**Лабораторная работа по теме № 8. Комплексный мониторинг узлов локальной сети.**

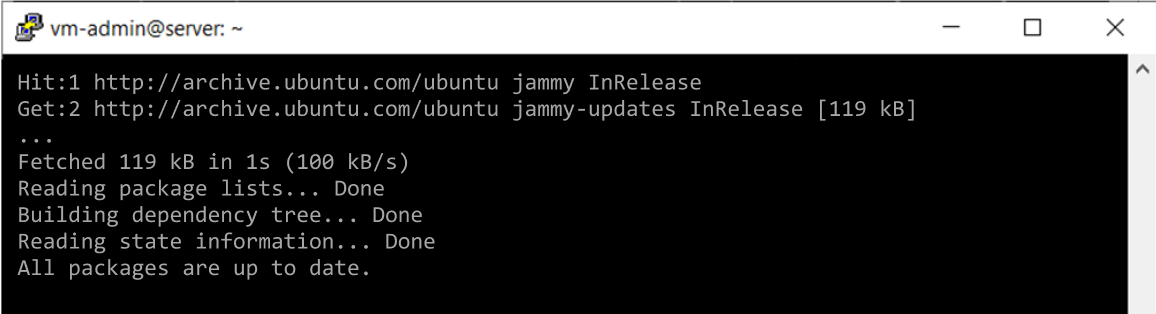
**Цель:** освоить навыки настройки системы мониторинга узлов локальной сети Zabbix.

**Задачи:**

1. **на виртуальной машине установить сервер системы мониторинга zabbix-server, веб-интерфейс zabbix-frontend, клиент zabbix-agent;**

**Обновление системы и установка необходимых пакетов:  
Откроем терминал на виртуальной машине и выполним команды:**

sudo apt update

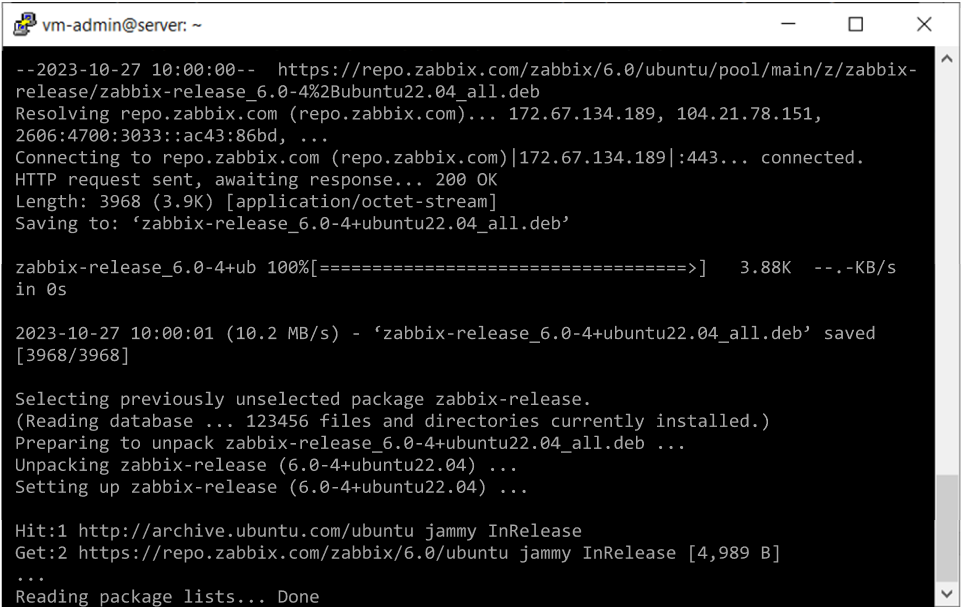


**Скачиваем пакет конфигурации репозитория Zabbix 6.0 LTS и устанавливаем его.**

wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release\_6.0-4%2Bubuntu22.04\_all.deb

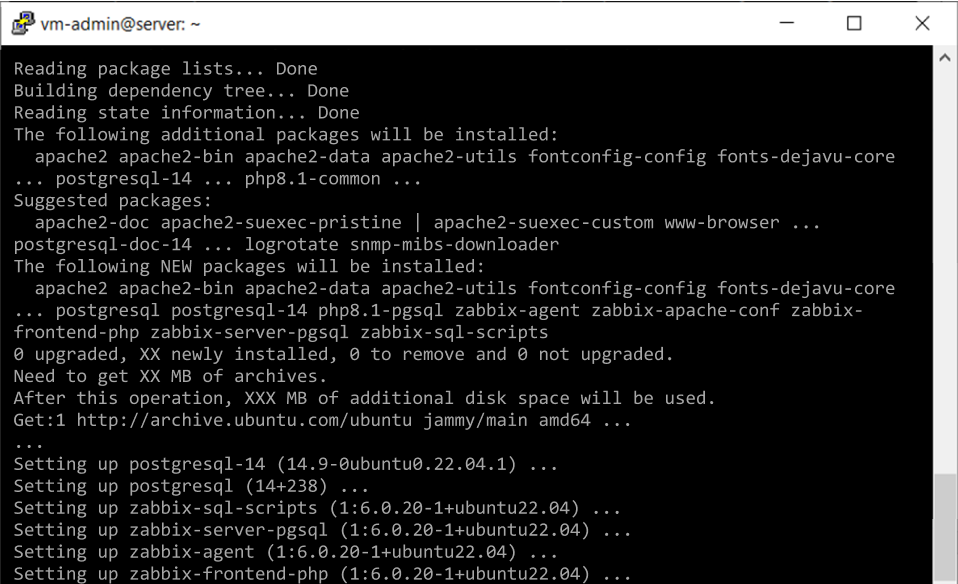
sudo dpkg -i zabbix-release\_6.0-4+ubuntu22.04\_all.deb

sudo apt update



Установка Zabbix сервера, веб-интерфейса, агента и базы данных PostgreSQL

sudo apt install zabbix-server-pgsql zabbix-frontend-php php8.1-pgsql zabbix-apache-conf zabbix-sql-scripts zabbix-agent postgresql -y



**Создание и настройка базы данных PostgreSQL**

sudo -u postgres createuser --pwprompt zabbix

Enter password for new role: password

Enter it again: password

**Настройка Zabbix сервера для работы с базой данных:**

**Редактируем файл конфигурации Zabbix сервера.**

sudo nano /etc/zabbix/zabbix\_server.conf

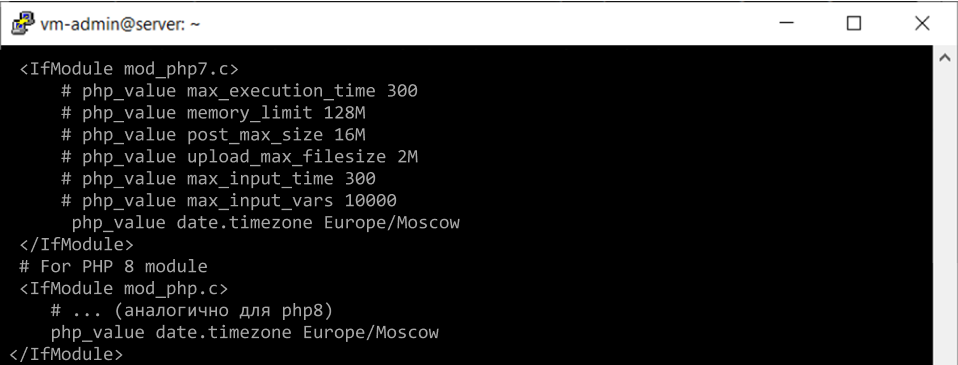
**Находим строку # DBPassword= , раскомментируем её (убираем #) и вписываем пароль, созданный для пользователя zabbix в PostgreSQL:**

DBPassword=password

Настройка PHP для Zabbix frontend (часовой пояс):  
Редактируем конфигурацию Apache для Zabbix.

sudo nano /etc/zabbix/apache.conf

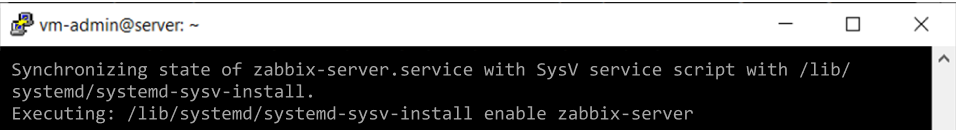
Находим секцию <IfModule mod\_php\*.c> и раскомментируем и устанавливаем правильный часовой пояс (Europe/Moscow):



**Запуск и автоматический старт сервисов:**

sudo systemctl restart zabbix-server zabbix-agent apache2 postgresql

sudo systemctl enable zabbix-server zabbix-agent apache2 postgresql



**Настройка брандмауэра**

**Разрешаем подключения к веб-интерфейсу (80) и портам Zabbix (10050, 10051).**

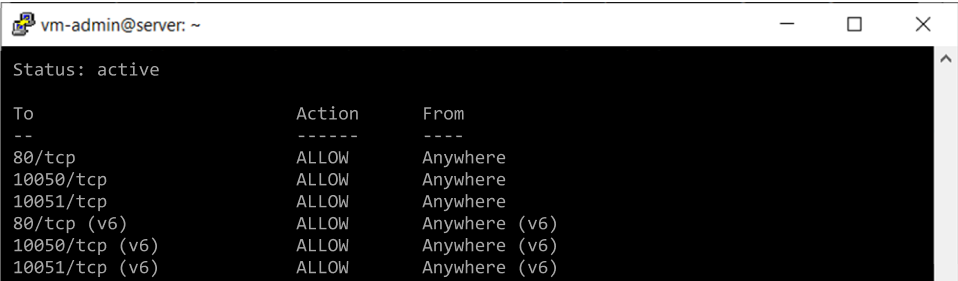
sudo ufw allow 80/tcp

sudo ufw allow 10050/tcp

sudo ufw allow 10051/tcp

sudo ufw enable

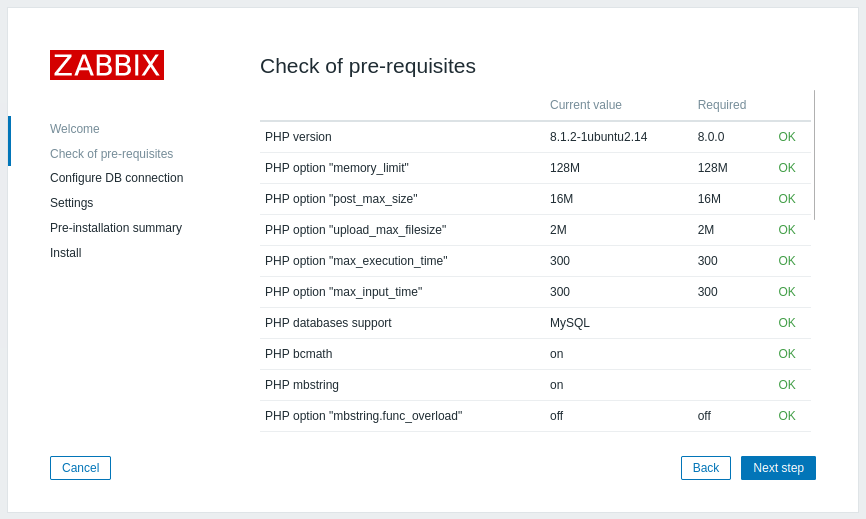
sudo ufw status

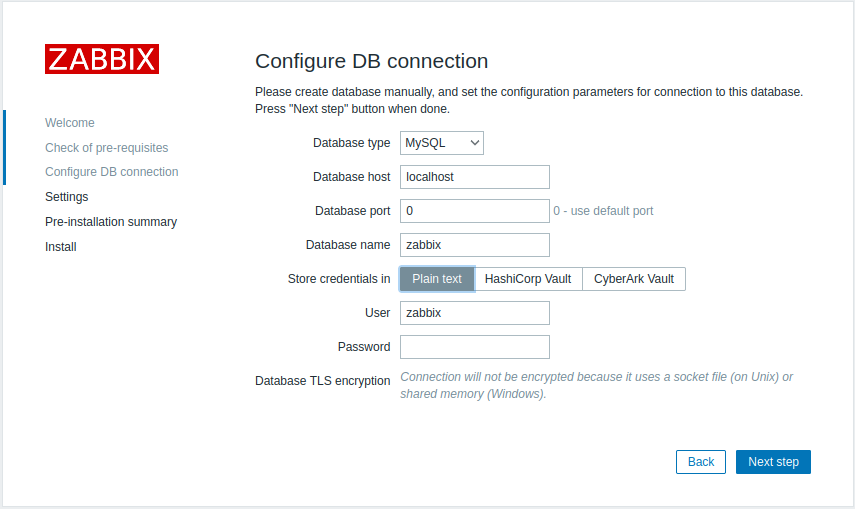


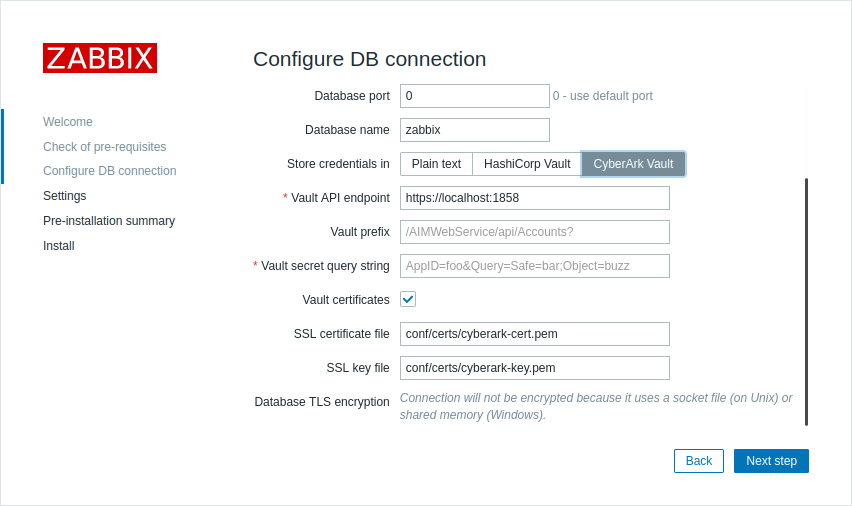
**Настройка Zabbix Frontend через веб-интерфейс:**

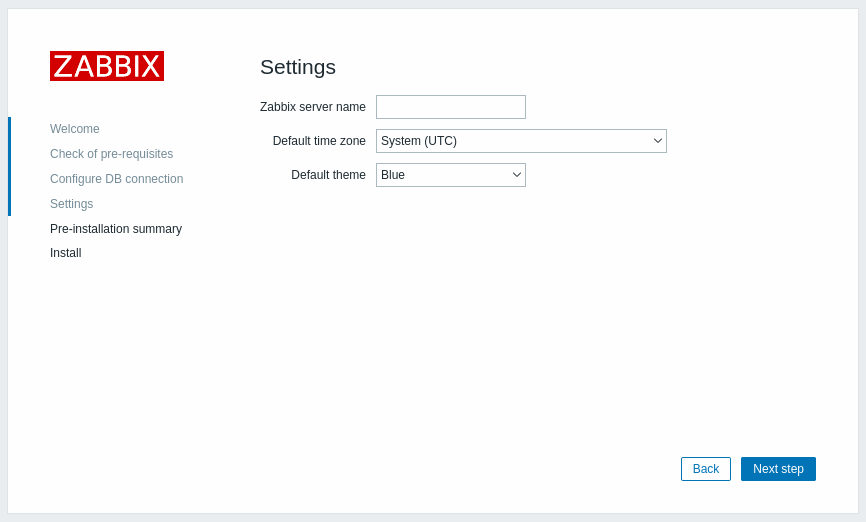
* Открываем браузер и переходим по адресу http://<VM\_IP>/zabbix.
* Видим экран приветствия Zabbix Setup. Нажимаем "Next step".
* Проверяется соответствие PHP-требованиям.
* Настраиваем подключение к базе данных
* Вводим имя Zabbix сервера.
* Проверяем сводку параметров. Нажимаем "Next step".
* Появляется страница входа. Логин по умолчанию: Admin (с большой буквы), пароль: zabbix.

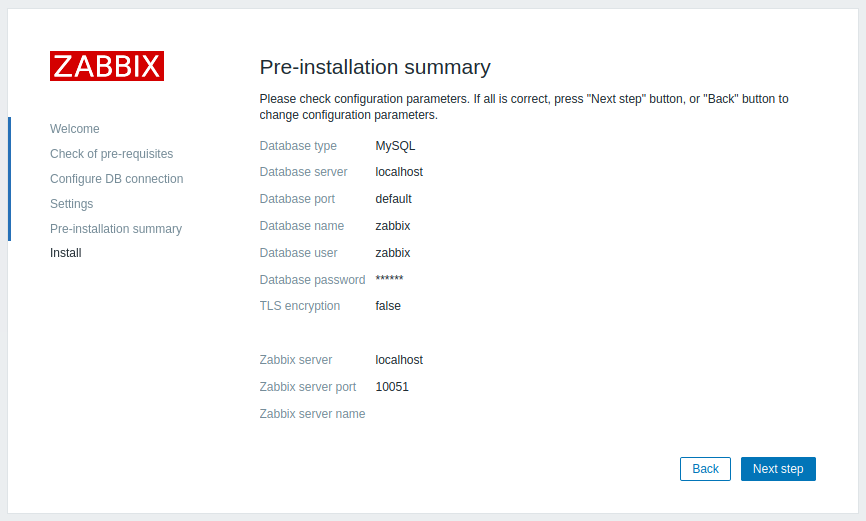


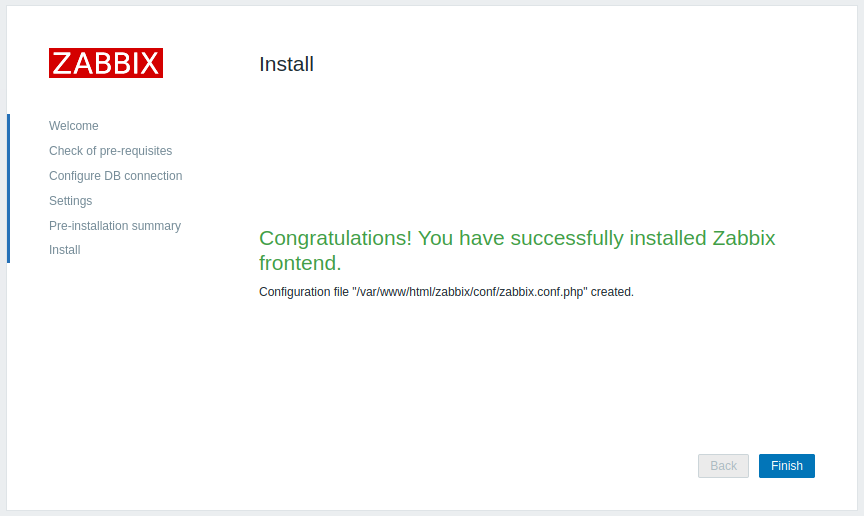


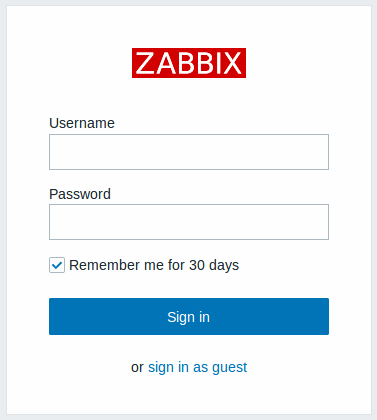












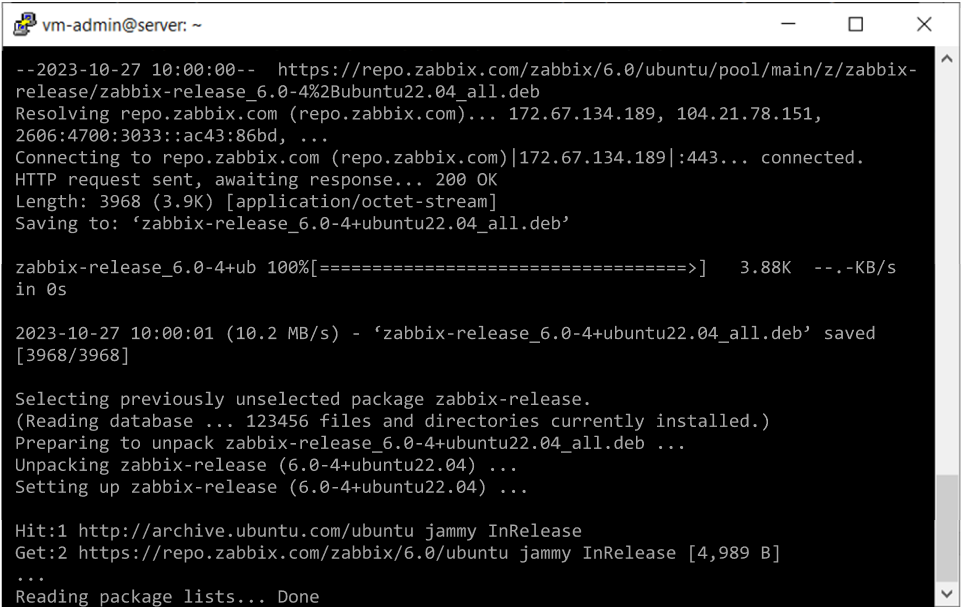
1. **на физической машине установить zabbix-agent и настроить отправку сведений на zabbix-server, установленный на виртуальной машине;**

**Установка репозитория Zabbix:**

wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release\_6.0-4%2Bubuntu22.04\_all.deb

sudo dpkg -i zabbix-release\_6.0-4+ubuntu22.04\_all.deb

sudo apt update



**Установка Zabbix Agent:**

sudo apt install zabbix-agent -y

**Настройка Zabbix Agent. Редактируем файл конфигурации агента на физической машине.**

sudo nano /etc/zabbix/zabbix\_agentd.conf

**Находим и изменяем следующие строки:**

**Указываем IP-адрес виртуальной машины, где работает Zabbix Server.**

Server=172.20.10.15

**Указываем IP-адрес и порт виртуальной машины Zabbix Server для активных проверок.**

ServerActive= 172.20.10.15:10051

**Указываем уникальное имя для этой физической машины. Это имя должно точно совпадать с именем хоста, которое мы будем создавать в веб-интерфейсе Zabbix.**

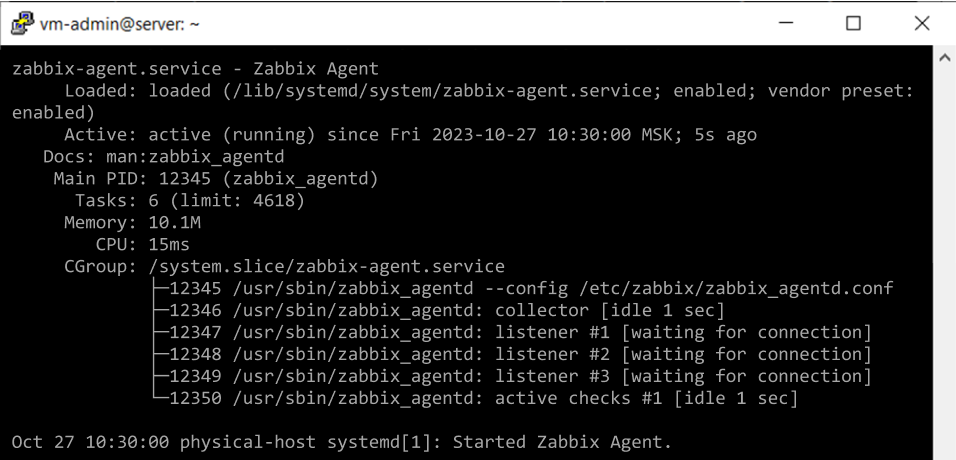
Hostname=Physical-Host-Lab

**Запуск и автоматический старт Zabbix Agent:**

sudo systemctl restart zabbix-agent

sudo systemctl enable zabbix-agent

sudo systemctl status zabbix-agent

****

**Настройка брандмауэра на Физической машине. Разрешаем входящие подключения *от* Zabbix сервера на порт агента (10050).**

sudo ufw allow from <VM\_IP> to any port 10050 proto tcp comment 'Allow Zabbix Server'

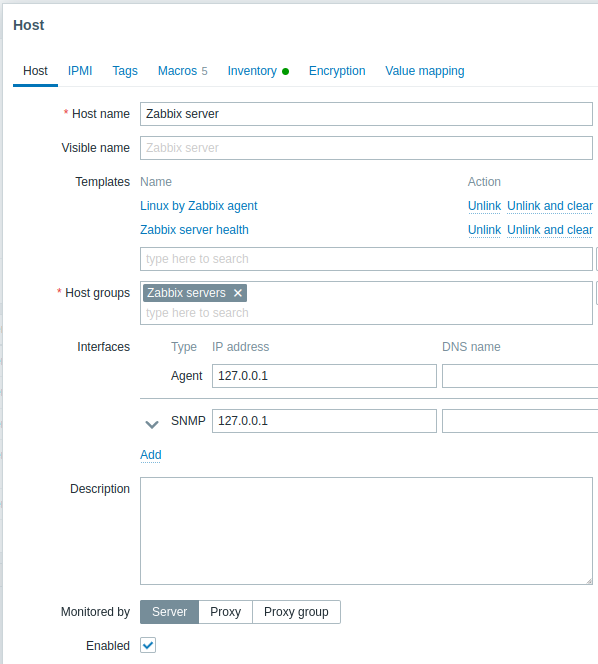
sudo ufw status

****

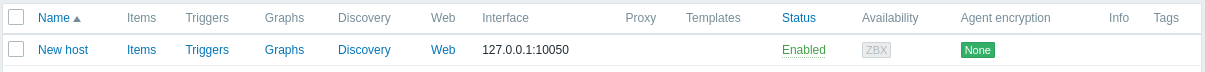
1. **через веб-интерфейс zabbix-frontend сконфигурировать мониторинг физической машины;**

Создание хоста:

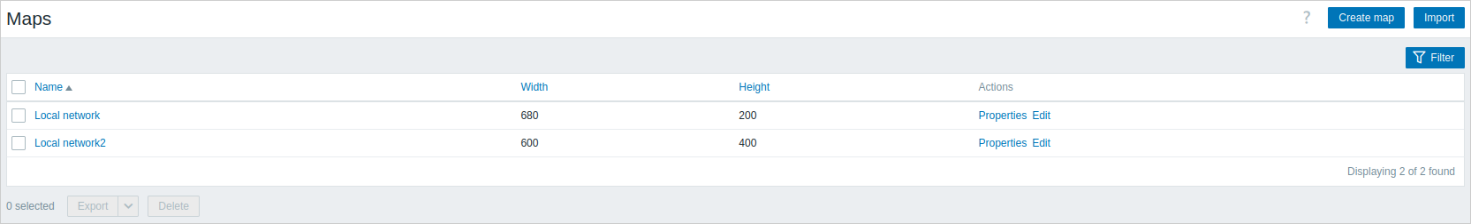
1. Переходим в раздел: Configuration -> Hosts.
2. Нажимаем кнопку Create host справа вверху.
3. На вкладке Host:
   * Host name.
   * Visible name: Можно ввести более понятное имя.
   * Groups.
   * Interfaces: Нажимаем Add и выбираем Agent.



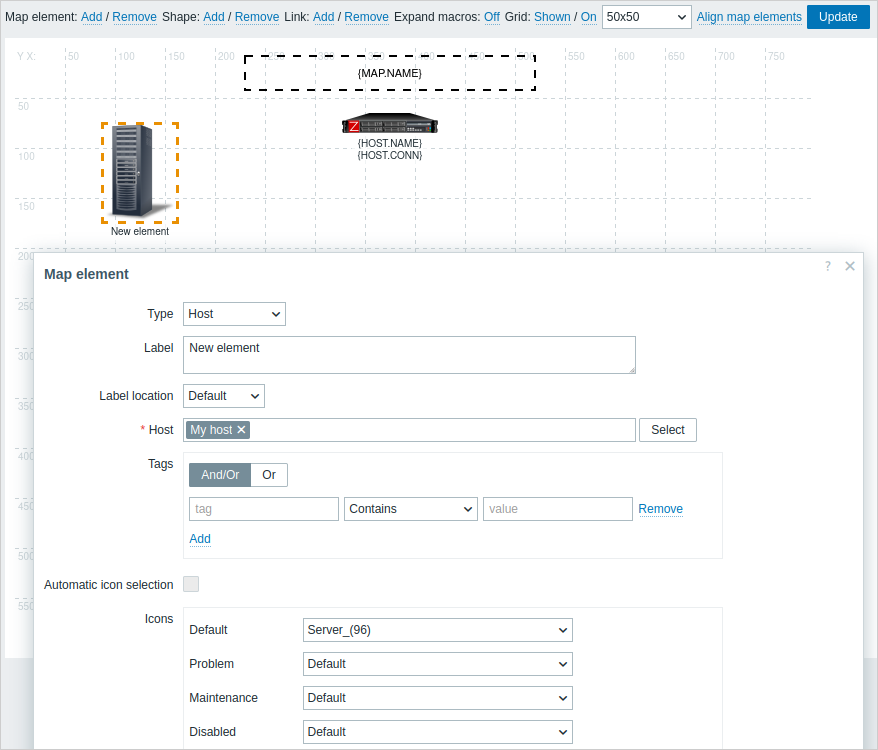
1. Переходим на вкладку Templates.
2. В поле Link new templates начинаем вводить Linux by Zabbix agent. Выбираем найденный шаблон (Template OS Linux by Zabbix agent).
3. Нажимаем большую синюю кнопку Add внизу формы для сохранения хоста.
4. Проверка статуса хоста:
   * Возвращаемся в Configuration -> Hosts.
   * В строке с созданным хостом (Physical-Host-Lab) в столбце Availability должен появиться зеленый значок ZBX.



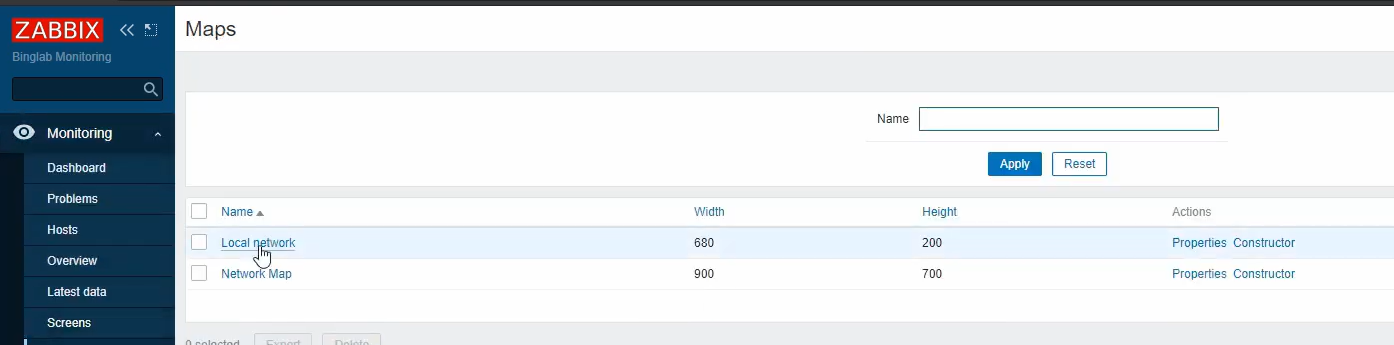
1. **добавить физическую машину на созданную при установке карту.**
2. **Переход к картам:**
   * В веб-интерфейсе переходим в раздел Monitoring -> Maps.
   * Обычно существует карта по умолчанию, например, Local network. Выбираем ее.



1. **Редактирование карты:**
   * Нажимаем на выпадающее меню Configuration of "Local network" и выбираем Edit map.
2. **Добавление элемента хоста:**
   * На панели инструментов карты нажимаем Add element (значок "+").
   * Перетаскиваем появившийся элемент хоста в нужное место на карте.



1. **Сохранение карты:**
   * Нажимаем кнопку Update справа вверху, чтобы сохранить изменения на карте.
2. **Просмотр карты:**
   * Снова переходим в Monitoring -> Maps и выбираем нашу карту. Теперь на ней должен отображаться добавленный хост (и, возможно, связь с сервером). Элемент хоста будет отображать статус, основанный на привязанных триггерах.



**Порядок защиты лабораторной работы.**

1. Продемонстрировать в браузере в веб-интерфейсе zabbix-frontend зеленые индикаторы, сообщающие о получении сведений от агентов на физической и виртуальной машинах.
2. Продемонстрировать в браузере карту сети из двух узлов.
3. Рассказать об обнаруженных с помощью системы мониторинга проблемах.