Бюджетное учреждение профессионального образования
Ханты-Мансийского автономного округа-Югры
«Междуреченский агропромышленный колледж»

СБОРНИК ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ (ПРОФЕССИОНАЛЬНЫЕ МОДУЛИ) ПО ПРОФЕССИИ 09.02.06 Сетевое и системное администрирование (сетевой и системный администратор)

г.п.Междуреченский 2025 год

Рассмотрено и рекомендовано к изданию на заседании методической комиссии (Протокол № 7, от 3 марта 2025 г.)

Сборник методических разработок Технологического профиля

В сборник вошли разработки фонда оценочных средств, по профессиональным модулям:

ПМ 01. Настройка сетевой инфраструктуры.
ПМ.02. Организация сетевого администрирования операционных систем.
ПМ.03. Эксплуатация объектов сетевой инфраструктуры.
ПМ.04. Эксплуатация операционных систем.
ПМ.05. Эксплуатация облачных сервисов

Разработчики; Деньгуб Андрей Анатольевич, Машер Виталий Валерьевич.

Цель сборника – систематизация, обобщение опыта области методических разработок преподавателей, мастеров производственного обучения методической комиссии «Технологических дисциплин».

СОЖЕРЖАНИЕ

ВВЕДЕНИЕ

Фонд оценочных средств является составной частью нормативно-методического обеспечения системы оценки качества освоения обучающимися ПМ. Оценка качества освоения обучающимися основных образовательных программ включает текущий контроль успеваемости, промежуточную и государственную итоговую аттестацию обучающихся.

Настоящий сборник позволяет проводить текущий контроль успеваемости и промежуточную аттестацию. Это помогает аттестовать обучающихся на соответствие их персональных достижений поэтапным требованиям соответствующей образовательной программы.

Данный вид контроля стимулирует у обучающихся стремление к систематической самостоятельной работе по изучению профессиональных модулей, овладению компетенциями.

Сборник методических разработок технологического профиля.
БУ «Междуреченский агропромышленный колледж»
26 марта 2025 года

Подписано в печать: 27.03.2025 г. Формат 60*90 1-16
Усл.печ.л 12,5.
Издательство: бюджетное учреждение профессионального образования Ханты-Мансийского автономного округа – Югры «Междуреченский агропромышленный колледж»
Российская Федерация, 628200, Ханты-Мансийский автономный округ – Югра, Кондинский район, поселок городского типа Междуреченский, улица Центральная, дом 54

Опишите основные этапы распознание текста с помощью программы ABBYY FineReader.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №25.

Создание и обработка документов в системе MS Publisher.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №26.

Использование инструментов поисковых систем. Работа с поисковыми серверами

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №27.

Использование программ для хранения информации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №28.

Использование облачных ресурсов. Размещение информации в облачных ресурсах.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №29.

Публикация мультимедиа контента на различных сервисах сети Интернет

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №30.

Раскройте понятие работа с текстовой информацией в персональном компьютере, форматы текстовых файлов,

ПМ 01. Настройка сетевой инфраструктуры.

Вопросы:

1. Классификация компьютерных сетей.
2. Модель взаимодействия открытых систем. Уровни модели OSI.
3. Методы защиты информации от ошибок. Классификация помехоустойчивых кодов
4. Помехоустойчивое кодирование. Кодирование с контролем четности
5. Помехоустойчивое кодирование. Код Хэмминга
6. Использование обратной связи. Основные термины.
7. Система с информационной обратной связью.
8. Система с решающей обратной связью.
9. Понятие коммутации. Коммутация каналов.
10. Понятие коммутации. Коммутация сообщений.
11. Понятие коммутации. Коммутация пакетов.
12. Способ передачи пакетов в сетях.
13. Протоколы. Стандартные стеки коммуникационных протоколов.
14. Стек протоколов TCP/IP.
15. Классы IP-адресов. Особые IP-адреса.
16. Стек протоколов IPX/SPX.
17. Семейство сетевых технологий Ethernet. Принцип работы Ethernet.
18. Принцип работы Ethernet. Взаимодействие на подуровнях LLC и MAC.
19. Характеристики физической среды передачи данных.
20. Коаксиальный кабель. Конструкция и характеристики.
21. Витая пара. Конструкция и характеристики.
22. Оптоволокно. Конструкция и характеристики.
23. Стандарты беспроводных сетей
24. Основные режимы работы беспроводных сетей
25. Область применения сетей Wi-Fi. Примеры использования.

Практические задания: **ЗАДАНИЕ № 1**

Текст задания: Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **192.168.0.0**

IP – адрес второй подсети **10.101.120.0** Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 2

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **156.140.125.0** IP – адрес второй подсети **130.120.110.16** Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 3

Текст задания: Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать

коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **113.240.23.24** IP – адрес второй подсети **120.4.110.200**
Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 4

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **119.4.155.16**
IP – адрес второй подсети **120.4.155.200**
Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 5

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **112.26.23.64** IP – адрес второй подсети **145.68.23.56**
Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 6

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **100.45.25.80**
IP – адрес второй подсети **12.26.85.40**
Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 7

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **13.75.96.56**
IP – адрес второй подсети **12.26.185.40** Максимальное количество IP-адресов – 6
Количество используемых хостов - 4

ЗАДАНИЕ № 8

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **30.56.82.16**
IP – адрес второй подсети **177.12.19.80**

Нормативные документы по охране труда при работе с персональным компьютером. Санитарно-гигиенические нормы при работе на персональном компьютере.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №13.

Опишите основные возможности текстового редактора. Создание документов в текстовом редакторе MS Word, форматирование текста, вставка таблиц, рисунков, формул.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №14.

Опишите средства и методы для защиты информации. Антивирусные программы.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №15.

Опишите назначение, возможности и применение электронных таблиц, принцип их построения и организации работы с ними. Правил ввода, обработки, оформления, редактирования данных и выполнения вычислительных операций. в MS Excel.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №16.

Опишите основные возможности программ для создания и обработки музыки. Работа с аудио файлами.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №17.

Опишите основные возможности программ для создания и обработки видео. Работа с видео файлами.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №18.

Опишите основные возможности программ для создания и обработки растровой графики.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №19.

Опишите основные возможности программ для создания и обработки векторной графики.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №20.

Опишите назначение, возможности и применения систем управления базами данных. Создание таблиц, форм, запросов и отчётов в СУБД MS Access.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №21.

Выполнение мероприятий по защите персональных данных. Принципы антивирусной защиты персонального компьютера.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №22.

Правила эксплуатации периферийного оборудования и компьютерной оргтехники.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №23.

Процесс конвертирования файлов. Основные понятия сжатия файла.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №24.

ПМ.05. ЭКСПЛУАТАЦИЯ ОБЛАЧНЫХ СЕРВИСОВ

5.1 Фонд оценочных средств для промежуточного контроля

Комплект материалов для оценки освоения теоретического курса ПМ

Задания для оценки освоения МДК.04.01

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1.

Опишите устройство персональных компьютеров, основные блоки, функции и технические характеристики.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2.

Раскройте понятие архитектуры, состава, функции и классификацию операционных систем персонального компьютера.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 3.

Опишите виды и назначения принтеров, их устройство и принцип действия, интерфейсы подключения и правила эксплуатации.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 4.

Опишите виды и назначения сканеров, их устройство и принцип действия, интерфейсы подключения и правила эксплуатации.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №5.

Опишите этапы установки и настройки основных компонентов операционной системы и драйверов периферийного оборудования.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 6.

Опишите назначение, возможности, правил эксплуатации мультимедийного оборудования, основные типы интерфейсов для подключения мультимедийного оборудования.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 7.

Раскройте понятие цифрового представления звуковой информации в персональном компьютере, форматы аудио файлов, конвертирование файлом

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 8.

Раскройте понятие цифрового представления графической информации в персональном компьютере, форматы графических файлов,

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 9.

Раскройте понятие цифрового представления видео информации в персональном компьютере, форматы видео файлов, конвертирование файлом.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №10.

Опишите принципы функционирования локальных и глобальных компьютерных сетей. Подключение сети, её настройка.

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №11.

Настройка беспроводной компьютерной сети. Изучение доступа и использование информационных ресурсов беспроводных компьютерных сетей

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №12.

Максимальное количество IP-адресов – 6Количество используемых хостов - 4

ЗАДАНИЕ № 9

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **188.52.195.72** IP – адрес второй подсети **111.45.32.16**
Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 10

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **11.52.74.80**
IP – адрес второй подсети **177.52.69.80** Максимальное количество IP-адресов – 6
Количество используемых хостов - 4

ЗАДАНИЕ № 11

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **112.126.123.64**
IP – адрес второй подсети **25.45.85.56**
Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 12

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **201.45.75.96** IP – адрес второй подсети **177.152.169.80**
Максимальное количество IP-адресов – 6 Количество используемых хостов4

ЗАДАНИЕ № 13

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **155.45.85.112** IP – адрес второй подсети **201.125.63.16**
Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 14

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **188.52.95.72** IP – адрес второй подсети **201.125.163.16** Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 15

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **37.45.95.32**

IP – адрес второй подсети **192.158.56.96** Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 16

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **137.145.95.32** IP – адрес второй подсети **192.58.56.96** Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 17

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **10.10.25.72**

IP – адрес второй подсети **112.56.35.80** Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 18

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **180.10.215.72** IP – адрес второй подсети **12.56.135.80** Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 19

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **187.140.115.72** IP – адрес второй подсети **12.156.15.80** Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 20

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать

15. Использования сторонних проприетарных решений для интеграции в облако
16. Установка и настройка Raid на linux
17. Установка и настройка Raid на windows server
18. Установка и настройка Zabbix-server
19. Установка и настройка файлового сервера на windows server, Linux
20. Установка и настройка OpenNAS
21. Обеспечение своевременного копирования, архивирования и резервирования данных.
22. Установка на серверы и рабочие станции: операционные системы и необходимое для работы программное обеспечение.
23. Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования
24. Осуществление конфигурирования программного обеспечения на серверах
25. Установка прав доступа и контроль использования сетевых ресурсов
26. Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов
27. Повышения безопасности функционирования программных средств и баз
28. Создание резервных копий баз данных
29. Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам

Вопросы к экзамену

1. Что представляет собой облачная безопасность данных.
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. Политика безопасности, сервер сетевых политик и защита сетевого доступа
8. Методики мониторинга состояния сети
9. Фильтрация трафика с помощью межсетевых экранов (firewall), списков контроля доступа (ACL)
10. Стратегия защиты от DoS и DDoS атак
11. Основные типы облачных хранилищ
12. Технологии резервного копирования в облачные сервисы
13. Технологии резервного копирования: общие правила хранения данных
14. Настройка сервисов сертификации на сервисах
15. Настройка сервисов аутентификации
16. Настройка системы мониторинга состояния сети и сервисов
17. Стратегии аварийного восстановления данных
18. Общие характеристики современных предоставляемых услуг хранения данных в сети Интернет
19. Системы управления состоянием защиты виртуальной среды
20. Развёртывание IT-инфраструктуры на базе IaaS
21. Развёртывание IT-инфраструктуры на базе PaaS
22. Развёртывание IT-инфраструктуры на базе SaaS
23. Контроль целостности виртуальных машин (гипервизоров)
24. Политики доступа пользователей к инфраструктуре
25. Технология VPN
26. Использование изолированной части инфраструктуры для тестирования новых версий программного обеспечения
27. Настройка механизмов управления правами доступа пользователей
28. Настройка отказоустойчивости
29. Настройка контроля целостности виртуальных машин гипервизоров
30. Установка криптографической системы безопасности на сервисы
31. Развёртывание защиты от DDoS атак
32. Моделирование угроз инфраструктуры по списку OWASP TOP 10
33. Установка и настройка системы фильтрации трафика Firewall
34. Установка системы резервного копирования данных

Вопросы к дифференцированному зачету Сетевая файловая система (NFS)

1. Сетевой протокол SMB
2. Мультипротокольная система хранения Unified Storage
3. Программно-определяемое хранилище SDS
4. Гиперконвергентные системы
5. Облака и эфемерные хранилища
6. Технология Raid
7. Валидация облачных данных
8. Контроль целостности облачных данных
9. Хеширование облачных данных
10. Резервация облачных данных
11. Миграция облачных данных
12. Оперативная аналитическая обработка данных
13. Интеллектуальный анализ данных
14. Инструментальные средства хранения и анализа данных

коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **185.26.53.80** IP – адрес второй подсети **124.156.18.80**
Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 21

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **12.45.85.144**
IP – адрес второй подсети **112.45.96.8**
Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 22

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **12.145.83.144** IP – адрес второй подсети **112.145.196.8**
Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 23

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **112.135.103.144**
IP – адрес второй подсети **112.135.0.8**
Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 24

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **26.85.73.8**
IP – адрес второй подсети **135.63.59.8**
Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 25

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **26.85.73.8**

IP – адрес второй подсети **123.61.81.16** Максимальное количество IP-адресов – 6
Количество используемых хостов - 4

ЗАДАНИЕ № 26

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **166.75.173.8** IP – адрес второй подсети **123.166.81.16**
Максимальное количество IP-адресов – 6 Количество используемых хостов - 4

ЗАДАНИЕ № 27

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **126.75.73.8**
IP – адрес второй подсети **153.161.81.16** Максимальное количество IP-адресов – 6
Количество используемых хостов - 4

ЗАДАНИЕ № 28

Текст задания:Создать сеть для трех ПК, разделенной на две подсети с использованием двух сетевых интерфейсов на одном из узлов. При монтаже сети необходимо использовать коммутационную панель, сетевую розетку и коммутатор/маршрутизатор. Используя сетевые утилиты проверить работоспособность подсети.

Конфигурация сети:

IP – адрес первой подсети **146.75.73.8**
IP – адрес второй подсети **10.121.181.16** Максимальное количество IP-адресов – 6
Количество используемых хостов – 4

Перечень вопросов и практических заданий для проведения экзамена по МДК.01.02 «Организация, принципы построения и функционирования компьютерных сетей»

Вопросы:

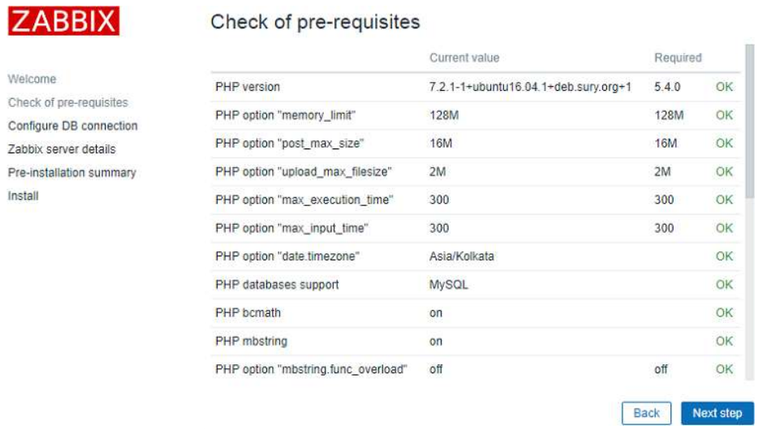
1. Основные компоненты сетей, сетевая среда и сетевые устройства. Перечислите основные компоненты сетей и различные виды сетевых устройств.
2. Планирование структуры сети Методика и начальные этапы проектирования сети.
3. Протокол разрешения адресов (ARP). Сформулируйте назначение протокола ARP и его применение в компьютерных сетях.
4. Протокол разрешения адресов (ARP). Параметр протокола ARP по которому определяется Мак адрес устройства.
5. Схемы адресов. Перечислите существующие протоколы ip адресации их принципиальные различия.
6. Сетевые протоколы и стандарты. Перечислите несколько уровней модели TCP/IP и опишите их функции.
7. Сетевые протоколы и стандарты. Перечислите несколько уровней модели OSI и опишите их функции.
8. Передача данных в сети. Перечислите и опишите функции двух основных протоколов, служащие для передачи данных в сети интернет.
9. Протоколы физического уровня. Перечислите протоколы физического уровня и их функции.

ПМ.04. ЭКСПЛУАТАЦИЯ ОПЕРАЦИОННЫХ СИСТЕМ.

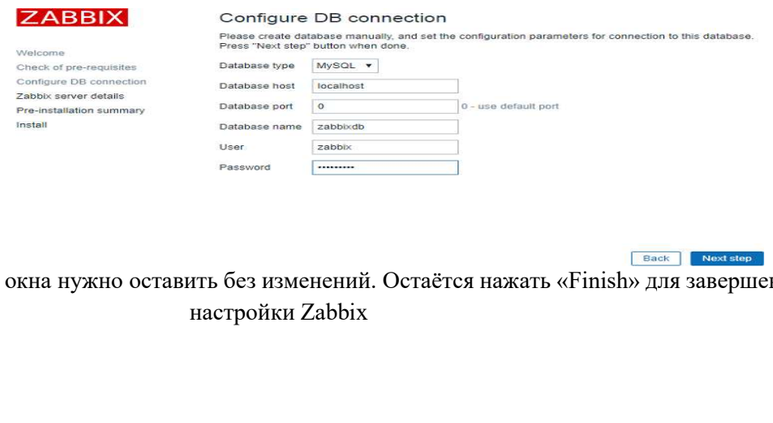
Вопросы к экзамену

МДК.04.01 Технологии виртуализации и автоматизации

1. Hypervisor (гипервизор),
2. Технологии виртуализации
3. Виртуализация ресурсов. compute, storage, network
4. Виртуальная коммутация. Передача сетевого состояния, datapath, удаленного управления трафиком, виртуальный NAT
5. Сетевой мост
6. Инструменты виртуализации. Qemu, KVM, Virt-manager
7. Снимок виртуальной машины
8. Клонирование и шаблоны виртуальных машин.
9. Востановление виртуальной машины
10. Мониторинг состояния виртуальной машины
11. Процедура миграции, резервного копирования и восстановления виртуальной машины.
12. Состояние дисков виртуальной машины
13. Решения виртуализации
14. Организация облачных сервисов на основе кластерного подхода.
15. Обзор технологий кластеризации
16. Кластер Proxmox VE. Узлы кластера. Отказоустойчивость. Репликация.
17. Кластера Kubernetes в среде Proxmox VE. Мастер-ноды Kubernetes.
18. Оркестрация контейнеров, Kube-Proxy
19. Компоненты управления Kubernetes
20. Диспетчер облачных контроллеров
21. Исполняемые среды контейнеров. Docker, containerd, CRI-O и Kubernetes CRI
22. Планирование, приоритезация и вытеснение
23. Администрирование кластера. Планирование кластера, ведение журнала в Kubernetes
24. Управление ресурсами кластера. Организация конфигураций ресурсов
25. Управление поведением VM/CT startup and shutdown
26. Резервное копирование и репликация виртуальных машин и контейнеров
27. Пакетные операции в kubectl
28. Архитектура для сбора логов.
29. Основы сбора логов в Kubernetes
30. Сбор логов на уровне узла
31. Архитектуры для сбора логов на уровне кластера.
32. Использование агента на уровне узлов
33. Прямой доступ к логам из приложения
34. Настройка пользовательских сервисов
35. Облачные бизнес-модели.
36. IaaS, PaaS и SaaS
37. IaaS. Ресурсы как услуга. Гибкие модели оплаты PaaS.
38. Балансировщик нагрузки и управление интернет-трафиком
39. Работа DNS
40. SaaS. Настройки приложений, мониторинга и резервного копирования
41. Миграции виртуальных серверов
42. Работа с Hypervisor: Настройка виртуальной маршрутизации
43. Работа с Hypervisor: Автоматизциия развёртывания виртуальных машин
44. Работа с Hypervisor: Конфигурация ресурсов виртуальных машин
45. Работа с Hypervisor: Развёртывание сервисов для конечного пользователя
46. Установка Kubernetes в среде Proxmox VE
47. Настройка Kubernetes в среде Proxmox VE
48. Работа с контейнерами Kubernetes в среде Proxmox VE
49. Оркестрациия Kubernetes в среде Proxmox VE



осле нажатия на кнопку «Next step» необходимо ввести параметры подключения к базе данных, которая была создана.



Параметры следующего окна нужно оставить без изменений. Остаётся нажать «Finish» для завершения настройки Zabbix

10. Протоколы канального уровня. Опишите назначение протокола канального уровня Point-to-Point Protocol over Ethernet (PPPoE)
11. Управление доступом к среде. Уровень модели OSI к которому можно соотнести подуровень «управление доступом к среде».
12. Управление доступом к среде. Опишите назначение под уровня модели OSI управление доступом к среде.
13. Протокол Ethernet .Опишите назначение технологии Ethernet, на каком уровне модели OSI работает технология Ethernet.
14. Коммутаторы локальных сетей. Опишите назначение коммутаторов локальных сетей и их отличие от маршрутизаторов.
15. Протокол разрешения адресов (ARP). Опишите схему работы протокола ARP.
16. Протоколы сетевого уровня. Опишите назначение и функции сетевого протокола RIP.
17. Маршрутизация. Перечислите существующие виды маршрутизации и способы их применения.
18. Маршрутизаторы.Опишите назначение маршрутизаторов и их отличие от коммутаторов.Настройка маршрутизатора Cisco. Опишите принцип настройки маршрутизатора Cisco, приведите пример настройки ip адресации и настройки vlan.
19. IP – адресация. Сформулируйте определение, IP-адрес это…
20. Разделение IP-сетей на подсети. Опишите назначение маски подсети и ее свойства. Запишите маску подсети 255.255.255.0 в двоичной форме.
21. Протоколы транспортного уровня. Опишите назначение протоколов транспортного уровня TCP, UDP.
22. Протоколы уровня приложений. Опишите назначение и функции протокола уровня приложений DNS.
23. Проектирование небольшой сети. Перечислите приложения для проектирования локальных сетей.
24. Поиск и устранение неполадок. Сформулируйте методы средства поиска и устранения неполадок в сети.
25. Cisco IOS. Базовая настройка устройств. Опишите базовую настройку маршрутизатора под управлением Cisco IOS, настраиваемые параметры и необходимые команды.
26. Концепция маршрутизации. Опишите концепцию динамической маршрутизации.
27. Конфигурация маршрутизатора. Сформулируйте пример базовой настройки маршрутизатора, а так же основные настройки.
28. Статическая маршрутизация. Какую маршрутизацию называют статической?
29. Настройка статических маршрутов. Опишите методы настройки статических маршрутов, а также команды применяемые для настройки маршрутов.
30. Динамическая маршрутизация. Опишите методы настройки динамической маршрутизации, а также команды применяемые для настройки маршрутизации. Перечислите протоколы динамической маршрутизации и их функции.
31. Сегментация IP-сетей. Перечислите протоколы которые используются для сегментирования IP-сетей и опишите их роли и функции.
32. Коммутируемые сети. Опишите вид коммутации сети на уровне ядра. Опишите вид коммутации сети на уровне распределения.
33. Конфигурация коммутатора. Сформулируйте пример базовой настройки коммутатора, а так же его основные настройки.
37. Сети VLAN. Опишите назначение сетей VLAN в крупных сетях.
38. Маршрутизация между сетями VLAN. Как включить маршрутизацию между сетями VLAN на коммутаторе.
39. Списки контроля доступа. Опишите назначение списков контроля доступа, а также их преимущества и недостатки.

40. Настройка стандартных ACL – списков. Опишите методы настройки стандартных ACL – списков на маршрутизаторе.

41. DHCPv4. Опишите методологию настройки DHCPv4 на роутере.

42. DHCPv6. Опишите методологию настройки DHCPv6 на роутере.

34. Преобразование NAT для IPv4. Опишите назначение технологии NAT, ее принцип действия, а также преимущества и недостатки данной технологии.

35. Настройка NAT. Опишите принцип настройки технологии NAT на маршрутизаторе.

36. Различные типы сети Ethernet. Перечислите существующие типы сети Ethernet и опишите характеристики этих сетей.

37. Беспроводная сеть. Перечислите существующие технологии беспроводных сетей и их характеристики.

38. Установка и подключение сетевого оборудования. Установка и подключение сетевого оборудования.

39. Настройка сети в Windows Server. Опишите назначение компонента Active Directory в Windows Server.

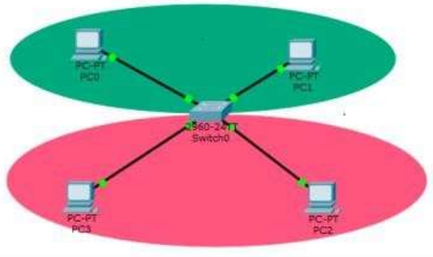
40. RAID-технологии. Опишите существующие RAID-технологии и принципы их работы.

Практические задания:

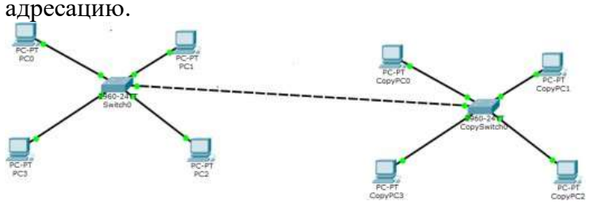
1. Выполните подключение к сетевому оборудованию в программе Cisco Packet Tracer. Добавьте в схему коммутатор Cisco 2960 и один компьютер, после настройте сеть. Настройте коммутатор с помощью консольного кабеля RS 232-Console.

Выполните первичную настройку коммутатора, установите пароль на enable, зашифруйте пароль, настройте транспортный протокол Telnet, подключитесь к Telnet по консоли.

2. Выполните настройку технологии VIRTUAL LOCAL AREA NETWORK в программе Cisco Packet Tracer. Сконфигурируйте схему подставленную на рисунке, в данном случае необходимо выбрать коммутатор Cisco 2960, изолируйте две подсети с помощью vlan, настройте IP адресацию.



1. Выполните настройку технологии Virtual Local Area Network в программе Cisco Packet Tracer. Сконфигурируйте схему подставленную на рисунке, в данном случае необходимо выбрать коммутатор Cisco 2960, изолируйте две подсети с помощью vlan, настройте IP адресацию.



2. Выполните настройку агрегации каналов etherchannel в программе Cisco Packet Tracer. Сконфигурируйте схему подставленную на рисунке, добавьте 2 коммутатора и 2 компьютера, настройте IP адресацию, соедините коммутаторы в агрегированный канал и выполите настройку. Для проверки отказоустойчивости от отключите один из портов.

Редактируем файл «/etc/opt/rh/rh-php72/php-fpm.d/zabbix.conf»: vi /etc/opt/rh/rh-php72/php-fpm.d/zabbix.conf

Раскоментируем строку и изменим значение: php_value[date.timezone] = Europe/Moscow **Запуск Zabbix-сервера и процессов агента Debian 10**

systemctl restart zabbix-server zabbix-agent apache2 systemctl enable zabbix-server zabbix-agent apache2

Ubuntu 20.04

systemctl restart zabbix-server zabbix-agent apache2 systemctl enable zabbix-server zabbix-agent apache2 **Centos 7**

systemctl restart zabbix-server zabbix-agent httpd rh-php72-php-fpm systemctl enable zabbix-server zabbix-agent httpd rh-php72-php-fpm **Настройка iptables в CentOS 7**

Отключаем и убираем из автозагрузки firewall:

systemctl stop firewalld systemctl disable firewalld

Устанавливаем службку iptables:

yum install iptables-services Создаем правила:

iptables -I INPUT 1 -p tcp --dport 1500 -j ACCEPT iptables -I INPUT 1 -p tcp --dport 80 -j ACCEPT Сохраняем правила:

service iptables save

Включаем сервис iptables в автозагрузку:

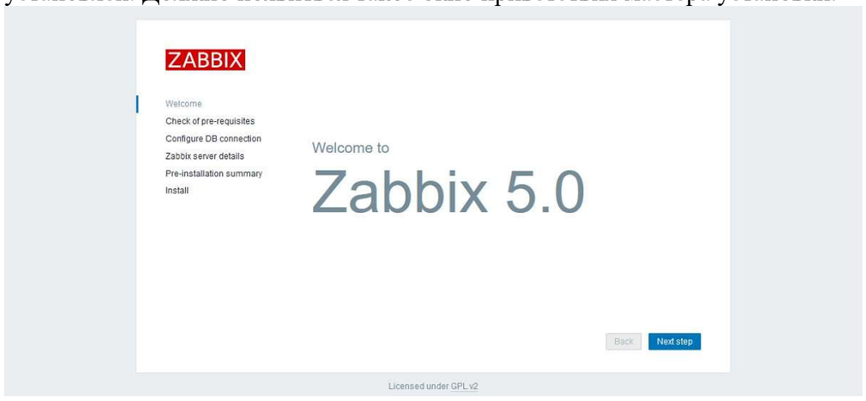
service iptables enable

Проверка доступности веб-интерфейса

Переходим по адресу «http: // server_ip_or_name / zabbix», где «server_ip_or_name» — IP-адрес или доменное имя сервера.

Настройка web-интерфейса

Для установки и настройки Zabbix через web-интерфейс нужно перейти на страницу, где он установлен. Должно появиться такое окно приветствия мастера установки.



Далее нужно нажать на кнопку продолжения установки «Next step». После этого отобразится анализ соответствия Zabbix-сервера всем системным требованиям текущего сервера. Возле каждого из них должен стоять параметр соответствия «Ок».

cd /tmp

Устанавливаем консольную утилиту wget:

apt -y install wget

Устанавливаем APT репозиторий с deb-пакетом, который управляет загрузкой и настройкой программного обеспечения MySQL:

wget https://dev.mysql.com/get/mysql-apt-config_0.8.13-1_all.deb dpkg -i mysql-apt-config_0.8.13-1_all.deb

Для установки последней версии нужно оставить все как есть и нажать ввод на «Ok» Устанавливаем MySQL сервер:

apt update

apt install mysql-server

Во время установки появится диалоговое окно конфигурации, в котором нужно будет задать пароль пользователя root для MySQL. Введите безопасный и надежный пароль, а затем подтвердите его.

После этого появится предупреждение о новой системе аутентификации, на основе SHA256, использующейся в MySQL. Нажимаем «Ok». Далее следует выбрать плагин аутентификации (если оставить вариант по умолчанию, будет использоваться рекомендуемый плагин) и нажать «Enter», чтобы завершить процесс установки.

Ubuntu 20.04

Устанавливаем MySQL сервер:

apt install mysql-server

Запускаем MySQL сервер и добавляем его в автозагрузку:

systemctl start mysql systemctl enable mysql

Производим первоначальную настройку MySQL:

mysql_secure_installation

На первом вопросе, жмём «2», а далее создаём пароль для root и на все вопросы отвечаем «Y» (yes).

CentOS 7

Устанавливаем репозиторий «epel-release»:

yum install epel-release Устанавливаем сервер MariaDB :

yum install mariadb-server

Запускаем сервер MariaDB и добавляем его в автозагрузку:

systemctl start mariadb systemctl enable mariadb

Производим первоначальную настройку MariaDB:

/usr/bin/mysql_secure_installation

На первом вопросе, жмём «Enter», так как пароль для root ещё не создан. Далее создаём пароль для root и на все вопросы отвечаем «Y» (yes).

Создание базы данных и пользователя

Это общий шаг для всех ОС. mysql -uroot -p

password

mysql> create database zabbix character set utf8 collate utf8_bin; mysql> create user zabbix@localhost identified by 'zabbix'; mysql> grant all privileges on zabbix.* to zabbix@localhost; mysql> quit;

Вместо «password» в данном примере вписываем пароль от root, заданный на предыдущем шаге. Имортируем исходную схему и данные:

zcat /usr/share/doc/zabbix-server-mysql*/create.sql.gz | mysql -uzabbix -p zabbix Появится диалоговое окно с требованием ввести пароль. Вводим «zabbix». Редактируем файл «/etc/zabbix/zabbix_server.conf»:

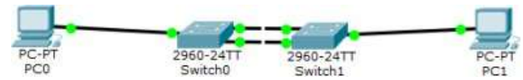
vi /etc/zabbix/zabbix_server.conf Раскоментируем строку и меняем значение: DBPassword=zabbix

Настройка PHP для веб-интерфейса Zabbix Debian 10 и Ubuntu 20.04

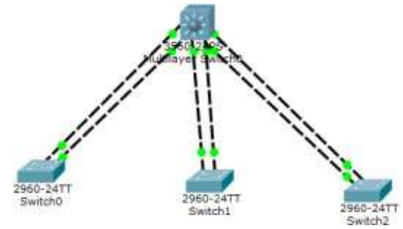
Редактируем файл «/etc/zabbix/apache.conf»: vi /etc/zabbix/apache.conf

Раскоментируем строку и изменим значение: php_value[date.timezone] = Europe/Moscow

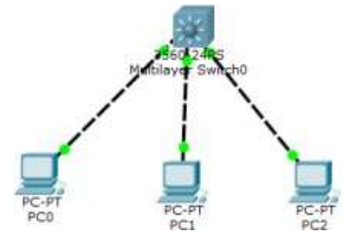
Centos 7



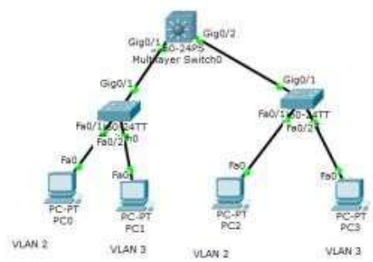
3. Выполните настройку динамической агрегации каналов etherchannel в программе Cisco Packet Tracer. Сконфигурируйте схему подставленную на рисунке, добавьте 3 коммутатора l-2 уровня и 1 коммутатор L-3 уровня, соедините коммутаторы в агрегированный канал и выполите настройку. Для проверки отказоустойчивости от отключите один из портов.



4. Выполните настройку коммутатора L3 уровня в программе Cisco Packet Tracer. Создать локальную сеть, состоящую из нескольких подсетей на основе коммутатора 3 уровня Cisco 3650, схема представлена на рисунке. Изолируйте сети с помощью технологии Vlan, для каждого компьютера создайте свою изолированную сеть, настройте IP адресацию. Выполите настройку по маршрутизации трафика между Vlan.

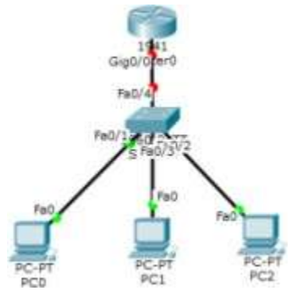


5. Выполните настройку трёх коммутаторов L3 и L2 уровня в программе Cisco Packet Tracer. Создать локальную сеть, состоящую из нескольких подсетей на основе коммутатора 3 уровня Cisco 3650, схема представлена на рисунке. Изолируйте сети с помощью технологии Vlan, для каждого компьютера создайте свою изолированную сеть, настройте IP адресацию. Выполите настройку по маршрутизации трафика между Vlan. Для настройке Vlan

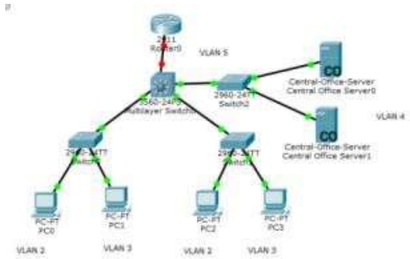


используйте команды access и trunk.

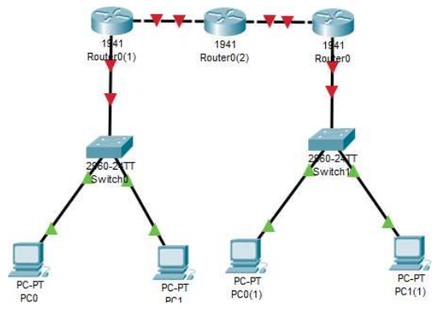
6. Выполните настройку маршрутизатора в программе Cisco Packet Tracer. Постройте маршрутизируемую IP-сеть, сконфигурируйте 3 компьютера, один коммутатор Cisco 2960, маршрутизатор Cisco 1941, для каждого компьютера создайте свою изолированную сеть Vlan, на маршрутизаторе создайте виртуальные саб интерфейсы с привязкой IP адресов, настройте IP адресацию на компьютерах.



7. Выполните настройку маршрутизатора и коммутатора в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте маршрутизируемую IP-сеть, сконфигурируйте 4 компьютера, 2 сервера, 3 коммутатора Cisco 2960, маршрутизатор Cisco 1941, для каждого компьютера создайте свою изолированную сеть Vlan, на маршрутизаторе создайте виртуальные интерфейсы Vlan с привязкой IP адресов, настройте IP адресацию на компьютерах.



8. Выполните настройку статической маршрутизации в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте маршрутизируемую IP-сеть, сконфигурируйте 4 компьютера, 2 коммутатора Cisco 2960, 3 маршрутизатора Cisco 1941, для каждого компьютера создайте свою изолированную сеть Vlan, на маршрутизаторе создайте виртуальные интерфейсы Vlan с привязкой IP адресов, настройте IP адресацию на компьютерах. Пропишите статические маршруты на роутерах.



9. Выполните настройку DHCP протокола на роутере в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте маршрутизируемую IP-сеть, сконфигурируйте 3 компьютера, 1 коммутатор Cisco 2960, 1 маршрутизатор Cisco 1941, выполите настройку DHCP на роутере с пулом адресов 192,168,1,1-192,168,1,100.

Включите протокол DHCP на компьютерах.

/var/lib/zabbix/alertscripts:/usr/lib/zabbix/alertscripts -v /var/lib/zabbix/localtime:/etc/localtime -p 10051:10051 -e DB_SERVER_HOST="zabbix-postgres" -e POSTGRES_USER="zabbix" -e POSTGRES_PASSWORD="zabbix" -d zabbix/zabbix-server-pgsql:alpine-latest

Остаётся запустить веб-сервер Zabbix:

docker run --name zabbix-web -p 80:8080 -p 443:8443 --network zabbix-net -e DB_SERVER_HOST="zabbix-postgres" -v /var/lib/zabbix/localtime:/etc/localtime -e POSTGRES_USER="zabbix" -e POSTGRES_PASSWORD="zabbix" -e ZBX_SERVER_HOST="zabbix- server" -d zabbix/zabbix-web-nginx-pgsql:alpine-latest

В примере используется Nginx.

Остаётся перейти по адресу: «http://<host_ip>/», и войти в веб-интерфейс, воспользовавшись логином

– «**Admin**», и паролем – «**zabbix**».

Ручная установка

Ниже мы покажем как развернуть Zabbix на VDS на примере трех ОС — Debian 10, Ubuntu 20.04 и CentOS 7.

Установка на Zabbix на Debian 10

Команды, вводимые в терминале на Debian 10 (Debian 9) практически идентичны Ubuntu 20.04., но есть некоторые отличия.

Установка системы мониторинга начинается с загрузки deb-пакета Zabbix 5:

wget https://repo.zabbix.com/zabbix/5.0/debian/pool/main/z/zabbix-release/zabbix-release_5.0-1+buster_all.deb

Далее его необходимо установить:

dpkg -i zabbix-release_5.0-1+buster_all.deb apt update

Далее нужно установить Zabix-сервер и агент для его мониторинга командой: apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-agent **Установка Zabbix на Ubuntu 20.04**

Для начала установки Zabbix 5 на Ubuntu загружаем и устанавливаем deb-пакет:

wget https://repo.zabbix.com/zabbix/5.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_5.0-1+focal_all.deb

dpkg -i zabbix-release_5.0-1+focal_all.deb apt update

Устанавливаем Zabix-сервер и агент:

apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-agent

Установка Zabbix на CentOS 7

Установка начинается с добавления репозитория, находящегося на официальном сайте. Сделать это можно при помощи последовательности двух команд:

rpm -Uvh https://repo.zabbix.com/zabbix/5.0/rhel/7/x86_64/zabbix-release-5.0-1.el7.noarch.rpm yum clean all

Далее нужно установить Zabix-сервер и агент:

yum install zabbix-server-mysql zabbix-agent

После этого нужно установить веб-интерфейс Zabix, последовательно выполнив ряд действий.

- Установить пакет актуального софта для CentOS из репозитория Red Hat Software Collections: yum install centos-release-scl
- Отредактировать файл «/etc/yum.repos.d/zabbix.repo» и включить репозиторий «zabbix-frontend», выполнив команду:

vi /etc/yum.repos.d/zabbix.repo

- Здесь следует заменить строку «enabled=0» на «enabled=1». [zabbix-frontend]

...

enabled=1

...

- Далее нужно установить пакеты веб-интерфейса Zabbix: yum install zabbix-web-mysql-scl zabbix-apache-conf-scl

Работа с сервером баз данных MySQL Debian 10

Переходим в директорию «/tmp»:

№5 Установка Zabbix-server на Linux

Развертывание приложения из iso-образа — готовое решение, которое значительно экономит время по сравнению с установкой вручную. Этот вариант подходит для быстрого развертывания Zabbix- сервера (MySQL/PostgreSQL) и Zabbix-прокси (MySQL/SQLite 3).

1. Для начала нужно зайти на официальный сайт приложения, где выложены архивы с готовыми решениями Zabbix под различные виртуальные платформы.
2. Выбрав нужный вариант, нужно скачать его, разархивировать и развернуть в соответствующей виртуальной машине.
3. После развертывания Zabbix, следует запустить его и залогиниться. Обычно, умолчанию логин: «root», пароль: «zabbix», либо эти параметры задаются произвольно в процессе установки.
4. Далее, нужно узнать IP-адрес, которое приложение получило командой «ip addr». Затем вписать полученный адрес в строку браузера в следующем виде: «http://<host_ip>/zabbix» (где

«host_ip» — адрес установленной версии Zabbix) и нажать ввод.

5. Осуществится переход в веб-интерфейс панели управления Zabbix-сервером, где можно сделать все необходимые настройки конфигурации.

Установка Zabbix из контейнеров Docker

Zabbix интегрирован с приложением для контейнеризации Docker. Об установке программы можно узнать здесь.

Каждый компонент Zabbix можно быстро развернуть в виде виртуального контейнера. Они доступны для скачивания на официальном сайте.

Docker-образы Zabbix поставляются для трех операционных систем:

- Ubuntu;
- AlpineLinux;
- CentOS.

Установку Zabbix-сервера можно произвести несколькими основными способами.

Вариант №1

Можно сразу установить готовый образ, включающий в себя Zabbix-сервер, MySQL, Nginx. Для этого нужно выполнить команду:

docker run --name some-zabbix-appliance -p 80:80 -p 10051:10051 -d zabbix/zabbix-appliance:latest Создастся Zabbix-экземпляр, прослушивающий 80 и 10051 порты.

Остаётся перейти по адресу: «http://<host_ip>/». В открывшемся веб-интерфейсе потребуется ввести логин – «**Admin**», пароль – «**zabbix**».

Вариант №2

Существует способ размещения Zabbix, при котором каждый компонент мониторинг-системы расположен в отдельном контейнере.

Для создаваемых контейнеров нужно создать сеть Docker:

docker network create zabbix-net

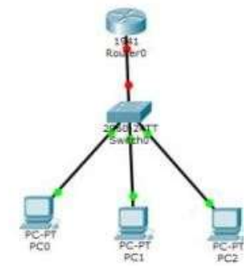
Теперь необходимо запустить контейнер с СУБД:

docker run -d --name zabbix-postgres --network zabbix-net -v /var/lib/zabbix/localtime:/etc/localtime -e POSTGRES_PASSWORD=zabbix -e POSTGRES_USER=zabbix postgres:alpine

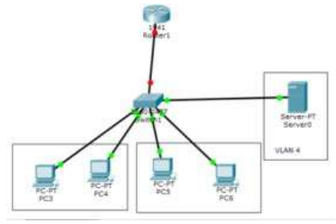
В примере используется Postgresql.

Далее стоит разместить контейнер с Zabbix-сервером:

docker run --name zabbix-server --network zabbix-net -v

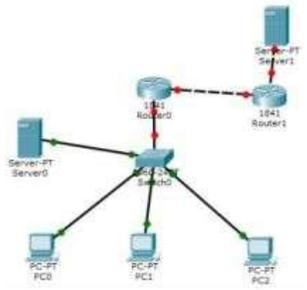


10. Выполните настройку DHCP протокола на сервере в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте маршрутизируемую IP-сеть, сконфигурируйте 4 компьютера, 1 сервер, 1 коммутатор Cisco 2960, 1 маршрутизатор Cisco 1941, изолируйте все сети с помощью Vlan, на роутере создайте виртуальные саб интерфейсы с привязанными IP адресами, выполите настройку DHCP на сервере.

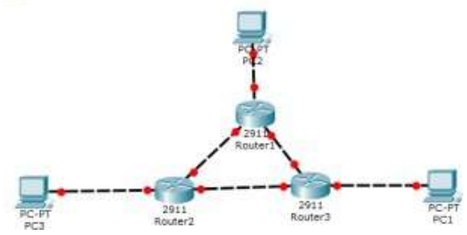


11. Выполните настройку протокола Network Address Tranclation (NAT) в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте маршрутизируемую IP-сеть, сконфигурируйте 3 компьютера, 1 сервер, 1 коммутатор Cisco 2960, 2 маршрутизатора Cisco 1941, изолируйте все сети с помощью Vlan, на роутере создайте виртуальные саб интерфейсы с привязанными IP адресами, назначьте белые IP адреса на роутере провайдера и на внешнем интерфейсе вашего роутера, так же необходимо прописать статические маршруты. Выполите настройку протокола NAT на роутере.

12. Выполните настройку протокола динамической маршрутизации OSPF в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте маршрутизируемую IP-сеть, сконфигурируйте 3 компьютера, 3 маршрутизатора Cisco 2911, настройте ip адресацию,

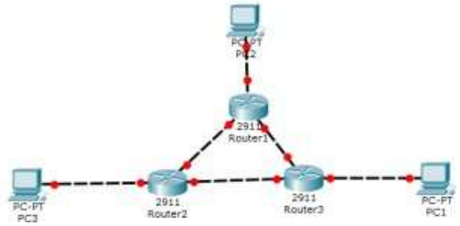


настройте loopback, далее настройте протокол OSPF.



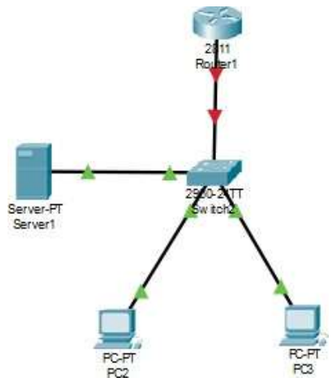
13. Выполните настройку протокола динамической маршрутизации EIGRP в программе

Cisco Packet Tracer. Схема приведена на рисунке. Постройте маршрутизируемую IP-сеть, сконфигурируйте 3 компьютера, 3 маршрутизатора Cisco 2911, настройте ip адресацию, настройте loopback, далее настройте протокол EIGRP.

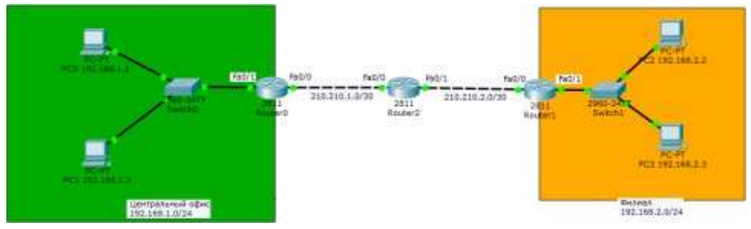


14. Выполните настройку списков контроля доступа (access list) в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте

15. маршрутизируемую IP-сеть, сконфигурируйте 2 компьютера, 1 сервер, 1 коммутатор, 1 маршрутизатор. Изолируйте все компьютеры с помощью Vlan, настройте виртуальные интерфейсы на роутере с IP адресами. Настройте Access листы таким образом, доступ для сервера должен иметь только компьютер бухгалтеров слева.

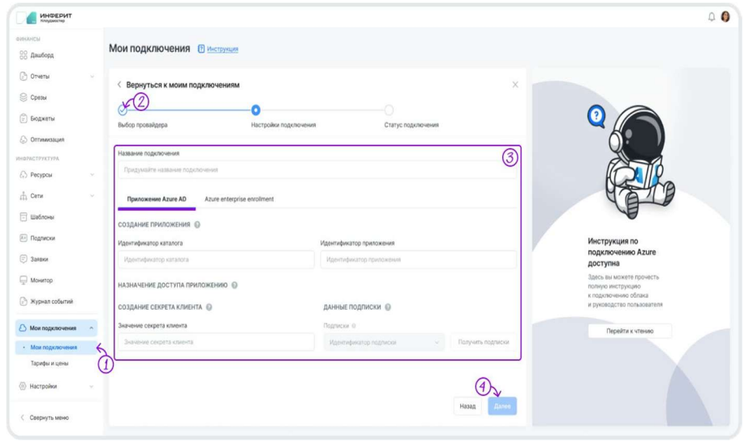


16. Выполните настройку Virtual Private Network (VPN) в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте маршрутизируемую IP-сеть, сконфигурируйте 4 компьютера, 2 коммутатора, 3 маршрутизатора. Настройте IP адресацию, настройте белую IP адресацию во внешней сети, настройте статические маршруты, настройте NAT, настройте протокол VPN.

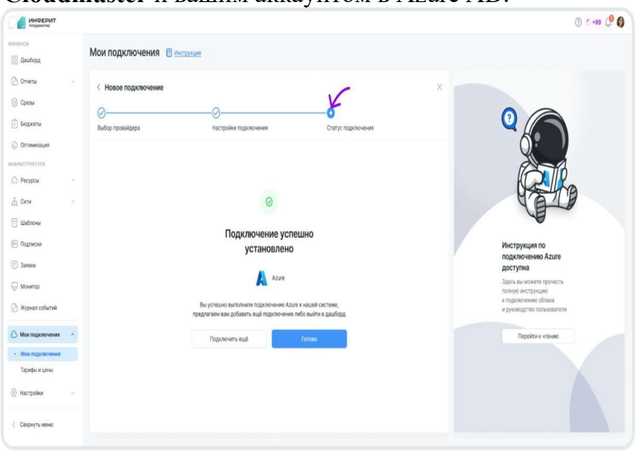


17. Выполните настройку протоколов syslog и ntp в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте IP-сеть, сконфигурируйте 2 компьютера, 1 коммутатор, 1 маршрутизатор. Настройте IP адресацию и протоколы SYSLOG, NTP.

Заполните необходимые данные, затем нажмите на кнопку **Получить подписки**. Если подключение к Azure прошло успешно, рядом с кнопкой активируется выпадающее меню со списком доступных подписок Azure. Выберите подписки и нажмите на кнопку **Подключить**.



В случае успешного прохождения процедуры подключения облака и указания необходимых авторизационных данных (идентификатора каталога, идентификатора приложения и секрета клиента) откроется последний шаг **Статус подключения**, подтверждающий установление соединения между **Cloudmaster** и вашим аккаунтом в Azure AD.



Перейдите к проверке успешности подключения. Длительность загрузки данных

В зависимости от объема сбор данных по инфраструктуре может занять до 10 минут.

Проверка успешности подключения

Проверьте подгрузку данных о подключении в подразделе **Мои подключения** и разделе **Бюджеты**. **Облако в подключениях**

Нажмите на подраздел **Мои подключения** боковой панели **Cloudmaster** и проверьте, отобразилось ли новое подключение в открывшемся подразделе. В карточке подключения проверьте его статус, дату создания и последнего обновления, а также валюту.

Валюта расчетов для Azure определяется автоматически по данным биллинга. Обновление информации по затратам в Azure производится раз в сутки в 02:00 UTC. **Подписки в Бюджетах**

Проверьте, отображаются ли ваши подписки и ресурсные группы.

Перейдите в раздел **Бюджеты** боковой панели. Нажмите на кнопку **Создать бюджет**.

В списке должны появиться выбранные вами подписки на стороне Azure по окончанию настройки подключения в **Cloudmaster**, а также ресурсные группы, если они созданы в облаке.

	Создание приложения Active Directory	Создание приложения и подписок (передавать данные пользователя требуется)	AzureВладелец или администратор недоступа пользователей
Через приложение Azure AD	Настройка прав доступа к подписке(-ам) Azure	Доступ для сбора данных по биллингу подписок Azure (передавать данные пользователя требуется)	Владелец или администратор доступа пользователей
	Настройка прав доступа к рекомендациям по оптимизации Azure	Мониторинг рекомендаций по оптимизации	Читатель (Reader)
Через Azure Enterprise Enrollment	API Доступ к биллингу в Azure Enterprise Enrollment на любом из уровней: на уровне аккаунта/департамента/аккаунта	Загрузка данных биллингового детализации	Биллинговый аккаунт

Настройка подключения

1. Авторизуйтесь в **Cloudmaster** в роли Администратора (см. статью **Авторизация в платформе Cloudmaster**).

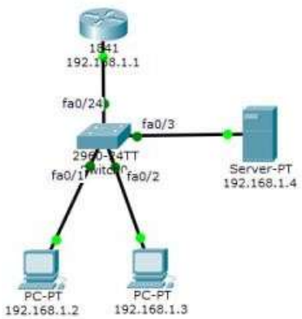
В боковой панели **Cloudmaster** перейдите в подраздел **Мои подключения**, нажмите на кнопку **Новое подключение** и затем — на карточку Azure.

2. При открытии модального окна по подключению облака Azure выберите один из двух способов подключения:
   - через **приложение Azure AD**, или
   - посредством **Azure Enterprise Enrollment**.

Подключение через Azure ADПодключение через Azure Enterprise Enrollment

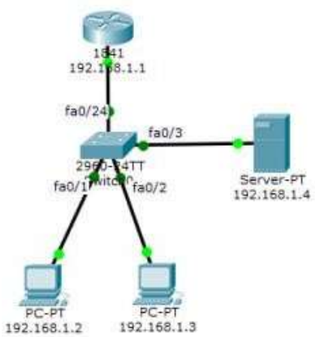
Модель авторизации в приложении Azure AD предполагает внесение следующих данных:

- имени подключения,
- Имя подключения при подключении к **Cloudmaster** произвольное, т.е. может отличаться от его имени на стороне провайдера Azure. Имя подключения в **Cloudmaster** помогает пользователю понять, что это за подключение.
- идентификатора каталога,
- идентификатора приложения, и
- значения секрета клиента. Подробнее о настройках Azure AD здесь.

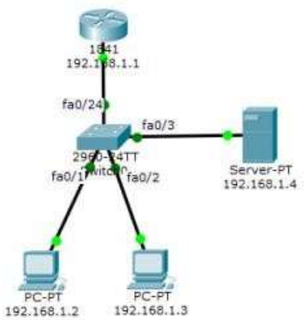


18. Выполните настройку протокола AAA на сервере в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте IP-сеть, сконфигурируйте

2 компьютера, 1 сервер, 1 коммутатор, 1 маршрутизатор. Настройте IP адресацию и протокол AAA на сервере.

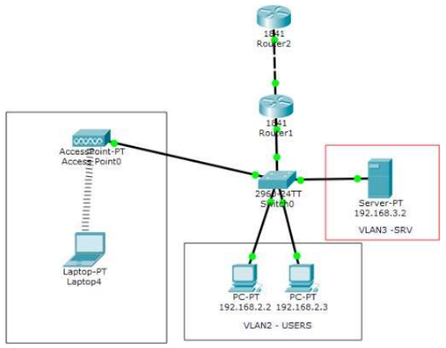


19. Выполните настройку протокола Trivial File Transfer Protocol (TFTP) на сервере в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте IP-сеть, сконфигурируйте 2 компьютера, 1 сервер, 1 коммутатор, 1 маршрутизатор. Настройте IP адресацию и протокол TFTP на сервере.

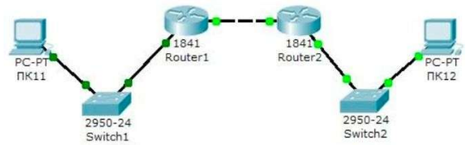


20. Выполните настройку протокола WIFI как точку доступа в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте IP-сеть, сконфигурируйте 2 компьютера, 1 ноутбук с WIFI, 1 точка доступа, 2 маршрутизатора. Настройте IP адресацию изолируйте все компьютеры с помощью Vlan, настройте виртуальные саб интрефейсы с адресами и WIFI.

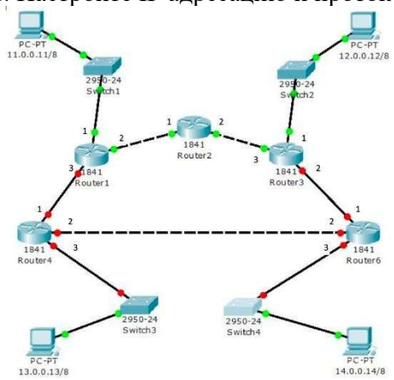
Выполните настройку протокола RIP в программе Cisco Packet Tracer. Схема приведена на



рисунке. Постройте IP-сеть, сконфигурируйте 2 компьютера, 2 коммутатора, 2 маршрутизатора. Настройте IP адресацию и протокол RIP на маршрутизаторах.



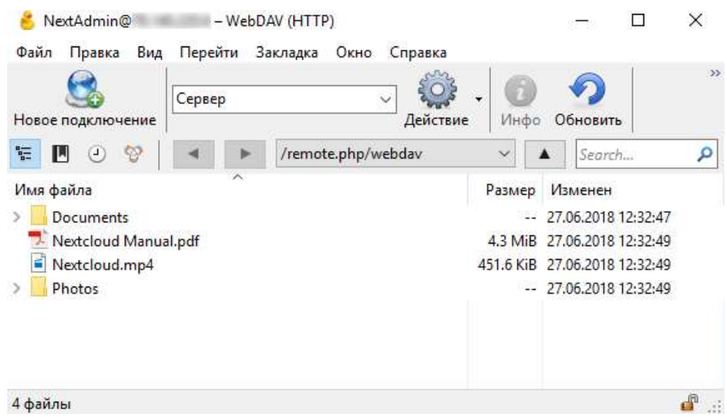
21. Выполните настройку протокола RIP в корпоративной сети в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте IP-сеть, сконфигурируйте 4 компьютера, 4 коммутатора, 6 маршрутизаторов. Настройте IP адресацию и протокол RIP на маршрутизаторах.



22. Выполните настройку протокола Vlan в корпоративной сети в программе Cisco Packet Tracer. Схема приведена на рисунке. Постройте IP-сеть, сконфигурируйте 6 компьютеров, 3 коммутатора L2, 1 коммутатор L3. Настройте IP адресацию, каждый компьютер изолируйте сетью Vlan.

Перечень вопросов и практических заданий для проведения экзамена по МДК.01.03 «Безопасность компьютерных сетей»

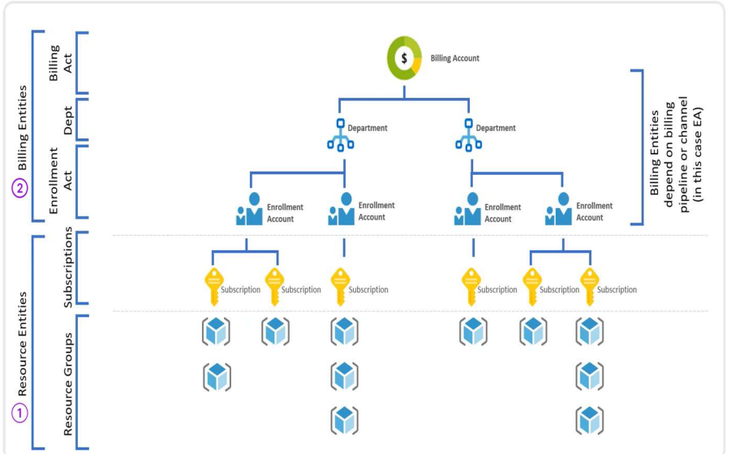
1. Основы информационной безопасности
2. Фундаментальные принципы безопасной сети. Современные угрозы сетевой безопасности
3. Вирусы, черви и троянские кони
4. Методы атак.
5. Безопасность сетевых устройств OSI. Безопасный доступ к устройствам.
6. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности.
7. Авторизация, аутентификация и учет доступа (AAA).
8. Свойства AAA. Локальная AAA аутентификация. Server-based AAA



№4 Установка облачного хранилища в Microsoft Azure

один из нескольких способов создания подключения Azure в зависимости от прав в рамках иерархии объектов биллинга Azure:

Объект биллинга	**Способ подключения Azure в Cloudmaster**
1. Ресурсные объекты	Через **приложение Azure AD** (можно задать подписки Azure, по которым вы хотите получать биллинговые отчеты)
2. Биллинговый аккаунт	Через API ключ **Azure enterprise enrollment** (можно подключить облако Azure на всех уровнях управления: на уровне биллингового аккаунта/департамента/аккаунта)



Доступные сценарии

В текущей версии **Cloudmaster** пользователям с подключением Azure доступны два сценария:

- учет затрат,

Сценарий доступен при создании подключения через **приложение Azure AD** и API ключ **Azure enterprise enrollment**.

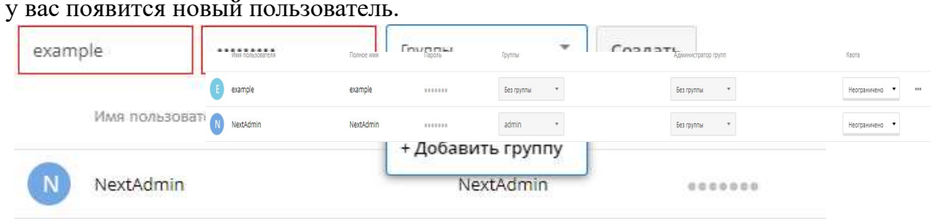
рекомендации по оптимизации.

- Сценарий доступен при создании подключения только через **приложение Azure AD**.

Настройка прав доступа

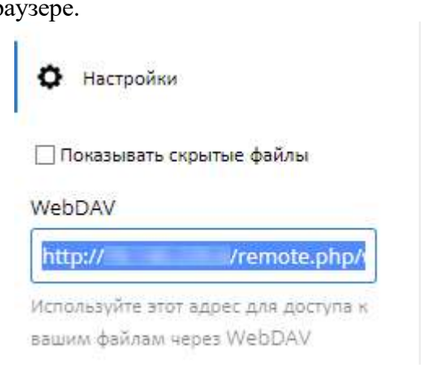
Способ подключения	**Действие**	**Цель**	**Необходимый уровень доступа в Azure**

Введите **Имя пользователя** и **Пароль**, при необходимости укажите группу. Нажмите **Создать**. В результате у вас появится новый пользователь.

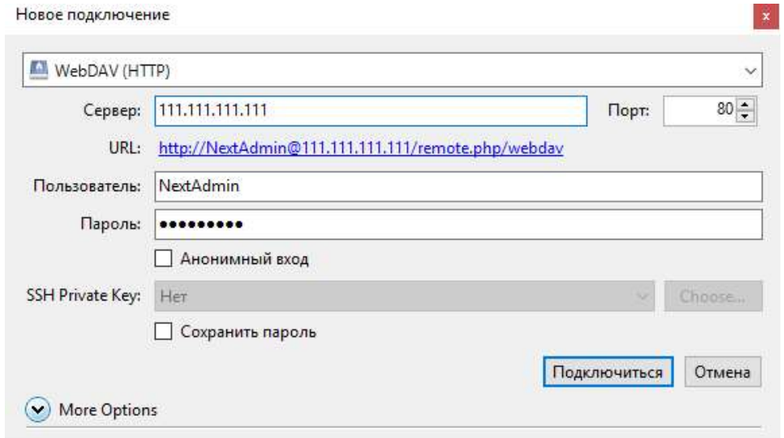


Подключение через WebDav-клиент Cyberduck

Подключение к облачному хранилищу можно сделать по протоколу WebDAV с помощью клиента Cyberduck. Установите приложение и создайте новое подключение. В качестве протокола выберете **WebDAV (HTTP)**. В поле **Сервер** введите адрес, который можно найти в настройках на странице в браузере.



Порт - 80, если вы не изменяли. Введите ваше **Имя пользователя** и **Пароль**. Нажмите **Подключиться**.



Произойдет подключение к хранилищу и откроется корневой каталог.

9. Реализация технологий брандмауэра. ACL. Технология брандмауэра.
10. Контекстный контроль доступа (CBAC). Политики брандмауэра, основанные на зонах
11. Реализация технологий предотвращения вторжения**.** IPS технологии.
12. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS
13. Безопасность локальной сети. Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2).
14. Конфигурация безопасности второго уровня. Безопасность беспроводных сетей, VoIP и SAN
15. Реализация технологий VPN. VPN. GRE VPN. Компоненты и функционирование IPSec VPN.
16. Реализация Site-to-siteIPSec VPN с использованием CLI. Реализация Site-to- siteIPSec VPN с использованием CCP. Реализация Remote-access VPN
17. Криптографические системы. Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей.
18. Управление безопасной сетью. Принципы безопасности сетевого дизайна. Безопасная архитектура.
19. Управление процессами и безопасность. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварийных ситуаций.
20. Жизненный цикл сети и планирование. Разработка регламентов компании и политик безопасности
21. Cisco ASA. Введение в Адаптивное устройство безопасности ASA
22. Конфигурация файрвола на базе ASA с использованием графического интерфейса ASDM
23. Конфигурация VPN на базе ASA с использованием графического интерфейса ASDM
24. Использование Microsoft System Center для мониторинга информационной инфраструктуры и реагирования на инциденты безопасности

Применение криптопровайдера КриптоПро CSP в стандартных приложенИспользование системы Zabbix для мониторинга информационной инфраструктуры и реагирования на инциденты безопасности

25. Классы атак в сетях на основе TCP/IP. Атаки на сетевом и транспортном уровне: Ping, flood, IP spoofing, пассивное сканирование. MITM атаки. Способы предотвращение атак
26. DOS и DDOS атаки. Атаки отказа в обслуживании DDOS. Виды DDOS атак. Предотвращение DDOS атак.
27. Обеспечение безопасности канального уровня. MITM атаки канального уровня: ARP-spoofing, DHCP-spoofing, VLAN-hopping
28. MAC-flooding, атаки на протокол STP. Способы предотвращения атак на канальном уровне
29. Протоколы SSL/TLS. Основные понятия протоколов SSL и TLS. Устройство, принцип работы протокола SSL Цифровые сертификаты. Аутентификация и обмен ключами

Практические задания:

1. Необходимо сохранить резервную копию документов не на физическом носителе. Создайте резервную копию 2 документов из папки в «облачном пространстве» на «яндекс диске».
2. Необходимо сохранить резервную копию документов не на физическом носителе. Создайте резервную копию 2 документов из папки в «облачном пространстве» на «Mail.ru».
3. Используя средства криптографической защиты зашифровать системой шифрования Цезаря свою фамилию, имя, отчество.

4. Используя средства криптографической защиты зашифровать алгоритмом двойных перестановок свою фамилию, имя, отчество.
5. Используя средства криптографической защиты используя шифр перестановки

зашифровать название своей специальности и название изучаемого модуля.

6. Используя средства криптографической защиты зашифровать системой шифрования Цезаря название своей специальности и название изучаемого модуля.

7. Используя средства криптографической защиты зашифровать алгоритмом двойных перестановок название своей специальности и название изучаемого модуля.

Используя средства криптографической защиты используя шифр перестановки зашифровать название своей специальности и название изучаемого модуля.

1.2 Фонд оценочных средств промежуточного контроля по ПМ.01 Настройка сетевой инфраструктуры

Экзамен (квалификационный) проводится непосредственно после завершения освоения программы профессионального модуля, т. е после изучения междисциплинарных курсов и прохождения учебной и (или) производственной практики в составе профессионального модуля. Экзамен (квалификационный) представляет собой форму независимой оценки результатов обучения с участием работодателей.

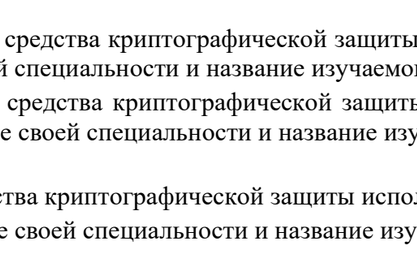
1. Назначение

Экзамен (квалификационный) является формой промежуточной аттестации по профессиональному модулю ПМ. 01 Настройка сетевой инфраструктуры, проводится с целью проверки готовности обучающегося к выполнению вида деятельности: Настройка сетевой инфраструктуры. Спецификацией устанавливается состав оценочных средств, используемых при организации экзамена (квалификационного) по ПМ. 01 Настройка сетевой инфраструктуры.

2. Время аттестации: на проведение аттестации отводится 4 часа, на подготовку – 30 минут .

1. Выполните базовую настройку устройств S1, R1, R2

а. Подключитесь с помощью консоли и активируйте привилегированный



режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

д. Назначьте cisco в качестве пароля VTY и включите вход по паролю. е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа (Используйте слово Warninng).

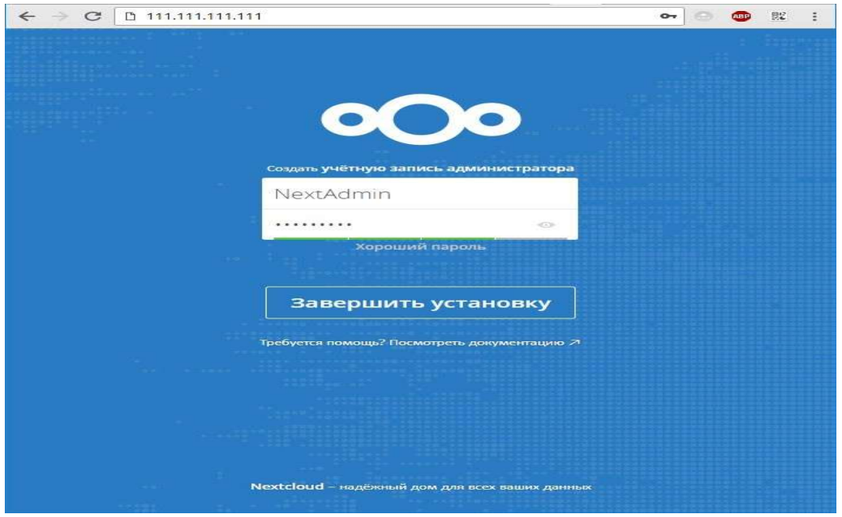
з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

2. **Настроите доступ по протоколу SSH на S1 и R2.**

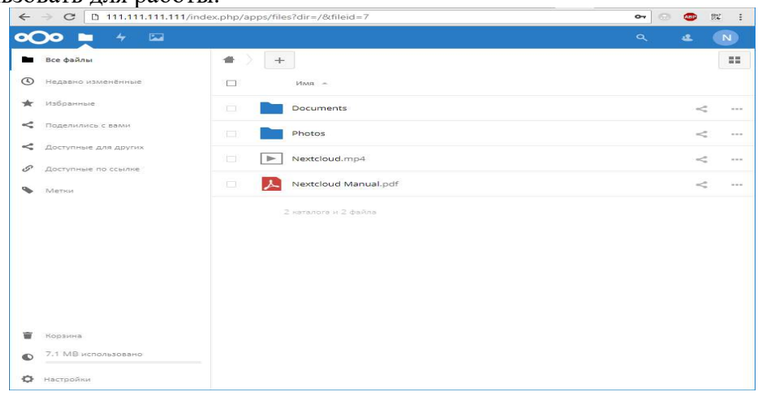
Измените имя домена на ccna.com

Подключение к хранилищу в браузере

Для подключения в браузере просто используйте ваш ip-адрес. При первом подключении к хранилищу необходимо создать учетную запись администратора, введите имя администратора и безопасный пароль. Нажмите **Завершить установку**.

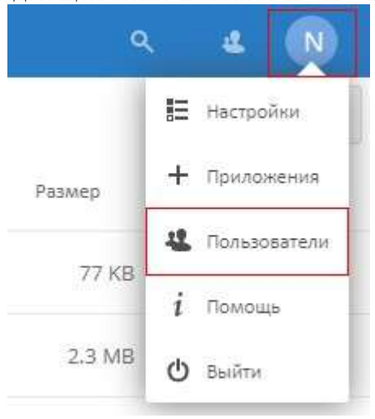


Далее перед Вами откроется интуитивный интерфейс с файлами и каталогами, который уже можно использовать для работы.



Создание пользователя

Для создания нового пользователя хранилища на главной странице в правом верхнем углу кликните вашу иконку и в выпадающем меню нажмите **Пользователи**.



иначе вы можете **потерять важную информацию**, поскольку некоторые типы массивов не переживут поломку еще одного накопителя (например, RAID-5).

Но как узнать, что диск вышел из строя и определить какой именно диск сломался?

В случае поломки любого из дисков вы заметите сильное **снижение производительности**.

№3 Установка NextCloud на Linux

Установка

В нашем примере установка производится на Ubuntu 16, на других дистрибутивах некоторые команды могут отличаться, но процедура остается прежней. Скачайте с помощью утилиты wget архив с последней версией продукта, на момент написания статьи последняя версия - 13.0.4, актуальную версию можно посмотреть на официальном сайте:

wget https://download.nextcloud.com/server/releases/nextcloud-13.0.4.tar.bz2

Также скачайте файл с контрольной суммой, или md5, или SHA256:

wget https://download.nextcloud.com/server/releases/nextcloud-13.0.4.tar.bz2.md5 И, наконец, загрузите цифровые подписи:

wget https://download.nextcloud.com/server/releases/nextcloud-13.0.4.tar.bz2.asc wget https://nextcloud.com/nextcloud.asc

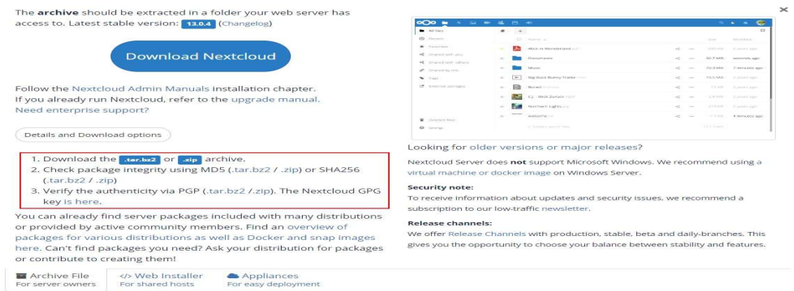
Проверьте контрольную сумму MD5 или SHA256:

md5sum -c nextcloud-13.0.4.tar.bz2.md5 < nextcloud-13.0.4.tar.bz2 sha256sum -c nextcloud-13.0.4.tar.bz2.sha256 < nextcloud-13.0.4.tar.bz2 В результате вы должны увидеть подобное сообщение:

nextcloud-13.0.4.tar.bz2: OK Проверьте цифровые подписи:

gpg --import nextcloud.asc

gpg --verify nextcloud-13.0.4.tar.bz2.asc nextcloud-13.0.4.tar.bz2 Разархивируйте скачанный архив:



tar -xjf nextcloud-13.0.4.tar.bz2 Скопируйте каталог на веб сервер:

cp -r nextcloud /var/www

Конфигурация веб-сервера Apache

Создайте с помощью текстового редактора vi конфигурационный файл и откройте его: vi /etc/apache2/sites-available/nextcloud.conf

Внесите следующие строки:

Alias /nextcloud "/var/www/nextcloud/" <Directory /var/www/nextcloud/> Options +FollowSymlinks AllowOverride All <IfModule mod_dav.c> Dav off </IfModule> SetEnv HOME /var/www/nextcloud SetEnv HTTP_HOME /var/www/nextcloud </Directory>

Примечание: у вас могут отличаться пути до каталога.

Далее создайте символьную ссылку:

ln -s /etc/apache2/sites-available/nextcloud.conf /etc/apache2/sites-enabled/nextcloud.conf Для корректной работы Nextcloud необходимо запустить следующие модули: a2enmod rewrite

a2enmod headers a2enmod env a2enmod dir a2enmod mime a2enmod setenvif

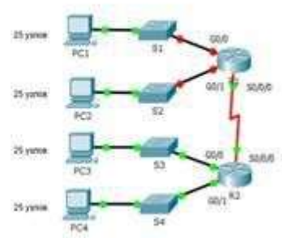
Также необходимо изменить права владения:

chown -R www-data:www-data /var/www/nextcloud/

Чтобы изменения вступили в силу перезапустите веб-сервер:

service apache2 restart

Топология



Создайте ключ RSA длиной 1024 бит.

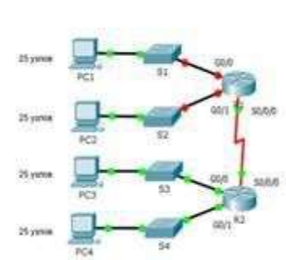
Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin с 15-м уровнем привилегированного доступа и зашифрованным паролем Adminp@ss.

3. Разбейте сеть на подсети

Топология



Разбейте сеть 192.168.0.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

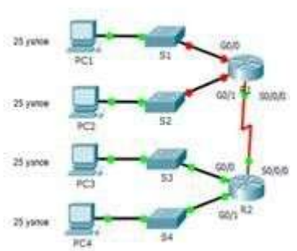
Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам. Последний из используемых IP-адресов назначьте узлам.

4. Выполните базовую настройку устройств S1, R1, R2

Топология



а. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

д. Назначьте cisco в качестве пароля VTY и включите вход по паролю. е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа (Используйте слово Warninng).

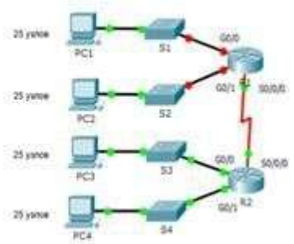
з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

5. Настроите доступ по протоколу SSH на S1 и R2.

Измените имя домена на ccna.com

Создайте ключ RSA длиной 1024 бит.

Топология



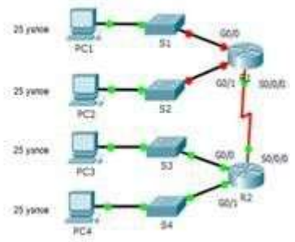
Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin1 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin1p@ss.

6. Разбейте сеть на подсети

Топология



Разбейте сеть 192.168.10.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

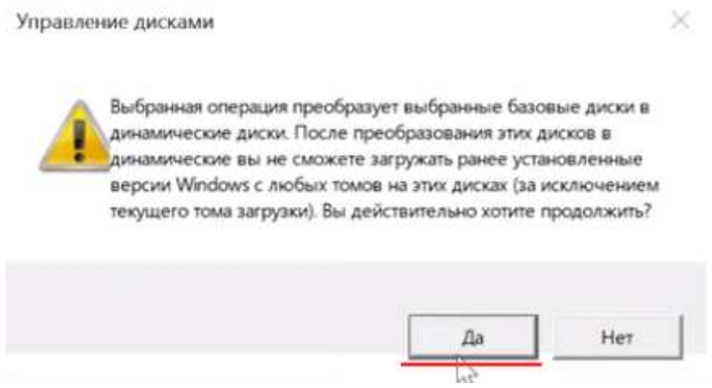
e. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

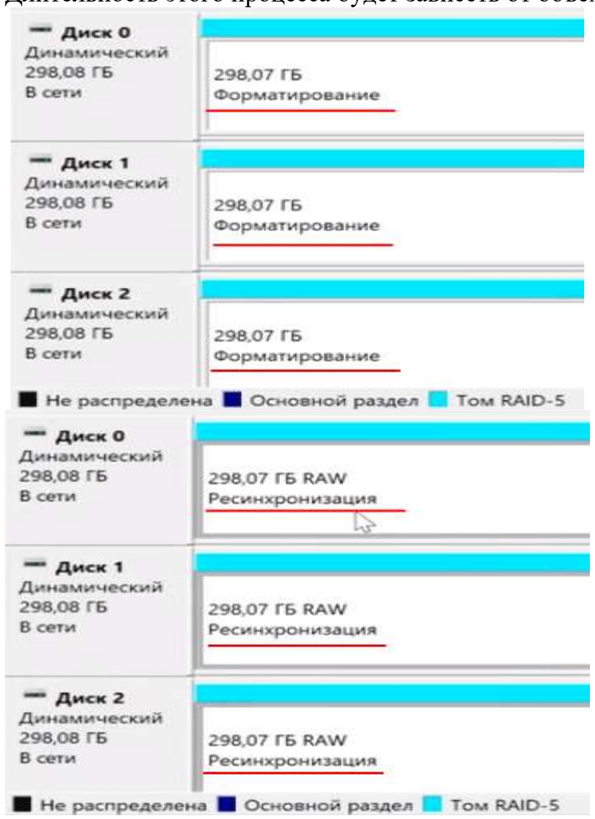
Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам. Последний из используемых IP-адресов назначьте узлам.

7. Выполните базовую настройку устройств S1, R1, R2



После этого запустится процесс **форматирования** и **ресинхронизации** всех дисков. Длительность этого процесса будет зависеть от объема ваших дисков и мощности сервера.



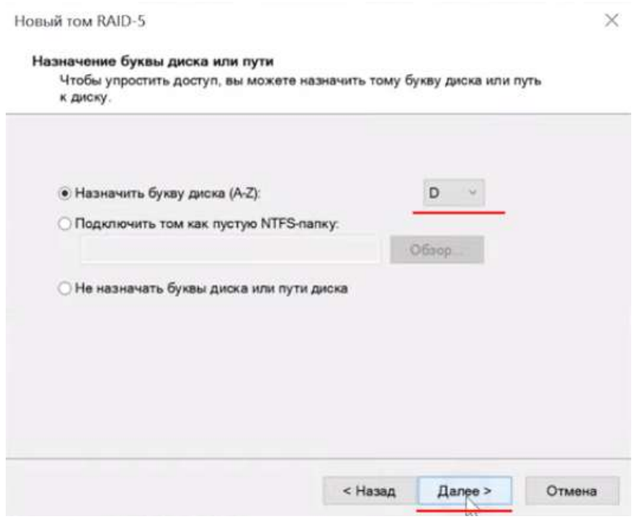
По окончании этих процессов вы получите новый **RAID-5 массив**, с которым можно будет работать как с обычным диском. Теперь можно отключить графический интерфейс и работать с сервером удаленно или через терминал.

Стоит также отметить, что при помощи этого способа можно создать также **RAID 0** (страйпинг), **RAID 1** (зеркалирование) и **JBOD** (объединение всех дисков в один большой без чередования или зеркалирования). Для этого на втором шаге выберите нужную вам опцию:

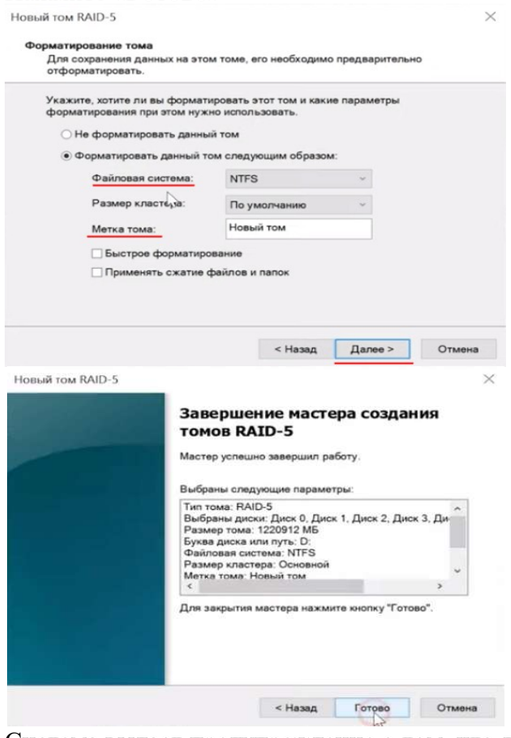
- **Добавить составной том** – для создания **JBOD**;
- **Добавить чередующийся том** – для создания массива **RAID 0**;
- **Создать зеркальный том** – для создания массива **RAID 1**;

Как определить вышедший из строя диск и заменить его в Windows Server?

Использование RAID массивов позволяет сохранить данные в случае поломки одного из накопителей. Однако, если любой из дисков вышел из строя – следует немедленно заменить его,

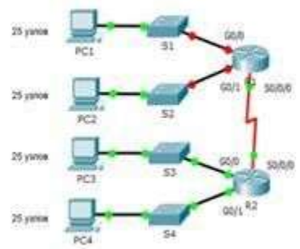


Шаг 5: Теперь выберите **файловую систему** и **имя массива**. Подтвердите действием нажатием кнопки «**Далее**». Мастер создания тома **RAID-5** покажет вам все параметры будущего массива. Нажмите «**Готово**»



Система выдаст предупреждение о том, что диски будут переконвертированы в динамические и что вся **информация будет удалена**. Подтвердите запуск конвертирования нажатием кнопки «**Да**»

Топология



а. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

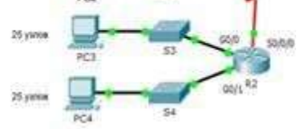
д. Назначьте cisco в качестве пароля VTY и включите вход по паролю. е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

8. Настроите доступ по протоколу SSH на S1 и R2.

Топология



Измените имя домена на ccna.com Создайте ключ RSA длиной 1024 бит.

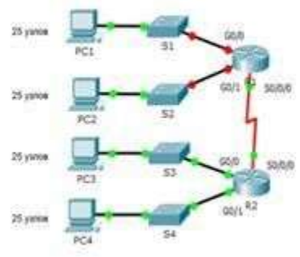
Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin2 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin2p@ss.

9. Разбейте сеть на подсети

Топология



Разбейте сеть 192.168.1.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу

GigabitEthernet 0/1 маршрутизатора R1.

е. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

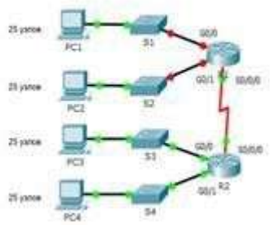
Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам. Последний из используемых IP-адресов назначьте узлам.

10. Выполните базовую настройку устройств S1, R1, R2

Топология



а. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

д. Назначьте cisco в качестве пароля VTY и включите вход по паролю. е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

11. Настроите доступ по протоколу SSH на S1 и R2.

Измените имя домена на ccna.com Создайте ключ RSA длиной 1024 бит.

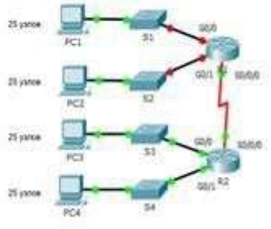
Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin3 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin3p@ss.

12. Разбейте сеть на подсети

Топология

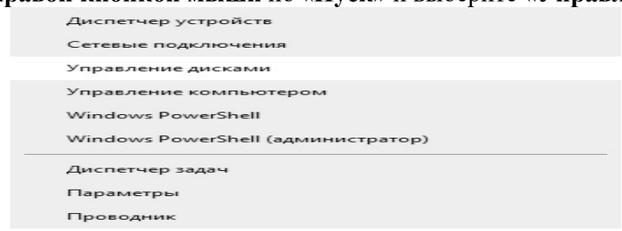


Разбейте сеть 192.168.3.0/24 на нужное количество подсетей:

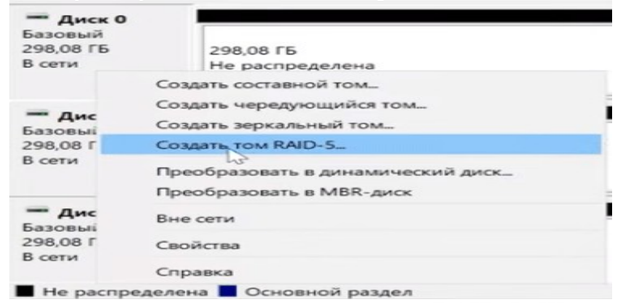
а. Назначьте подсеть 0 локальной сети (LAN1), подключенной к интерфейсу

как вы отключите графический интерфейс вашего сервера. Процесс создания массива прост и выглядит так же, как и в Windows 10. Для примера, создадим RAID 5 в Windows Server, предварительно подключив к нему все диски из которых будет состоять наш массив. Для **создания RAID 5 в Windows Server** следует:

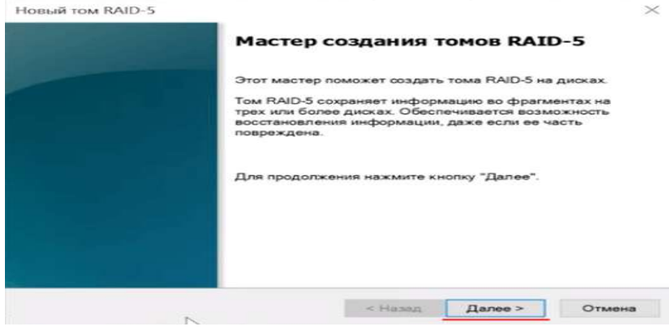
Шаг 1: Щелкните **правой кнопкой мыши** по «**Пуск**» и выберите «**Управление дисками**»



Шаг 2: В менеджере дисков будут отображаться все подключенные диски. Щелкните **правой кнопкой мыши** по одному из нужных дисков и выберите «**Создать том RAID-5**»



Шаг 3: Перед вами откроется **мастер создания томов RAID-5**. Щелкните «**Далее**», затем добавьте диски в массив используя кнопку «**Добавить**» и снова нажмите «**Далее**»



Шаг 4: Выберите **букву** для вашего массива и нажмите «**Далее**»

B XOR C Таким образом, значение P будет равно результату операции XOR между данными на дисках A, B и C.

При чтении данных с дисков A, B и C RAID-контроллер может использовать блок четности (P) для восстановления данных на отказавшем диске. Например, при отказе диска B RAID-контроллер использует данные на дисках A, C и P для восстановления данных, хранившихся на диске B. Но для такого RAID-массива нам необходимо как минимум три диска.

Установка

После того как выбор RAID-системы сделан, необходимо обновить и установить системные пакеты на нашей машине для их корректной работы:

apt update && apt upgrade -y Копировать

Если на диске имеются важные данные, создайте их резервную копию с помощью приведенной ниже команды:

tar -czvf backup.tar.gz /etc && scp backup.tar.gz root@65.44.32.1:/etc/backup/ Копировать

Необходимо изменить IP-адрес на IP вашей машины. Проверьте, установлен ли в вашем дистрибутиве Linux пакет для работы с RAID. В большинстве случаев это будет пакет **mdadm**. Установить его можно с помощью менеджера пакетов вашего дистрибутива (например, apt, yum, dnf). В нашем примере мы будем использовать пакетный менеджер apt, в вашем случае используйте его в соответствии с вашей ОС. Если вы забыли метку диска, необходимо набрать:

lsblk Копировать

После этого установите необходимое программное обеспечение, в нашей инструкции это будет

mdadm, которое позволяет создать программную RAID-систему для диска в Linux: apt install mdadm

Копировать

Теперь мы можем использовать **mdadm** для создания массива, выберем **RAID 1**, создадим виртуальное устройство контроллера и укажем необходимые диски для использования.

Важно отметить! В зависимости от архитектуры вашей сети вам необходимо решить. Будете ли вы использовать загрузочный диск ОС в RAID-системе или нет. Если ответ положительный, то необходимо убедиться, что загрузчик поддерживает версию md. Создадим массив командой, приведенной ниже:

sudo mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sdc /dev/sdb Копировать

В утилите **mdadm** — это основная синтаксическая команда, опция **–create** позволяет создать массив,

/dev/mdo –level=1 устройство RAID 1, **–raid-devices=2 /dev/sdc /dev/sdb** в этой части мы указываем два используемых диска для нашего массива.

Проверим состояние процесса с помощью следующей команды:

cat /proc/mdstat Копировать

Скриншот №7 — Проверка массива

Для нашего массива необходимо создать единую файловую систему для всех дисков, мы будем использовать ext4 для наших целей:

sudo mkfs.ext4 /dev/md0 Копировать

Смонтируем RAID-систему в точку файловой системы:

sudo mkdir /mnt/md sudo mount /dev/md0 /mnt/md Копировать

Добавьте RAID-систему в автозагрузку при старте, после чего откройте nano командой ниже и поставьте Tab в красное поле:

echo "/dev/md0 /mnt/md ext4 defaults 0 0" >> /etc/fstab

Копировать nano /etc/fstab Копировать

После этого перезагрузим службу:

systemctl daemon-reload Копировать

И введем команду, чтобы убедиться в корректности работы файловой системы и RAID: lsblk Копировать

№2 Установка Raid на windows server

в Windows Server можно создать RAID массив, который обеспечит сохранность данных в случае выхода из строя одного из дисков. Создавать программный RAID рекомендуется перед тем,

GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

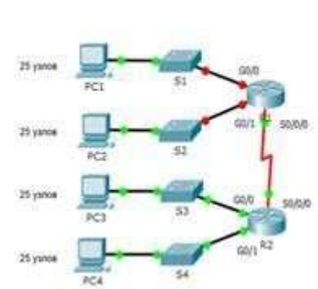
Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам. Последний из используемых IP-адресов назначьте узлам.

13. Выполните базовую настройку устройств S1, R1, R2

Топология



a. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

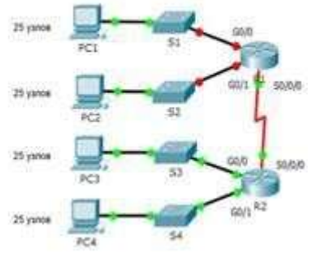
д. Назначьте cisco в качестве пароля VTY и включите вход по паролю. е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

14. Настройте доступ по протоколу SSH на S1 и R2.

Топология



Измените имя домена на ccna.com Создайте ключ RSA длиной 1024 бит.

Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin4 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin4p@ss.

3. Разбейте сеть на подсети

Разбейте сеть 192.168.0.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 3 каналу WAN между маршрутизаторами R1 и R2.

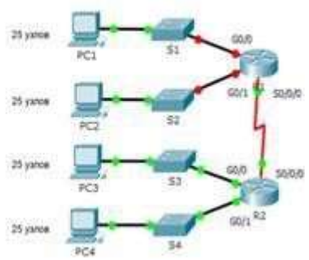
Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам. Последний из используемых IP-адресов назначьте узлам.

15. Выполните базовую настройку устройств S1, R1, R2

Топология



a. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

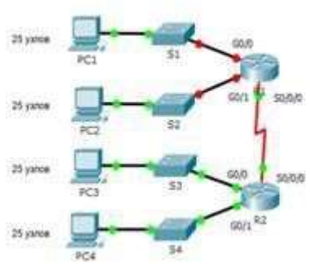
д. Назначьте cisco в качестве пароля VTY и включите вход по паролю. е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

16. Настроите доступ по протоколу SSH на S1 и R2.

Топология



Измените имя домена на ccna.com Создайте ключ RSA длиной 1024 бит.

Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

- Монтирование RAID-массива: настройка автоматического монтирования RAID-массива при загрузке системы;
- Тестирование и проверка: проверка правильности конфигурации RAID-массива и его работоспособности путем создания, записи и чтения тестовых данных.

Требования

- Root—права;
- Debian 11 или более поздняя версия;
- Некоторые знания о работе ОС;
- Подключение к Интернету.

VPS сервер с Debian от 430 ₽/месСоздайте виртуальный сервер на Debian 11/12 за 1 минуту

Добавим диск

В зависимости от инфраструктуры выберите способ подключения диска в систему. Для физической машины — подключиться к свободному порту, для виртуальной машины — заглянуть на вкладку гипервизора и добавить текущий или целевой диск, в другом случае, если вы выбрали VPS—сервер Serverspace, вы можете добавить необходимое пространство через главную панель:

Выберите облачные технологии и серверы, затем выберите вкладку Настройки и прокрутите страницу до появления томов, затем нажмите кнопку Добавить:

Во всплывающем окне выберите необходимое дисковое пространство, установите флажок и перезапустите сервер по кнопке ниже, после чего убедитесь, что диск подключен. В терминале введите команду:

lsblk Копировать

Итак, два диска в системе есть и они подключены. На следующем шаге необходимо выбрать формат RAID.

RAID схемы

В различных связках, комбинациях и архитектурах выделяют несколько современных RAID—схем для использования:

RAID 0

Представляет собой базовый метод передачи данных путем чередования блоков информации между двумя или более дисками. При этом целые данные делятся на части, что повышает пропускную способность за счет использования нескольких дисков вместо одного накопителя. Однако в этом случае возникает существенная проблема: отсутствие отказоустойчивости. Если хотя бы один диск будет поврежден, то все данные превратятся в мусор. Эта простая система используется для временного хранения данных и систем с требованиями быстрого чтения и записи информации.

RAID 1

Представляет собой основной метод передачи данных путем зеркалирования и синхронизации информации между двумя или более дисками. При этом все данные копируются на другое хранилище. При этом работает параметр отказоустойчивости и сохранения данных системы при повреждении одного из дисков, но отсутствует быстрая скорость записи данных по сравнению с

RAID 5

Эти решения являются компромиссом между скоростью ввода-вывода и отказоустойчивостью в RAID-системе. Целостность данных будет возможна благодаря алгоритму блоков четности, которые сохраняют данные более надежно.

Процесс вычисления блоков четности зависит от уровня RAID и используемого алгоритма четности. Рассмотрим процессы вычисления блоков четности для RAID 5 и RAID 6, которые являются наиболее распространенными уровнями RAID, использующими блоки четности.

Предположим, у нас есть 4 диска A, B, C и P (где P — диск четности), и мы хотим записать данные на диски A, B и C. Для вычисления блока четности для данных, которые мы хотим записать на диски A, B и C, используется операция XOR (исключающее ИЛИ) над данными на этих дисках.

Пример:

Допустим, у нас есть данные 10101010, которые необходимо записать на диски A, B и C. Тогда процесс вычисления блока четности (P) будет выглядеть следующим образом: **P = A XOR**

- lastName
- displayName
- userName

Если у пользователя нет этих атрибутов, процесс будет завершаться следующей ошибкой

```
ERROR: StatusCode: BadRequest

Message: Processing of the HTTP request resulted in an exception. Please see the HTTP response returned by the 'Response' property of this exception for details.
Web Response:
{"schema":["urn:ietf:params:scim:api:messages:2.0:Error"],"detail":"Request is unparsable, syntactically incorrect, or violates schema.","status":"400",
```

Многозначные атрибуты

AWS не поддерживает следующие многозначные атрибуты:

- эл. почта
- номера телефонов;

При попытке передать многозначные значения для таких атрибутов будет возникать следующее сообщение об ошибке:

```
ERROR: StatusCode: BadRequest

Message: Processing of the HTTP request resulted in an exception. Please see the HTTP response returned by the 'Response' property of this exception for details.
Web Response:
{"schema":["urn:ietf:params:scim:api:messages:2.0:Error"],"detail":"Request is unparsable, syntactically incorrect, or violates schema.","status":"400",
```

Эту ситуацию можно решить двумя способами

1. Убедитесь, что у пользователя есть только одно значение для атрибутов номера телефона и адреса электронной почты.
2. Удалите дублирующиеся значения этих атрибутов. Например, наличие двух различных атрибутов, сопоставленных с идентификатором Microsoft Entra ID, сопоставленным с "phoneNumber_" на стороне AWS, приведет к ошибке, если оба атрибута имеют значения в идентификаторе Microsoft Entra. Такую ошибку можно устранить, только ограничив сопоставление поля "phoneNumber_" одним атрибутом.

Недопустимые знаки

В настоящее время Центр удостоверений AWS IAM не позволяет использовать некоторые другие символы, поддерживаемые идентификатором Microsoft Entra, например tab (\t), новой строкой (\n), возвращаемой каретки (\r) и символами, такими как " <||>;|:%".

Дополнительные советы по устранению неполадок с AWS IAM Identity Center см. здесь.

Дополнительные ресурсы

- Управление подготовкой учетных записей пользователей для корпоративных приложений
- Что такое доступ к приложениям и Центр удостоверений IAM с идентификатором Microsoft Entra?

Следующие шаги

- Сведения о просмотре журналов и получении отчетов о действиях по подготовке

МДК.04.03 Технологии хранения и анализа данных

№1 Установка Raid на linux

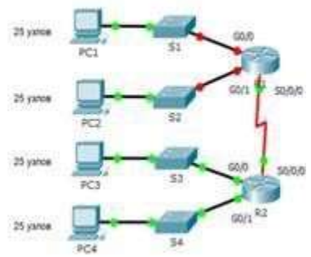
Конфигурирование RAID-массива включает в себя несколько основных этапов:

- Подготовка дисков: обеспечение доступности и подготовка физических дисков, которые будут использоваться в RAID-массиве. Диски могут быть новыми или содержать данные, которые необходимо сохранить;
- Выбор уровня RAID: определение оптимального уровня RAID-массива в соответствии с требованиями системы. Например, RAID 1 для обеспечения отказоустойчивости данных, RAID 0 для повышения производительности или RAID 5/6 для достижения баланса между отказоустойчивостью и производительностью;
- Создание массива RAID: использование утилиты mdadm (Multiple Device Administration) для создания логического RAID-массива на основе выбранного уровня RAID и физических дисков;
- Конфигурирование файловой системы: форматирование RAID-массива с использованием выбранной файловой системы для хранения данных;

Создайте пользователя admin5 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin5p@ss.

17. Разбейте сеть на подсети

Топология



Разбейте сеть 192.168.12.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 3 каналу WAN между маршрутизаторами R1 и R2.

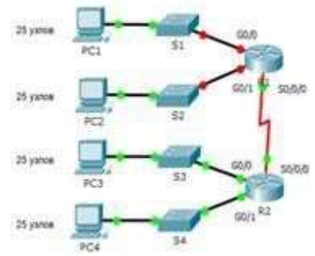
Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам. Последний из используемых IP-адресов назначьте узлам.

18. Выполните базовую настройку устройств S1, R1, R2

Топология



а. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

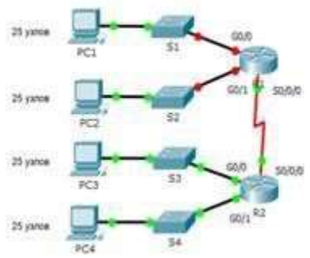
д. Назначьте cisco в качестве пароля VTY и включите вход по паролю. е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

19.Настройте доступ по протоколу SSH на S1 и R2.

Топология



Измените имя домена на ccna.com Создайте ключ RSA длиной 1024 бит.

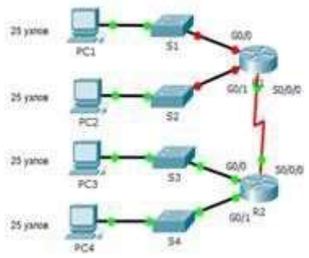
Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin6 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin6p@ss.

20.Разбейте сеть на подсети

Топология



Разбейте сеть 172.16.6.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

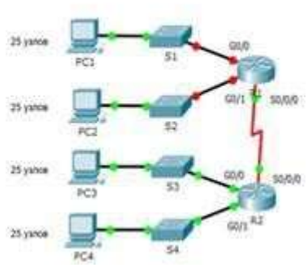
Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам. Последний из используемых IP-адресов назначьте узлам.

21. Выполните базовую настройку устройств S1, R1, R2

Топология



a. Подключитесь с помощью консоли и активируйте привилегированный режим

JIT-доступ к приложению с помощью PIM для групп

С помощью PIM для групп вы можете предоставить JIT-доступ к группам в Amazon Web Services и сократить количество пользователей, имеющих постоянный доступ к привилегированным группам в AWS.

Настройка корпоративного приложения для единого входа и подготовки

1. Добавьте центр удостоверений AWS IAM в клиент, настройте его для подготовки, как описано в приведенном выше руководстве, и запустите подготовку.
2. Настройка единого входа в AWS IAM Identity Center.
3. Создайте группу, которая предоставит всем пользователям доступ к приложению.
4. Назначьте группу приложению Центра удостоверений AWS.
5. Назначьте тестового пользователя в качестве прямого члена группы, созданной на предыдущем шаге, или предоставьте им доступ к группе через пакет доступа. Эту группу можно использовать для постоянного, неадминистрационного доступа в AWS.

Включение PIM для групп

1. Создайте вторую группу в идентификаторе Microsoft Entra. Эта группа предоставит доступ к разрешениям администратора в AWS.
2. Доведите группу под управлением в Microsoft Entra PIM.
3. Назначьте тестового пользователя право на группу в PIM с набором ролей участником.
4. Назначьте вторую группу приложению Центра удостоверений AWS IAM.
5. Используйте подготовку по запросу для создания группы в Центре удостоверений AWS IAM.
6. Войдите в Центр удостоверений AWS IAM и назначьте вторую группу необходимых разрешений для выполнения задач администратора.

Теперь любой конечный пользователь, который был разрешен для группы в PIM, может получить JIT-доступ к группе в AWS, активировав членство в группе.

Основные рекомендации

- Сколько времени требуется для подготовки пользователя к приложению?:

○ Когда пользователь добавляется в группу в идентификаторе Microsoft Entra ID за пределами активации членства в группе с помощью идентификатора Microsoft Entra ID управление привилегированными пользователями (PIM):

▪ Членство в группе подготавливается в приложении во время следующего цикла синхронизации. Цикл синхронизации выполняется каждые 40 минут.

○ Когда пользователь активирует членство в группе в PIM идентификатора Microsoft Entra ID:

▪ Членство в группе подготавливается в течение 2–10 минут. При наличии высокой частоты запросов в один раз запросы регулируются с частотой 5 запросов в 10 секунд.

▪ Для первых пяти пользователей в течение 10-секундного периода активации членства в группе для определенного приложения членство в группах подготавливается в приложении в течение 2–10 минут.

▪ Для шестого пользователя и выше в течение 10-секундного периода активации членства в группе для определенного приложения членство в группе подготавливается к приложению в следующем цикле синхронизации. Цикл синхронизации выполняется каждые 40 минут. Ограничения регулирования относятся к корпоративному приложению.

• Если пользователю не удается получить доступ к необходимой группе в AWS, просмотрите приведенные ниже советы по устранению неполадок, журналы PIM и журналы подготовки, чтобы убедиться, что членство в группе было успешно обновлено. В зависимости от того, как было разработано целевое приложение, может потребоваться дополнительное время для вступления в силу членства в группе в приложении.

• Вы можете создавать оповещения о сбоях с помощью Azure Monitor.

• Деактивация выполняется во время регулярного добавочного цикла. Он не обрабатывается немедленно с помощью подготовки по запросу.

Советы по устранению неполадок Отсутствующие атрибуты

При подготовке пользователя в AWS они должны иметь следующие атрибуты.

- firstName

urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:division	Строка
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:costCenter	Строка
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:organization	Строка
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:manager	Справочные материалы

В разделе "Сопоставления" выберите **"Синхронизировать группы Microsoft Entra" с Центром**

удостоверений AWS IAM.

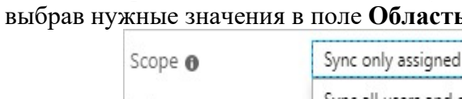
Просмотрите атрибуты группы, синхронизированные с идентификатором Microsoft Entra с ЦЕНТРОМ удостоверений AWS IAM, в **разделе "Сопоставление** атрибутов". Атрибуты, выбранные как свойства с меткой **Сопоставление**, используются для сопоставления групп в AWS IAM Identity Center при операциях обновления. Нажмите кнопку **Сохранить**, чтобы зафиксировать все изменения.

12.

Атрибут	**Тип**	**Поддерживается для фильтрации**
displayName	Строка	✓
externalId	Строка	
members	Справочные материалы	

13. Чтобы настроить фильтры области, ознакомьтесь со следующими инструкциями, предоставленными в руководстве по фильтрам области.

14. Чтобы включить службу подготовки Microsoft Entra для Центра удостоверений AWS IAM, измените **состояние** подготовки на **"Включено"** в **разделе Параметры**.



15. Определите пользователей и (или) группы для подготовки в AWS IAM Identity Center, выбрав нужные значения в поле **Область** в разделе **Параметры**.

16. Когда будете готовы выполнить подготовку, нажмите кнопку **Сохранить**.

После этого начнется цикл начальной синхронизации всех пользователей и групп, определенных в поле **Область** в разделе **Параметры**. Начальный цикл занимает больше времени, чем последующие циклы, которые происходят примерно каждые 40 минут до запуска службы подготовки Microsoft Entra.

Шаг 6. Мониторинг развертывания

После настройки подготовки используйте следующие ресурсы для мониторинга развертывания:

1. Используйте журналы подготовки, чтобы определить, какие пользователи были подготовлены успешно или неудачно

2. Используйте индикатор выполнения, чтобы узнать состояние цикла подготовки и приблизительное время до его завершения.

3. Если конфигурация подготовки находится в неработоспособном состоянии, приложение перейдет в режим карантина. Дополнительные сведения о режимах карантина см. здесь.

EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

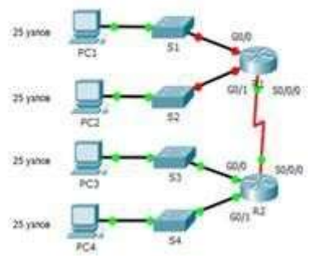
д. Назначьте cisco в качестве пароля VTY и включите вход по паролю. е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

22. Настройте доступ по протоколу SSH на S1 и R2.

Топология



Измените имя домена на ccna.com Создайте ключ RSA длиной 1024 бит.

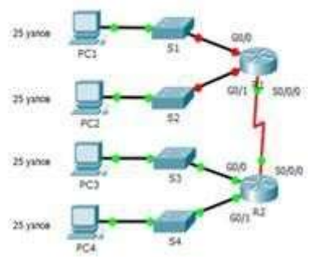
Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin7 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin7p@ss.

23. Разбейте сеть на подсети

Топология



Разбейте сеть 192.168.7.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

е. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

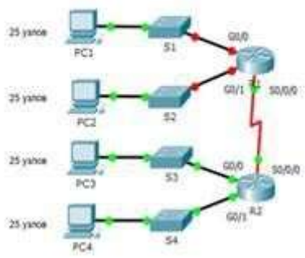
Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам. Последний из используемых IP-адресов назначьте узлам.

24. **Выполните базовую настройку устройств S1, R1, R2**

Топология



a. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

д. Назначьте cisco в качестве пароля VTY и включите вход по паролю. е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

2. Настройте доступ по протоколу SSH на S1 и R2. Измените имя домена на ccna.com

Создайте ключ RSA длиной 1024 бит.

Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin8 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin8p@ss.

25. Разбейте сеть на подсети

Разбейте сеть 192.168.8.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

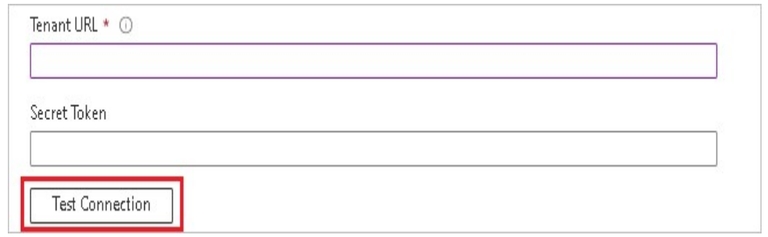
e. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам. Последний из используемых IP-адресов назначьте узлам.

26. Выполните базовую настройку устройств S1, R1, R2



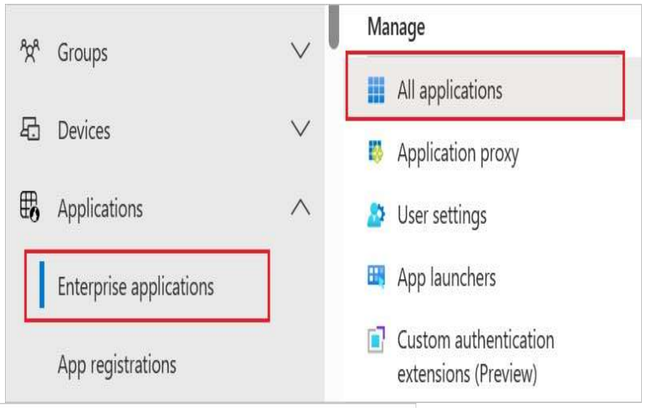
7. В поле **Электронная почта для уведомлений** введите адрес электронной почты пользователя или группы, которые должны получать уведомления об ошибках подготовки, а также установите флажок **Отправить уведомление по электронной почте при сбое**.

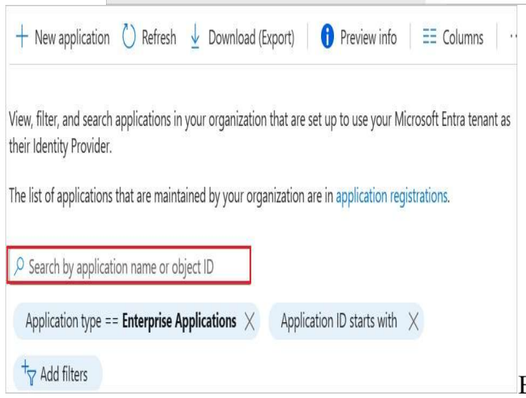
8. Выберите **Сохранить**.

9. **В разделе "Сопоставления"** выберите **"Синхронизировать пользователей Microsoft Entra" с ЦЕНТРОМ** удостоверений AWS IAM.

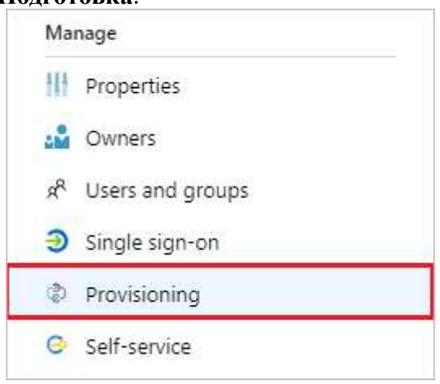
10. Просмотрите атрибуты пользователя, синхронизированные с идентификатором Microsoft Entra с ЦЕНТРОМ удостоверений AWS IAM, в **разделе "Сопоставление** атрибутов". Атрибуты, выбранные как **соответствующие** свойства, используются для сопоставления учетных записей пользователей в AWS IAM Identity Center при операциях обновления. Если вы решили изменить соответствующий целевой атрибут, необходимо убедиться, что API Центра удостоверений AWS IAM поддерживает фильтрацию пользователей на основе этого атрибута. Нажмите кнопку **Сохранить**, чтобы зафиксировать все изменения.

Атрибут	**Тип**	**Поддерживается для фильтрации**
userName	Строка	✓
active	Логический	
displayName	Строка	
title	Строка	
emails[type eq "work"].value	Строка	
preferredLanguage	Строка	
name.givenName	Строка	
name.familyName	Строка	
name.formatted	Строка	
addresses[type eq "work"].formatted	Строка	
addresses[type eq "work"].streetAddress	Строка	
addresses[type eq "work"].locality	Строка	
addresses[type eq "work"].region	Строка	
addresses[type eq "work"].postalCode	Строка	
addresses[type eq "work"].country	Строка	
phoneNumbers[type eq "work"].value	Строка	
externalId	Строка	
локаль	Строка	
timezone	Строка	
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:employeeNu mber	Строка	
urn:ietf:params:scim:schemas:extension:enterprise:2.0:User:department	Строка	





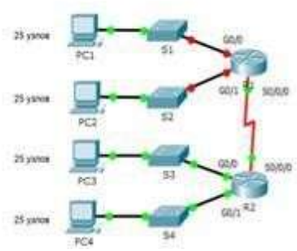
3. В списке приложений выберите **AWS IAM Identity Center**.
4. Выберите вкладку **Подготовка**.



5. Для параметра **Режим подготовки к работе** выберите значение **Automatic** (Автоматически).

6. В разделе **Учетные данные администратора** укажите **URL-адрес клиента** для AWS IAM Identity Center и **секретный токен**, полученный ранее на шаге 2. Нажмите кнопку **"Тестировать Подключение"**, чтобы убедиться, что идентификатор Microsoft Entra может подключиться к Центру удостоверений AWS IAM.

Топология



a. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

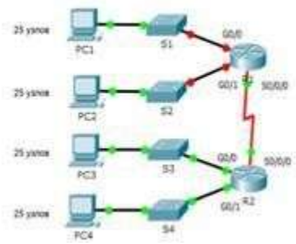
д. Назначьте cisco в качестве пароля VTY и включите вход по паролю. е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

27. Настройте доступ по протоколу SSH на S1 и R2.

Топология



Измените имя домена на ccna.com Создайте ключ RSA длиной 1024 бит.

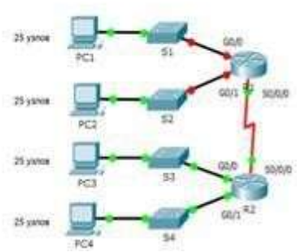
Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin9 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin9p@ss.

28. Разбейте сеть на подсети

Топология



Разбейте сеть 192.168.9.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

е. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

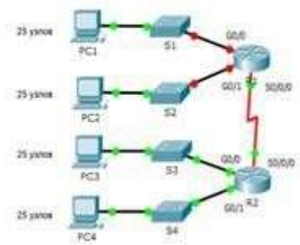
Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам. Последний из используемых IP-адресов назначьте узлам.

29. Выполните базовую настройку устройств S1, R1, R2

Топология



а. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

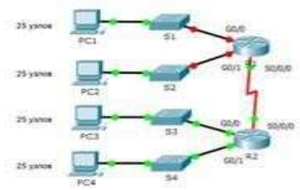
д. Назначьте cisco в качестве пароля VTY и включите вход по паролю. е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

30. Настройте доступ по протоколу SSH на S1 и R2.

Топология



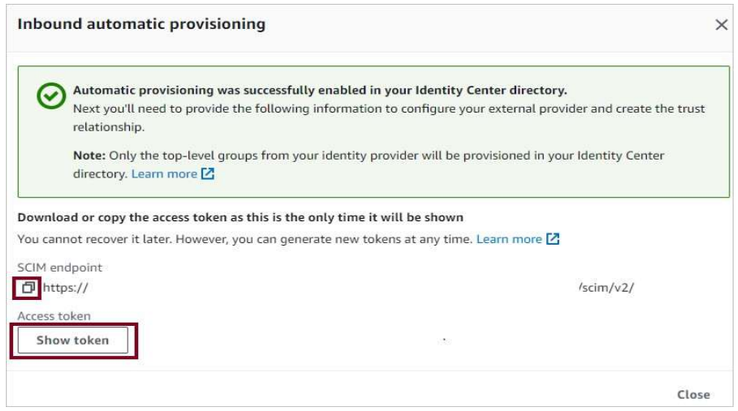
Измените имя домена на ccna.com Создайте ключ RSA длиной 1024 бит.

Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin10 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin10p@ss.

31. Разбейте сеть на подсети



Шаг 3. Добавление Центра удостоверений AWS IAM из коллекции приложений Microsoft Entra Добавьте Центр удостоверений AWS IAM из коллекции приложений Microsoft Entra, чтобы начать управление подготовкой в Центре удостоверений AWS IAM. Если вы ранее настроили AWS IAM Identity Center для единого входа, вы можете использовать то же приложение. Дополнительные сведения о добавлении приложения из коллекции см. здесь.

Шаг 4. Определение того, кто находится в область для подготовки

Служба подготовки Microsoft Entra позволяет область, которые подготавливаются на основе назначения приложению и на основе атрибутов пользователя или группы. Если вы решили область, которые подготовлены к приложению на основе назначения, можно выполнить следующие действия, чтобы назначить пользователей и группы приложению. Если вы решили область, кто подготовлен исключительно на основе атрибутов пользователя или группы, можно использовать фильтр области, как описано здесь.

• Начните с малого. Протестируйте небольшой набор пользователей и групп, прежде чем выполнять развертывание для всех. Если в область подготовки включены назначенные пользователи и группы, проверьте этот механизм, назначив приложению одного или двух пользователей либо одну или две группы. Если в область включены все пользователи и группы, можно указать фильтр области на основе атрибутов.

• Если требуются дополнительные роли, можно обновить манифест приложения, чтобы добавить новые роли.

Шаг 5. Настройка автоматической подготовки пользователей в Центре удостоверений AWS IAM

В этом разделе описаны инструкции по настройке службы подготовки Microsoft Entra для создания, обновления и отключения пользователей и групп в TestApp на основе назначений пользователей и (или) групп в идентификаторе Microsoft Entra.

Чтобы настроить автоматическую подготовку пользователей для Центра удостоверений AWS IAM в идентификаторе Microsoft Entra ID:

1. Войдите в Центр администрирования Microsoft Entra как минимум облачные приложения Администратор istrator.
2. **Обзор корпоративных приложений>удостоверений>**

образа системы.

Система попытается просканировать диски сервера на наличие полных резервных копий ОС. Будет предложен последний доступный образ восстановления. Но вы можете выбрать из списка, если их несколько**(Select a system image**):

2. Нажмите кнопку Далее и попадете в меню дополнительных параметров:

Важно! Если выбрать опцию Форматировать и переразметить диски, утилита переформатирует диски и разделы на сервере, чтобы повторить разделы из резервной копии. Если этот параметр не включен, утилита восстановления удалит и заменит данные только в системном разделе, где установлена ОС. Кнопка **Исключить диски...** при включенной опции Форматировать и переразметить диски позволит исключить диски из процесса переформатирования.

3. Диски и разделы, затронутые восстановлением, будут перечислены в следующем окне:

4. Нажмите кнопку **Finish** и дождитесь завершения восстановления.Восстановление отдельных папок, разделов или состояния системы

Эта функция доступна в графическом интерфейсе компонента Windows Server Backup.

1. Запустите компонент резервного копирования: **Пуск - Диспетчер сервера - Инструменты -**

Резервное копирование Windows Server и выберите **Восстановление ...**.

2. Выберите, где будет находиться резервная копия - локально на сервере или в другом месте, например, на сетевом хранилище. В примере рассматривается вариант с резервной копией на сетевом диске (Remote Shared Folder), выберите второй пункт:

3. Введите адрес сетевого хранилища:

4. Выберите дату и время требуемого резервного копирования:

5. Далее выберите **тип восстановления** (на скриншоте приведено описание каждой опции). В примере восстановим **Файлы и папки**:

6. Выберем восстановление файлов рабочего стола:

7. Настроим параметры восстановления:

8. Проверяем и нажимаем **Восстановить**

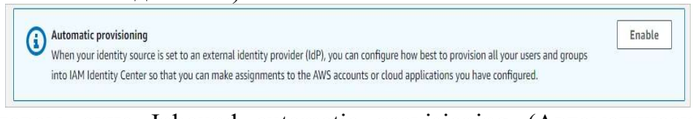
Дожидаемся завершения и выходим из утилиты. **Другие типы восстановления работают аналогичным образом.**

№19 Настройка системы идентификации (IAM) Шаг 1. Планирование развертывания подготовки

1. Узнайте, как работает служба подготовки.
2. Определите, кто находится в область для подготовки.
3. Определите, какие данные необходимо сопоставить между идентификатором Microsoft Entra и Центром удостоверений AWS IAM.

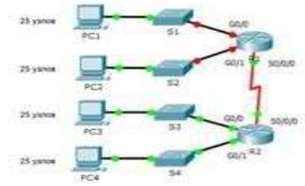
Шаг 2. Настройка Центра удостоверений AWS IAM для поддержки подготовки с помощью идентификатора Microsoft Entra

1. Откройте AWS IAM Identity Center.
2. Выберите элемент **Settings** (Параметры) на панели навигации слева.
3. В разделе **Settings** (Параметры) щелкните Enable (Включить) в разделе Automatic provisioning (Автоматическая подготовка).



4. В диалоговом окне Inbound automatic provisioning (Автоматическая подготовка входящего трафика) скопируйте и сохраните значения **SCIM endpoint** (Конечная точка SCIM) и **Access Token** (Маркер доступа) (отображается после нажатия кнопки Show Token (Показать маркер)). Эти значения вводятся в **поле "URL-адрес** клиента" и **"Секретный маркер** " на вкладке "Подготовка" приложения Центра удостоверений AWS IAM.

Топология



Разбейте сеть 172.16.10.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

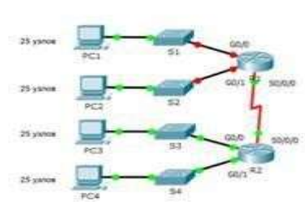
Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам. Последний из используемых IP-адресов назначьте узлам.

32. Выполните базовую настройку устройств S1, R1, R2

Топология



a. Подключитесь с помощью консоли и активируйте привилегированный режим EXEC.

б. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.

в. Назначьте class в качестве зашифрованного пароля привилегированного режима EXEC.

г. Назначьте cisco в качестве пароля консоли и включите режим входа в систему по паролю.

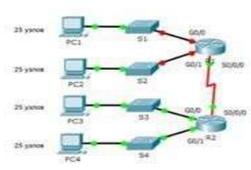
д. Назначьте cisco в качестве пароля VTY и включите вход по паролю. е. Зашифруйте открытые пароли.

ж. Создайте баннер, который предупреждает о запрете несанкционированного доступа(Используйте слово Warninng).

з. Сохраните текущую конфигурацию в файл загрузочной конфигурации

33. Настройте доступ по протоколу SSH на S1 и R2.

Топология



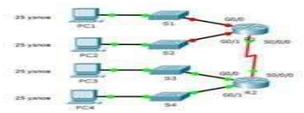
Измените имя домена на ccna.com Создайте ключ RSA длиной 1024 бит.

Настройте линии VTY для доступа по протоколу SSH.

Используйте локальные профили пользователей для аутентификации.

Создайте пользователя admin11 с 15-м уровнем привилегированного доступа и зашифрованным паролем Admin11p@ss.

34. Разбейте сеть на подсети



Разбейте сеть 192.168.11.0/24 на нужное количество подсетей:

a. Назначьте подсеть 0 локальной сети (LAN 1), подключенной к интерфейсу GigabitEthernet 0/0 маршрутизатора R1.

b. Назначьте подсеть 1 локальной сети (LAN2), подключенной к интерфейсу GigabitEthernet 0/1 маршрутизатора R1.

e. Назначьте подсеть 4 каналу WAN между маршрутизаторами R1 и R2.

Завершите документирование схемы адресации в соответствии со следующими рекомендациями.

Назначьте первые используемые IP-адреса маршрутизатору R1 для двух каналов локальной сети (LAN) и одного канала сети WAN.

Второй из используемых IP-адресов назначьте коммутаторам. Последний из используемых IP-адресов назначьте узлам.

Вам нужно будет выполнить несколько команд в командной строке. Сначала проверим подключение к Интернету.

Проверка сетевого подключения

Выполним команды в последовательности:

wpeinit

ping google.com

Если в DC включен DHCP, то, скорее всего, соединение доступно и пинг будет успешным. Если команда ping показала отсутствие соединения, значит, необходимо настроить сетевое подключение вручную.

Настройка сетевого подключения

1. Перед настройкой проверьте активный и подключенный сетевой интерфейс: netsh interface show interface
2. Вы получите список интерфейсов (их может быть несколько). Вам нужно будет захватить имя интерфейса, который **включен, подключен**:
3. Перед выполнением следующей команды узнайте сетевые параметры вашего сервера (эта информация обычно доступна в деталях заказа в личном кабинете хостинг-провайдера). Вам понадобятся основной IP-адрес, маска и шлюз. Настройте интерфейс:

netsh interface ip set address name="Ethernet" static 192.168.0.115 255.255.255.0 192.168.0.1

name="" - это имя интерфейса, которое мы узнали ранее 192.168.0.115 - основной IP-адрес сервера (пример) 255.255.255.0 - маска сети (пример)

192.168.0.1 - шлюз (пример)

4. Далее добавьте dns-сервер Google с помощью команды:

netsh interface ip set dnsserver "Ethernet" static 8.8.8.8

5. С помощью команды **ping google.com** проверьте, подключены ли вы к сети (см. скриншот успешного ping выше).

Подключение сетевого хранилища к серверу

Подключите хранилище с помощью команды:

net use z: \\u114***.introserv.cloud\u114***

*\\u114***.introserv.cloud\u114*** - адрес сетевого хранилища, замените строку на свои данные.* Вам будет предложено ввести имя и пароль. Введите свои текущие данные. Вы должны получить сообщение об успехе:

Проверка резервных копий и полное восстановление системы

1. Проверьте наличие резервных копий в хранилище:

wbadmin get versions -backupTarget:\\u114***.introserv.cloud\u114***

Вас интересуют строки **идентификатора версии**. В примере вы видите, что у вас есть полная резервная копия системы от 09/08/2023 20:10.

Запомните эту информацию в том формате, в котором вы ее получили. Вам доступны 2 варианта восстановления

- Восстановление всей системы со всеми разделами на дисках:

wbadmin start sysrecovery -version:08/09/2023-20:10 -backupTarget:\\u114***.introserv.cloud\u114*** -

restoreAllVolumes -recreateDisks

-backupTarget: указывает на сетевое хранилище.

-version: указывает на выбранную вами резервную копию

*Параметр **-restoreAllVolumes** указывает, что вы хотите восстановить все разделы*

*Параметр **-recreateDisks** указывает, что средство восстановления должно воссоздать разделы (**Примечание - этот параметр сотрет все данные на дисках и запишет данные из резервной копии в воссозданные разделы**).*

- Восстановление только системного раздела, на котором установлена ОС

Выполняется командой:

wbadmin start sysrecovery -version:08/09/2023-20:10 -backupTarget:\\u114***.introserv.cloud\u114***

Полное восстановление образа системы, расположенного на одном из дисков сервера

1. В меню WinRE в пункте **Устранение неполадок** выберите пункт **Восстановление**

В случае несоблюдении стандарта можно попробовать отредактировать файл **/etc/multipath.conf** В **/etc/multipath.conf** надо добавить секцию *multipaths* с подсекцией *multipath*, где вписать сопоставления wwid и alias, например:

multipaths {
multipath {
wwid 8iqn.1998-01.com.vmware:529f9d5bdb8ebd45- cf97c35adc6ecc5f,L,0x0000000000000000
alias 360000000000000000e00000000120001
}
}

После редактирования необходимо рестартовать сервис **multipath** командой в CLI services restart multipath.

Пример из CLI вывода команды storage iscsi-luns с измененным именем LUN:

```
spacevm 192.168.11.111 # storage iscsi_luns
protocol   vend/prod/rev multipath                      uuid                             serial size
scsi:iscsi YADRO,TATLIN  360000000000000000e00000000030003 360000000000000000e00000000030003 beaf33 2.0G
scsi:iscsi YADRO,TATLIN  360000000000000000e00000000030002 360000000000000000e00000000030002 beaf32 2.0G
scsi:iscsi YADRO,TATLIN  360000000000000000e00000000030001 360000000000000000e00000000030001 beaf31 2.0G
scsi:iscsi YADRO,TATLIN  360000000000000000e00000000030004 360000000000000000e00000000030004 beaf34 2.0G
scsi:iscsi YADRO,TATLIN  360000000000000000e00000000030004 360000000000000000e00000000030004 beaf34 2.0G
scsi:iscsi YADRO,TATLIN  360000000000000000e00000000030003 360000000000000000e00000000030003 beaf33 2.0G
scsi:iscsi YADRO,TATLIN  360000000000000000e00000000030001 360000000000000000e00000000030001 beaf31 2.0G
scsi:iscsi YADRO,TATLIN  360000000000000000e00000000030002 360000000000000000e00000000030002 beaf32 2.0G
spacevm 192.168.11.111 #
```

Проверка подключения

create iscsi target record ISCSIADM = 'sudo /sbin/iscsiadm -m'

cleandb = f'{ISCSIADM} node --targetname {target} --portal {source} -o delete' newcmd = f'{ISCSIADM} node --targetname {target} --portal {source} -o new'

enable CHAP if needed if username and password:

cmd = f"{ISCSIADM} node --targetname {target} --portal {source} " \

f"-o update -n node.session.auth.authmethod -v CHAP " \

f"-o update -n node.session.auth.username -v {username} " \

f"-o update -n node.session.auth.password -v {password}"

connect

cmd = f'{ISCSIADM} node --targetname {target} --portal {source} -l'

cmd = f'{ISCSIADM} node --targetname {target} --portal {source} -o update -n node.startup -v automatic'

check

cmd = 'multipath -ll'

№18 Установка резервного восстановления доступа на сервисы

1. Подключитесь к серверу через IP-KVM (iDRAC, IPMI, iRMC), чтобы получить доступ к консоли сервера.
2. Затем войдите в **среду восстановления Windows** , используя установочный образ ОС Windows Server. Подключите образ диска к серверу и загрузитесь с него (в разных версиях IP-KVM могут быть отличия в интерфейсе, но механизм везде одинаков).
3. После загрузки с диска вы попадете в первое окно для выбора языка и настроек клавиатуры. Нажмите кнопку **Далее**
4. На следующем шаге выберите опцию **Восстановить компьютер**.
5. В следующем меню выберите пункт **Устранение неполадок**.

Теперь у вас есть возможность использовать Командную строку, если резервный образ системы хранится в сетевом хранилище. Если резервная копия системы находится на диске, перейдите к разделу **Восстановление образа системы (восстановление Windows с помощью определенного файла образа системы)**.

ПМ.02. Организация сетевого администрирования операционных систем.

Задание 1:

Проверяемые результаты обучения: У6, З1, З2, З11, З12.

Текст задания:

Вариант - I

1. Какими встроенными возможностями обладает сетевая ОС?

a. поддерживает сетевые протоколы
b. поддерживает доступ к удаленным ресурсам
c. поддерживает модуляцию и демодуляцию
d. поддерживает фильтрацию сетевого трафика

2. Укажите сетевые приложения

a. NovellNetWare
b. почтовые системы
c. сетевые базы данных
d. Windows XP

3. Для каких лицензий типично перечисление большого количества условий, запрещающих определённые варианты использования ПО?

a. для проприетарных лицензий
b. для лицензий свободного ПО
c. для лицензий открытого ПО

4. Разрешают ли проприетарные лицензии передачу ПО третьим лицам?

a. большинство проприетарных лицензий запрещают
b. большинство проприетарных лицензий разрешают
c. все подобные лицензии разрешают
d. все подобные лицензии запрещают

5. Кому принадлежат авторские права на ПО в случае открытой лицензии?

a. издателю ПО
b. пользователю
c. организации

6. Сможет ли пользователь использовать ПО в случае отказа принять условия проприетарной лицензии?

a. сможет, но программа будет иметь функциональные ограничения
b. сможет, но программой можно будет пользоваться не более 30 дней
c. не сможет

7. В каких лицензиях любые изменения программы, сделанные пользователем и распространённые дальше, должны сопровождаться исходным кодом этих изменений?

a. в проприетарных
b. в открытых

8. Перечислите коммерческие статусы программ.

9. Дайте определение следующим понятиям: «сетевая операционная система», «лицензия на программное обеспечение».

10. Какие задачи решает сетевая ОС?

Ответы

Номер вопроса	Ответ
1	A,b,d
2	b,c
3	A
4	A
5	A
6	C
7	B
8	бесплатные, бесплатные с рекламой, условно-бесплатные, коммерческие, комплекты для обновления
9	Сетевая операционная система — это операционная система со встроенными возможностями для работы в компьютерных сетях. Лицензия на программное обеспечение — это правовой инструмент, определяющий использование и распространение программного обеспечения, защищённого авторским правом.
10	Главными задачами сетевых ОС являются разделение ресурсов сети (например, дисковые пространства) и администрирование сети.

Критерии оценки:
«5» - 9-10 верных ответов;
«4» - 7-8 верных ответов;
«3» - 5-6 верных ответов;
«2» - менее 5 верных ответов.

Вариант - II

1. Какими встроенными возможностями обладает сетевая ОС?

a. поддерживает сетевое оборудование
b. поддерживает доступ к удаленным ресурсам
c. поддерживает модуляцию и демодуляцию
d. поддерживает протоколы авторизации

2. Укажитесетевыеприложения

a. NovellNetWare
b. LANtastic
c. сетевые базы данных
d. системы автоматизации коллективной работы

3. В каких лицензиях пользователю разрешается использовать одну или несколько копий ПО с сохранением прав на эти копии за издателем ПО?

a. для проприетарных лицензий
b. для лицензий свободного ПО
c. для лицензий открытого ПО

4. Разрешают ли проприетарные лицензии передачу ПО третьим лицам?

a. большинство проприетарных лицензий запрещают
b. большинство проприетарных лицензий разрешают
c. все подобные лицензии разрешают


```
spacevm 192.168.11.111 # storage iscsi_luns
protocol   vend/prod/rev multipath                    uuid                                 serial size
scsi:iscsi YADRO,TATLIN  3600000000000000000e00000000030003 3600000000000000000e00000000030003 beaf33 2.0G
scsi:iscsi YADRO,TATLIN  3600000000000000000e00000000030002 3600000000000000000e00000000030002 beaf32 2.0G
scsi:iscsi YADRO,TATLIN  3600000000000000000e00000000030001 3600000000000000000e00000000030001 beaf31 2.0G
scsi:iscsi YADRO,TATLIN  3600000000000000000e00000000030004 3600000000000000000e00000000030004 beaf34 2.0G
scsi:iscsi YADRO,TATLIN  3600000000000000000e00000000030004 3600000000000000000e00000000030004 beaf34 2.0G
scsi:iscsi YADRO,TATLIN  3600000000000000000e00000000030003 3600000000000000000e00000000030003 beaf33 2.0G
scsi:iscsi YADRO,TATLIN  3600000000000000000e00000000030001 3600000000000000000e00000000030001 beaf31 2.0G
scsi:iscsi YADRO,TATLIN  3600000000000000000e00000000030002 3600000000000000000e00000000030002 beaf32 2.0G
spacevm 192.168.11.111 #
```

1. Пересканировать *scsi* шину узла можно в CLI командой storage rescan-scsi-bus. Так как размер LUN проверяется на всех узлах, где он виден, то стоит пересканировать шину на всех них. Для удобства можно это делать из CLI контроллера через node nodes-cli 'storage rescan-scsi-bus'.
2. Рестартовать сервис *multipathd* в CLI командой services restart multipath. Так как размер LUN проверяется на всех узлах, где он виден, то стоит рестартовать сервис на всех них. Для удобства можно это делать из CLI контроллера через node nodes-cli 'services restart multipath'.

Проверить изменение размера LUN можно, посмотрев в CLI вывод команды storage luns (storage fc- luns, storage iscsi-luns). Необходимо учитывать, что размер в CLI выводится в Гибибайтах (Тебибайтах и т.д.). В Web-интерфейсе контроллера размер LUN выводится в Гигабайтах (для удобства, так как в других местах выводится в таких же единицах) и изменяется автоматически после того, как узел увидел новый размер LUN.

Пример из CLI вывода команды storage iscsi-luns:

Именование LUN (iqn)

Именование LUN должно происходить согласно стандартам: RFC3721 (IQN part)
The following is an example of an iSCSI name string from a storage service provider:

```
Organization  String Naming Defined by Org.
Type  Date Authority Naming Authority
---+-+ +-+ +-+ +-+ +-+    ---------------
   | | | | | | | | |
iqn.1995-11.com.example.ssp:customers.4567.disks.107 RFC3721 (EUI part)
```

The details of
constructing EUI-64 identifiers are specified by the IEEE
Registration Authority (see https://www.rfc-editor.org/rfc/rfc3721.html#ref-EUI64). Example iSCSI name:

```
Type  EUI-64 identifier (ASCII-encoded hexadecimal)
+--++-+---
|  ||
eui.02004567A425678D RFC3980
```

An example of an iSCSI name with a 64-bit NAA value follows:

```
Type  NAA identifier (ASCII-encoded hexadecimal)
+- -+-+ +-----
|  ||
```

naa.52004567BA64678D

An example of an iSCSI name with a 128-bit NAA value follows:

```
Type  NAA identifier (ASCII-encoded hexadecimal)
+- -+-+ +----------------
|  ||
```

naa.62004567BA64678D0123456789ABCDEF

Настройки multipath

Для просмотра настроек multipath в CLI есть команда storage multipath-conf.

Для сканирования доступных путей в CLI есть команда storage scsi-host-discovery.

Для изменения политики группировки путей LUN в CLI есть команда storage modify-multipath-path- grouping-policy [policy].

По умолчанию *path_grouping_policy = failover*. Варианты *path_grouping_policy*:

- *failover* - One path per priority group.
- *multibus* - All paths in one priority group.
- *group_by_serial* - One priority group per serial number.
- *group_by_prio* - One priority group per priority value. Priorities are determined by callout programs specified as a global, per-controller or per-multipath option in the configuration file.
- *group_by_node_name* - One priority group per target node name. Target node names are fetched in

/sys/class/fc_transport/target*/node_name.

Для изменения политики выбора путей LUN в CLI есть команда storage modify-multipath-path-selector [path_selector].

По умолчанию *path_selector = service-time 0*. Варианты *path_selectorservice-time 0* - Send the next bunch of I/O down the path with the shortest estimated service time, which is determined by dividing the total size of the outstanding I/O to each path by its relative throughput.

- *round-robin 0* - Loop through every path in the path group, sending the same amount of I/O to each.
- *queue-length 0* - Choose the path for the next bunch of I/O based on the amount of outstanding I/O to the path.

Подключение FC хранилища

1. При физическом подключении блочного хранилища по FC к серверу контроллер выдаст подсказку у сервера о том, что есть неизвестные блочные хранилища.
2. Если есть подсказка, то стоит перейти во вкладку сервера *Хранилища* – **Блочные хранилища** и нажать кнопку **Сканировать**. Если на сервера найдутся незарегистрированные в базе контроллера хранилища, то они создадутся в базе или обновится связь с теми, что есть в базе.
3. Если хранилище подключено к разным узлам по разным wwn (путям), то стоит включить в настройках Multipath I/O и выставить Режим использования Multipath I/O в *failover*. Тогда при подключении узлов будет проверяться наличие хотя бы одного активного пути из всех.
4. Командой storage hba-npiv в CLI можно увидеть имеющиеся FC карточки, включая состояние их портов (**port_state** и **speed**);
5. Увидеть FC LUNs можно в CLI командой storage fc-luns;
6. Командой storage multipath в CLI можно увидеть LUN и пути, по которым они доступны;
7. Просмотр wwns подключенных хранилищ возможен во вкладке сервера *Хранилища* – **Блочные хранилища** по кнопке **WWNS** или в CLI командой storage fc-wwns;
8. Просмотр локальных wwns сервера возможен во вкладке сервера *Хранилища* – **Блочные хранилища** по кнопке **Локальные WWNS** или в CLI командой storage local-wwns;
9. Пересканировать scsi шину узла можно в CLI командой storage rescan-scsi-bus.
10. В некоторых случаях (например, этого требуют FCoE адаптеры HPE630FLB) для включения FC функционала на них необходимо выполнить команду CLI net fcoe enable <adapter>, например, net fcoe enable eno3.

Действия после изменения размера LUN на хранилище или его удаления.

В том случае, если LUN был сначала виден на серверах Space, а потом его удалили в хранилище или изменили его размер, то автоматически обновление информации об этом действии не произойдет.

Стоит попробовать:

d. все подобные лицензии запрещают

5. Кому принадлежат авторские права на ПО в случае проприетарной лицензии?

a. пользователю
b. организации
c. издателю ПО

6. Сможет ли пользователь использовать ПО в случае отказа принять условия свободной лицензии?

a. сможет, но программа будет иметь функциональные ограничения
b. сможет, но программой можно будет пользоваться не более 30 дней
c. не сможет
d. сможет

7. В каких лицензиях любые изменения программы, сделанные пользователем и распространённые дальше, должны сопровождаться исходным кодом этих изменений?

a. в проприетарных
b. в полусвободных
c. в открытых

8. Перечислите формы распространения программ.

9. Дайте определение следующим понятиям: «сетевая операционная система», «лицензия на программное обеспечение».

10. Какие задачи решает сетевая ОС?

Ответы

Номер вопроса	Ответ
1	A,b,d
2	C,d
3	A
4	A
5	C
6	D
7	C
8	коробочные версии, OEM-версии, Slim-версии, электронные версии.
9	Сетевая операционная система — это операционная система со встроенными возможностями для работы в компьютерных сетях. Лицензия на программное обеспечение — это правовой инструмент, определяющий использование и распространение программного обеспечения, защищённого авторским правом.
10	Главными задачами сетевых ОС являются разделение ресурсов сети (например, дисковые пространства) и администрирование сети.

Критерии оценки:
«5» - 9-10 верных ответов;
«4» - 7-8 верных ответов;

«3» - 5-6 верных ответов;
«2» - менее 5 верных ответов.

Задание 2:
Проверяемые результаты обучения: У6, З1, З2, З11, З12.

Блиц-опрос:
1. Что такое утилита?
2. Перечислите виды утилит.
3. Что такое компрессия данных?
4. Какие существуют методы сжатия?
5. Укажите типы архивов, которые можно создать с помощью программы WinRAR?
6. Какие методы обновления архивов поддерживает WinRAR?
7. Охарактеризуйте локальное приложение.
8. Охарактеризуйте централизованное сетевое приложение.
9. Охарактеризуйте распределенное приложение.

Критерии оценки:
«5» - правильные и полные ответы на 3 вопроса;
«4» - правильные и полные ответы на 2 вопроса;
«3» - нечеткие ответы на вопросы;
«2» - в ответе студента проявляется незнание основного материала изученных тем.

Задание 1:
Проверяемые результаты обучения: У7, У8, З5.

Блиц-опрос:
1. Охарактеризуйте сигнатурный анализ.
2. Охарактеризуйте эвристический анализ.
3. Что такое шифрование?
4. Какие состояния безопасности информации обеспечивает шифрование?
5. Охарактеризуйте тайнопись и криптографию с ключом.
6. Чем отличаются симметричные криптоалгоритмы от асимметричных?
7. Охарактеризуйте шифрование на уровне дисков.
8. Что такое ЭЦП?
9. Как ставится и проверяется ЭЦП?
10. Что такое цифровой сертификат?

Критерии оценки:
«5» - правильные и полные ответы на 3 вопроса;
«4» - правильные и полные ответы на 2 вопроса;
«3» - нечеткие ответы на вопросы;
«2» - в ответе студента проявляется незнание основного материала изученных

- описание (редактируемый параметр);
- тип подключения;
- локация;
- дата и время создания;
- дата и время обновления;
- target;
- состояние Multipath I/O (редактируемый параметр);
- производитель (редактируемый параметр);
- опции iSCSI;
- sources (редактируемый параметр);
- серверы (раскрывающийся список, с возможностью добавления (передобавления) и удаления. При добавлении сервера в открывшемся окне необходимо для проверки соединения с сервером нажать кнопку **Проверить**, после чего выбрать сервер из доступных и нажать кнопку **ОК**.

В окне **Хранилища** – **Сетевые хранилища** – **Блочные** – <имя блочного хранилища> – **LUN** содержится информация о LUNs на хранилище (device, подключение, размер и статус). Имеется

возможность обновления, сканирования хранилища, а также поиск дискового устройства в сетях хранения по адресу.

При нажатии на существующий LUN в открывшемся окне доступны следующие операции:

- обновление информации по кнопке
- форматирование в файловую систему. При нажатии на кнопку **Форматировать в ФС** в открывшемся окне необходимо выбрать из раскрывающегося списка тип файловой системы, после чего подтвердить операцию, нажав кнопку **ОК**. Подробности смотрите в HOWTO создать общий(е) для кластера пул(ы) данных GFS2 на LUN(s), если уже есть кластерный транспорт gfs2;
- монтирование. При нажатии на кнопку **Монтировать** необходимо подтвердить операцию, нажав кнопку **ОК**;
- размонтирование. При нажатии на кнопку **Размонтировать** необходимо подтвердить операцию, нажав кнопку **ОК**.

Также в данном окне содержится следующая информация:

- ID;
- путь;
- target_dev;
- тип шины;
- размер;
- тип файловой системы;
- тип кэширования;
- статус;
- хранилище;
- серийный номер;
- серверы (раскрывающийся список);
- сообщения о работе LUN с возможностью их сортировки по признакам – «По всем типам»,

«Ошибки», «Предупреждения», «Информационные».

События

В окне **Хранилища** – **Сетевые хранилища** – **Блочные** – <имя блочного хранилища> – **События** содержится события, зарегистрированные в системе, возникающие при работе с блочными сетевыми хранилищами с возможностью их сортировки по признакам - «По всем типам», «Ошибки»,

«Предупреждения», «Информационные».

Теги

В окне **Хранилища** – **Сетевые хранилища** – **Блочные** – <имя блочного хранилища> – **Теги** содержится список присвоенных хранилищу меток. Также имеется возможность обновления, создания и применения тега.

нескольких маршрутов (состояние Multipath I/O);

- тип подключения (выбор из раскрывающегося списка);
- имя сервера для монтирования сразу после создания (выбор из раскрывающегося списка);
- IP-адрес или доменное имя сервера хранения и порт;
- проверить доступность сервера и получить список доступных таргетов по кнопке **Получить доступные таргеты (target)**;
- имя iSCSI target;
- логин и пароль для подключения (если требуется);
- производитель (выбор из раскрывающегося списка);
- описание хранилища.

Для подтверждения операции необходимо нажать кнопку **ОК**. Для подключения серверов к созданному хранилищу необходимо:

- нажать на название хранилища в списке;
- в открывшемся окне во вкладке **Информация** рядом с надписью «Серверы» нажать кнопку добавления сервера. При этом открывается окно с возможностью выбора серверов, к которым будет подключено данное хранилище. После заполнения окна необходимо подтвердить операцию, нажав кнопку **ОК**.

После добавления серверов рядом с надписью «Серверы» появится количество серверов и кнопка раскрытия списка серверов.

При использовании хранилища, подключаемого по FC, СХД предоставляет блочные устройства LUN на аппаратном уровне в соответствии с правилами, настроенными на FC коммутаторе и на стороне СХД. Для настройки правил подключения (презентации) LUN с СХД к серверам необходимо обратиться к документации производителя СХД и FC коммутатора. При использовании схемы прямого подключения СХД к серверам SpaceVM (схема DAS - Direct Attached Storage) настройка производится на самом СХД.

Для регистрации в системе управления подключенных LUN необходимо знать адрес WWN порта СХД, с которого происходит обслуживание подключений от серверов SpaceVM. Это необходимо для того, чтобы система управления SpaceVM собрала в группу только те LUN, которые подключены от этого WWN. Это сделано для возможности группировки LUN по WWN СХД, если по FC доступно более одного СХД. При регистрации система опрашивает все блочные устройства, подключенные к серверу, находит имеющие пометку о подключенных по шине FC и презентованные от указанного WWN.

После подключения блочных хранилищ к серверам SpaceVM видимые активные LUN можно использовать как LVM-shared хранилища, как часть ZFS-пула, форматировать их в кластерную файловую систему (OCFS2/GFS2) и подключать их напрямую к ВМ. Не рекомендуется подключать напрямую в ВМ LUN, презентованный по FC. Это связано с тем, что ВМ создаст на этом LUN загрузочную область, которая будет доступна аппаратному серверу, так как FC LUN подключается на уровне основной системы ввода-вывода (BIOS/UEFI).

При установке SpaceVM на сервер с уже подключенным по FC СХД следует обратить внимание на то, что при установке FC LUN могут отображаться в конце списка доступных к установке накопителей, но при загрузке гипервизора могут переместиться в начало списка (занять место диска

/dev/sda). Для предотвращения такого поведения необходимо корректно настроить FC карту сервера (FC HBA) и параметры презентуемых LUN на стороне СХД.

Окно состояния блочного хранилища

В окне состояния блочного хранилища содержится информация, разделенная на группы:

- информация;
- LUN;
- события;
- задачи;
- теги.

В окне **Хранилища** – **Сетевые хранилища** – **Блочные** – <имя блочного хранилища> – **Информация** содержатся следующие сведения:

- название (редактируемый параметр);

тем.

Задание 2:

Проверяемые результаты обучения: У7, У8, З5, З11.

Текст задания:Вариант - I

1. **Наиболее распространенными Интернет-сервисами являются**:
a. сетевые протоколы
b. служба WWW
c. передача электронных сообщений и блоков данных
d. сетевые базы данных
2. **Укажите ПО для работы с Интернетом**
a. NovellNetWare
b. Почтовые программы
c. Windows XP
3. **К браузерам относят:**
a. Firefox
b. JavaScript
c. Outlook Express
d. Safari
4. **Функций Web сервера является**
a. обеспечения большей устойчивости браузера
b. предоставление доступа к части локальной файловой системы
c. взаимодействие между клиентом и сервером
5. **Интернет-вещаниевключает:**
a. Новостные ленты
b. Базы данных
c. Сообщения о результатах выборов
d. Web-браузер
6. **ПО для программирования и разработки приложений**
a. VBScript, GoogleGhrome
b. SecureLock, TrueCrypt, DriveCrypt Plus Pack
c. Delphi, C++ Builder фирмы Borland
7. **В настоящее время языки типа Ассемблера обычно используют:**
a. для создания систем искусственного интеллекта
b. в виде вставок в программы на языках высокого уровня
8. **Перечислите Специализированные языки разработчика**
9. **Дайте определение следующим понятиям: «Интернет», «Web-браузер».**
10. **Наиболее популярными веб-серверами являются**

Ответы

Номер вопроса	Ответ
1	b,c
2	b,
3	A, d
4	B
5	A, c
6	C

7	В
8	Специализированные языки разработчика используют для создания конкретных типов программного обеспечения. К ним относят: языки баз данных; языки создания сетевых приложений; языки создания систем искусственного интеллекта и т. д.
9	Интернет - глобальная информационная сеть, части которой логически взаимосвязаны друг с другом посредством единого адресного пространства, основанного на протоколе TCP/IP. Web-браузер - это программное обеспечение для просмотра web-сайтов, то есть для запроса web-страниц из WWW, для их обработки и вывода, и для реализации перехода от одной страницы к другой.
10	Наиболее популярными веб-серверами являются Apache и Internet Information Server (IIS).

Критерии оценки:
«5» - 9-10 верных ответов;
«4» - 7-8 верных ответов;
«3» - 5-6 верных ответов;
«2» - менее 5 верных ответов.
Вариант - II

1. Наиболее распространенными Интернет-сервисами являются:
a. сетевые протоколы
b. служба передачи файлов FTP
c. сетевые базы данных
d. передача электронных сообщений и блоков данных
2. Укажите ПО для работы с Интернетом
a. Браузер
b. NovellNetWare
c. Windows XP
3. К браузерам относят:
a. Firefox
b. GoogleGhrome
c. Outlook Express
d. JavaScript
4. Функций Web сервера является
a. обеспечения большей устойчивости браузера
b. предоставление доступа к части локальной файловой системы
c. взаимодействие между клиентом и сервером
5. Интернет-вещаниевключает:
a. Таблицы
b. Видео
c. Новостные ленты
d. Web-браузер
6. ПО для программирования и разработки приложений

Если вы планируете использовать хранилище для хранения бэкапов, для повышения отказоустойчивости мы рекомендуем выбрать пул из другой зоны доступности или региона. Выберите подсеть, в которой будет находиться хранилище. Тип подсети зависит от того, к чему нужно подключить хранилище:

- облачную приватную подсеть — хранилище будет доступно для облачных серверов и кластеров Managed Kubernetes только в том сегменте пула, который вы выбрали на предыдущем шаге;
- подсеть глобального роутера Selectel — хранилище будет доступно для выделенных серверов, а также облачных серверов и кластеров Managed Kubernetes, которые находятся в других сегментах пула. Посмотрите примеры настройки сетевой связности через глобальный роутер в инструкциях Подключить файловое хранилище к выделенному серверу, Подключить файловое хранилище к облачному серверу в другом пуле, Подключить файловое хранилище к кластеру Managed Kubernetes в другом пуле.

Введите приватный IP-адрес хранилища или оставьте первый доступный адрес из подсети, который назначается по умолчанию. После создания хранилища IP-адрес нельзя будет изменить.

Выберите тип файлового хранилища. Хранилища отличаются скоростью чтения/записи и значениями пропускной способности:

- HDD Базовое;
- SSD Универсальное;
- SSD Быстрое.

После создания тип хранилища нельзя будет изменить.

Укажите размер хранилища: от 50 ГБ до 50 ТБ. После создания можно будет увеличить файловое хранилище, но нельзя уменьшить.

Выберите протокол:

- NFSv4 — для подключения хранилища к серверам с операционной системой Linux и другими Unix-системами;
- CIFS SMBv3 — для подключения хранилища к серверам с операционной системой Windows. После создания протокол нельзя будет изменить.

Проверьте стоимость файлового хранилища. Нажмите **Создать**.

Примонтируйте файловое хранилище в зависимости от продукта.

Процесс монтирования зависит от операционной системы на облачном сервере и протокола файлового хранилища: NFSv4 или CIFS SMBv3.

- NFSv4
- CIFS SMBv3
- Linux
- Windows

1. Подключитесь к серверу.
2. Установите пакет для работы с протоколом NFS:

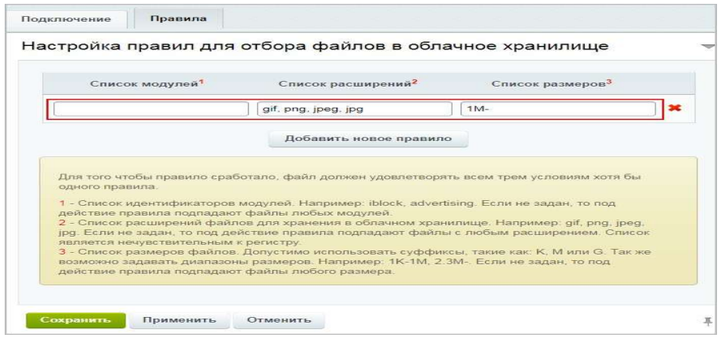
`sudo apt install nfs-common` Создайте папку для монтирования хранилища:
`sudo mkdir -p /mnt/nfs` Примонтируйте файловое хранилище:
`sudo mount -vt nfs "<filestorage_ip_address>:/shares/share-<mountpoint_uuid>" /mnt/nfs`
Укажите:

- <filestorage_ip_address> — IP-адрес файлового хранилища. Можно посмотреть в панели управления в разделе **Облачная платформа → Файловое хранилище →** страница хранилища **→** вкладка **Настройки →** поле **IP**;
- <mountpoint_uuid> — ID точки монтирования. Можно посмотреть в панели управления в разделе **Облачная платформа → Файловое хранилище →** страница хранилища **→** блок **Подключение →** вкладка **GNU/Linux**.

№17 Установка облачного хранилища типа: блочное

Для подключения блочного хранилища iSCSI необходимо перейти в раздел **Хранилища - Сетевые хранилища - Блочные** основного меню и нажать кнопку **Добавить блочное хранилище**. В открывшемся окне необходимо заполнить следующие поля:

- название сетевого хранилища;
- определить возможность подключения узлов сети хранения данных с использованием

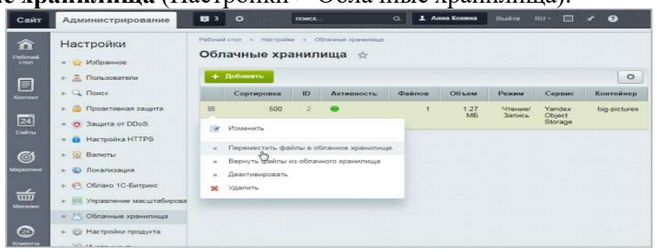


В колонке **Список модулей** укажите названия модулей , данные которых будут загружаться в облачное хранилище. Если оставить поле пустым, то под действие правила будут подпадать файлы любых модулей.

В колонке **Список расширений** укажите расширения файлов для хранения в облачном хранилище. **Например:** gif, png, jpeg, jpg. Если поле не заполнено, то под действие правила подпадают статические файлы с любым расширением. Список является нечувствительным к регистру.

В колонке **Список размеров** укажите размеры файлов. Допустимо использовать суффиксы, такие как: **K**, **M** или **G**. Также возможно задавать диапазоны размеров. **Например:** 1M- (т.е. в облачное хранилище будут выгружаться файлы размером более одного мегабайта). Если поле не заполнено, то под действие правила подпадают файлы любого размера.

3. Нажмите кнопку **Сохранить**. Новый контейнер появится в списке на странице **Облачные хранилища** (Настройки > Облачные хранилища):



Перенесите уже имеющиеся на сайте файлы в облачное хранилище с помощью одноименного пункта меню.

Примечание: По окончанию процедуры переноса файлов будет выведено сообщение о результате. В случае неудачного подключения на странице будет выведен текст ошибки (текст выдается сервисом облачного хранения файлов).

Новые загружаемые файлы будут автоматически проверяться на соответствие правилу и сохраняться в облачное хранилище. Ссылки на файлы будут также автоматически формироваться с учетом их расположения в облачном хранилище.

№16 Установка облачного хранилища типа: файловое

В панели управления перейдите в раздел **Облачная платформа → Файловое хранилище**. Нажмите **Создать хранилище**.

Введите новое имя хранилища или оставьте имя, которое создано автоматически. Выберите пул, в котором будет расположено хранилище.

Если с помощью файлового хранилища нужно увеличить дисковое пространство, выберите пул, в котором расположен облачный сервер или кластер Managed Kubernetes. Для подключения хранилища нужно будет только примонтировать его. В остальных случаях (в том числе, при подключении хранилища к выделенному серверу) нужно настроить сетевую связность между сервером/кластером и хранилищем через глобальный роутер.

a. SecureLock, TrueCrypt, DriveCrypt Plus Pack
b. Visual C++, Visual Basic, Visual Ada
c. BestCrypt, S-Tools, WinDefender

7. В настоящее время языки типа Ассемблера обычно используют:

a. при написании сравнительно простых программ, взаимодействующих непосредственно с техническими средствами
b. в виде динамического изменения информации, передаваемой по каналам Интернета

8. Перечислите ряд отличий между браузерами

9. Дайте определение следующим понятиям: «Протоколы», «Служба WWW».

10. Наиболее популярными являются следующие браузеры

Ответы

Номер вопроса	Ответ
1	b,d
2	A
3	A, b
4	B
5	B,c
6	B
7	A
8	Между браузерами существует ряд отличий, например:некоторые скрипты на языке JavaScript приводят к аварийному завершению IE, а бразузер Firefox способен корректно их обрабатывать;некоторые HTML-тэги по-разному обрабатываются IE и Firefox;IE, в отличие от Firefox, не в полной мере поддерживает каскадируемые таблицы стилей Cascading Style Sheets (CSS) 2.0;последовательность обработки HTML-тэгов при визуализации страницы отличается в различных браузерах;некоторые атрибуты стилей работают в Firefox, но не работают в IE.
9	Протоколы — это правила взаимодействия между компьютерами в сети. Служба WWW (World Wide Web) - основная служба в сети Интернет, позволяющая получать доступ к информации на любых серверах, подключенных к сети.
10	Внастоящеевремянаиболеепопулярнымиявляютсяследующиебраузеры: Internet Explorer (IE), Opera, Firefox, Google Ghrome, Safari.

Критерии оценки:

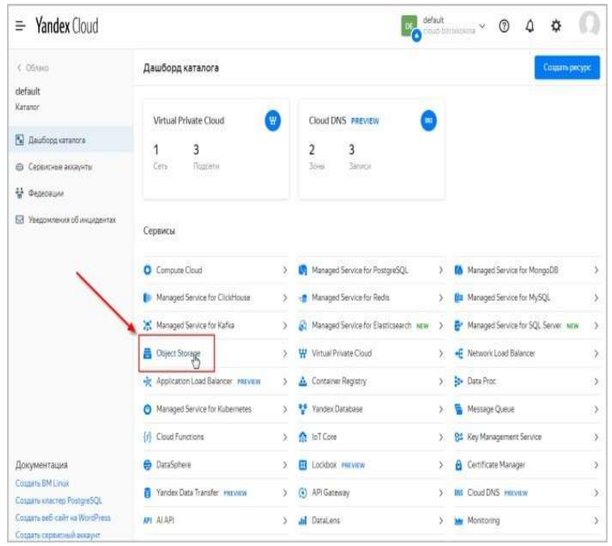
«5» - 9-10 верных ответов;
«4» - 7-8 верных ответов;
«3» - 5-6 верных ответов;
«2» - менее 5 верных ответов.

Задание 3:

Проверяемые результаты обучения: У7, У8, З5, З11.

Блиц-опрос:

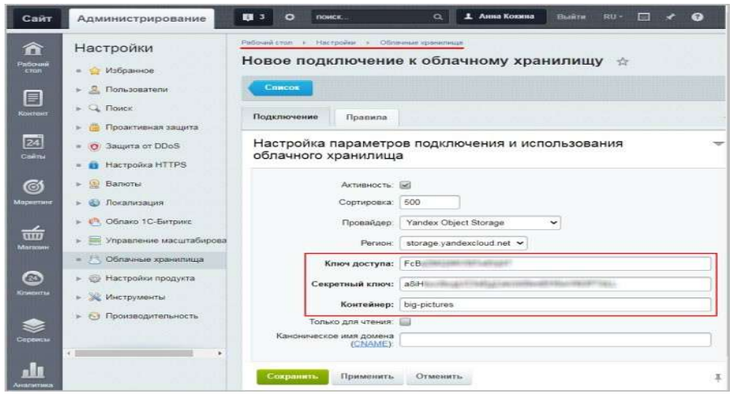
1. Что такое почтовый клиент?
2. Какие почтовые службы вы знаете?
3. Электронная почта.
4. Для чего используется брандмауэр?
5. Охарактеризуйте электронные доски объявлений.
6. Для чего используются утилиты сервера?
7. Укажите утилиты командной строки.
8. Укажите утилиты сервера от корпорации Microsoft.
9. Перечислите утилиты сервера от сторонних производителей.
10. Что такое SQL – сервер?



В качестве пользователя выберите созданный ранее **сервисный аккаунт**; В уровне доступа укажите **FULL_CONTROL**;
Нажмите кнопку **Добавить**, а затем сохраните изменения.

Действия на стороне сайта

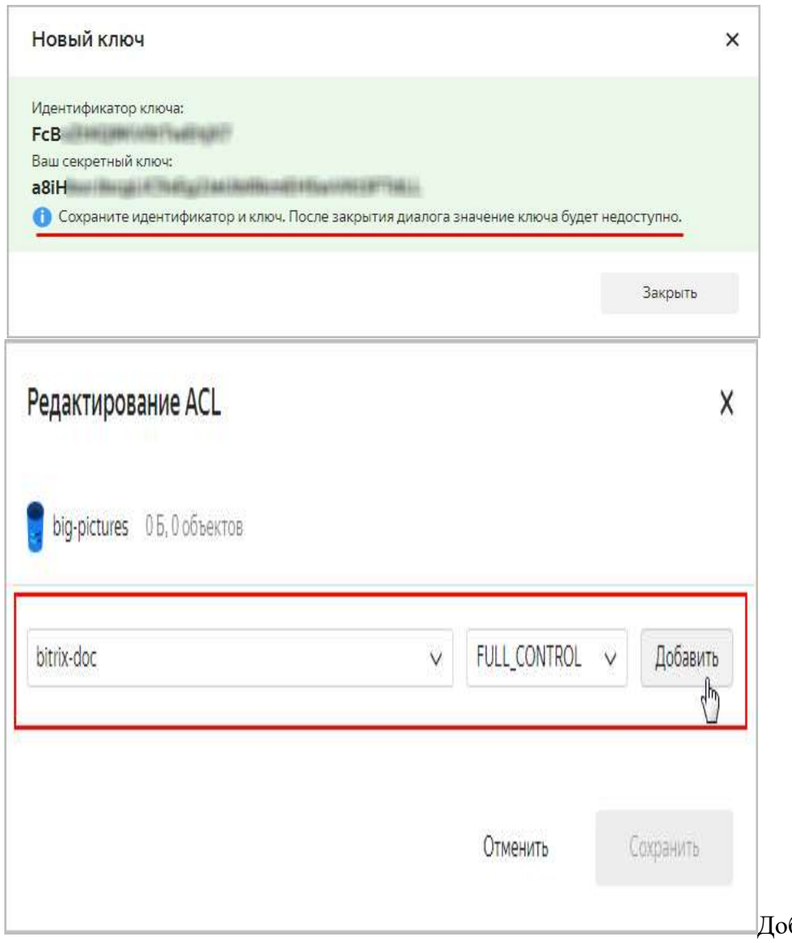
1. Добавьте новое подключение на странице **Облачные хранилища** (Настройки > Облачные хранилища). Откроется форма вида:



Провайдер - выберите из списка **Yandex Object Storage**; **Регион** - устанавливается автоматически;
Ключ доступа и **Секретный ключ** - укажите идентификатор ключа сервисного аккаунта на **Yandex Object Storage** и секретный ключ;
Контейнер - пропишите название созданного ранее бакета;
Только для чтения - при отмеченной опции новые файлы будут сохраняться не в контейнере, а на хостинге с проектом.

Важно! Поле "Каноническое имя домена" не нужно заполнять. Оно предназначено для разработчиков и служит для налаживания более эффективной раздачи контента клиентам. Требуются дополнительные сторонние настройки и соответствующие навыки.

2. Перейдите во вкладку **Правила** и задайте условия, по которым будет происходить отбор файлов для загрузки в облачное хранилище:



Добавьте описание и нажмите кнопку **Создать**. В открывшемся окне отобразятся сгенерированные идентификатор ключа (**Ключ доступа**) и секретный ключ:

Важно! Необходимо сохранить идентификатор и ключ. После закрытия диалога значение ключа будет недоступно.

3. Теперь осталось создать контейнер (бакет).

В дашборде нужного каталога выберите сервис **Object Storage**:

Нажмите кнопку Создать бакет и заполните поля открывшейся формы.

Далее нужно привязать созданный бакет к сервисному аккаунту. В списке действий (иконка-троеточие справа от названия бакета) выберите пункт ACL бакета.

Откорректируйте настройки:

ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ОЦЕНКИ ОСВОЕНИЯ МДК.02.02. ОРГАНИЗАЦИЯ АДМИНИСТРИРОВАНИЯ КОМПЬЮТЕРНЫХ СЕТЕЙ

Промежуточный контроль на проверку освоения МДК 02.02:

Проверяемые результаты обучения: У1, У2, У4, У5, У6, З1, З2, З3, З5.

Блиц-опрос 1:

1. Какова основная цель сетевого администрирования? Чем отличаются понятия сетевого администрирования и системного администрирования?
2. Назовите основные виды задач сетевого администрирования. Приведите примеры конкретных задач на каждый вид.
3. Чем отличаются версии операционных систем Microsoft Windows Server 2003?
4. Что такое оснастка (snap-in)?
5. Объясните, что означают свойства «платформонезависимость» и «открытость» применительно к стеку протоколов TCP/IP.
6. Что такое ARPANET?
7. Поясните, для чего предназначена модель OSI? Где она применяется?
8. Назовите функции канального, сетевого и транспортного уровней модели OSI.
9. Чем отличается модель DARPA (DoD) от модели OSI? Как вы думаете, почему?
10. Что такое RFC? В файлах какого формата издаются RFC?
11. Для чего используется протокол ICMP? Протокол ARP?
12. Поясните принцип работы утилит ping и tracert.

Блиц-опрос 2:

1. Перечислите виды и примеры адресов, используемых в стеке TCP/IP.
2. Из каких частей состоит IP-адрес?
3. Как определяется номер подсети в IP-адресе?
4. Каков диапазон возможных адресов у сети класса C?
5. Определите номер подсети на основе маски: 116.98.04.39/27.
6. Каковы основные особенности протокола IPv6&
7. Поясните принцип работы протокола ARP.
8. Для чего необходимы доменные имена?
9. Для чего нужна служба DNS?
10. Что такое корневой домен?
11. Каково было предназначение файла hosts? Используется ли он сегодня?
12. Чем отличается служба DNS от системы DNS?
13. Объясните принцип действия итеративного и рекурсивного запроса.
14. В чем отличие доменных имен от имен NetBIOS?

Блиц-опрос 3:

1. Для решения какой проблемы предназначен протокол DHCP?
2. Почему адреса предоставляются в аренду на время, а не навсегда?
3. Перечислите основные параметры DHCP.
4. Назовите диапазоны частных адресов. Для чего они нужны?
5. Поясните значение сообщений DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK.
6. Какая информация хранится в каталоге Active Directory? Где находится сам каталог?
7. Что такое домен?
8. Чем отличается контроллер домена от других узлов сети?
9. Какова цель логической структуризации каталог Active Directory?
10. Сколько всего может быть создано глобальных идентификаторов GUID?
11. Чем аутентификация отличается от авторизации?
12. Объясните понятия «доверенный» и «доверяющий» домен. В каком случае один домен может быть доверенным и доверяющим одновременно?

Промежуточный контроль на проверку освоения МДК 02.02:

Проверяемые результаты обучения: У1, У2, У4, У5, У7, У8, З1, З2, З5, З11.

Тест 1:

Текст задания:

1. Какие протоколы относятся к транспортному уровню четырехуровневой модели стека протоколов TCP/IP?

1. ARP
2. TCP
3. UDP
4. IP
5. ICMP
6. Выберите все правильные ответы

2. **Что протокол IPSec добавляет к пакетам для аутентификации данных?**

1. Заголовок аутентификации (заголовок AH)
2. Заголовок подписи (заголовок SH)
3. Заголовок авторизации (заголовок AvH)
4. Заголовок цифровой подписи (заголовок DSH)

3. **Что из предложенного входит в процедуру согласования IPSec?**

1. Только соглашение безопасности ISAKMP
2. Соглашение безопасности ISAKMP и одно соглашение безопасности IPSec
3. Соглашение безопасности ISAKMP и два соглашения безопасности IPSec
4. Только два соглашения безопасности IPSec

4. **Протокол ESP из IPSec:**

1. Обеспечивает только конфиденциальность сообщения
2. Обеспечивает только аутентификацию данных
3. Обеспечивает конфиденциальность и аутентификацию сообщения

Удаление служб из Firewalld

Чтобы удалить службы ftp и smtp, выполните команду:

```
sudo firewall-cmd --zone=public --remove-service=ftp
```

```
sudo firewall-cmd --zone=public --remove-service=smtp
```

Блокировка любых входящих и исходящих пакетов

Можно заблокировать любые входящие или исходящие пакеты / соединения, используя Firewalld. Это известно как “panic-on” Firewalld. Для этого выполните:

```
sudo firewall-cmd --panic-on
```

В вашем терминале будет отображаться текст «success».

После этого вы не сможете выполнить ping или просмотреть любой веб-сайт. Чтобы отключить этот запрет, выполните команду:

```
sudo firewall-cmd --panic-off
```

Добавление IP-адреса в Firewalld

```
sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source
address="192.168.1.4" accept'
```

Таким образом, Firewalld будет принимать пакеты IPv4 от источника IP 192.168.1.4.

Блокировка IP-адреса от Firewalld

Аналогично, чтобы заблокировать любой IP-адрес:

```
sudo firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source
address="192.168.1.4" reject'
```

При этом Firewalld будет удалять / отбрасывать все пакеты IPv4 из исходного IP 192.168.1.4.

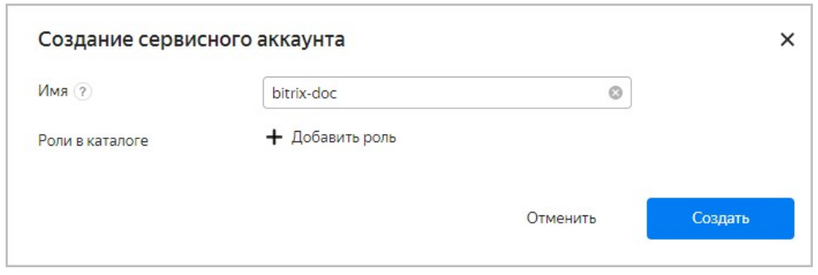
№15 Установка облачного хранилища типа: объектное

Рассмотрим подробнее процесс подключения облачного хранилища на примере Yandex Object Storage .

Действия на стороне Yandex Object Storage

Прежде всего необходимо зарегистрироваться на сайте сервиса Yandex Object Storage.

1. Создайте сервисный аккаунт согласно инструкции :



Укажите имя аккаунта.

Примечание: Имя нового аккаунта может содержать строчные буквы латинского алфавита, цифры и дефисы. Первый символ должен быть буквой. Последний символ не должен быть дефисом. Допустимая длина — от 3 до 63 символов.

При желании можно задать роль (не обязательно).

2. Далее необходимо создать ключ доступа. Кликните по созданному сервисному аккаунту и нажмите кнопку Создать новый ключ, выберите пункт Создать статический ключ доступа.

```
sudo firewall-cmd --get-zones
```

```
yurii@Sedicomm:~$ sudo firewall-cmd --get-active-zones
public
  interfaces: enp0s3
```

Чтобы узнать зону по умолчанию, выполните команду:

```
sudo firewall-cmd --get-default-zone
```

Для служб

```
yurii@Sedicomm:~$ sudo firewall-cmd --get-default-zone
public
```

```
sudo firewall-cmd --get-services
```

Здесь можно увидеть сервис, охваченный Firewalld.

Установка зоны по умолчаниюВажно отметить, что после каждой модификации вам нужно перезагрузить Firewalld, чтобы изменения вступили в силу.

```
sudo firewall-cmd --set-default-zone=internal
```

или

```
sudo firewall-cmd --set-default-zone=public
```

После изменения зоны проверьте, изменилась ли она или нет.

```
sudo firewall-cmd --get-default-zone
```

Добавление порта в общественной зоне

```
sudo firewall-cmd --permanent --zone=public --add-port=80/tcp
```

Это команда добавит TCP-порт 80 в публичную зону. Также можно добавить желаемый порт, заменив 80 на любой необходимый.

Теперь перезагрузите Firewalld.

```
sudo firewall-cmd --reload
```

После проверьте статус, чтобы узнать, был ли добавлен порт tcp 80 или нет.

```
sudo firewall-cmd --zone=public --list-ports
```

Здесь вы можете увидеть, что был добавлен TCP-порт 80. Также можно ввести:

```
sudo firewall-cmd --zone=public --list-all
```

Удаление порта из общественной зоны

Чтобы удалить порт Tcp 80 из общественной зоны, введите следующее.

```
sudo firewall-cmd --zone=public --remove-port=80/tcp
```

В вашем терминале будет отображен текст «success».

Добавление служб в Firewalld

Чтобы добавить службу ftp в Firewalld, выполните команду приведенную ниже:

```
sudo firewall-cmd --zone=public --add-service=ftp
```

В вашем терминале будет отображаться текст «success».

```
sudo firewall-cmd --zone=public --add-service=smtp
```

Аналогичным образом для добавления услуги smtp выполните команду:

При желании можно заменить ftp и smtp на собственный сервис, который вы хотите добавить.

4. Не обеспечивает ни конфиденциальность, ни аутентификацию

5. **Виртуальные частные сети:**

1. Передают частные данные по выделенным сетям
2. Инкапсулируют частные сообщения и передают их по общественной сети
3. Не используются клиентами Windows
4. Могут использоваться с протоколами L2TP или PPTP

6. **Основные отличия протоколов L2TP и PPTP состоят в следующем (выберите все возможные варианты):**

1. Протокол L2TP обеспечивает не конфиденциальность, а только туннелирование
2. Протокол PPTP используется только для туннелирования TCP/IP
3. Протокол L2TP может использоваться со службами IPSec, а протокол PPTP используется самостоятельно
4. Протокол PPTP поддерживается крупнейшими производителями, а протокол L2TP является стандартом корпорации Microsoft

7. **Служба, осуществляющая присвоение реальных IP-адресов узлам закрытой приватной сети, называется:**

1. NAT
2. PAT
3. Proxy
4. DHCP
5. DNS

9. **На каком из четырех уровней модели стека протоколов TCP/IP к передаваемой информации добавляется заголовок, содержащий поле TTL (time-to-live)?**

1. На уровне приложений (application layer)
2. На транспортном уровне (transport layer)
3. На сетевом уровне (internet layer)
4. На канальном уровне (link layer)

10. **На каком уровне четырехуровневой модели стека протоколов TCP/IP работает служба DNS?**

1. На Уровне приложений (application layer)
2. На Транспортном уровне (transport layer)
3. На Межсетевом уровне (internet layer)
4. На Канальном уровне (link layer)

11. **Какой транспортный протокол используется протоколом Simple Mail Transfer Protocol (SMTP)?**

1. TCP
2. UDP
3. ICMP
4. Ни один из перечисленных

12. **Назовите отличия концентраторов (hub) от коммутаторов 2-го уровня (switch).**

1. Коммутаторы работают на более высоком уровне модели OSI, чем концентраторы
2. Коммутаторы не могут усиливать сигнал, в отличие от концентраторов

3. Коммутаторы избирательно ретранслируют широковещательные кадры, концентраторы передают широковещательные кадры на все свои порты
4. Коммутаторы анализируют IP-адреса во входящем пакете, а концентраторы анализируют MAC-адреса

Критерии оценки:
«5» - 10-11 верных ответов;
«4» - 7-9 верных ответов;
«3» - 5-6 верных ответов;
«2» - менее 5 верных ответов.

Тест 2:

1. **В описании правил для межсетевого экрана FreeBSD действие fwd означает:**
   a. Установление вероятности совершения действия
   b. Имитацию задержки пакетов
   c. Перенаправление пакетов на обработку другой программе
   d. Перенаправление пакетов на другой узел
2. **Выберите верное утверждение:**
   a. Протокол L2TP не имеет встроенных механизмов защиты информации
   b. Протокол L2TP не применяется при создании VPN
   c. Протокол PPTP более функциональный и гибкий чем L2TP, но требует более сложных настроек
3. **3.Служба IPSec может быть использована:**
   a. Только для шифрования
   b. Только для аутентификации
   c. Для аутентификации и шифрования
   d. Не может быть использования ни для шифрования, ни для аутентификации
4. **4.«Злоумышленник генерирует широковещательные ICMP- запросы от имени атакуемого узла». Это описание метода:**
   a. Маскарадинг
   b. Смерфинг
   c. Активная имитация
   d. Пассивная имитация
5. **межсетевом экране FreeBSD действие reject соответствует действию**
   a. unreach net
   b. unreach host
   c. unreach port
6. **Протокол RIP:**
   a. Не имеет механизма предотвращения зацикливания
   b. Имеет простой и не эффективный механизм предотвращения зацикливания
   c. Имеет высокоэффективный механизм предотвращения зацикливания
7. **Какой протокол служит, в основном, для передачи мультимедийных данных, где важнее своевременность, а не надежность доставки.**

Как установить Firewalld

Перед установкой Firewalld убедитесь, что вы остановили iptables. Для этого введите:

```
sudo systemctl stop iptables
```

Затем убедитесь, что iptables больше не используется вашей системой:

```
sudo systemctl mask iptables
```

Теперь проверьте состояние iptables:

```
sudo systemctl status iptables
```

Теперь все готово для установки Firewalld.

Для Ubuntu

Чтобы установить Firewalld на Ubuntu, сначала необходимо удалить UFW, а затем установить. Чтобы удалить UFW, выполните команду приведенную ниже.

```
sudo apt-get remove ufw
```

После удаления UFW введите:

```
sudo apt-get install firewall-applet
```

```
yurii@Sedicomm:~$ sudo apt-get remove ufw
Чтение списков пакетов… Готово
Построение дерева зависимостей
Чтение информации о состоянии… Готово
Следующие пакеты устанавливались автоматически и больше не требуются:
  libfprint-2-tod1 libllvm10
Для их удаления используйте «sudo apt autoremove».
Следующие пакеты будут УДАЛЕНЫ:
  ufw
Обновлено 0 пакетов, установлено 0 новых пакетов, для удаления отмечено 1 пакетов, и 2 пакетов не обновлено.
После данной операции объём занятого дискового пространства уменьшится на 846 kB.
Хотите продолжить? [Д/н] y
(Чтение базы данных … на данный момент установлено 168407 файлов и каталогов.)
Удаляется ufw (0.36-6) …
Skip stopping firewall: ufw (not enabled)
Обрабатываются триггеры для man-db (2.9.1-1) …
yurii@Sedicomm:~$ sudo apt-get install firewall-applet
Чтение списков пакетов… Готово
Построение дерева зависимостей
Чтение информации о состоянии… Готово
Следующие пакеты устанавливались автоматически и больше не требуются:
  libfprint-2-tod1 libllvm10
```

Или вы можете открыть Ubuntu Software Center и посмотреть или скачать «firewall-applet», а затем установить его на вашу систему Ubuntu.

Для RHEL, CentOS & Fedora

Введите ниже команду для установки Firewalld в вашей системе CentOS.

```
sudo yum install firewalld firewall-config -y
```

Как настроить Firewalld

Перед настройкой мы должны знать его статус после установки. Чтобы это узнать, введите следующее:

```
sudo systemctl status firewalld
```

Поскольку Firewalld работает на основе зон, необходимо проверить все зоны и сервисы, даже учитывая, что мы еще не сделали никакой настройки.

Для зон

```
sudo firewall-cmd --get-active-zones
```

или

ATM 622	50 MB/sec

Реальная скорость передачи данных некоторых сетевых протоколов.

Для работы без потерь производительности рекомендуется использовать не более четырех устройств на одной SCSI шине или не более двух устройств при наличии на шине таких устройств, как диски и т. п. Кроме того, следует заметить, что при работе с лентами значительно снижается общая производительность SCSI шины, поэтому рекомендуется выносить ленточные устройства на отдельный контролер или по возможности не использовать их на SCSI шине с критичными по скорости доступа устройствами.

Накопитель	Утилизация шины
SLR	3 MB/sec
DDS-3	5 MB/sec
EXABYTE-8900	9 MB/sec
DLT7000	20 MB/sec

Утилизация шины современными ленточными устройствами.

№13 Установка Firewall

№14 Настройка системы фильтрации трафика Firewall

Firewalld — динамически управляемый **брандмауэр** с поддержкой зон сети, который определяет уровень доверия сетевых подключений или интерфейсов. Он поддерживает IPv4, настройки брандмауэра IPv6, мосты Ethernet и IP-наборы. Он также предоставляет интерфейс для служб или приложений для непосредственного добавления правил брандмауэра.

Первая модель брандмауэра с system-config-firewall / lokkit была статической, и каждое изменение требовало полного перезапуска брандмауэра. Она включала также выгрузку модулей ядра сетевого фильтра брандмауэра и загрузку модулей, необходимых для новой конфигурации. Разгрузка модулей привела к нарушению состояния брандмауэра и установлению соединений.

Демон брандмауэра динамически управляет Firewalld и применяет изменения без его перезапуска. Поэтому нет необходимости перезагружать все модули ядра брандмауэра. Но использование демона требует, чтобы все изменения брандмауэра выполнялись синхронизировано с этим демоном.

Демон Firewall не может разобрать правила брандмауэра, добавленные инструментами командной строки iptables и ebtables. Демон предоставляет информацию о текущих настройках активного брандмауэра через D-BUS, а также принимает изменения через D-BUS с использованием методов проверки подлинности PolicyKit.

Таким образом, Firewalld использует зоны и службы вместо цепочек и правил для выполнения операций, и может управлять правилами динамического обновления и модификации без нарушения существующих сеансов и соединений.

Firewalld имеет следующие функции:

- API D-Bus.
- Временные правила брандмауэра.
- Богатый язык для описания правил брандмауэра.
- Поддержка IPv4 и IPv6 NAT.
- Зоны межсетевого экрана.
- Поддержка IP-набора.
- Логи отклоненных пакетов.
- Прямой интерфейс.
- Lockdown: Белый список приложений, которые могут изменить брандмауэр.
- Поддержка iptables, ip6tables, ebtables и брандмауэров ipset firewall.
- Автоматическая загрузка модулей ядра Linux.
- Интеграция с Puppet.

Чтобы узнать больше о Firewalld, перейдите по этой ссылке.

a. TCP
b. UDP
c. TCP, UDP

8. **Протокол передачи команд и сообщений об ошибках.**
a. ICMP
b. SMTP
c. TCP

9. **С помощью какой команды можно просмотреть таблицу маршрутизации**
a. Route
b. Ping
c. Tracert

10. **Что означает MAC-адрес, IP-адрес компьютера, Физический адрес**
a. Адрес компьютера во внешней сети

11. **Какой порт может использоваться клиентом (со своей стороны) при подключении к Web-серверу**
a. 80
b. 1030
c. 28

Критерии оценки:
«5» - 10-11 верных ответов;
«4» - 7-9 верных ответов;
«3» - 5-6 верных ответов;
«2» - менее 5 верных ответов.

Задания для оценки освоения МДК 02.03.

Типовые задания для оценки освоения состоят из тестирования.

Проверяемые результаты обучения: У1, У2, У3, У4, У5, З1, З2, З3, З5.

Задание 1:

Текст задания:

ОБЩИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ ТЕСТА

Внимательно прочитайте задание, выберите правильный вариант ответа.

Вы можете воспользоваться справочными материалами, имеющимися на столе преподавателя.

Время выполнения задания – 30 мин.

Задание выполняется на компьютере (электронный тест) и сдается для проверки отчет теста.

№ Задания	Вопросы	Варианты ответов

1.	**WiFi является –** а) промышленным названием технологии беспроводной передачи данных и относится к группе стандартов IEEE 802.11 б) провайдером сети Интернет в) специальный канал связи для выхода в Интернет	Эталон ответа а)
2.	**Сейчас реализовано и используется 4 основные стандарты для Wi-Fi сетей, это:** а) 802.11a, 802.11b, 802.11c и 802.11d, б) 802.11a, 802.11b, 802.11g и 802.11n, в) 802.11q, 803.11b, 804.11g и 805.11n,	Эталон ответа б)
3.	**Тип организации Wi-Fi сетей Infrastructure** а) При такой организации сети все устройства подключаются к точке доступа (Access Point) б) Способ организации сети между устройствами напрямую без точки доступа. Такой способ применяется, когда нужно соединить два ноутбука или компьютера между собой	Эталон ответа а)
4.	**Тип организации Wi-Fi сетей Ad-Hoc** а) При такой организации сети все устройства подключаются к точке доступа (Access Point) б) Способ организации сети между устройствами напрямую без точки доступа. Такой способ применяется, когда нужно соединить два ноутбука или компьютера между собой	Эталон ответа б)
5.	**WEP и WPA – это** а)протоколы фильтрации данных в сетях Wi-Fi б) протокол шифрования, использующий довольно нестойкий алгоритм RC4	Эталон ответа б)
6.	**Основной компонент IIS:** а) почтовый сервер. б) веб-сервер; в) ftp-сервер;	Эталон ответа б)
7.	**Обратный прокси -** а) ускоряет обработку запросов путем	Эталон ответа в)
	предоставления данных, сохраненных во время предыдущего запроса от того же самого или других клиентов б) данный тип прокси-сервера предоставляет административный контроль за передаваемым через него содержимым в) прокси-сервер, который ставится по соседству с одним или несколькими веб-серверами	

чтению». К преимуществам это способа можно отнести несколько большую скорость работы с файлами, доступность данных (только по чтению), и сохранение целости данных во время резервного копирования. Кроме того, этот способ принадлежит к «логическому» способу резервного копирования, и поэтому каждый из файлов может быть индивидуально сохранен или восстановлен. Недостатки способа заключаются в невозможность модификации сохраняемых данных вовремя процеса резервного копирования.

- Создание «моментального снимка» файловой системы. Некоторые из файловых систем (например VxFS) позволяют создание «моментального снимка» данных для его последующего резервного копирования. После получения «снимка» данные копируются на носители со скоростью режима «только по чтению» и сохраняется общая целостность данных. Изменения файловой системы во время резервного копирования накапливаются дополнительно и по завершению процесса

«накатываются» на «снимок». К недостаткам данного способа можно отнести требование к целостности данных в момент создания «снимка», необходимость в дополнительном дисковом пространстве для накопления изменений, снижение производительности работы с файлами в момент резервного копирования и доступность данного способа только для некоторых файловых систем.

- Сохранение «активной» файловой системы. В этом случае происходит сохранение всех (даже открытых) файлов на файловой системе, совершенно прозрачно для пользователей. Сохранение

«активной» файловой системы является самой медленной операцией из всех перечисленных выше. Данные во время процесса резервного копирования могут утерять целостность, работа с открытыми файлами может потребовать дополнительных операций резервного копирования. Главное преимущество этого способа в том, что доступ к данным сохраняется как по чтению, так и по записи.

Конфигурация сети для резервного копирования.

В настоящий момент практически любое устройство резервного копирования имеет скорость чтения/записи данных на ленту превышающую скорость работы Ethernet (10 BaseT). Поэтому при планировании сетевого резервного копирования следует обратить внимание на протоколы, имеющие большую пропускную способность, такие как FastEthernet или FDDI. При использовании Solstice Backup в качестве программного обеспечения и современных ленточных накопителей легко достижима скорость передачи данных до 4 мегабайт/секунду. С такой нагрузкой легко справиться любой из перечисленных выше протоколов, в случае если единовременно вы планируете сохранять данные только с одного сервера. В случае появления второго потока данных утилизация сети станет неприемлемо большой. В этом случае возможно использование ATM, в силу его гарантированной полосы пропускания или выделенные сети резервного копирования для каждого из сетевых клиентов.

Используя трехзвенную архитектуру пакетов резервного копирования Solstice Backup или Sun Enterprise NetBackup возможно размещение нескольких узлов хранения данных в разных точках сети. В случае большого объемами данных видится благоразумным выделение одной или нескольких специализированных станций как серверов резервного копирования, расположенных в разных точках сети. Станция на базе одного процессора UltraSPARC, с оперативной памятью 128 мегабайт, ATM интерфейсом и несколькими SCSI/WIDE интерфейсами способна сохранять данные из сети на

устройства со скоростью 12-15 мегабайт в секунду.

Сетевой протокол	**Скорость передачи данных**
Ethernet (10BaseT)	0,75 MB/sec
FastEthernet (100BaseT)	7,5 MB/sec
GigabitEthernet (1000BaseT)	50 MB/sec
FDDI	8 MB/sec
ATM 155	11,6 MB/sec

силу последовательного доступа к устройству (на современных дисках эта скорость около 6-7 мегабайт в секунду). В случае использования дисковых массивов эта скорость значительно выше.

Логическое копирование понимает под собой копирование данных на более высоком, файловом уровне. В этом случае производится анализ атрибутов данных, что приводит к значительного количеству операций поиска и чтения.

В среднем потери скорости при логическом копировании достигают восьми раз по сравнению с физическим копированием. Кроме того, если операции поиска занимают большое количество времени (например на файловых серверах с большим количеством файлов) устройство не получает постоянный поток данных от системы и постоянно выполняет операции старта и останова, что весьма критично для ленточных накопителей типа helican scan (см выше). К преимуществам логического копирования можно отнести возможность отслеживания версий объектов и соответственно возможность выполнения операций икрементального копирования.

Для оценки скорости поступления данных весьма полезной может оказаться следующая таблица.

Технология	**Пиковая скорость чтения**	**Пиковая скорость записи**
4 GB 5400RPM	5,6 MB/sec	2,8 MB/sec
4 GB 7200RPM	9,3 MB/sec	4,2 MB/sec
9 GB 7200RPM	8,7 MB/sec	4,1 MB/sec

При планировании системы резервного копирования необходимо оценить такие требования системы как: целостность сохраняемых данных против доступности системы во время процесса резервного копирования. Как правило целостность данных может быть легко достигнута остановкой системы и проведением резервного копирования. В случае требования постоянной доступности системы, подлежащей резерному копированию, необходимо использование специальных инструментов (таких как создание «моментального снимка» данных, дополнительного

«зеркалирования» данных или специальных системных модулей) для обеспечения целостности сохраняемых данных.

В случае большого объема данных весьма полезно развить их на несколько секций, каждая из которых будет сохраняться и восстанавливаться индивидуально. Более важно то, что данные секции могут быть сохранены и восстановлены параллельно на несколько устройств.

Очень важен вопрос автоматизации и удаленного управления процессом резервного копирования. Согласно данным компании Marketing Research большинство компаний затрачивает в семь раз больше средств на управление и поддержку процесса резервного копирования, чем на приобретение программного и аппаратного обеспечения для него. Автоматизированные устройства и специальное программное обеспечение позволит значительно снизить эту статью расходов.

Восстановление данных. В случае восстановления данных с ленты всегда следуйте золотому правилу: защитите ленту от записи на физическом уровне перед ее использованием. Кроме того, необходимо утитывать, что операция восстановления данных порой медленнее чем сама операция резервного копирования, потому как системе необходимо производить выборки в базе индексов и поиск данных на носителях, кроме того операция записи данных на диск медленней чем операция чтения.

Резервное копирование файловой системы

Резервное копирование файловой системы может быть выполненно несколькими способами:

- Резервное копирование файловой системы на «низком» уровне. Файловая система размонтируется и данные сохраняются непосредственно с устройства на носители. При этом значительно возрастает скорость резервного копирования за счет быстрого доступа к дискам. К недостаткам данного способа относится недоступность данных во время процесса резервного копирования.
- Резервное копирование файловой системы доступной «только по чтению». Файловая система, подлежащая резервному копирования, монтируется в режиме доступа «только по

8.	**Кэширующий прокси-сервер** а) ускоряет обработку запросов путем предоставления данных, сохраненных во время предыдущего запроса от того же самого или других клиентов б) данный тип прокси-сервера предоставляет административный контроль за передаваемым через него содержимым в) прокси-сервер, который ставится по соседству с одним или несколькими веб-серверами	Эталон ответа а)
9.	**Веб-прокси, фильтрующий содержимое** а) ускоряет обработку запросов путем предоставления данных, сохраненных во время предыдущего запроса от того же самого или других клиентов б) данный тип прокси-сервера предоставляет административный контроль за передаваемым через него содержимым в) прокси-сервер, который ставится по соседству с одним или несколькими веб-серверами	Эталон ответа б)
10.	**Анонимный прокси-сервер** а) сочетает в себе функции прокси- сервера и шлюза б) применяется для анонимизации веб-серфинга, т.е. для сокрытия информации о серфере в) позволяет получить доступ к веб-страницам приписывая имя прокси-	Эталон ответа б)
	сервера к их адресу	
1.	**Прозрачный прокси** а) сочетает в себе функции прокси- сервера и шлюза б) применяется для анонимизации веб-серфинга, т.е. для сокрытия информации о серфере в) позволяет получить доступ к веб-страницам приписывая имя прокси- сервера к их адресу	Эталон ответа а)
12.	**Суффиксный прокси-сервер** а) сочетает в себе функции прокси- сервера и шлюза б) применяется для анонимизации веб-серфинга, т.е. для сокрытия информации о серфере в) позволяет получить доступ к веб-страницам приписывая имя прокси- сервера к их адресу	Эталон ответа в)

13.	**SOCKS proxy –** а) предназначен для организации работы браузеров и других программ, использующих протокол HTTP б) прокси сервер передающий абсолютно все данные от клиента к серверу, не изменяя и не добавляя ничего	Эталон ответа б)
14.	**HTTP-прокси** а) предназначен для организации работы браузеров и других программ, использующих протокол HTTP б) прокси сервер передающий абсолютно все данные от клиента к серверу, не изменяя и не добавляя ничего	Эталон ответа а)
15.	**Squid —** а) программный пакет, реализующий функцию кэширующего прокси- сервера для протоколов HTTP, FTP, Gopher и (в случае соответствующих настроек) HTTPS	Эталон ответа а)
	б) программа контроля трафика в сети и выявления неисправностей	
16.	**DeleGate –** а) программа контроля трафика в сети и выявления неисправностей б)многоцелевой прокси-сервер, работающий с различными TCP-, UDP- протоколами, такими как HTTP, HTTPS, FTP, NNTP, SMTP, SOCKS, IMAP, ICP и т. д.	Эталон ответа б)
17.	**UserGate –** а) программный пакет, реализующий функцию кэширующего прокси- сервера для протоколов HTTP, FTP, Gopher и (в случае соответствующих настроек) HTTPS б) это комплексное решение для подключения пользователей к сети Интернет, обеспечивающее полноценный учет трафика, разграничение доступа и предоставляющее встроенные средства сетевой защиты.	Эталон ответа б)
18.	**ICP** а) связывает между собой кэш-серверы в равноправно-подчиненную иерархию б) кэш-серверы отслеживаются посредством «списка членства в группе», автоматически обновляемого с помощью функции Time-to-Live (TTL), регулярно проверяющей дееспособность активных серверов.	Эталон ответа а)

Чтобы создать сеть VDC:

1. Перейдите в раздел **Data Centers**.
2. Выберите виртуальный дата-центр.
3. В блоке **Networking** перейдите в пункт **Networks**.
4. Нажмите на кнопку **NEW**.
5. В окне **New Organization VDC Network** на вкладке **Scope** выберите VDC, в котором необходимо разместить сеть.
6. На вкладке **Network type** в поле **Type** выберите тип сети:

- **Isolated network** – частная сеть без доступа в интернет;
- **Routed network** – сеть, подключаемая к шлюзу. Возможна настройка доступа в интернет (необходимо настроить правила NAT и Firewall).

7. Если выбран тип сети "Routed", на вкладке **Edge Connection** выберите подключение к Edge Gateway.
8. На вкладке **General** укажите в поле **Name** введите название сети.
9. В поле **Gateway CIDR** введите адрес шлюза по умолчанию и префикс сети. Пример: необходимо создать сеть 10.0.0.0/24 с выделением всех клиентских адресов в IP Pool. В данном случае Gateway CIDR – адрес 10.0.0.1/24.
10. В поле **Description** введите описание сети, если это необходимо.
11. (Опционально) На вкладке **Static IP Pools**:

- В поле **Static IP Pools** введите диапазон адресов, которые будут автоматически присваиваться VM при выставлении данной опции в свойствах сетевого интерфейса, и нажмите на кнопку **ADD**. Выбирайте IP-адреса из сети, указанной в **Gateway CIDR**. Адрес шлюза по умолчанию, указанный в Gateway CIDR, не должен входить в Static IP Pool. Например: 10.0.0.2 – 10.0.0.254.

Возможно назначать статические IP-адреса вручную или присваивать их с помощью DHCP.

12. (Опционально) На вкладке **DNS** заполните поля **Primary DNS**, **Secondary DNS** и **DNS Suffix**. Если есть собственный DNS-сервер, укажите его IP, например:

- первичный DNS-адрес (**Primary DNS**): 8.8.8.8;
- вторичный DNS-адрес (**Secondary DNS**): 8.8.4.4.

13. На вкладке **Ready to Complete** проверьте настройки и нажмите на кнопку **FINISH**.

№12 Установка системы резервного копирования данных

Перед выбором устройства резервного копирования и программного обеспечения необходимо не забыть и о еще одном не маловажном факторе в системе резервного копирования — конфигурации системы целиком. На данный момент накопители на магнитных лентах не всегда являются самой медленной частью системы (например скорость Sun StorEdge L3500 составляет 50 MB/sec, что быстрее или эквивалентно скорости работы ATM622). Целью данной главы является демонстрация основных принципов, основывась на которых можно спроектировать систему резервного копирования.

Самое главное

Основной момент в реализации системы резервного копирования — это постановка, реализация и соблюдение политики и правил работы системы. Для этого обычно создается некий набор документов, описывающий обязаности операторов и администратора системы резервного копирования, действия персонала при необходимости восстановления или внепланового копирования данных или реагирование персонала на случай стихиного бедствия. К работа над этими документами должны быть привлечены не только администраторы системы, но и служба безопастности предприятия и сервисные службы фирм, где приобретается техника, носители и программное обеспечение.

В дальнейшем каждый вовлеченный в процесс резервного копирования должен точно следовать этим инструкциям.

Общие принципы/вопросы конфигурации

Операции резервного копирования можно разделить на физические и логические.

Под физическим резервным копированием понимается копирование на носитель содержимого устройства на физическом уровне. В этом случае достигается значительная скорость чтения данных в

чтобы нанести ущерб, прежде чем, их обнаружат. OWASP рекомендует разработчикам вести системные журналы и выполнять оперативный контроль, а также составлять планы реагирования на нарушения, чтобы знать, что делать, когда их приложение атаковали.

№10 Настройка микросегментации сети виртуального дата-центра

№11 Настройка макросегментации сети виртуального дата-центра

Для виртуального дата-центра возможно создание дополнительных виртуальных сетей. Данные сети будут доступны для всех vApp данного VDC.

Чтобы создать сеть VDC:

1. Перейдите в раздел **Data Centers**.
2. Выберите виртуальный дата-центр.
3. В блоке **Networking** перейдите в пункт **Networks**.
4. Нажмите на кнопку **NEW**.
5. В окне **New Organization VDC Network** на вкладке **Scope** выберите сферу распространения сети: на конкретный VDC или на всю группу, состоящую из нескольких дата-центров.
6. На вкладке **Network Type** выберите тип сети:

- **Isolated network** – частная сеть без доступа в интернет;
- **Routed network** – сеть, подключаемая к шлюзу. Возможна настройка доступа в интернет.

7. Если выбран тип сети **Routed network**, на вкладке **Edge Connection**:

- Выберите Edge, к которому будет подключаться сеть.
- В поле **Interface type** выберите тип интерфейса:
- **Internal interface** – внутренний (системный) интерфейс;
- **Subinterface** – виртуальный интерфейс;
- **Distributed** – распределенный интерфейс передачи данных.

8. На вкладке **General** в поле **Name** введите название сети.
9. В поле **Description** введите описание сети, если это необходимо.
10. В поле **Gateway CIDR** введите адрес шлюза. Пример: необходимо создать сеть 10.0.0.0/24 с выделением всех клиентских адресов в IP Pool. В данном случае Gateway CIDR – адрес 10.0.0.1/24.
11. Если необходимо предоставить доступ к данной сети из всех VDC организации, включите опцию **Shared**.
12. Если необходимо включить функции одновременного использования подсети IPv4 и IPv6, включите опцию **Dual-Stack Mode**.
13. На вкладке **Static IP Pool**, если необходимо, в поле **Static IP pools** введите диапазон адресов, которые будут автоматически присваиваться VM при выставлении данной опции в свойствах сетевого интерфейса, и нажмите на кнопку **ADD**. Например: 10.0.0.2 – 10.0.0.254.
14. На вкладке **DNS** введите:

- первичный DNS-адрес (**Primary DNS**); например: 8.8.8.8, если необходимо;
- вторичный DNS-адрес (**Secondary DNS**); например: 8.8.4.4, если необходимо;
- DNS-суффикс (**DNS suffix**), если необходимо.

Примечание

Primary DNS – это авторитетный сервер, хранящий главную копию файла данных зоны, сопровождаемую администратором системы.

Secondary DNS – также авторитетный, но копирует главный файл зоны с первичного сервера.

15. На вкладке **Ready to Complete** проверьте технические характеристики создаваемой сети и нажмите на кнопку **FINISH**.

NSX-T

Примечание

По умолчанию уже создана сеть с адресацией 192.168.100.0/24. Она подключена к Edge Gateway. Последующие действия описывают создание только дополнительных сетей, если они необходимы или если стандартная адресация не подходит.

Для виртуального дата-центра возможно создание дополнительных виртуальных сетей. Данные сети будут доступны для всех vApp данного VDC.

19.	**CARP** а) связывает между собой кэш-серверы в равноправно-подчиненную иерархию б) кэш-серверы отслеживаются посредством «списка членства в группе», автоматически обновляемого с помощью функции Time-to-Live (TTL), регулярно проверяющей	Эталон ответа б)
	дееспособность активных серверов.	
20.	**Squid** а) позволяет создавать иерархию Proxy (иерархию кэшей) б) не позволяет создавать иерархию Proxy (иерархию кэшей)	Эталон ответа а)
21.	**Брандмауэр - это** а) специальная служебная программа, предназначенная для контроля за сетевыми интерфейсами, контролирует выход программ в интернет, является своего рода защитой от проникновения вирусов и предотвращает их распространение. б) специальный антивирусный пакет	Эталон ответа а)
22.	**Трансляция ip NAT** а) позволяет узлу, который не имеет действительного, зарегистрированного глобального уникального IP адреса, автоматически получать IP адреса на сервере б) позволяет узлу, который не имеет действительного, зарегистрированного глобального уникального IP адреса, осуществлять связь с другими узлами через сети передачи данных.	Эталон ответа б)
23.	**Трансляция ip NAT бывает** а) Статическая трансляция NAT б) Динамическая трансляция NAT в) Трансляция на основе портов PAT	Эталон ответа а), б), в)
24.	**Веб-сервер —** а) это сервер, обслуживающий запросы к одному или нескольким сайтам Всемирной паутины (веб-сайтам) б) это HTML-страницы, изображения, файлы, медиа-потоки или другие данные, которые необходимы клиенту в) программа, обрабатывающая сообщения, которые приходят на 80-й порт (стандартная настройка; можно конечно, настроиться и на любой другой порт), и работающая с	Эталон ответа а), в)
	протоколом HTTP (Hypertext Transfer Protocol)	

25.	**Функции WEB-сервера** а) управление передачей документов; б) ведение журнала активности клиентов; в) контроль активности пакетов в сети; г) поддержание безопасности данных; д)обеспечение работы средств интерактивной работы с клиентом.	та а), б), г), д)
26.	**IIS - это** а) Веб сервер б) Протокол в) Устройство передачи данных	Эталон ответа а)
27.	**Microsoft SQL Server** а) система управления реляционными базами данных (СУРБД), разработанная корпорацией Microsoft б) язык программирования высокого уровня для баз данных	Эталон ответа а)

5.2 Фонд оценочных средств для проведения промежуточного контроля

Вопросы к экзамену

. Как называется комбинация IP-адреса и номера порта?

. Какое устройство, преобразует аналоговый сигнал в цифровой и обратно?

. В каких файловых системах возможно включение управления квотами в Windows Server ?

. Для удаленного подключения к компьютеру с IP адресом 192.168.0.5 необходимо ввести команду

. DNS (Domain Name System) - это…

. Вы добавили к вашей сети еще 20 компьютеров. Сеть разбита концентратором на два сегмента, длина каждого из них не превышает допустимую стандартом. Однако сеть работает крайне нестабильно и медленно, сигнализатор коллизий на концентраторе горит почти постоянно. Как с наименьшими затратами восстановить работоспособность сети?

. Сколько жил используется в витой паре при передаче данных в сети Ethernet?

. Где могут быть использованы сетевые ресурсы?

. Какая команда используется в ОС Windows для подключения удаленного ресурса в качестве локального диска?

0. Какой тип кабеля наиболее восприимчив к электромагнитным помехам?

1. К основным возможностям сетевых операционных систем можно отнести

2. Что позволяет технология использования кэширования?

3. Как называется *и*ерархически построенная база данных параметров и настроек в большинстве операционных систем?

функции в коде, которые не используются, и сделав так, чтобы сообщения об ошибках были более общего характера.

7. Межсайтовый скриптинг

Уязвимости, связанные с межсайтовым скриптингом возникают тогда, когда веб-приложение разрешает пользователям добавлять пользовательский код в URL-адрес или на веб-сайт, который будут видеть и другие пользователи. Эту уязвимость можно использовать для того, чтобы запустить вредоносный код JavaScript в браузере жертвы атаки. Например, злоумышленник может отправить жертве письмо по электронной почте от доверенного банка, в котором будет находиться ссылка на веб-сайт этого банка. Эта ссылка может содержать вредоносный код JavaScript, добавленный в конце URL-адреса. Если сайт этого банка не защищен как следует от межсайтового скриптинга, то этот вредоносный код запуститься в веб-браузере жертвы, когда она перейдет по ссылке.

Для того, чтобы смягчить последствия межсайтового скриптинга, рекомендуется избегать ненадежных HTTP-запросов, а также проверять и/или пользовательский контент. Также современные среды разработки, такие как ReactJS и Ruby on Rails, имеют определенную встроенную защиту от межсайтового скриптинга.

8. Небезопасная десериализация

Целью этой угрозы является множество веб-приложений, которые часто сериализуют и десериализуют данные. Сериализация – это получение объектов из кода приложения и их преобразование в формат, который можно использовать для других целей, например, для сохранения данных на диск или потоковой передачи данных. Десериализация – это противоположный процесс, то есть преобразование сериализованных данных обратно в объекты, которые сможет использовать приложение. Сериализация чем-то похожа на упаковку мебели в коробки, когда вы переезжаете, а десериализация, соответственно, - на распаковку этих коробок и сборку мебели после того, как вы уже переехали. В таком контексте небезопасную десериализацию можно представить, как, если бы грузчики повредили содержимое коробок до того, как их распакуют.

Небезопасная десериализация – это результат десериализации данных из ненадежных источников, и она может привести к серьезным последствиям, таким как DDoS-атаки и атаки с целью выполнения кода. Несмотря на то, что можно предпринять некоторые шаги, чтобы найти злоумышленников, например, обеспечить контроль за десериализацией и проводить проверки соответствия типов, единственным надежным способом защититься от подобного рода проблем – запретить десериализацию из ненадежных источников.

9. Использование компонентов с известными уязвимостями

Многие современные веб-разработчики в своих веб-приложениях используют такие компоненты, как библиотеки и фреймворки. Эти компоненты – это части программного обеспечения, которые помогают разработчикам избежать лишней работы и обеспечить приложение необходимой функциональностью; распространенный пример таких компонентов - «клиентские» фреймворки, такие как React, и небольшие библиотеки, которые используются для общих условных обозначений или A/B тестирования. Некоторые злоумышленники ищут уязвимости именно в этих компонентах, чтобы потом иметь возможность организовывать атаки. Некоторые их самых популярных компонентов используются сотнями тысяч веб-сайтов; злоумышленник, который найдет брешь в системе безопасности хотя бы одного из этих компонентов, сможет сделать сотни тысяч сайтов уязвимыми для эксплойтов.

Разработчики компонентов регулярно предоставляют исправления и обновления для устранения известных уязвимостей, но разработчики веб-приложений не всегда используют исправленные или самые последние версии компонентов в своих приложениях. Чтобы минимизировать риск запуска компонентов с известными уязвимостями, разработчикам следует удалять из своих проектов компоненты, которые они не используют, а также брать компоненты только из надежного источника и постоянно их обновлять.

10. Неудовлетворительное ведение системного журнала и невыполнение оперативного контроля

Многие веб-приложения предпринимают не достаточное количество действий для того, чтобы можно было обнаружить утечку данных. Среднее время обнаружения утечки составляет примерно 200 дней с момента, как она произошла. У злоумышленников есть достаточно времени,

Некоторые стратегии устранения уязвимостей в аутентификации подразумевают использование двухфакторной аутентификации (2FA - two-factor authentication), а также ограничения или задержки повторных попыток входа в систему с помощью ограничения скорости.

3. Раскрытие конфиденциальных данных

Если веб-приложение никак не защищает конфиденциальные данные, такие как финансовые сведения и пароли, то злоумышленники могут получить доступ к этим данным и использовать их в гнусных целях. Один из самых популярных методов кражи конфиденциальной информации – это атака «по пути».

Потенциальный риск раскрытия данных можно минимизировать, если зашифровать все конфиденциальные данные и отключить кэширование* любой такой информации. Кроме того, разработчики веб-приложений должны позаботиться о том, чтобы без необходимости конфиденциальные данные в приложениях не хранились.

*Кэширование – это способ временного хранения данных для их повторного использования. Например, веб-браузеры часто кэшируют веб-страницы, так что, если пользователь повторно посещает эти страницы в течение какого-то фиксированного промежутка времени, у браузера нет необходимости снова загружать их из Интернета.

4. Атака на внешние сущности XML (XEE – XML External Entities)

Это атака на веб-приложение, которое анализирует ввод XML*. Этот ввод может иметь ссылки на внешние сущности, которые пытаются использовать уязвимость в синтаксическом анализаторе. Под

«внешней сущностью» в данном контексте подразумевается устройство хранения, например, жесткий диск. Синтаксический анализатор XML можно обманным путем заставить отправить данные неавторизованной внешней сущности, которая в свою очередь может передать эти данные злоумышленнику.

Лучший способ предотвратить XEE-атаки – это передавать веб-приложению данные менее сложного типа, например, JSON**, или хотя бы исправить синтаксические анализаторы XML и перестать использовать внешние сущности в XML-приложении.

*XML, или Extensible Markup Language (что переводится как «расширяемый язык разметки») – это язык разметки, который является удобным для восприятия человеком и машиночитаемым.

Поскольку он довольно сложный и у него есть уязвимости с точки зрения безопасности, его постепенно перестают использовать.

**Нотация объектов JavaScript, или JSON – это тип простой и удобной для восприятия человеком нотации, которую часто используют для передачи данных через Интернет. Несмотря на то, что изначально он был создан для JavaScript, JSON не зависит от языка и может интерпретироваться различными языками программирования.

5. Нарушенное управление доступом

Управление доступом относится к системе, которая контролирует доступ к информации или функциям. Неисправные средства контроля доступа позволяют злоумышленникам обходить авторизацию и выполнять какие-то задачи, как если бы они были пользователями с привилегиями, например, администраторами. Например, веб-приложение может позволить пользователю поменять учетную запись, в которую он вошел, просто изменив часть URL-адреса без какой-либо дополнительной проверки.

Средства управления доступом можно защитить с помощью маркеров авторизации*, которые должны использовать веб-приложения, и строгого контроля за ними.

*Многие службы, когда пользователь входит в систему, предоставляют маркеры авторизации. Каждый привилегированный запрос, который делает пользователь, требует, чтобы у этого пользователя был маркер авторизации. Это безопасный способ убедиться, что пользователь является тем, за кого себя выдает, и при этом не нужно вводить свои учетные данные для входа в систему.

6. Неверная конфигурация безопасности

Неверная конфигурация безопасности – это самая распространенная уязвимость из данного списка, и она часто является результатом того, что в приложении используются конфигурации по умолчанию или отображаются чересчур подробные сообщения об ошибках. Например, приложение может показать пользователю излишне содержательное сообщение об ошибке, что может помочь в выявлении уязвимостей в приложении. Этого можно избежать, удалив все

4. попытались начать сеанс на одном из компьютеров домена - User1, но получили системное сообщение о том, что контроллер домена недоступен или не найдена учетная запись компьютера. С помощью «Active Directory Users and Computers» Вы определили, что учетная запись компьютера User1 отключена. Какое решение позволит максимально оперативно решить проблему по разрешению входа на данный компьютер?

5. Клиент (Client) - это…

6. Что представляет из себя тонкий клиент?

7. На каком уровне коммуникационной модели OSI функционируют Telnet и SMTP?

8. наиболее быстро узнать, работает и подключен к сети компьютер с ipадресом 192.168.37.2 ?

9. Пользователь маршрутизируемой сети сконфигурировал TCP/IP вручную и правильно ввел IP адрес и маску подсети. Шлюз по умолчанию был введен неверно. Каким будет результат приведенной выше последовательности действий?

20. К какому классу сети принадлежит компьютер с адресом 115.23.46.34 ?

21. Какой символ используется для создания скрытого ресурса в операционной системе Windows?

22. Какие два действия следует предпринять, чтобы защитить профили пользователей от несанкционированного просмотра?

23. Какой тип тома следует выбрать для хранения критически важной информации, которая должна быть доступна в течение рабочего дня, при условии, что на жестком диске должно быть как можно больше свободного места?

24. Что обязательно нужно присвоить открывая общий доступ к папке ?

25. необходимо чтобы получить удаленный доступ к рабочему столу Windows с использованием встроенных механизмов Windows?

Ситуационное исследование.

1. Проверьте состояние связи с двумя узлами: www.ya.ru и www.intuit.ru;

В качестве результата отразить для каждого из исследуемых узлов в виде таблицы:

№ п/п	Процент потерянных пакетов	Среднее время приема-передачи	Количество маршрутизаторов (с учетом шлюза) до опрашиваемого узла	IP адрес узла	Класс сети, к которой принадлежит данный узел	Имя узла, полученное по IP адресу узла
1.						

2.						

2. Провести трассировку двух работоспособных узлов: www.ya.ru и www.intuit.ru. Результат запротоколировать в таблице:

№ узла	Время прохождения пакета № 1	Время прохождения пакета № 2	Время прохождения пакета № 3	Среднее время прохождения пакета	DNS – имя маршрутизатора	IP – адрес маршрутизатор а
1.						
2.						

3. Установите и настройте сервер DNS (выполните предварительную конфигурацию компьютера, на котором будет установлен сервер DNS: проверьте, что серверу DNS назначен статический IP адрес (например, 192.168.1.1));

4. Создайте зону прямого просмотра myzone.ru.

5. Используя программу виртуализации для ОС VirtualBox, с установленной операционной системой Windows Server и Windows выполните следующее задание: Установите DHCP сервер, который имеет статически заданный IP адрес 192.168.1.1, компьютер пользователя (клиентская машина) автоматически получает настройки от DHCP сервера; Сконфигурируйте DHCP сервер: введите имя области IP адресов, которые вы будете раздавать клиентским машинам.

6. Используя программу виртуализации для ОС VirtualBox, с установленной операционной системой Windows выполните следующее задание: Произведите установку серверной операционной системы Windows Server; Произведите начальную настройку Windows Server.

7. Используя программу виртуализации для ОС VirtualBox, с установленной операционной системой Windows Server и Windows выполните следующее задание: Произведите назначение роли серверу (Windows Server)- назначьте серверу роль «Контроллер домена». Используйте полное DNS– имя нового домена – mydomain.com; Произведите начальную настройку Windows Server ; Выполните настройку сетевого интерфейса (IP – адрес – 192.168.1.2 , Маска подсети – 255.255.255.0, Основной шлюз -192.168.1.1); Добавьте компьютер с Windows в новый домен.

8. Используя программу виртуализации для ОС VirtualBox, с установленной операционной системой Windows Server и Windows выполните следующее задание: Установите и настройте файловый сервер (размер квот – 50 Мб, предупреждение о квоте – 40 Мб, при превышении дискового пространства – не выделять место на диске); Установите и настройте web-сервер; Установите и настройте ftp – сервер.

9. Используя программу виртуализации для ОС VirtualBox, с установленной операционной системой Windows Server и Windows выполните следующее задание: Выполните резервное копирование системных конфигурационных файлов; Выполните восстановление системных конфигурационных файлов; Создайте точку восстановления

Используя программу виртуализации для ОС VirtualBox, с установленной операционной системой Windows Server и Windows выполните следующее задание:

10. Установите Active Directory;

a) Создайте новый каталог (подразделение/контейнер) в корне сервера;

b) Создайте новую учетную запись пользователя в ранее созданном контейнере;

c) Создайте группу пользователей в ранее созданном контейнере;

d) Включите созданного ранее пользователя во вновь созданную группу;

e) Выполните редактирование политики безопасности домена, созданную автоматически;

Например, вы хотите ограничить одновременное количество подключений на отметке в 30, а временной отрезок для одновременного количества подключений лимитирован 3 секундами. Конфигурация выглядит следующим образом:

limit_conn_zone $binary_remote_addr zone=perip: 30m; limit_req_zone $binary_remote_addr zone=dynamic:30m rate=3r/s;

Конфигурация пропустит только 3 запроса в секунду, а остальные станут в очередь. Значение очереди задается параметром burst. Например, значение burst равно 7. Когда количество запросов будет выше 10, модуль поставит 7 запросов в очередь, а остальные завершатся с ошибкой.

Программный фильтр. «Глушим» DDoS-атаки

Защита от DDoS-атак сервера возможна с помощью веб-приложений. Программный фильтр трафика использует JavaScript, недоступный ботам, поэтому DDoS-атаки упираются в страницу-заглушку.

Работа фильтра предельно проста. В конфигурации указываются условия для блокировки ботов, и, когда посетитель отвечает указанным условиям, он перенаправляется на страницу-заглушку, вместо запрашиваемой страницы. Фильтр позволяет указать причину перенаправления.

Облачные сервисы для защиты от DDoS-атак

Корпоративные сайты часто становятся целью атак, и бесплатных инструментов защиты бывает недостаточно. Для бизнеса простой сайта выливается в потерю прибыли и потенциальных клиентов. Timeweb Cloud предлагает эффективное решение – защита от DDoS. Вы получите гарантию защиты от 99% атак, включая сложные и мощные атаки на ваш ресурс. Решение фильтрует весь входящий трафик и обеспечивает обнаружение и отражение атак на сетевом уровне L3/4 и на уровне приложений L7.

№9 Моделирование угроз инфраструктуры по списку OWASP TOP 10 OWASP Top-10 – это отчет, который постоянно обновляется и в котором в общих чертах описываются проблемы безопасности веб-приложений с акцентом на 10 самых важных. Отчет составлен группой экспертов по безопасности со всего мира. OWASP называет Top-10

«предупреждающим документом» и рекомендует всем компаниям взять его на вооружение в своей работе, чтобы свести к минимуму и/или устранить угрозы безопасности.

Ниже приведены угрозы безопасности, которые описаны в отчете OWASP Top-10 за 2017 год.

1. Инъекционная атака

Инъекционные атаки происходят в тот момент, когда ненадежные данные отправляются интерпретатору кода через форму ввода данных или какими-то другими путями. Например, злоумышленник может ввести код базы данных SQL в форму, которая предполагается для ввода имени пользователя. Если данная форма не защищена как положено, то это приведет к выполнению этого кода SQL. Такая атака известна как атака путем внедрения кода SQL, или SQL-инъекция.

Инъекционные атаки можно предотвратить путем проверки и/или очистки данных, которые отправляет пользователь. (Проверка подразумевает отклонение подозрительных данных, а очистка – удаление подозрительных частей данных.) Кроме того, администратор баз данных может настроить элементы управления для того, чтобы свести к минимуму объем информации, который может быть получен в результате инъекционной атаки.

2. Нарушенная аутентификация

Уязвимости в системах аутентификации (входа) могут позволить злоумышленникам получить доступ к учетным записям пользователей или даже скомпрометировать всю систему с помощью учетной записи администратора. Например, злоумышленник может взять список с тысячами известных комбинаций имени пользователя и пароля, которые были получены во время утечки данных, и написать скрипт, чтобы попробовать все эти комбинации в системе входа с целью проверить, есть ли среди них те, которые работают.

или подсети.

• IPRange. Задает диапазон IP-адресов, не воспринимаемых инструментом в качестве подсети. Также в IPTables можно использовать критерии Owner, State, TOS, TTL, Unclean Match, чтобы задать персонализированные настройки, эффективно защищая свой ресурс от DDoS-атак.

Модуль ядра ipset позволяет сделать список адресов, нарушающих указанный лимит подключений. Параметр ipset timeout установит временное ограничение для созданного списка, достаточное, чтобы переждать DDoS-атаку.

Важно! Стандартные настройки IPTables возвращаются к базовым после перезагрузки системы. Сохранить установленные настройки помогут дополнительные утилиты (iptables-save или iptables- persistent), но рекомендуется начинать с опций по умолчанию, чтобы не сохранить настройки с ошибками, блокирующими доступ к серверу вообще всем.

ConfigServer Security and Firewall. Простая и понятная DDoS-защита сервера

IPTables – удобный и эффективный инструмент, хотя довольно сложен в настройке. Придется разобраться с управлением, дополнительными скриптами, а если что-то пойдет не так, то ваш ресурс станет «закрытым клубом» для нескольких пользователей.

CSF – это конфигуратор «под ключ», где вам достаточно задать правильные параметры и не беспокоиться о безопасности сервера.

Установка серверного файрвола

Предварительный этап установки – загрузка двух дополнительных компонентов, обеспечивающих работу CSF: интерпретатора Perl и библиотеки libwww. Следующий шаг – непосредственно установка ConfigServer Security and Firewall. Инструмент отсутствует в официальном репозитории, поэтому придется скачать его по ссылке или загрузить уже готовый архив:

```
cd /usr/src
wget https://download.configserver.com/csf.tgz
```

Распакуйте архив и переместите его в папку с файлами защитника, затем выполните установку инструмента. При условии отсутствия ошибок переходите к настройке CSF.

Настройка серверного файрвола

Стандартные настройки ConfigServer and Firewall активны в течение 5 минут, после чего все измененные конфигурации сбрасываются. Тестовый формат удобен для проведения экспериментов и понимания ошибок установленной конфигурации. Изменение значения Testing на 0 переводит инструмент в рабочий режим.

Основные параметры конфигурации

Правильная настройка конфигурации обеспечит надежную защиту от DDoS-атак сервера. Основные команды в CSF:

• Указать входящие порты:

TCP_IN = "22,23,25,36,75,87”

• Указать исходящие порты:

TCP_IN = "22,23,25,36,75,87”

•Настройка почтовых оповещений (подключение к SSH сопровождается отправкой уведомления на почту):

• Добавление IP-адреса в список исключений (актуально для команды, обслуживающей сервер):

csf -a 192.168.0.7

• Запрещение на подключение к серверу для конкретного IP-адреса:

csf -d 192.168.0.6

Модули Nginx. Пример настройки конфигурации

Как защитить сервер от DDoS-атак еще более простыми способами? Используйте модули nginx (limit_conn и limit_req). Первый модуль отвечает за ограничение максимального количества подключений к серверу, а второй – лимитирует количество подключений за определенный временной отрезок.

f) Присоедините клиентскую машину под управлением Windows к домену;

11. Используя программу виртуализации для ОС VirtualBox, с установленной операционной системой Windows Server 2008 и Windows выполните следующее задание:

1. Создайте новый домен cpandl.com.
2. Добавьте новые учетные записи, со следующими параметрами:

Имя учетной записи	Имя входа пользователя	Адрес электронной почты	Группа
ADRMSSRVC	ADRMSSRVC		
ADRMSADMIN	ADRMSADMIN		Администраторы предприятия
Nicolai	NHOLLIDA	nhollida@cpandl.com	Сотрудники Финансы
Andrey	SRAILSON	adnry@cpandl.com	Инженеры

12. Используя программу виртуализации для ОС VirtualBox, с установленной операционной системой Windows Server 2008 выполните следующее задание:

a) Установите роль сервера Файловые службы (File Services)
b) Установите следующие дисковые квоты,
c) С использованием групповой политики: Предел 200 Мб с уведомлением пользователя
d) Назначьте общий доступ к папкам, используя проводник Windows.
e) Назначьте общий доступ к папкам, используя мастер подготовки общих папок.

13. В организации, состоящей из трех отделов, необходимо модернизировать локальную сеть и произвести подключение к Интернету. В первом отделе планируется добавить 5 персональных компьютеров и один принтер, во втором отделе – добавить 10 персональных компьютеров и мультимедийный проектор, в третьем отделе- 2 персональных компьютера и один принтер. Все отделы расположены на разных этажах. Вам необходимо составить опросный

лист, для выяснения потребностей организации и произвести расчет потребности организации в аппаратном и программном обеспечении;

14. В крупной организации, занимающейся продажей строительных материалов, необходимо организовать корпоративную сеть. Офисы организации «разбросаны» по районам города. Всего имеется 5 офисов. В каждом офисе имеется административный отдел и отдел по работе с клиентами. В головном отделе так же имеется отдел бухгалтерии. В каждом отделе планируется использовать от двух до пяти компьютеров. Вам необходимо составить проектную документацию по расчету потребности организации в аппаратном (в том числе и сетевом) и программном обеспечении, а также необходимо рассчитать стоимость лицензионного ПО;

15. В крупной организации, занимающейся продажей строительных материалов, необходимо организовать корпоративную сеть. Офисы организации «разбросаны» по районам города. Всего имеется 5 офисов. В каждом офисе имеется административный отдел и отдел по работе с клиентами. В головном отделе так же имеется отдел бухгалтерии. В каждом отделе планируется использовать от двух до пяти компьютеров. Вам необходимо составить проектную документацию по расчету потребности организации в аппаратном (в том числе и сетевом) и программном обеспечении, а также необходимо рассчитать стоимость лицензионного ПО;

16. Используя программу виртуализации для ОС VirtualBox, с установленной операционной системой Windows Server 2008 выполните следующее задание:

a) Настройте аудит Active Directory сервера;

17. В сети 190. 48. 0. 0. необходимо выделить подсети, так что бы к каждой подсети можно было подключить до 63 хостов. Какую маску подсети следует выбрать, чтобы допустить рост числа сетей в будущем? Назначить первые пять IPадресов первой подсети.

18. В сети класса B, разделенной на 30 подсетей, необходимо добавить 25 новых подсетей в ближайшие два года. В каждой подсети необходимо подключить до 600 хостов. Какую маску подсети следует выбрать? Назначить первые пять IPадресов первой подсети

19. Используя программу виртуализации для ОС VirtualBox, с установленной

операционной системой Windows Server и Windows выполните следующее задание: Установите DHCP сервер, который имеет статически заданный IP адрес 192.168.1.1, компьютер пользователя (клиентская машина) автоматически получает настройки

от DHCP сервера; Сконфигурируйте DHCP сервер: введите имя области IP адресов, которые вы будете раздавать клиентским машинам.

20. Установите и настройте сервер DNS (выполните предварительную конфигурацию компьютера, на котором будет установлен сервер DNS: проверьте, что серверу DNS назначен статический IP адрес (например, 192.168.1.1);

	isolation.tools.unity.taskbar.disable, isolation.tools.unity.windowcontents.disable, isolation.tools.unityactive.disable, isolation.tools.unityinterlockoperation.disable, isolation.tools.vixmessage.disable, isolation.tools.vmxdndversionget.disable, log.keepold, log.rotatesize, remotedisplay.maxconnections, remotedisplay.vnc.enabled, tools.guestlib.enablehostinfo, tools.setinfo.sizelimit, vmsafe.agentaddress, vmsafe.agentport, vmsafe.enable

№7 Развёртывание защиты от DoS атак Настройка режима защиты от DoS-атак

Включение и настройку режима защиты от DoS-атак выполняют в окне редактирования правила фильтрации. При этом осуществляется контроль параметров состояния соединений. Этот режим действует для данного правила при наличии следующих условий:

поле "Действие" содержит значение "Пропустить";

установлена отметка в поле "Контролировать состояние соединения".

Для настройки параметров правила фильтрации:

1. В окне редактирования правила фильтрации установите отметку в поле "Защита от DoS-атак" и нажмите кнопку "Параметры...".

На экране появится диалог "Параметры защиты от DoS-атак".

2. Заполните поля диалога и нажмите кнопку "OK".

Ограничить количество соединений	Максимальное количество соединений, которое может быть установлено по указанному правилу фильтрации
Тайм-аут соединений	Время, по истечении которого неактивное соединение будет автоматически разорвано
Ограничить интенсивность соединений/сек.	Количество новых соединений, регистрируемых для данного правила, в секунду

№8 Развёртывание защиты от DDoS атак Эффективные инструменты защиты сервера от DDoS-атак

Если не использовать решения, предлагаемые хостингами, платные сервисы и программы, защитить сервер от DDoS-атак помогут:

- IPTables;
- CSF (ConfigServer Security and Firewall);
- Модули Nginx;
- Программный фильтр.

IPTables. Блокировка ботов по IP-адресам

Инструмент IPTables помогает защитить сервер от простейших DDoS-атак. Основная функция – фильтрация входящего трафика через специальные таблицы. Владельцу ресурса доступна возможность добавления таблиц.

В каждой таблице содержится свод правил, регулирующий поведение инструмента в конкретной ситуации. По умолчанию варианта реагирования всего два: ACCEPT (открытие доступа) и REJECT (блокировка доступа).

В IPTables можно настроить предельное количество подключений. Когда с одного IP-адреса поступит больше подключений, инструмент заблокирует ему доступ к ресурсу. Расширить функционал инструмента можно дополнительными критериями:

- Limit. Устанавливает ограничение для подключения пакетов за выбранную единицу времени.
- Hashlimit. Работает по аналогии с критерием Limit, но действие распространяется уже на группы хостов, подсети и порты.
- Mark. Используется для пометки пакетов, ограничения трафика и фильтрации.
- Connlimit. Ограничивает количество одновременных подключений для одного IP-адреса

Оперативная память	memsize, mem.hotadd, sched.mem.max, sched.mem.min, sched.mem.minsize, sched.mem.shares
Настройки дисплея и видеопамяти	mks.enable3d, svga.autodetect, svga.maxheight, svga.maxwidth, svga.numdisplays, svga.present, svga.vramsize
Настройки контроллеров SCSI	Атрибуты, соответствующие регулярному выражению scsi(\d+)\.(?:present|sharedbus|virtualdev)
Настройки контроллеров SATA	Атрибуты, соответствующие регулярному выражению sata(\d+)\.(?:present|pcislotnumber)
Настройки HDD	Атрибуты, соответствующие регулярному выражению (?:scsi|sata|ide)(\d+:\d+)\..+
Настройки CD/DVD	Атрибуты, соответствующие регулярному выражению (?:ide|sata)(\d+:\d+)\..+
Дисковод Floppy	Атрибуты, соответствующие регулярному выражению floppy(\d+)\..+
Настройки PCI устройств	Атрибуты, соответствующие регулярному выражению pcipassthru(\d+)\..+
Настройки сетевых адаптеров	Атрибуты, соответствующие регулярному выражению ethernet(\d+)\..+
Настройки последовательных портов	Атрибуты, соответствующие регулярному выражению serial(\d+)\..+
Настройки параллельных портов	Атрибуты, соответствующие регулярному выражению parallel(\d+)\..+
Настройки контроллеров и устройств USB	ehci.present, usb.present, usb_xhci.present атрибуты, соответствующие регулярному выражению usb\.autoconnect\.device\d+
Контроль протокола VMCI	vmci.filter.enable, vmci0.id, vmci0.present, vmci0.unrestricted
Параметры, контролируемые политиками безопасности vGate	isolation.bios.bbs.disable, isolation.device.connectable.disable, isolation.device.edit.disable, isolation.ghi.host.shellaction.disable, isolation.monitor.control.disable, isolation.tools.autoinstall.disable, isolation.tools.diskshrink.disable, isolation.tools.diskwiper.disable, isolation.tools.disptoporequest.disable, isolation.tools.dnd.disable, isolation.tools.getcreds.disable, isolation.tools.ghi.autologon.disable, isolation.tools.ghi.launchmenu.change, isolation.tools.ghi.protocolhandler.info.disable, isolation.tools.ghi.trayicon.disable, isolation.tools.guestdndversionset.disable, isolation.tools.memschedfakesamplestats.disable, isolation.tools.paste.disable, isolation.tools.setguioptions.enable, isolation.tools.trashfolderstate.disable, isolation.tools.unity.disable, isolation.tools.unity.push.update.disable,
Параметр политики	**Атрибуты VMX-файла**

ПМ 03 Эксплуатация объектов сетевой инфраструктуры.

1. Назначение

Спецификацией устанавливаются требования к содержанию и оформлению вариантов теста.

Тест входит в состав комплекса оценочных средств и предназначен для *промежуточного* контроля, оценки знаний и умений аттестуемых, соответствующих основным показателям оценки результатов подготовки по программе учебной дисциплины «Операционные системы и среды» основной профессиональной образовательной программы по специальности 09.02.07 «Информационные системы и программирование».

2. Контингент аттестуемых: обучающиеся ОГБОУ СОТА.

3. Форма и условия аттестации: в электронном виде на ПК после изучения разделов 1 - 5.

4. Время тестирования:

выполнение 60 мин.

5. Перечень объектов контроля и оценки

Наименование объектов контроля и оценки	Уровень усвоения	Литера категории действия	Количество учебных задач
У1 Создание и мониторинг процессов.	3	А	3
У2 Создание учетных записей пользователей, групп.	3	А	3
У3 Планирования учетных записей пользователей, групп.	3	А	3
У4 Настройка параметров пароля.	3	А	3
У7 Диагностика работы компьютерной сети.	3	А	2
У8 Выполнение аудита ресурсов сети.	3	А	2
З1 Основные функции администрирования вычислительных сетей.	1	В	2
З2 Основные функции контроллера домена.	2	П	2
З6 Основные шаблоны планирования учетных записей, специализированные утилиты.	3	А	3
З7 Основные правила выбора параметров пароля	2	П	2
Итого:			25

6. Структура теста

Тест
В – 1

Блок задач с выбором ответа (ВО)
Количество заданий 4

Задача 1, 6, 10, 20

Набор административного инструментария, используемый для управления компьютером, называется

Варианты ответов:

1 оснастка «Управление компьютером»
2 элемент «Служебные программы»
3 оснастка консоли
4 элемент «Свойства системы»

Ответ: оснастка «Управление компьютером»

Блок задач на установление последовательности (УП)
Количество заданий 6

Задача 2, 8, 13, 16, 18, 23

Осуществите переключение пользователя стандартными средствами ОС серии Windows

Запишите ответ в виде последовательности объектов/понятий.
Объекты/понятия:

1 Активизация кнопки «Пуск»
2 Активизация вкладки «Завершение сеанса»
3 Выбор учетной записи нового пользователя
4 Активизация учетной записи нового пользователя
5 Выбор параметра «Смена пользователя»

Ответ: 12534

Блок задач на установление соответствия (УС)
Количество заданий 5

Задача 4, 12, 15, 22, 24

Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца.

Объекты

1 Поток	А Вытесняющее планирование
2 Алгоритм планирования	Б Синхронизация потоков
3 Мультипрограммирование	В Единица работы ОС
4 Блокирующая переменная	Г Способ организации вычислительного процесса
5 Динамический планировщик ОС	Д Реализация алгоритма планирования

Определите соответствующие пары объектов и запишите в виде: число-буква

Ответ: 1 2А, 2 4Б, 3 1В, 4 3Г, 5 5Д

Блок задач с кратким ответом (КО)
Количество заданий 10

Задача 3, 5, 7, 9, 11, 14, 17, 19, 21, 25

Статус	Описание и доступные операции
Отключен	Контроль целостности для ВМ не настроен
Ошибка подсчета	В процессе подсчета контрольных сумм произошла ошибка. В зависимости от ошибки следует дождаться изменения статуса или выполнить согласование повторно. Если согласование недоступно, кнопка "Согласовать" будет недоступна
Целостность нарушена	Целостность ВМ нарушена. Подробности о событии можно найти в сообщениях журнала событий (см. Просмотр журнала событий). При этом отклонение изменений недоступно, возможно только согласование изменений
В процессе согласования	Запущен процесс согласования изменений и расчет новых эталонных контрольных сумм
Целостность согласована	Согласование изменений выполнено
Изменен VMX- файл	VMX-файл был изменен. Можно выполнить согласование или отклонение изменений

Контролируемые атрибуты VMX-файла

Политика "Доверенная загрузка виртуальных машин vSphere" может быть настроена для контроля параметров VMX-файла (отмечены один или несколько пунктов в списке "Контроль конфигурации ВМ", см. Настройка объектов контроля). В этом случае при проверке изменений параметров ВМ сравниваются не только контрольные суммы файлов конфигурации, но и значения отдельных атрибутов VMX-файла. Проверка изменения значений выполняется для набора предопределенных атрибутов и атрибутов, соответствующих регулярному выражению. В таблице ниже перечислены параметры политики "Доверенная загрузка виртуальных машин vSphere" и соответствующие им атрибуты VMX-файла.

Параметр политики	Атрибуты VMX-файла
щие настройки виртуальной машины	bios.bootdelay, bios.bootretry.delay, bios.bootretry.enabled, bios.forcesetuponce, chipset.onlinestandby, disable_acceleration, displayname, firmware, guestos, logging, monitor.virtual_exec, monitor.virtual_mmu, powertype.poweroff, powertype.poweron, powertype.reset, powertype.suspend, sched.swap.hostlocal, tools.synctime, tools.upgrade.policy, toolscripts.afterpoweron, toolscripts.afterresume, toolscripts.beforepoweroff, toolscripts.beforesuspend, uuid.bios, vmx.buildtype, wwn.enabled, wwn.node, wwn.port, wwn.type, bios440.filename, config.version, extendedconfigfile, nvram, sched.swap.derivedname, vc.uuid, virtualhw.version атрибуты, соответствующие регулярному выражению
Параметр политики	**Атрибуты VMX-файла**
	hpet\d+\.present
Настройки CPU	numvcpus, cpuid.corespersocket, vcpu.hotadd, sched.cpu.affinity, sched.cpu.htsharing, sched.cpu.shares, sched.cpu.max, sched.cpu.min, sched.cpu.units атрибуты, соответствующие регулярному выражению cpuid\.(?:0|1|80000001)\.e[a-d]x(?:\.amd)

Целостность BIOS ВМ	По умолчанию данный пункт отмечен. Удалите отметку, чтобы выключить контроль целостности файлов конфигурации BIOS (файлов NVRAM)
Перечень снимков ВМ	По умолчанию данный пункт отмечен. Удалите отметку, чтобы выключить контроль целостности файлов конфигурации снимков ВМ (файлов VMSD)
Контроль конфигурации ВМ	Список параметров конфигурации ВМ (атрибутов VMX-файла), контролируемых политикой (подробнее о соответствии контролируемых параметров и конкретных атрибутов VMX-файла см. ниже). Удалите отметку в нужной строке списка, чтобы отменить контроль за изменением значений соответствующего свойства ВМ

Внимание! При редактировании параметров политики "Доверенная загрузка виртуальных машин vSphere" нужно повторить назначение данной политики виртуальной машине. При конвертации виртуальной машины в шаблон для контроля целостности полученного шаблона нужно назначить ему политику "Контроль целостности шаблонов виртуальных машин" (см. Настройка контроля целостности шаблона ВМ ESXi).

3. После внесения всех изменений нажмите кнопку "Сохранить".

Внимание! Для всех виртуальных машин, которым назначена политика "Доверенная загрузка виртуальных машин vSphere", блокируются операции удаления и конвертации ВМ в шаблон.

Расчет контрольных сумм

Целостность ВМ контролируется агентами vGate, установленными на ESXi-сервер (см. Установка агента vGate).

Для каждой ВМ, на которую назначается политика "Доверенная загрузка виртуальных машин vSphere", рассчитывается эталонная контрольная сумма (КС), которая используется для контроля целостности. При миграции ВМ с другого сервера необходимо пересчитать КС, согласовав изменения виртуальной машины в разделе "Виртуальные машины" веб-консоли, иначе будет зафиксировано нарушение целостности.

Контроль изменений и статус ВМ

На ESXi-сервере каждые 10 минут (а также при запуске ВМ или при проверке политик вручную) выполняется сравнение эталонной контрольной суммы ВМ с текущей. При несовпадении контрольных сумм ВМ фиксируется нарушение целостности, изменяется статус ВМ (значение в колонке "Контроль целостности") и может быть запрещен запуск данной ВМ.

Примечание. Запуск ВМ в случае несовпадения контрольных сумм не будет заблокирован, если в настройках политики "Доверенная загрузка виртуальных машин vSphere" отмечен пункт "Разрешен запуск ВМ при нарушении целостности" (данный вариант включен по умолчанию).

Администратор может в зависимости от статуса ВМ принять изменения (согласовать) либо отклонить их (см. Согласование и отклонение изменений). При согласовании изменений эталонная контрольная сумма ВМ заменяется текущей (т. е. контрольная сумма пересчитывается). Кроме того, при согласовании изменений в базе сохраняется текущий конфигурационный файл ВМ. При отклонении изменений текущий конфигурационный файл заменяется эталонным (сохраненным в базе при последнем согласовании).

Внимание! При отклонении изменений конфигурации ВМ будут также затронуты параметры, не контролируемые политикой "Доверенная загрузка виртуальных машин vSphere".

В таблице перечислены статусы ВМ, приведено их описание, а также указаны возможные действия администратора с ВМ.

Активизация какой кнопки приведет к открытию компонента «Учетная запись»?

Ответ: пуск

7. Оценка решения тестовых задач, выполнения теста

За правильный ответ на вопросы или верное решение задачи выставляется положительная оценка – 1 балл.

За неправильный ответ на вопросы или неверное решение задачи выставляется отрицательная оценка 0 баллов.

15 – 19 баллов - 3(удовлетворительно)
20 – 23 балла – 4(хорошо)
24 -25 баллов – 5 (отлично)

8. Трудоемкость выполнения теста

Трудоемкость выполнения/решения, мин (час)	Количество задач/вопросов по типу тестовой формы			
	ВО	УС	УП	КО
	4	5	6	10
Одной (го) задачи/вопроса	1 мин	3 мин	3,5 мин	2 мин
Всего задания	4 мин	15 мин	21 мин	20 мин
	60 мин			

9. Перечень используемых нормативных документов

ФГОС СПО по специальности 09.02.07 «Информационные системы и программирование»

Типовое положение об образовательном учреждении среднего профессионального образования

Основная профессиональная образовательная программа по специальности 09.02.07 «Информационные системы и программирование»

Положение о текущем контроле знаний и промежуточной аттестации студентов (обучающихся) техникума

10. Рекомендуемая литература для разработки оценочных средств и подготовки обучающихся к аттестации

1 Операционные системы, среды и оболочки. Учеб. пособие// Партыка Т. Л., Попов И. И. -2-е изд., испр. и доп., - М.: Форум, 2017. - 528 с.

11. Перечень материалов, оборудования и информационных источников, используемых в аттестации

- ПЭВМ
- Программный продукт, предназначенный для проведения тестирования с подсчетом результатов в соответствии с указанными выше критериями оценки.

Авторы-составители:

И.А. Кашталинская

Спецификация практического задания

1. Назначение

Спецификацией устанавливаются требования к содержанию и оформлению вариантов оценочного средства.

Практическое задание входит в состав комплекса оценочных средств и предназначено для *текущего* контроля и оценки знаний и умений обучающихся, соответствующих основным показателям оценки знаний и умений обучающихся, соответствующих основным показателям оценки результатов подготовки по программе учебной дисциплины «Операционные системы и среды» основной профессиональной образовательной программы по специальности 09.02.07 «Информационные системы и программирование».

2. Контингент аттестуемых: обучающиеся ОГБПОУ СОТА.

3. Условия аттестации: контроль проводится после изучения тем учебной дисциплины 5.1, 5.2 форме лабораторной работы.

4. Время контроля:

выполнение 1 час

5. Структура варианта практического задания

Основная задача: оценка знаний и умений обучающихся, соответствующих основным показателям оценки результатов подготовки по программе учебной дисциплины.

Краткая характеристика

Для реализации личностного потенциала обучающимся предлагаются задания разных уровней.

Задание первого варианта состоит из 8 задач, выполнение которых является пошаговым действием в достижении результата. Выполнение каждой задачи невозможно без результата предыдущей. Задачи данного варианта носят репродуктивный характер.

Задание второго варианта состоит из пяти задач, в которых указаны исходные данные для выполнения действия и средства выполнения, но отсутствует комментарий к выполнению. Задачи данного варианта носят частично-поисковый характер.

Третий вариант включает пять задач, в которых указаны исходные данные. Обучающийся должен выбрать средства выполнения, описать алгоритм действий для достижения результата. Задания носят поисковый характер.

Вариант 1

1 Используя среду разработки приложений Delphi, создайте приложение, запускающее другое приложение по команде пользователя. Создаваемое приложение должно содержать следующие элементы:

- однострочное редактируемое текстовое поле для ввода имени исполняемого файла с возможным путем доступа;
- кнопка «Запустить процесс»;
- кнопка «Очистить поле»;
- кнопка «Выход».

Приложение, которое будет запускаться с помощью созданного вами, может содержать только один элемент – кнопку, закрывающую запущенное приложение. Форма приложения имеет вид (рисунок 1)

3. Выберите **myBackendPool**.
4. В разделе **Тип цели** выберите **Виртуальная машина** из раскрывающегося списка.
5. В разделе **Целевой объект** выберите связанный сетевой интерфейс для **myVM** в раскрывающемся списке.
6. Повторите эти действия для **myVM2**.
7. Щелкните **Сохранить**.
8. Прежде чем переходить к следующему шагу, дождитесь завершения развертывания.

Тестирование шлюза приложений

Хотя NGINX не требуется для создания шлюза приложений, вы установили его, чтобы проверить, успешно ли создан шлюз приложений в Azure. Используйте веб-службу для тестирования шлюза приложений:

1. Найдите общедоступный IP-адрес для шлюза приложений на странице **Обзор**.

Вы также можете выбрать **Все ресурсы**, ввести *myAGPublicIPAddress* в поле поиска, а затем выбрать его в результатах поиска. Общедоступный IP-адрес отобразится в Azure на странице **Обзор**.

2. Скопируйте общедоступный IP-адрес и вставьте его в адресную строку браузера.
3. Проверьте ответ. Допустимый ответ подтверждает, что шлюз приложений создан и может успешно подключиться к серверу.

Очистка ресурсов

Если вам уже не нужны ресурсы, созданные с помощью шлюза приложений, удалите группу ресурсов. Удалив ее, вы также удалите шлюз приложений и все связанные с ним ресурсы.

Чтобы удалить группу ресурсов:

1. На портале Azure в меню слева выберите **Группы ресурсов**.
2. На странице **Группы ресурсов** выполните поиск группы **myResourceGroupAG** в списке и выберите ее.
3. На странице **группы ресурсов** выберите **Удалить группу ресурсов**.
4. Введите *myResourceGroupAG* в поле **Введите имя группы ресурсов**, а затем выберите **Удалить**.

№6 Настройка контроля целостности виртуальных машин гипервизоров Настройка объектов контроля

vGate позволяет выполнить детальную настройку контроля целостности ВМ: разрешить или запретить запуск ВМ при нарушении целостности конфигурации;

выбрать файлы конфигурации ВМ (файлы VMX, NVRAM, VMSD), для которых будет осуществляться проверка соответствия контрольных сумм;

выбрать параметры конфигурации ВМ (параметры VMX-файла), изменение значений которых будет контролироваться политикой "Доверенная загрузка виртуальных машин vSphere".

Настройка выполняется при редактировании параметров политики "Доверенная загрузка виртуальных машин vSphere".

Для настройки параметров политики:

1. В главном меню выберите раздел "Политики безопасности" и откройте набор политик, включающий политику "Доверенная загрузка виртуальных машин vSphere" (см. Создание наборов политик).

2. Настройте параметры политики "Доверенная загрузка виртуальных машин vSphere".

Параметр	Описание
Разрешен запуск ВМ при нарушении целостности	По умолчанию данный пункт отмечен. Удалите отметку, чтобы запретить запуск ВМ при несовпадении контрольных сумм файлов конфигурации ВМ, контролируемых настройками политики

новые. В этом примере вы создадите две виртуальные машины, которые будут использоваться в Azure как внутренние серверы для шлюза приложений.

Для этого сделайте следующее:

1. Создайте две новые виртуальные машины Linux *myVM* и *myVM2*, которые будут использоваться в качестве внутренних серверов.
2. Установите NGINX на виртуальных машинах, чтобы убедиться, что шлюз приложений успешно создан.
3. Добавить внутренние серверы к внутренним пулам.

Создание виртуальной машины

1. На портале Azure выберите **Создать ресурс**. Откроется окно **Создание ресурса** .
2. В разделе **Виртуальная машина** выберите **Создать**.
3. На вкладке **Основы** введите для следующих параметров виртуальной машины такие значения:

- **Группа ресурсов.** Выберите **myResourceGroupAG** для имени группы ресурсов.
- **Имя виртуальной машины**. Введите *myVM* для имени виртуальной машины.
- **Изображение**: Ubuntu Server 20.04 LTS — 2-е поколение.
- **Тип проверки подлинности**: пароль
- **Имя пользователя**. Введите имя для имени администратора.
- **Пароль**. Введите пароль администратора.
- В поле **Общедоступные входящие порты** выберите значение **Нет**.

2. Примите остальные значения по умолчанию и щелкните **Далее: Диски**.
3. Примите значения по умолчанию на вкладке **Диски**, а затем выберите **Далее: Сети**.
4. На вкладке **Сети** убедитесь, что для параметра **Виртуальная сеть** выбрано значение **myVNet**, а для параметра **Подсеть** — значение **myBackendSubnet**.
5. В поле **Общедоступный IP-адрес** выберите значение **Нет**.
6. Примите остальные значения по умолчанию и щелкните **Далее: управление**.
7. Выберите **Далее: мониторинг** и установите для параметра **Диагностика загрузки** значение **Отключить**. Примите другие значения по умолчанию и выберите **Review + create** (Просмотр и создание).
8. На вкладке **Review + create** (Просмотр и создание) проверьте параметры, устраните ошибки проверки, а затем выберите **Создать**.
9. Прежде чем продолжить, дождитесь завершения создания виртуальной машины.

Установка NGINX для тестирования

В этом примере NGINX устанавливается на виртуальных машинах только для проверки успешного создания шлюза приложений в Azure.

1. Откройте Cloud Shell Bash. Для этого щелкните значок **Cloud Shell** на верхней панели навигации портал Azure а затем выберите **Bash** в раскрывающемся списке.
2. Выполните следующую команду, чтобы установить NGINX на виртуальной машине: Azure CLIКопировать

Открытие Cloud Shell az vm extension set \
--publisher Microsoft.Azure.Extensions \
--version 2.0 \
--name CustomScript \
--resource-group myResourceGroupAG \
--vm-name myVM \
--settings '{ "fileUris": ["https://raw.githubusercontent.com/Azure/azure-docs-powershell-samples/master/application-gateway/iis/install_nginx.sh"], "commandToExecute": "./install_nginx.sh" }'

3. Создайте вторую виртуальную машину и установите NGINX, выполнив описанные ранее действия. Используйте *myVM2* для имени виртуальной машины и параметра **--vm-name** командлета.

Добавление серверов во внутренние пулы

1. Выберите **Все ресурсы**, а затем — **myAppGateway**.
2. Выберите **Серверные пулы** в меню слева.

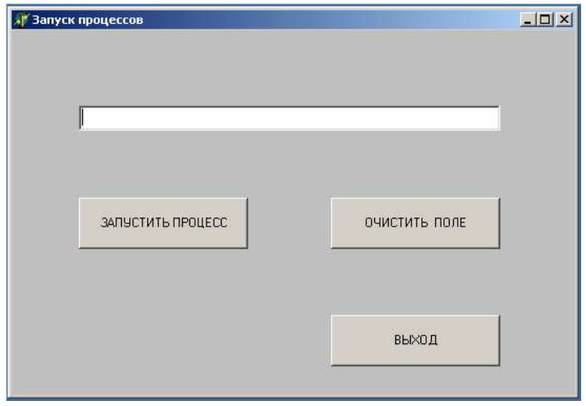


Рисунок 1 – Вид приложения, запускающего процесс

Ниже приведен код обработчика кнопки, создающей процесс.

```
procedure TForm1.Button1Click(Sender: TObject);

// пример запуска дочернего процесса
begin
Line:=Edit1.Text;
{подготовка структуры StartUpInfo }
FillChar(StartUpInfo, SizeOf(StartUpInfo), 0);
with StartUpInfo do
begin
cb:=SizeOf(StartUpInfo);  //Указание размера структуры
{флаг Startf_useshowwindow заставляет учитывать параметр wShowWindow, флаг startf_forceonfeedback  переводит указатель мыши в режим «обратной связи» - он ждет окончания создания дочернего процесса.}
dwFlags:=Startf_useshowwindow or startf_forceonfeedback;
{окно нового процесса должно быть видимым}
wShowWindow:=sw_ShowNormal;
end;
{создаем дочерний процесс}
CreateProcess(nil, PChar(Line), nil, nil, false, normal_priority_class, nil, nil,Startupinfo, PrOCinfo);
end;
```

2 Запустите Диспетчер задач Windows. Для этого щелкните правой кнопкой мыши в свободном месте Панели задач и из появившегося контекстного меню выберите соответствующий пункт «Диспетчер задач».

3 Просмотрите вкладки Диспетчера задач, активизировав каждую из них поочередно. Откройте вкладку «Процессы» щелчком по ней левой кнопки мыши.

4 С помощью главного меню Диспетчера задач измените вид окна программы таким образом, чтобы отображались показатели: объем виртуальной памяти, базовый приоритет и счетчик потоков для всех процессов. Определите эти показатели для созданного вами приложения. (Вид – Столбцы).

5 Запустите ваше приложение для создания процессов. (Диспетчер задач – Приложения – Новая задача – путь (обзор)).

6 Проверьте наличие имени вашего приложения в списке выполняющихся процессов Диспетчера задач. (Вкладка «Приложения»). Определите параметры процесса вашего приложения.

7 Запустите созданное приложение посредством Проводника (Пуск-Все программы-Стандартные-Проводник).

8 Запустите с помощью созданного приложения стандартную программу «Калькулятор», предварительно определив ее адрес.

Вариант 2

1 Используя среду разработки приложений Delphi, создайте приложение, запускающее другое приложение по команде пользователя. Создаваемое приложение должно содержать следующие элементы:

- однострочное редактируемое текстовое поле для ввода имени исполняемого файла с возможным путем доступа;
- кнопка «Запустить процесс»;
- кнопка «Очистить поле»;
- кнопка «Выход».

Приложение, которое будет запускаться с помощью созданного вами, может содержать только один элемент – кнопку, закрывающую запущенное приложение.

2 Используя главное меню Диспетчера задач, определите базовые параметры созданного процесса (объем виртуальной памяти, базовый приоритет, счетчик потоков).

3 Определите с помощью Диспетчера задач, присутствует ли имя вашего приложения в списке выполняющихся процессов. Определите параметры процесса вашего приложения.

4С помощью созданного вами приложения создайте процесс, запустите его на выполнение.

5 Определите с помощью Диспетчера задач, присутствует ли имя вашего процесса в списке выполняющихся процессов. Определите параметры процесса.

6 Запустите созданное приложение посредством Проводника. Сохраните созданные приложения в папке с номером вашей группы.

Вариант 3

1 Используя среду разработки приложений Delphi, создайте приложение, запускающее другое приложение по команде пользователя. Создаваемое приложение должно содержать следующие элементы:

- однострочное редактируемое текстовое поле для ввода имени исполняемого файла с возможным путем доступа;
- кнопка «Запустить процесс»;
- кнопка «Очистить поле»;
- кнопка «Выход».

Приложение, которое будет запускаться с помощью созданного вами, может содержать только один элемент – кнопку, закрывающую запущенное приложение.

2 Определите параметра созданного приложения (объем виртуальной памяти, базовый приоритет, счетчик потоков).

3 С помощью созданного вами приложения создайте процесс, запустите его на выполнение

4 Определите параметры созданного приложения.

5 Запустите созданное приложение посредством Проводника. Сохраните созданные приложения в папке с номером вашей группы.

6. Система оценки знаний

Отлично: выполнен вариант 3. Ошибки отсутствуют (допущена незначительная ошибка).

Хорошо: выполнен вариант 3, допущено не более 3-х неточностей/ошибок; выполнен вариант 2, ошибки отсутствуют (допущены незначительные недочеты/ошибки, но не более 3-х).

Удовлетворительно: выполнен вариант 3, допущено 4-5 неточностей/ошибок; выполнен вариант 2, допущено не более 4 неточностей/ошибок; выполнен вариант 1, ошибки отсутствуют (допущено не более 3-х неточностей/ошибок).

Неудовлетворительно: допущено большее количество ошибок; задания выполнены частично или не выполнены.

Вариант 1

3. По завершении выберите **Next: серверные компоненты**. **Вкладка "Серверные компоненты"**

Серверный пул используется для перенаправления запросов на внутренние серверы, на которых обслуживается запрос. Внутренние пулы могут состоять из сетевых адаптеров, масштабируемых наборов виртуальных машин, общедоступных IP-адресов, внутренних IP-адресов, полных доменных имен и таких мультитенантных серверных частей, как служба приложений Azure. В этом примере показано, как создать пустой серверный пул со своим шлюзом приложений, а затем добавить в этот серверный пул целевые серверные объекты.

1. На вкладке **Серверные компоненты** выберите элемент **Добавление серверного пула**.
2. В открывшемся окне **Добавить внутренний пул** введите следующие значения для создания пустого внутреннего пула.

• **Name** (Имя). Введите *myBackendPool* в качестве имени внутреннего пула.

• **Добавление внутреннего пула без целей**. Чтобы создать серверный пул без целевых объектов, выберите **Да**. После создания шлюза приложения вы добавите серверные целевые объекты.

3. В окне **Добавление внутреннего пула** выберите **Добавить**, чтобы сохранить конфигурацию внутреннего пула и вернуться на вкладку **Серверные компоненты**.
4. На вкладке **Серверные компоненты** выберите **Далее: конфигурация**. **Вкладка "Конфигурация"**

На вкладке **Конфигурация** созданный интерфейсный и внутренний пул подключается с помощью правила маршрутизации.

1. Выберите элемент **Добавление правила маршрутизации** в столбце **Правила маршрутизации**.
2. В открывшемся окне **Добавление правила маршрутизации** введите *myRoutingRule* в поле **Имя правила**.
3. В поле **Приоритет** ведите нужный номер.
4. Для правила маршрутизации требуется прослушиватель. На вкладке **Прослушиватель** в

окне **Добавление правила маршрутизации** введите следующие значения для прослушивателя.

• **Имя прослушивателя**. Введите *myListener* в качестве имени прослушивателя.**Интерфейсный IP-адрес**. Выберите **Общедоступные**, чтобы выбрать общедоступный IP-адрес, который вы создали для интерфейсных серверов.

Примите значения по умолчанию для других параметров на вкладке **Прослушиватель**, а затем выберите вкладку **Серверные целевые объекты**, чтобы настроить остальную часть правила маршрутизации.

5. На вкладке **Серверные целевые объекты** выберите значение **myBackendPool** для параметра **Серверный целевой объект**.
6. В области **Параметры серверной части** щелкните **Добавить**, чтобы создать новый параметр серверной части. Этот параметр определяет поведение для правила маршрутизации. В открывшемся окне **Добавление параметра серверной части** введите *myBackendSetting* в

поле **Имя параметра серверной части**. Сохраните значения по умолчанию для других параметров в этом окне, а затем щелкните **Добавить**, чтобы вернуться к окну **Добавление правила маршрутизации**.

7. В окне **Добавление правила маршрутизации** выберите **Добавить**, чтобы сохранить правило маршрутизации и вернуться на вкладку **Конфигурация**.
8. По завершении выберите **Next: Теги** , а затем **Далее: Отзыв и создание**. **Вкладка "Просмотр и создание"**

Просмотрите параметры на вкладке **Просмотр и создание**, а затем выберите **Создать**, чтобы создать виртуальную сеть, общедоступный IP-адрес и шлюз приложения. Создание шлюза приложений в Azure может занять несколько минут.

Дождитесь успешного завершения развертывания перед переходом к следующему разделу.

Добавление серверных целевых объектов

В этом примере мы будем использовать виртуальные машины в качестве целевых объектов серверной части. Вы можете использовать существующие виртуальные машины или создать

№3 Настройка сервисов сертификации на сервисах
№4 Настройка сервисов аутентификации на сервисах
№5 Настройка системы мониторинга состояния сети и сервисов
Вход в Azure
Войдите на портал Azure.
Создание шлюза приложений

1. Выберите **Создать ресурс** в верхнем левом меню портала Azure. Появится окно **Создать**.
2. Выберите **Сети**, а затем в списке **Рекомендованные** выберите **Шлюз приложений**.

Вкладка "Основные сведения"

1. На вкладке **Основные сведения** введите значения для следующих параметров шлюза приложений.

- **Группа ресурсов.** Выберите **myResourceGroupAG** для группы ресурсов. Выберите **Создать** для создания группы ресурсов, если она еще не существует.
- **Имя шлюза приложений**. Введите *myAppGateway* для имени шлюза приложений.
- **Уровень**: выберите **WAF версии 2**.
- **Политика WAF**: выберите **Создать**, введите имя новой политики и нажмите кнопку **ОК**.

При этом создается базовая политика WAF с управляемым набором правил (CRS).

2. В Azure для обмена между создаваемыми ресурсами необходима виртуальная сеть. Вы можете создать новую виртуальную сеть или использовать существующую. В этом примере вы можете создать виртуальную сеть одновременно со шлюзом приложений. Экземпляры Шлюза приложений создаются в отдельных подсетях. В этом примере создаются две подсети: одна — для шлюза приложений, а вторая — для внутренних серверов.

В разделе **Настройка виртуальной сети** создайте виртуальную сеть, выбрав команду **Создать**. В открывшемся окне **Создание виртуальной сети** введите следующие значения, которые будут использоваться для создания виртуальной сети и двух подсетей.Name (Имя). Введите *myVNet* для имени виртуальной сети.

- Имя подсети (Подсеть шлюза приложений). В сетке Подсети будет показана подсеть с именем *По умолчанию*. Измените имя этой подсети на *myAGSubnet*.

Подсеть шлюза приложений может содержать только шлюзы приложений. Другие ресурсы запрещены.

- Имя подсети (подсеть внутреннего сервера). Во второй строке таблицы Подсети введите *myBackendSubnet* в столбце Имя подсети.
- Диапазон адресов (подсеть внутреннего сервера). Во второй строке таблицы Подсети введите диапазон адресов, которые не пересекаются с диапазоном адресов *myAGSubnet*. Например, если диапазон адресов *myAGSubnet* равен 10.21.0.0/24, введите *10.21.1.0/24* для диапазона адресов *myBackendSubnet*.

Выберите **ОК**, чтобы закрыть окно **Создание виртуальной сети** и сохранить настройки виртуальной сети.

3. На вкладке **Основные сведения** примите значения по умолчанию для других параметров и выберите **Далее: интерфейсные серверы**.

Вкладка "Интерфейсные серверы"

1. На вкладке **Интерфейсные серверы** убедитесь, что для параметра **Тип IP-адреса интерфейсных серверов** установлено значение **Общедоступный**.

Вы можете настроить внешний IP-адрес как **общедоступный** или **оба** в своем варианте использования. В этом примере мы будем использовать общедоступный интерфейсный IP-адрес.

Примечание

Для номера SKU Шлюз приложений версии 2 сейчас поддерживаются **общедоступные** и **внешние** типы IP-адресов. В настоящее время не поддерживается только **конфигурация частных** интерфейсных IP-адресов.

2. Выберите команду **Добавить новый** для параметра **Общедоступный IP-адрес** и введите *myAGPublicIPAddress* в качестве имени общедоступного IP-адреса. Затем нажмите кнопку **ОК**.

1 Планирование потоков включает решение следующих задач

- ☐ Определение времени смены текущего активного потока
- ☐ Запуск нового потока на выполнение
- ☐ Выбор для выполнения потока из очереди готовых потоков
- ☐ Выбор для выполнения потока из очереди ожидающих потоков
- ☐ Определение времени запуска задачи

2 Укажите последовательность, в которой прикладные программные среды транслируют системные вызовы. *Запишите ответ в виде последовательности объектов/понятий.*

Объекты/понятия:

1 результат обработки запроса для приложения
2 выполнение запроса
3 преобразование вызовов «чужих» приложений в интерфейс «своей» операционной системы
4 обращение к ядру операционной системы
5 обработка системных вызовов «чужих» приложений

Ответ: 53421

3 Единица информации, передаваемая как единое целое между двумя устройствами в сети – пакет.

4 Смена активного потока происходит если:

- ☐ Поток завершился и покинул систему
- ☐ Произошла ошибка
- ☐ Поток находится в активном состоянии
- ☐ Выполняется чтение жесткого диска
- ☐ Поток перешел в состояние готовности

5 Процесс, при котором два или более устройства пытаются получить доступ к одному и тому же системному ресурсу называется конфликт.

6 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 API	А сеть на основе клиентов и серверов
2 сетевая служба	Б международный стандарт
3 POSIX	В сеть, включающая узлы всех типов
4 сеть с выделенным сервером	Г интерфейс прикладного программирования
5 гибридная сеть	Д сетевой сервис

Ответ 1Г, 2Д, 3Б, 4А 5В

7 Операционная система отдельного компьютера, способного работать в сети, называется сетевой.

8 В какой последовательности реализуется системный вызов в микроядерной архитектуре ядра операционной системы? *Запишите ответ в виде последовательности объектов/понятий.*

Объекты/понятия:

1 запрос разрешения обслуживания

2 запрос сервера
3 обработка запроса «сервер - микроядро»
4 обработка запроса «микроядро - приложение»
5 сигнал «Разрыв связи»

Ответ: 12345

9 Набор правил и соглашений для передачи данных по сети называется протокол.

10 Реализация системных вызовов должна обеспечивать:

- Переключение в режим готовности
- Переключение в привилегированный режим
- Единое стандартное обращение к системным вызовам для всех аппаратных платформ, на которых работает операционная система
- Высокая скорость вызова процедур операционной системы
- Высокая скорость работы процессора

11 Установите последовательность смены режимов для операционной системы классической структуры. *Запишите ответ в виде последовательности объектов/понятий.*
Объекты/понятия:
1 пользовательский режим
2 системный вызов
3 привилегированный режим
4 сигнал подтверждения готовности
5 сигнал «Разрыв связи»

Ответ: 12435

12 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 одноранговая сеть	А передача информации между компьютерами
2 серверная часть	Б распределяют работу между ресурсами сети
3 распределенная операционная система	В требования к сетевой операционной системе
4 безопасность	Г локальные ресурсы и услуги сети в общем пользовании
5 транспортные средства	Д сеть на основе одноранговых узлов

Ответ 1Д, 2Г, 3Б, 4В 5А

13 В какой последовательности выполняется обработка системных вызовов в монолитной операционной системе. *Запишите ответ в виде последовательности объектов/понятий.*
Объекты/понятия:
1 запрос разрешения обслуживания
2 обработка запросов
3 выполнение запроса, готовность обслуживания
4 работа приложения
5 сигнал «Разрыв связи»

Ответ: 12345

возможность импорта ova/ovf формата. MCS поддерживает загрузку формата RAW, для которого требуется конвертация с помощью стандартной утилиты из пакета Qemu. Ещё он поддерживает конвертацию на лету при загрузке через веб-интерфейс портала. Azure позволяет загружать собственные образы в формате VHD (формат Hyper-V).

SLA

Уровни SLA отличаются между платформами. MCS и Azure предоставляют SLA в рамках доступности на каждый из облачных сервисов, а также на отдельные параметры внутри сервиса – например, на IOPS для блочных устройств. **Яндекс же оперирует только доступностью сервиса, не включая характеристики отдельных компонент.** Все провайдеры компенсируют часть счета на услуги в зависимости от времени простоя сервиса. Яндекс отдельно упоминает о возможности полной компенсации платежей в случае потери данных клиента.

IAM

Все платформы предоставляют сервис управления учетными записями и правами Identity and Access Management (IAM).

Яндекс для этого требует наличия учетной записи в сервисе Яндекс.Паспорт или интеграцию с внешним провайдером учетных записей посредством протокола SAML, например, AD FS, и позволяет управлять квотами и правами в контексте облачных услуг.

Компания Mail.ru Group расширила функционал, заложенный в IAM для Openstack в части работы с собственным сервисом S3, и близка по возможностям к сервису платформы Яндекс.Облако.

Обе платформы не предполагают сценариев интеграции IAM для собственных приложений клиента.

Наиболее богатый функционал IAM у Azure. Кроме управления облачной инфраструктурой есть возможность получить Active Directory, как услугу. Есть возможность использовать IAM для интеграции с приложениями в облаке для управления учетными записями клиентов компании. Все платформы поддерживают управление собственными SSH ключами для Linux систем.

Управляемые сервисы VPN и DNS

Для полноценного использования платформы IaaS нам требуются такие сервисы, как Managed VPN и Managed DNS. Azure позволяет управлять внешними и внутренними DNS зонами, обычными или техническими DNS записями, а также автоматически регистрировать новые DNS записи при создании ВМ. В MCS функционал ограничен созданием внутренней DNS зоны и автоматической регистрацией ВМ в ней, с возможностью создания произвольного имени или же привязки DNS- записи к сетевому порту (IP адресу), но без возможности управления техническими записями. В платформе Яндекс.Облако отсутствует возможность управлять записям DNS.

Если говорить об организации защищенного подключения и пиринга, то наиболее полный функционал у Azure. В нём есть поддержка режимов client-to-site, site-to-site и прямого пиринга по протоколу BGP. Пропускная способность VPN-линка к Azure ограничивается оконечным оборудованием клиента. MCS поддерживает только режим site-to-site для протокола IPSec. Яндекс – только технологию прямого соединения (название сервиса — Yandex.Cloud Interconnect) по протоколу BGP. Для организации защищенного канала VPN к платформе Яндекс.Облако потребуется развернуть Cisco CSR, Mikrotik CHR или другое VPN решение из маркетплейса.

On-Premise решение для частного облака

Все поставщики облачных услуг предоставляют возможность развертывания своей платформы на оборудовании заказчика (on-premise). Частное облако может быть интегрировано с публичной платформой от данного поставщика для организации гибридного решения с единым порталом управления, репликацией машин и Disaster Recovery площадкой в публичном облаке. Есть отличие предоставления сервиса и вот в чём оно состоит. Microsoft и Яндекс поставляют собственные решения в виде готового к установке в ЦОД оборудования. Компания Mail.ru Group может поставить свое решение на оборудование клиента, совместимого с их платформой.

МДК.04.02 Безопасность облачных сервисов

№1 Развёртывание WAF (Web Application Firewall)

№2 Настройка WAF (Web Application Firewall)

IBM. Объем доработок KVM, которые выполнили разработчики MCS, компания не раскрывает. В части SDS для блочных устройств и сервиса NFS используется решение CEPH – его тоже дорабатывала команда MCS. Для объектного хранилища S3 были переиспользованы технологии облачного диска Mail.ru Group. В качестве сетевого решения применяется решение на базе OpenvSwitch, однако механизмы управления Control plane были серьезно переработаны. Это дало жизнь проекту Sprut.

Для управления платформой MCS был реализован отдельный портал, в котором реализованы самые популярные сервисы, а также доступен нативный интерфейс OpenStack Horizon. Для тонкой настройки сервисов предоставляется доступ к OpenStack CLI или OpenStack API. Есть также возможность использовать решение Infrastructure as Code (IaC) которое будет обращаться напрямую к API платформы. Работу с OpenStack поддерживает большинство систем управления конфигурацией, что упрощает встраивание облака MCS в DevOps конвейер и внешние системы управления облачными ресурсами.

Как было у Яндекса? Первую версию своей платформы компания разрабатывала для себя.

Яндекс, так же, как и Mail.ru Group ориентировался на архитектуру и компоненты OpenStack. Однако, потом компания отказалась от нее. Было принято решение начать с «чистого листа. Яндекс переиспользовал базовые инфраструктурные компоненты, которые у них уже были. К ним компания дополнительно разработала недостающие модули и платформу управления.

В качестве гипервизора компания Яндекс также использует KVM. В его разработку инвестированы большие ресурсы. Решения SDS и SDN были разработаны компанией

самостоятельно. SDS основан на собственной СУБД Yandex Database (YDB) для хранения мета- данных о размещении виртуальных машин и Network Block Storage (NBS) как сервиса предоставления блочных устройств виртуальным машинам, также YDB используется и в S3-совместимом решении в составе платформы. Яндекс, в отличии от MCS и Azure, не предлагает сервис NFS в составе услуг, рекомендуя развернуть его на базе виртуальной машины. В качестве SDN используется переработанная платформа OpenContrail. Её разрабатывали Juniper Networks, которая с недавнего времени входит в Linux Foundation, как платформа TungstenFabric.

Использование собственной платформы управления ограничивает возможности по встраиванию ресурсов Яндекс.Облака в конвейер DevOps или внешние системы управления облачными ресурсами. В настоящий момент заявлена поддержка IaC Terraform с помощью разработанного компанией провайдера. Ещё существует неофициальная поддержка работы с Ansible. Однако, среди популярных систем для управления Гибридными Облаками (Cloud Management Platforms) – таких как Red Hat CloudForms, Morpheus, Scalr, поддержка отсутствует. Компания также разработала и поддерживает свою собственную утилиту YC CLI для работы с платформой из командной строки с собственным набором команд.

Хранение данных

У MCS есть репликация блочных устройств между зонами доступности, что позволяет запустить виртуальную машину с теми же данными на любой из площадок, а также получить высокопроизводительный локальный диск NVMe или общее СХД по протоколу ISCSI. Azure предлагает репликацию объектных хранилищ как внутри зоны доступности, так и между зонами в пределах географического региона, а также сервис Azure Site Recovery для репликации блочных устройств. Обе платформы предоставляют сервис NFS.

В платформе Яндекс.Облако нет синхронной репликации блочных устройств между зонами доступности. Реплицируются только резервные копии и S3-хранилище. Репликация данных для Яндекса.Облака может быть реализована средствами приложения или СУБД. Отсутствие репликации блочных устройств связано с тем, что ЦОДы располагаются достаточно далеко и синхронная репликация будет вносить значительные задержки в дисковый ввод-вывод. Сервис NFS платформой Яндекс.Облако не предоставляется.

Образы виртуальных машин

В отличие от Azure, **в MCS отсутствует возможность развернуть ВМ с использованием enterprise-level дистрибутива ОС Linux (RHEL, SLES, OEL).** Платформа Яндекс.Облако позволяет развернуть ВМ с ОС RHEL версии 7.8, но подписку клиент должен оформлять самостоятельно через стороннюю организацию.

Оба провайдера поддерживают загрузку собственных образов ОС. Яндекс поддерживает форматы qcow (qemu), vhd (Microsoft Hyper-V/Azure) и vmdk (VMware ESXi), но отсутствует

14 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 ядро	А системные обрабатывающие программы
2 сетевая операционная система	Б клиентская часть сетевой службы
3 редиректор	В совокупность клиентской и серверной части
4 отладчик	Г совокупность операционных систем всех ПЭВМ в сети
5 сетевая служба	Д модули, выполняющие основные функции операционной системы

Ответ 1Д, 2Г, 3Б, 4А 5В

15 Правило, связанное с объектом и используемое для управления доступом пользователей к этому объекту называется разрешение.

16 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 операционная система	А критерий эффективной работы операционной системы
2 контроллер диска	Б предоставление пользователю расширенной виртуальной машины
3 задача операционной системы	В определяет функционирование операционной системы
4 пропускная способность	Г распознает различные операции завершения работы с диском
5 подсистема управления процессами	Д «скрывает» от программиста особенности работы аппаратуры ПЭВМ

Ответ 1Д, 2Г, 3Б, 4А 5В

17 Характеристика класса объектов или устройств в сети – свойство.

18 Укажите последовательность реализации множественных прикладных сред в микроядерной структуре ядра операционной системы. *Запишите ответ в виде последовательности объектов/понятий.*

Объекты/понятия:

1 системный вызов приложения
2 обработка и выполнение запроса прикладной среды
3 запрос прикладной среды
4 пересылка результата обработки запроса приложению
5 результат запроса обрабатывается микроядром

Ответ: 13254

19 Можно ли обеспечить привилегии операционной системы без учета функции аппаратного слоя? (да \ нет)

20 Служба, поддерживающая транспорты для асинхронного обмена сообщениями между узлами – ISM.

21 Укажите средства синхронизации процессов и потоков в операционной системе

- □ <u>События</u>
- □ <u>Таймеры</u>
- □ <u>Критические секции</u>
- □ Сигналы прерывания
- □ Запросы

22 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 аудит операционной системы	А пользовательская задача выполняется на ПЭВМ , где выполнен логический вход
2 администратор операционной системы	Б Поддержка отказоустойчивости операционной системы
3 резервирование	В пользователь не имеет сведений о ПЭВМ, где выполняется его задача
4 сетевая операционная система	Г средство защиты данных, фиксация всех событий безопасности системы
5 распределенная операционная система	Д Отслеживание списка событий в операционной системе

Ответ 1Г, 2Д, 3Б, 4А 5В

23 Средство вычислительной системы, которое может быть выделено процессу на определенный интервал времени – <u>ресурс</u>.

24 Укажите последовательность реализации совместимости на основе множественных равноправных API. *Запишите ответ в виде последовательности объектов/понятий.*

Объекты/понятия:

1 системный вызов приложения
2 обращение API к менеджеру ресурсов
3 нахождение операционной системой необходимого API
4 пересылка результата обработки запроса приложению
5 обращение менеджера ресурсов к базовым механизмам
6 обращение базовых механизмов на уровень машинозависимых задач

Ответ: 132564

25 Вставьте пропущенное слово.

При сетевой топологии <u>кольцо</u> данные передаются от одного компьютера к другому поочередно, последовательно.

Вариант 2

Укажите средства синхронизации процессов и потоков операционной системы

- □ Флаги
- □ <u>Блокирующие переменные</u>
- □ Бинарные переменные
- □ <u>Семафоры</u>
- □ Тупики

- Запущен планировщик заданий, обрабатывающий большую группу серверов и запускающий приложение на нескольких машинах как на одной;
- Балансировщик нагрузки управляет интернет-трафиком;
- Работа DNS автоматизирована;
- Реализована форма контейнеризации (FreeBSD Jail, Solaris Zones, Linux Containers), предотвращающая вмешательство одного приложения в работу другого.

Первый и последний пункты — это те элементы, которые способствовали росту популярности Docker. Технология Linux Container давно являлась частью ядра ОС Linux, но автоматизировать их использование решились только крупные компании или PaaS-провайдеры.

Компании используют архитектуры и микросервисы, ориентированные на работу с программным обеспечением, потому что они предлагают возможности по автоматическому развертыванию и тестированию кода, а также масштабирования в зависимости от нагрузки. Этот функционал и реализует PaaS.

К сожалению, такой подход имеет один серьезный недостаток. Вы передаете часть контроля своеобразному черному ящику и попадаете в зависимость от него. Однако в противном случае компании постоянно заново изобретают велосипед или начинают использовать медленные инструменты.

Немного о SaaS

В случае SaaS потребитель приобретает возможность пользоваться приложениями поставщика, выполняемыми в облаке.

Программное обеспечение как услуга (SaaS) — последний уровень облачных вычислений, который чаще всего дополняет PaaS, как видно из схемы в начале статьи. Это полнофункциональное приложение для пользователя, выполняющее определенные функции — например работу с изображениями или звуком. Наиболее популярной формой оплаты в этом сегменте остается подписка.

В случае SaaS в зону ответственности облачного провайдера передаются вопросы настройки приложений, мониторинга и резервного копирования. Поэтому такая модель работы не требует наличия в команде организации технического специалиста — все делает провайдер.

Архитектура IaaS платформы

Модель обслуживания Infrastructure-as-a-Service (IaaS), как описано в стандарте NIST, это возможность предоставить клиенту вычислительные, сетевые ресурсы и ресурсы хранения данных, на базе которых клиент сам размещает и управляет операционными системами и приложениями.

Современная IaaS платформа включает в себя гипервизор, предоставляющий вычислительные ресурсы, программно-определяемую систему хранения данных software-defined storage (SDS) для размещения данных и программно-определяемую сеть software-defined networking (SDN) как средство организации сетевого доступа к ресурсам IaaS.

Референтная платформа нашего сравнения, Azure от компании Microsoft, начинает свою историю еще в далеком 2003-м году с приобретения компании Connetix и их продукта Virtual PC с целью догнать конкурента VMware и их продукт GSX Server, вышедший двумя годами ранее. Спустя время продукт Virtual PC интегрировали в состав платформы Windows Server. Он появился в версии 2008, но только к версии 2012 были реализованы SDS на базе Scale-Out File Server и Storage Spaces и SDN на базе Hyper-V Network Virtualization. Это позволило построить целиком программно- определяемую платформу IaaS без привязки к аппаратным возможностям СХД или оборудования ЛВС.

Платформа Azure поддерживается большинством современных DevOps утилит как для построения конвейера непрерывного развертывания, так и для автоматизации рутинных задач. У Azure функциональный веб-интерфейс и подробно документированный API. Все крупные игроки по разработке платформ автоматизации и управления облачными платформами поддерживают Azure. Утилита командной строки Azure CLI доступна как расширение PowerShell и как отдельная утилита для платформ Windows, Linux и MacOS X.

Компания Mail.ru Group для своего облака взяла наработки платформы OpenStack. К 2020 году компания перешла на полностью собственный дистрибутив, который не связан с open-source версией платформы. В качестве гипервизора используется функция ядра ОС Linux Kernel-based Virtual Machine (KVM), основным разработчиком которого является компания Red Hat, ныне часть

На третьем уровне расположился IaaS — серверы, хранилища, сети, вычислительная инфраструктура, которую клиент получает в пользование для запуска своих решений. Описанная структура может быть представлена в виде следующей схемы:

Для демонстрации этих трех типов услуг часто применяется аналогия с пиццей — своеобразная

«Pizza as a Service». Когда потребитель заказывает и поедает пиццу в кафе или ресторане, то это SaaS, а если заказывает её себе на дом, то это PaaS. Если же он пошел в магазин, купил ингредиентов и приготовил блюдо самостоятельно, то, можно сказать, что это IaaS.

Теперь слегка углубимся в каждую из этих технологий и начнем с конца стека — IaaS. Что такое IaaS

При выборе IaaS, вы получите серверы, сетевые ресурсы и хранилища в качестве подключаемой услуги. Получается, что компания приобретает вычислительные ресурсы у поставщика, избегая необходимости закупать собственное железо и поддерживать его. При этом сервис может быть предоставлен по типу публичного облака, частного облака или комбинированного подхода.

Понятие IaaS включает в себя следующие особенности:

- Ресурсы — это услуга. Клиент имеет возможность в любое время увеличивать и уменьшать объемы потребляемых ресурсов
- С физическими ресурсами могут работать несколько пользователей благодаря возможностям виртуализации
- Гибкие модели оплаты (например, вариант pay as you go, когда компания платит только за потребляемые мощности)

Учитывая все вышесказанное, можно определить, когда следует использовать IaaS-решения. Обращаться к IaaS стоит в том случае, компания иногда испытывает нужду в повышении мощностей при всплесках нагрузки — то есть имеется потребность в оперативном масштабировании инфраструктуры.

Еще один вариант — компания представляет собой стартап, у которого нет средств на приобретение собственного «железа» и его поддержание, или же организация хочет запустить экспериментальное направление бизнеса и закупать оборудование для этого не всегда бывает целесообразно (проект может не взлететь).

Однако несмотря на гибкость и масштабируемость IaaS, технология имеет определенные ограничения. В связи с этим есть ситуации, когда использовать её не рекомендуется. Например, компания является игроком регулируемой отрасли, правила которой не разрешают хранение данных на серверах, не принадлежащих компании.

Здесь хотелось бы добавить, что существует мнение, якобы не стоит использовать облачные решения для бизнес-критичных приложений. Однако отметим, что это не так. Критичное бизнес-приложение может быть развернуто на производительном сервере с 16 ядрами и терабайтами памяти, в котором предусмотрено дублирование ряда компонентов (в том числе и на более высоких уровнях).

Что такое PaaS

Платформа как услуга, или PaaS, упрощает развертку приложений и управление ими, при этом скрывая внутри себя работу с серверами, балансировку нагрузки, DNS и др. Поэтому отпадает необходимость нанимать инженеров для обслуживания инфраструктуры. Это позволяет разработчикам уделять больше внимания разработке и проблемам развертывания.

Здесь следует отметить, поскольку PaaS является вторым уровнем пирамиды облачных услуг, то он строится на основе IaaS, однако еще сильнее уменьшает время с момента генерации идеи до её воплощения. Это достигается за счет большей автоматизации процессов и абстракции от железа.

Чтобы абстрагировать концепцию работы с серверами, было проделано следующее:

- Реализована система сборки, компилирующая и хранящая код;
- Внедрена база данных управления приложениями, следящая за версиями и метаданными;

2 Укажите последовательность действий при активизации оснастки «Управление компьютером» для операционных систем серии Windows. *Запишите ответ в виде последовательности объектов/понятий.*

Объекты/понятия:

1 активизация кнопки «Пуск»
2 выбор команды «Панель управления»
3 активизация компонента «Учетные записи пользователей»
4 выбор подменю «Выбрать задание»

Ответ: 1234

3 Группа компьютеров, образующих часть сети и использующих общую базу данных каталога называется домен.

4 Укажите методы использования внешней памяти

- ☐ Страничное распределение
- ☐ Сигнальное распределение
- ☐ Сегментное распределение
- ☐ Перемещаемые разделы
- ☐ Фиксированная очередь

5 Операционная система называется мобильной, если ее код легко переносится с процессора одного типа на процессор другого типа.

6 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 пользовательский процесс	А инициализирует операционная система
2 операционная система	Б обеспечение безопасности данных вычислительной системы
3 средства отказоустойчивости операционной системы	В разрешение входа в систему
4 системный процесс	Г инициализируется пользователем
5 администратор системы	Д удовлетворяет запросы на ресурсы

Ответ 1Г, 2Д, 3Б, 4А 5В

7 Как называется топология сети, если в ее структуре каждый компьютер через специальный сетевой адаптер подключен отдельным кабелем к объединяющему устройству? (Звезда)

8 В какой последовательности реализуется переключение пользователей в операционных систем серии Windows? *Запишите ответ в виде последовательности объектов/понятий.*

Объекты/понятия:

1 активизировать кнопку «Пуск»
2 активизировать кнопку «Завершение сеанса»
3 нажать кнопку «Смена пользователей»
4 выбор учетной записи нового пользователя

Ответ: 1324

9 Служба, поддерживающая транспорты для асинхронного обмена сообщениями между узлами, называется ISM.

10 Определите события, требующие перераспределения процессорного времени:

- ☐ Аппаратные прерывания
- ☐ Ошибка выполнения активной задачи
- ☐ Неупорядоченная обработка прерываний
- ☐ Прерывания от таймера
- ☐ Диспетчеризация прерываний

11 Установите последовательность действий при создании нового имени для учетной записи в операционной системе серии Windows. *Запишите ответ в виде последовательности объектов/понятий.*

Объекты/понятия:

1 активизация компонента «Учетные записи пользователя»
2 выбор изменяемой учетной записи
3 выбор вкладки «Изменение имени»
4 задание нового имени в открывшемся диалоговом окне
5 активизация кнопки «Сменить имя»

Ответ: 21435

12 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 учетная запись пользователя	А применяют для управления доступом, в качестве списка рассылки
2 контроллер домена	Б применяют для работы с рядовым сервером
3 локальная группа	В применяют в электронной почте
4 группа безопасности	Г применяют для управления входом пользователя в сеть
5 группа распространения	Д применяют для разрешения на ресурсы в домене

Ответ 1Д, 2Г, 3Б, 4А 5В

13 В какой последовательности можно удалить учетную запись пользователя, созданную средствами операционных систем серии Windows? *Запишите ответ в виде последовательности объектов/понятий.*

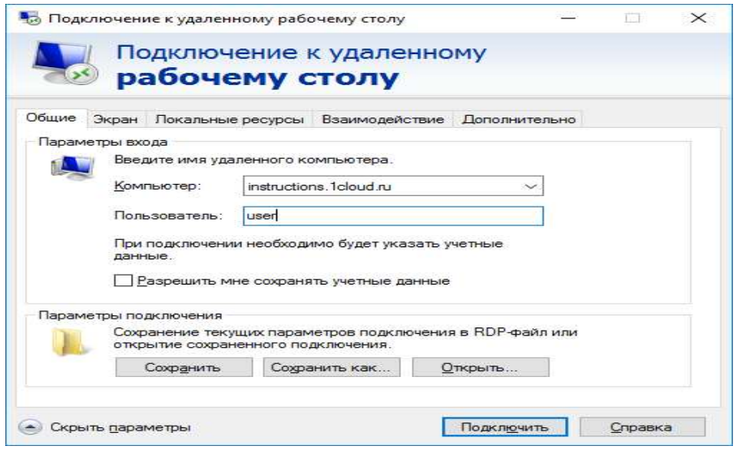
Объекты/понятия:

1 активизация компонента «Учетная запись пользователя»
2 выбор учетной записи
3 активизация кнопки «Удаление учетной записи»
4 выбор кнопки «Удалить эти файлы»
5 выбор кнопки «Удалить учетную запись»

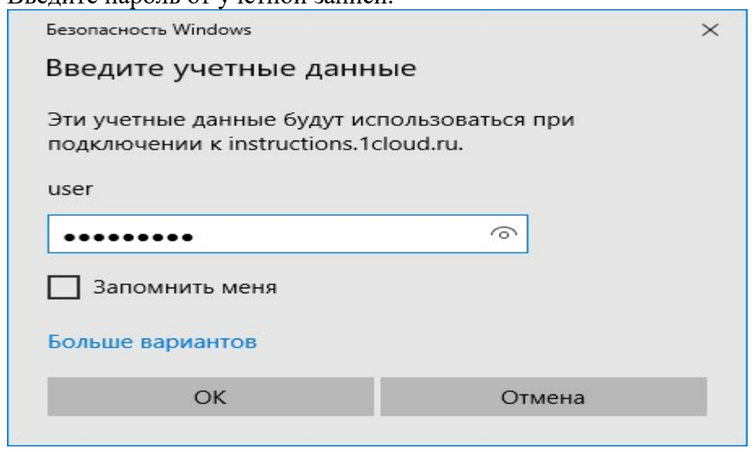
Ответ: 12345

14 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

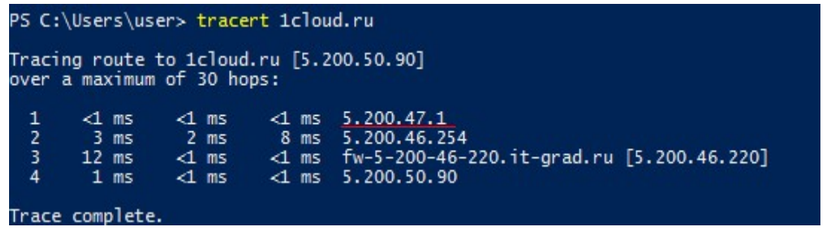
1 время входа в систему	А логическая связь между доменами, обеспечивающая сквозную проверку подлинности



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:

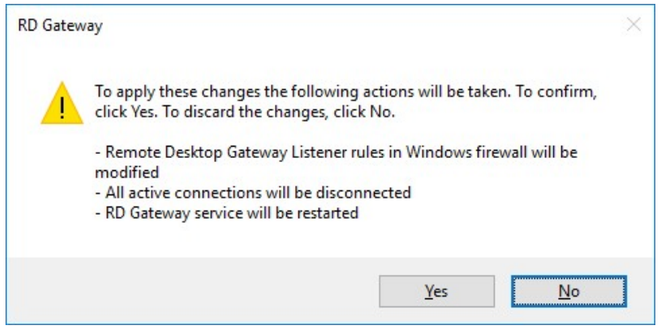


№13 Работа с Облачными бизнес-моделями IaaS: Установка.

№14 Работа с Облачными бизнес-моделями IaaS: Автоматизация. развёртывание виртуальной машины.

№15 Работа с Облачными бизнес-моделями IaaS: Балансировщик нагрузки виртуальных машин.

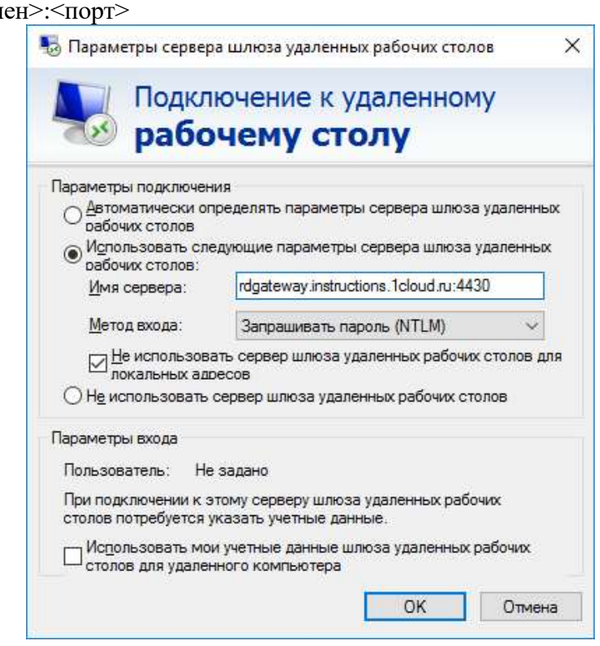
Стек облачных технологий состоит из трех частей, каждая из которых представляет отдельную категорию сервисов. На верхнем уровне располагается SaaS — по сути, это облачные приложения, доступ к которым предоставляется через веб-интерфейс. За ним следует PaaS — платформа для самостоятельной разработки и развертывания приложений.



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 ОК:
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.

2 домен	Б упрощенный поиск пользователя в сети
3 рабочая группа	В совокупность пользователей, ПЭВМ, контактов, других групп
4 доверительные отношения	Г администрируется как единый объект
5 группа	Д системное событие

Ответ 1Д, 2Г, 3Б, 4А 5В

15 Операционная система, являющаяся совокупностью операционных систем всех компьютеров сети, называется сетевая.

16 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 транспортные средства операционной системы	А совокупность клиентской и серверной частей операционной системы
2 коммуникационные протоколы	Б преобразует форматы запросов к ресурсам
3 редиректор	В переносят сообщения клиентской и серверной частей операционной системы по сети
4 клиентская часть операционной системы	Г распознает и перенаправляет запрос к удаленному компьютеру
5 сетевые средства операционной системы	Д поддерживают общий набор коммуникационных протоколов

Ответ 1Д, 2В, 3Г, 4Б 5А

17 Программа или процесс, выполняющий конкретную системную функцию по поддержке других программ, называется служба.

18 Укажите последовательность действий при активизации оснастки «Управление компьютером» для операционных систем серии Windows. *Запишите ответ в виде последовательности объектов/понятий.*
Объекты/понятия:
1 активизация кнопки «Пуск»
2 выбор команды «Панель управления»
3 активизация компонента «Учетные записи пользователей»
4 выбор подменю «Выбрать задание»

Ответ: 1234

19 Совокупность пользователей, компьютеров, контактов для управления доступом или в качестве списков рассылки называется группа.

20 Путь, по которому два устройства обмениваются данными в сети непосредственно друг с другом, называется канал.

21 Смена активного потока происходит если:
- ☐ Всем потокам предоставляют равные кванты времени
- ☐ Поток перешел в состояние ожидания
- ☐ Поток перешел в состояние готовности
- ☐ Потоку выделен новый квант времени

- Поток исчерпал квант времени

22 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 доступность	А доступ к данным только авторизованных пользователей
2 безопасность ПЭВМ	Б запрет неавторизованным пользователям модификации данных
3 целостность	В защита от удаленного несанкционированного доступа в сети
4 сетевая безопасность	Г авторизованные пользователи всегда получат доступ к данным
5 конфиденциальность	Д проблемы защиты данных ПЭВМ

Ответ 1Г, 2Д, 3Б, 4В 5А

23 Пароль – набор знаков, который должен быть введен пользователем для проверки учетного имени и получения доступа к ресурсам.

24 Укажите последовательность реализации совместимости на основе множественных равноправных API. *Запишите ответ в виде последовательности объектов/понятий.*

Объекты/понятия:

1 системный вызов приложения
2 обращение API к менеджеру ресурсов
3 нахождение операционной системой необходимого API
4 пересылка результата обработки запроса приложению
5 обращение менеджера ресурсов к базовым механизмам
6 обращение базовых механизмов на уровень машинозависимых задач

Ответ: 132564

25 *Вставьте пропущенное слово.* Пользователю сетевой операционной системы необходимо знать, на каком компьютере в сети хранятся файлы, с которыми он работает.

Вариант 3

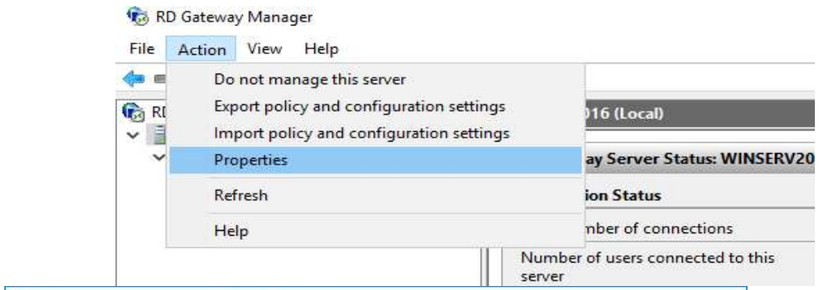
1 Укажите, к каким последствиям приводит отсутствие синхронизации процессов и потоков в операционной системе

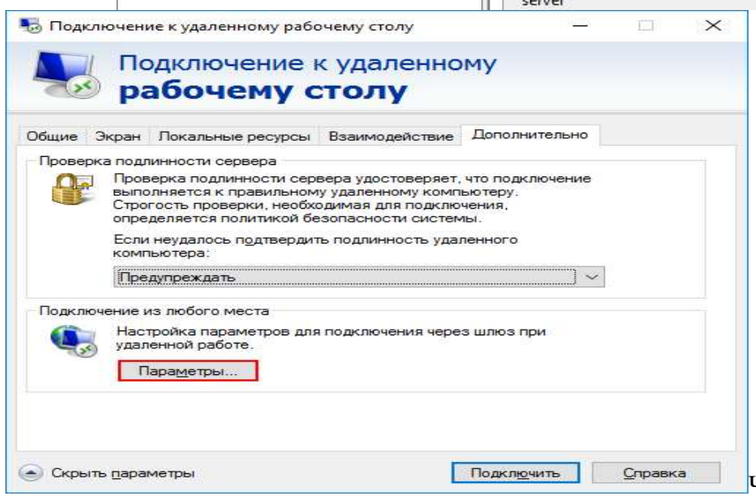
- Тупики
- Гонки
- Критические секции
- Сигналы
- Семафоры

2 Укажите последовательность изменения типа учетной записи пользователя средствами операционных систем серии Windows. *Запишите ответ в виде последовательности объектов/понятий.*

Объекты/понятия:

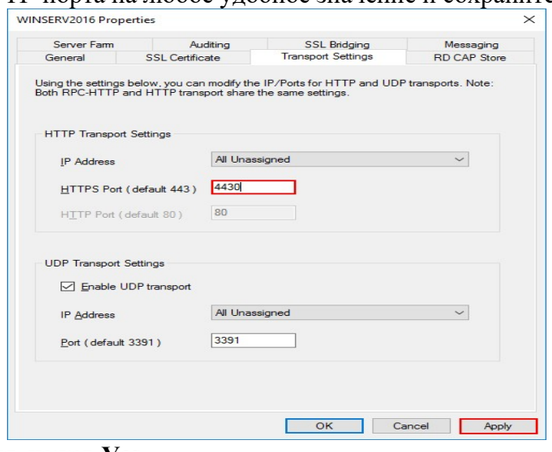
1 выбор нового типа учетной записи
2 выбор учетной записи, которую необходимо изменить
3 активизация кнопки «Изменить тип учетной записи»
4 активизация компонента «Учетные записи пользователя»
5 выбор кнопки «Изменить тип учетной записи»



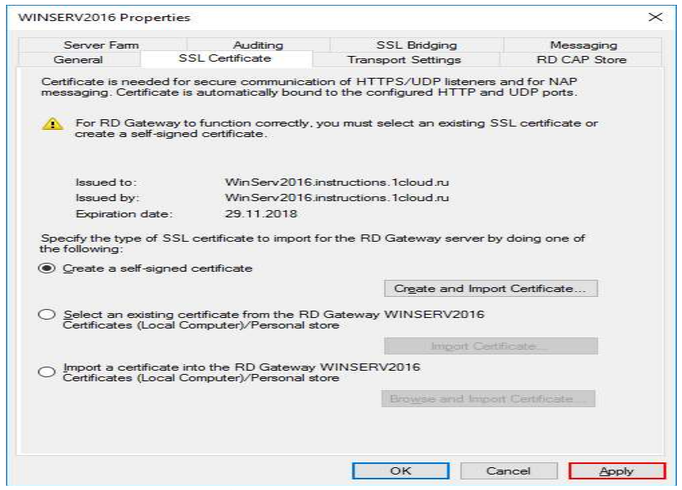


Чтобы изменить номер порта для шлюза RD, щелкните правой кнопкой мыши имя сервера и выберите свойства в консоли управления удаленным рабочим столом (Action →Properties).

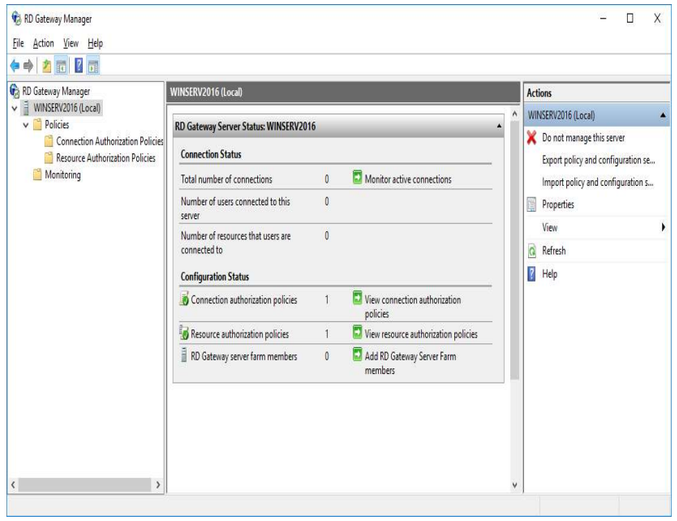
Измените значение HTTP-порта на любое удобное значение и сохраните изменения.



Подтвердите изменения, нажав **Yes**.



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.

Ответ: 42513

3 Устройство, которое позволяет передавать и принимать информацию от компьютера по телефонной линии, называется модем.

4 Укажите методы использования внешней памяти

- ☐ Фиксированные разделы
- ☐ Динамические разделы
- ☐ Сегментно-страничное распределение
- ☐ Универсальное распределение
- ☐ Сдвигаемые разделы

5 Служба, поддерживающая транспорты для асинхронного обмена сообщениями между узлами, называется ISM.

6 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 неумышленные угрозы	А использование недокументированных возможностей операционной системы для проникновения через уязвимые места в систему безопасности
2 риск	Б целенаправленные действия для нанесения ущерба
3 умышленные угрозы	В атака
4 реализованная угроза	Г ошибочные действия локальных пользователей, ненадежная работа программ
5 незаконное проникновение	Д вероятностная оценка возможного ущерба

Ответ 1Г, 2Д, 3Б, 4В 5А

7 Как называется список программ или задач, ожидающих выполнения? (Очередь)

8 В какой последовательности реализуется системный вызов в микроядерной архитектуре ядра операционной системы. *Запишите ответ в виде последовательности объектов/понятий.*

Объекты/понятия:

1 запрос разрешения обслуживания
2 запрос сервера
3 обработка запроса «сервер - микроядро»
4 обработка запроса «микроядро - приложение»
5 сигнал «Разрыв связи»

Ответ: 12345

9 Микроядерная архитектура операционной системы включает микроядро, приложения пользователя, серверы.

10 Укажите задачи операционной системы по управлению файлами и устройствами

- ☐ Параллельная работа устройств ввода – вывода и процессора
- ☐ Разделение устройств и данных между процессами
- ☐ Поддержка нескольких файловых систем

- Определение скорости обмена данными
- Поддержка менеджера ввода - вывода

11 Установите последовательность для создания новой учетной записи пользователя стандартными средствами операционных систем серии Windows. *Запишите ответ в виде последовательности объектов/понятий.*

Объекты/понятия:

1 открытие окна «Управление компьютером»
2 активизация компонента «Учетные записи пользователя»
3 задание в диалоговом окне имени учетной записи, нажатие кнопки «Далее»
4 выбор типа учетной записи
5 выбор задания «Создание учетной записи», активизация кнопки «Создать»

Ответ: 12534

12 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 пароль	А набор правил и соглашений для передачи данных по сети
2 рядовой сервер	Б средство защиты, используемое для управления входом в систему и организация доступа к ПЭВМ и ресурсам
3 контроллер домена	В хранит сведения об объектах сети
4 каталог	Г ПЭВМ, не являющаяся контроллером домена
5 протокол	Д управляет входом пользователя в сеть

Ответ 1Г, 2Г, 3Д, 4В 5А

13 В какой последовательности можно создать пароль для учетной записи пользователя средствами операционных систем серии Windows *Запишите ответ в виде последовательности объектов/понятий.*

Объекты/понятия:

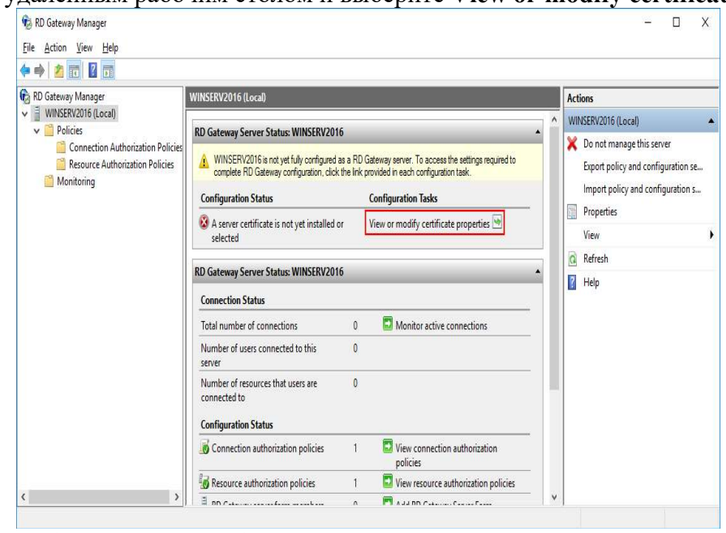
1 выбор компонента «Учетные записи пользователя»
2 создать пароль, заполнив диалоговые поля
3 активизировать кнопку «Создать пароль»
4 выбрать вкладку «Изменение учетной записи»
5 активизировать кнопку «Создать пароль»

Ответ: 14325

14 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 разрешение	А ПЭВМ, предоставляющая общие ресурсы пользователям сети
2 общий ресурс	Б предоставляется владельцем объекта
3 ресурс	В элемент (оборудование), которое может быть подключено к сети или ПЭВМ

управления удаленным рабочим столом и выберите **View or modify certificate properties**.

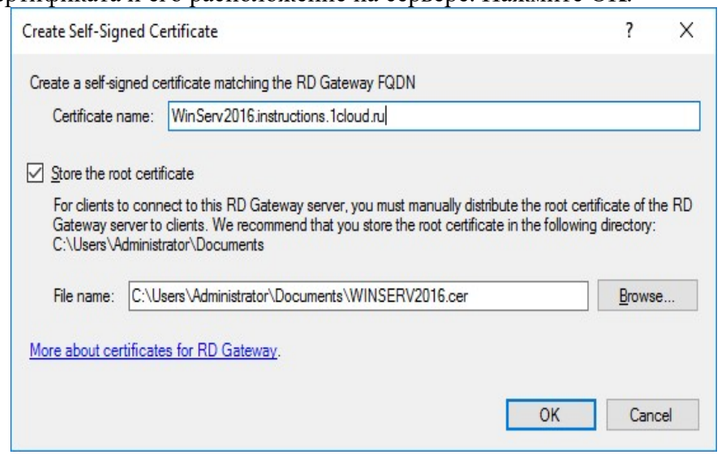


Возможно 3 способа импорта сертификатов:

- создание самоподписанного сертификата и его импорт;
- импорт ранее загруженного сертификата (самоподписанного или стороннего);
- загрузка стороннего сертификата (например, Comodo) и его импорт;

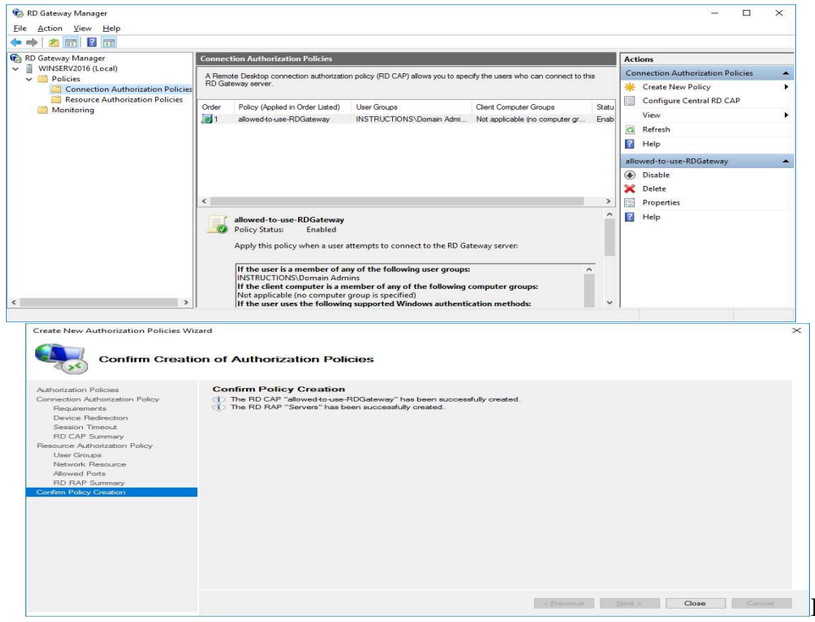
Выберите подходящий вам способ, в нашем примере мы рассмотрим первый случай с генерацией и импортом самоподписанного сертификата.

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



Сертификат будет сгенерирован.

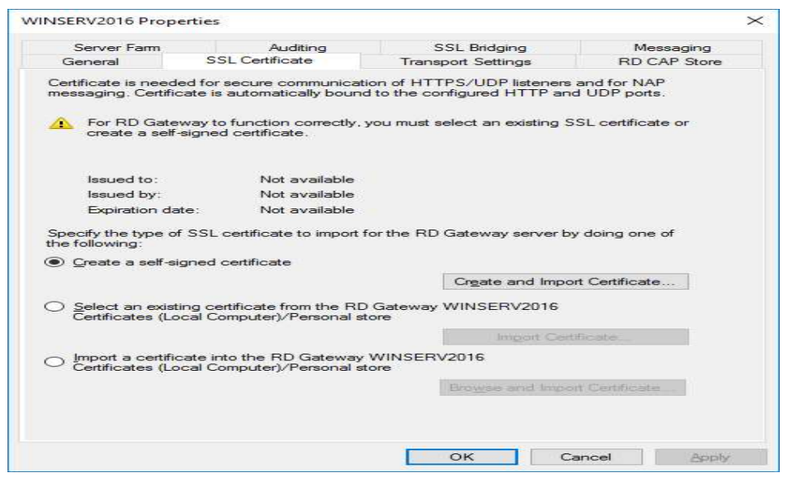
В результате отобразится - кому, кем и до какого числа выдан ssl-сертификат. Нажмите Apply для сохранения изменений.



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



4 устройство	Г ресурсы, доступные для пользователей сети
5 сервер	Д элемент, который может быть предоставлен в пользование объекту сети

Ответ 1Б, 2Г, 3Д, 4В 5А

15 Переносимые операционные системы имеют несколько вариантов реализации для разных платформ. Такое свойство операционной системы называется многоплатформенность.

16 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 одноранговая сеть	А сеть крупной организации
2 сеть с выделенным сервером	Б крупные сети с повышенной функцией безопасности, выделенной клиентской частью
3 гибридные сети	В небольшая сеть организации
4 локальная сеть	Г крупные сети с повышенной функцией безопасности
5 глобальная сеть	Д сети небольшой организации (до 30 ПЭВМ) с выделенной клиентской частью

Ответ 1Д, 2Г, 3Б, 4В 5А

17 Как называются несколько одинаковых принтеров, подключенных к одному серверу печати и функционирующих как единый принтер? (пул).

18 Укажите последовательность реализации множественных прикладных сред в микроядерной структуре ядра операционной системы. *Запишите ответ в виде последовательности объектов/понятий.*

Объекты/понятия:

1 системный вызов приложения
2 обработка и выполнение запроса прикладной среды
3 запрос прикладной среды
4 пересылка результата обработки запроса приложению
5 результат запроса обрабатывается микроядром

Ответ: 13254

19 Разъем, к которому подключаются устройства USB, - порт.

20 Устройство, которое переводит аналоговые сигналы в цифровую форму, называется модем.

21 Реализация системных вызовов должна обеспечивать

- Контроль со стороны операционной системы за корректной работой процессов
- Расширение набора системных вызовов
- Высокая скорость печати
- Высокая скорость вызова процедур операционной системы
- Контроль операционной системы за корректным использованием системных вызовов

22 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 сетевой сервис	А сетевые службы
2 клиент – серверная система	Б инициализация запросов в сети
3 серверная часть операционной системы	В интерфейс между сервером и клиентом
4 клиентская часть операционной системы	Г сетевые службы, объединенные в виде некоторого набора программ
5 сетевые оболочки	Д пассивное ожидание запросов

Ответ 1В 2А, 3Д, 4Б 5Г

23 Средство защиты, используемое для управления входом в систему по учетным записям пользователя, - пароль.

24 В какой последовательности реализуется переключение пользователей в операционных систем серии Windows? *Запишите ответ в виде последовательности объектов/понятий.*

Объекты/понятия:

1 активизировать кнопку «Пуск»
2 активизировать кнопку «Завершение сеанса»
3 нажать кнопку «Смена пользователей»
4 выбор учетной записи нового пользователя

Ответ: 1324

24 Безопасность – это набор стандартных служб и протоколов сети на основе криптографии.

Вариант 4

1 Укажите функции операционной системы по управлению памятью в мультипрограммном режиме

- ☐ Отслеживание наличия свободной и занятой памяти
- ☐ Обработка запросов приложений
- ☐ Установка парольной защиты приложений
- ☐ Защита памяти процессов от взаимного вмешательства
- ☐ Выделение памяти процессам

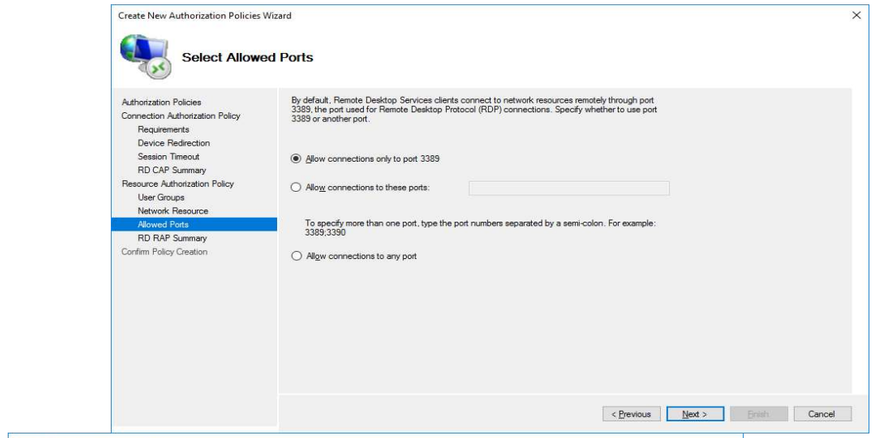
2 В какой последовательности реализуется переключение пользователей в операционных систем серии Windows? *Запишите ответ в виде последовательности объектов/понятий.*

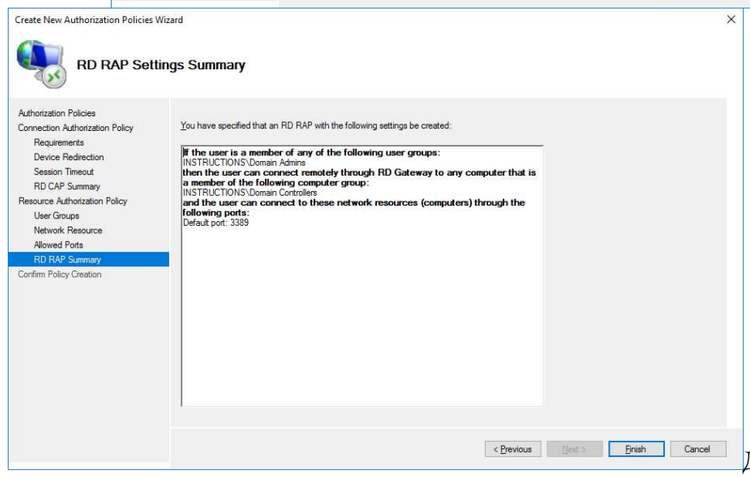
Объекты/понятия:

1 активизировать кнопку «Пуск»
2 активизировать кнопку «Завершение сеанса»
3 нажать кнопку «Смена пользователей»
4 выбор учетной записи нового пользователя

Ответ: 1324

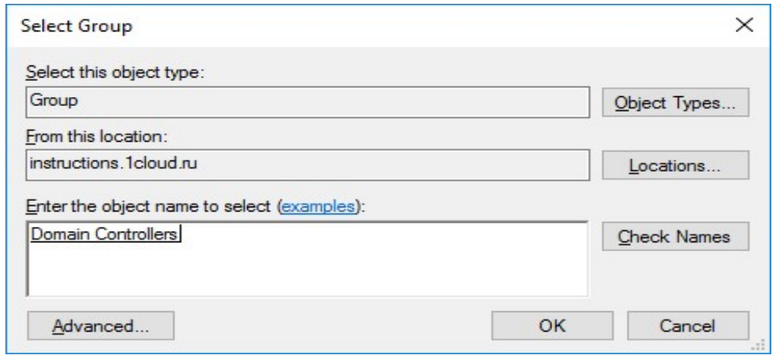
3 Как называется топология сети, если компьютер получает данные, предназначенные для другого компьютера, и пересылает их далее по сети последовательно? (кольцо)



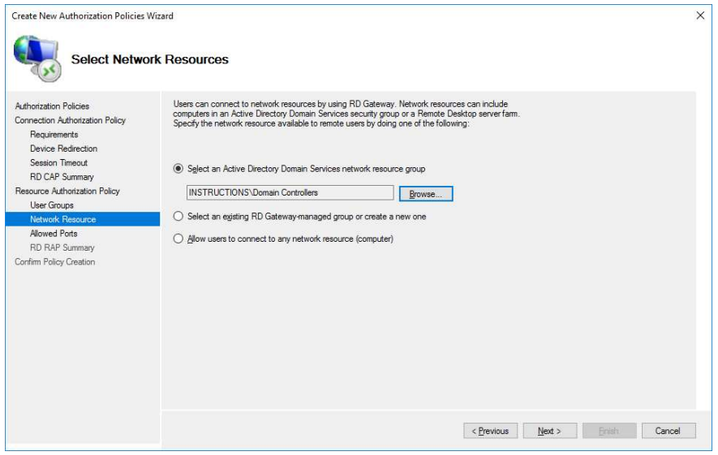


Далее отобразится результат создания политик.

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.

4 Укажите, какие методы распределения памяти можно рассматривать как частный случай виртуальной памяти

- ☐ Распределение динамическими разделами
- ☐ Распределение фиксированными разделами
- ☐ Страничное распределение
- ☐ Сегментное распределение
- ☐ Сегментно-страничное распределение

5 Любое оборудование, которое может быть подсоединено к локальной сети, называется сетевое устройство.

6 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 выделенный сервер сети	А ПЭВМ, обращающаяся с запросом к ресурсам другого компьютера
2 клиентский узел	Б сеть, включающая узлы всех типов
3 одноранговый узел	В ПЭВМ, обслуживающая только запросы других ПЭВМ сети
4 гибридная сеть	Г сеть, включающая узлы «клиент», «сервер»
5 сеть с выделенным сервером	Д компьютер, совмещающий функции клиентской и серверной частей

Ответ 1В, 2А, 3Д, 4Б 5Г

7 Устройство, которое добавляется в структуру сети для поддержки возможности трансляции, - это шлюз.

8 Установите последовательность действий при создании нового имени для учетной записи в операционной системе серии Windows. *Запишите ответ в виде последовательности объектов/понятий.*
Объекты/понятия:

1 активизация компонента «Учетные записи пользователя»
2 выбор изменяемой учетной записи
3 выбор вкладки «Изменение имени»
4 задание нового имени в открывшемся диалоговом окне
5 активизация кнопки «Сменить имя»

Ответ: 21435

9 Как называется процесс определения прав пользователя в сети? (авторизация)

10 Выберите верные утверждения

- ☐ Драйвер выполняет низкоуровневые функции управления устройствами ввода - вывода
- ☐ Драйвер выполняет функции управления файловой системой
- ☐ Все функции драйверов вызываются по прерыванию
- ☐ Драйвер является частью подсистемы ввода – вывода
- ☐ Драйвер организует взаимодействие модулей ядра операционной системы
- ☐ Драйвер функционирует в привилегированном режиме

11 Установите последовательность смены режимов для операционной системы классической структуры. *Запишите ответ в виде последовательности объектов/понятий.*

Объекты/понятия:
1 пользовательский режим
2 системный вызов
3 привилегированный режим
4 сигнал подтверждения готовности
5 сигнал «Разрыв связи»

Ответ: 12435

12 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 политика безопасности	А предотвращает доступ к сети нежелательных лиц, разрешает вход для легальных пользователей
2 аутентификация	Б контроль доступа легальных пользователей
3 идентификация	В комплекс мер по защите сети организации от нелегального проникновения
4 авторизация	Г фиксация событий, связанных с доступом к защищаемым системным ресурсам
5 аудит	Д сообщение пользователям своего идентификатора системе

Ответ 1В, 2А, 3Д, 4Б 5Г

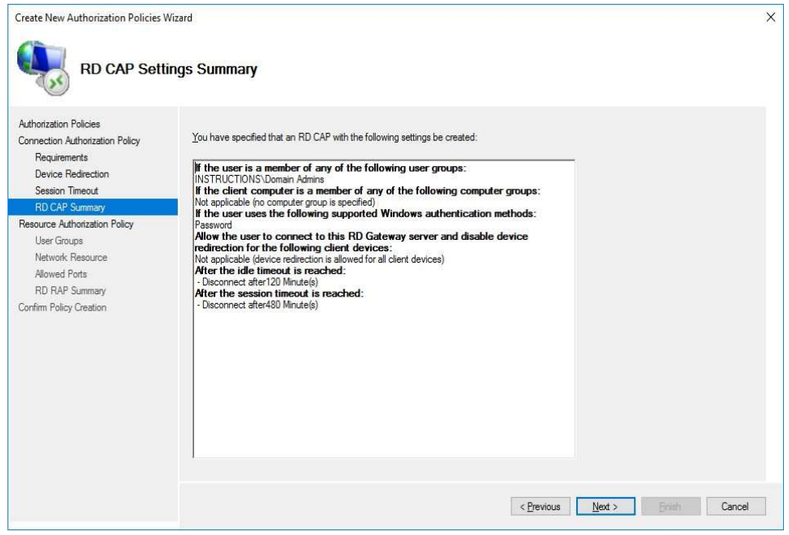
13 В какой последовательности выполняется обработка системных вызовов в монолитной операционной системе. *Запишите ответ в виде последовательности объектов/понятий.*
Объекты/понятия:
1 запрос разрешения обслуживания
2 обработка запросов
3 выполнение запроса, готовность обслуживания
4 работа приложения
5 сигнал «Разрыв связи»

Ответ: 12345

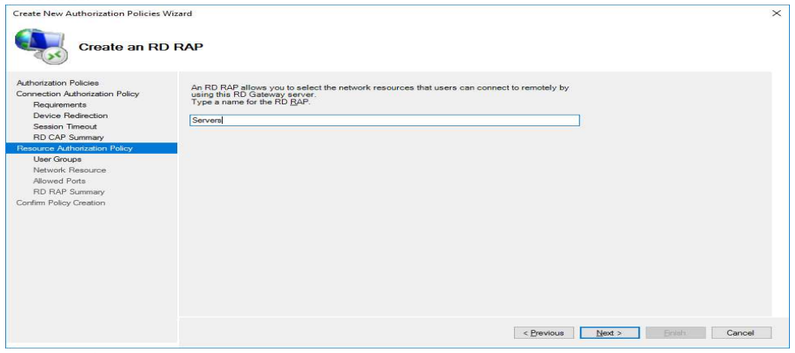
14 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 домен	А иерархическая распределенная система сопоставления доменных имен
2 система доменных имен	Б обладают полным доступом к домену или компьютеру
3 политика	В группа компьютеров в сети, образующих общую базу данных каталога
4 администратор	Г содержит все сведения, определяющие пользователя в операционной системе
5 учетная запись	Д способ автоматизации работы администратора по настройке

Ответ 1В, 2А, 3Д, 4Б 5Г

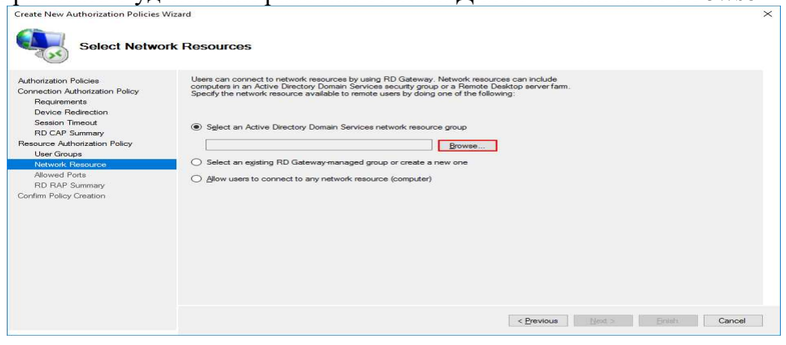


Далее вы перейдете к настройке политики авторизации ресурсов. Введите удобное имя политики.

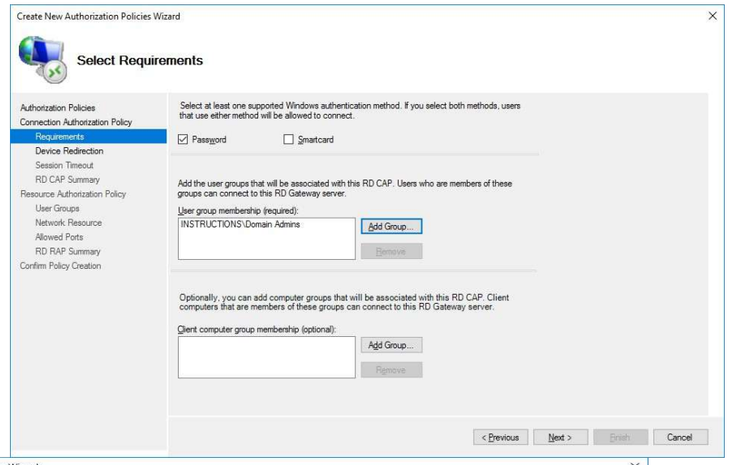


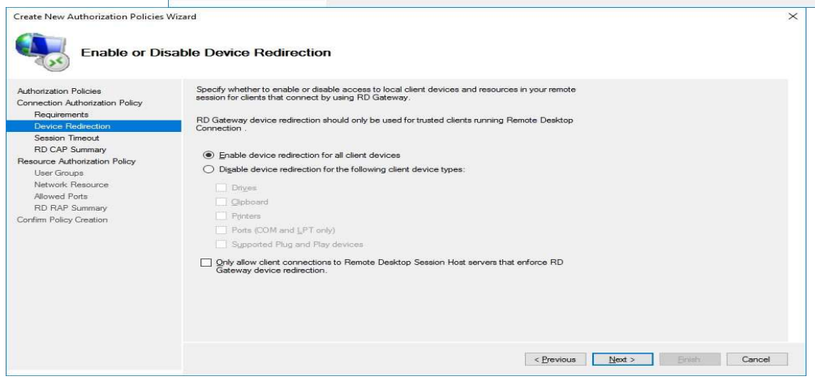
Также добавьте группы пользователей, которые смогут подключаться к сетевым ресурсам.

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

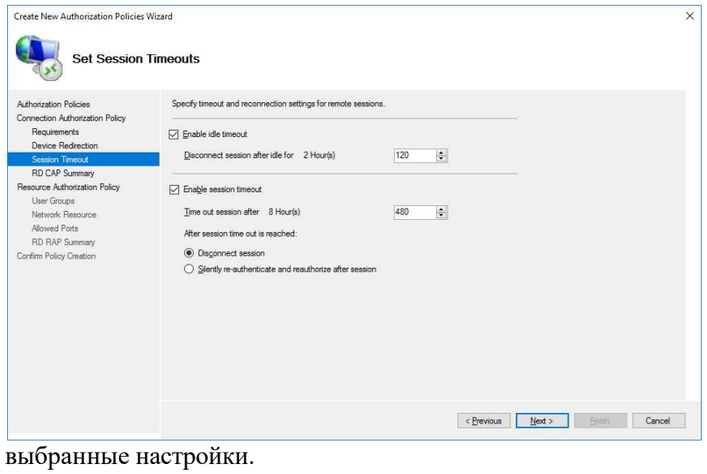


Выберите устройства и ресурсы удаленной сессии, которые будут доступны клиентам использующие шлюз.





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



Перепроверьте выбранные настройки.

15 Как называется коммуникационная линия, предназначенная для передачи данных между объектами операционной системы? (Шина)

16 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 клиентская часть операционной системы	А правила взаимодействия компьютера при передаче сообщений по сети
2 средства управления локальными ресурсами компьютера	Б обеспечивают передачу сообщений между компьютерами сети
3 серверная часть	В реализация функций операционной системы автономного компьютера
4 транспортные средства операционной системы	Г средства предоставления локальных ресурсов в общее пользование
5 коммуникационный протокол	Д не получает непосредственного доступа к ресурсам другого компьютера в сети

Ответ 1Д, 2В, 3Г, 4Б 5А

17 Адрес, соответствующий всем узлам в конкретном сегменте сети, - это широковещание.

18 В какой последовательности можно удалить учетную запись пользователя, созданную средствами операционных систем серии Windows? *Запишите ответ в виде последовательности объектов/понятий.*

Объекты/понятия:

1 активизация компонента «Учетная запись пользователя»
2 выбор учетной записи
3 активизация кнопки «Удаление учетной записи»
4 выбор кнопки «Удалить эти файлы»
5 выбор кнопки «Удалить учетную запись»

Ответ: 12345

19 Как называется процесс маскирования сообщений или данных с целью скрытия их содержания? (Шифрование)

20 Группа независимых компьютеров, работающих вместе как единая система, предоставляющая клиентам общий набор служб, называется кластер.

21 Выберите события, требующие перераспределения процессорного времени

- ☐ Прерывание от таймера при завершении кванта времени, отведенного выполняемой задаче
- ☐ Просмотр планировщиком очереди процессов
- ☐ Запрос ввода – вывода
- ☐ Выгрузка части процесса на диск
- ☐ Освобождение ресурса

22 Подберите к каждому объекту в левом столбце характеризующую его фразу из правого столбца. Определите соответствующие пары объектов и запишите в виде: число-буква

1 владелец	А объединение компьютеров, предназначенное для упрощения поиска пользователем объектов
2 администратор	Б Совокупность пользователей для управления доступом
3 группа	В объект операций по управлению
4 агент	Г пользователь, управляющий разрешениями объекта
5 рабочая группа	Д пользователь, ответственный за настройку и управление контроллером домена, локальным компьютером

Ответ 1Г, 2Д, 3Б, 4В 5А

23 Любой компьютер или программа, подключающиеся к службам другого компьютера в сети, - это клиент.

24 Укажите, в какой последовательности можно создать пароль для учетной записи пользователя средствами операционных систем серии Windows? *Запишите ответ в виде последовательности объектов/понятий.*

Объекты/понятия:

1 выбор компонента «Учетные записи пользователя»
2 создать пароль, заполнив диалоговые поля
3 активизировать кнопку «Создать пароль»
4 выбрать вкладку «Изменение учетной записи»
5 активизировать кнопку «Создать пароль»

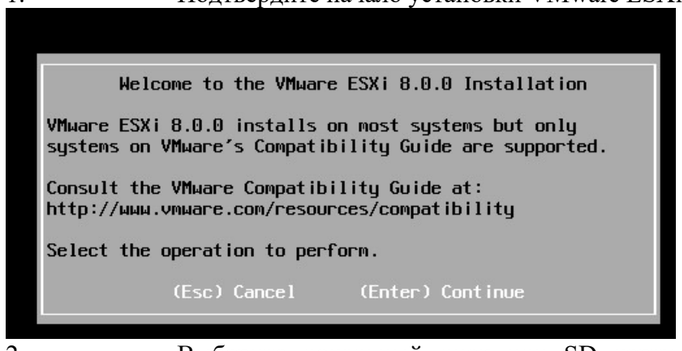
Ответ: 14325

25 Как называется устройство, преобразующее аналоговые сигналы в цифровую форму? (модем)

№1 Работа с Hypervisor: Установка и настройка hosted

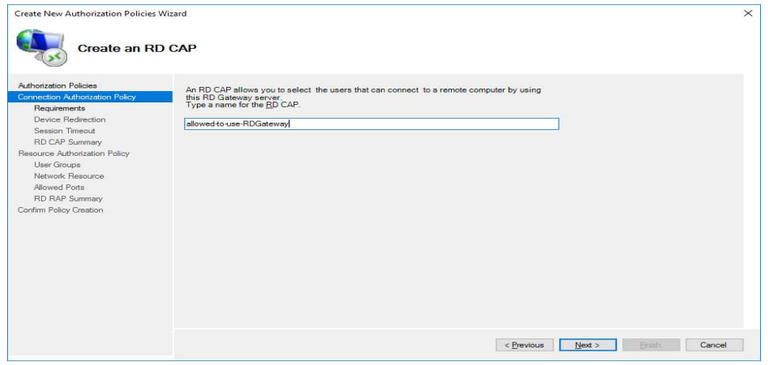
№2 Работа с Hypervisor: Установка и настройка нативного Hypervisor.

1. Подтвердите начало установки VMware ESXi 8.0.0;

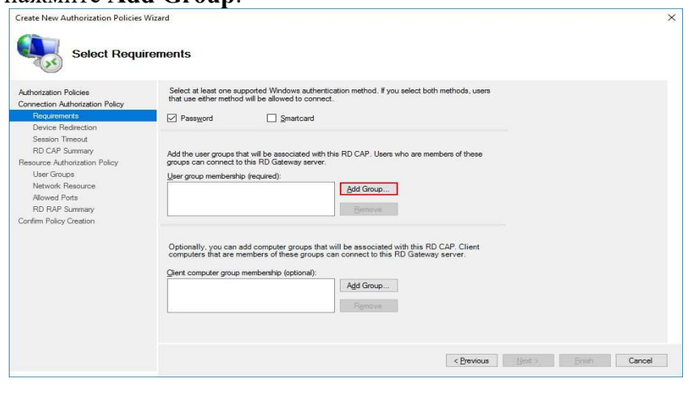


2. Выберите локальный диск или SD карту, на который нужно установить операционную систему. Рекомендуется диск размером не менее 10 Гб;

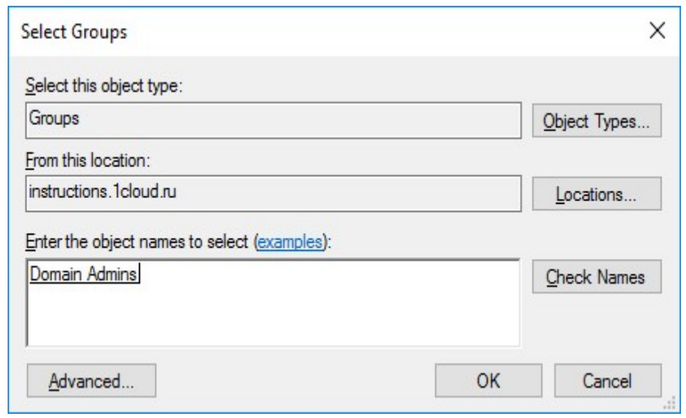
Введите удобное имя для политики авторизации подключения.



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**.

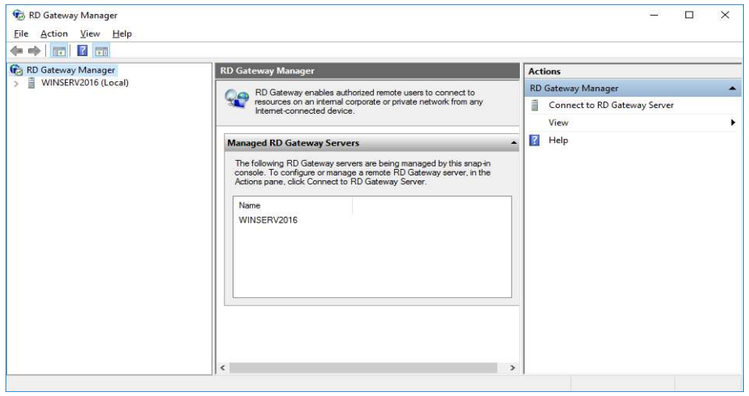


Выберите нужную группу, например, администраторов домена или контроллеры домена. Выполнить поиск можно с помощью кнопки **Check Names**.

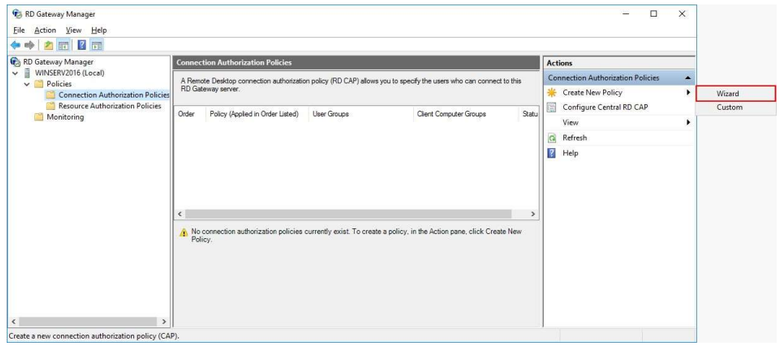


После добавления групп можно переходить к следующему действию.

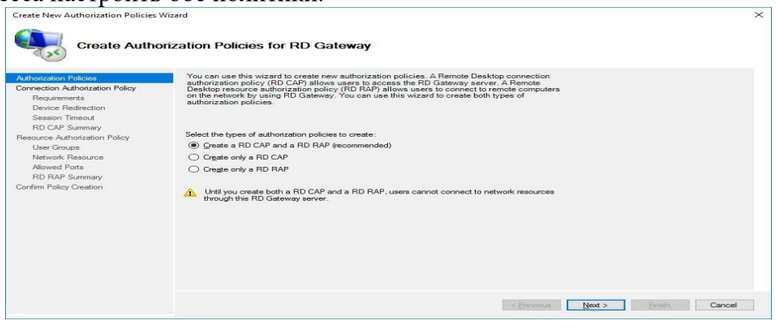
Перед вами откроется менеджер шлюза.

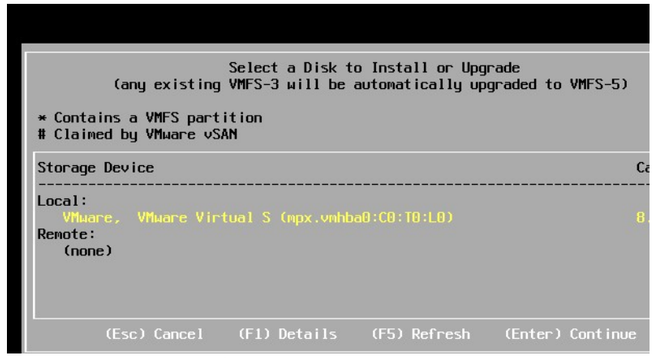


Для создания политик авторизации в древовидной структуре откройте **RD Gateway Manager → <Имя сервера> → Policies → Connection Authorization Policies**. В вертикальном меню Actions справа выберите **Create New Policy → Wizard**.



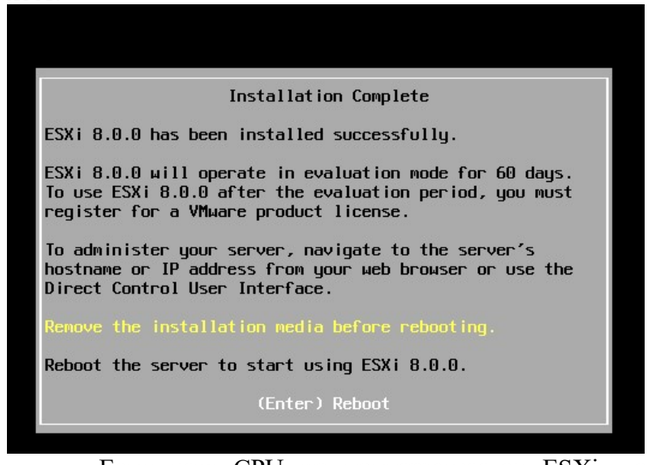
В открывшемся окне выберите Create RD CAP and RD RAP (recommended), чтобы с помощью одного процесса настроить обе политики.





3. Выберите раскладку клавиатуры;
4. Введите и подтвердите пароль root (не менее 7 символов);

5. После завершения установки извлечите установочную флешку и перезагрузите хост.



Если ваш CPU не поддерживается ESXi, то при установке появится ошибка: Unsupported CPU:

CPU_SUPPORT_ERROR: The CPU in this host is not supported by ESXI 8.0.0

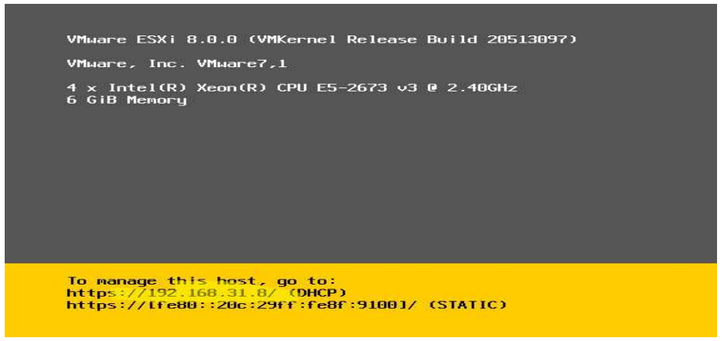
В тестовой среде вы можете игнорировать совместимость CPU с помощью параметра allowLegacyCPU=true. Для этого нажмите при загрузке Shift+O и выполните команду:

<ENTER: Apply options and boot>

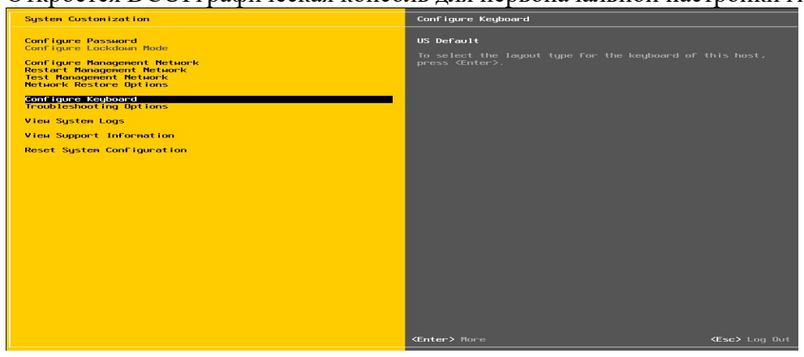
> cdromBoot runweasel allowLegacyCPU=true

Гипервизор VMware vSphere установлен. Если ваш сервер подключен к сети с DHCP сервером он автоматически получит IP адрес, который вы увидите в консоли гипервизора (называется она Direct Console User Interface, DCUI).

Этот IP адрес используется для управления гипервизором из web- интерфейса.

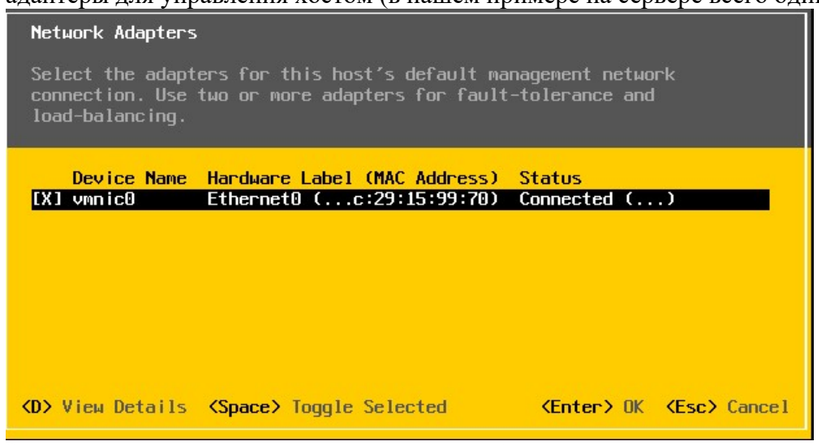


Для управления настройками VMware Hypervisor на экране DCUI нажмите **F2**, введите логин (по умолчанию root) и пароль, заданный в процессе установки.
Откроется DCUI графическая консоль для первоначальной настройки гипервизора.

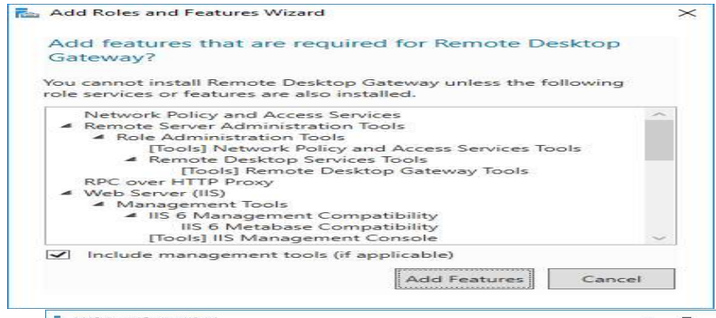


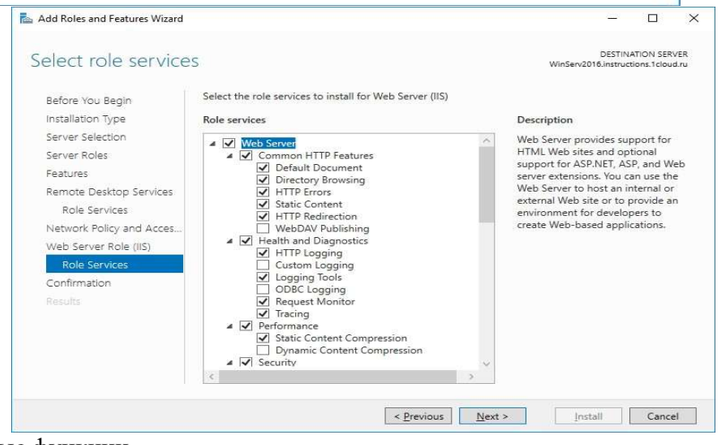
Здесь можно настроить следующие опции:

1. **Configure Password** — изменить пароль:
2. В секции **Configure Management Network** можно настроить параметры сетевых адаптеры для управления хостом (в нашем примере на сервере всего один сетевой адаптер);



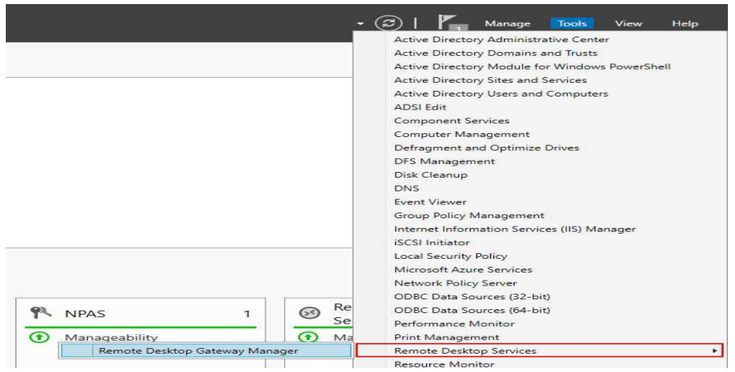
3. Можно задать номер **VLAN**, в котором находится интерфейс управления сервером;
4. Настройте параметры IPv4 и/или IPv6 сетевого интерфейса. Можно их отключать, назначать динамические или статические IP. В большинсвтах случаях адрес, подсеть и адрес шлюза на сервере задаются вручную;





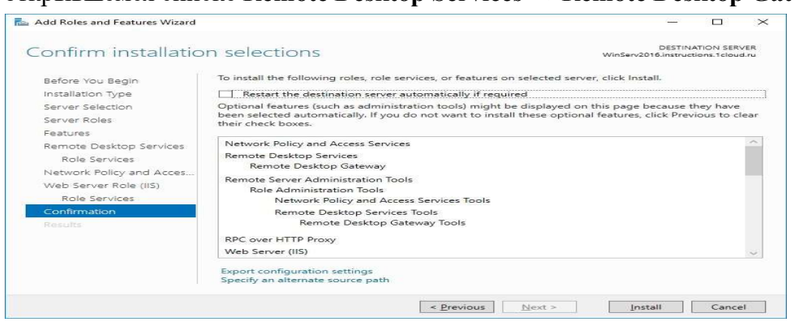
Добавьте данные функции.

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

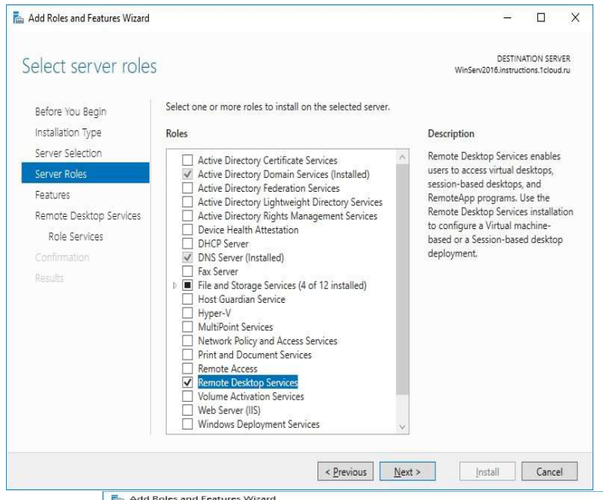


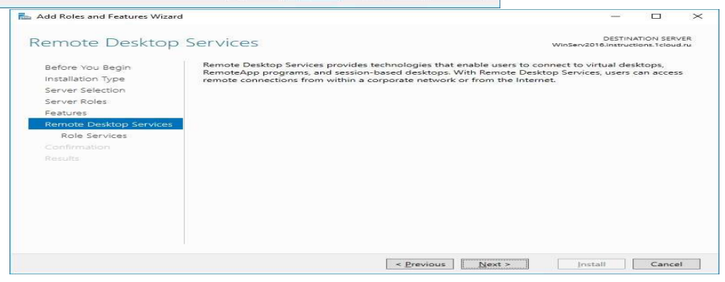
Создание политики авторизации подключения и ресурсов

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

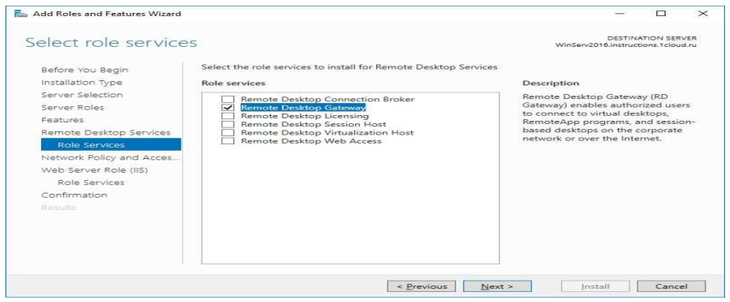


Далее вы увидите краткую информацию о роли.

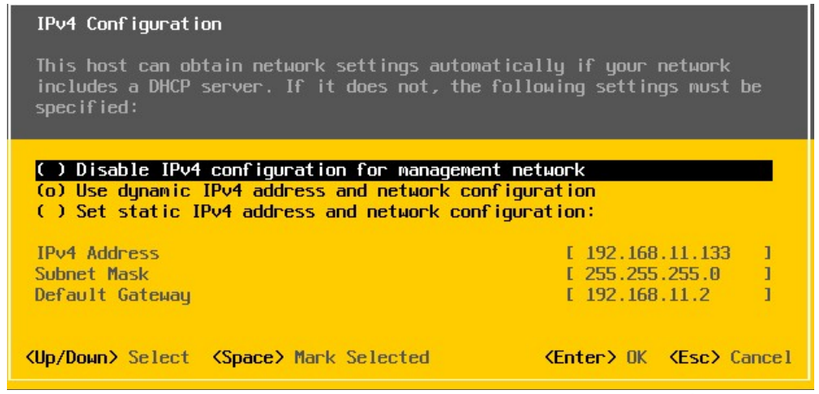




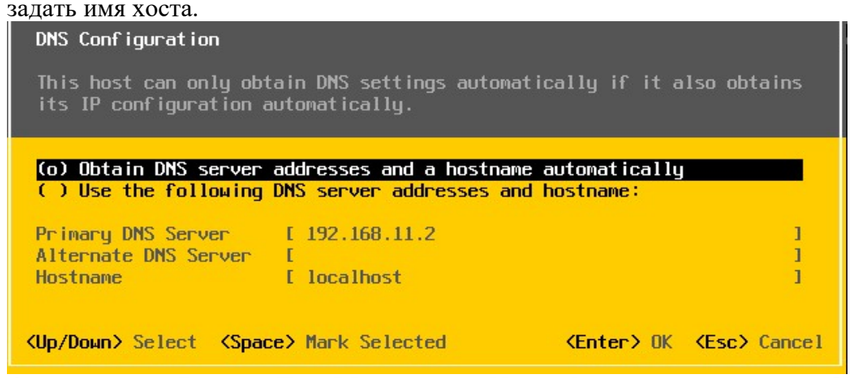
Далее добавьте сервис **Remote Desktop Gateway**.



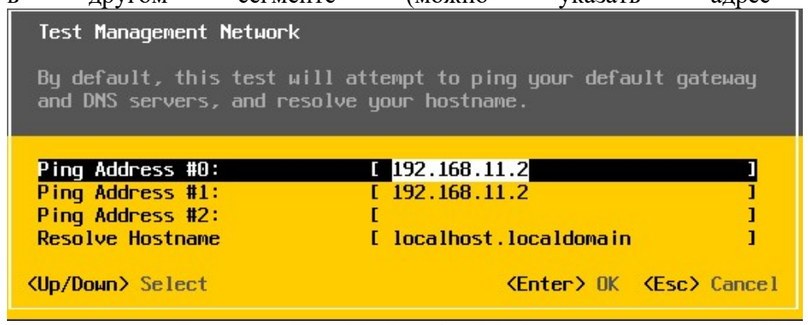
Для работы этого сервиса необходимо веб-сервер IIS и дополнительные административные инструменты, они будут предложены автоматически, если не были установлены ранее.



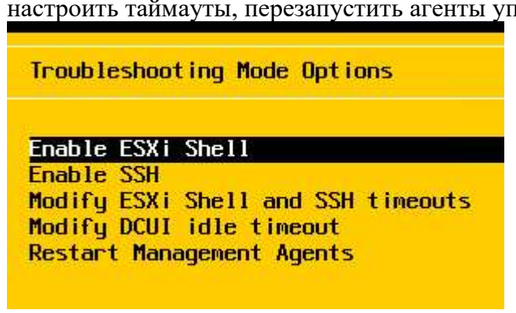
5. **DNS Configuration** – здесь можно указать primary и secondary DNS сервера и задать имя хоста.



6. В меню **Test Management Network** можно проверить работу сети (командой ping) и разрешение имен через DNS. Проверьте что с хоста доступны IP адреса шлюза, и сервера в другом сегменте (можно указать адрес DNS сервера).



7. В разделе **Troubleshooting Mode** можно: включить SSH доступ к хосту VMware, настроить таймауты, перезапустить агенты управления ESXi.



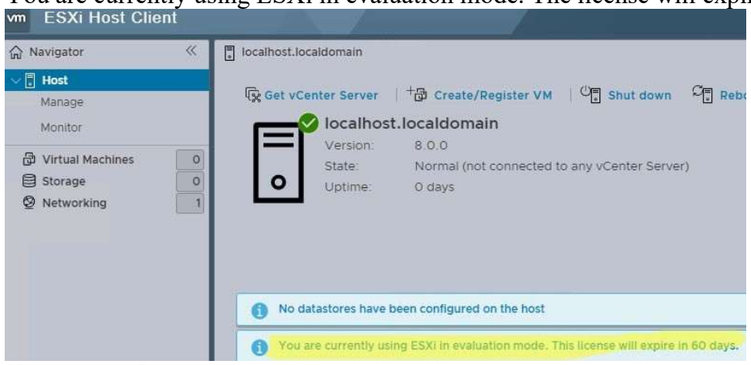
Через SSH консоль вы можете установить обновления на хосте ESXi.

Первоначальная настройка VMware vSphere Hypervisor закончена. Можно подключаться через Web- интерфейс.

Настройка VMware ESXi через Web-интерфейс Host Client

Веб-интерфейс Host Client – основной интерфейс управления VMware Hypervisor. Чтобы подключиться к веб интерфейсу, откройте браузер на своем компьютере и введите в адресную строку IP адрес вашего хоста ESXi (который отображается в консоли DCUI). Введите логин (root) и пароль.

Обратите внимание, что в консоли Host Client отображается надпись:
You are currently using ESXi in evaluation mode. The license will expire in 60 days.



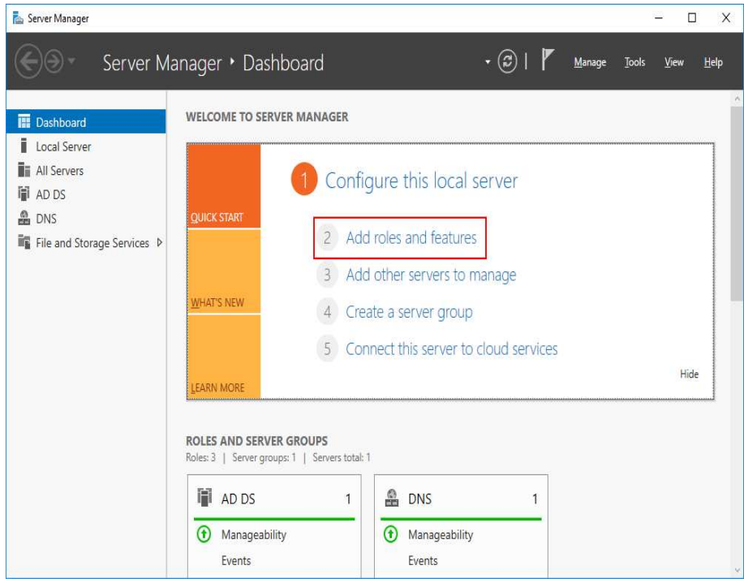
Установим бесплатный ключ vSphere Hypervisor, который вы получили ранее.
Перейдите в раздел **“Manage” -> “Licensing” -> “Assign License”** и активируйте лицензию.

Если не активировать лицензию, через 60 дней все запущенные ВМ продолжат работу, но вы не сможете включить новые ВМ или перезагрузить имеющиеся ВМ.

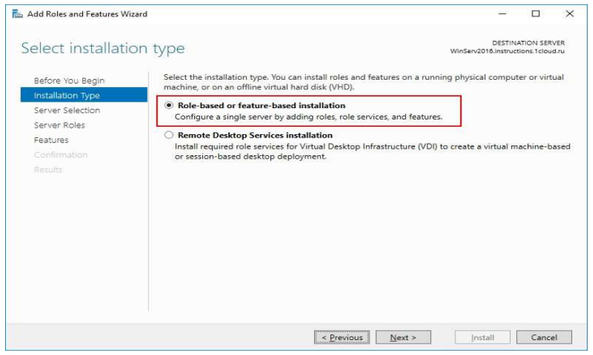
Для гипервизора активирована неограниченная по времени (Expires: Never) лицензия с неограниченным объемом оперативной памяти для виртуальных машин. Каждой виртуальной машине вы сможете выделить до 8 виртуальных vCPU (Up to 8-way virtual SMP).

Базовые настройки ESXi находятся в разделе Manage.

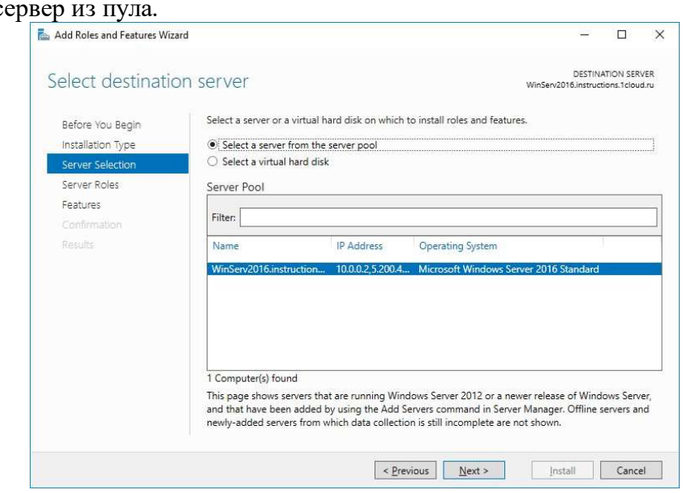
Откройте **Диспетчер серверов** и выберите пункт **Add roles and features**.



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



Выберите ваш сервер из пула.



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

• Beats – это облегченные агенты, которые устанавливаются на периферийных хостах для сбора различных типов данных и последующей их пересылки в стек. Например, это может быть Filebeat, Metricbeat, Packetbeat, Winlogbeat и другие.

• Kibana – это инструмент для визуализации и анализа данных, интегрированный с Elasticsearch. Рабочий процесс ELK Stack представлен на картинке ниже:

Здесь Beats и Logstash совместно выполняют сбор и обработку логов, Elasticsearch хранит их, а Kibana создает визуализацию.

№11 Настройка виртуальных машин для шлюза удалённого рабочего стола

№12 Настройка межплатформенный бесклиентский шлюз удаленного рабочего стола

Remote Desktop Gateway — роль, которая использует протокол удаленного рабочего стола RDP через протокол HTTPS, благодаря которому пользователи могут установить безопасное, зашифрованное соединение с внутренними сетевыми ресурсами, где выполняются их приложения. Основное преимущество заключается в том, что пользователю не нужно устанавливать VPN-соединение с корпоративной сетью перед подключением к серверу терминалов. Вместо этого они подключаются к серверу терминалов через шлюз.

RD Gateway предоставляет множество преимуществ:

• шлюз позволяет удаленным пользователям подключаться к внутренним сетевым ресурсам через Интернет, используя зашифрованное соединение, без необходимости подключения виртуальных частных сетей (VPN);

• шлюз предоставляет комплексную конфигурацию безопасности, которая позволяет контролировать доступ к определенным внутренним сетевым ресурсам;

• шлюз обеспечивает одноточечное RDP-соединение и не позволяет удаленным пользователям получать доступ ко всем внутренним сетевым ресурсам;

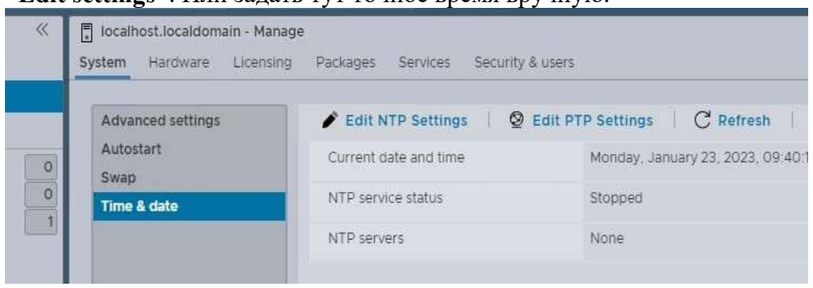
• шлюз позволяет подключаться к внутренним сетевым ресурсам, которые размещаются за брандмауэрами в частных сетях и между NAT;

• консоль диспетчера шлюза позволяет настраивать политики авторизации для определения условий, которые должны быть выполнены для удаленных пользователей при подключении к внутренним сетевым ресурсам. Например, можно указать: кто может подключаться к сетевым ресурсам и к каким сетевым ресурсам (группам серверов), должны ли клиентские компьютеры быть членами групп безопасности Active Directory, разрешено ли перенаправление устройства и диска;

• консоль диспетчера шлюза предоставляет инструменты, которые помогут отслеживать состояние шлюза. Используя диспетчер, вы можете указать события (например, неудачные попытки подключения к серверу шлюза служб терминалов), которые вы хотите отслеживать для целей аудита.

*Примечание: для подключения через шлюз ваш сервер должен входить в домен Active Directory, настройка шлюза может выполняться на любом сервере в домене от имени администратора домена*Установка роли

В первую очередь рекомендуется настроить правильное время. Вы можете задать параметры подключения к NTP-серверу в разделе **“Manage” -> “System” -> “Time&date” -> “Edit settings”**. Или задать тут точное время вручную.



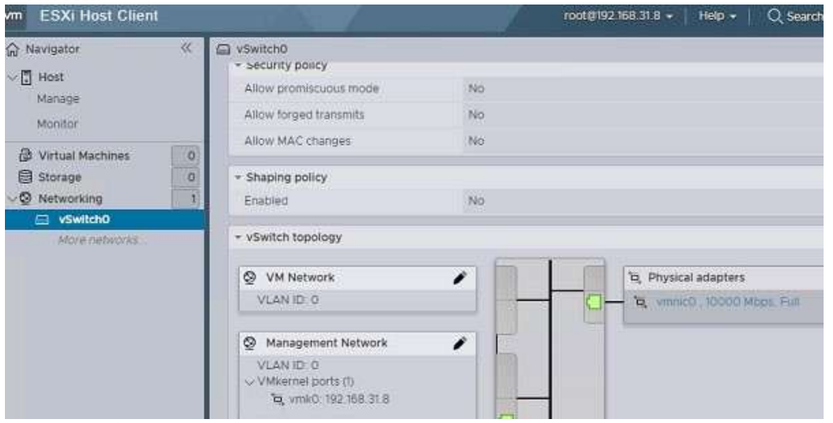
В разделе **Networking** вы можете управлять виртуальными сетями. Одно из базовых понятий в Hypervisor – виртуальный коммутатор.

Виртуальный коммутатор (vSphere Switch или vSwitch) – это виртуальное устройство, которое передает данные между виртуальными машинами внутри сервера и передает данные наружу через физический NIC. Есть два вида виртуальных коммутаторов:

• **Standard Switches** — простой виртуальный коммутатор, логически находится внутри физического сервера.

• **Distributed Switches** — распределенный виртуальный коммутатор, может быть распространен на несколько физических серверов (не доступен в бесплатной версии VMWare Hypervisor, да и в платной редакции VMWare vSphere доступен только в Enterprise Plus редакции**)**.

В ESXi по умолчанию уже создан один виртуальный коммутатор **vSwitch0**, который включает в себя один физический адаптер vmnic0 и две группу портов – служебная (Management Network) дляуправления гипервизором и сеть для передачи данных (VM Network). Интерфейс управления гипервизором vmk0 (vmkernel port) включен в группу Management Network.



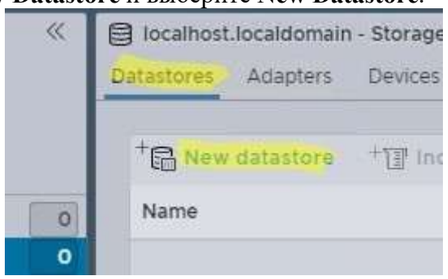
В большинстве случаев на отдельно стоящем гипервизоре вам будет достаточно одного виртуального коммутатора. Дополнительные портов нужно создавать, если вы хотите изолировать виртуальные машины друг от друга, использовать различные настройки VLAN для группы портов.

Не нужно вносить изменения в Management Network или vmkernel port без особой необходимости, иначе вы можете потерять доступ к вашему интерфейсу управления гипервизором. Если вы потеряли доступ к гипервизору, вы можете сбросить сетевые настройки с помощью меню **Restore Network Settings** в консоли DCUI.

Следующий этап – создать хранилище, в котором будет находится файлы виртуальных машин. ESXi позволяет использовать для хранения ВМ как локальные диски или USB флешки (официально не рекомендуется использовать флешки под VMFS), так и внешние хранилища, подключенные к хосту VMWare по iSCSI, NFS или Fibre Channel.

В этом примере мы будем использовать локальный диск в качестве хранилища. Перейдите в раздел **Storage** -> **Devices** и проверьте какие диски доступны (в некоторых случая нужно нажать Rescan для обнаружения).

Затем перейдите на вкладку **Datastore** и выберите **New Datastore**.

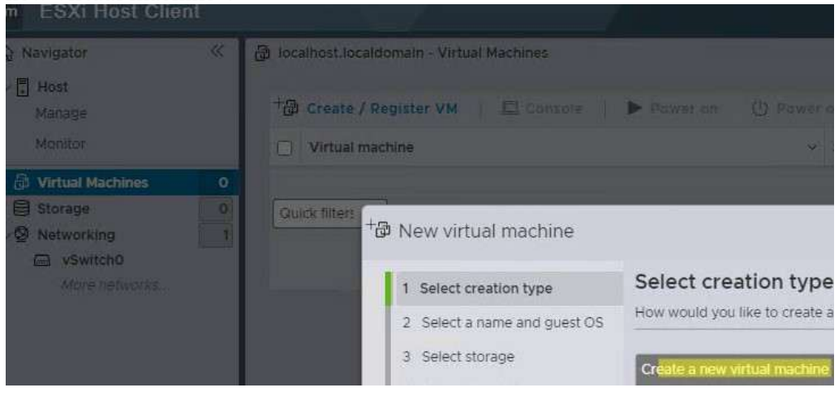


Укажите имя хранилища и выберите диск, где его создать. VMFS –файловая система VMware, которая используется для хранения (вы можете получить доступ к данным на VMFS в том числе из Windows и Linux).

Выберите, что будете использовать под VMFS датостору весь диск.

№3 Работа с Hypervisor: Установка и настройка виртуальных машин.

В Web-интерфейсе выберите “Virtual Machines” -> “Create / Register VM” -> “Create a new virtual machine”.



В K8s отсутствует встроенная возможность ведения журнала на уровне кластера. Для ее реализации пользователи используют разные подходы. Ниже приведем два самых распространенных способа обработки логов:

- Использование агента ведения журналов (logging-agent) на уровне узла.

Один из способов сбора и обработки логов в Kubernetes на уровне кластера — это использование агента ведения журналов на уровне узла. Этот агент (например, Fluentd или Logstash) является компонентом, работающим на каждом узле кластера. Он отвечает за сбор, обработку и отправку логов агрегатору. Его интеграция происходит за счет объекта DaemonSet, который добавляет копию агента на каждый рабочий узел кластера.

- Использование дополнительного контейнера sidecar на уровне пода или узла.

Sidecar — это дополнительный контейнер, который работает вместе с основным контейнером в одном поде или на одном узле. Правильно настроенный sidecar-контейнер собирает логи из файла, сокета или journald, а затем передает их в собственные потоки stdout или stderr.

Для сбора логов разных форматов рекомендуется настраивать несколько sidecar-контейнеров. В таком случае каждый из них будет перенаправлять логи из общего тома в свой поток stdout.

Чтобы посмотреть на собранные логи, можно воспользоваться уже знакомой командой: kubectl logs название_пода название_sidecar-контейнера

Инструменты логирования Kubernetes

В данном разделе инструкции мы рассмотрим некоторые популярные инструменты с открытым исходным кодом, которые подойдут для сбора логов в Kubernetes.

Fluentd, Fluent Bit и Fluent Operator

Fluentd и Fluent Bit – это два агента ведения логов, которые предназначены для сбора, фильтрации, агрегации и передачи логов в различных средах, в том числе и в Kubernetes. Fluentd больше подойдет для обработки собранных логов из-за наличия различных плагинов. Fluent Bit, в свою очередь, подойдет для сбора логов и их отправки конечным адресатам.

Fluent Operator – это инструмент, разработанный для управления и автоматического развертывания агентов Fluentd и Fluent Bit в среде Kubernetes. Он упрощает процесс их установки, настройки и масштабирования в кластере с помощью ресурсов Custom Resource Definitions (CRD). С помощью Fluent Operator пользователь может развернуть каждый из агентов по отдельности, либо Fluent Bit в сочетании с Fluentd.

Процесс работы с Fluent Operator изображен на следующей картинке: Ниже перечислены пользовательские ресурсы Fluent Operator:

- Системные ресурсы:
- FluentBit – используется для создания демонов Fluent Bit и его конфига;
- FluentBitConfig – используется для определения набора подключаемых модулей (ввод, вывод, фильтрация), которым будет управлять FluentBit, и генерации финальной конфигурации в виде секрета;
- Input – модуль конфигурации для сбора логов;
- Parser – модуль конфигурации для анализа логов;
- Filter – модуль конфигурации для фильтрации логов;
- OutPut – модуль конфигурации для отправки логов на указанный носитель. Взаимосвязь и работа ресурсов представлены на следующей картинке:

Elasticsearch, Logstash и Beats, Kibana (ELK Stack/Elastic Stack)

ELK Stack – это комбинация трех популярных инструментов для сбора, агрегации, обработки и визуализации данных логов: Elasticsearch, Logstash и Kibana. С 2015 года к ним был добавлен Beats для повышения производительности, а весь стек был переименован в Elastic Stack.

- Elasticsearch – это поисковый и аналитический движок, который используется для хранения и индексации структурированных и неструктурированных данных, включая логи.
- Logstash – это агент для сбора, обработки и доставки логов. Иногда вместо него пользователи ставят агент Fluentd, который считается более стандартным решением для среды K8s. В таком случае получается не ELK-стек, а EFK.

NAME READY STATUS RESTARTS AGE IP NODE NOMINATED NODE READINESS GATES

shell-demo-7h995 1/1 Running 0 9h 10.250.116.129 serverw <none> <none> shell-demo-qp6k5 1/1 Running 2 9h 10.250.77.15 master <none> <none> Теперь убедитесь, что мы можем пинговать оба ip-адреса с обоих серверов:

master > ping 10.250.116.129 master > ping 10.250.77.15 server2 > ping 10.250.116.129 server2 > ping 10.250.77.15

После этого у вас должен быть запущен кластер k8s из proxmox.

№10 Настройка логирования контейнеров.

Логирование – это процесс сбора, записи и хранения данных о различных событиях, действиях и состоянии системы или приложения в определенном формате. Данный процесс относится к такому свойству распределенных систем, как наблюдаемость или observability.

Данные, которые собираются в процессе логирования, могут включать в себя:

- Общую информацию о ходе работы системы;
- Предупреждения о потенциальных проблемах;
- Записи о возникших ошибках в системе, которые требуют рассмотрения и устранения;
- Отладочную информацию;
- Записи о действиях пользователей или системы для аудита, обеспечения безопасности и выявления несанкционированных действий.

В Kubernetes логирование – это процесс сбора, управления и анализа логов, сгенерированных контейнерами приложения и компонентами Kubernetes для выполнения мониторинга, отладки и обнаружения проблем в среде кластера.

В данной инструкции мы рассмотрим процесс логирования в среде Kubernetes, начиная от ее архитектуры и заканчивая инструментами для обработки логов.

Архитектура логирования в Kubernetes

В данном разделе инструкции мы рассмотрим архитектуру сбора логов в Kubernetes. Ниже будут приведены основные уровни сбора логов:

- Сбор логов на уровне подов.

Каждый под фиксирует логи своих контейнеров, сгенерированные приложением. Вы можете изучить их сразу после создания и настройки пода, используя для этого командную строку.

На картинке выше изображен процесс логирования на уровне контейнеров пода. Здесь некоторый контейнер app-container пода my-pod отправляет логи в стандартные

потоки stdout и stderr контейнеризированного приложения, где stdout – это поток вывода, а stderr – ошибок. Агент kubelet, подключенный к среде выполнения контейнера с помощью CRI, отвечает за обработку и контроль логов, собранных контейнером.

Чтобы посмотреть логи пода в Kubernetes, необходимо воспользоваться следующей командой: kubectl logs название_пода

Кроме того, вы можете столкнуться с ситуацией, когда внутри вашего пода развернуто несколько контейнеров, а логи нужны только от одного из них. Для этого к предыдущей команде необходимо добавить специальный флаг и имя контейнера:

kubectl logs название_пода -c название_контейнера

В результате выполнения команд будут показаны журналы, сгенерированные контейнером или целым подом приложения. Они могут содержать информацию о статусе приложения, ошибках или успешных и неудачных операциях.

Если на рабочих узлах установлена systemd, то kubelet записывает системные логи в journald, а для их чтения используется команда:

journalctl -u kubelet

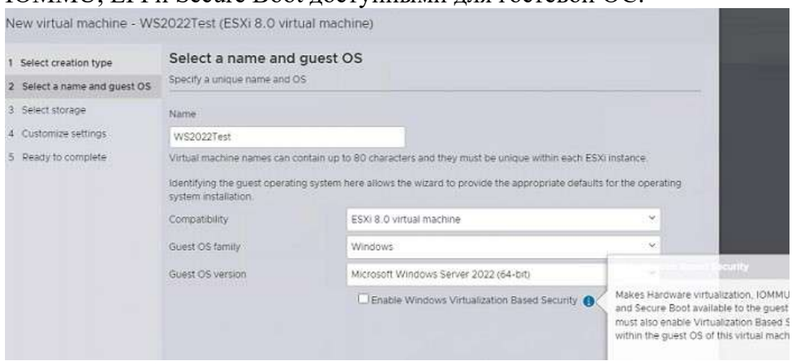
Если на узле отсутствует systemd, то запись логов будет осуществляться в log-файлы в каталог /var/log.

- Сбор логов на уровне кластера.

Задайте имя виртуальной машины. Выберите тип и версию гостевой операционной системы. В нашем примере это:

- Guest OS Family: Windows
- Guest OS Version: Microsoft Windows Server 2022 (64 bit)

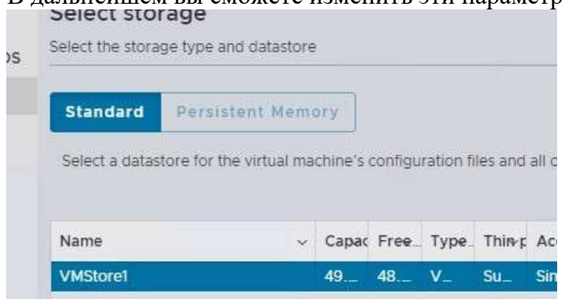
Включите чек-бокс “Windows Virtualization Based Security”, если хотите сделать IOMMU, EFI и Secure Boot доступными для гостевой ОС.



Установка Windows 11 в гостевой ОС на ESXi описана в этой статье.

Выберите хранилище данных (datastore, который вы создали ранее), где будут хранится файлы конфигурации виртуальной машины и ее виртуальные диски.

В дальнейшем вы сможете изменить эти параметры ВМ.



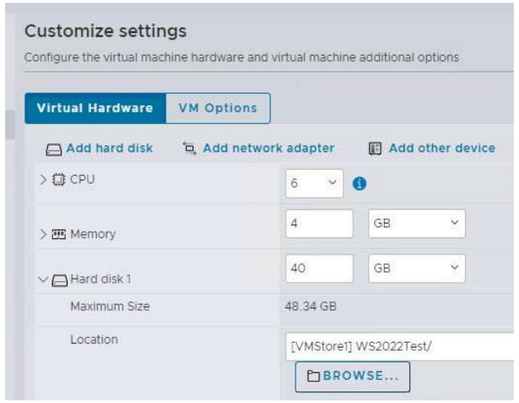
Если на датасторе недостаточно место, появится сообщение о том, что вам нужно увеличить размер VMFS хранилища.

На следующем шаге настраиваются базовые параметры виртуальной машины: количество CPU, объем оперативной памяти, размер жесткого диска, сетевые адаптеры, CD/DVD приводы и т.д.

Виртуальные диски ВМ хранятся на хранилище в виде файлов с расширением VMDk (вы можете расширить или сжать такие виртуальные диски в ESXi). Конфигурация ВМ хранится в файле

.VMX.

Чтобы подключить ВМ к сети нужно поместить ее виртуальный сетевой адаптер в группу портов VM Network на коммутаторе vSwitch0 (если вы ничего не перенастроили).

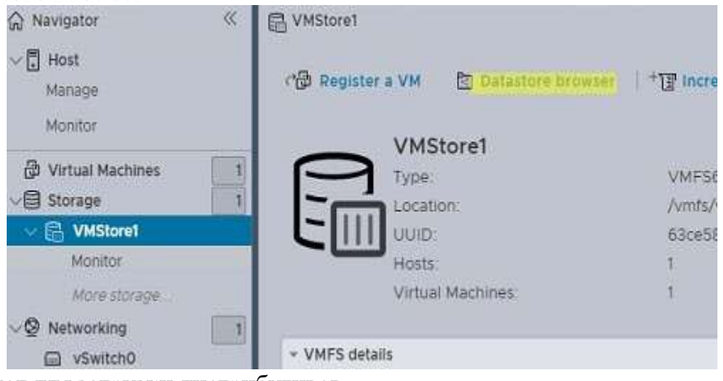


Если вы назначите для ВМ более 8 vCPU, то при ее включении появится ошибка: “Failed to power on virtual machine. There are insufficient licenses to complete this operation”. Это ограничение лицензии Free vSphere Hypervisor.

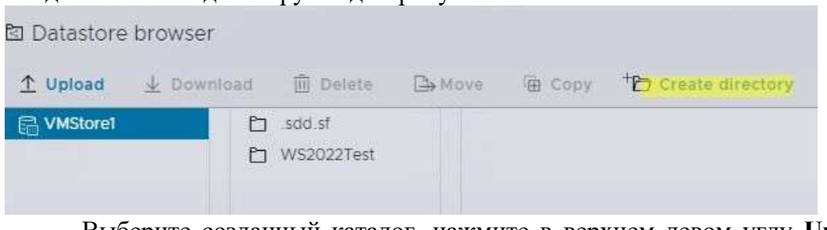
На следующем экране будет предложено проверить все настройки виртуальной машины и подтвердить их.

Теперь нужно установить операционную систему (она называется гостевой ОС) в виртуальную машину VMware.

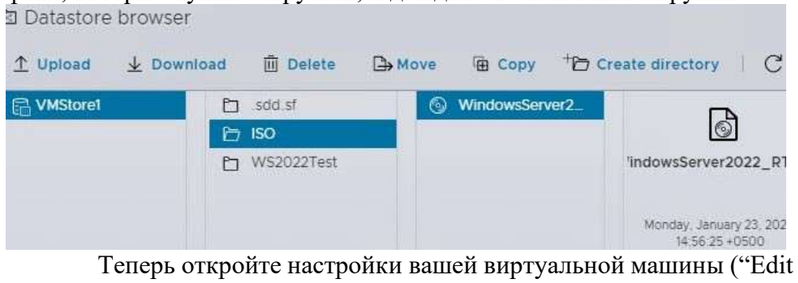
Загрузите установочный образ (ISO файл) с дистрибутивом нужной ОС в локальное хранилище VMware. В левом меню выберите ваше VMFS хранилище в разделе Storage и нажмите **Datastore Browser**.



Создайте каталог для загрузки дистрибутивов.



Выберите созданный каталог, нажмите в верхнем левом углу **Upload**, выберите ISO файл, которые нужно загрузить, и дождитесь окончания загрузки.



Теперь откройте настройки вашей виртуальной машины (“Edit Settings”).

Запустите vpn и убедитесь, что master и server2 могут подключаться друг к другу: master > ping 10.0.0.2

server2 > ping 10.0.0.1

Теперь установите, kubeadm как раньше, и исправьте, --node-ip как мы делали раньше. Теперь мы можем присоединиться к узлу:

kubeadm join 10.0.0.1:6443 --token j9dg9i.u023uf023pr902u4 \

--discovery-token-ca-cert-hash sha256:bb69ce79896847304175499 2927ce3b8154b526485055a0bf9fdd34c2aa34944

3.4. Убедиться, что все в порядке

Несколько вещей, которые мы можем сделать, чтобы убедиться, что все в порядке, сначала проверьте, что все узлы готовы и используют ip vpn:

$ kubectl get node -o wide root@k8s:~# kubectl get node -o wide

NAME STATUS ROLES AGE VERSION INTERNAL-IP EXTERNAL-IP OS-IMAGE KERNEL-VERSION CONTAINER-RUNTIME

master Ready master 9h v1.15.2 10.0.0.1 <none> Ubuntu 18.04 LTS 4.15.18-13-pve docker://19.3.1

server2 Ready <none> 9h v1.15.3 10.0.0.2 <none> CentOS Linux 7 (Core) 3.10.0-957.27.2.el7.x86_64 docker://1.13.1

Если внутренние IP неверны, проверьте настройки calico, помните, что вам может потребоваться сначала воссоздать кластер с помощью kubeadm reset, поскольку calico упоминает, что последующее изменение конфигурации может не возыметь эффекта.

Также убедитесь, что calico в порядке:

$ curl -O -L https://github.com/projectcalico/calicoctl/releases/download/v3.8.2/calicoctl

$ chmod +x calicoctl

$ DATASTORE_TYPE=kubernetes KUBECONFIG=~/.kube/config ./calicoctl get node -o wide NAME ASN IPV4 IPV6

k8s (64512) 10.0.0.1/32

server2 (64512) 10.0.0.2/32

$ DATASTORE_TYPE=kubernetes KUBECONFIG=~/.kube/config ./calicoctl node status Calico process is running.

IPv4 BGP statu

| PEER-ADDRESS | PEER-TYPE | STATE | SINCE | INFO |

| 10.0.0.2 | node-to-node mesh | up | 07:22:50 | Established |

+++++----------- ----- ---------- ----------

Если это не так, убедитесь, что настройки calico верны и брандмауэр в порядке: master > $ nc -v 10.0.0.3 179

Connection to 10.0.0.3 179 port [tcp/bgp] succeeded!

Теперь убедитесь, что межузловые соединения работают должным образом:

$ cat > test-daemonset.yaml apiVersion: apps/v1

kind: DaemonSet metadata:

name: shell-test labels:

k8s-app: shell-test

spec:

selector:

matchLabels:

name: shell-test template:

metadata:

labels:

name: shell-test spec:

containers:

- name: shell-test

image: debian:stable-slim Теперь примените набор демонов:

$ kubectl apply -f test-daemonset.yaml

$ kubectl get pod -o wide

Теперь убедитесь, что мы загрузились должным образом:

$ ls -l /dev/kmsg [this should exist]

$ wg show

[this should show wireguard is started]

Теперь мы можем приступить к установке kubernetes:

$ apt-get update && apt-get install -y apt-transport-https curl

$ curl -s https://packages.cloud.google.com/apt/doc/apt-key.gpg | apt-key add -

$ cat <<EOF >/etc/apt/sources.list.d/kubernetes.list deb https://apt.kubernetes.io/ kubernetes-xenial main EOF

$ apt-get update

$ apt-get install -y kubelet kubeadm kubectl

$ apt-mark hold kubelet kubeadm kubectl

Чтобы убедиться, что kubernets подключается с правильным IP и будет использовать VPN для подключения, мы должны сообщить kubelet, чтобы он использовал ip vpn-сервера:

$ echo "KUBELET_EXTRA_ARGS=--node-ip=10.0.0.1" >> /etc/default/kubelet Теперь мы можем настроить kubeadm:

Обязательно укажите pod-network-cidr и service-cidr, если они перекрываются с вашей обычной локальной сетью, как это и есть в моем случае, поскольку я запускаю 192.168.x.x в своей локальной сети proxmox. Обратите внимание, что я добавляю дополнительный apiserver-cert-extra-sans, поэтому я могу просто подключиться к серверу api с его ip-адреса локальной сети.

Чтобы убедиться, что это сработает, нам нужно игнорировать все предполетные ошибки, но это должно работать просто отлично.

$ kubeadm init --pod-network-cidr=10.250.0.0/16 --service-cidr=172.31.0.0/16 --apiserver-advertise-address

10.0.0.1 --apiserver-cert-extra-sans k8s.mydomain.com --apiserver-cert-extra-sans 192.168.1.13 --apiserver-

cert-extra-sans 10.0.0.1 --ignore-preflight-errors=all Далее скопируйте конфигурацию kubectl:

$ mkdir -p $HOME/.kube

$ sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config

$ sudo chown $(id -u):$(id -g) $HOME/.kube/config И примените конфигурацию calico

$ curl https://docs.projectcalico.org/v3.8/manifests/calico.yaml -O

$ vim calico.yaml

Change:

IP_AUTODETECTION_METHOD: "interface=wg*" CALICO_IPV4POOL_CIDR: "10.250.0.0/16"

Значение IP_AUTODETECTION_METHOD должно быть wg0, чтобы все узлы подключались через VPN, это гарантировало, что он нормально работает без NAT, и все будет в безопасности.

CALICO_IPV4POOL_CIDR Необходим, чтобы убедиться, что все модули созданы в правильной сети. Если это правильно, мы можем применить конфигурацию сети:

$ kubectl apply -f calico.yaml

Обратите внимание на команду join, чтобы мы могли добавить еще один узел.

Мне нравится, что k8s также планирует модули на главном сервере, чего по умолчанию не происходит, поэтому мне нужно запустить:

$ kubectl taint nodes --all node-role.kubernetes.io/master-

3.3. Добавляем еще один узел

1. Подготовьте узел, в этом примере "server2", с помощью wireguard VPN на сервере 2:

[Interface]

PrivateKey = wPMsKBkqbdz1WBx8MhYM7/GwzYd6U7DWuef1FoeUdkg= Address = 10.0.0.2/32

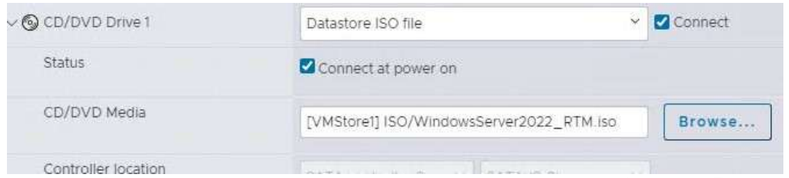
MTU = 1500[Peer]

PublicKey = 8q+JKbrXDs86lnBvAl4lx6QiCzgoOOaAc7jtjz/lFBM= AllowedIPs = 10.0.0.0/24

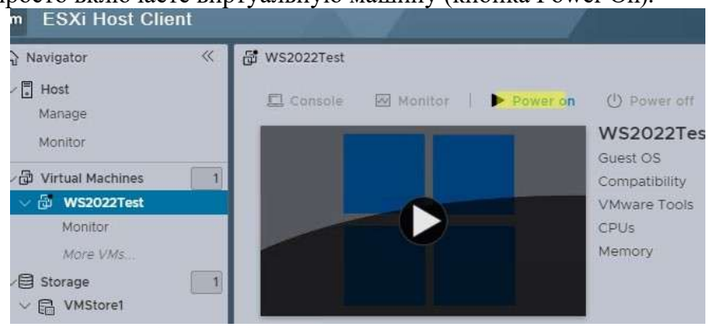
Endpoint = 123.123.123.123:55555

PersistentKeepalive = 15

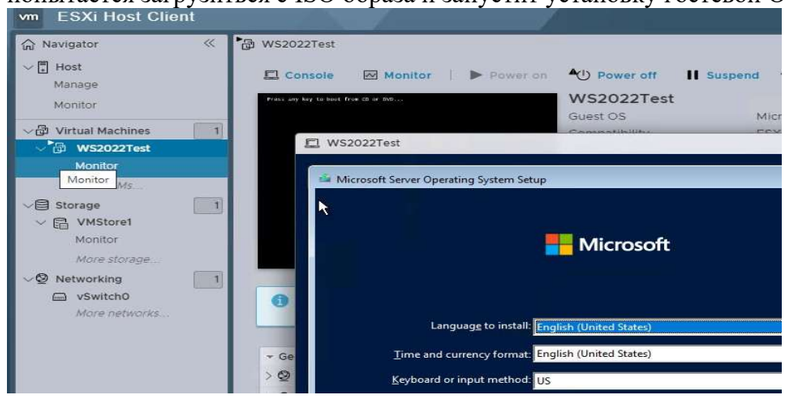
В секции CD/DVD Drive укажите что вы хотите подключить образ из **Datastore ISO file**. Нажмите кнопку Browse и выберите ваш ISO файл. Включите опции Connect и Connet at power on.



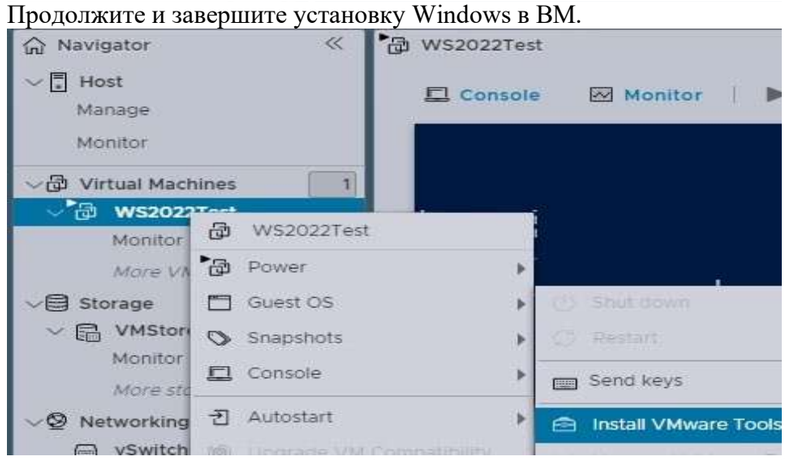
Затем просто включаете виртуальную машину (кнопка Power On).



Чтобы открыть экран (консоль) виртуальной машины, нажмите на вкладку Console. ВМ попытается загрузиться с ISO образа и запустит установку гостевой ОС.



Продолжите и завершите установку Windows в ВМ.



После окончания установки обязательно установите пакет VMTools (это набор драйверов и служб для виртуальной машины). Выберите в меню ВМ Guest OS -> Install VMware Tools.

В гостевой ОС откройте виртуальный CD привод и запустите файл setup.exe.

№4 Работа с Hypervisor: Автоматизация развёртывания виртуальных машин

Для начала необходимо подготовить хост — ту систему, на которой будут разворачиваться виртуальные машины. В случае если они нужны для локальных тестов и всё будет крутиться на том же компьютере, где вы сидите — всё просто и прозрачно. Однако, зачастую получается ситуация, когда виртуалки нужны в итоге в совершенно другом месте — в датацентре на живом окружении, на соседнем сервере или на бабушкином нетбуке. Дело в том, что из коробки скрипты Vagrant делают все операции на локалхосте. В принципе, никто не мешает сначала развернуть это у себя, настроить- поиграться, а потом смигрировать на далёкий гипервизор, но тут оказывается, что это занимает прилично времени даже когда сервер находится в одном сегменте сети с вами. В случае же, когда надо разворачиваться через VPN в датацентре на другом краю земли — это может занимать больше часа на каждый инстанс, и при этом может понадобиться совершать лишние действия: экспорт- импорт в моём случае, плюс перенастройка сети, если виртуальные коммутаторы называются по- разному.

Поэтому оптимальным решением я для себя выбрал поднятие Vagrant на всех гипервизорах, где планируется его частое использование. Это ускоряет процесс (даже для одной машины — ведь бокс весит значительно меньше VHD файла развёрнутого образа), однако добавляет лишнего софта на сервера. К счастью, Chocolatey и Vagrant не требуют GUI, так что их легко можно установить даже на бесплатном Hyper-V Server.

Задача эта в целом довольно тривиальная:

• Установка роли Hyper-V в Windows 8 или Server 2012 требует перезагрузки и делается через Server Manager для любителей GUI (ссылка есть в материалах в конце статьи) или при помощи PowerShell с административными привилегиями:

Install-WindowsFeature –Name Hyper-V -IncludeManagementTools

• Шоколатье ставится из Powershell одной командой:

iex ((new-object net.webclient).DownloadString('https://chocolatey.org/install.ps1'))

• Ну, а Vagrant поднимается уже из Chocolatey:

choco install vagrant

Вообще, если вы не любите засорять сервера лишними программами или предпочитает всегда использовать наисвежайшие версии (следует понимать, что несмотря на то, что в репозитарии обычно лежит самая последняя версия — появляется она там не мгновенно) — можно вполне обойтись без Шоколатье, установив Vagrant вручную из дистрибутива. Он поставляется в виде msi- пакета, так что проблем с установкой из консоли быть не должно. Но лично я предпочитаю первый вариант не только потому, что люблю шоколад — просто я привык так ставить вообще весь софт, даже на домашнем ноутбуке.

В этот момент мы сталкиваемся с первым подводным камнем (я уже предупреждал, что путь будет тернист?). Дело в том, что наш бродяга (а именно так переводится “vagrant”) от версии к версии ставит себя в разные каталоги, и в последнем на данный момент релизе он снова начал устанавливаться прямо в корень системного диска в папку C:\HashiCorp\Vagrant. Всё бы ничего, но он периодически забывает прописывать путь к своей папке в переменную окружения, поэтому система может не находить его, если не вводить полный путь к бинарнику. Лечится это простой командой в Powershell:

$env:Path+=”;C:\HashiCorp\Vagrant\bin”

Для командной строки нужно использовать команду setx с ключом /M. Например, если нужно поменять расположение папки, где он будет хранить боксы (по умолчанию он хранит их на своей папке на диске C, что может не очень понравится, когда на системном диске немного места):

setx VAGRANT_HOME «X:/your/path» /M

net.ipv6.conf.all.forwarding=1

Виртуальные машины теперь должны быть доступны (например, через SSH) по их присвоенным IP-адресам.

№6 Установка Kubernetes в среде Proxmox VE

№7 Настройка Kubernetes в среде Proxmox VE

Базовые компоненты:

1. Nodes – виртуальная (физическая) машина, на мощностях которой запущены

2. Отредактируйте конфигурационный файл /etc/pve/lxc/$ID.conf и добавьте следующую часть: lxc.apparmor.profile: unconfined

lxc.cgroup.devices.allow: a lxc.cap.drop:

lxc.mount.auto: "proc:rw sys:rw"

Если вы используете zfs в proxmos, обязательно создайте том ext4, поскольку zfs не поддерживается kubeadm See: https://github.com/corneliusweig/kubernetes-lxd

zfs create -V 50G mypool/my-dockervol zfs create -V 5G mypool/my-kubeletvol mkfs.ext4 /dev/zvol/mypool/my-dockervol mkfs.ext4 /dev/zvol/mypool/my-kubeletvol

Затем обязательно смонтируйте его внутри контейнера:

mp0: /dev/zvol/mypool/my-dockervol,mp=/var/lib/docker,backup=0 mp1: /dev/zvol/mypool/my-kubeletvol,mp=/var/lib/kubelet,backup=0 Затем убедитесь, что conntrack работает в контейнере

$ sudo conntrack -L

Теперь мы можем настроить необходимый нам VPN, смотрите документацию по установке wireguard

$ sudo add-apt-repository ppa:wireguard/wireguard

$ sudo apt-get update

$ sudo apt-get install wireguard Создайте конфигурацию:

$ cat > /etc/wireguard/wg0.conf [Interface]

Address = 10.0.0.1/32 ListenPort = 55555

PostUp = iptables -A FORWARD -i wg0 -j ACCEPT; iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

PostDown = iptables -D FORWARD -i wg0 -j ACCEPT; iptables -t nat -D POSTROUTING -o eth0 -j MASQUERADE

PrivateKey = WNeaIBT40mN/asu9zXrPeSYA+4pFmZA9lUBvHTx+TG8=

MTU = 1500

[Peer]

server2

PublicKey = NSWzZOIUHPqRxOxUmB/A7+Gs6oECYGojREvGs/ZEi2o=

AllowedIPs = 10.0.0.2/32

[Peer]

server3

PublicKey = JhT41so2SiITMe2uqPoNB40kkwxRqyklWiILyhT1uVY= AllowedIPs = 10.0.0.3/32

И запустите vpn:

$ wg-quick up wg0

$ wg show

Чтобы убедиться, что мы запускаем vpn при загрузке, и исправить некоторые другие мелкие проблемы, создайте следующий файл rc.local:

$ cat > /etc/rc.local #!/bin/sh -e

Kubeadm 1.15 needs /dev/kmsg to be there, but it's not in lxc, but we can just use /dev/console instead

see: https://github.com/kubernetes-sigs/kind/issues/662 if [! -e /dev/kmsg]; then

ln -s /dev/console /dev/kmsg

fi

Make sure our VPN is setup so we can connect to the other nodes wg-quick up wg0

https://medium.com/@kvaps/run-kubernetes-in-lxc-container-f04aa94b6c9c mount --make-rshared /' > /etc/rc.local

exit 0

Установите разрешения и перезагрузите компьютер.

$ chmod +x /etc/rc.local

sudo reboot

./kube_nginx.yaml

Буквально через небольшой промежуток времени можем смотреть результат ее выполнения с помощью команды **kubectl get pods**. Пример представлен ниже.

$ kubectl get pods

NAME READY STATUS RESTARTS AGE

nginx-deployment-546bf458b5-2kqlz 1/1 Running 0

3m

nginx-deployment-546bf458b5-kbhql 1/1 Running 0

3m

Как мы видим, 2 пода развернуты и находятся в состоянии **Running**. Теперь создадим сервис,

который будет заниматься организацией доступа снаружи к нашим контейнерам. В даном примере мы прокинем 80 TCP порт на внешний IP адрес. Вообще это можно сделать разными способами взависимости от типа Kubernetes кластера. В случае с GKE проще всего создать **Service** с типом **LoadBalancer**. Мы пишем следующий файл **kube_loadbalancer.yaml**, в котором описываем балансировку на наше приложение nginx с внешнего TCP/80 порта на внутренний TCP/80 порт.

apiVersion: v1 kind: Service metadata:

name: nginx-load-balancer spec:

type: LoadBalancer selector:

app: nginx ports:

- protocol: TCP port: 80

targetPort: 80 name: http

После того, как файл будет создан, точно так же, как и при инициализации файла с Deployment, выполняем **kubectl apply** для запуска сервиса в работу.

$ kubectl apply -f

./kube_loadbalancer.yaml

После небольшого промежутка времени можем проверить то, что наш сервис балансировки удачно запустился и работает, с помощью **kubectl get service**. По указанному EXTERNAL-IP в выводе сервиса LoadBalancer по TCP/80 порту можем удостовериться в работе нашего nginx сервиса.

$ kubectl get service

NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE

kubernetes ClusterIP 10.12.0.1 <none> 443/TCP 5m nginx-load-balancer LoadBalancer 10.12.1.240 x.x.x.x 80:32267/TCP

5m

Напоследок хочется поделиться командой, с помощью которой можно удалить из кластера

сервисы, приложения или поды, которые перестали быть нужны. Так, чтобы убрать запущенные в данной статье поды из кубера, мы должны выполнитью следующую команду **kubectl delete**.

$ kubectl delete -f

./kube_nginx.yaml

№9 Оркестрация Kubernetes в среде Proxmox VE Шаг 1: Подготовьте хост proxmox

Убедитесь, что загружены следующие модули:

cat /proc/sys/net/bridge/bridge-nf-call-iptables

Теперь убедитесь, что возможность подкачки равна 0, чтобы swap не использовался, иначе kubernetes не запустится:

cat /proc/sys/vm/swappiness [should be 0]

Определите новый

sysctl vm.swappiness=0

Отключите SWAP, для очистки области SWAP потребуется некоторое время #s wapoff -a

Теперь дождитесь, пока swap опустеет.

Шаг 1: Создание контейнера kubernetes

1. Создайте новый контейнер в proxmox, убедившись, что ему присвоен 0 swap, и сделайте его привилегированным контейнером

контейнеры.

2. Pods – базовые модули управления приложениями, состоящие из одного или нескольких контейнеров.

3. Volume – ресурс, позволяющий одновременно запускать несколько контейнеров.

4. Kube-Proxy – комплекс из прокси-сервера и модуля балансировки нагрузки, позволяющий маршрутизировать входящий трафик под конкретный контейнер Pods.

5. Kubelet – транслятор статусов Pods на узле и контроллер корректности работы контейнера и образа в целом.

Перечисленные компоненты устанавливаются автоматически при помощи сторонних инструментов или вручную, по отдельности. Они составляют модуль под названием Master Node, где собраны все управляющие и контролирующие функции. Через API они связываются с контейнерами, считывают их показатели, дают команду на запуск, штатную остановку или принудительное закрытие.

Процесс установки Kubernetes

При выборе автоматической установки вникать в детали не понадобится, но требуется выделить достаточное количество системных ресурсов, чтобы платформа работала бесперебойно. Например, при небольшом количестве контейнеров и простой взаимосвязи достаточно 1-2 процессорных ядер, 2-4 Гб оперативки и двух виртуальных машин, выполняющих функции Master и Worker Node.

Инсталляция на Ubuntu

Проще всего воспользоваться одной из готовых реализаций – Minikube или Kubespray. Если нужно установить Kubernetes на сервер с операционной системой Ubuntu вручную, понадобятся права суперпользователя. Начнем с установки Docker для узла. Перечень команд для этого выглядит следующим образом:

apt-get update

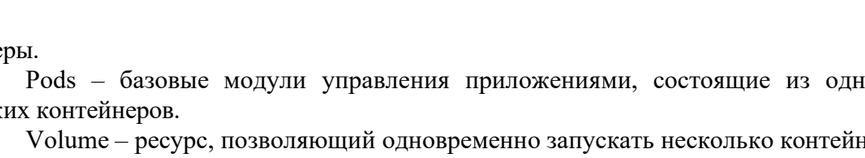
apt-get install -y docker.io

При необходимости организовать создание контейнеров более новых версий перечень команд будет несколько иным:

apt-get update apt-get install -y \

apt-transport-https \ ca-certificates \ curl \

software-properties-common



curl -fsSL https://download.docker.com/linux/ubuntu/gpg | apt-key add –

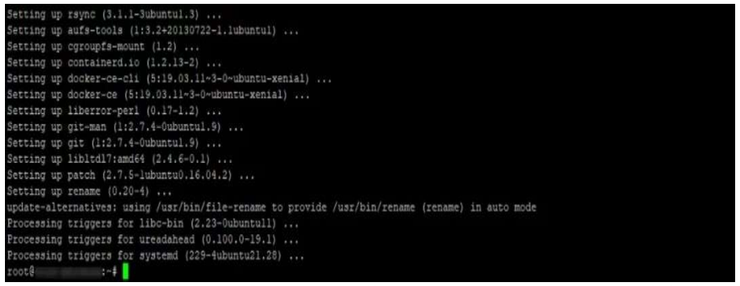
add-apt-repository \

"deb [arch=amd64] https://download.docker.com/linux/$(. /etc/os-release; echo "$ID") \

$(lsb_release -cs) \

stable" apt-get update

apt-get install -y docker-ce docker-ce-cli containerd.io

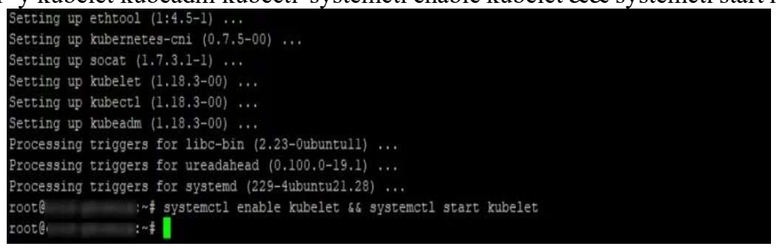


Docker для одного узла установлен. Следующий шаг – установка модулей kubeadm (создание и настройка кластеров), kubelet (их запуск на хостах), kubectl (настройка компонентов, входящих в кластер). Для этого вводятся следующие команды:

apt-get update && apt-get install -y apt-transport-https software-properties-common curl -s https://packages.cloud.google.com/apt/doc/apt-key.gpg | apt-key add -

add-apt-repository "deb http://apt.kubernetes.io/ kubernetes-xenial main" apt-get update

apt-get install -y kubelet kubeadm kubectl systemctl enable kubelet && systemctl start kubelet



Настройка Kubernetes

Сначала указывается сервер, на который был инсталлирован Kubernetes. Он становится первичным, где будут запускаться остальные операции. Инициализация выполняется при помощи команды:

kubeadm init --pod-network-cidr=10.244.0.0/16

В результате создается адрес виртуальной сети Pods (цифры выбираются по желанию пользователя). По умолчанию используется указанный IP. При правильной обработке команды на дисплее будет отображаться команда для присоединения остальных Nods-кластеров к первичному серверу, чтобы создать в итоге рабочую систему.

Следующие команды задают пользователя, который будет управлять работой комплекса: mkdir -p $HOME/.kube

sudo cp -i /etc/kubernetes/admin.conf $HOME/.kube/config sudo chown $(id -u):$(id -g) $HOME/.kube/config

Теперь можно настраивать Container Network Interface (CNI, сетевой интерфейс контейнера).

Чтобы избавить себя от рутины ручного ввода команд, рекомендуется установить плагин Flannel или ему подобный (Weave Net, Calico). Первый устанавливается так:

kubectl apply -f https://raw.githubusercontent.com/coreos/flannel/master/Documentation/kube- flannel.yml

После ввода команды на экране отображаются имена всех созданных ресурсов.

Теперь пользователь добавляет Nods в существующий кластер. Для этого требуется подключение к серверу через SSH, установка модулей Docker, Kubelet, Kubeadm (вопрос рассматривался выше). Выполнение команды:

kubeadm join --token <token> <control-plane-host>:<control-plane-port> --discovery-token-ca-cert-

hash sha256:<hash>

Остается получить токен авторизации кластера. Если подключение SSH еще не прервано, повторно заходить на сервер не нужно. Токен выдается после ввода команды:

kubeadm token list

По умолчанию он действует 24 часа. Если поставлена задача добавить новый узел по завершении периода, новый создается командой:

kubeadm token create

Вывод выглядит примерно так:

5didvk.d09sbcov8ph2amjw

На этом все. Система готова к эксплуатации. Дальнейшие действия пользователя зависят от стоящих задач и опыта.№8 Работа с контейнерами Kubernetes в среде Proxmox VE

Для данного пример выберем запуск веб сервера nginx в конфигурации из 2 реплик. То есть, так называемый **под**, будет содержать по 1 контейнеру Docker с сервисом nginx. Таких подов мы для примера запустим 2. Вся конфигурация для работы сервисов в Kubernetes делается через **yaml файлы**. Это касается и запуска подов, приложений, а также различных дополнительных сервисов.

Мы создадим новый файл **kube_nginx.yaml** в нашей рабочей директории. Содержание данного файла привожу ниже.

apiVersion: apps/v1 kind: Deployment metadata:
name: nginx-deployment spec:
selector:
matchLabels:
app: nginx replicas: 2 template:
metadata:
labels:
app: nginx spec:
containers:
- name: nginx
image: nginx:1.15.9-alpine ports:
- containerPort: 80 protocol: TCP

Очень важный параметр, который определяет назначение данного конфигурационного файла – это **kind**. Здесь в данном конкретном примере мы будем использовать – **Deployment.** Это наиболее популярный способ развертывания приложения, который позволяет легко менять его параметры, а также количество подов в работе. Также возможно выбрать в качестве типа kind – **Pod**. По большому счету конфигурационный файл будет аналогичным, однако обслуживание в продакшен среде может усложниться.

Для запуска наших контейнеров выполняем команду **kubectl apply**. С помощью нее мы можем как запустить поды, сервисы и т.д. в первый раз, так и внести изменения в их работу.

$ kubectl apply -f