# Ответы на билеты

[**Ответы на билеты 1**](#_kbd9lhy2w73s)

[Билет 1 2](#_zh6x1uta9i5z)

[Билет 1 другая версия 5](#_qmmsb684onn5)

[Билет 2 7](#_8cewzkf7b18g)

[Билет 3 9](#_c2hncnmozayl)

[Билет 4 12](#_oc4t3dhu1ymj)

[Билет 5 15](#_oa06ud379e1w)

[Билет 6 20](#_38roffha5sfc)

[Билет 7 24](#_k76moyiz4ix7)

[Билет 8 27](#_jsupz91ykhip)

[Билет 9 31](#_we0rajj52vcc)

[Билет 10 37](#_uqns19icc44q)

[Билет 11 41](#_6x3al3n4iyso)

[Билет 12 47](#_co6n2w52032p)

[Билет 13 53](#_qjq029x63pld)

[Билет 14 54](#_5q58vxae4mi3)

[Билет 15 56](#_n8y7imjhfdtd)

[Билет 16 61](#_hh0wz2ykahq9)

[Билет 17 67](#_19j82ma46pf4)

[Билет 18 74](#_q6p64g6o27el)

[Билет 19 81](#_d47oj2fn107l)

[Билет 20 88](#_7ooz9u94r6uj)

[Билет 21 94](#_sv8j2kgke70t)

[Билет 22 100](#_y43g153s4oql)

[Билет 23 103](#_jpugxsk4c8yj)

[Билет 24 104](#_mo7i2bowjv1r)

[Билет 25 105](#_3e2k50ge4k05)

[Теория (объединенный документ) 108](#_svqgl66l9yrc)

| Билет 1 | |
| --- | --- |
| Вопрос 1  Выполнить настройку ролей DNS и DHCP на Linux Server (В качестве ОС использовать Ubuntu Server). | Настройка ролей DNS и DHCP на Linux Server (Ubuntu Server)  Настройка DHCP сервера  1.Установите пакет DHCP-сервера:  sudo apt update  sudo apt install isc-dhcp-server  2.Отредактируйте конфигурационный файл /etc/dhcp/dhcpd.conf:  sudo nano /etc/dhcp/dhcpd.conf  Добавьте конфигурацию (пример):  subnet 192.168.1.0 netmask 255.255.255.0 {  range 192.168.1.100 192.168.1.200;  option routers 192.168.1.1;  option domain-name-servers 192.168.1.1;  option domain-name "example.com";  }  3.Укажите сетевой интерфейс в /etc/default/isc-dhcp-server:  INTERFACESv4="eth0"  4.Запустите и включите сервис:  sudo systemctl start isc-dhcp-server  sudo systemctl enable isc-dhcp-server  Настройка DNS сервера (BIND9)  1.Установите BIND9:  sudo apt install bind9  2.Настройте файл зоны в /etc/bind/named.conf.local:  zone "example.com" {  type master;  file "/etc/bind/db.example.com";  };  3.Создайте файл зоны (пример /etc/bind/db.example.com):  $TTL 604800  @ IN SOA ns1.example.com. admin.example.com. (  2023050101 ; Serial  604800 ; Refresh  86400 ; Retry  2419200 ; Expire  604800 ) ; Negative Cache TTL  ;  @ IN NS ns1.example.com.  @ IN A 192.168.1.1  ns1 IN A 192.168.1.1  www IN A 192.168.1.10  4.Проверьте конфигурацию и перезапустите BIND:  sudo named-checkconf  sudo systemctl restart bind9  sudo systemctl enable bind |
| Вопрос 2  Выполнить мониторинг и анализ работы локальной сети с помощью Zabbix. | Мониторинг сети с помощью Zabbix  Установка Zabbix сервера  1.Добавьте репозиторий Zabbix:  wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release\_6.0-1+ubuntu20.04\_all.deb  sudo dpkg -i zabbix-release\_6.0-1+ubuntu20.04\_all.deb  sudo apt update  2.Установите Zabbix сервер, фронтенд и агент:  sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent  3.Настройте базу данных (предварительно установите MySQL):  sudo mysql -uroot -p  CREATE DATABASE zabbix CHARACTER SET utf8 COLLATE utf8\_bin;  CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'password';  GRANT ALL PRIVILEGES ON zabbix.\* TO 'zabbix'@'localhost';  FLUSH PRIVILEGES;  exit  4.Импортируйте схему данных:  zcat /usr/share/doc/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -p zabbix  5.Настройте файл конфигурации Zabbix сервера (/etc/zabbix/zabbix\_server.conf):  DBHost=localhost  DBName=zabbix  DBUser=zabbix  DBPassword=password  6.Запустите сервисы:  sudo systemctl restart zabbix-server zabbix-agent apache2  sudo systemctl enable zabbix-server zabbix-agent apache2  7.Завершите настройку через веб-интерфейс: http://server\_ip/zabbix  Настройка мониторинга сети  1.Добавьте хосты (VM1 и VM2) в Zabbix через веб-интерфейс  2.Установите Zabbix агент на Windows VM (скачайте с официального сайта)  3.Настройте триггеры для мониторинга:  o Доступность узлов (ICMP ping)  o Загрузка CPU, памяти  o Сетевой трафик  4.Создайте дашборды для визуализации данных |
| Вопрос 3  Какие виды Физического вмешательства в инфраструктуру сети вы знаете. | Виды физического вмешательства в инфраструктуру сети  Физическое вмешательство - это воздействие на аппаратные компоненты сети. Основные виды:  1.Несанкционированный доступ к оборудованию:  o Подключение к коммутаторам/маршрутизаторам  o Установка снифферов (анализаторов трафика)  o Подключение неавторизованных устройств  2.Повреждение оборудования:  o Уничтожение или порча серверов, кабелей  o Отключение электропитания  o Воздействие электромагнитными импульсами  3.Кража оборудования:  o Серверов, коммутаторов, маршрутизаторов  o Жестких дисков с конфиденциальными данными  o Резервных копий  4.Перехват данных:  o Врезка в кабельные линии  o Установка устройств прослушки  o Использование беспроводных атак (Wi-Fi)  5.Подмена оборудования:  o Замена легальных устройств на модифицированные  o Установка аппаратных закладок  Меры защиты:   * Физическая охрана серверных * Видеонаблюдение * Контроль доступа (электронные пропуска) * Использование защищённых телекоммуникационных шкафов * Шифрование данных на носителях * Регулярный аудит оборудования |

| Билет 2 |  |
| --- | --- |
| Вопрос 1  Выполнить настройку роли SMB сервера на Linux Server (В качестве ОС использовать Ubuntu Server). | **1. Настройка SMB-сервера на Ubuntu Server**  **Установка:**  bash  CopyEdit  apt update  apt install samba -y  **Создание папки и файла:**  bash  CopyEdit  mkdir -p /srv/share  echo "Файл с сервера" > /srv/share/README.txt  chmod -R 777 /srv/share  chown -R nobody:nogroup /srv/share  **Настройка /etc/samba/smb.conf:**  Добавить в **конец файла**:  conf  CopyEdit  [Share]  comment = Общая папка  path = /srv/share  browseable = yes  read only = no  guest ok = yes  force user = nobody  **Перезапуск Samba:**  bash  CopyEdit  systemctl restart smbd  **Проверка с Windows:**   1. Открыть «Проводник» 2. Ввести:   php-template |
| Вопрос 2  Проанализируйте работу нескольких устройств и постройте графики их показателей с помощью Zabbix. | **Что нужно:** На всех клиентах (например, Windows и вторая VM с Ubuntu) — установлен **Zabbix Agent**  В файле агента указан IP сервера: 192.168.0.107  Хосты добавлены через веб-интерфейс Zabbix: Configuration → Hosts → Create host  **Просмотр графиков:**  Перейди в интерфейс Zabbix:  http://192.168.0.107/zabbix  Вход: Admin / zabbix  Открой:  Monitoring → Hosts — список хостов  Monitoring → Latest data — данные по каждому хосту  Monitoring → Graphs — готовые графики по шаблонам  Выбери:  Устройство (win-pc, linux-pc)  Метрику (CPU, RAM, network) |
| Вопрос 3  Определение Активного сетевого оборудования. Какое оборудование используется. | **Активное сетевое оборудование:**  Устройства, которые требуют электропитания для работы и используются для усиления, управления и маршрутизации сетевого трафика.  **Примеры:**   * Маршрутизаторы. * Коммутаторы. * Концентраторы. * Сетевые карты. |

| Билет 3 |  |
| --- | --- |
| Вопрос 1  Выполнить настройку роли FTP сервера на Linux Server (В качестве ОС использовать Ubuntu Server). | **1. Установка FTP-сервера (vsftpd)** bash  CopyEdit  sudo apt update  sudo apt install vsftpd -y **2. Настройка vsftpd** Открываем конфигурационный файл:  bash  CopyEdit  sudo nano /etc/vsftpd.conf  🔽 Найди и измени/раскомментируй следующие строки:  conf  CopyEdit  write\_enable=YES  local\_enable=YES  anonymous\_enable=YES  anon\_root=/srv/ftp  ❗ anonymous\_enable=YES — чтобы можно было подключаться без логина и пароля  ❗ anon\_root=/srv/ftp — где будут лежать файлы **3. Создание FTP-папки и файла** bash  CopyEdit  sudo mkdir -p /srv/ftp  echo "Файл с FTP-сервера" | sudo tee /srv/ftp/ftp-readme.txt  sudo chmod -R 755 /srv/ftp **4. Перезапуск сервера** bash  CopyEdit  sudo systemctl restart vsftpd  sudo systemctl enable vsftpd **5. Проверка с Windows****📥 Скачивание:**  1. Открой браузер в Windows или Проводник 2. Введи:   cpp  CopyEdit  ftp://<IP\_UBUNTU>  📌 Например:  cpp  CopyEdit  ftp://192.168.0.107  → Должен открыться доступ и быть виден файл ftp-readme.txt **На экзамене:**  | **Что смотреть** | **Где найти** | | --- | --- | | IP Ubuntu | ip a на интерфейсе ens33 | | Файлы FTP | Папка /srv/ftp | | Проверка на Windows | Через ftp://<ip> в Проводнике | |
| Вопрос 2  Выполнить установку и настройку программы для мониторинга систем. | Ты можешь выбрать **любой простой мониторинг**. На экзамене самый быстрый способ — установить **Netdata**, потому что:   * Устанавливается одной командой * Имеет веб-интерфейс * Наглядно показывает нагрузку, порты, сеть, память, диски  **Установка Netdata:** bash  CopyEdit  bash <(curl -Ss https://my-netdata.io/kickstart.sh) --disable-telemetry  Установка займёт 1–2 минуты, автоматическая. **После установки:** Netdata будет доступна в браузере по:  cpp  CopyEdit  http://<IP\_UBUNTU>:19999  Например:  cpp  CopyEdit  http://192.168.0.107:19999  На Windows зайди через браузер и проверь, отображаются ли:   * Загрузка CPU * RAM * Сеть * Работа дисков |
| Вопрос 3  Определение Пассивного сетевого оборудования. Какое оборудование используется. | **Пассивное сетевое оборудование:**  Компоненты, которые не требуют электропитания для своей работы и используются для соединения и поддержки активного оборудования и передачи данных в сети.  **Примеры:**   * Кабели (коаксиальный кабель, витая пара, оптоволокно). * Сетевые разъемы и соединители. * Патч-панели. * Шкафы и стойки для размещения оборудования. |

| Билет 4 |  |
| --- | --- |
| Вопрос 1  Выполнить настройку роли сервера базы данных MySQL на Linux Server (В качестве ОС использовать Ubuntu Server). Проверка сервера осуществляется любым из возможных способов. | **1. Установка MySQL Server** bash  CopyEdit  sudo apt update  sudo apt install mysql-server -y **2. Проверка и запуск службы** Проверим, запущен ли MySQL:  bash  CopyEdit  sudo systemctl status mysql  Если нужно — запусти вручную:  bash  CopyEdit  sudo systemctl start mysql  sudo systemctl enable mysql **3. Настройка безопасности (опционально)** Можно выполнить встроенный скрипт настройки:  bash  CopyEdit  sudo mysql\_secure\_installation  Рекомендуется:   * Установить root-пароль * Удалить анонимных пользователей * Отключить удалённый root-доступ * Удалить тестовую БД  **4. Проверка, что MySQL работает****Способ 1: через CLI** bash  CopyEdit  sudo mysql  Внутри:  sql  CopyEdit  SHOW DATABASES;  Если ты видишь:  pgsql  CopyEdit  +--------------------+  | Database |  +--------------------+  | information\_schema |  | mysql |  | performance\_schema |  | sys |  +--------------------+  значит сервер **работает**. |
| Вопрос 2  Проанализируйте работу сети с использованием протокола SNMP. | **Что такое SNMP:** **SNMP (Simple Network Management Protocol)** — протокол мониторинга сетевых устройств (роутеры, коммутаторы, сервера) через UDP-порт 161.  **Как проанализировать работу сети через SNMP** Можно использовать утилиту snmpwalk для опроса устройств. **Установка на Ubuntu:** bash  CopyEdit  sudo apt install snmp snmpd -y **Настройка SNMP-демона:** Открой:  bash  CopyEdit  sudo nano /etc/snmp/snmpd.conf  Найди строку:  conf  CopyEdit  agentAddress udp:127.0.0.1:161  И замени на:  conf  CopyEdit  agentAddress udp:161,udp6:[::1]:161  Разреши доступ (для теста):  conf  CopyEdit  rocommunity public  Сохрани → перезапусти:  bash  CopyEdit  sudo systemctl restart snmpd **Проверка:** bash  CopyEdit  snmpwalk -v 2c -c public 127.0.0.1  Если видишь длинный список iso.3.6.1... — значит SNMP работает |
| Вопрос 3  Какие типы Полосы пропускания вы знаете. | **Типы полосы пропускания:**   * **Симметричная** (одинаковая скорость загрузки и отдачи, например, выделенные линии). * **Асимметричная** (разная скорость загрузки и отдачи, например, DSL, DOCSIS). * **Гарантированная (выделенная)** (фиксированная пропускная способность). * **Разделяемая (общая)** (пропускная способность распределяется между пользователями).   **Факторы, влияющие на полосу пропускания:**   * Тип используемого сетевого оборудования. * Сетевые протоколы. * Загрузка сети. |

| Билет 5 |  |
| --- | --- |
| Вопрос 1  Выполнить настройку роли веб сервера на Linux Server (В качестве ОС использовать Ubuntu Server). | **1. Установка веб-сервера Apache**  bash  CopyEdit  sudo apt update  sudo apt install apache2 -y  **2. Перезапуск и автозапуск**  bash  CopyEdit  sudo systemctl restart apache2  sudo systemctl enable apache2  **3. Открыть порт 80 (если включён UFW)**  bash  CopyEdit  sudo ufw allow 80/tcp  Проверь статус:  bash  CopyEdit  sudo systemctl status apache2  **4. Проверка веб-сервера**  По умолчанию веб-документы лежат в:  css  CopyEdit  /var/www/html/index.html  Можно изменить файл:  bash  CopyEdit  echo "Привет с веб-сервера Apache!" | sudo tee /var/www/html/index.html  **5. Проверка с Windows**  Открой браузер в Windows и введи:  cpp  CopyEdit  http://<IP\_UBUNTU>  Например:  cpp  CopyEdit  http://192.168.0.107  Если permisssion denied  **Правильно — нужно отредактировать или перезаписать файл.**  Вот два простых варианта:  **Вариант 1: Быстрая замена содержимого**  bash  CopyEdit  echo "Привет с Apache от $USER" | sudo tee /var/www/html/index.html  **Вариант 2: Редактировать через nano**  bash  CopyEdit  sudo nano /var/www/html/index.html  И вставь туда:  html  CopyEdit  <!DOCTYPE html>  <html>  <head><title>Apache Test</title></head>  <body>  <h1>Привет с веб-сервера Apache!</h1>  </body>  </html>  Сохрани: Ctrl + O, затем Enter, затем Ctrl + X  **После этого:**  Открой на Windows в браузере:  cpp  CopyEdit  http://<IP\_UBUNTU>  → Увидишь страницу с твоим заголовком. |
| Вопрос 2  Постройте топологию сети с помощью Zabbix. | **🔧 Как это делается:****1. Убедись, что в Zabbix добавлены** хосты **(сервер, Windows-ПК и т.д.)****2. Перейди в веб-интерфейс:** arduino  CopyEdit  http://192.168.0.107/zabbix **3. В меню:** arduino  CopyEdit  Monitoring → Maps → Create map **4. Задай имя карты (например, LocalNetMap)** Нажми **Add**. **5. Теперь в списке → нажми** Edit **на созданной карте.****6. Внутри карты:**  * Нажми **Add element** * Выбери хост (например, Ubuntu, Windows-PC) * Назначь иконку (например, сервер, ПК) * Повтори для всех узлов  **7. Чтобы соединить — выбери элемент → нажми** Link **→ укажи другой элемент** (можно задать **триггер**, чтобы цвет связи менялся при проблеме) |
| Вопрос 3  Виды факторов, влияющие на Полосу пропускания. | **Полоса пропускания** — это максимально возможная скорость передачи данных по каналу за единицу времени (обычно измеряется в Мбит/с или Гбит/с).  Основные факторы:   | **Фактор** | **Как влияет** | | --- | --- | | Тип среды передачи | Витая пара (Cat 5/6), оптоволокно, Wi-Fi — разные лимиты | | Пропускная способность оборудования | Ограничения роутеров, коммутаторов, портов и кабелей | | Количество пользователей | Чем больше устройств — тем выше нагрузка |   ФАКТОР КАК ВЛИЯЕТ  📶 Уровень помех Экранирование, перекрёстные сигналы, качество соединений  ⚙️ Протоколы и нагрузка приложений VPN, видео, стримы сильно нагружают канал  🚨 Ошибки и перегрузки сети Потери пакетов → повторные передачи → падение эффективности  📐 Топология сети Неоптимальные пути = задержки и потери |

| Билет 6 |  |
| --- | --- |
| Вопрос 1  Выполнить настройку роли прокси сервера на Linux Server (В качестве ОС использовать Ubuntu Server). | **1. Установка Squid** bash  CopyEdit  sudo apt update  sudo apt install squid -y  **2. Основной конфигурационный файл:** bash  CopyEdit  sudo nano /etc/squid/squid.conf  **3. Разрешаем доступ из локальной сети** Найди блок:  conf  CopyEdit  http\_access deny all  И **добавь до него**:  conf  CopyEdit  acl localnet src 192.168.0.0/24  http\_access allow localnet  Убедись, что:  conf  CopyEdit  http\_port 3128  **оставлен как есть** — это порт, на котором Squid будет слушать. **4. Перезапуск** bash  CopyEdit  sudo systemctl restart squid  **5. Проверка с Windows****На клиенте (например, Windows 10):**  1. Открой браузер → настройки → «Сеть / Прокси» 2. Включи ручную настройку прокси 3. Укажи:    * **IP Ubuntu-сервера** (посмотри через ip a, например: 192.168.0.107)    * **Порт: 3128**  **Проверка:**  1. Перейди в браузере на сайт (например, [https://example.com](https://example.com/)) 2. Если всё работает → **значит трафик проходит через Ubuntu-прокси** |
| Вопрос 2  Определить количество и диапазон ip адресов подсети, если номер подсети - 26.219.128.168, маска подсети – 255.255.255.128. | **📐 Как использовать ipcalc** Если она не установлена — ставим:  bash  CopyEdit  sudo apt install ipcalc -y  Затем запускаем:  bash  CopyEdit  ipcalc 26.219.128.168 255.255.255.128 **🔍 Пример вывода:** text  CopyEdit  Address: 26.219.128.168  Netmask: 255.255.255.128 = 25  Network: 26.219.128.128/25  Broadcast: 26.219.128.255  HostMin: 26.219.128.129  HostMax: 26.219.128.254  Hosts/Net: 126 **📊 Разбор билетов:****📌** Билет №2 – IP-подсеть **Адрес:** 26.219.128.168  **Маска:** 255.255.255.128 **(= /25)** **👉 Через ipcalc:** bash  CopyEdit  ipcalc 26.219.128.168 255.255.255.128 **✍️ Ответ:**  * Сетевой адрес: **26.219.128.128** * Диапазон IP: **с 26.219.128.129 до 26.219.128.254** * Broadcast: **26.219.128.255** * Количество пригодных IP: **126**   **Адрес:** 26.219.128.168  **Маска:** 255.255.255.128 **(тот же пример)**  👉 Повторно, ты можешь ввести ту же команду:  ipcalc 26.219.128.168 255.255.255.128 |
| Вопрос 3  Паспорт технических устройств. Ключевые компоненты паспорта технических устройств. | **Паспорт технических устройств. Ключевые компоненты:**  **Паспорт технического устройства — это официальный документ, содержащий полную информацию о параметрах, характеристиках и условиях эксплуатации оборудования.**   * Наименование и модель устройства. * Серийный номер и инвентарный номер. * Технические характеристики (производительность, мощность, интерфейсы). * Дата изготовления и срок эксплуатации. * Условия эксплуатации (температура, влажность, электропитание). * Гарантийные обязательства и сервисные контакты. * История обслуживания и ремонтов. |

| Билет 7 | |
| --- | --- |
| Вопрос 1  Выполнить настройку роли веб сервера в докер контейнере на Linux Server (В качестве ОС использовать Ubuntu Server). | Настройка веб-сервера в Docker контейнере на Ubuntu Server  Установка Docker  1.Обновите пакеты и установите зависимости:  sudo apt update  sudo apt install apt-transport-https ca-certificates curl software-properties-common  2.Добавьте официальный GPG-ключ Docker:  curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg  3.Добавьте репозиторий Docker:  echo "deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/ubuntu $(lsb\_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null  4.Установите Docker:  sudo apt update  sudo apt install docker-ce docker-ce-cli [containerd.io](http://containerd.io)  5.Проверьте установку:  sudo docker run hello-world  Развертывание веб-сервера Nginx в контейнере  1.Запустите контейнер с Nginx:  sudo docker run --name my-nginx -d -p 80:80 nginx  • --name my-nginx - имя контейнера  • -d - запуск в фоновом режиме  • -p 80:80 - проброс портов (хост:контейнер)  2.Проверьте работу:  curl http://localhost:8080  Или откройте в браузере IP-адрес сервера.  Создание пользовательского веб-приложения  1.Создайте директорию и HTML-файл:  mkdir ~/my-website  echo "<h1>Мой сайт в Docker</h1>" > ~/my-website/index.html  2.Запустите контейнер с монтированием вашего сайта:  sudo docker run --name custom-nginx -d -p 8080:80 -v ~/my-website:/usr/share/nginx/html nginx  3.Проверьте результат на порту 8080. |
| Вопрос 2  Определить количество и диапазон ip адресов подсети, если номер подсети - 26.219.128.0, маска подсети – 255.255.192.0. | Определение количества и диапазона IP-адресов подсети  Дано:  IP-адрес сети: 26.219.128.0  Маска подсети: 255.255.192.0  Шаг 1. Определение класса сети  Адрес 26.219.128.0 принадлежит классу A (диапазон 1.0.0.0 - 126.255.255.255), но современные сети используют бесклассовую адресацию (CIDR).  Шаг 2. Перевод маски в CIDR-нотацию  255.255.192.0 в бинарном виде:  11111111.11111111.11000000.00000000  Количество единиц = 18, значит маска /18.  Шаг 3. Расчет количества хостов  Количество бит для хостов = 32 - 18 = 14 бит.  Количество адресов = 2^14 = 16,384.  Доступных хостов = 16,384 - 2 (сеть и broadcast) = 16,382.  Шаг 4. Определение диапазона адресов  Маска 255.255.192.0 означает, что меняется третий октет на 64 (192 = 11000000 в бинарном виде, где меняются 2 бита).  Диапазон сети:  Начальный адрес: 26.219.128.0 (адрес сети)  Конечный адрес: 26.219.191.255 (broadcast)  Доступные адреса: 26.219.128.1 - 26.219.191.254 |
| Вопрос 3  Определение Физическая карта сети. | Физическая карта сети — это схематическое представление реальной инфраструктуры компьютерной сети, которое отображает:  Все физические устройства (серверы, компьютеры, маршрутизаторы, коммутаторы, точки доступа и т.д.).  Способы их соединения (типы кабелей — Ethernet, оптоволокно, беспроводные связи).  Расположение оборудования (географическое или в пределах здания, например, серверная комната, этажи, рабочие станции).  Ключевые элементы:  Оборудование (модели, порты, MAC-адреса).  Топология подключений (звезда, кольцо, шина и др.).  Технические характеристики (длина кабелей, скорость соединений, типы разъемов).  Отличие от логической топологии:  Физическая карта показывает реальные соединения, а логическая — пути передачи данных (IP-адреса, VLAN, маршруты). |

| Билет 8 | |
| --- | --- |
| Вопрос 1  Выполнить настройку роли прокси сервера в докер контейнере на Linux Server (В качестве ОС использовать Ubuntu Server). | Настройка прокси-сервера в Docker контейнере на Ubuntu Server  Установка Docker  1.Обновите пакеты и установите зависимости:  sudo apt update  sudo apt install apt-transport-https ca-certificates curl software-properties-common  2.Добавьте официальный GPG-ключ Docker:  curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg  3.Добавьте репозиторий Docker:  echo "deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/ubuntu $(lsb\_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null  4.Установите Docker:  sudo apt update  sudo apt install docker-ce docker-ce-cli containerd.io  5.Проверьте установку:  sudo docker run hello-world  Запуск прокси-сервера Squid в контейнере  1.Создадим конфигурационный файл:  mkdir ~/squid-config  echo "http\_port 3128  acl localnet src 192.168.0.0/16  http\_access allow localnet  http\_access deny all" > ~/squid-config/squid.conf  2.Запустим контейнер:  sudo docker run --name squid-proxy -d \  -p 3128:3128 \  -v ~/squid-config/squid.conf:/etc/squid/squid.conf \  ubuntu/squid:latest  3. Проверим работу:  curl -x http://localhost:3128 <http://example.com>  Настройка клиентов (VM1 и VM2)  Для Linux (VM1):  export http\_proxy="http://<IP\_сервера>:3128"  export https\_proxy="http://<IP\_сервера>:3128"  Для Windows (VM2):  1. Откройте "Параметры" > "Сеть и Интернет" > "Прокси"  2. Включите "Использовать прокси-сервер"  3. Введите адрес сервера и порт 3128 |
| Вопрос 2  Определить находятся ли два узла А и В в одной подсети, если адреса компьютеров А и В 26.219.123.6 и 26.218.102.31. Маска подсети 255.255.192.0. | Определение нахождения узлов в одной подсети  Дано:  Узел A: 26.219.123.6  Узел B: 26.218.102.31  Маска подсети: 255.255.192.0 (/18)  Алгоритм проверки:  Перевести IP-адреса и маску в бинарный вид  Применить операцию AND между IP и маской  Сравнить результаты  Расчет:  Маска 255.255.192.0 в бинарном виде:  11111111.11111111.11000000.00000000  Для узла A (26.219.123.6):  26.219.123.6 = 00011010.11011011.01111011.00000110  AND 255.255.192.0 = 11111111.11111111.11000000.00000000  --------------------------------------------  Результат: 00011010.11011011.01000000.00000000 = 26.219.64.0  Для узла B (26.218.102.31):  26.218.102.31 = 00011010.11011010.01100110.00011111  AND 255.255.192.0 = 11111111.11111111.11000000.00000000  --------------------------------------------  Результат: 00011010.11011010.01000000.00000000 = 26.218.64.0  Вывод:  Адреса сетей разные (26.219.64.0 ≠ 26.218.64.0), значит узлы находятся в разных подсетях. |
| Вопрос 3  Определение Логической топологии сети. Какие типы топологии вы знаете. | Логическая топология сети: определение и типы  Определение:  Логическая топология сети - это способ организации передачи данных между узлами сети, определяющий маршруты потоков информации и правила взаимодействия устройств, независимо от их физического расположения.  Основные типы логических топологий:  Шина (Bus):  Все устройства подключены к одному общему каналу  Данные передаются всем, но принимает только адресат  Пример: классические Ethernet сети на коаксиальном кабеле  Звезда (Star):  Все устройства подключены к центральному узлу (коммутатору)  Центральный узел управляет передачей данных  Наиболее распространенная в современных LAN  Кольцо (Ring):  Устройства соединены в замкнутый круг  Данные передаются по кругу от узла к узлу  Пример: Token Ring, FDDI  Сетка (Mesh):  Полносвязная: каждый узел соединен со всеми остальными  Частично-связная: несколько путей между узлами  Используется в WAN и критически важных сетях  Дерево (Tree):  Иерархическая структура с корневым узлом  Комбинация "звезд", соединенных между собой  Используется в крупных корпоративных сетях  Гибридные топологии:  Комбинация нескольких базовых топологий  Например: звезда-кольцо, звезда-шина  Особенности логической топологии в задании:  В представленной сети (VM1 - Server - VM2) используется топология "звезда", где:  Сервер выступает центральным узлом  VM1 и VM2 являются конечными узлами  Все взаимодействие идет через сервер |

| Билет 9 | |
| --- | --- |
| Вопрос 1  Выполнить настройку роли сервера БД MySQL + Adminer (Реализовать в контейнерах Docker) на Linux Server (В качестве ОС использовать Ubuntu Server). | Настройка MySQL и Adminer в Docker  Установка Docker  1.Обновите пакеты и установите зависимости:  sudo apt update  sudo apt install apt-transport-https ca-certificates curl software-properties-common  2.Добавьте официальный GPG-ключ Docker:  curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg  3.Добавьте репозиторий Docker:  echo "deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/ubuntu $(lsb\_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null  4.Установите Docker:  sudo apt update  sudo apt install docker-ce docker-ce-cli containerd.io  5.Проверьте установку:  sudo docker run hello-world  Запуск MySQL сервера в контейнере  sudo docker run --name mysql-server -d \  -e MYSQL\_ROOT\_PASSWORD=mysecretpassword \  -e MYSQL\_DATABASE=exampledb \  -e MYSQL\_USER=exampleuser \  -e MYSQL\_PASSWORD=examplepass \  -p 3306:3306 \  mysql:8.0  Запуск Adminer (веб-интерфейс для управления БД)  sudo docker run --name adminer -d \  -p 8080:8080 \  --link mysql-server:db \  adminer  Проверка работы:  1. MySQL доступен на localhost:3306  2. Adminer доступен в браузере: http://<IP\_сервера>:8080  Для входа используйте:  Система: MySQL  Сервер: db (или IP контейнера mysql-server)  Пользователь: exampleuser  Пароль: examplepass  База данных: exampledb |
| Вопрос 2  Выполнить установку и настройку программы для мониторинга систем. | Установка и настройка Zabbix  Подготовка сервера  1.Обновите систему:  sudo apt update && sudo apt upgrade -y  2.Установите необходимые зависимости:  sudo apt install -y apache2 php php-mysql php-mbstring php-gd php-xml php-bcmath php-ldap mariadb-server  Настройка базы данных MariaDB  1.Запустите защищенную настройку MySQL:  sudo mysql\_secure\_installation  (Ответьте на вопросы: установите пароль root, удалите анонимных пользователей, отключите удаленный root-доступ, удалите тестовую БД)  2.Создайте базу данных для Zabbix:  sudo mysql -uroot -p  Введите в консоли MySQL:  CREATE DATABASE zabbix CHARACTER SET utf8 COLLATE utf8\_bin;  CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'zabbix\_password';  GRANT ALL PRIVILEGES ON zabbix.\* TO 'zabbix'@'localhost';  FLUSH PRIVILEGES;  EXIT;  Установка Zabbix Server  1.Добавьте репозиторий Zabbix:  wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release\_6.0-4+ubuntu$(lsb\_release -rs)\_all.deb  sudo dpkg -i zabbix-release\_6.0-4+ubuntu$(lsb\_release -rs)\_all.deb  sudo apt update  2.Установите Zabbix компоненты:  sudo apt install -y zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent  3.Импортируйте начальную схему данных:  zcat /usr/share/doc/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -p zabbix  (Введите пароль пользователя zabbix, который создавали ранее)  Настройка Zabbix Server  1.Отредактируйте конфигурационный файл:  sudo nano /etc/zabbix/zabbix\_server.conf  Найдите и измените параметры:  DBHost=localhost  DBName=zabbix  DBUser=zabbix  DBPassword=zabbix\_password  2.Настройте PHP для Zabbix:  sudo nano /etc/php/8.1/apache2/php.ini  Проверьте и измените при необходимости:  max\_execution\_time = 300  memory\_limit = 128M  post\_max\_size = 16M  upload\_max\_filesize = 2M  date.timezone = Europe/Moscow # Укажите свой часовой пояс  3.Перезапустите сервисы:  sudo systemctl restart apache2 zabbix-server zabbix-agent  sudo systemctl enable apache2 zabbix-server zabbix-agent  Завершение установки через веб-интерфейс  1.Откройте в браузере: http://<IP\_сервера>/zabbix  2.Следуйте инструкциям мастера установки:  Проверьте требования (все должно быть OK)  Настройте подключение к БД:  Тип БД: MySQL  Хост: localhost  Порт: 3306  Имя БД: zabbix  Пользователь: zabbix  Пароль: zabbix\_password  Укажите данные сервера (имя можно оставить по умолчанию)  Проверьте все параметры и завершите установку  Логин: Admin (с большой буквы), пароль: zabbix  Настройка мониторинга хостов  1.Добавьте сервер в мониторинг:  Перейдите в "Configuration" → "Hosts"  Нажмите "Create host"  Укажите:  Host name: Ubuntu Server  Groups: Linux servers  IP address: 127.0.0.1  На вкладке "Templates" добавьте шаблон "Linux by Zabbix agent"  2.Добавьте Windows VM:  Установите Zabbix Agent на Windows:  Скачайте с https://www.zabbix.com/download\_agents  Установите, укажите в конфиге (C:\Program Files\Zabbix Agent\zabbix\_agentd.conf):  Server=<IP\_вашего\_zabbix\_сервера>  ServerActive=<IP\_вашего\_zabbix\_сервера>  Hostname=Windows VM  В веб-интерфейсе Zabbix добавьте новый хост аналогично Linux, но с шаблоном "Windows by Zabbix agent"  3.Настройте дашборды:  Перейдите в "Monitoring" → "Dashboards"  Создайте новый дашборд или используйте предустановленные  Добавьте виджеты для отображения CPU, памяти, дисков и сети  Дополнительные настройки  1.Настройка email-оповещений:  "Administration" → "Media types" → "Email"  Настройте SMTP параметры  В "Users" назначьте email для пользователя Admin  2.Установка дополнительных агентов:  Для более детального мониторинга можно установить:  sudo apt install zabbix-agent2  Конфигурация находится в /etc/zabbix/zabbix\_agent2.conf  3.Обновление Zabbix:  sudo apt update && sudo apt upgrade zabbix-\*  sudo systemctl restart zabbix-server zabbix-agent apache2 |
| Вопрос 3  Какие типы Полосы пропускания вы знаете. | типы полосы пропускания  1. По способу распределения:  Выделенная (Dedicated):  Фиксированная полоса, гарантированная для одного пользователя/приложения  Пример: выделенные линии T1/E1, оптические каналы  Разделяемая (Shared):  Полоса распределяется между несколькими пользователями  Пример: обычный Ethernet, Wi-Fi, DOCSIS (кабельный интернет)  2. По ширине:  Узкая полоса (Narrowband):  До 56 Кбит/с (модемные соединения)  IoT устройства (LoRaWAN, Zigbee)  Широкая полоса (Broadband):  Высокоскоростные соединения (от 1 Мбит/с)  DSL, кабельный интернет, оптоволокно  Ультра-широкая полоса (Ultra-wideband):  Очень высокие скорости (1 Гбит/с и выше)  5G, оптоволокно FTTH  3. По технологии передачи:  Симметричная:  Одинаковая скорость загрузки и выгрузки  Пример: выделенные линии, оптоволокно  Асимметричная:  Разная скорость загрузки и выгрузки  Пример: ADSL (обычно download > upload)  4. По назначению:  Голосовая полоса:  Оптимизирована для передачи голоса (телефония)  Диапазон 300-3400 Гц  Данные:  Для передачи цифровых данных  Может быть от Кбит/с до Тбит/с  Мультимедийная:  Для видео, аудио потоков  Требует высокой и стабильной полосы  Измерение полосы пропускания:  В битах в секунду (бит/с, Кбит/с, Мбит/с, Гбит/с)  Пропускная способность канала (throughput)  Задержка (latency) и джиттер также влияют на эффективную полосу |

| Билет 10 | |
| --- | --- |
| Вопрос 1  Выполнить настройку роли FTP сервера на Linux Server (В качестве ОС использовать Ubuntu Server). | Настройка FTP сервера и анализ сети  1. Настройка FTP сервера на Ubuntu Server  Установка vsftpd (Very Secure FTP Daemon)  sudo apt update  sudo apt install vsftpd  Базовая конфигурация  1.Отредактируйте конфигурационный файл:  sudo nano /etc/vsftpd.conf  2.Измените/добавьте следующие параметры:  anonymous\_enable=NO  local\_enable=YES  write\_enable=YES  chroot\_local\_user=YES  allow\_writeable\_chroot=YES  local\_umask=022  pasv\_min\_port=40000  pasv\_max\_port=50000  listen=YES  listen\_ipv6=NO  3.Создайте пользователя для FTP (если нужно):  sudo adduser ftpuser  sudo mkdir -p /home/ftpuser/ftp  sudo chown nobody:nogroup /home/ftpuser/ftp  sudo chmod a-w /home/ftpuser/ftp  sudo mkdir /home/ftpuser/ftp/files  sudo chown ftpuser:ftpuser /home/ftpuser/ftp/files  4.Разрешите FTP в firewall (если используется):  sudo ufw allow 20/tcp  sudo ufw allow 21/tcp  sudo ufw allow 40000:50000/tcp  sudo ufw enable  5.Перезапустите службу:  sudo systemctl restart vsftpd  sudo systemctl enable vsftpd  Проверка работы  1.С Linux клиента:  ftp <IP\_сервера>  (используйте логин/пароль созданного пользователя)  2.С Windows клиента:  • Используйте File Explorer: ftp://<IP\_сервера>  • Или программу FileZilla |
| Вопрос 2  2. Определить количество и диапазон ip адресов подсети, если номер подсети - 26.219.128.168, маска подсети – 255.255.255.128. | Определение количества и диапазона IP-адресов подсети  Дано:  • IP-адрес сети: 26.219.128.168  • Маска подсети: 255.255.255.128 (/25)  Шаг 1. Определение адреса сети  1.Переведите адрес и маску в бинарный вид:  26.219.128.168 = 00011010.11011011.10000000.10101000  255.255.255.128 = 11111111.11111111.11111111.10000000  2.Примените операцию AND:  00011010.11011011.10000000.10101000 (26.219.128.168)  AND  11111111.11111111.11111111.10000000 (255.255.255.128)  =  00011010.11011011.10000000.10000000 (26.219.128.128)  Адрес сети: 26.219.128.128  Шаг 2. Расчет количества хостов  Маска /25 означает:  • 25 бит для сети  • 7 бит для хостов (32-25=7)  • Количество адресов: 2^7 = 128  • Доступных хостов: 128 - 2 = 126 (минус адрес сети и broadcast)  Шаг 3. Определение диапазона адресов  • Адрес сети: 26.219.128.128  • Первый доступный адрес: 26.219.128.129  • Последний доступный адрес: 26.219.128.254  • Broadcast адрес: 26.219.128.255  Шаг 4. Проверка принадлежности исходного адреса  Исходный адрес 26.219.128.168 находится в диапазоне 26.219.128.129-254, значит он является допустимым адресом хоста в этой подсети. |
| Вопрос 3  Какие виды Физического вмешательства в инфраструктуру сети вы знаете. | Виды физического вмешательства в инфраструктуру сети  1. Несанкционированный доступ к оборудованию  Подключение посторонних устройств к коммутаторам/маршрутизаторам  Установка снифферов (анализаторов трафика)  Физический перехват данных через tap-устройства  2. Повреждение оборудования  Умышленная порча кабелей (медных/оптических)  Вывод из строя активного оборудования (серверов, коммутаторов)  Отключение электропитания (включая ИБП)  3. Кража оборудования  Хищение серверов или сетевого оборудования  Кража жестких дисков с конфиденциальными данными  Изъятие резервных носителей информации  4. Подмена оборудования  Установка модифицированных устройств с закладками  Замена легального оборудования на компрометированное  Установка несертифицированных компонентов  5. Электромагнитное воздействие  Использование TEMPEST-атак для перехвата данных  Применение электромагнитных импульсов для вывода оборудования из строя  Создание помех в беспроводных сетях  6. Визуальный шпионаж  Подглядывание за вводимыми паролями  Фотографирование сетевых диаграмм и конфигураций  Сбор информации по мусору (дампстер-дайвинг)  Методы защиты:  Физическая безопасность:  Охраняемые серверные помещения  Запертые телекоммуникационные шкафы  Видеонаблюдение  Контроль доступа:  Системы биометрической идентификации  Журналы учета посещений  Разграничение зон доступа  Защита данных:  Шифрование хранимой информации  Уничтожение носителей по специальным процедурам  Регулярные резервные копии  Мониторинг:  Датчики вскрытия оборудования  Системы обнаружения вторжений  Контроль целостности оборудования |

| Билет 11 | |
| --- | --- |
| Вопрос 1    Выполнить настройку ролей DNS и DHCP на Linux Server (В качестве ОС использовать Ubuntu Server). | Настройка ролей DNS и DHCP на Linux Server (Ubuntu Server)  Настройка DHCP сервера  1.Установите пакет DHCP-сервера:  sudo apt update  sudo apt install isc-dhcp-server  2.Отредактируйте конфигурационный файл /etc/dhcp/dhcpd.conf:  sudo nano /etc/dhcp/dhcpd.conf  Добавьте конфигурацию (пример):  subnet 192.168.1.0 netmask 255.255.255.0 {  range 192.168.1.100 192.168.1.200;  option routers 192.168.1.1;  option domain-name-servers 192.168.1.1;  option domain-name "example.com";  }  3.Укажите сетевой интерфейс в /etc/default/isc-dhcp-server:  INTERFACESv4="eth0"  4.Запустите и включите сервис:  sudo systemctl start isc-dhcp-server  sudo systemctl enable isc-dhcp-server  Настройка DNS сервера (BIND9)  1.Установите BIND9:  sudo apt install bind9  2.Настройте файл зоны в /etc/bind/named.conf.local:  zone "example.com" {  type master;  file "/etc/bind/db.example.com";  };  3.Создайте файл зоны (пример /etc/bind/db.example.com):  $TTL 604800  @ IN SOA ns1.example.com. admin.example.com. (  2023050101 ; Serial  604800 ; Refresh  86400 ; Retry  2419200 ; Expire  604800 ) ; Negative Cache TTL  ;  @ IN NS ns1.example.com.  @ IN A 192.168.1.1  ns1 IN A 192.168.1.1  www IN A 192.168.1.10  4.Проверьте конфигурацию и перезапустите BIND:  sudo named-checkconf  sudo systemctl restart bind9  sudo systemctl enable bind |
| Вопрос 2  Постройте топологию сети с помощью Zabbix. | Построение топологии сети в Zabbix  Предварительная настройка Zabbix:  Убедитесь, что Zabbix сервер установлен и работает  Установите и настройте Zabbix агенты на всех узлах сети  1. Установка Zabbix сервера на Linux Server (Ubuntu)  Установка необходимых компонентов  sudo apt update  sudo apt upgrade -y  sudo apt install -y apache2 php php-mysql php-mbstring php-gd php-xml php-bcmath mariadb-server  Настройка базы данных  sudo mysql\_secure\_installation  # Следуйте инструкциям, установите пароль для root  sudo mysql -uroot -p  В MySQL выполните:  CREATE DATABASE zabbix CHARACTER SET utf8 COLLATE utf8\_bin;  CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'ваш\_пароль';  GRANT ALL PRIVILEGES ON zabbix.\* TO 'zabbix'@'localhost';  FLUSH PRIVILEGES;  EXIT;  Установка Zabbix  wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release\_6.0-4+ubuntu$(lsb\_release -rs)\_all.deb  sudo dpkg -i zabbix-release\_6.0-4+ubuntu$(lsb\_release -rs)\_all.deb  sudo apt update  sudo apt install -y zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent  Импорт начальной схемы  zcat /usr/share/doc/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -p zabbix  Настройка конфигурации  sudo nano /etc/zabbix/zabbix\_server.conf  Измените параметры:  DBHost=localhost  DBName=zabbix  DBUser=zabbix  DBPassword=ваш\_пароль  Запуск сервисов  sudo systemctl restart zabbix-server zabbix-agent apache2  sudo systemctl enable zabbix-server zabbix-agent apache2  Доступ к веб-интерфейсу  Откройте в браузере: http://<IP\_Linux\_Server>/zabbix  • Логин: Admin (с большой буквы)  • Пароль: zabbix  2. Установка Zabbix агента на Linux Server (тот же сервер)  Уже установлен вместе с сервером. Проверьте конфигурацию:  sudo nano /etc/zabbix/zabbix\_agentd.conf  Убедитесь, что есть:  Server=127.0.0.1  ServerActive=127.0.0.1  Hostname=Linux Server  3. Установка Zabbix агента на Windows 10 (VM 2)  1. Скачайте агент для Windows:  o Перейдите на https://www.zabbix.com/download\_agents  o Выберите версию, соответствующую вашей Windows (обычно Windows 64-bit)  o Скачайте архив (например, zabbix\_agent-6.0.15-windows-amd64-openssl.zip)  2. Установка:  o Распакуйте архив в C:\Program Files\Zabbix Agent  o Отредактируйте файл конфигурации C:\Program Files\Zabbix Agent\conf\zabbix\_agentd.conf:  Server=<IP\_Linux\_Server>  ServerActive=<IP\_Linux\_Server>  Hostname=Windows 10  o Откройте командную строку (как администратор) и выполните:  cd "C:\Program Files\Zabbix Agent\bin"  zabbix\_agentd.exe -c "C:\Program Files\Zabbix Agent\conf\zabbix\_agentd.conf" -i  zabbix\_agentd.exe -c "C:\Program Files\Zabbix Agent\conf\zabbix\_agentd.conf" -s  4. Настройка мониторинга в веб-интерфейсе Zabbix  Добавление хостов  Войдите в веб-интерфейс Zabbix  Перейдите: Configuration → Hosts → Create host  Для Linux Server:  Host name: Linux Server  Groups: Linux servers  IP address: <IP\_Linux\_Server>  На вкладке Templates: Link new templates → Template OS Linux by Zabbix agent  Для Windows 10:  Host name: Windows 10  Groups: Windows servers  IP address: <IP\_Windows\_10>  На вкладке Templates: Link new templates → Template OS Windows by Zabbix agent  Проверка подключения  На главной странице перейдите: Monitoring → Hosts  Убедитесь, что в колонке "Availability" для обоих хостов зеленая иконка "ZBX"  5. Настройка карты сети в Zabbix  Перейдите: Monitoring → Maps → Create map  Настройте основные параметры:  Name: "Office Network"  Width: 800  Height: 600  Добавьте элементы:  Нажмите "Add" → выберите "Host"  Добавьте оба хоста (Linux Server и Windows 10)  Расположите их на карте  Добавьте соединение:  Нажмите "Add" → выберите "Link"  Соедините два хоста линией  Можно настроить тип и цвет линии  Сохраните карту:  Нажмите "Update" и "Save" |
| Вопрос 3  Виды факторов, влияющие на Полосу пропускания. | Факторы, влияющие на полосу пропускания  Технические факторы  Физическая среда передачи:  Витая пара (Cat5e - до 1 Гбит/с, Cat6 - до 10 Гбит/с)  Оптоволокно (одномодовое/многомодовое)  Беспроводные технологии (Wi-Fi 5/6)  Оборудование:  Пропускная способность коммутаторов/маршрутизаторов  Качество сетевых карт  Нагрузка на процессоры сетевых устройств  Конфигурация сети:  Настройки QoS (Quality of Service)  VLAN и сегментация сети  Использование дуплексных режимов  Внешние факторы  Загрузка сети:  Количество активных пользователей  Тип передаваемого трафика (видео, голос, данные)  Коллизии в Ethernet-сетях  Помехи и наводки:  Электромагнитные помехи (для медных кабелей)  Перекрестные наводки (crosstalk)  Для Wi-Fi: соседние сети, физические преграды  Протоколы и накладные расходы:  Заголовки протоколов (TCP/IP, Ethernet)  Шифрование трафика (VPN, SSL/TLS)  Механизмы контроля ошибок и повторной передачи  Методы оптимизации  Аппаратные решения:  Обновление сетевой инфраструктуры  Использование балансировщиков нагрузки  Внедрение агрегации каналов (LACP)  Программные методы:  Настройка приоритезации трафика (QoS)  Компрессия данных  Кэширование контента  Архитектурные подходы:  Сегментация сети (VLAN)  Использование CDN для веб-контента  Оптимальное размещение серверов |

| Билет 12 | |
| --- | --- |
| Вопрос 1  Выполнить настройку роли сервера БД MySQL + Adminer (Реализовать в контейнерах Docker) на Linux Server (В качестве ОС использовать Ubuntu Server). | Настройка MySQL и Adminer в Docker  Установка Docker  1.Обновите пакеты и установите зависимости:  sudo apt update  sudo apt install apt-transport-https ca-certificates curl software-properties-common  2.Добавьте официальный GPG-ключ Docker:  curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg  3.Добавьте репозиторий Docker:  echo "deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/ubuntu $(lsb\_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null  4.Установите Docker:  sudo apt update  sudo apt install docker-ce docker-ce-cli containerd.io  5.Проверьте установку:  sudo docker run hello-world  Запуск MySQL сервера в контейнере  sudo docker run --name mysql-server -d \  -e MYSQL\_ROOT\_PASSWORD=mysecretpassword \  -e MYSQL\_DATABASE=exampledb \  -e MYSQL\_USER=exampleuser \  -e MYSQL\_PASSWORD=examplepass \  -p 3306:3306 \  mysql:8.0  Запуск Adminer (веб-интерфейс для управления БД)  sudo docker run --name adminer -d \  -p 8080:8080 \  --link mysql-server:db \  adminer  Проверка работы:  1. MySQL доступен на localhost:3306  2. Adminer доступен в браузере: http://<IP\_сервера>:8080  Для входа используйте:  Система: MySQL  Сервер: db (или IP контейнера mysql-server)  Пользователь: exampleuser  Пароль: examplepass  База данных: exampledb |
| Вопрос 2  Проанализируйте работу нескольких устройств и постройте графики их показателей с помощью Zabbix. | Анализ работы устройств и построение графиков в Zabbix  Предварительные требования:  Убедитесь, что Zabbix сервер установлен и работает  Агенты Zabbix установлены на всех мониторируемых устройствах  1. Установка Zabbix сервера на Linux Server (Ubuntu)  Установка необходимых компонентов  sudo apt update  sudo apt upgrade -y  sudo apt install -y apache2 php php-mysql php-mbstring php-gd php-xml php-bcmath mariadb-server  Настройка базы данных  sudo mysql\_secure\_installation  # Следуйте инструкциям, установите пароль для root  sudo mysql -uroot -p  В MySQL выполните:  CREATE DATABASE zabbix CHARACTER SET utf8 COLLATE utf8\_bin;  CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'ваш\_пароль';  GRANT ALL PRIVILEGES ON zabbix.\* TO 'zabbix'@'localhost';  FLUSH PRIVILEGES;  EXIT;  Установка Zabbix  wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release\_6.0-4+ubuntu$(lsb\_release -rs)\_all.deb  sudo dpkg -i zabbix-release\_6.0-4+ubuntu$(lsb\_release -rs)\_all.deb  sudo apt update  sudo apt install -y zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent  Импорт начальной схемы  zcat /usr/share/doc/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -p zabbix  Настройка конфигурации  sudo nano /etc/zabbix/zabbix\_server.conf  Измените параметры:  DBHost=localhost  DBName=zabbix  DBUser=zabbix  DBPassword=ваш\_пароль  Запуск сервисов  sudo systemctl restart zabbix-server zabbix-agent apache2  sudo systemctl enable zabbix-server zabbix-agent apache2  Доступ к веб-интерфейсу  Откройте в браузере: http://<IP\_Linux\_Server>/zabbix  • Логин: Admin (с большой буквы)  • Пароль: zabbix  2. Установка Zabbix агента на Linux Server (тот же сервер)  Уже установлен вместе с сервером. Проверьте конфигурацию:  sudo nano /etc/zabbix/zabbix\_agentd.conf  Убедитесь, что есть:  Server=127.0.0.1  ServerActive=127.0.0.1  Hostname=Linux Server  3. Установка Zabbix агента на Windows 10 (VM 2)  1. Скачайте агент для Windows:  o Перейдите на https://www.zabbix.com/download\_agents  o Выберите версию, соответствующую вашей Windows (обычно Windows 64-bit)  o Скачайте архив (например, zabbix\_agent-6.0.15-windows-amd64-openssl.zip)  2. Установка:  o Распакуйте архив в C:\Program Files\Zabbix Agent  o Отредактируйте файл конфигурации C:\Program Files\Zabbix Agent\conf\zabbix\_agentd.conf:  Server=<IP\_Linux\_Server>  ServerActive=<IP\_Linux\_Server>  Hostname=Windows 10  o Откройте командную строку (как администратор) и выполните:  cd "C:\Program Files\Zabbix Agent\bin"  zabbix\_agentd.exe -c "C:\Program Files\Zabbix Agent\conf\zabbix\_agentd.conf" -i  zabbix\_agentd.exe -c "C:\Program Files\Zabbix Agent\conf\zabbix\_agentd.conf" -s  4. Настройка мониторинга устройств  Добавление устройств в мониторинг:  В веб-интерфейсе Zabbix: Configuration → Hosts  Для Linux Server:  Host name: Linux Server  Groups: Linux servers  IP address: <IP\_Linux\_Server>  Templates: Template OS Linux by Zabbix agent  Для Windows 10:  Host name: Windows 10  Groups: Windows servers  IP address: <IP\_Windows\_10>  Templates: Template OS Windows by Zabbix agent  Проверка сбора данных:  Monitoring → Latest data  Выберите нужный хост и проверьте собираемые метрики  Создание графиков  Графики для CPU:  Configuration → Hosts → выберите хост → Graphs → Create graph  Название: "CPU Usage"  Добавьте элементы:  system.cpu.util[,user]  system.cpu.util[,system]  system.cpu.util[,idle]  Графики для памяти:  Создайте новый график "Memory Usage"  Добавьте элементы:  vm.memory.size[total]  vm.memory.size[used]  vm.memory.size[free]  Графики для сети:  Создайте график "Network Traffic"  Добавьте элементы для сетевого интерфейса:  net.if.in[eth0]  net.if.out[eth0]  Создание комплексных дашбордов  Monitoring → Dashboards → Create dashboard  Добавьте виджеты:  Графические (выберите созданные графики)  Проблемы (для отображения текущих инцидентов)  Системная информация  Настройте расположение виджетов |
| Вопрос 3  Паспорт технических устройств. Ключевые компоненты паспорта технических устройств. | Паспорт технических устройств: ключевые компоненты  Основные разделы паспорта технического устройства  Общие сведения:  Наименование устройства  Производитель и модель  Серийный номер  Дата изготовления  Гарантийные обязательства  Технические характеристики:  Аппаратные параметры (CPU, RAM, HDD/SSD)  Сетевые интерфейсы (тип, скорость, MAC-адреса)  Потребляемая мощность  Физические размеры и вес  Программное обеспечение:  Установленная ОС и версия  Базовое ПО (если предусмотрено)  Драйверы и их версии  Поддерживаемые протоколы  Информация о подключении:  Схема подключения  IP-адреса (если есть)  Учетные данные для доступа (логины/пароли)  Порт подключения  Эксплуатационные параметры:  Рабочие температуры  Влажность эксплуатации  Рекомендуемые условия работы  Ресурс работы  Техническое обслуживание:  График ТО  Рекомендуемые процедуры обслуживания  Контакты сервисных центров  Безопасность:  Уровни защиты (IP, IK)  Сертификаты соответствия  Рекомендации по информационной безопасности  Пример паспорта для сервера  1. Общие сведения:  Наименование: Сервер Dell PowerEdge R750  Серийный номер: ABC123456789  Дата ввода в эксплуатацию: 15.03.2023  2. Технические характеристики:  Процессор: 2 x Intel Xeon Silver 4310 (12 ядер)  Память: 128 GB DDR4 ECC  Диски: 4 x 480GB SSD RAID 10  Сетевые интерфейсы: 4 x 1Gbps, 2 x 10Gbps  3. Программное обеспечение:  ОС: Ubuntu Server 22.04 LTS  Дополнительное ПО: Docker CE, Zabbix Agent  4. Сетевая информация:  Основной IP: 192.168.1.100  MAC-адрес: 00:1A:2B:3C:4D:5E  Доступ: SSH (порт 22), Web (порт 80, 443)  5. Эксплуатационные параметры:  Рабочая температура: +10°C до +35°C  Влажность: 20-80% без конденсации  6. Обслуживание:  Контакт сервиса: support@dell.com  Телефон: +1-800-999-9999  7. Безопасность:  Сертификаты: CE, FCC, UL  Рекомендации: Регулярное обновление ПО |

| Билет 13 | |
| --- | --- |
| Вопрос 1  Выполнить настройку Windows Server, установить и настроить роли службы каталогов Active Directory | [Выполнить настройку Windows Server, установить и настроить роли службы каталогов Active Directory.](#_sv8j2kgke70t) |
| Вопрос 2  Определить маску подсети, соответствующую указанному диапазону ip адресов: 119.38.0.1–119.38.255.254. | Определение маски подсети для диапазона IP-адресов 119.38.0.1 – 119.38.255.254  🔹 Шаг 1: Анализ диапазона  Начальный IP: 119.38.0.1  Конечный IP: 119.38.255.254  Количество адресов:  119.38.0.0 — адрес сети (не используется).  119.38.255.255 — широковещательный адрес (не используется).  Доступные адреса: 256 × 256 − 2 = 65 534 (что соответствует маске /16).  🔹 Шаг 2: Вычисление маски    🔹 Шаг 3: Верификация  Адрес сети: 119.38.0.0/16  Broadcast: 119.38.255.255  Доступные адреса: 119.38.0.1 – 119.38.255.254.  Вывод: Маска 255.255.0.0 (/16) корректно покрывает указанный диапазон. |
| Вопрос 3  Классификация регламентов технических осмотров. | [Классификация регламентов технических осмотров.](#_3e2k50ge4k05) |

| Билет 14 | |
| --- | --- |
| Вопрос 1  Выполнить настройку Квот и файлового экранирования в FSRM на Windows Server. | [Выполнить настройку Квот и файлового экранирования в FSRM на Windows Server.](#_y43g153s4oql) |
| Вопрос 2  Разбить на 10 подсетей блок адресов 192.168.1.0/25. Указать первый и последний IP-адрес в подсети. |  |
| Вопрос 3  Технические осмотры объектов сетевой инфраструктуры. | [Технические осмотры объектов сетевой инфраструктуры.](#_sv8j2kgke70t) |

| Билет 15 | |
| --- | --- |
| Вопрос 1  Выполнить настройку правил в редакторе групповых политик на Windows Server и отключить командную строку, PowerShell и запретить редактирование служб реестра. | Настройка групповых политик для ограничения доступа к CMD, PowerShell и реестру  🔹 Шаг 1: Открытие редактора групповых политик (GPO)  На Windows Server откройте «Group Policy Management» (gpmc.msc).  Создайте новую политику или отредактируйте существующую:  ПКМ на «Group Policy Objects» → «New».  Назовите политику (например, «Restrict\_System\_Tools»).  Нажмите ПКМ на политику → «Edit».  🔹 Шаг 2: Отключение командной строки (CMD)  Перейдите по пути:  Конфигурация пользователя → Политики → Административные шаблоны → Система  Найдите параметр «Запретить использование командной строки».  Включите его и выберите:  «Да» (запрет всех сценариев, включая CMD и BAT-файлы).  «Показывать сообщение» (например, "Доступ запрещен администратором").  🔹 Шаг 3: Отключение PowerShell  В том же разделе (Система) найдите:  «Запуск только указанных приложений Windows».  Включите политику и добавьте в список разрешенных программ (например, notepad.exe, explorer.exe).  Важно: Не добавляйте powershell.exe и pwsh.exe — это запретит их запуск.  🔹 Шаг 4: Запрет редактирования реестра  Перейдите по пути:  Конфигурация пользователя → Политики → Административные шаблоны → Система  Найдите параметр «Запретить доступ к средствам редактирования реестра».  Включите его → «Да».  🔹 Шаг 5: Дополнительные ограничения (опционально)  Запрет диспетчера задач:  В разделе Система → «Ctrl+Alt+Del Options» → «Remove Task Manager».  Блокировка MMC:  «Ограничить доступ к консоли MMC» → Включить.  🔹 Шаг 6: Применение политики  Свяжите GPO с нужным подразделением (OU):  Перетащите политику на OU в Group Policy Management.  Обновите политики на клиентах:  powershell  gpupdate /force  🔹 Проверка работы  На клиенте:  Попробуйте открыть CMD или PowerShell → должно появиться сообщение о запрете.  Попытка запустить regedit → доступ будет заблокирован. |
| Вопрос 2  Определить количество и диапазон ip адресов подсети, если номер подсети - 26.219.128.168, маска подсети – 255.255.255.128. | [Определить количество и диапазон ip адресов подсети, если номер подсети - 26.219.128.168, маска подсети – 255.255.255.128.](#_d47oj2fn107l) |
| Вопрос 3  Протокол SNMP. Набор услуг. Общие характеристики | Протокол SNMP: набор услуг и общие характеристики  1. Определение и назначение  SNMP (Simple Network Management Protocol) — это стандартный протокол прикладного уровня (UDP-порт 161/162), предназначенный для управления и мониторинга сетевых устройств (маршрутизаторы, коммутаторы, серверы, принтеры, IoT-устройства).  Основные задачи:  Сбор статистики (загрузка CPU, трафик, ошибки).  Удаленное управление конфигурацией.  Оповещение о критических событиях (траппы).        3.2. Community-строки  public — только чтение (мониторинг).  private — чтение и запись (управление).  В SNMPv3: Используются логины/пароли с ролями (noAuthNoPriv, authNoPriv, authPriv).  3.3. Портовая система  UDP 161 — запросы от менеджера к агенту.  UDP 162 — trap-сообщения от агента к менеджеру.  4. Примеры использования  4.1. Запрос имени устройства через SNMPv2c  bash  snmpget -v 2c -c public 192.168.1.1 1.3.6.1.2.1.1.5.0  Вывод:  SNMPv2-MIB::sysName.0 = STRING: Router1  4.2. Настройка trap-оповещений  На агенте (Cisco Router):  cisco  snmp-server host 192.168.1.100 traps public  snmp-server enable traps cpu threshold  На менеджере (Zabbix):  Настройка триггера на прием trap IF-MIB::linkDown.  5. Безопасность SNMP  Риски:  Перехват community-строк (особенно в v1/v2c).  DoS-атаки через флуд запросами.  Утечка конфигурации устройств.  Рекомендации:  Используйте SNMPv3 с шифрованием.  Ограничьте доступ по IP (snmp-server community private RO 192.168.1.0/24).  Запретите SNMP на внешних интерфейсах.  6. Интеграция с системами мониторинга  Zabbix/PRTG: Автоматический сбор данных через SNMP-шаблоны.  Prometheus: Используйте snmp\_exporter для конвертации OID в метрики.  ✅ Итог  SNMP — ключевой протокол для мониторинга сетевых устройств.  Основные услуги: GET/SET, TRAP, MIB/OID.  Безопасность: SNMPv3 предпочтительнее v2c/v1.  Использование: От мониторинга нагрузки до управления конфигурацией. |

| Билет 16 | |
| --- | --- |
| Вопрос 1  Выполнить настройку правил в редакторе групповых политик на Windows Server и отключить доступ к Корзине, доступ к Диспетчеру Задач и запретить добавление файлов на Рабочий Стол. | Настройка групповых политик для ограничения доступа к Корзине, Диспетчеру задач и Рабочему столу  🔹 Шаг 1: Открытие редактора групповых политик (GPO)  На Windows Server откройте «Group Policy Management» (gpmc.msc).  Создайте новую политику или отредактируйте существующую:  ПКМ на «Group Policy Objects» → «New».  Назовите политику (например, «Restrict\_User\_Access»).  Нажмите ПКМ на политику → «Edit».  🔹 Шаг 2: Отключение доступа к Корзине  Перейдите по пути:  Конфигурация пользователя → Политики → Административные шаблоны → Рабочий стол  Найдите параметр «Удалить значок "Корзина" с рабочего стола».  Включите его → «Enabled».  Примечание: Это скроет значок, но не удалит саму Корзину.  🔹 Шаг 3: Запрет доступа к Диспетчеру задач  Перейдите по пути:  Конфигурация пользователя → Политики → Административные шаблоны → Система → Варианты действий после нажатия Ctrl+Alt+Del  Найдите параметр «Удалить диспетчер задач».  Включите его → «Enabled».  Проверка: Попытка открыть Диспетчер задач (Ctrl+Shift+Esc) выдаст ошибку.  🔹 Шаг 4: Запрет добавления файлов на Рабочий стол  Перейдите по пути:  Конфигурация пользователя → Политики → Административные шаблоны → Рабочий стол  Найдите параметр «Запретить сохранение изменений на рабочем столе».  Включите его → «Enabled».  Эффект: Пользователи не смогут создавать/копировать файлы на Рабочий стол.  🔹 Шаг 5: Дополнительные ограничения (опционально)  Скрытие всех значков рабочего стола:  В том же разделе включите «Скрыть и отключить все элементы на рабочем столе».  Блокировка контекстного меню:  Конфигурация пользователя → Политики → Административные шаблоны → Рабочий стол → Контекстное меню → «Запретить доступ к контекстному меню».  🔹 Шаг 6: Применение политики  Свяжите GPO с нужным подразделением (OU):  Перетащите политику на OU в Group Policy Management.  Обновите политики на клиентах:  powershell  gpupdate /force  🔹 Проверка работы  На клиенте:  Попытка открыть Корзину → значок исчезнет.  Запуск Диспетчера задач → ошибка "Администратор отключил Диспетчер задач".  Копирование файла на Рабочий стол → действие заблокировано. |
| Вопрос 2  Определить находятся ли два узла А и В в одной подсети, если адреса компьютеров А и В 26.219.123.6 и 26.218.102.31. Маска подсети 255.255.192.0 | [Определить находятся ли два узла А и В в одной подсети, если адреса компьютеров А и В 26.219.123.6 и 26.218.102.31. Маска подсети 255.255.192.0](#_7ooz9u94r6uj) |
| Вопрос 3  Виды оборудования для диагностики и сертификации кабельных систем. Общие характеристики. | Виды оборудования для диагностики и сертификации кабельных систем  1. Кабельные тестеры (базовая диагностика)  Назначение: Проверка целостности кабеля, обрывов, коротких замыканий и перекрестов.  Характеристики:  Типы кабелей: Витая пара (UTP/FTP), коаксиал, телефонные линии.  Функции:  Проверка правильности обжима (прямой/кроссовер).  Определение длины кабеля (TDR-анализ).  Поиск повреждений с точностью до 1–3 метров.  Примеры:  Fluke MicroScanner — проверка целостности и карта разводки.  \*Klein Tools VDV501-852\* — тестирование RJ45/RJ11.  2. Анализаторы целостности (Certifiers)  Назначение: Сертификация кабеля по стандартам (TIA/EIA-568, ISO/IEC 11801).  Характеристики:  Измеряемые параметры:  Затухание (Insertion Loss).  NEXT (Near-End Crosstalk).  Возвратные потери (Return Loss).  Задержка распространения (Propagation Delay).  Стандарты: Cat5e, Cat6, Cat6a, Cat7.  Примеры:  \*Fluke DSX-8000\* — сертификация до Cat8.  VIAVI CertiFiber Pro — для оптических кабелей.  3. TDR-анализаторы (Time Domain Reflectometers)  Назначение: Точное определение места обрыва/короткого замыкания.  Характеристики:  Принцип работы: Отправка импульса и анализ отраженного сигнала.  Точность: До 10 см.  Примеры:  \*Fluke LinkRunner AT-2000\* — для медных кабелей.  AEM TestPro CV100 — TDR + проверка целостности.  4. OTDR-анализаторы (для оптики)  Назначение: Диагностика волоконно-оптических линий (ВОЛС).  Характеристики:  Измеряемые параметры:  Потери на стыках/разъемах.  Длина сегмента.  Место обрыва.  Дальность: До 150 км.  Примеры:  \*EXFO FTB-200\* — компактный OTDR.  \*VIAVI OTDR MTS-6000\* — профессиональный анализ.  5. Анализаторы передачи (Network Analyzers)  Назначение: Тестирование пропускной способности и качества сигнала.  Характеристики:  Поддержка протоколов: Ethernet (10/100/1000 Mbps), PoE.  Функции:  Аналитр пакетов (Packet Loss, Jitter).  Тестирование PoE (напряжение, мощность).  Примеры:  Fluke Networks EtherScope — анализ LAN/Wi-Fi.  NetAlly AirCheck G2 — для беспроводных и проводных сетей.  6. Мультиметры и тональные генераторы  Назначение: Поиск кабелей в пучке, проверка напряжения.  Характеристики:  Тональные генераторы:  Генерация сигнала для трассировки (например, Fluke Pro3000).  Мультиметры:  Измерение напряжения, сопротивления (например, Klein Tools MM700).  7. Тепловизоры и микроскопы (для оптики)  Назначение:  Тепловизоры: Поиск перегрева контактов.  Микроскопы: Проверка чистоты/повреждений феррулов оптических разъемов.  Примеры:  Fluke Ti480 — тепловизор для ЦОД.  VIAVI FiberChek Probe — микроскоп для ВОЛС.  Критерии выбора оборудования  Тип кабеля (медь/оптика).  Требуемая точность (для сертификации — анализаторы, для поиска обрывов — TDR).  Бюджет (тестеры дешевле, OTDR — дорого).  Важно: Для соответствия стандартам (например, Cat6a) используйте сертификационные анализаторы. Для повседневного ремонта достаточно TDR/тестеров. |

| Билет 17 | |
| --- | --- |
| Вопрос 1  Выполнить развёртывание BitLocker на Windows Server. | Развертывание BitLocker на Windows Server  Цель: Включить шифрование дисков BitLocker на Windows Server для защиты данных.  ОС: Windows Server (2016/2019/2022)  Примечание:  - BitLocker требует TPM (Trusted Platform Module) версии 1.2 или выше (рекомендуется 2.0).  - Если TPM отсутствует, можно использовать USB-ключ или пароль (менее безопасно).  - Для работы BitLocker на сервере должна быть установлена роль BitLocker Drive Encryption (если используется Windows Server без GUI, потребуется доустановка компонентов).  Шаг 1: Проверка поддержки TPM  1. Откройте диспетчер устройств (`devmgmt.msc`).  2. Разверните раздел "Устройства безопасности".  - Если есть "Доверенный платформенный модуль" (TPM) версии 1.2/2.0 – можно использовать его.  - Если TPM нет, BitLocker можно настроить через групповую политику (см. Шаг 3).  Шаг 2: Установка компонента BitLocker (если не установлен)  1. Откройте "Диспетчер серверов" → "Добавить роли и компоненты".  2. Перейдите в "Компоненты" → "Функции".  3. Найдите и отметьте:  - "Шифрование диска BitLocker" (основной компонент).  - "Инструменты управления BitLocker" (для PowerShell/GUI).  4. Завершите установку.  Шаг 3: Настройка групповой политики (если нет TPM)  Если TPM отсутствует, нужно разрешить BitLocker работать без него:  1. Откройте `gpedit.msc` (локальная политика) или групповую политику домена.  2. Перейдите:  ```  Конфигурация компьютера → Административные шаблоны → Компоненты Windows → Шифрование диска BitLocker → Диски операционной системы  ```  3. Включите политику:  - "Этот параметр политики позволяет настроить требование дополнительной проверки подлинности при запуске".  - Выберите "Разрешить BitLocker без совместимого TPM" → "Требовать пароль" или "Требовать USB-устройство".  Шаг 4: Включение BitLocker через графический интерфейс  1. Откройте "Панель управления" → "BitLocker Drive Encryption".  2. Выберите диск (системный или дополнительный) → "Включить BitLocker".  3. Выберите метод разблокировки:  - Использовать TPM (если есть).  - Ввести пароль (если нет TPM).  - Сохранить ключ восстановления (обязательно! В файл/печать/USB).  4. Выберите режим шифрования:  - "Новый режим шифрования" (XTS-AES 256-bit, лучше для SSD/NVMe).  - "Совместимый режим" (AES-CBC 128/256-bit, для старых систем).  5. Запустите процесс шифрования (может занять время).  Шаг 5: Включение BitLocker через PowerShell (альтернатива)  ```powershell  # Проверить статус BitLocker  Manage-bde -status  # Включить BitLocker на диске C: с TPM + паролем  Enable-BitLocker -MountPoint "C:" -EncryptionMethod XtsAes256 -UsedSpaceOnly -Password (ConvertTo-SecureString "ВашПароль" -AsPlainText -Force) -PasswordProtector  # Добавить ключ восстановления (сохранить в файл)  $RecoveryKeyPath = "C:\BitLocker\_Recovery\_Key.txt"  Manage-bde -protectors -add C: -RecoveryPassword | Out-File -FilePath $RecoveryKeyPath  # Принудительно завершить шифрование (если зависло)  Resume-BitLocker -MountPoint "C:"  ```  Шаг 6: Проверка работы BitLocker  1. Перезагрузите сервер.  2. Если настроен TPM – диск разблокируется автоматически.  3. Если установлен пароль/USB – система запросит его при загрузке.  4. Проверить статус можно командой:  ```powershell  Manage-bde -status C:  ```  или через "Управление BitLocker" в панели управления.  Дополнительные рекомендации  - Резервное копирование ключа восстановления – критически важно!  - Шифрование только используемого пространства (`-UsedSpaceOnly`) быстрее, но менее безопасно.  - BitLocker + гибернация – если сервер использует гибернацию, убедитесь, что файл `hiberfil.sys` тоже зашифрован. |
| Вопрос 2  Постройте топологию сети с помощью Zabbix. | Построение топологии сети в Zabbix  Цель: Визуализировать сетевую инфраструктуру (включая две ВМ: Windows Server и Windows 10) с помощью Zabbix для мониторинга связей и состояния узлов.  Шаг 1: Подготовка Zabbix  1. Установите Zabbix Server (если ещё не установлен):  - На отдельной ВМ или сервере разверните Zabbix (подойдёт Zabbix 6.0 LTS).  - Используйте официальную инструкцию для вашей ОС: [Zabbix Installation Guide](https://www.zabbix.com/download).  2. Добавьте узлы в мониторинг:  - Windows Server и Windows 10 должны быть добавлены как хосты в Zabbix.  - Установите Zabbix Agent на обе ВМ:  - Для Windows: скачайте агент с [официального сайта](https://www.zabbix.com/download\_agents).  - Настройте `zabbix\_agentd.conf`:  ```ini  Server=IP\_Zabbix\_Server  ServerActive=IP\_Zabbix\_Server  Hostname=Windows\_Server (или Win10)  ```  - Перезапустите службу:  ```powershell  Restart-Service ZabbixAgent  ```  Шаг 2: Обнаружение сети  1. Настройка Network Discovery:  - В веб-интерфейсе Zabbix перейдите:  Configuration → Discovery → Create discovery rule.  - Укажите диапазон IP-адресов вашей сети (например, `192.168.1.1-254`).  - Выберите проверку доступности через ICMP ping или Zabbix agent.  2. Автоматическое добавление хостов:  - В разделе "Actions" настройте автоматическое добавление обнаруженных узлов:  - Event source: "Discovery"  - Action: "Add host", "Link template" (например, `Template OS Windows`).  Шаг 3: Настройка карты сети (Network Map)  1. Создание карты:  - Перейдите: Monitoring → Maps → Create map.  - Нажмите "Add" → "Host" и выберите ваши ВМ (Windows Server и Win10).  2. Добавление связей:  - Используйте инструмент "Link", чтобы соединить узлы (например, если они в одной подсети).  - Для автоматического отображения связей включите "Automatic map creation" на основе данных LLDP/CDP (если оборудование поддерживает).  3. Пример ручной настройки:  - Добавьте роутер (если есть) и соедините его с обеими ВМ.  - Настройте иконки (например, серверная иконка для Windows Server, ПК для Win10).  Шаг 4: Использование Zabbix Low-Level Discovery (LLD) для автоматизации  1. Настройка LLD для сетевых интерфейсов:  - Zabbix автоматически обнаружит сетевые интерфейсы хостов с помощью шаблона `Template Net Network Interfaces Generic`.  - Проверьте данные в Monitoring → Latest data для каждого хоста.  2. Добавление триггеров:  - Например, триггер на недоступность интерфейса:    ```plaintext  {Template Net Network Interfaces Generic:net.if.status[ifAlias].last()} = 0  ```  Шаг 5: Проверка и доработка  1. Убедитесь, что все узлы отображаются корректно:  - Проблемные узлы подсвечиваются красным.  - Связи отображают реальную физическую топологию.  2. Если узлы не отображаются:  - Проверьте настройки firewall (разрешите ICMP/Zabbix-трафик).  - Убедитесь, что Zabbix Agent запущен и отвечает.  Итоговая топология в Zabbix  - Windows Server и Windows 10 отображаются как узлы.  - Связи между ними показаны (если есть прямое взаимодействие).  - Возможные проблемы (например, обрыв связи) визуализируются на карте. |
| Вопрос 3  Определение Регулярного резервирования. Организация удалённого оповещения о неполадках. | Определение регулярного резервирования  Регулярное резервирование (Backup) — это процесс периодического автоматического копирования данных, конфигураций или состояния системы для их восстановления в случае сбоев, потерь или атак.  # Ключевые характеристики:  1. Автоматизация – резервирование выполняется по расписанию (ежедневно, еженедельно и т. д.).  2. Полные/инкрементные/дифференциальные копии – в зависимости от стратегии.  3. Хранение в нескольких местах – локально + облако/удалённый сервер (правило 3-2-1).  4. Проверка целостности – тестовые восстановления для гарантии работоспособности.  Организация удалённого оповещения о неполадках  Для мониторинга резервных копий и оперативного реагирования на сбои используются системы оповещения.  # Способы настройки оповещений:  1. Встроенные средства резервного ПО  - Veeam, Acronis, Bacula поддерживают email/SMS-уведомления.  - Пример настройки в Veeam:    ```plaintext  Настройки → Уведомления → Добавить SMTP-сервер → Указать email админа.  ```  2. Интеграция с Zabbix/Prometheus  - Мониторинг статуса задач резервирования через API/скрипты.  - Триггеры для оповещения:    ```plaintext  {Backup\_Job:status.last()} = "Failed" → Отправка в Telegram/Slack.  ```  3. Скрипты и планировщики  - Windows (Powershell):  ```powershell  $LastBackup = Get-Date -Date (Get-ChildItem "D:\Backups\\*" | Sort LastWriteTime | Select -Last 1).LastWriteTime  if ((New-TimeSpan -Start $LastBackup -End (Get-Date)).TotalHours -gt 24 {  Send-MailMessage -From "backup@domain.com" -To "admin@domain.com" -Subject "Backup FAILED" -Body "Последняя копия старше 24 часов!" -SmtpServer "smtp.domain.com"  }  ```  - Linux (Bash + Cron):    ```bash  #!/bin/bash  if [ ! -f "/backups/last\_backup\_$(date +%Y-%m-%d).tar.gz" ]; then  curl -X POST -H 'Content-Type: application/json' -d '{"text":"Backup failed!"}' https://hooks.slack.com/services/XXX  fi  ```  4. Облачные сервисы (AWS SNS, Azure Alerts)  - Настройка правил в AWS CloudWatch или Azure Monitor для событий резервирования.  Пример готового решения  Для Windows Server + Zabbix:  1. Настройте резервное копирование в Windows Server Backup.  2. Добавьте проверку в Zabbix через UserParameter:  ```ini  UserParameter=backup.check, powershell -command "if ((Get-WBSummary).LastBackupResultHR -eq 0) { echo 1 } else { echo 0 }"  ```  3. Создайте триггер:    ```plaintext  {backup.check.last()} = 0 → Оповещение в Telegram через webhook.  ```  Критерии эффективного оповещения  - Мгновенность – уведомления при первых признаках проблемы.  - Мультиканальность – email + мессенджеры (Telegram, MS Teams).  - Минимизация ложных срабатываний – фильтрация по уровню критичности. |

| Билет 18 | |
| --- | --- |
| Вопрос 1  Выполнить настройку DNS и DHCP на Windows Server. | Настройка DNS и DHCP на Windows Server  Цель:  Развернуть DNS-сервер для разрешения имён в локальной сети.  Настроить DHCP-сервер для автоматической раздачи IP-адресов клиентам (например, Windows 10).  Используемая ОС: Windows Server 2016/2019/2022.  Часть 1: Установка и настройка DNS-сервера  Шаг 1: Установка роли DNS-сервера  Откройте Диспетчер серверов → "Добавить роли и компоненты".  Выберите "Установка ролей или компонентов" → Далее.  Выберите сервер → Отметьте "DNS-сервер".  Завершите установку (перезагрузка не требуется).  Шаг 2: Настройка зоны DNS  Откройте DNS-менеджер (dnsmgmt.msc).  Создайте прямую зону (Forward Lookup Zone):  ПКМ по "Прямые зоны просмотра" → "Создать зону".  Выберите "Основная зона" → Укажите имя (например, localdomain).  Сохраните зону в файл → Настройте "Разрешить динамические обновления" (если нужно).  Добавьте A-запись (соответствие имени и IP):  ПКМ по зоне → "Создать узел (A или AAAA)".  Введите имя (например, win10-pc) и IP-адрес (например, 192.168.1.100).  (Опционально) Настройте обратную зону (Reverse Lookup Zone):  ПКМ по "Обратные зоны" → "Создать зону" → Укажите сеть (например, 192.168.1.0/24).  Часть 2: Установка и настройка DHCP-сервера  Шаг 1: Установка роли DHCP-сервера  В Диспетчере серверов → "Добавить роли и компоненты".  Выберите "DHCP-сервер" → Установите.  После установки завершите настройку DHCP (в уведомлении).  Шаг 2: Настройка DHCP-пула  Откройте DHCP-менеджер (dhcpmgmt.msc).  Создайте новый пул адресов:  ПКМ по IPv4 → "Создать область".  Укажите:  Имя (например, LAN\_Pool).  Диапазон IP (например, 192.168.1.100-192.168.1.200).  Маска подсети (255.255.255.0).  Шлюз по умолчанию (например, 192.168.1.1).  DNS-сервер (укажите IP этого сервера, например, 192.168.1.2).  Срок аренды (по умолчанию 8 дней).  Активируйте область → "Да".  Шаг 3: Резервация IP (опционально)  Если нужно закрепить IP за устройством (например, для сервера):  В DHCP-менеджере → "Резервирования адресов".  ПКМ → "Создать резервирование".  Введите:  MAC-адрес устройства (например, с ipconfig /all на Windows 10).  Желаемый IP (например, 192.168.1.50).  Часть 3: Проверка работы DNS и DHCP  Проверка DHCP (на клиенте Windows 10)  Откройте командную строку → Выполните:  bash  ipconfig /release && ipconfig /renew  Убедитесь, что клиент получил IP из диапазона DHCP:  bash  ipconfig /all  Проверка DNS (на клиенте Windows 10)  Попробуйте пропинговать имя хоста, созданное в DNS:  bash  ping win10-pc.localdomain  Должен отобразиться IP, указанный в A-записи.  Часть 4: Дополнительные настройки  Интеграция DNS и DHCP  Чтобы DHCP автоматически регистрировал имена клиентов в DNS:  В DHCP-менеджере → "Свойства IPv4" → вкладка "DNS".  Отметьте:  "Всегда обновлять записи DNS".  "Включать имена клиентов в DNS".  Настройка политик DHCP (если нужно)  Можно создать разные пулы для VLAN или устройств.  Возможные проблемы и решения  Проблема Решение  Клиент не получает IP - Проверьте, что служба DHCP запущена, а firewall разрешает UDP-порты 67/68.  DNS-запросы не разрешаются - Убедитесь, что в настройках DHCP указан правильный DNS-сервер.  Ошибка "Нет доступных серверов DHCP" - Проверьте, что сервер авторизован в Active Directory (если используется). |
| Вопрос 2  Проанализируйте работу сервера и выведите графики загруженности за разный период времени. | Анализ загруженности сервера и построение графиков  Для мониторинга производительности Windows Server и визуализации данных используются:  Встроенные средства (Performance Monitor, Task Manager) – для быстрой проверки.  Zabbix/Prometheus + Grafana – для детализированных отчётов.  PowerShell-скрипты – для автоматизации сбора данных.  Способ 1: Performance Monitor (PerfMon) – встроенный инструмент Windows  Шаг 1: Сбор данных  Откройте Performance Monitor (perfmon.msc).  Перейдите в Data Collector Sets → User Defined → Создать новый набор.  Добавьте счётчики для мониторинга:  CPU: Processor(\_Total)\% Processor Time  Память: Memory\% Committed Bytes in Use  Диск: LogicalDisk(C:)\Disk Read/Write Bytes/sec  Сеть: Network Interface(\*)\Bytes Total/sec  Настройте временной интервал (например, каждые 5 сек.) и сохраните данные в .blg-файл.  Шаг 2: Визуализация  В Performance Monitor откройте вкладку "Graph".  Загрузите сохранённые данные через "View Log Data".  Постройте графики за нужный период:  Краткосрочный анализ (часы/дни) – динамика в реальном времени.  Долгосрочный (недели/месяцы) – тренды нагрузки.  Пример графика (CPU и память):  Performance Monitor Graph  Способ 2: Zabbix + Grafana – профессиональный мониторинг  Шаг 1: Настройка Zabbix  Убедитесь, что Zabbix Agent установлен на сервере и отправляет данные.  Добавьте шаблоны для Windows:  Template OS Windows by Zabbix agent (CPU, память, диск).  Template App IIS (если используется веб-сервер).  Проверьте собранные данные в Monitoring → Latest Data.  Шаг 2: Визуализация в Grafana  Импортируйте готовый дашборд (например, Windows Server Dashboard).  Настройте фильтры по времени:  Последние 24 часа – для оперативного анализа.  Неделя/месяц – для выявления аномалий.  Пример дашборда:  Grafana Dashboard  Способ 3: PowerShell + CSV/Excel – для отчётов  Шаг 1: Сбор данных скриптом  powershell  # Запись метрик в CSV каждые 5 минут (запускать в планировщике)  $Metrics = @{  Timestamp = Get-Date -Format "yyyy-MM-dd HH:mm:ss"  CPU = (Get-Counter '\Processor(\_Total)\% Processor Time').CounterSamples.CookedValue  Memory = (Get-Counter '\Memory\% Committed Bytes in Use').CounterSamples.CookedValue  Disk = (Get-Counter '\LogicalDisk(C:)\% Disk Time').CounterSamples.CookedValue  }  $Metrics | Export-Csv -Path "C:\Server\_Metrics.csv" -Append -NoTypeInformation  Шаг 2: Построение графиков в Excel  Откройте CSV в Excel → выделите данные.  Вставьте график ("Вставка" → "График").  Настройте оси:  X: Временная шкала.  Y: Значения CPU, памяти, диска.  .  Рекомендации  Для краткосрочного анализа используйте PerfMon.  Для долгосрочного – Zabbix + Grafana.  Для ад-hoc отчётов – PowerShell + Excel. |
| Вопрос 3  Обслуживание физических компонентов. Контроль состояния аппаратного обеспечения. | Методы контроля состояния  🔹 1. Встроенные средства Windows  Монитор ресурсов (resmon) – проверка CPU, RAM, диска, сети.  Журналы событий (eventvwr.msc) – фильтр по HardwareEvents.  PowerShell:  powershell  # Проверка дисков (S.M.A.R.T.)  Get-PhysicalDisk | Select FriendlyName, HealthStatus, OperationalStatus  # Проверка температуры (требует сторонних модулей, например, OpenHardwareMonitor)  Invoke-WebRequest -Uri "http://localhost:8085/data.json" | ConvertFrom-Json | Select -ExpandProperty Children | Where Name -eq "Temperature"  🔹 2. Сторонние утилиты  CPU/GPU/RAM:  HWMonitor – мониторинг температур и напряжений.  Core Temp – контроль нагрева процессора.  Диски:  CrystalDiskInfo – проверка S.M.A.R.T. для HDD/SSD.  smartctl (Linux/macOS) – детальная диагностика:  bash  sudo smartctl -a /dev/sda  Сеть:  iperf3 – тест пропускной способности.  🔹3. Профилактическое обслуживание  🔧 1. Чистка от пыли  Раз в 3–6 месяцев (в зависимости от запылённости):   * Отключите сервер от питания. * Сжатым воздухом очистите: * Вентиляторы, * Радиаторы CPU, * Блок питания.   🔧 2. Проверка соединений  Плотность установки компонентов:   * Оперативная память, * Кабели дисков (SATA/SAS), * Разъёмы питания.   🔧 3. Замена термопасты  Раз в 2–3 года (для CPU/GPU):   * Снимите кулер, * Удалите старую пасту, * Нанесите тонкий слой новой (например, Arctic MX-4).   🔧 4. Ротация дисков (если используется RAID)  Раз в год проверяйте состояние дисков в RAID-массиве.  🔹4. Автоматизация мониторинга  📊 1. Zabbix/Prometheus + Grafana  Настройте дашборды для отслеживания:   * Температур (IPMI), * Ошибок дисков (smartctl), * Нагрузки на сеть. |

| Билет 19 | |
| --- | --- |
| Вопрос 1  Выполнить настройку Политики паролей и Политики блокировки учётных записей на Windows Server. | Настройка политики паролей и блокировки учетных записей на Windows Server  Цель:  Обеспечить безопасность учетных записей с помощью политики сложных паролей.  Защититься от перебора паролей через политику блокировки учетных записей.  Используемые инструменты:  Локальная политика безопасности (secpol.msc) – для standalone-серверов.  Групповая политика (GPO) – для доменных контроллеров (gpmc.msc).  🔐 Часть 1: Настройка политики паролей  🔹 Способ 1: Через "Локальную политику безопасности" (для локального сервера)  Откройте secpol.msc (Local Security Policy).  Перейдите:  Параметры безопасности → Политика учетных записей → Политика паролей  Настройте параметры:    Сложность пароля означает:   * Нельзя использовать имя пользователя. * Должны быть цифры, буквы (A-Z, a-z), спецсимволы (!@#$%^&\*).   Нажмите Применить.  🔹 Способ 2: Через GPO (для Active Directory)  Откройте gpmc.msc (Group Policy Management).  Создайте новую политику (например, "Password Policy GPO") или редактируйте Default Domain Policy.  Перейдите:  Конфигурация компьютера → Политики → Параметры Windows → Параметры безопасности → Политика учетных записей → Политика паролей  Настройте аналогичные параметры, как в Локальной политике.  Обновите политику на клиентах:  powershell  gpupdate /force  🔒 Часть 2: Настройка политики блокировки учетных записей  🔹 Способ 1: Через "Локальную политику безопасности"  Откройте secpol.msc.  Перейдите:  Параметры безопасности → Политика учетных записей → Политика блокировки учетных записей  Настройте параметры:  Параметр Рекомендуемое значение  Порог блокировки учетной записи 5 неверных попыток входа  Сброс счетчика блокировки через 30 минут  Длительность блокировки учетной записи 30 минут (или "Навсегда" до разблокировки админом)  Нажмите Применить.  🔹 Способ 2: Через GPO (для Active Directory)  Откройте gpmc.msc.  Перейдите в "Политика блокировки учетных записей" (как в Части 1).  Настройте те же параметры.  Обновите политику:  powershell  gpupdate /force  🔍 Часть 3: Проверка работы политик  1. Проверка политики паролей  Попробуйте сменить пароль пользователя на слишком простой (например, 12345).  Должна появиться ошибка:  "Пароль не соответствует требованиям сложности".  2. Проверка блокировки учетной записи  Попробуйте ввести неверный пароль 5 раз (если порог = 5).  Учетная запись заблокируется (проверить можно командой):  powershell  net accounts  Вывод должен содержать:  Порог блокировки: 5  Длительность блокировки: 30 минут  3. Разблокировка учетной записи (если нужно)  Через lusrmgr.msc (Локальные пользователи):  ПКМ на пользователе → Свойства → Снять галочку "Заблокировать учетную запись".  Через PowerShell:  powershell  Unlock-ADAccount -Identity "Username" # Для AD |
| Вопрос 2  Определить количество и диапазон ip адресов подсети, если номер подсети - 26.219.128.168, маска подсети – 255.255.255.128. | Определение количества и диапазона IP-адресов в подсети  Дано:  IP-адрес подсети: 26.219.128.168  Маска подсети: 255.255.255.128  🔹 Шаг 1: Определение типа маски  Маска 255.255.255.128 в CIDR-формате (префиксная запись):  Переводим каждый октет маски в двоичный вид:  255.255.255.128 = 11111111.11111111.11111111.10000000  Считаем количество единиц: /25 (25 бит занято под сеть).  🔹 Шаг 2: Расчёт количества хостов  Формула для подсчёта доступных IP:  Количество хостов = 2^(32 - префикс) - 2  Для /25:  2^(32-25) - 2 = 2^7 - 2 = 128 - 2 = 126 хостов  (Минус 2 — это адрес сети и широковещательный адрес.)  🔹 Шаг 3: Определение адреса сети и широковещательного адреса  Переводим IP и маску в двоичный вид:  IP: 26.219.128.168 → 00011010.11011011.10000000.10101000  Маска: 255.255.255.128 → 11111111.11111111.11111111.10000000  Вычисляем адрес сети (AND-операция):  00011010.11011011.10000000.10101000 (IP)  AND  11111111.11111111.11111111.10000000 (Маска)  -----------------------------------  00011010.11011011.10000000.10000000 → 26.219.128.128  Адрес сети: 26.219.128.128  Широковещательный адрес (Broadcast):  Инвертируем маску: 00000000.00000000.00000000.01111111  Применяем OR к адресу сети:  26.219.128.128 | 0.0.0.127 = 26.219.128.255  Broadcast: 26.219.128.255  🔹 Шаг 4: Определение диапазона IP-адресов  Начальный IP (первый доступный): 26.219.128.129  Конечный IP (последний доступный): 26.219.128.254  Диапазон хостов: 26.219.128.129 – 26.219.128.254 |
| Вопрос 3  Определение Масштабируемости сети. Какие ключевые аспекты Масштабируемости вы знаете. | Определение масштабируемости сети  Масштабируемость сети — это её способность эффективно расширяться (увеличивать количество узлов, трафик, сервисы) без значительного снижения производительности или увеличения сложности управления.  🔹 Ключевые аспекты масштабируемости  1. Горизонтальная vs Вертикальная масштабируемость    Что лучше?  Горизонтальная масштабируемость предпочтительна для облачных и распределённых систем (например, микросервисы).  Вертикальная имеет ограничения (максимальная мощность железа) и требует простоя.  2. Модульность и стандартизация  Использование стандартных протоколов (TCP/IP, HTTP, BGP) для совместимости.  Разделение на подсети/VLAN для изоляции трафика и упрощения масштабирования.  Микросервисная архитектура вместо монолитной (каждый сервис масштабируется независимо).  3. Балансировка нагрузки  Технологии:  Аппаратные балансировщики (F5 BIG-IP).  Программные (Nginx, HAProxy, AWS ALB).  Алгоритмы: Round Robin, Least Connections, IP Hash.  Пример:  При увеличении числа пользователей веб-приложения добавляются новые серверы, а балансировщик распределяет запросы между ними.  4. Эффективное использование ресурсов  Кэширование (CDN, Redis) — снижает нагрузку на серверы.  Оптимизация маршрутизации (OSPF, BGP) — предотвращает "бутылочные горлышки".  Сжатие данных (GZIP, Brotli) — уменьшает объём передаваемого трафика.  5. Автоматизация и оркестрация  Инструменты:  IaC (Infrastructure as Code): Terraform, Ansible.  Оркестрация: Kubernetes, Docker Swarm.  Преимущества: Быстрое развёртывание новых узлов, минимизация ручных ошибок.  Пример:  В облаке AWS можно автоматически добавлять EC2-инстансы при росте нагрузки (Auto Scaling Group).  6. Поддержка высокоскоростных технологий  Апгрейд сетевого оборудования:  Переход с 1 Gbps на 10/100 Gbps.  Использование SDN (Software-Defined Networking) для гибкого управления.  Оптические каналы (DWDM) для магистральных соединений.  7. Резервирование и отказоустойчивость  Избыточность компонентов:  Двойные маршрутизаторы, LACP для линков.  RAID-массивы для дисков.  Геораспределённые ЦОДы — защита от локальных аварий.  8. Мониторинг и аналитика  Инструменты: Zabbix, Prometheus, Grafana.  Метрики для анализа:  Загрузка CPU/RAM/диска.  Latency, Packet Loss.  Прогнозирование роста на основе исторических данных.  🔹 Уровни масштабируемости  Физический: Добавление серверов, коммутаторов, каналов связи.  Логический: Оптимизация VLAN, QoS, маршрутизации.  Прикладной: Балансировка нагрузки, кэширование, микросервисы.  🔹 Примеры плохой масштабируемости  Единый сервер БД для высоконагруженного приложения.  Статическая маршрутизация в сети с 1000+ узлов.  Отсутствие автоматизации (всё настраивается вручную). |

| Билет 20 | |
| --- | --- |
| Вопрос 1  Выполнить настройку Active Directory на Windows Server, создать несколько подразделений, групп пользователей и выполнить делегировать различные права для этих групп (не меньше 3 групп). | Настройка Active Directory (AD) с созданием подразделений, групп и делегированием прав  Цель:  Установить роль AD Domain Services на Windows Server.  Создать подразделения (OU) и группы пользователей.  Делегировать права для 3 групп (например, Администраторы, Пользователи, Гости).  🔹 Шаг 1: Установка Active Directory Domain Services (AD DS)  Откройте Диспетчер серверов → "Добавить роли и компоненты".  Выберите "Установка ролей или компонентов" → Далее.  Отметьте Active Directory Domain Services → Завершите установку.  После установки нажмите "Повысить роль до контроллера домена".  Настройка нового домена:  Тип развертывания: "Добавить новый лес" → Укажите имя домена (например, example.local).  Задайте пароль режима восстановления служб (DSRM).  Настройте NetBIOS-имя (например, EXAMPLE).  Завершите настройку → сервер перезагрузится.  🔹 Шаг 2: Создание подразделений (OU)  Откройте "Active Directory Users and Computers" (dsa.msc).  ПКМ по домену (example.local) → Создать → Подразделение.  Создайте структуру OU (например):  IT (для IT-отдела)  Finance (для бухгалтерии)  HR (для кадров)  🔹 Шаг 3: Создание групп пользователей  В каждой OU создайте группы безопасности:  IT\_Admins (в OU IT)  Finance\_Users (в OU Finance)  HR\_Staff (в OU HR)  Как создать группу:  ПКМ на OU → Создать → Группа.  Укажите имя группы → "Глобальная" и "Безопасности".  Добавьте пользователей в группы:  Создайте пользователей через ПКМ на OU → "Создать" → "Пользователь".  Перетащите пользователей в нужные группы.  🔹 Шаг 4: Делегирование прав группам  Примеры прав для 3 групп:    Как делегировать:  Откройте "Active Directory Users and Computers".  ПКМ на OU (например, IT) → "Делегировать управление".  В мастере делегирования:  Добавьте группу (например, IT\_Admins).  Выберите "Создание/удаление пользователей" и "Управление групповыми политиками".  Для Finance\_Users выберите "Чтение/запись всех свойств".  Для HR\_Staff → "Сброс паролей".  🔹 Шаг 5: Проверка работы  Для IT\_Admins:  Попробуйте создать пользователя в OU IT → должно получиться.  Попробуйте создать пользователя в OU HR → должна быть ошибка доступа.  Для HR\_Staff:  Откройте свойства пользователя в OU HR → должна быть доступна кнопка "Сбросить пароль".  Для Finance\_Users:  Проверьте, что можно редактировать поля пользователей в OU Finance, но нельзя удалять их.  🔹 Дополнительные настройки (опционально)  1. Групповые политики (GPO) для OU  Настройте разные политики для каждой OU (например, запрет USB для Finance).  powershell  gpmc.msc → ПКМ на OU → "Создать объект групповой политики".  2. Логирование изменений  Включите аудит событий в gpedit.msc:  Конфигурация компьютера → Политики → Политики аудита → Аудит изменений AD. |
| Вопрос 2  Определить находятся ли два узла А и В в одной подсети, если адреса компьютеров А и В 26.219.123.6 и 26.218.102.31. Маска подсети 255.255.192.0. | Определение, находятся ли узлы A и B в одной подсети  Дано:  IP узла A: 26.219.123.6  IP узла B: 26.218.102.31  Маска подсети: 255.255.192.0  🔹 Шаг 1: Перевод маски в CIDR и двоичный вид  Маска 255.255.192.0 в префиксной записи (CIDR):  Двоичное представление маски:  255.255.192.0 = 11111111.11111111.11000000.00000000  Количество единиц: /18 (первые 18 бит — сеть, остальные — хосты).  🔹 Шаг 2: Определение адреса сети для каждого узла  Формула:  Адрес сети = IP & Маска  (где & — побитовое И).  Для узла A (26.219.123.6):  Переводим в двоичный вид:  26.219.123.6 → 00011010.11011011.01111011.00000110  Применяем маску (&):  00011010.11011011.01111011.00000110 (IP A)  &  11111111.11111111.11000000.00000000 (Маска)  --------------------------------  00011010.11011011.01000000.00000000 → 26.219.64.0  Адрес сети A: 26.219.64.0/18  Для узла B (26.218.102.31):  Переводим в двоичный вид:  26.218.102.31 → 00011010.11011010.01100110.00011111  Применяем маску (&):  00011010.11011010.01100110.00011111 (IP B)  &  11111111.11111111.11000000.00000000 (Маска)  --------------------------------  00011010.11011010.01000000.00000000 → 26.218.64.0  Адрес сети B: 26.218.64.0/18  🔹 Шаг 3: Сравнение адресов сетей  Сеть узла A: 26.219.64.0/18  Сеть узла B: 26.218.64.0/18  Вывод:  Адреса сетей разные (26.219.64.0 ≠ 26.218.64.0), значит, узлы не в одной подсети.  🔹 Проверка через утилиту ipcalc (Linux)  bash  ipcalc 26.219.123.6/18  ipcalc 26.218.102.31/18  Результат:  Для A: Network: 26.219.64.0/18  Для B: Network: 26.218.64.0/18 |
| Вопрос 3  Определение Узла сети. Какие причины увеличения узлов сети вы знаете. | Определение узла сети  Узел сети — это любое устройство, подключенное к сети и имеющее уникальный идентификатор (IP-адрес, MAC-адрес). Примеры:  Компьютеры, серверы, ноутбуки.  Принтеры, IP-камеры, IoT-устройства.  Маршрутизаторы, коммутаторы (управляемые).  🔹 Причины увеличения количества узлов в сети  1. Рост организации  Новые сотрудники → больше рабочих станций.  Открытие филиалов → добавление серверов и сетевого оборудования.  2. Развитие ИТ-инфраструктуры  Внедрение IoT-устройств (умные датчики, камеры).  Подключение облачных сервисов (виртуальные машины, контейнеры).  3. Модернизация технологий  Переход на VoIP → новые IP-телефоны.  Внедрение беспроводных устройств (Wi-Fi 6, BYOD — личные гаджеты сотрудников).  4. Резервирование и отказоустойчивость  Добавление дублирующих серверов (кластеризация).  Развертывание геораспределенных узлов (CDN, резервные ЦОДы).  5. Безопасность и сегментация  Создание изолированных подсетей (VLAN) для разных отделов.  Добавление файрволов, IDS/IPS как отдельных узлов.  6. Требования законодательства  Внедрение систем видеонаблюдения (например, по закону о персональных данных).  Развертывание резервных серверов для соответствия стандартам (GDPR, ФЗ-152).  🔹 Последствия увеличения узлов |

| Билет 21 | |
| --- | --- |
| Вопрос 1  Выполнить настройку Active Directory на Windows Server | Пошаговая настройка Active Directory (AD) на Windows Server  🔹 Шаг 1: Установка роли AD Domain Services  Откройте «Диспетчер серверов» → «Добавить роли и компоненты».  Выберите «Установка ролей или компонентов» → Далее.  Отметьте «Active Directory Domain Services» → Добавить компоненты → Установить.  После установки нажмите «Повысить этот сервер до контроллера домена».  🔹 Шаг 2: Настройка нового домена  В мастере развертывания выберите:  «Добавить новый лес» → Укажите имя домена (напр., yourcompany.local).  Задайте пароль режима восстановления (DSRM).  Оставьте остальные параметры по умолчанию → Далее.  Проверьте предупреждения (если DNS-зона не создана, мастер предложит её настроить автоматически).  Завершите настройку → Сервер перезагрузится.  🔹 Шаг 3: Создание структуры OU (подразделений)  Откройте «Active Directory Users and Computers» (dsa.msc).  ПКМ по домену → Создать → Подразделение.  Создайте иерархию (пример):  yourcompany.local  ├── Departments  │ ├── IT  │ ├── Finance  │ └── HR  └── Servers  🔹 Шаг 4: Добавление пользователей и групп  Создание пользователей:  ПКМ на OU (напр., IT) → Создать → Пользователь.  Заполните поля: Имя, Фамилия, Логин (напр., user1), пароль (отметьте «Сменить пароль при следующем входе»).  Создание групп:  ПКМ на OU → Создать → Группа.  Укажите имя (напр., IT\_Admins) → Тип: Глобальная, Безопасности.  Добавьте пользователей в группы: перетащите их в нужные группы.  🔹 Шаг 5: Делегирование прав (на примере 3 групп)  Для IT\_Admins (полный доступ к OU IT):  ПКМ на OU IT → Делегировать управление → Добавьте группу IT\_Admins.  Выберите «Создание/удаление пользователей» + «Управление групповыми политиками».  Для Finance\_Users (чтение/запись в OU Finance):  Выберите «Чтение всех свойств» + «Запись всех свойств».  Для HR\_Staff (сброс паролей в OU HR):  Выберите «Сброс паролей пользователей».  🔹 Шаг 6: Настройка групповых политик (GPO)  Откройте «Group Policy Management» (gpmc.msc).  ПКМ на OU → «Создать объект GPO» (напр., IT\_Password\_Policy).  Настройте политики (пример для IT):  Требовать сложные пароли:  Конфигурация компьютера → Политики → Параметры Windows → Параметры безопасности → Политика учетных записей.  Запретить USB-накопители:  Конфигурация пользователя → Политики → Административные шаблоны → Система → Доступ к съемным запоминающим устройствам.  🔹 Шаг 7: Проверка работы  Для IT\_Admins:  Попробуйте создать пользователя в OU IT → Должно получиться.  Попытка создать пользователя в OU HR → Доступ запрещен.  Для HR\_Staff:  Сбросьте пароль пользователя в OU HR → Должно работать.  Для Finance\_Users:  Измените телефон пользователя в OU Finance → Проверьте, что изменения сохраняются. |
| Вопрос 2  Определить маску подсети, соответствующую указанному диапазону IP-адресов: 119.38.0.1–119.38.255.254. | Определение маски подсети для диапазона IP-адресов 119.38.0.1 – 119.38.255.254  🔹 Шаг 1: Анализ диапазона  Начальный IP: 119.38.0.1  Конечный IP: 119.38.255.254  Количество адресов:  119.38.0.0 — адрес сети (не используется).  119.38.255.255 — широковещательный (не используется).  Доступные адреса: 256 × 256 − 2 = 65 534 (это соответствует маске /16).  🔹 Шаг 2: Вычисление маски  Определяем сетевую часть:  Первые два октета (119.38) неизменны во всех адресах диапазона → значит, маска покрывает их.  Двоичный вид:  119.38.0.0 = 01110111.00100110.00000000.00000000  Маска: 11111111.11111111.00000000.00000000 (/16)  Десятичная запись маски: 255.255.0.0.  Проверка через формулу:    🔹 Шаг 3: Верификация  Адрес сети: 119.38.0.0/16  Broadcast: 119.38.255.255  Доступные адреса: 119.38.0.1 – 119.38.255.254.  Вывод: Маска 255.255.0.0 (/16) корректно покрывает указанный диапазон. |
| Вопрос 3  Технические осмотры объектов сетевой инфраструктуры. | Технические осмотры объектов сетевой инфраструктуры  Цель: Обеспечить стабильную работу сети, выявить и устранить потенциальные проблемы до их возникновения.  🔹 1. Виды технических осмотров  1.1 Плановые осмотры  Периодичность: Ежеквартально/ежемесячно.  Что проверяется:  Физическое состояние оборудования (серверы, коммутаторы, кабели).  Работоспособность систем охлаждения и вентиляции.  Логи событий (перегрев, сбои питания).  1.2 Внеплановые осмотры  Причины:  После аварий (например, перебои электропитания).  При резком росте нагрузки на сеть.  По требованию аудита безопасности.  1.3 Профилактические осмотры  Фокус: Предупреждение проблем.  Примеры:  Чистка серверов от пыли.  Проверка состояния ИБП и аккумуляторов.  🔹 2. Ключевые объекты проверки    🔹 3. Этапы проведения осмотра  3.1 Подготовка  Составьте чек-лист (пример ниже).  Уведомите сотрудников о времени осмотра (если требуется остановка услуг).  3.2 Физический осмотр  Оборудование:  Проверьте вентиляторы на запыленность.  Убедитесь, что кабели надежно подключены и не перегнуты.  Питание:  Тестируйте ИБП под нагрузкой.  Проверьте заземление.  3.3 Программная проверка  Сеть:  bash  ping -t 8.8.8.8 # Проверка внешней доступности  netstat -tuln # Открытые порты  Серверы:  powershell  Get-EventLog -LogName System -EntryType Error -Newest 10 # Критические ошибки  3.4 Документирование  Зафиксируйте все найденные проблемы в отчете (формат: Excel/спец. ПО).  Приоритезируйте исправления:  Критично (например, перегрев сервера).  Рекомендации (замена старых кабелей).  🔹 4. Чек-лист для осмотра  ✅ Оборудование  Нет перегрева (CPU < 70°C, диски < 50°C).  Все вентиляторы работают.  Нет поврежденных кабелей.  ✅ Сеть  Нет ошибок на интерфейсах (CRC, collisions).  DHCP и DNS отвечают.  ✅ Безопасность  Все патчи установлены.  Резервные копии актуальны.  🔹 5. Инструменты для автоматизации  Мониторинг: Zabbix, PRTG, SolarWinds.  Инвентаризация: NetBox, RackTables.  Документирование: DokuWiki, Confluence.  🔹 6. Типовые проблемы и решения |

| Билет 22 | |
| --- | --- |
| Вопрос 1  Выполнить настройку Квот и файлового экранирования в FSRM на Windows Server. | Настройка квот и файлового экранирования в FSRM на Windows Server  🔹 Шаг 1: Установка роли FSRM (File Server Resource Manager)  Откройте Диспетчер серверов → "Добавить роли и компоненты".  Выберите "Роль файловых служб" → "Служба управления ресурсами файлового сервера".  Завершите установку (перезагрузка не требуется).  🔹 Шаг 2: Настройка квот дискового пространства  Цель: Ограничить объем данных для пользователей/групп.  Откройте FSRM (fsrm.msc).  Перейдите в "Квоты" → "Создать квоту".  Укажите:  Путь: Папка (например, D:\Shared).  Тип квоты:  "Ограничить пространство" (например, 5 ГБ).  "Не применять квоту" (только мониторинг).  Шаблон: Выберите "200 МБ с уведомлением" (или создайте свой).  Настройте уведомления:  При 85% заполнения: Email или запись в журнал событий.  При 100%: Блокировка записи.  Пример PowerShell:  powershell  New-FsrmQuota -Path "D:\Shared" -Size 5GB -Template "200 MB Limit with Notification"  🔹 Шаг 3: Настройка файлового экранирования  Цель: Блокировать опасные типы файлов (например, .exe, .bat).  В FSRM перейдите в "Экраны файлов" → "Создать экран файла".  Укажите:  Путь: D:\Shared.  Тип экрана:  "Активный" (блокировка).  "Пассивный" (только логирование).  Группа файлов: Выберите "Исполняемые файлы" (или создайте свою).  Настройте уведомления (аналогично квотам).  Создание своей группы файлов:  Перейдите в "Группы файлов" → "Создать группу файлов".  Добавьте расширения (например, .mp3, .avi).  Пример PowerShell:  powershell  New-FsrmFileGroup -Name "Media Files" -IncludePattern @("\*.mp3", "\*.avi")  New-FsrmFileScreen -Path "D:\Shared" -Active -IncludeGroup "Media Files"  🔹 Шаг 4: Настройка отчетов и аудита  В FSRM выберите "Отчеты по управлению" → "Настроить параметры отчетов".  Добавьте расписание (например, еженедельный отчет о квотах).  Укажите получателей (Email администратора).  Пример отчета:  FSRM Report  🔹 Шаг 5: Проверка работы  Попробуйте скопировать файл .exe в D:\Shared → должно появиться сообщение о блокировке.  Заполните папку данными до лимита квоты → попытка записи нового файла должна завершиться ошибкой. |
| Вопрос 2  Проанализируйте работу сервера и выведите графики загруженности за разный период времени. | [Проанализируйте работу сервера и выведите графики загруженности за разный период времени.](#_q6p64g6o27el) |
| Вопрос 3  Определение Масштабируемости сети. Какие ключевые аспекты Масштабируемости вы знаете. | [Определение Масштабируемости сети. Какие ключевые аспекты Масштабируемости вы знаете.](#_d47oj2fn107l) |

| Билет 23 | |
| --- | --- |
| Вопрос 1  Выполнить настройку Windows Server, установить и настроить роли службы каталогов Active Directory. | [Выполнить настройку Windows Server, установить и настроить роли службы каталогов Active Directory.](#_sv8j2kgke70t) |
| Вопрос 2  Определить находятся ли два узла А и В в одной подсети, если адреса компьютеров А и В 26.219.123.6 и 26.218.102.31. Маска подсети 255.255.192.0. | [Определить находятся ли два узла А и В в одной подсети, если адреса компьютеров А и В 26.219.123.6 и 26.218.102.31. Маска подсети 255.255.192.0](#_7ooz9u94r6uj) |
| Вопрос 3  .Определение Регулярного резервирования. Организация удалённого оповещения о неполадках. | [Определение Регулярного резервирования. Организация удалённого оповещения о неполадках.](#_19j82ma46pf4) |

| Билет 24 | |
| --- | --- |
| Вопрос 1  Выполнить развёртывание BitLocker на Windows Server. | [Выполнить развёртывание BitLocker на Windows Server.](#_19j82ma46pf4) |
| Вопрос 2  Постройте топологию сети с помощью Zabbix. | [Постройте топологию сети с помощью Zabbix.](#_19j82ma46pf4) |
| Вопрос 3  Определение Узла сети. Какие причины увеличения узлов сети вы знаете. | [Определение Узла сети. Какие причины увеличения узлов сети вы знаете.](#_7ooz9u94r6uj) |

| Билет 25 | |
| --- | --- |
| Вопрос 1  Выполнить настройку Active Directory на Windows Server, создать несколько подразделений, групп пользователей и выполнить делегировать различные права для этих групп (не меньше 3 групп). | [Выполнить настройку Active Directory на Windows Server, создать несколько подразделений, групп пользователей и выполнить делегировать различные права для этих групп (не меньше 3 групп).](#_7ooz9u94r6uj) |
| Вопрос 2  Определить маску подсети, соответствующую указанному диапазону IP-адресов: 119.38.0.1–119.38.255.254. | [Определить маску подсети, соответствующую указанному диапазону IP-адресов: 119.38.0.1–119.38.255.254.](#_sv8j2kgke70t) |
| Вопрос 3  Классификация регламентов технических осмотров. |  |

## Теория (объединенный документ)

Объединенный документ: Ответы на вопросы по сетевой инфраструктуре и оборудованию

1. Виды физического вмешательства в инфраструктуру сети:

Повреждение кабелей (обрыв, перегиб, перегрызание).

Отключение электропитания (отключение ИБП, генераторов).

Кража или повреждение сетевого оборудования (серверы, маршрутизаторы, коммутаторы).

Установка несанкционированных устройств (анализаторы трафика, скрытые Wi-Fi точки доступа).

Физическое проникновение в серверные помещения (взлом, подкуп персонала).

2. Типы полосы пропускания:

Симметричная (одинаковая скорость загрузки и отдачи, например, выделенные линии).

Асимметричная (разная скорость загрузки и отдачи, например, DSL, DOCSIS).

Гарантированная (выделенная) (фиксированная пропускная способность).

Разделяемая (общая) (пропускная способность распределяется между пользователями).

Факторы, влияющие на полосу пропускания:

Тип используемого сетевого оборудования.

Сетевые протоколы.

Загрузка сети.

3. Паспорт технических устройств. Ключевые компоненты:

Наименование и модель устройства.

Серийный номер и инвентарный номер.

Технические характеристики (производительность, мощность, интерфейсы).

Дата изготовления и срок эксплуатации.

Условия эксплуатации (температура, влажность, электропитание).

Гарантийные обязательства и сервисные контакты.

История обслуживания и ремонтов.

4. Физическая карта сети:

Это схема, отображающая реальное расположение сетевых устройств (серверы, коммутаторы, маршрутизаторы) и физических соединений (кабели, оптоволокно) с указанием расстояний и местоположения.

5. Логическая топология сети. Типы топологий:

Определение: Способ организации передачи данных между узлами сети, не зависящий от физического расположения.

Типы топологий:

Шина (Bus) — все устройства подключены к одной линии.

Звезда (Star) — все устройства подключены к центральному узлу.

Кольцо (Ring) — данные передаются по замкнутому контуру.

Сетка (Mesh) — каждый узел соединён с несколькими другими.

Дерево (Tree) — иерархическая структура с ветвлением.

Гибридная — комбинация нескольких топологий.

6. Классификация регламентов технических осмотров:

Плановые (регулярные) — по графику (ежедневно, еженедельно, ежемесячно).

Внеплановые — при авариях или подозрении на неисправность.

Профилактические — для предупреждения поломок.

Аварийные — после сбоев для восстановления работы.

7. Технические осмотры объектов сетевой инфраструктуры:

Проверка состояния кабелей и разъёмов.

Контроль работы активного оборудования (коммутаторы, маршрутизаторы).

Проверка систем охлаждения и электропитания.

Анализ журналов событий и ошибок.

Тестирование резервных систем.

8. Оборудование для диагностики и сертификации кабельных систем:

Кабельные тестеры (проверка целостности, обрывов, замыканий).

Анализаторы сети (Fluke, WireXpert) — измерение скорости, затухания, помех.

OTDR (оптический рефлектометр) — диагностика ВОЛС.

TDR (рефлектометр для медных кабелей).

Генераторы тона и детекторы (поиск кабелей).

9. Регулярное резервирование и удалённое оповещение:

Определение: Автоматическое создание резервных копий данных по расписанию.

Организация оповещения:

Использование SNMP-мониторинга.

SMS/E-mail уведомления при срабатывании триггеров.

Интеграция с системами типа SIEM (Security Information and Event Management).

Протокол SNMP:SNMP (Simple Network Management Protocol) — это протокол управления сетью, используемый для мониторинга и управления сетевыми устройствами. Он позволяет собирать информацию об устройствах в сети, такую как загрузка процессора, использование памяти, состояние интерфейсов и другую статистику.

10. Обслуживание физических компонентов. Контроль аппаратного обеспечения:

Очистка от пыли и замена термопасты.

Проверка вентиляции и температуры.

Контроль состояния жёстких дисков (SMART).

Тестирование блоков питания и ИБП.

Обновление микропрограмм (firmware).

11. Масштабируемость сети. Ключевые аспекты:

Определение: Способность сети расширяться без потери производительности.

Аспекты:

Горизонтальная (добавление новых устройств).

Вертикальная (увеличение мощности существующих устройств).

Модульность (возможность добавления компонентов без перестройки всей сети).

Балансировка нагрузки (распределение трафика между узлами).

12. Узел сети. Причины увеличения узлов:

Определение: Любое устройство, подключённое к сети (серверы, ПК, IoT-устройства).

Причины увеличения:

Рост числа пользователей.

Развитие IoT (умные устройства, датчики).

Внедрение новых сервисов (облачные хранилища, VoIP).

Расширение филиалов компании.

Повышение отказоустойчивости (дублирование узлов).

13. Пассивное и активное сетевое оборудование:

Пассивное сетевое оборудование:Компоненты, которые не требуют электропитания для своей работы и используются для соединения и поддержки активного оборудования и передачи данных в сети.

Примеры:

Кабели (коаксиальный кабель, витая пара, оптоволокно).

Сетевые разъемы и соединители.

Патч-панели.

Шкафы и стойки для размещения оборудования.

Активное сетевое оборудование:Устройства, которые требуют электропитания для работы и используются для усиления, управления и маршрутизации сетевого трафика.

Примеры:

Маршрутизаторы.

Коммутаторы.

Концентраторы.

Сетевые карты.