может быть присвоено второму RAID массиву. Для того чтобы переименовать массив, его придется пересобрать. Для этого сначала остановите существующий массив:

sudo mdadm --stop /dev/md127

Затем выполните команду переименования. Синтаксис у неё такой:

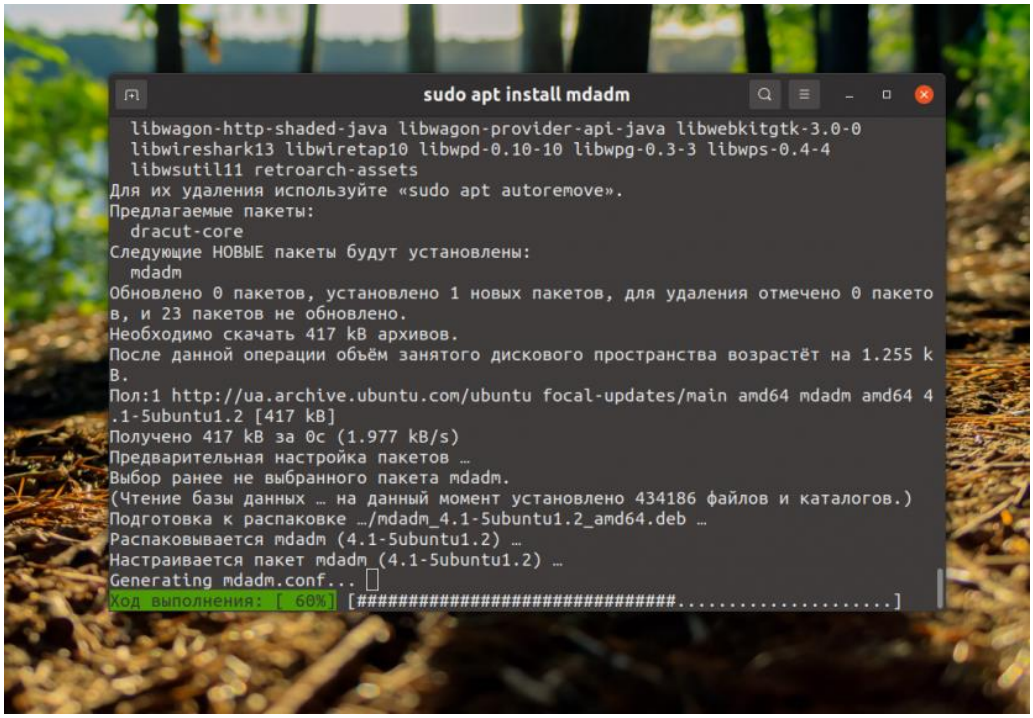
$ sudo mdadm --assemble --update=name --name=номер /dev/md_номер список устройств

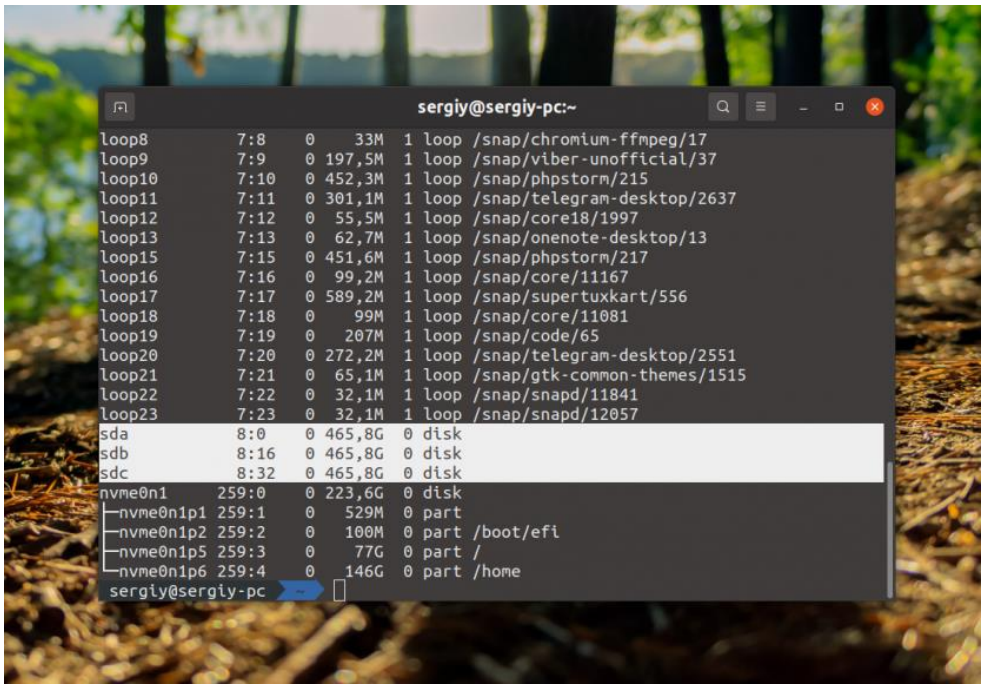
Например:

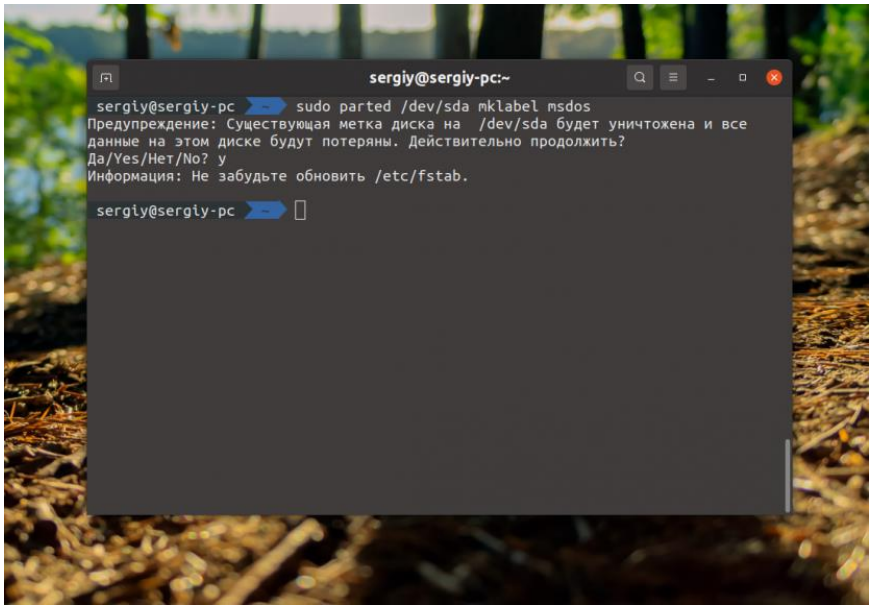
sudo mdadm --assemble --update=name --name=0 /dev/md0 /dev/sda1 /dev/sdb1 /dev/sdc1

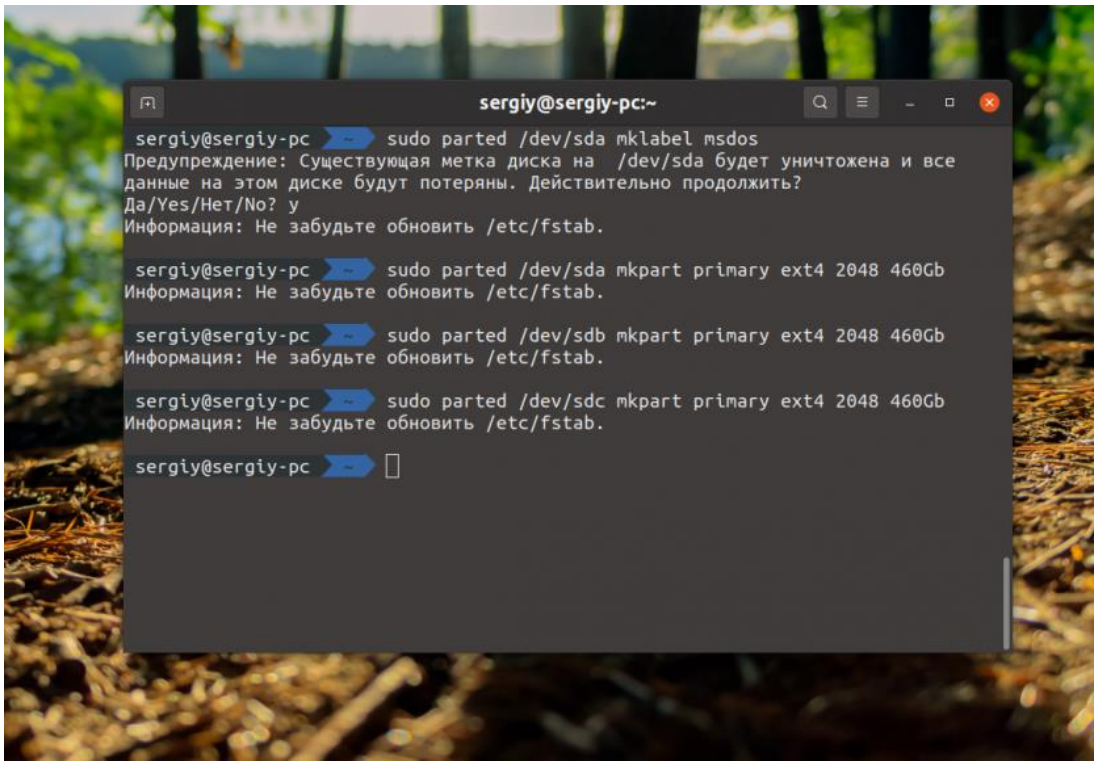
После этого следует повторить предыдущий шаг для уже правильного сохранения RAID устройства.

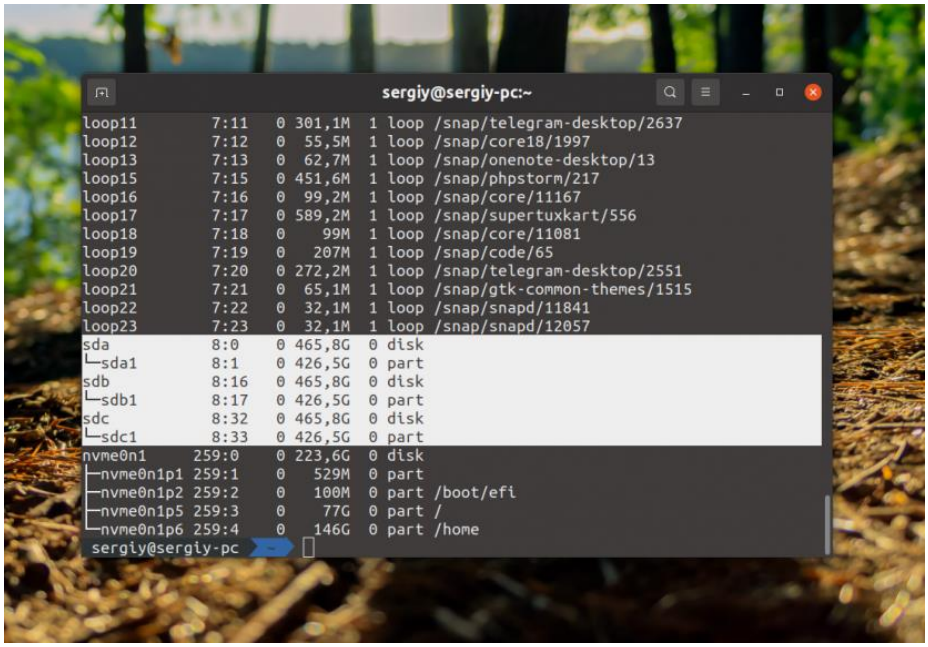
Эталон ответа:

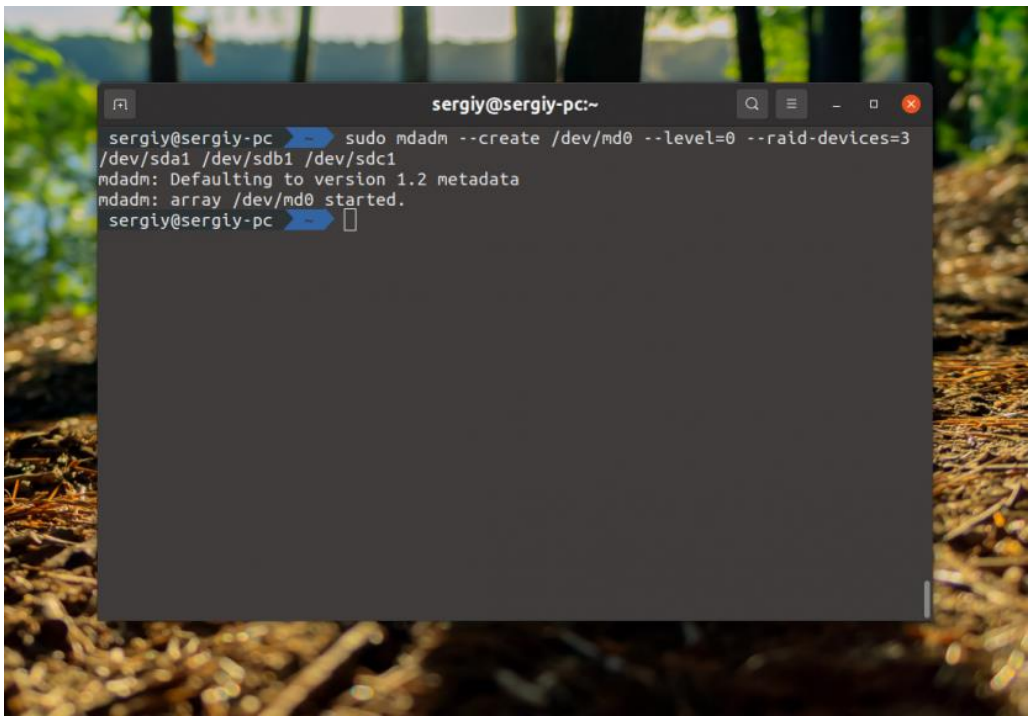


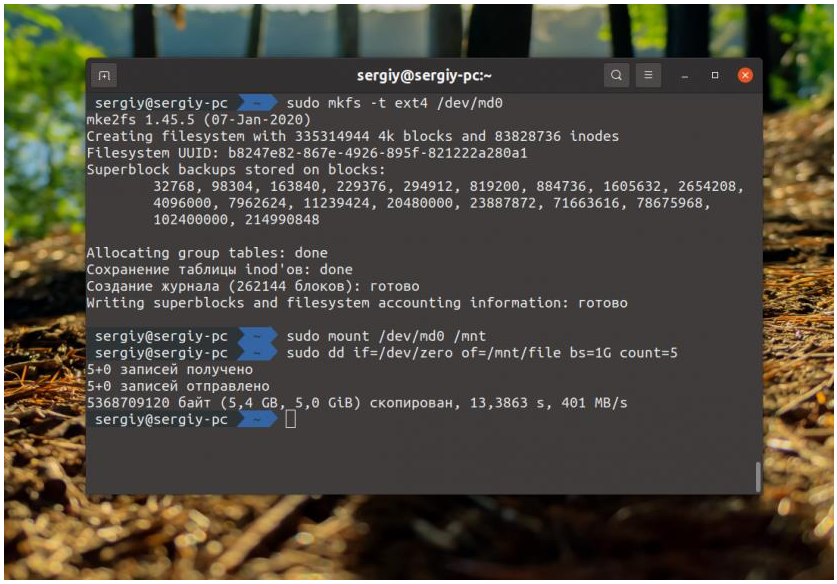

sergiy@sergiy-pc:~
loop8 7:8 0 33M 1 loop /snap/chromium-ffmpeg/17
loop9 7:9 0 197,5M 1 loop /snap/viber-unofficial/37
loop10 7:10 0 452,3M 1 loop /snap/phpstorm/215
loop11 7:11 0 301,1M 1 loop /snap/telegram-desktop/2637
loop12 7:12 0 55,5M 1 loop /snap/core18/1997
loop13 7:13 0 62,7M 1 loop /snap/onenote-desktop/13
loop15 7:15 0 451,6M 1 loop /snap/phpstorm/217
loop16 7:16 0 99,2M 1 loop /snap/core/11167
loop17 7:17 0 589,2M 1 loop /snap/supertuxkart/556
loop18 7:18 0 99M 1 loop /snap/core/11081
loop19 7:19 0 207M 1 loop /snap/code/65
loop20 7:20 0 272,2M 1 loop /snap/telegram-desktop/2551
loop21 7:21 0 65,1M 1 loop /snap/gtk-common-themes/1515
loop22 7:22 0 32,1M 1 loop /snap/snapd/11841
loop23 7:23 0 32,1M 1 loop /snap/snapd/12057
sda 8:0 0 465,8G 0 disk
sdb 8:16 0 465,8G 0 disk
sdc 8:32 0 465,8G 0 disk
nvme0n1 259:0 0 223,6G 0 disk
├─nvme0n1p1 259:1 0 529M 0 part
├─nvme0n1p2 259:2 0 100M 0 part /boot/efi
├─nvme0n1p5 259:3 0 77G 0 part /
└─nvme0n1p6 259:4 0 146G 0 part /home
sergiy@sergiy-pc ~

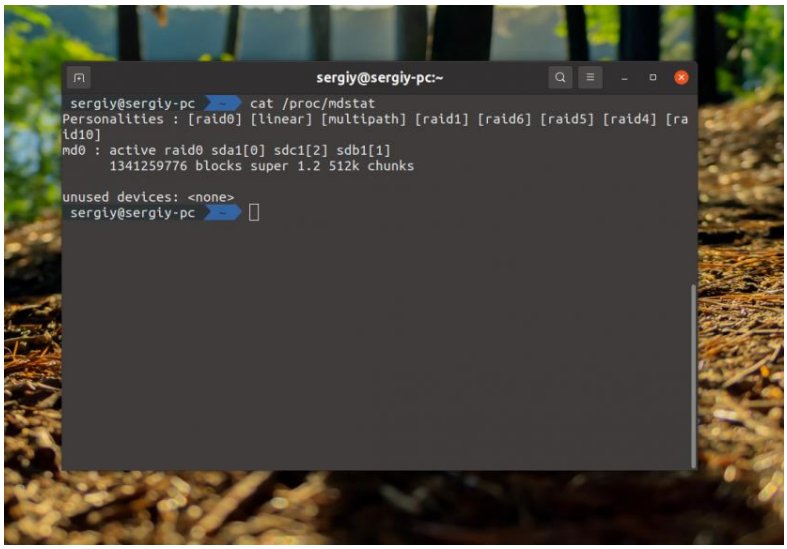

sergiy@sergiy-pc:~
sergiy@sergiy-pc ~ sudo parted /dev/sda mklabel msdos
Предупреждение: Существующая метка диска на /dev/sda будет уничтожена и все данные на этом диске будут потеряны. Действительно продолжить?
Да/Yes/Нет/No? y
Информация: Не забудьте обновить /etc/fstab.
sergiy@sergiy-pc ~

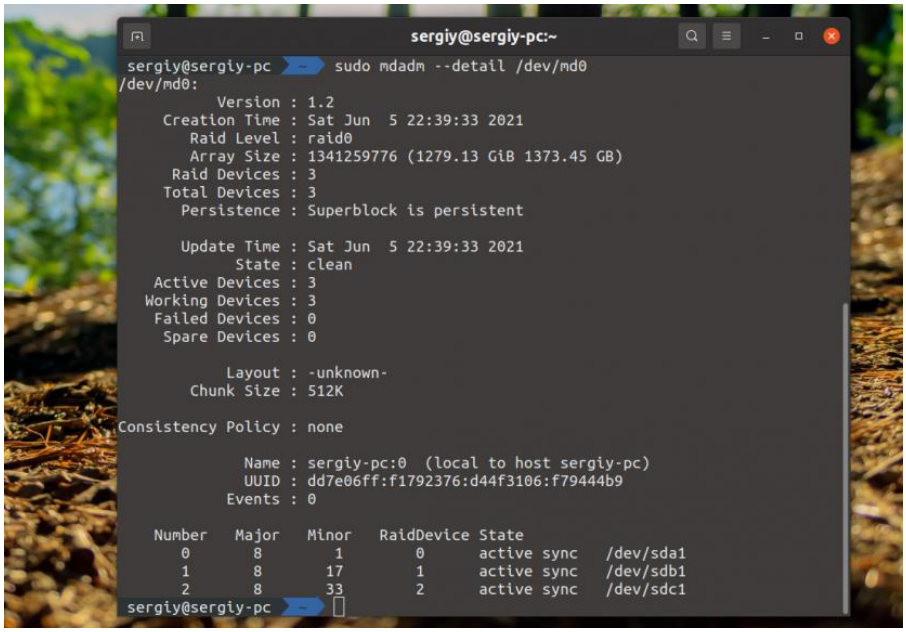

sergiy@sergiy-pc:~
sergiy@sergiy-pc ~ sudo parted /dev/sda mklabel msdos
Предупреждение: Существующая метка диска на /dev/sda будет уничтожена и все данные на этом диске будут потеряны. Действительно продолжить?
Да/Yes/Нет/No? y
Информация: Не забудьте обновить /etc/fstab.
sergiy@sergiy-pc ~ sudo parted /dev/sda mkpart primary ext4 2048 460Gb
Информация: Не забудьте обновить /etc/fstab.
sergiy@sergiy-pc ~ sudo parted /dev/sdb mkpart primary ext4 2048 460Gb
Информация: Не забудьте обновить /etc/fstab.
sergiy@sergiy-pc ~ sudo parted /dev/sdc mkpart primary ext4 2048 460Gb
Информация: Не забудьте обновить /etc/fstab.
sergiy@sergiy-pc ~

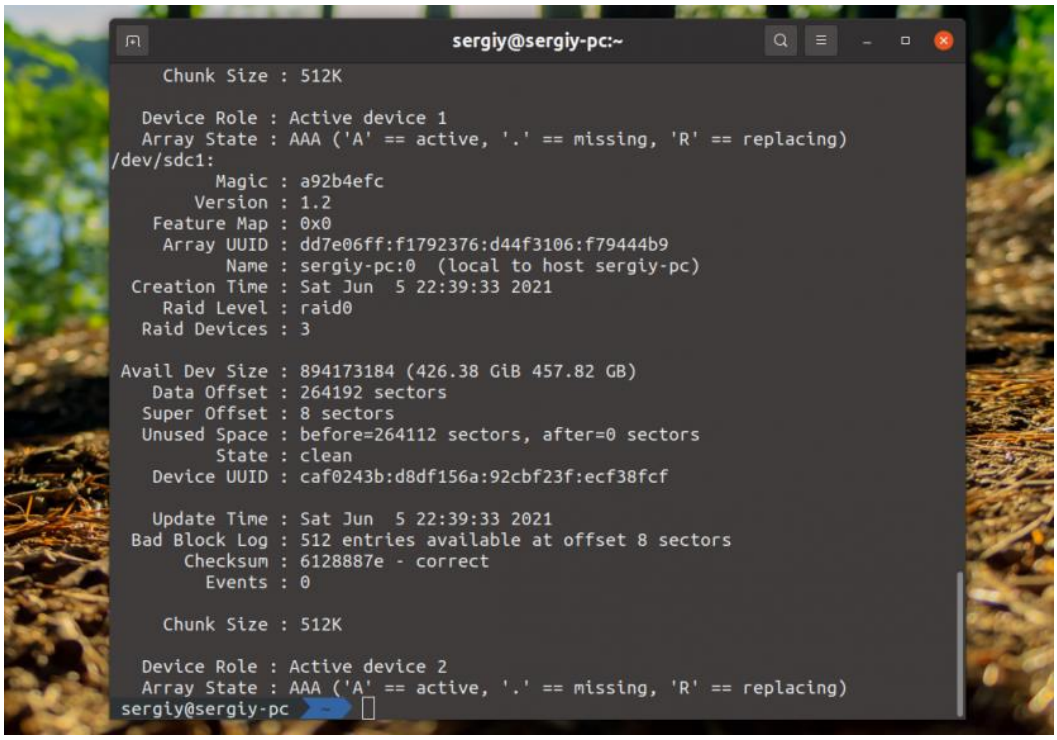

sergiy@sergiy-pc:~
loop11 7:11 0 301,1M 1 loop /snap/telegram-desktop/2637
loop12 7:12 0 55,5M 1 loop /snap/core18/1997
loop13 7:13 0 62,7M 1 loop /snap/onenote-desktop/13
loop15 7:15 0 451,6M 1 loop /snap/phpstorm/217
loop16 7:16 0 99,2M 1 loop /snap/core/11167
loop17 7:17 0 589,2M 1 loop /snap/supertuxkart/556
loop18 7:18 0 99M 1 loop /snap/core/11081
loop19 7:19 0 207M 1 loop /snap/code/65
loop20 7:20 0 272,2M 1 loop /snap/telegram-desktop/2551
loop21 7:21 0 65,1M 1 loop /snap/gtk-common-themes/1515
loop22 7:22 0 32,1M 1 loop /snap/snapd/11841
loop23 7:23 0 32,1M 1 loop /snap/snapd/12057
sda 8:0 0 465,8G 0 disk
└─sda1 8:1 0 426,5G 0 part
sdb 8:16 0 465,8G 0 disk
└─sdb1 8:17 0 426,5G 0 part
sdc 8:32 0 465,8G 0 disk
└─sdc1 8:33 0 426,5G 0 part
nvme0n1 259:0 0 223,6G 0 disk
├─nvme0n1p1 259:1 0 529M 0 part
├─nvme0n1p2 259:2 0 100M 0 part /boot/efi
├─nvme0n1p5 259:3 0 77G 0 part /
└─nvme0n1p6 259:4 0 146G 0 part /home
sergiy@sergiy-pc ~

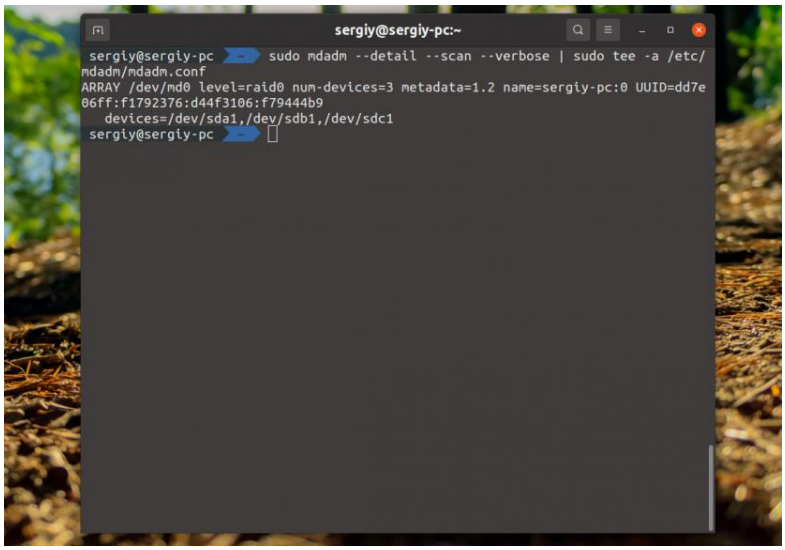

sergiy@sergiy-pc:~
sergiy@sergiy-pc ~ sudo mdadm --create /dev/md0 --level=0 --raid-devices=3
/dev/sda1 /dev/sdb1 /dev/sdc1
mdadm: Defaulting to version 1.2 metadata
mdadm: array /dev/md0 started.
sergiy@sergiy-pc ~


sergiy@sergiy-pc:~
sergiy@sergiy-pc ~ sudo mkfs -t ext4 /dev/md0
mke2fs 1.45.5 (07-Jan-2020)
Creating filesystem with 335314944 4k blocks and 83828736 inodes
Filesystem UUID: b8247e82-867e-4926-895f-821222a280a1
Superblock backups stored on blocks:
32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
4096000, 7962624, 11239424, 20480000, 23887872, 71663616, 78675968,
102400000, 214990848
Allocating group tables: done
Сохранение таблицы inod'ов: done
Создание журнала (262144 блоков): готово
Writing superblocks and filesystem accounting information: готово
sergiy@sergiy-pc ~ sudo mount /dev/md0 /mnt
sergiy@sergiy-pc ~ sudo dd if=/dev/zero of=/mnt/file bs=1G count=5
5+0 записей получено
5+0 записей отправлено
5368709120 байт (5,4 GB, 5,0 GiB) скопирован, 13,3863 s, 401 MB/s
sergiy@sergiy-pc ~


sergiy@sergiy-pc:~
sergiy@sergiy-pc ~ cat /proc/mdstat
Personalities : [raid0] [linear] [multipath] [raid1] [raid6] [raid5] [raid4] [ra
id10]
md0 : active raid0 sda1[0] sdc1[2] sdb1[1]
1341259776 blocks super 1.2 512k chunks
unused devices: <none>
sergiy@sergiy-pc ~


sergiy@sergiy-pc:~
sergiy@sergiy-pc ~ sudo mdadm --detail /dev/md0
/dev/md0:
Version : 1.2
Creation Time : Sat Jun 5 22:39:33 2021
Raid Level : raid0
Array Size : 1341259776 (1279.13 GiB 1373.45 GB)
Raid Devices : 3
Total Devices : 3
Persistence : Superblock is persistent
Update Time : Sat Jun 5 22:39:33 2021
State : clean
Active Devices : 3
Working Devices : 3
Failed Devices : 0
Spare Devices : 0
Layout : -unknown-
Chunk Size : 512K
Consistency Policy : none
Name : sergiy-pc:0 (local to host sergiy-pc)
UUID : dd7e06ff:f1792376:d44f3106:f79444b9
Events : 0
Number Major Minor RaidDevice State
0 8 1 0 active sync /dev/sda1
1 8 17 1 active sync /dev/sdb1
2 8 33 2 active sync /dev/sdc1
sergiy@sergiy-pc ~


sergiy@sergiy-pc:~
Chunk Size : 512K
Device Role : Active device 1
Array State : AAA ('A' == active, '.' == missing, 'R' == replacing)
/dev/sdc1:
Magic : a92b4efc
Version : 1.2
Feature Map : 0x0
Array UUID : dd7e06ff:f1792376:d44f3106:f79444b9
Name : sergiy-pc:0 (local to host sergiy-pc)
Creation Time : Sat Jun 5 22:39:33 2021
Raid Level : raid0
Raid Devices : 3
Avail Dev Size : 894173184 (426.38 GiB 457.82 GB)
Data Offset : 264192 sectors
Super Offset : 8 sectors
Unused Space : before=264112 sectors, after=0 sectors
State : clean
Device UUID : caf0243b:d8df156a:92cbf23f:ecf38fcf
Update Time : Sat Jun 5 22:39:33 2021
Bad Block Log : 512 entries available at offset 8 sectors
Checksum : 6128887e - correct
Events : 0
Chunk Size : 512K
Device Role : Active device 2
Array State : AAA ('A' == active, '.' == missing, 'R' == replacing)
sergiy@sergiy-pc ~



Практическая работа № 5 Установка Zabbix-server на Linux

Инструкция для обучающихся
Внимательно прочитайте задание. Выполните необходимые операции.

Время выполнения задания – 60 минут.

Задание:

Задание:

1. Установка Zabbix Server

1.1. Для работы *Zabbix Server* необходимо установить NGINX:

sudo apt install -y nginx

1.2. Загрузите deb-пакет из репозитория:

sudo wget <https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-4%2Bubuntu22.04_all.deb>

sudo dpkg -i zabbix-release_6.0-4+ubuntu22.04_all.deb

sudo apt update

1.3. Установите *Zabbix Server*, *Zabbix Frontend* и *Zabbix Agent*:

sudo apt install -y zabbix-server-mysql zabbix-frontend-php zabbix-nginx-conf zabbix-sql-scripts zabbix-agent

2. Установка и конфигурация MySQL

2.1. Установите и активируйте MySQL:

sudo apt install -y mysql-server

sudo systemctl enable --now mysql

2.2. Запустите MySQL от имени скперпользователя root:

sudo mysql

2.3. После входа в консоль MySQL выполните запрос, подставив свои значения в поля 'root','localhost' и 'password':

ALTER USER 'root'@'localhost' IDENTIFIED WITH mysql_native_password BY 'password';

2.4. Ожидаемый ответ консоли MySQL с подтверждением внесённых изменений:

Query OK, 0 rows affected (0.01 sec)

2.5. Выйдите из сеанса для пользователя root :

quit;

2.6. Запустите скрипт mysql_secure_installation и в интерактивном режиме согласитесь удалить тестовую базу данных и аккаунт анонимного пользователя:

/usr/bin/mysql_secure_installation

Securing the MySQL server deployment.

Enter password for user root: <password-here>

VALIDATE PASSWORD COMPONENT can be used to test passwords

and improve security. It checks the strength of password

and allows the users to set only those passwords which are

secure enough. Would you like to setup VALIDATE PASSWORD component?

Press y|Y for Yes, any other key for No: n

Using existing password for root.

Change the password for root ? ((Press y|Y for Yes, any other key for No) : n

By default, a MySQL installation has an anonymous user,

allowing anyone to log into MySQL without having to have

a user account created for them. This is intended only for

testing, and to make the installation go a bit smoother.

You should remove them before moving into a production

environment.

Remove anonymous users? (Press y|Y for Yes, any other key for No) : y

Normally, root should only be allowed to connect from

'localhost'. This ensures that someone cannot guess at

the root password from the network.

Disallow root login remotely? (Press y|Y for Yes, any other key for No) : n

By default, MySQL comes with a database named 'test' that

anyone can access. This is also intended only for testing,

and should be removed before moving into a production

environment.

Remove test database and access to it? (Press y|Y for Yes, any other key for No) : y

Reloading the privilege tables will ensure that all changes

made so far will take effect immediately.

Reload privilege tables now? (Press y|Y for Yes, any other key for No) : y

Success.

All done!

3. Создание базы данных для Zabbix в MySQL

3.1. Начните сеанс пользователя root в MySQL:

mysql -uroot -p

3.2. Создайте базу данных zabbix:

create database zabbix character set utf8mb4 collate utf8mb4_bin;

3.3. Создайте пользователя zabbix. Не забудьте задать пароль:

create user zabbix@localhost identified by 'password';

grant all privileges on zabbix.* to zabbix@localhost;

SET GLOBAL log_bin_trust_function_creators = 1;

quit;

3.4. Создайте схему данных для Zabbix:

zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p zabbix

3.5. Введите пароль пользователя zabbix для доступа к MySQL, заданный на шаге 3.3., и дождитесь завершения выполнения скрипта.

4. Настройка Zabbix Server

4.1. Откройте файл конфигурации zabbix_server.conf с помощью текстового редактора, например:

sudo nano /etc/zabbix/zabbix_server.conf

4.2 Укажите пароль пользователя zabbix (заданный на шаге 3.3) для доступа к MySQL:

Option: DBPassword

Database password.

Comment this line if no password is used.

#

Mandatory: no

Default:

DBPassword=

DBPassword=password

4.3. Сохраните изменения и выйдите.

5. Настройка Zabbix Frontend

5.1. Отредактируйте /etc/zabbix/nginx.conf :

sudo nano /etc/zabbix/nginx.conf

5.2. Раскомментируйте директивы listen и server_name и присвойте им значения:

listen 8080;

server_name example.com; # change-me.com

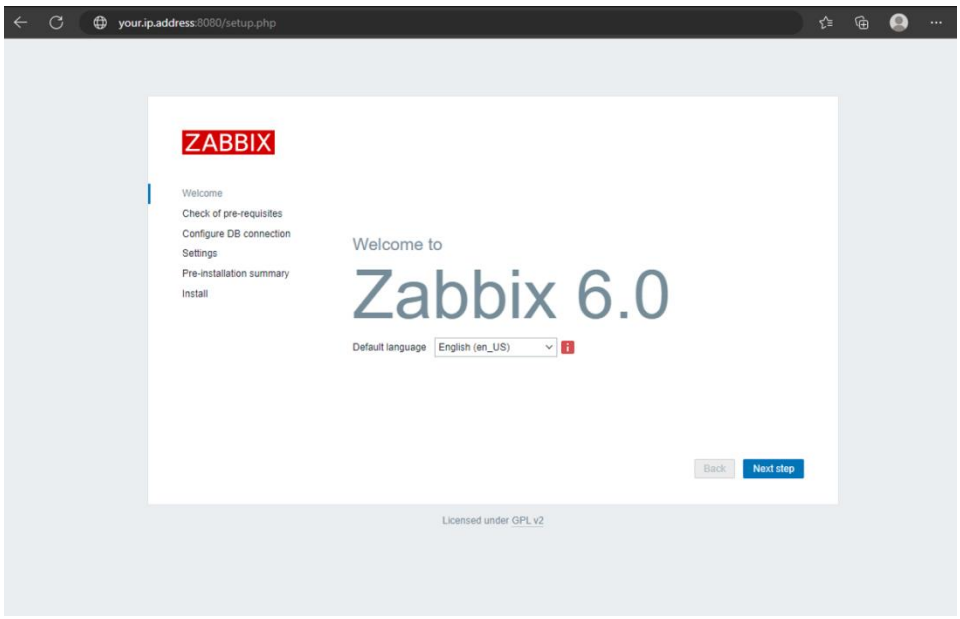
5.3. Запустите службы *Zabbix Server*, *Zabbix Agent*, *Zabbix Frontend* и *NGINX*:

sudo systemctl daemon-reload

sudo systemctl enable --now zabbix-server zabbix-agent nginx php8.1-fpm

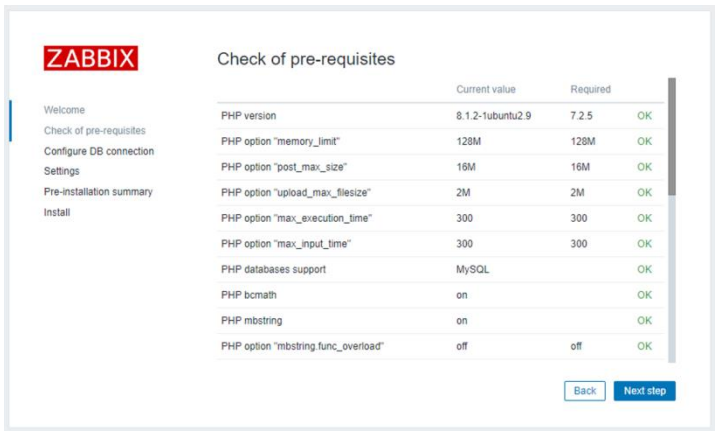
6. Использование Zabbix Frontend

6.1. Для доступа к *Zabbix Frontend* перейдите по адресу http://machine-ip-address:8080:



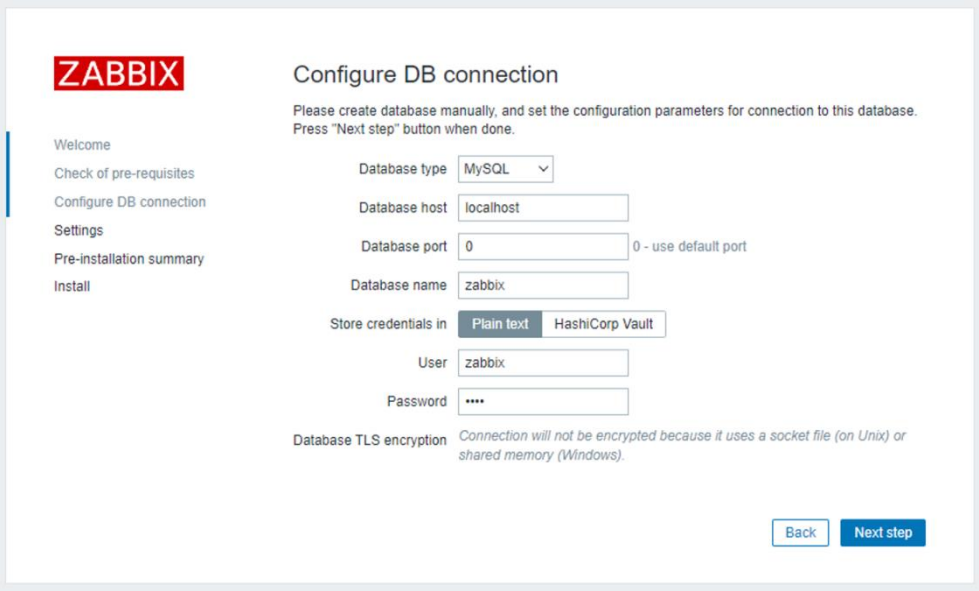
Начальная страница Zabbix Frontend

6.2. Удостоверьтесь, что конфигурация сервера была применена успешно:



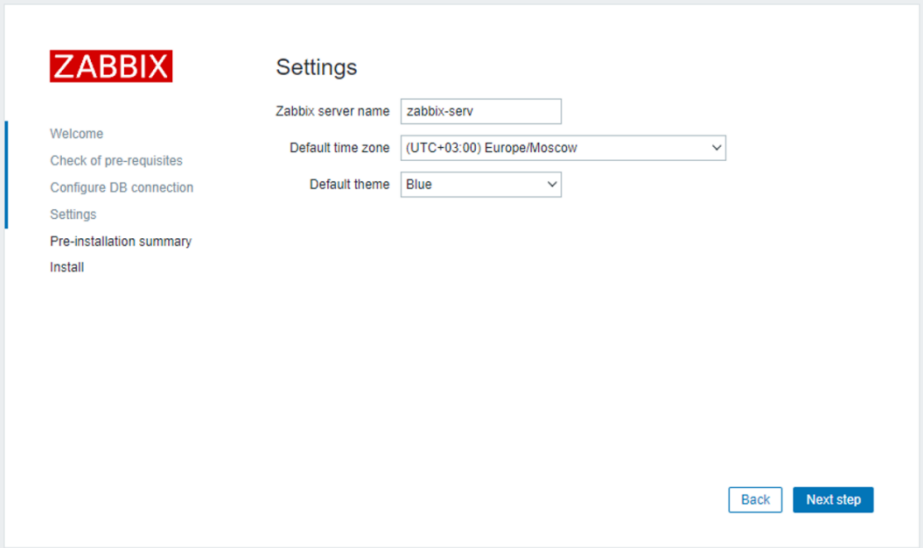
Проверка конфигурации Zabbix Server

6.3. Настройте строки подключения к базе данных MySQL:

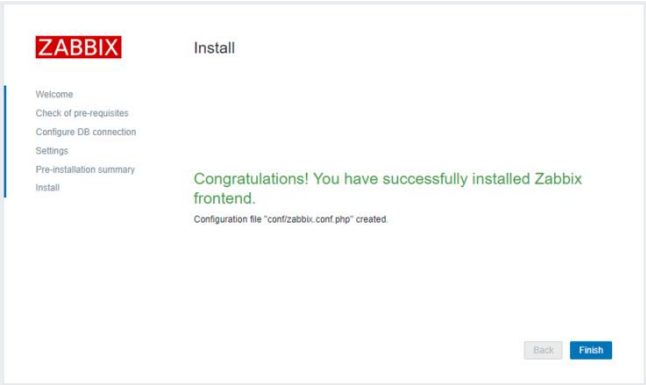


Настройка подключения Zabbix к БД MySQL

6.4. Задайте имя Zabbix Server, настройте часовой пояс и тему Zabbix Frontend:



Настройка имени и часового пояса Zabbix Server

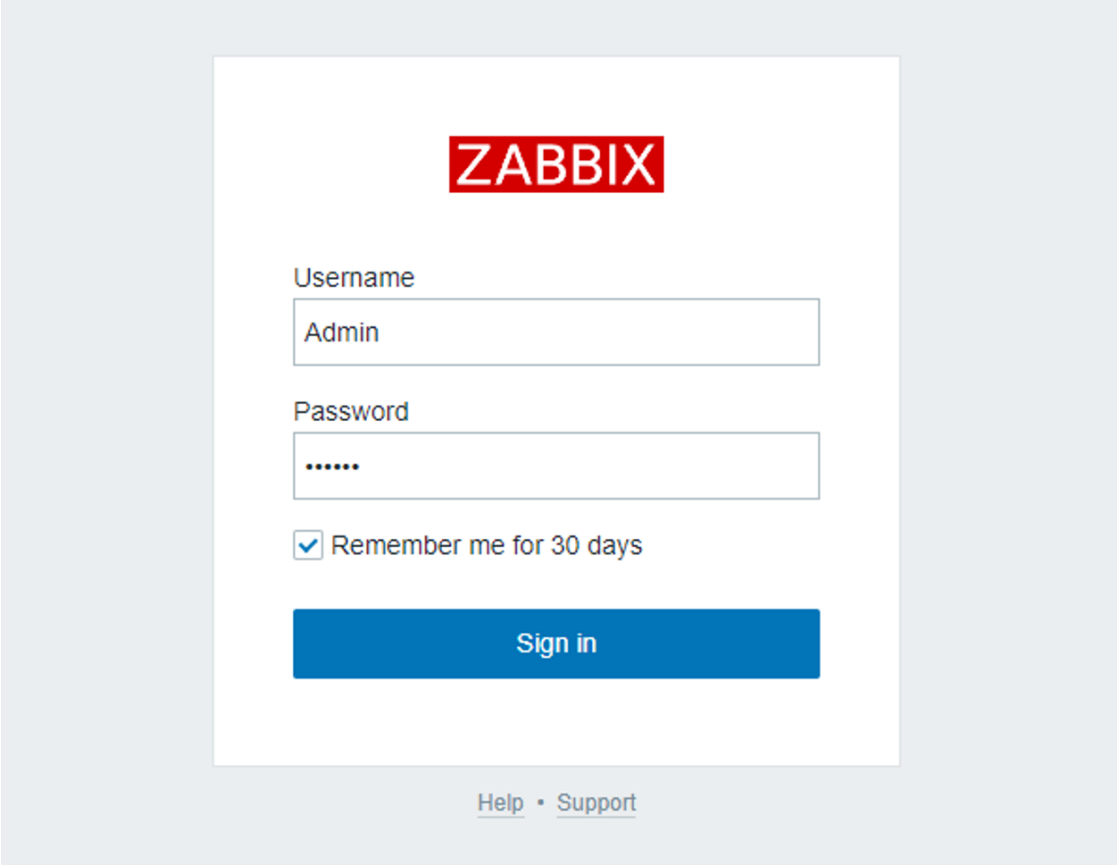


Завершение установки Zabbix Frontend

6.5. В открывшейся форме ведите учётные данные встроенного суперпользователя:

Admin

zabbix



Вход в Zabbix Frontend

7. Настройка службы Zabbix Agent

Примечание
Следующие шаги предназначены исключительно для настройки мониторинга ресурсов машины с установленным Zabbix Server.

Для установки и настройки Zabbix Agent на сторонние машины используйте соответствующие инструкции. См. статью «Zabbix Agent. Инструкции по установке».

7.1 . Отредактируйте файл конфигурации /etc/zabbix/zabbix_agentd.conf:

sudo nano /etc/zabbix/zabbix_agentd.conf

7.2. В файле конфигурации необходимо указать IP-адрес *Zabbix Server*. Если сервер развёрнут на наблюдаемой машине укажите IP-адрес 127.0.0.1 (если интерфейс loopback не настроен иначе):

Option: Server

List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of Zabbix ser>

```
#       Incoming connections will be accepted only from the hosts listed here.
#       If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' are treated eq>
#       and '::/0' will allow any IPv4 or IPv6 address.
#       '0.0.0.0/0' can be used to allow any IPv4 address.
#       Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
#
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=your.server.ip.address
Server=127.0.0.1
```

7.3. Отредактируйте директиву ServerActive:

```
ServerActive=127.0.0.1
```

7.4. Разрешите в сетевом экране использование порта 10050:

```
sudo ufw allow 10050/tcp
```

7.5. Примените изменения:

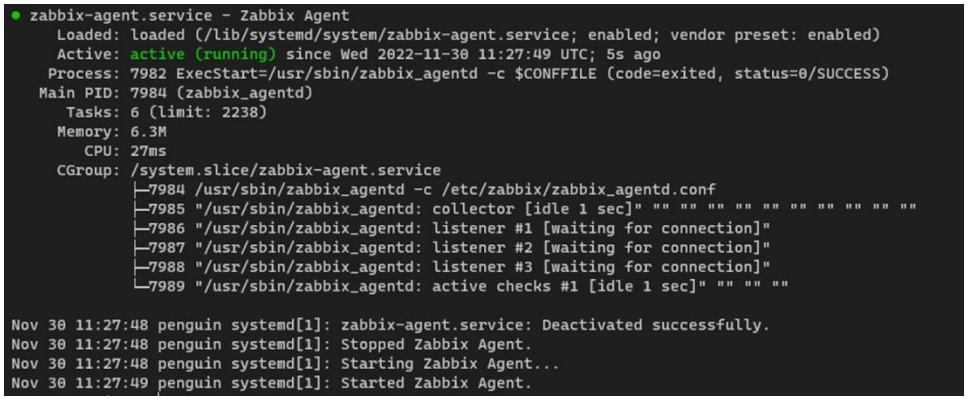
```
sudo systemctl daemon-reload
sudo ufw reload
```

7.6. Запустите *Zabbix Agent* и добавьте его в список автозагрузки:

```
sudo systemctl enable  --now zabbix-agent
```

7.7. Удостоверьтесь, что служба работает:

```
systemctl status zabbix.agent
```



Ожидаемый статус сервиса Zabbix Agent

8. Добавление Linux-хоста в сеть мониторинга

Добавление агента в сеть мониторинга выполняется аналогично разделу 4. «Добавление Linux-хоста в сеть мониторинга» инструкции «Zabbix Agent. Инструкции по установке для Ubuntu 22.04». При настройке используйте IP-адрес интерфейса loopback (127.0.0.1).

3.2. Контрольно-оценочные материалы для промежуточной аттестации

Формой промежуточной аттестации по МДК.05.01 является дифференцированный зачет.

Перечень вопросов:

№	Перечень теоретических вопросов
1.	Технология развертывания программного обеспечения на физическом оборудовании с использованием виртуализации: понятие гипервизора. Виртуализация ресурсов: compute, storage, network
2.	Виртуальная коммутация: передача сетевого состояния, datapath, удаленного управления трафиком, виртуальный NAT. Сетевой мост
3.	Инструменты виртуализации: Qemu, KVM, Virt-manager
4.	Снимок машины. Восстановление машины. Состояние виртуальной машины. Процедура миграции, резервного копирования и восстановления виртуальной машины. Состояние дисков виртуальной машины
5.	Организация облачных сервисов на основе кластерного подхода. Обзор технологий кластеризации
6.	Кластер Proxmox VE: Узлы кластера. Отказоустойчивость. Репликация.
7.	Кластеры Kubernetes в среде Proxmox VE: Мастер-ноды Kubernetes.
8.	Оркестрация контейнеров, Kube-Proxy, Компоненты управления Kubernetes
9.	Диспетчер облачных контроллеров
10.	Исполняемые среды контейнеров: Docker, containerd, CRI-O и Kubernetes CRI. Планирование, приоритизация и вытеснение

Условия выполнения

1. Количество билетов для экзаменующегося: 1
2. Время подготовки к ответу: 30 минут
3. Требования к устным ответам:
   Полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом.
4. Оборудование: учебная аудитория, стол, стул, пишущая ручка, бумага.

Результаты промежуточной аттестации фиксируются в протоколе.

Формой промежуточной аттестации по МДК.05.02 **является дифференцированный зачет**

Перечень вопросов:

№	Перечень теоретических вопросов
1.	Понятие безопасности облачных сервисов
2.	Виды угроз безопасности для облачных сервисов.
3.	Современные методики и технологии защиты облачных данных.
4.	Шифрование данных в облаке
5.	Использование сложных паролей и многофакторной аутентификации
6.	Технология защиты: SSL
7.	Методики мониторинга состояния сети
8.	Стратегия защиты от DoS и DDoS атак
9.	Технологии резервного копирования облака, общие правила хранения данных
10.	Стратегии аварийного восстановления данных

Формой промежуточной аттестации по МДК.05.03 **является дифференцированный зачет**

Перечень вопросов:

№	Перечень теоретических вопросов
1.	Понятие NFS
2.	Понятие SMB
3.	Понятие InfiniBand (IB)
4.	Понятие Unified storage
5.	Понятие SDS
6.	Понятие пиперконвергентной системы
7.	Понятие облака и эфемерного хранилища
8.	Технология Raid
9.	Валидация облачных данных
10.	Контроль целостности облачных данных

Критерии оценки устных ответов

(Указываются критерии оценки в зависимости от видов заданий. Оставить только те критерии, которые преподаватель будет использовать))

В системе оценки знаний и умений используются **следующие критерии** (скорректировать в соответствии с особенностями дисциплины):

«Отлично» – за глубокое и полное овладение содержанием учебного материала, в котором обучающийся легко ориентируется, владение понятийным аппаратом за умение связывать теорию с практикой, решать практические задачи, высказывать и обосновывать свои суждения. Отличная отметка предполагает грамотное, логичное изложение ответа (как в устной, так и в письменной форме), качественное внешнее оформление.

«Хорошо» – если обучающийся полно освоил учебный материал, владеет понятийным аппаратом, ориентируется в изученном материале, осознанно применяет знания для решения практических задач, грамотно излагает ответ, но содержание и форма ответа имеют некоторые неточности.

«Удовлетворительно» – если обучающийся обнаруживает знание и понимание основных положений учебного материала, но излагает его неполно, непоследовательно, допускает неточности в определение понятий, в применении знаний для решения практических задач, не умеет доказательно обосновать свои суждения.

«Неудовлетворительно» – если обучающийся имеет разрозненные, бессистемные знания, не умеет выделять главное и второстепенное, допускает ошибки в определение понятий, искажает их смысл, беспорядочно и неуверенно излагает материал, не может применять знания для решения практических задач; за полное незнание и непонимание учебного материала или отказ отвечать.

.