МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова

Навчально-науковий інститут автоматики і електротехніки
(повне найменування інституту, назва факультету)

Кафедра програмованої електроніки, електротехніки і телекомунікацій
(повна назва кафедри)

«Допущений до захисту»
Завідувач кафедри _____ В. М. Рябенький
д.т.н., професор
« 16 » червня 2025 р.

Кваліфікаційна робота

на здобуття першого (бакалаврського) рівня вищої освіти
(освітньо-кваліфікаційний рівень)

на тему: Система моніторингу локальної мережі закладу освіти

Виконав: студент 4397ст3 групи
_____ О. І. Пілявський
(підпис)

Керівник роботи:
старший викладач кафедри ПЕЕТ
(посада, науковий ступінь, вчене звання)
_____ С. Л. Трибулькевич
(підпис)

м. Миколаїв – 2025 року

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Національний університет кораблебудування імені адмірала Макарова
Навчально-науковий інститут автоматики та електротехніки

Кафедра програмованої електроніки, електротехніки і телекомунікацій
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітня програма Телекомунікації

«ЗАТВЕРДЖУЮ»
Гарант освітньої програми
_____ О.К.Жук
(підпис)
« 14 » квітня 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
на здобуття ступеня вищої освіти «бакалавр**»**
(освітньо-кваліфікаційний рівень)

Студенту Пілявському Олександру Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Система моніторингу локальної мережі закладу освіти

керівник роботи Трибулькевич Сергій Леонідович, старший викладач кафедри ПЕЕТ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом ректора № УЧ-343 від « 23 » квітня 2025 року.

2. Термін подання роботи: 10 червня 2025 року

3. Вихідні дані по роботі: Технічні характеристики обладнання, специфікації програмного забезпечення, середовище віртуалізації Proxmox VE 8.2, система моніторингу Zabbix 7.0, налаштування мережевого обладнання (маршрутизатори, точки доступу Wi-Fi, IP- камери, сервери), топологія мережі, SNMP, сценарії Telegram-оповіщення, VPN-тунелі L2TP/IPSec, сценарії автоматизації у Zabbix.

4. Перелік питань, що належать до розробки (найменування розділів)

Розділ 1. Призначення та область застосування розроблюваного виробу
Розділ 2. Технічна характеристика
Розділ 3. Опис та обґрунтування вибраної конструкції
Розділ 4. Розрахунки, підтверджуючі працездатність і надійність конструкції
Розділ 5. Охорона праці

5. Перелік презентаційних матеріалів Презентація на захист кваліфікаційної роботи. Схема мережі (структурна схема). Скриншоти з інтерфейсів Proxmox та Zabbix. Приклади Telegram-оповіщень. Фото/схеми підключення обладнання. Дашборди моніторингу в Zabbix. Графіки навантаження мережі.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Розділ 5	Тубальцев А. М.		

7. Дата видачі завдання « 24 » квітня 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання на кваліфікаційну роботу	01.04.2025 – 05.04.2025	виконано
2	Аналіз предметної області, постановка задач	06.04.2025 – 10.04.2025	виконано
3	Дослідження існуючих систем моніторингу	11.04.2025 – 15.04.2025	виконано
4	Вибір програмно-апаратного забезпечення	16.04.2025 – 20.04.2025	виконано
5	Розгортання віртуального середовища (Proxmox)	21.04.2025 – 25.04.2025	виконано
6	Встановлення та налаштування Zabbix 7.0	26.04.2025 – 01.05.2025	виконано
7	Додавання мережевого обладнання до моніторингу	02.05.2025 – 06.05.2025	виконано
8	Розробка карт мережі, система оповіщень через Telegram	07.05.2025 – 11.05.2025	виконано
9	Інтеграція VPN L2TP/IPSec	12.05.2025 – 15.05.2025	виконано
10	Опис архітектури рішення, структура моніторингової системи	20.05.2025 – 24.05.2025	виконано
11	Розділ з охорони праці	25.05.2025 – 30.05.2025	виконано
12	Оформлення пояснювальної записки та графічного матеріалу	01.06.2025 – 10.06.2025	виконано
13	Підготовка до попереднього захисту	11.06.2025 – 13.06.2025	виконано
14	Захист кваліфікаційної роботи	25.06.2025	виконано

Студент _____ О. І. Пілявський
(підпис) (прізвище та ініціали)

Керівник роботи _____ С. Л. Трибулькевич
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

У даному дипломному проекті виконано розгортання системи моніторингу на базі Zabbix 7.0 для контролю мережі навчального закладу. Проведено аналіз систем моніторингу Cacti, Nagios, Icinga, Nedi, Ntop, Observium та The Dude, що дозволило обрати Zabbix як найбільш оптимальне рішення для потреб закладу. Було розгорнуто віртуальне середовище Proxmox та налаштовано моніторинг маршрутизаторів, Wi-Fi точок, серверів і систем відеоспостереження. Створено карти мережі та систему оповіщення через Telegram для швидкого реагування на збої. Впроваджена система дозволяє ефективно контролювати роботу критичних компонентів мережі, підвищуючи її стабільність і безпеку.

SUMMARY

This thesis project implemented a monitoring system based on Zabbix 7.0 to oversee the network of educational institution. An analysis of monitoring systems such as Cacti, Nagios, Icinga, Nedi, Ntop, Observium, and The Dude was conducted, resulting in the selection of Zabbix as the most suitable solution for the institution’s needs. A Proxmox virtual environment was deployed, and monitoring of routers, Wi-Fi access points, servers, and surveillance systems was configured. Network maps and a Telegram-based notification system were created for prompt response to failures. The implemented system effectively monitors critical network components, enhancing its stability and security.

КЛЮЧОВІ СЛОВА

Віртуалізація, мережевий моніторинг, гіпервізор, Proxmox, Zabbix, Telegram, сервер, Wi-Fi, роутер, SNMP, мережеві карти, система оповіщення, IP-адреса, Web-сервер, веб-інтерфейс, термінал, адміністратор.

KEYWORDS

Virtualization, network monitoring, hypervisor, Proxmox, Zabbix, Telegram, server, Wi-Fi, router, SNMP, network maps, alerting system, IP address, web server, web interface, terminal, administrator.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ ТА ТЕРМІНІВ

IP-адреса – ідентифікатор для адресації комп'ютерів чи пристроїв у мережах;

Wi-Fi – бездротовий зв’язок;

ОЗП – оперативний запам'ятовувальний пристрій;

ОС – операційна система;

ПО – програмне забезпечення;

SNMP – Simple Network Management Protocol (Простий протокол управління мережею);

ДБЖ – джерело безперебійного живлення;

MIB – Management Information Base (База управління інформацією);

VM – віртуальна машина;

KVM (Kernel-based Virtual Machine) — це віртуалізаційна технологія, яка дозволяє використовувати можливості ядра Linux для створення віртуальних машин.

ВСТУП

Моніторинг мережевого обладнання та критичного програмного забезпечення є однією з ключових задач у системному адмініструванні. Важливість цієї задачі полягає у тому, що вона дозволяє не просто реагувати на проблеми, а передбачати їх, що значно спрощує роботу системних адміністраторів. Для більшості організацій, не пов’язаних безпосередньо з IT, важливо не те, як функціонує інфраструктура, а результат – стабільність роботи після змін в мережі. Завчасний моніторинг дозволяє забезпечити стабільність та ефективність.

Сьогодні практично всі бізнес-процеси залежать від роботи цифрових систем, таких як ERP, CRM, або в IT компаніях. Збої в роботі цих систем можуть призвести до фінансових втрат і зниження продуктивності. Сучасні рішення з моніторингу дозволяють оперативно отримувати інформацію про стан мережі та інфраструктури, даючи можливість системним адміністраторам своєчасно запобігти проблемам. Це особливо важливо в умовах зростаючого навантаження на мережі через збільшення кількості бізнес-додатків.

Моніторинг комп'ютерної мережі навчального закладу є прикладом того, як застосування систем моніторингу може суттєво спростити управління обладнанням, дозволяючи адміністраторам зосередитися на запобіганні проблем і забезпеченні безперебійної роботи інфраструктури. Це допомагає не тільки зекономити ресурси, але й мінімізувати простої та підвищити продуктивність роботи систем.

					172.4397ст3.КР.ПЗ.Р1		
Змн.	*Арк.*	*№ документу*	*Підпис*	*Дата*			
Розробник		Пілявський О. І.			ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ЗАСТОСУВАННЯ РОЗРОБЛЮВАНОГО ВИРОБУ	*Літ.*	*Арк.* 9 / *Аркушів*
Консультант							
Н. контр.		Добрінова Л. П.				НУК імені адмірала Макарова	
Керівник		Трибулькевич С. Л.					
Зав. каф.		Рябенький В. М.					

РОЗДІЛ 1. ПРИЗНАЧЕННЯ ТА ОБЛАСТЬ ЗАСТОСУВАННЯ РОЗРОБЛЮВАНОГО ВИРОБУ

1.1. Основні відомості

В умовах сучасного розвитку інформаційних технологій більшість комп'ютерних систем взаємодіють через локальні мережі або Інтернет. Це створює потребу в моніторингу для ефективного управління інформаційними потоками та забезпечення стабільної роботи мережі. Наявність програмного забезпечення для моніторингу дозволяє фахівцям з легкістю отримувати дані про стан мережі, її топологію та обладнання, що в кінцевому підсумку спрощує контроль і управління системами. Без таких інструментів робота адміністратора значно ускладнюється, оскільки зростає ризик пропустити важливі події або неполадки в мережі.

1.2. Коротка характеристика області та умов використання виробу

Система, що розробляється, інтегрується в поточну мережу державного закладу освіти для підвищення стабільності локальної мережі та серверного обладнання. Вона підтримує розгортання на різних платформах віртуалізації серверів, таких як ZABBIX, Proxmox, Windows Server 2022, Debian, що дозволяє адаптувати її під різні інфраструктури.

До задач системи відносяться моніторинг:

– некерованих мережевих комутаторів;

– маршрутизаторів;

– точок доступу WiFi;

– IP системи відеоспостереження;

– апаратного забезпечення системи серверної віртуалізації.

					172.4397ст3.КР.ПЗ.Р2	
Змн.	*Арк.*	*№ документу*	*Підпис*	*Дата*		
Розробник		Пілявський О. І.			ТЕХНІЧНА ХАРАКТЕРИСТИКА	*Літ.* / *Арк.* 11 / *Аркушів*
Консультант						
Н. контр.		Добрінова Л. П.				НУК імені адмірала Макарова
Керівник		Трибулькевич С. Л.				
Зав. каф.		Рябенький В. М.				

РОЗДІЛ 2. ТЕХНІЧНА ХАРАКТЕРИСТИКА

2.1. Основні технічні характеристики обладнання

До складу системи входять:

відеореєстратор – 1 шт.;

відеокамери – 14 шт.;

некеровані комутатори – 30 шт.;

точки доступу WiFi – 40 шт.;

маршрутизатор – 1 шт.;

серверне обладнання – 2 шт.;

віртуальні машини – 2 шт.;

робочі станції – 200 шт.

TP-Link TL-SG1005D:

Тип: Настільний гігабітний некерований комутатор;

Кількість портів: 5 портів Gigabit Ethernet;

Живлення: 5V ⎓ 0.6A;

Версія: V9.0;

Серійний номер: S/N: 2197595001264.

TP-Link Archer C54:

Тип: Дводіапазонний Wi-Fi маршрутизатор;

Підтримка: AC1200 Wi-Fi (2.4GHz і 5GHz);

Живлення: 9V ⎓ 0.85A;

Версія: V1.0;

Серійний номер: S/N: 22200R01037.

TP-Link TL-SF1008D:

Тип: Настільний некерований комутатор;

Кількість портів: 8 портів 10/100Mbps Ethernet;

Живлення: 5V ⎓ 0.6A;

Версія: V8.0;

Серійний номер: S/N: 2159282007565.

TP-Link TL-SF1016D:

Тип: Настільний некерований комутатор;

Кількість портів: 16 портів 10/100Mbps Ethernet;

Живлення: 9V ⎓ 1A;

Індикатори: Для кожного порту для статусу підключення та активності.

D-Link DES-1016D:

Тип: Комутатор некерований;

Кількість портів: 16 портів Fast Ethernet 10/100Mbps;

Живлення: 9V ⎓ 1A;

Версія: H/W Ver: D4;

Серійний номер: S/N: F3PZ198001115.

Netis ST3108GS:

Тип: Гігабітний Ethernet некерований комутатор;

Кількість портів: 8 портів;

Живлення: 5V ⎓ 800mA;

Версія: V2;

Серійний номер: S/N: 1102215108800102.

TP-Link LS108G:

Тип: Настільний гігабітний некерований комутатор;

Кількість портів: 8 портів Gigabit Ethernet;

Живлення: 9V ⎓ 0.85A;

Версія: V4.0;

Серійний номер: S/N: 2246295002044.

MikroTik 3011:

Тип: Роутер;

Кількість портів: 10 портів;

Живлення: 24V ⎓ 1.2A;

Серійний номер: S/N: HGF09Z0EP33/R2.

Сервер 1 (Windows Server 2022):

Процесор: Intel i7-4770 3.7 ГГц;

Оперативна пам'ять: 16 ГБ;

SSD: 120 ГБ;

HDD: 1 ТБ;

Відеоадаптер: Intel Graphics 4600;

Живлення: 450W.

Сервер 2 (Proxmox):

Процесор: AMD Ai-9800;

Оперативна пам'ять: 16 ГБ;

SSD: 256 ГБ;

Живлення: 450W.

Dahua DHI-NVR2116-4KS2 Відеореєстратор:

Модель: DHI-NVR2116-4KS2;

Підтримка: 16 каналів, 4K H.265+/H.264+;

Вага: 1.0 кг;

Розмір: 364 мм x 96 мм x 261 мм;

Підтримка P2P, Smart Search, HD відео, QR код;

Виробник: Dahua Vision Technology Co., Ltd;

Дата виготовлення: 05/2021.

2MP IP камери Hikvision DS-2CD1321-I(F) (2.8 мм):

Модель: Hikvision DS-2CD1321-I(F);

Тип: 2МП IP камера;

Об'єктив: 2.8 мм (ширококутний);

Матриця: 1/2.8" Progressive Scan CMOS;

Роздільна здатність: 1920x1080 (Full HD), 2 мегапікселі;

Світлочутливість: 0.01 Люкс (F1.2, AGC увімкнено);

Інфрачервона підсвітка: до 30 метрів;

Компресія відео: H.264 / MJPEG;

Кількість кадрів: до 30 кадрів/с при 1920x1080;

Підтримка WDR: DWDR (цифровий широкодинамічний діапазон);

Динамічний діапазон: 120dB;

Захист: IP67 (захист від пилу та води);

Живлення: DC 12V ± 25%, PoE (802.3af);

Споживана потужність: 5W (макс.);

Робоча температура: від -30°C до +60°C;

Підтримка мережевих протоколів: TCP/IP, HTTP, DHCP, DNS, NTP, RTSP, RTP, TCP, UDP;

Вага: приблизно 350 г.

2.2. Програмне забезпечення

Операційна система – Linux, Debian 12, AlmaLinux, Windows Server 2022, Windows 10, 11;

База даних – MySQL;

Web-сервер – Apache;

Віддалений доступ – VPN.

					172.4397ст3.КР.ПЗ.РЗ		
Змн.	*Арк.*	*№ документу*	*Підпис*	*Дата*			
Розробник		Пілявський О. І.			ОПИС ТА ОБҐРУНТУВАННЯ ВИБРАНОЇ КОНСТРУКЦІЇ	*Літ.*	*Арк.* 16 / *Аркушів*
Консультант							
Н. контр.		Добрінова Л. П.				НУК імені адмірала Макарова	
Керівник		Трибулькевич С. Л.					
Зав. каф.		Рябенький В. М.					

РОЗДІЛ 3. ОПИС ТА ОБҐРУНТУВАННЯ ВИБРАНОЇ КОНСТРУКЦІЇ

3.1. Системи моніторингу

3.1.1. Nagios

Nagios — це потужна система моніторингу мережі та IT-інфраструктури, яка вже багато років активно розвивається. Вона написана мовою програмування C, що забезпечує високу продуктивність і надійність. Nagios надає широкі можливості для моніторингу, які задовольнять потреби системних і мережевих адміністраторів.

Програма має зручний, швидкий та інтуїтивно зрозумілий веб-інтерфейс, а її серверна частина відзначається стабільністю та гнучкістю налаштувань. Хоча первинне налаштування може здатися складним для новачків, саме ця гнучкість робить Nagios універсальним інструментом, який можна адаптувати практично під будь-яке завдання моніторингу.

Подібно до системи Cacti, Nagios має велике і активне співтовариство користувачів та розробників, які підтримують проект та створюють численні плагіни. Завдяки цьому доступні рішення для моніторингу як апаратного, так і програмного забезпечення — від простих перевірок доступності через ping до складної інтеграції з іншими інструментами, наприклад, Webinject, який використовується для тестування вебзастосунків і вебсервісів.

Nagios дозволяє здійснювати постійне спостереження за станом серверів, сервісів, мережевих з’єднань і будь-яких пристроїв, що працюють за протоколом IP. Серед можливих метрик моніторингу — вільний дисковий простір, завантаження оперативної пам’яті та процесора, використання ліцензій FlexLM, температура повітря на виході сервера, затримки в мережах WAN або Інтернет і багато іншого.

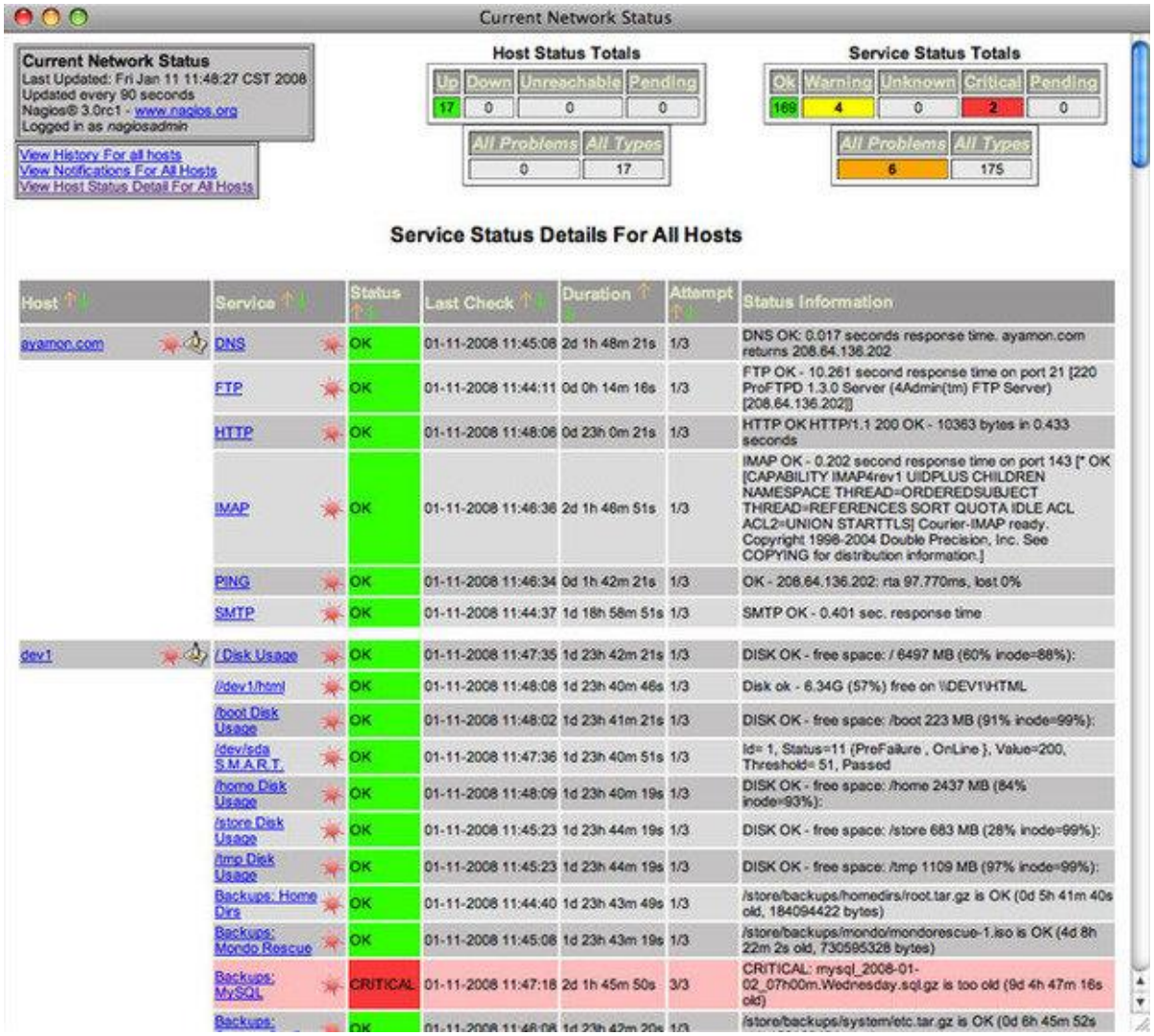

Рисунок 3.1 – Інтерфейс Nagios

Жодна система для моніторингу мережі або серверів не буде ефективною без механізмів сповіщення, і Nagios повністю відповідає цим вимогам. Програма підтримує надсилання сповіщень через електронну пошту, SMS-повідомлення та популярні інтернет-месенджери. Окрім цього, у Nagios реалізована система ескалацій, яка дозволяє точно визначити, кого, яким чином і за яких умов слід інформувати про інциденти.

За допомогою веб-інтерфейсу можна підтвердити проблему, тимчасово вимкнути повідомлення або залишити адміністративний коментар, що полегшує координацію роботи між фахівцями.

Також у Nagios передбачена функція візуального представлення інфраструктури, де всі пристрої зображаються у вигляді логічної схеми

мережі. Колірне маркування дозволяє в реальному часі оцінити стан кожного компонента та оперативно реагувати на збої.

Одним із недоліків системи є складність первинного налаштування: більшість конфігураційних дій виконується через командний рядок, що може створити труднощі для початківців. Водночас користувачам, які мають досвід роботи з конфігураційними файлами в Linux або Unix, цей підхід не викличе особливих труднощів.

Хоча повне використання потенціалу Nagios може вимагати чималих зусиль, можливості системи з раннього виявлення проблем і широка гнучкість у моніторингу мережевих та серверних компонентів роблять її надзвичайно цінним інструментом.

3.1.2. Cacti

Історія Cacti починається з інструменту MRTG (Multi Router Traffic Grapher), створеного ще в 1990-х роках розробником Тобіасом Отікером. MRTG був покликаний візуалізувати дані про пропускну здатність мережевих пристроїв за допомогою простої кільцевої бази даних. З часом цей інструмент еволюціонував у Rrdtool — набір утиліт для збору, збереження та графічного представлення динамічних показників, таких як навантаження на процесор, трафік чи температура. Сьогодні Rrdtool активно використовується в багатьох open-source системах моніторингу.

На основі цього фундаменту з’явився Cacti — сучасне рішення з відкритим кодом, яке продовжує традиції MRTG, але значно розширює їх можливості. Cacti спеціалізується на візуалізації статистичних даних у вигляді графіків і підтримує моніторинг широкого спектра параметрів — від використання диска до обертів вентиляторів у системних блоках. Якщо певний показник можна відстежити — його, ймовірно, можна інтегрувати у Cacti.

Cacti є безкоштовною системою, яка зазвичай встановлюється як частина LAMP-стека (Linux, Apache, MySQL, PHP) і забезпечує централізовану платформу для створення графіків на основі числових даних.

Завдяки підтримці SNMP (Simple Network Management Protocol), система може працювати практично з будь-яким обладнанням, яке надає числові метрики — серверами на базі Linux або Windows, маршрутизаторами, комутаторами тощо.

Крім вбудованих функцій, Cacti підтримує імпорт шаблонів від сторонніх розробників, що дозволяє ще більше розширити перелік сумісних пристроїв і сервісів. Таким чином, Cacti є гнучким і потужним інструментом для візуального представлення стану інфраструктури в режимі реального часу.

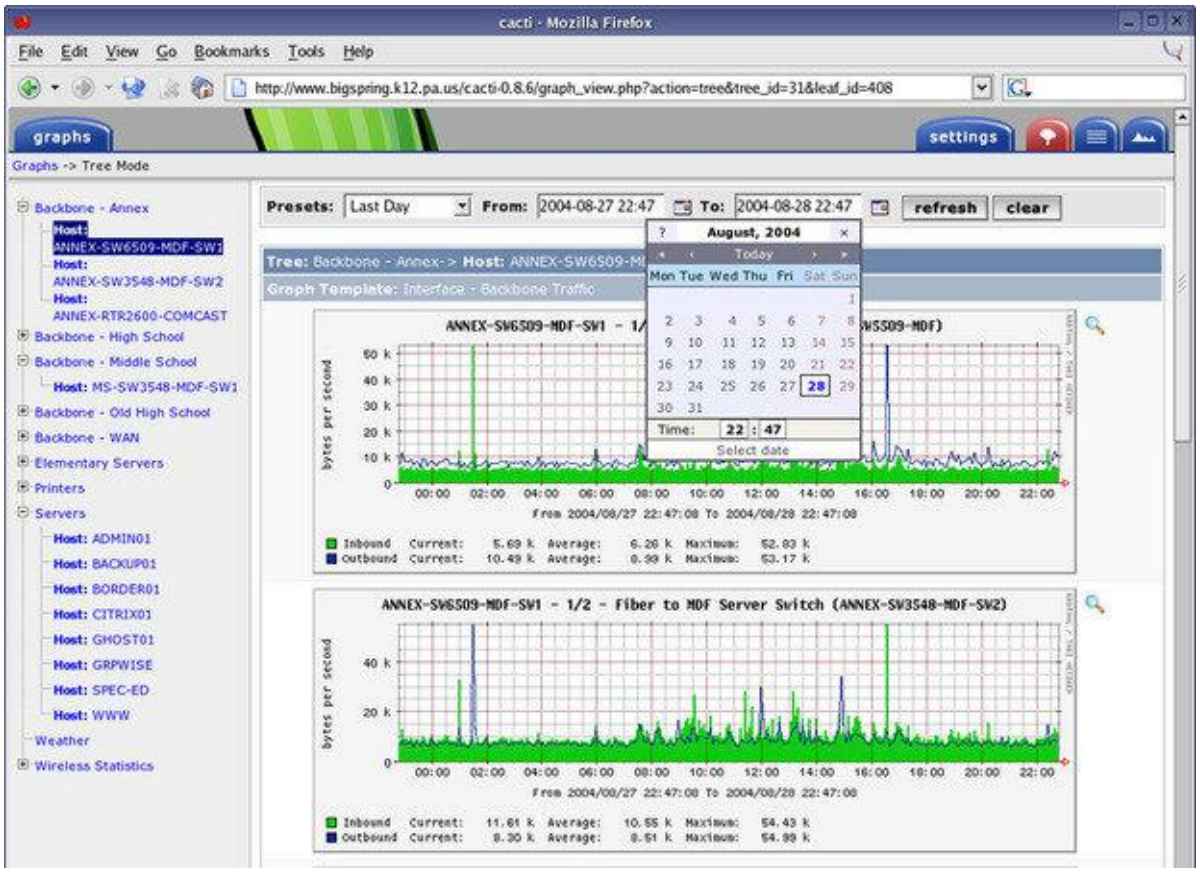

Рисунок 3.2 – Інтерфейс Cacti

Попри те, що SNMP є основним методом збору даних у Cacti, система також підтримує використання скриптів, написаних мовами Perl або PHP. Архітектура Cacti ефективно розділяє процеси збору інформації та її візуалізації, що дозволяє зручно повторно використовувати зібрані дані для створення різних графіків і звітів.

Користувачі можуть легко взаємодіяти з графіками: вибирати певні часові проміжки, деталізувати окремі ділянки просто за допомогою миші —

наприклад, виділяючи потрібну область для аналізу. Це дає змогу швидко переглядати статистику за роки й виявляти потенційні аномалії або закономірності в роботі серверів та мережевого обладнання.

Один із корисних інструментів — Network Weathermap, плагін на PHP, який дає змогу створювати інтерактивні мапи мережі. Вони відображають навантаження на мережеві канали в режимі реального часу, а при наведенні курсора на з'єднання з'являється відповідний графік завантаження. Такі карти часто виводять на великі екрани в серверних або мережевих центрах, що дозволяє технічному персоналу цілодобово контролювати стан мережевої інфраструктури.

Таким чином, Cacti є потужним інструментом для графічного аналізу й моніторингу, який підтримує величезну кількість типів метрик. Його гнучкість і можливість адаптації до специфічних потреб роблять систему надзвичайно корисною, хоча в деяких випадках складність налаштування може виявитися викликом для користувачів-початківців.

3.1.3. Ntop

Проєкт Ntop, відомий сьогодні як Ntopng, за останні роки пройшов значну еволюцію, перетворившись на один із провідних інструментів для аналізу мережевого трафіку. Його головною перевагою є поєднання потужного функціоналу з легким і швидким веб-інтерфейсом, що робить його зручним для щоденного використання.

Програма реалізована мовою програмування C, що забезпечує високу продуктивність і мінімальне споживання ресурсів. Для запуску достатньо одного процесу, який прив'язується до потрібного мережевого інтерфейсу — це вся базова конфігурація, необхідна для старту.

Ntopng не потребує додаткових залежностей чи складної інтеграції — він є повністю автономним рішенням, готовим до використання одразу після встановлення.

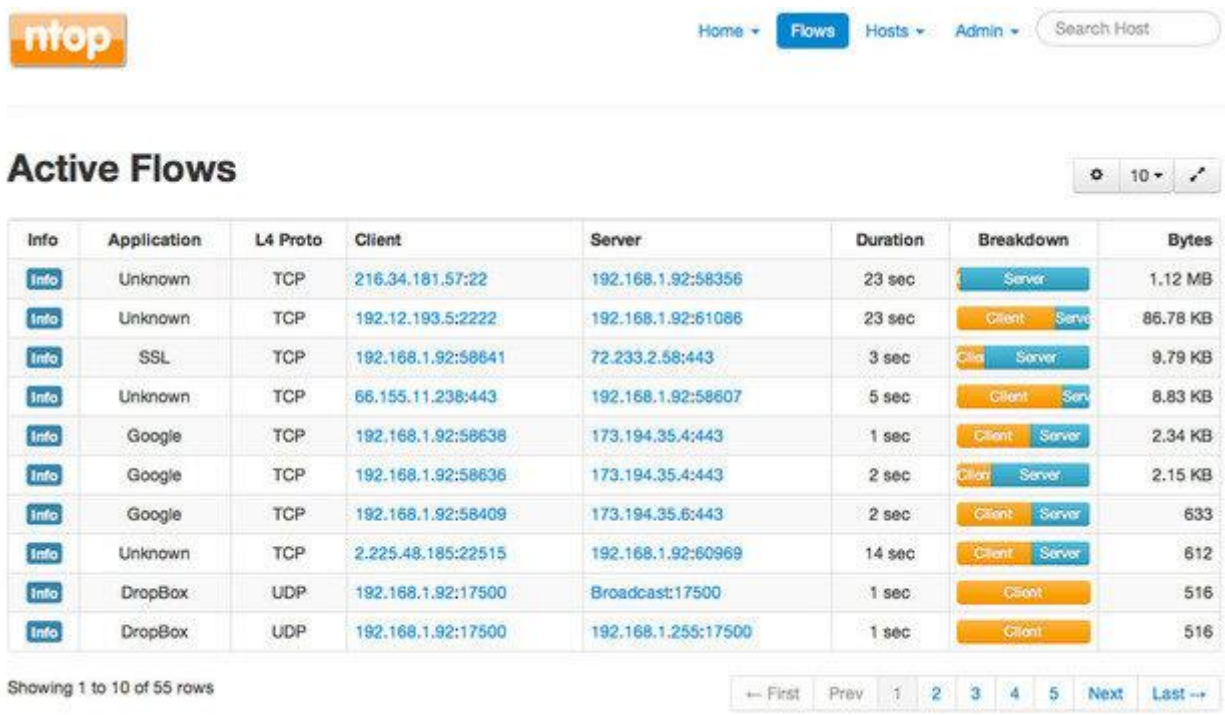

Рисунок 3.3 – Інтерфейс Ntop

Однією з головних переваг Ntopng є наочні графіки та таблиці, що відображають поточний та історичний трафік, включаючи протоколи, джерела, призначення та історію конкретних транзакцій. Користувачі можуть переглядати статистику по хостах з обох кінців з'єднань. Крім того, система має розширену підтримку графіків і діаграм для моніторингу використання мережі в реальному часі, а також модульну архітектуру, що дозволяє легко додавати нові можливості, наприклад, моніторинг через NetFlow та sFlow.

Ntopng також включає підтримку Nbox — апаратного монітора, який інтегрується безпосередньо в систему для ще більшої точності моніторингу. Інтерфейс API на основі мови програмування Lua дозволяє легко додавати розширення та автоматизувати процеси.

Однією з ключових функцій Ntopng є можливість зберігати дані про хости в RRD-файлах для забезпечення безперервного збору та аналізу інформації.

Одним із найбільш корисних застосувань Ntopng є моніторинг мережевих сегментів. Наприклад, якщо на карті мережі деякі канали підсвічуються червоним, можна швидко отримати звіт, що містить інформацію про проблемний сегмент і хости, що його викликають. Це дає можливість оперативно виявляти та усувати проблеми в мережі.

Такий рівень видимості мережі важко переоцінити, і його досягнення є надзвичайно простим. Досить запустити Ntopng на будь-якому інтерфейсі, налаштованому на рівні комутатора, для моніторингу додаткових портів або VLAN.

3.1.4. Icinga

Icinga починалася як розширення популярної системи моніторингу Nagios, але згодом була повністю переписана та стала незалежним проєктом, відомим як Icinga 2. На сьогоднішній день обидві версії — Icinga 1.x та Icinga 2 — активно розвиваються, і користувачі мають змогу вибирати між ними. Icinga 1.x забезпечує сумісність із великою кількістю плагінів і конфігурацій Nagios, що полегшує перехід для тих, хто вже працював з цією системою.

Натомість Icinga 2 була спроектована з акцентом на зручність використання та високу продуктивність. Вона отримала модульну архітектуру та підтримку багатопоточності, що відрізняє її від Nagios і старішої версії Icinga 1.

Як і Nagios, Icinga є потужною платформою для моніторингу і оповіщення, але має значні вдосконалення у вигляді більш інтуїтивно зрозумілого веб-інтерфейсу та покращеного користувацького досвіду.

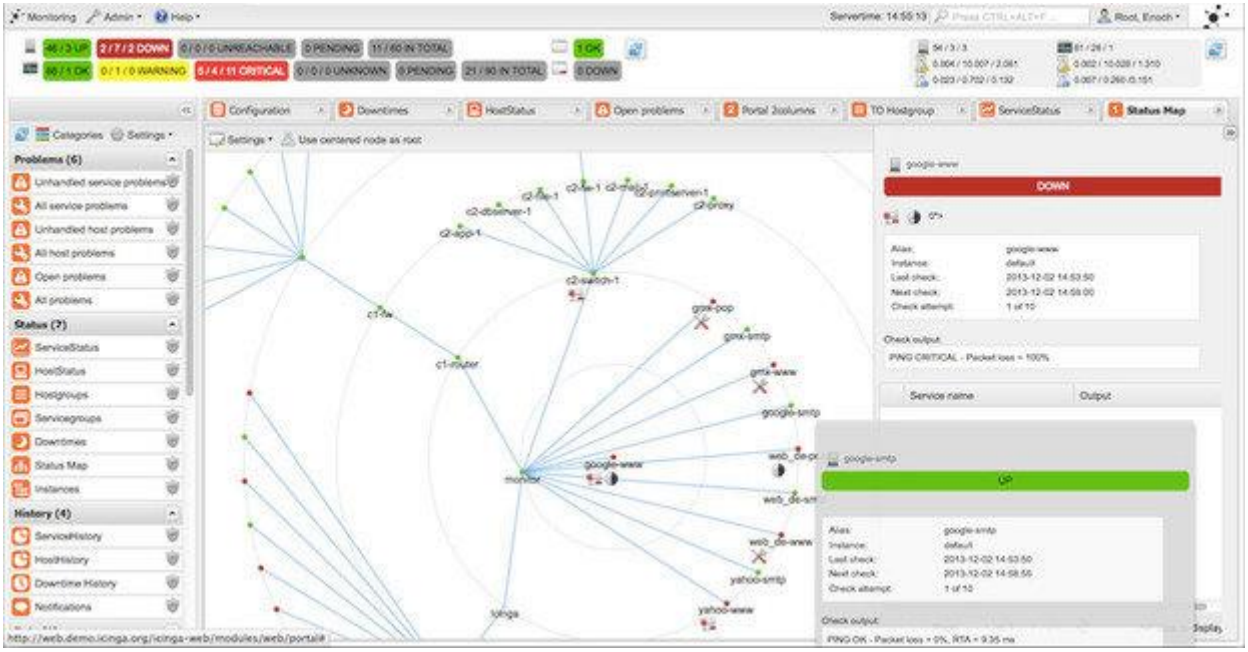

Рисунок 3.4 – Інтерфейс Icinga

Як і Nagios, система Icinga дозволяє здійснювати моніторинг всіх пристроїв, які використовують протокол IP, з можливістю глибокої інтеграції через SNMP. Крім того, Icinga підтримує використання плагінів і додатків, які можна налаштовувати відповідно до потреб користувача.

Одна з основних переваг Icinga порівняно з Nagios полягає в тому, що конфігурацію можна здійснювати через веб-інтерфейс, а не через редагування конфігураційних файлів вручну. Це дає користувачам, які віддають перевагу графічному управлінню системою, значну зручність.

Icinga також добре інтегрується з рядом програмних пакетів для моніторингу та візуалізації даних, таких як PNP4Nagios, ingraph і Graphite, що забезпечує гнучкість у відображенні інформації про мережу. Окрім цього, система підтримує розширену функціональність для створення детальних звітів.

3.1.5. Nedi

Якщо вам коли-небудь доводилося використовувати Telnet для пошуку пристроїв у мережі, підключаючись до комутаторів і перевіряючи Mac-адреси, або якщо ви хочете мати можливість визначати фізичне розташування вашого

обладнання (чи, що навіть важливіше, знати, де воно знаходилося раніше), то вам варто звернути увагу на Nedi.

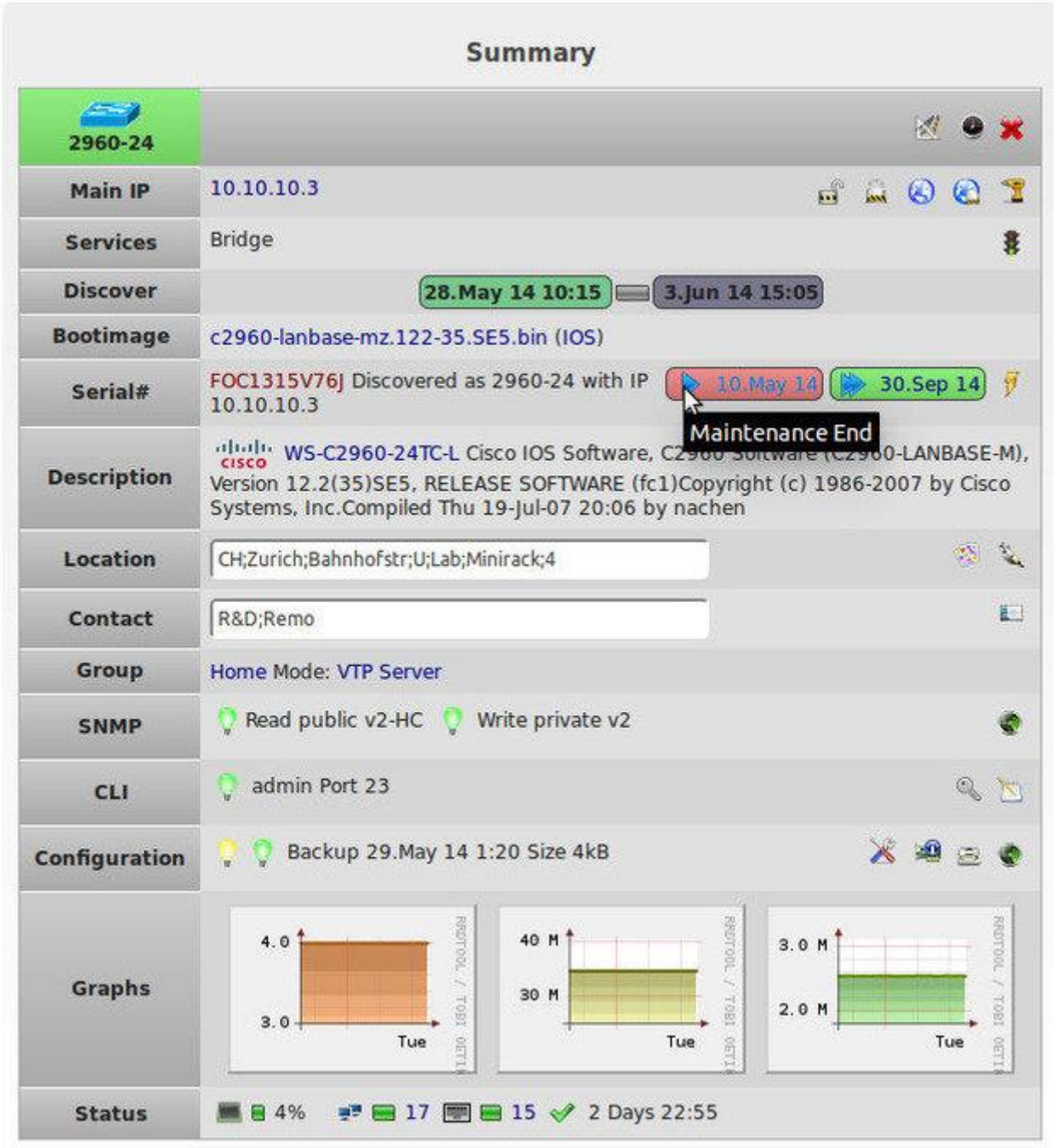

Рисунок 3.5 – Інтерфейс Nedi

Це безкоштовне програмне забезпечення, яке працює на LAMP платформі, регулярно перевіряє MAC-адреси та таблиці ARP на мережевих комутаторах, зберігаючи інформацію про кожен виявлений пристрій у локальній базі даних. Хоча Nedi не такий популярний, як інші рішення, він є

чудовим інструментом для управління корпоративними мережами, де пристрої постійно змінюються і переміщуються.

Через веб-інтерфейс Nedi дозволяє здійснювати пошук пристроїв за MAC-адресою, IP-адресою або DNS-іменем. Програма збирає детальну інформацію з кожного мережного пристрою, зокрема серійні номери, версії прошивки, конфігурації модулів, параметри часу тощо. Nedi можна використовувати для відстеження MAC-адрес втрачених або викрадених пристроїв — якщо ці пристрої знову з'являться в мережі, програма повідомить про це.

Процес виявлення пристроїв відбувається за допомогою cron з заданими інтервалами. Конфігурація досить проста, оскільки все налаштування зводиться до одного конфігураційного файлу, який дозволяє здійснювати гнучке налаштування, зокрема пропускати пристрої на основі регулярних виразів або меж мережі. Nedi використовує Cisco Discovery Protocol та Link Layer Discovery Protocol для виявлення нових комутаторів і маршрутизаторів, а також підключається до них для збору їхніх даних. Після початкової конфігурації процес виявлення пристроїв відбувається швидко.

В певних випадках Nedi можна інтегрувати з Cacti, що дає можливість прив'язати виявлені пристрої до графіків у Cacti для більш детального моніторингу.

3.1.6. Observium

Observium — це потужний інструмент для моніторингу мережевого обладнання та серверів, який підтримує велику кількість пристроїв, що використовують протокол SNMP. Як частина LAMP стеку, Observium відзначається простотою в установці та налаштуванні. Для цього потрібно здійснити стандартну установку Apache, PHP та MySQL, створити базу даних і налаштувати Apache. Програма працює як окремий сервер, з власною URL-адресою для доступу.

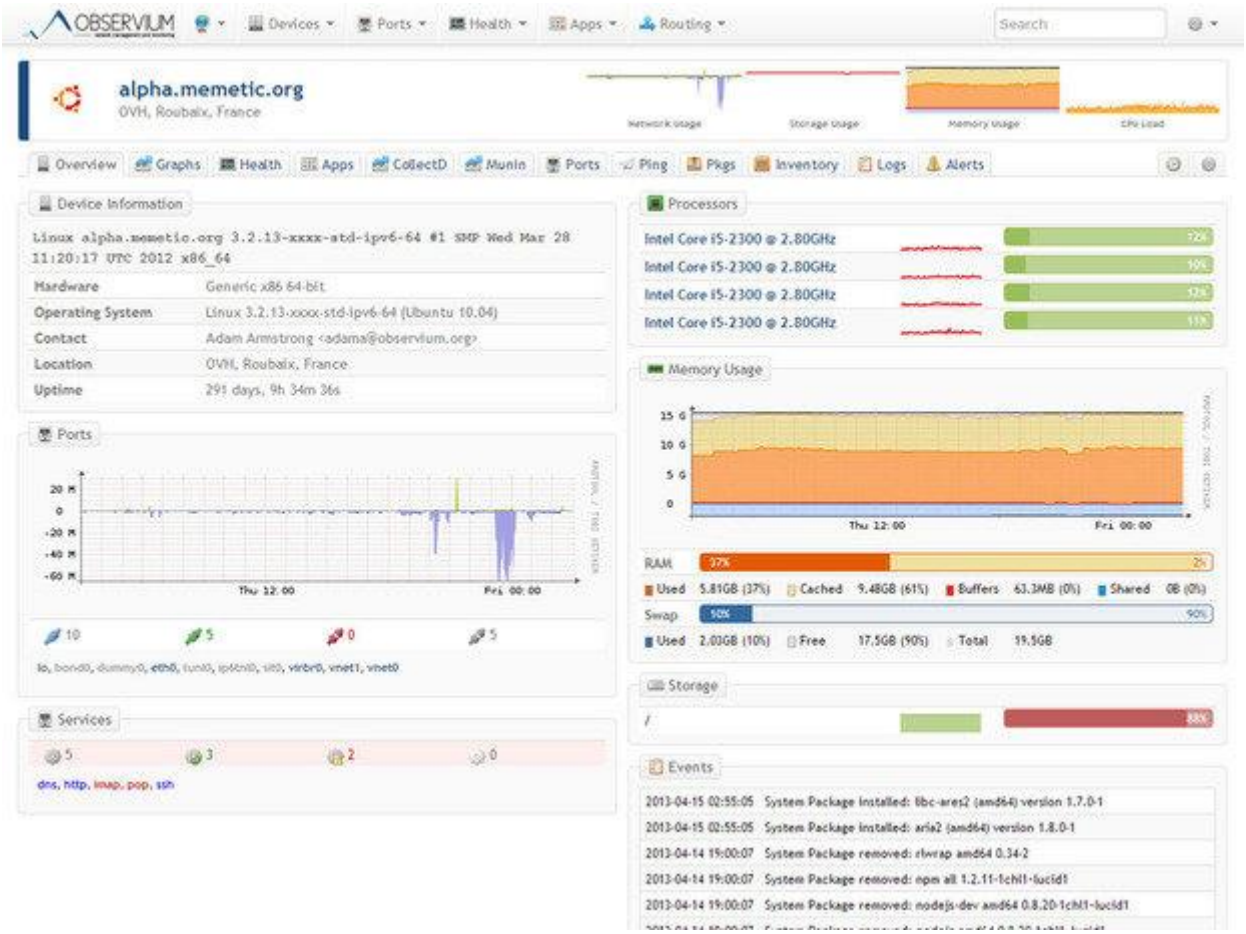

Рисунок 3.6 – Інтерфейс Observium

Observium поєднує в собі моніторинг систем і мереж з аналізом тенденцій продуктивності. Він може бути настроєний для відстеження практично будь-яких показників.

Observium об'єднує моніторинг систем та мереж з аналізом тенденцій продуктивності. Цей інструмент можна налаштувати для відстеження майже будь-яких показників.

Використовуючи графічний інтерфейс, можна додавати хости й мережі, налаштовувати діапазони для автоматичного виявлення та дані SNMP, що дозволяє Observium досліджувати мережу та збирати інформацію з кожної виявленої системи. Також підтримується виявлення мережевих пристроїв через CDP, LLDP чи FDP. Агентів можна розгортати на Linux-системах для збору додаткових даних.

Вся зібрана інформація доступна через зручний інтерфейс, що надає потужні можливості для статистичного відображення даних у вигляді діаграм і графіків. Користувач може отримати все, від часу відгуку ping і SNMP до графіків пропускної здатності, фрагментації та кількості IP-пакетів. Залежно від пристрою, ці дані можуть бути доступні для кожного виявленого порту.

Що стосується серверів, то Observium може показувати стан ЦП, ОЗП, сховищ, свопу, температури та інші параметри через журнал подій. Також можна збирати й візуалізувати продуктивність для різних сервісів, таких як Apache, MySQL, BIND, Memcached, Postfix та інших.

Observium також ефективно працює як віртуальна машина, що дозволяє йому стати основним інструментом для моніторингу стану серверів і мереж будь-якого масштабу. Це чудовий спосіб додати автоматичне виявлення та візуалізацію даних у мережу.

3.1.7. Zabbix

Zabbix є повноцінним рішенням для моніторингу мережі та систем, яке об'єднує різні функціональні можливості в одному веб-інтерфейсі. Він дозволяє налаштувати моніторинг і збір даних з різноманітних серверів та мережевих пристроїв, що забезпечує нагляд за їхнім станом та продуктивністю.

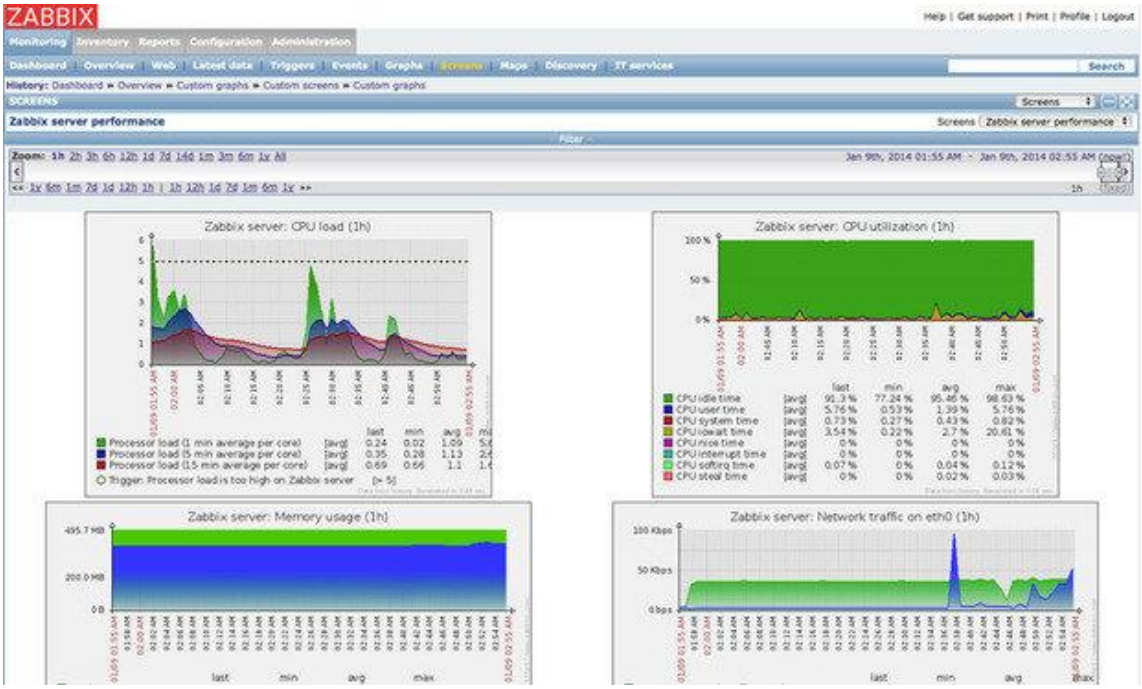

Рисунок 3.7 – Інтерфейс Zabbix

Zabbix надає потужні можливості для моніторингу серверів і мереж, включаючи підтримку віртуалізації та моніторинг веб-додатків. В основному він використовує програмні агенти, встановлені на контрольованих системах, але також може працювати без агентів через SNMP або інші протоколи. Zabbix підтримує гіпервізори, зокрема VMWare, забезпечуючи моніторинг продуктивності гіпервізора та його активності, а також додатково забезпечує підтримку серверів Java-додатків, веб-сервісів і баз даних.

Хости можуть бути додані вручну або автоматично, і Zabbix має широкий набір шаблонів для популярних операційних систем і сервісів. Це також дозволяє інтегрувати користувацькі перевірки, написані на різних мовах програмування, таких як Perl і Python.

Zabbix пропонує налаштування моніторингових панелей та інтерфейсу, що дозволяє зосередити увагу на найбільш важливих компонентах мережі. Можна налаштувати повідомлення й ескалацію подій з автоматичними діями, включаючи запуск віддалених команд на хостах.

Зібрані дані можуть бути представлені у вигляді графіків, карт та екранів, надаючи користувачеві зручний доступ до інформації. Хоча

початкове налаштування може бути складним, автоматичне виявлення та шаблони значно полегшують інтеграцію. Також є можливість запуску Zabbix як віртуального пристрою для популярних гіпервізорів.

3.1.8. The Dude

The Dude – це мережевий монітор від відомого латвійського виробника, досить простий у встановленні та використанні, але має дуже багаті можливості. До його переваг слід віднести низький поріг входу – ви можете почати використовувати продукт відразу, з налаштуваннями з коробки, не розбираючись у тонкощах налаштування. Так, в результаті вийде досить проста система, але вона працюватиме і її можна буде послідовно ускладнювати, додаючи ті чи інші функції. Такий підхід здається нам кращим, ніж спроби реалізувати відразу складну систему, не маючи належного досвіду роботи в даній галузі.

Серверна частина The Dude працює тільки в RouterOS, це означає, що буде потрібно або пристрій з його підтримкою, або віртуальна машина з Cloud Hosted Router (CHR).

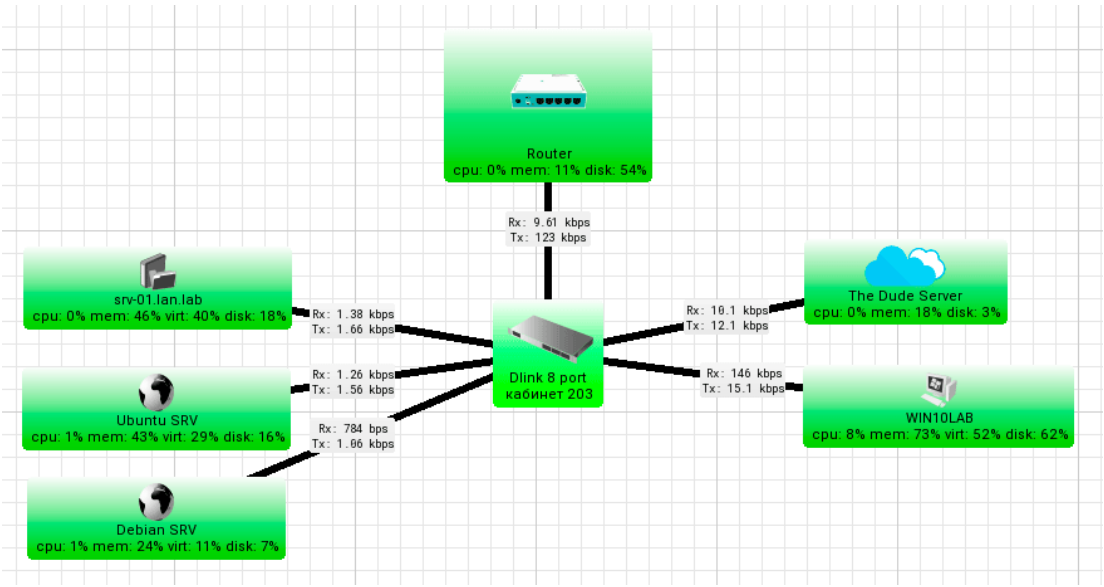

Рисунок 3.8 – Інтерфейс The Dude

Dude підтримує ICMP, SNMP моніторинг, а також безліч інших приємностей.

Переваги The Dude:

безкоштовний (Щоправда, останні версії вимагають придбання ліцензії на RouterOS, але для The Dude можна обійтися і 1 Демо Ліцензією);

дуже простий у встановленні та використанні;

дуже наочний.

3.2. Структура системи моніторингу

Структура системи наведена на рис. 3.9. Розгортання виконується на фізичний сервер, Proxmox VE 8.2 – віртуалізаційної платформи на базі відкритого коду, яка дозволяє створювати та керувати віртуальними машинами та контейнерами. Proxmox VE 8.2 забезпечує інтеграцію з KVM для віртуальних машин і LXC для контейнерів, а також надає можливості для роботи з кластерами та резервного копіювання.. У якості операційної системи платформи моніторингу використовується Linux Debian 12.

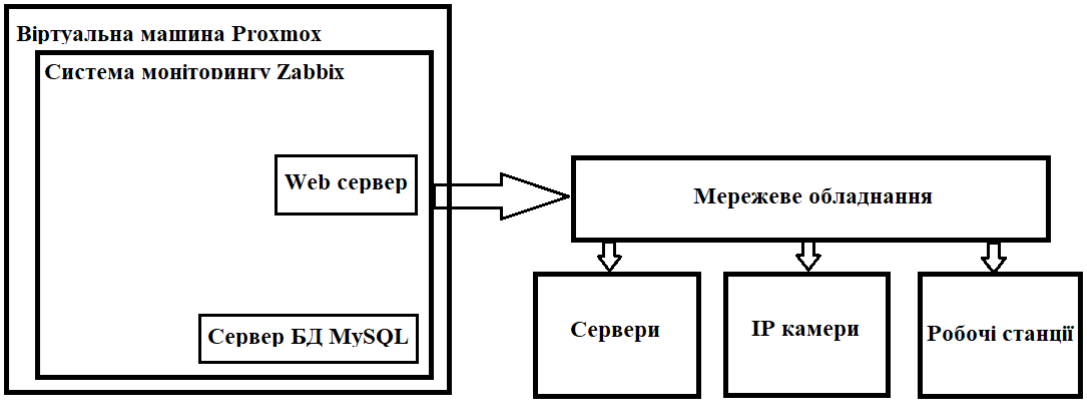

Рисунок 3.9 – Структурна схема системи

Моніторингова система на основі Zabbix

Zabbix – це потужна система моніторингу, яка дозволяє забезпечити контроль за мережевими пристроями, серверами та додатками. Основна мета

впровадження такої системи – спрощення роботи системного адміністратора, зокрема у випадку мережі навчального закладу, де система моніторингу значно полегшує відстеження стану обладнання та своєчасне реагування на неполадки.

Моніторингова система включає в себе такі компоненти:

Сервер моніторингу, який регулярно отримує та обробляє дані з підключених об'єктів, аналізує їх і при необхідності запускає скрипти для повідомлень про несправності або критичні ситуації.

Базу даних, яка може бути на основі MySQL, PostgreSQL, SQLite або Oracle. У ній зберігається вся інформація про стан мережі, попередження та історія збоїв.

Веб-інтерфейс, створений на PHP, що забезпечує доступ до даних моніторингу через зручний і гнучкий веб-інтерфейс, де можна отримувати звіти, налаштовувати параметри моніторингу та переглядати графіки.

Агент Zabbix, який встановлюється на моніторинговані пристрої та збирає інформацію про їх стан. Агент є опціональним – система також підтримує моніторинг за допомогою SNMP (версії 1, 2, 3), запуску зовнішніх скриптів, які надають необхідні дані, або використання вбудованих перевірок, таких як перевірка доступності через протоколи HTTP, SSH, FTP, ping тощо. Крім того, можна заміряти час відповіді сервісів для оцінки їх ефективності.

Такий підхід дозволяє не тільки вчасно виявляти проблеми, але й прогнозувати можливі відмови на основі зібраної статистики, що значно полегшує управління IT-інфраструктурою та підвищує її надійність.

					172.4397ст3.КР.ПЗ.Р4		
Змн.	*Арк.*	*№ документу*	*Підпис*	*Дата*			
Розробник		Пілявський О. І.			РОЗРАХУНКИ, ПІДТВЕРДЖУЮЧІ ПРАЦЕЗДАТНІСТЬ І НАДІЙНІСТЬ КОНСТРУКЦІЇ	*Літ.*	*Арк.* 33 / *Аркушів*
Консультант							
Н. контр.		Добрінова Л. П.				НУК імені адмірала Макарова	
Керівник		Трибулькевич С. Л.					
Зав. каф.		Рябенький В. М.					

РОЗДІЛ 4. РОЗРАХУНКИ, ПІДТВЕРДЖУЮЧІ ПРАЦЕЗДАТНІСТЬ І НАДІЙНІСТЬ КОНСТРУКЦІЇ

4.1. Розгортання віртуалізаційної платформи Proxmox

4.1.1. Загальні відомості Proxmox

Proxmox VE — це платформа віртуалізації, яка дозволяє керувати як віртуальними машинами на основі **KVM**, так і контейнерами на основі **LXC**. Однією з основних переваг Proxmox є його гнучкість і простота в управлінні. Інтерфейс Proxmox доступний через веб-браузер, що робить його зручним для адміністратора.

4.1.2. Основні компоненти Proxmox VE:

KVM (Kernel-based Virtual Machine), що забезпечує повну віртуалізацію, дозволяючи запускати ізольовані операційні системи з доступом до віртуального апаратного забезпечення. KVM використовує апаратну підтримку віртуалізації, яка присутня у процесорах Intel та AMD.

LXC (Linux Containers), яке забезпечує контейнеризацію, що дозволяє створювати ізольовані середовища для додатків, які поділяють ядро з хост-системою. Контейнери використовують менше ресурсів порівняно з повною віртуалізацією, оскільки їм не потрібно емулювати все апаратне забезпечення. Було прийнято рішення використовувати Proxmox, бо він надає наступні дії:

Легкість в управлінні надає веб-інтерфейс, який спрощує процес управління віртуальними машинами. Через інтерфейс можна створювати, запускати, зупиняти і керувати віртуальними машинами та контейнерами.

Підтримка кластеризації, яке дозволяє об'єднувати кілька серверів в єдиний кластер. Це підвищує стійкість до відмов, оскільки в разі збою одного сервера інші можуть автоматично взяти на себе його навантаження.

Моментальні знімки (Snapshots), дозволяє створювати резервні копії віртуальних машин або контейнерів в поточному стані. Це корисно для відновлення у разі помилок або збоїв.

В ході вибору системи віртуалізації було порівняно KVM та LXC:

KVM є повноцінною віртуалізацією, що дозволяє запускати окремі операційні системи з доступом до віртуальних апаратних ресурсів. Це може бути корисно для запуску Windows або інших не-Linux операційних систем.

LXC є легшою віртуалізацією і краще підходить для Linux-додатків. Він використовує ядро хост-системи і займає менше ресурсів.

4.1.3. Встановлення та налаштування Proxmox

4.1.3.1. Підготовка

Для того щоб завантажити останню версію Proxmox VE треба, спочатку перейти на офіційний сайт Proxmox VE та завантажити останню версію ISO-файлу. Це забезпечило доступ до всіх найновіших оновлень та функцій системи віртуалізації.

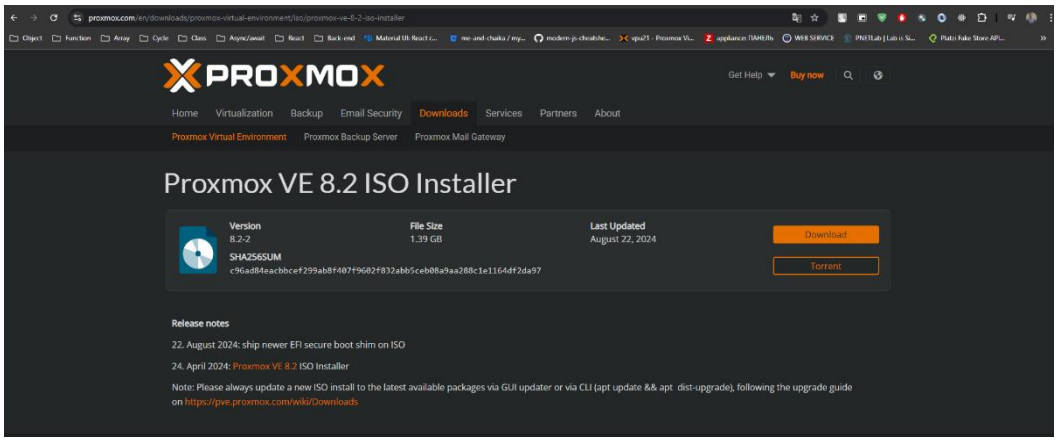

Рисунок 4.1 – Офіційний сайт Proxmox

Для створення завантажувального USB-накопичувача використано програму Rufus, яка дозволяє швидко підготувати USB-носій до завантаження, завантаживши на нього ISO-файл Proxmox. Це зручний інструмент для роботи на Windows, оскільки дозволяє легко зробити накопичувач завантажувальним.

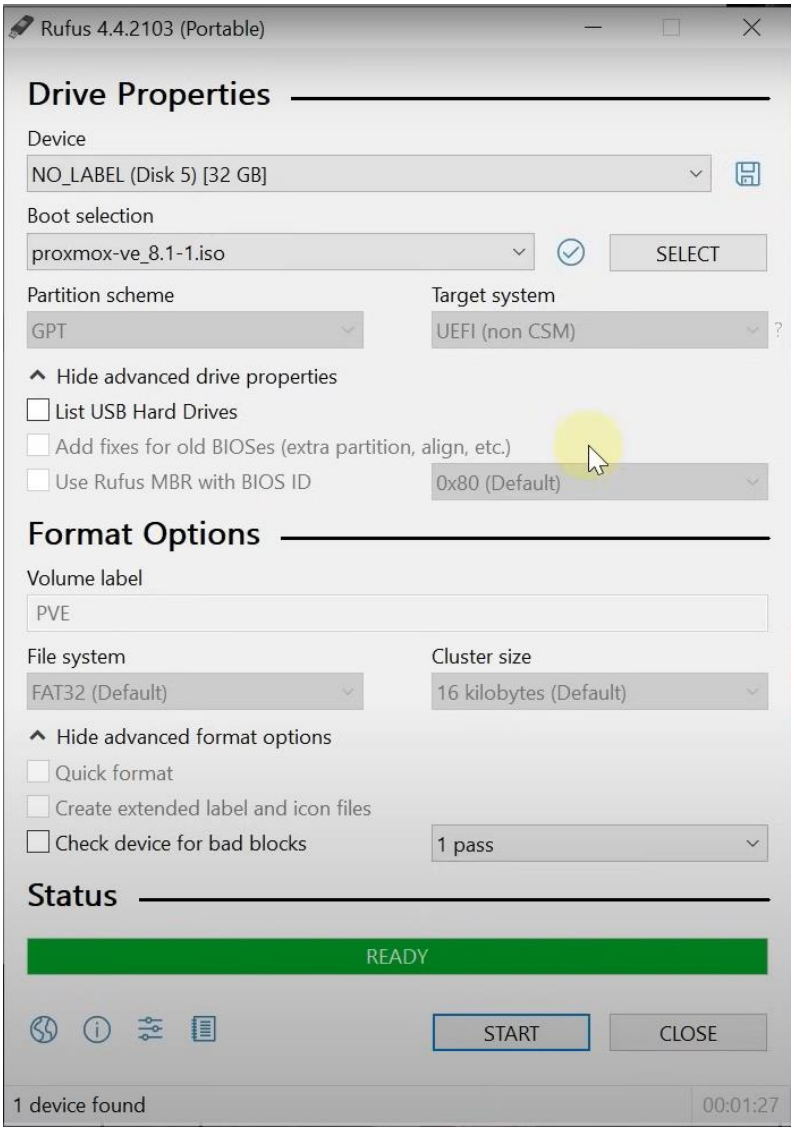

Рисунок 4.2 – Створення завантажувального носія

4.1.3.2. Встановлення Proxmox VE

Після підключення USB-накопичувача до сервера налаштовано BIOS для завантаження з USB. Після перезавантаження сервер автоматично завантажив інсталяційне середовище Proxmox.

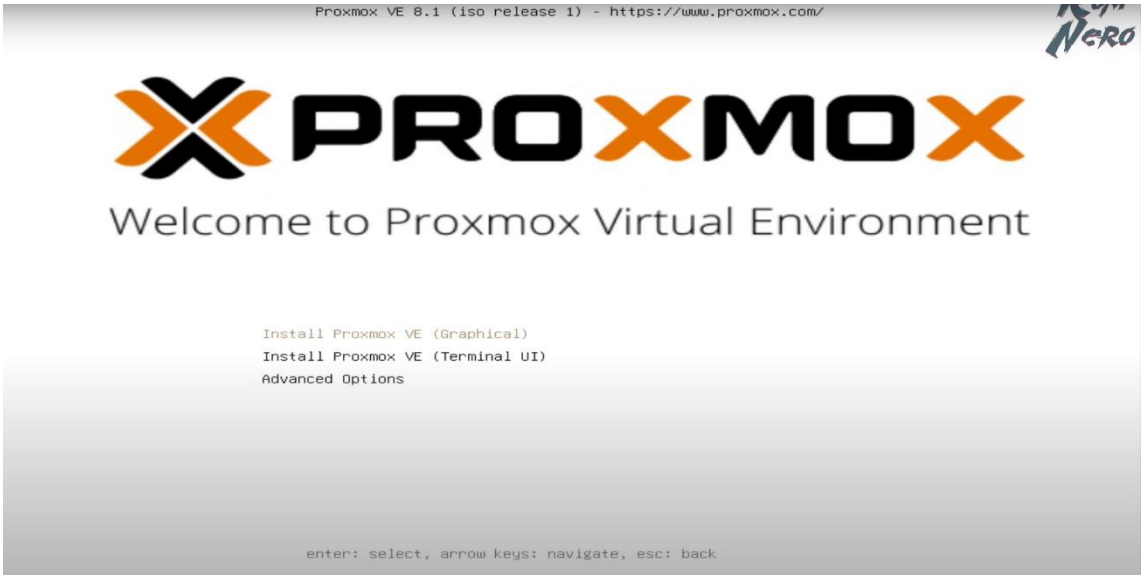

Рисунок 4.3 – Завантаження з USB-накопичувача

У стартовому меню обрано опцію «Install Proxmox VE».

Для продовження інсталяції «Прийнятя умови ліцензійної угоди».

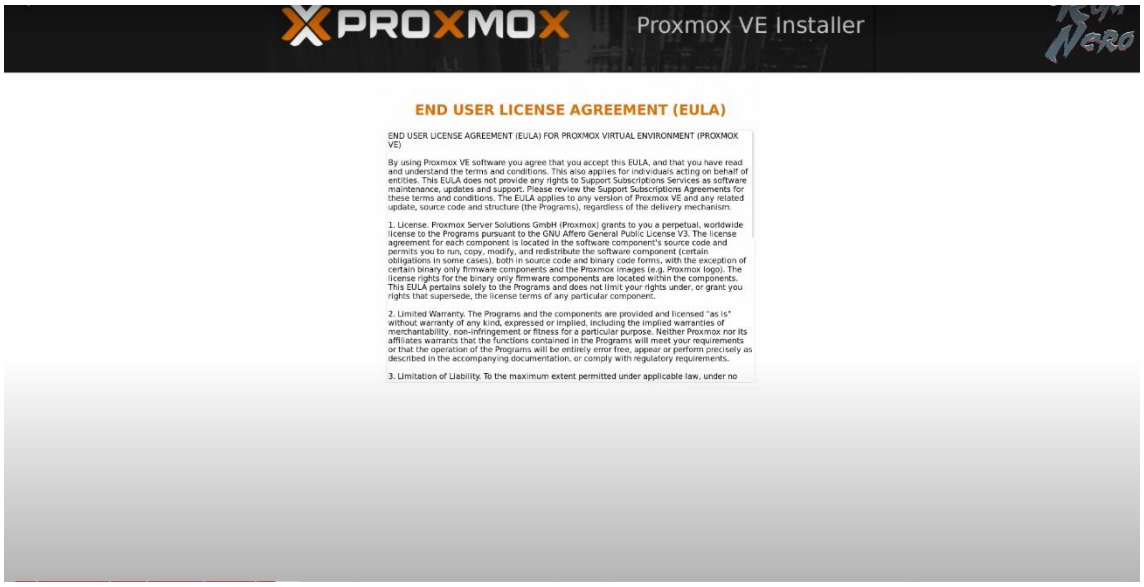

Рисунок 4.4 – Прийняття ліцензійної угоди

Вибір диска для встановлення: Обрано диск для встановлення Proxmox — SSD диск ємністю 256 ГБ. Було важливо переконатися, що всі важливі дані були збережені, оскільки диск буде відформатовано.

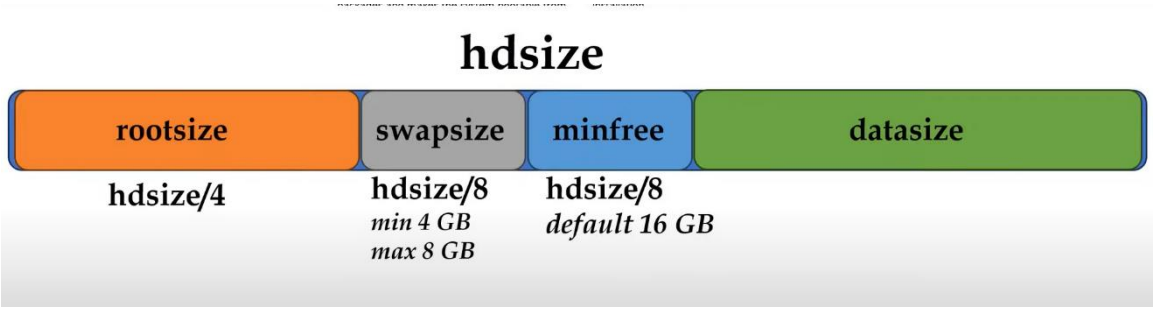

Рисунок 4.5 – Автоматичне створення дисків Proxmox

Було автоматично створено розділи диска для кореневої файлової системи, підкачувальної пам'яті, резерву та користувацьких даних відповідно до загальної ємності диска.

rootsize: Цей розділ призначений для кореневої файлової системи і зазвичай отримує чверть від загального розміру диска (позначено як `hdsize/4`), забезпечуючи достатньо місця для системних файлів.

swapsize: Цей розділ використовується як підкачувальна пам’ять (swap), яка допомагає при нестачі оперативної пам'яті. Розмір swap обчислюється як `hdsize/8`, з мінімумом 4 ГБ і максимумом 8 ГБ.

minfree: Це мінімальний резерв вільного місця на диску, щоб уникнути повного заповнення. За замовчуванням для цього резерву виділяється `hdsize/8`, або 16 ГБ.

datasize: Цей розділ містить решту доступного дискового простору і призначений для зберігання користувацьких даних та віртуальних машин.

Таким чином, Proxmox ділить простір на критичні частини для системи, підкачувальної пам'яті, резерву та даних, автоматично визначаючи їхній розмір відповідно до загальної ємності диска.

Введення країни, часового поясу та розкладки клавіатури: Встановлено параметри для України:

Часовий пояс: UTC +2:00 (Київський час).

Розкладка клавіатури: Англійська та Українська.

Створення облікового запису адміністратора (root): Для адміністратора системи задано пароль Admin-vpu21 та вказано email-адресу (pilyavskiy_o_i@mk.vpu21.com.ua) для отримання системних повідомлень.

4.1.4. Налаштування мережі та імені сервера

Для налаштування мережі було зроблені такі дії:

– Введено IP-адресу сервера — 192.168.111.3, яка відповідає локальній мережі.

– Використано стандартну маску підмережі 255.255.255.0 для локальної мережі.

– Вказано IP шлюзу мережі: 192.168.111.1, який підключає сервер до зовнішніх мереж.

– Введено два DNS-сервери:

192.168.111.1 – локальний DNS сервер.

8.8.8.8 – DNS сервер Google для додаткової надійності.

– Введено назву сервера vpu21, яка буде використовуватися для ідентифікації цього хоста в Proxmox та в локальній мережі.

4.1.5. Фіналізація установки

Після введення всіх необхідних даних натиснуто кнопку Install для початку встановлення. Після завершення установки сервер автоматично перезавантажився.

4.1.6. Перший вхід в Proxmox VE

Після перезавантаження було відкрито веб-браузер на іншому комп'ютері в мережі та введено адресу: https://192.168.111.3:8006

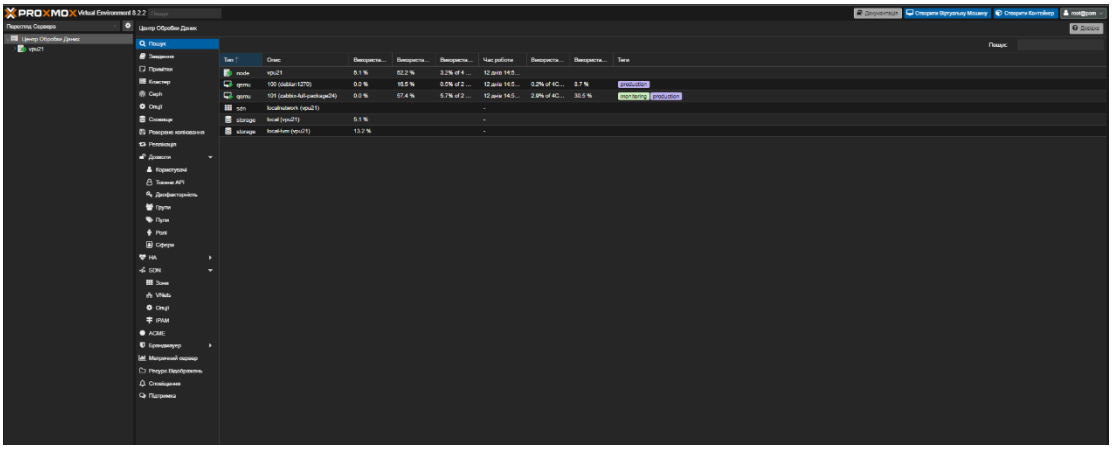

Рисунок 4.6 – Перший вхід в Proxmox VE

Оскільки Proxmox використовує самопідписаний SSL-сертифікат, браузер видав попередження про незахищене з'єднання, для якого було додано виняток.

Вхід в систему: Виконано вхід з обліковими даними адміністратора:

Логін: root

Пароль: Admin-vpu21

Базові налаштування після встановлення

Після входу в веб-інтерфейс або через термінал виконано команди для оновлення системи:

```
apt update && apt full-upgrade
```

Це оновило систему до останніх стабільних версій програмного забезпечення та виправило потенційні проблеми безпеки.

Таким чином, сервер Proxmox успішно налаштований, і тепер він готовий до подальшого використання для створення та керування віртуальними машинами.

4.2. Розгортання системи моніторингу Zabbix 7.0 готове рішення

4.2.1. Загальні відомості Zabbix

Zabbix — це система моніторингу, яка дозволяє відстежувати стан серверів, мережевих пристроїв, додатків та інших ресурсів у реальному часі. Вона підтримує різноманітні протоколи збору даних і надає можливість створювати власні тригери, графіки, дашборди та сповіщення.

Основні можливості Zabbix 7.0:

– Zabbix Agent встановлюється на сервер або комп'ютер і збирає інформацію про використання ресурсів (CPU, RAM, диск, мережеві інтерфейси).

– Zabbix підтримує SNMP для збору інформації з мережевих пристроїв, таких як комутатори, маршрутизатори та інші елементи інфраструктури.

– Zabbix дозволяє створювати графіки продуктивності та дашборди, на яких можна відстежувати в режимі реального часу стан всіх моніторованих пристроїв.

– Система дозволяє налаштовувати тригери, які активуються у випадку збоїв, і надсилати сповіщення через різні канали (email, SMS, Telegram).

Було прийнято рішення використовувати Zabbix, бо він надає наступні дії:

Масштабованість: система може обробляти дані з тисяч пристроїв одночасно.

Гнучка система моніторингу: підтримка різних типів моніторингу (агент, SNMP, ICMP, HTTP, FTP).

Автоматизація: можливість автоматизувати дії у разі збоїв (наприклад, перезапуск сервера, якщо спостерігається проблема з процесором або мережею).

4.2.2. Встановлення та налаштування Zabbix

Підготовка до розгортання

На сервері з ім'ям "vpu21" з IP-адресою `192.168.111.3`, який працює на **Proxmox VE 8.2**, була здійснена підготовка до розгортання моніторингової системи Zabbix 7.0. Першим кроком стало завантаження готового **ISO-файл Zabbix** з офіційного сайту. Це ISO-зображення містить усі необхідні компоненти для автоматичної установки сервера Zabbix на базі операційної системи Linux.

Для забезпечення успішного процесу розгортання було виконано наступні попередні дії:

Перед тим як створювати віртуальну машину, необхідно було переконатися, що всі пакунки на сервері актуальні. Це можна зробити за допомогою команди:

```
apt update && apt upgrade
```

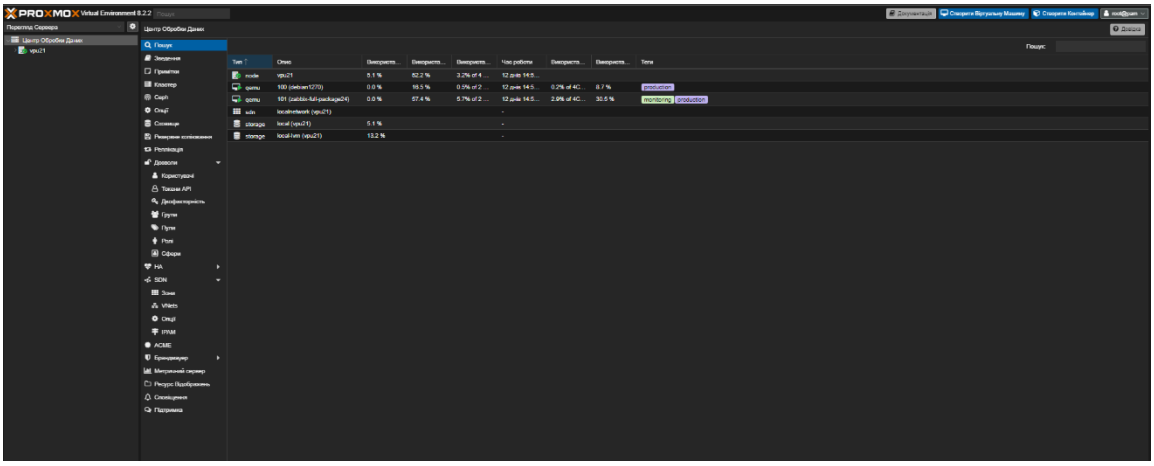

Рисунок 4.7 – Вхід в Proxmox VE

Для встановлення Zabbix, ISO-образ було завантажено в Proxmox через веб-інтерфейс у розділ ISO Images, використовуючи кнопку Upload для додавання файлу до сховища.

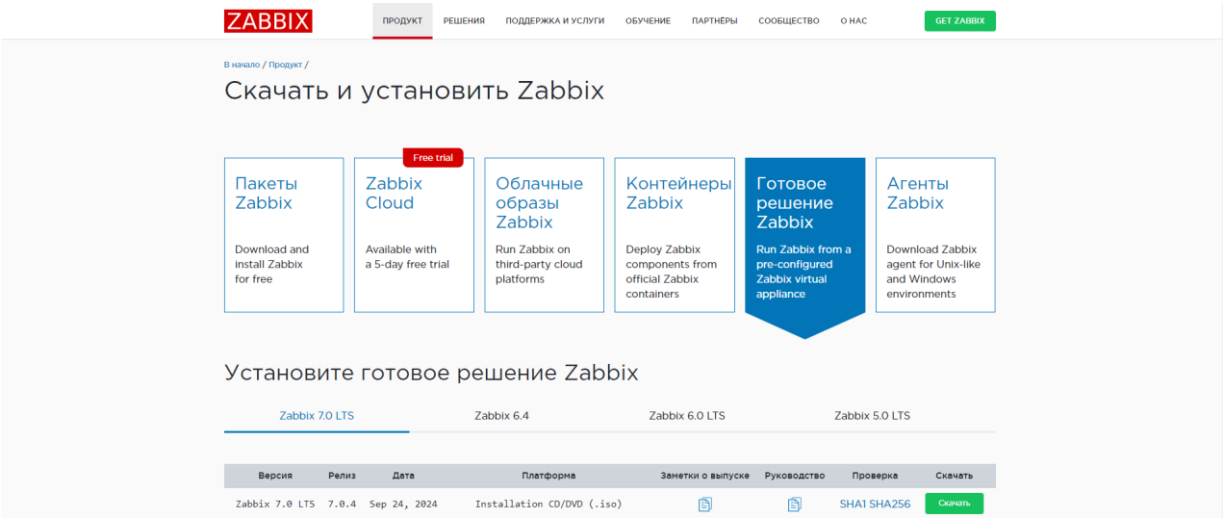

Рисунок 4.8 – Офіційний сайт Zabbix

4.2.3. Створення віртуальної машини в Proxmox

Для розгортання Zabbix 7.0 на віртуальній машині у Proxmox було виконано такі кроки:

– Перейдено за адресою https://192.168.111.3:8006.

– У головному інтерфейсі обрано вузол "vpu21" для створення віртуальної машини.

– У розділі Create VM створено нову віртуальну машину з такими параметрами:

– Призначено унікальний ідентифікатор для віртуальної машини.

– **Ім'я віртуальної машини**: "zabbix-full-package24" для легкої ідентифікації.

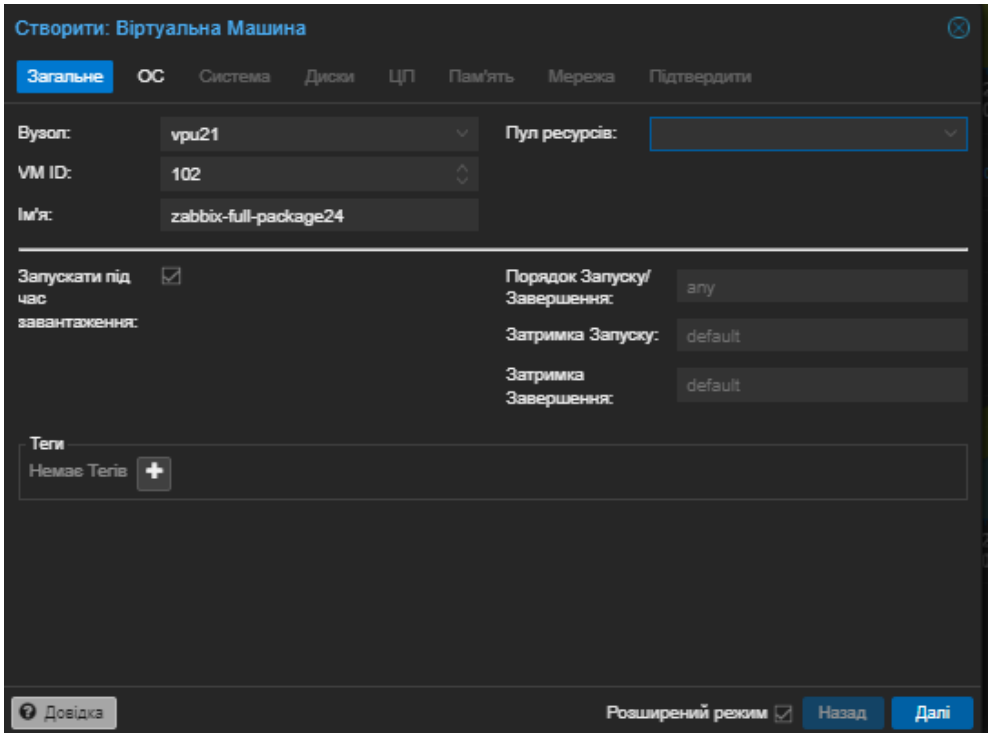

Рисунок 4.9 – Загальні налаштування віртуальної машини

4.2.4. **Налаштування ISO-образу**:

Обрано раніше завантажений ISO-образ Zabbix 7.0 зі сховища.

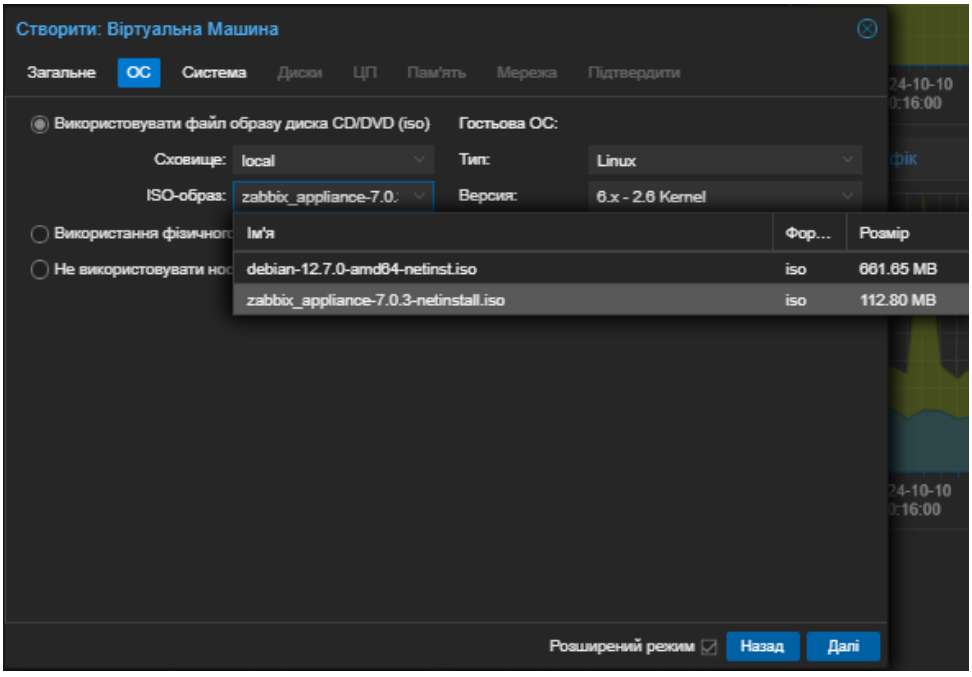

Рисунок 4.10 – Обрання завантаженого ISO-образ Zabbix 7.0

4.2.5. **Конфігурація апаратних ресурсів**:

CPU: Виділено 2 ядра для обробки завдань Zabbix.

RAM: Призначено 8 GB оперативної пам'яті, що відповідає базовим потребам для невеликих інсталяцій.

Жорсткий диск: Виділено 60 GB простору на диску, достатнього для зберігання даних та логів моніторингу.

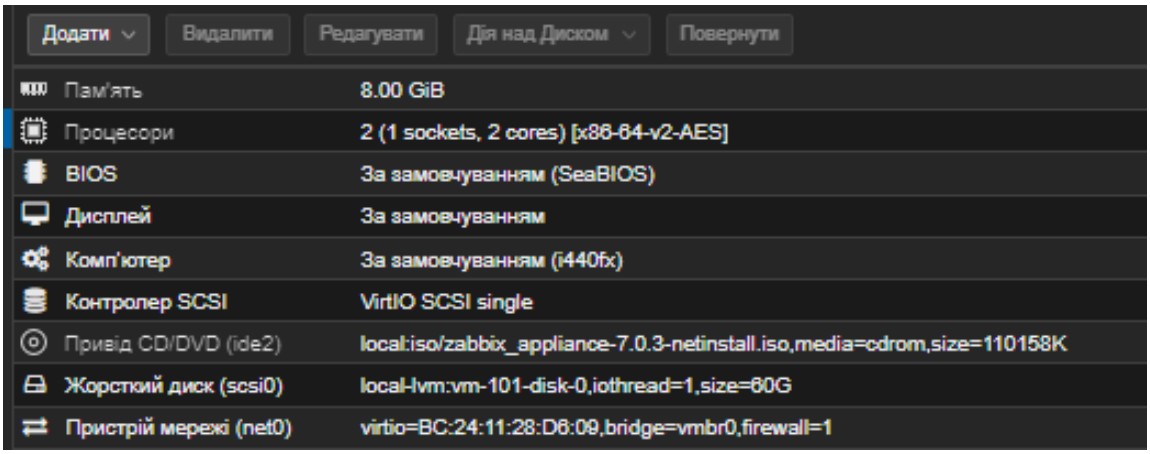

Рисунок 4.11 – Конфігурація апаратних ресурсів

4.2.6. **Налаштування мережі**:

Налаштовано мережевий інтерфейс для використання статичної IP-адреси 192.168.111.120, що забезпечує стабільний доступ до веб-інтерфейсу Zabbix.

Фіналізація створення: Після введення всіх параметрів натиснуто кнопку Finish для завершення створення віртуальної машини.

4.2.7. Установка Zabbix 7.0

Після створення віртуальної машини було запущено процес установки Zabbix 7.0:

– Вибрано щойно створену машину у списку та натиснув кнопку **Start** для її запуску.

– Підключено до консолі віртуальної машини через веб-інтерфейс Proxmox для прямого керування процесом установки.

Процес установки:

Установник Zabbix ISO автоматично розпочався, і обрано повну установку для автоматичної конфігурації всіх компонентів (веб-сервера, бази даних MySQL та Zabbix-сервера).

На одному з етапів було запропоновано створити користувача з адміністративними правами. Вказано логін **root** і пароль **zabbix** для адміністратора.

Після успішної інсталяції, машина автоматично перезавантажилася, і Zabbix-сервер розпочав свою роботу.

4.2.8. Налаштування Zabbix 7.0

Після установки системи Zabbix було проведено початкові налаштування:

– **Доступ до веб-інтерфейсу**:

– Відкрито браузер і перехід за адресою `http://192.168.111.120/zabbix`

– Вхід у систему з обліковими даними адміністратора:

Логін: Admin

Пароль: zabbix

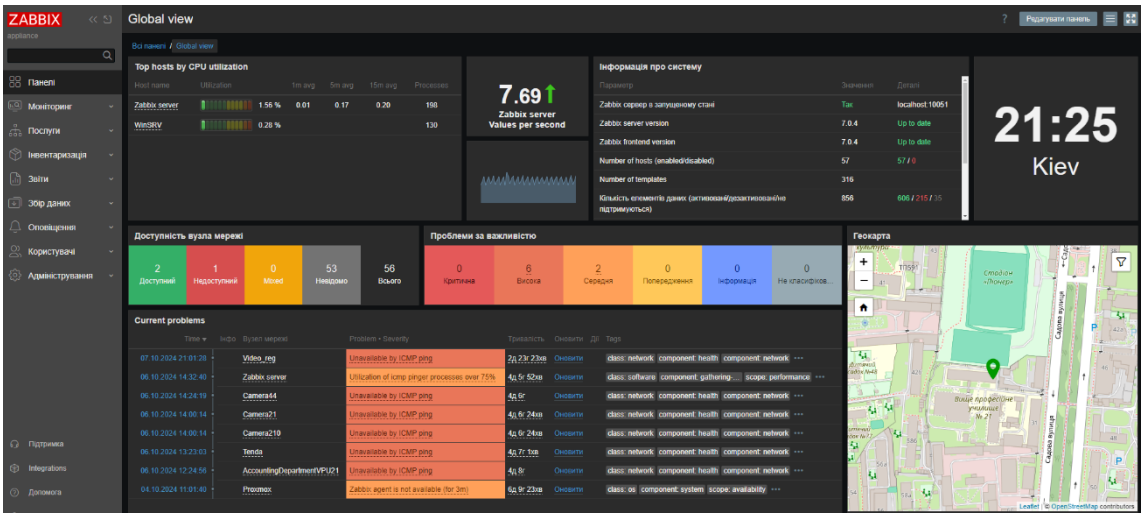

Рисунок 4.12 – Перший запуск в веб браузері

Додавання користувачів:

Перейдено до налаштувань користувачів для додавання нових.

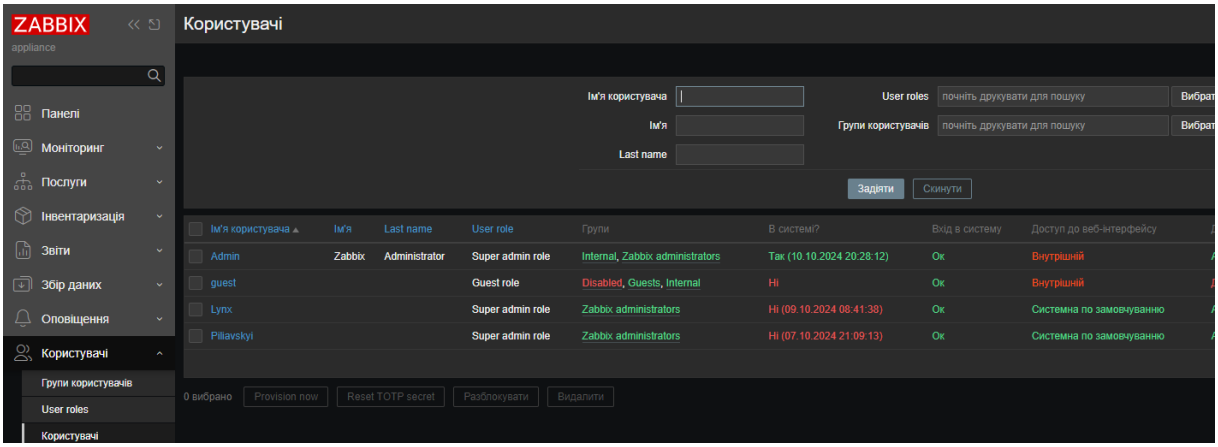

Рисунок 4.13 – Налаштування користувачів

Додано нового користувача Piliavskyi з паролем Admin-vpu21 для адміністративного доступу.

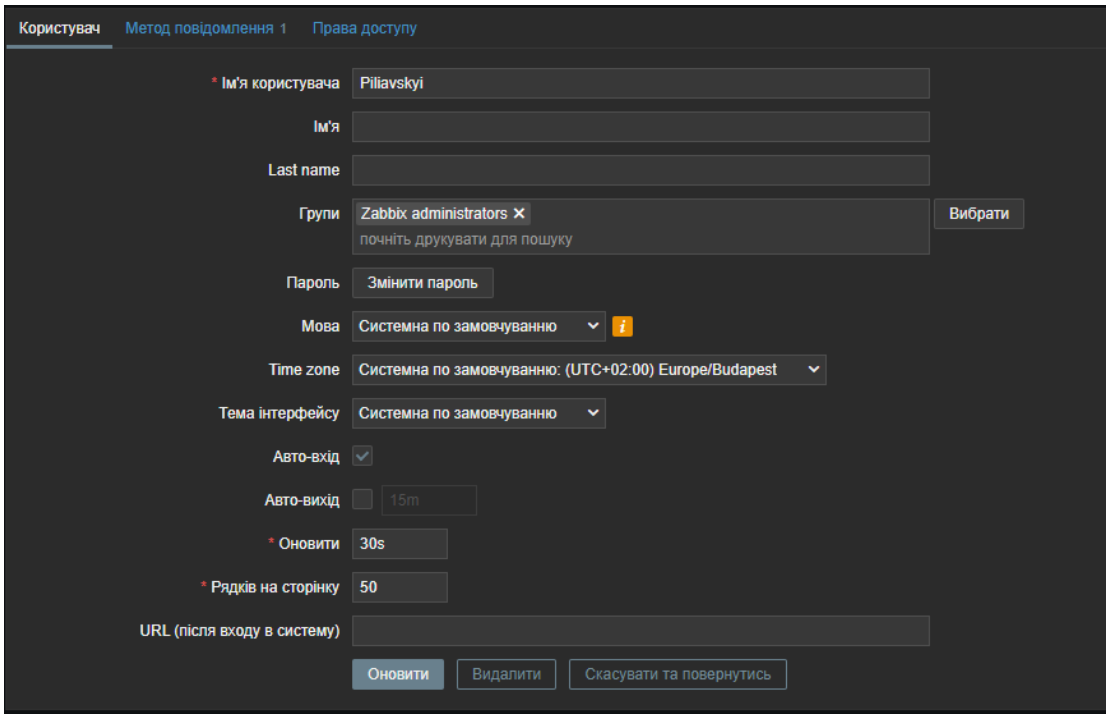

Рисунок 4.14 – Додавання нового користувача Piliavskyi

Також створено додаткового користувача Lynx для можливості обмеженого доступу, якщо необхідно додатково залучити інших операторів.

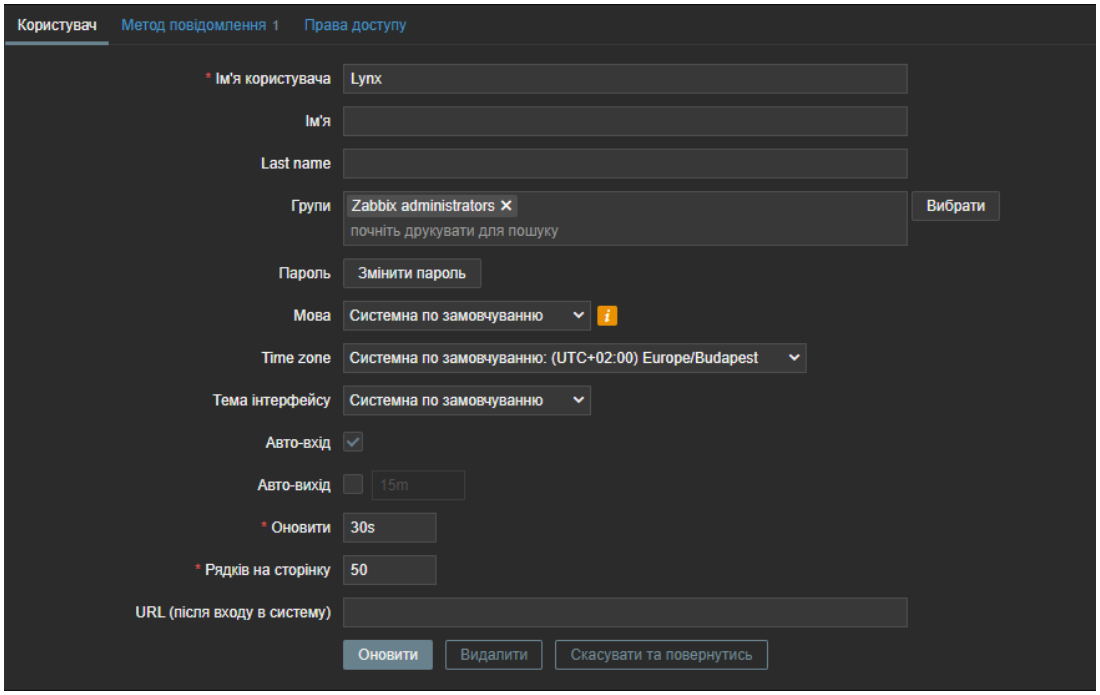

Рисунок 4.14 – Додавання нового користувача Lynx

Налаштування сервера Zabbix:

Встановлено основні параметри конфігурації, включаючи:

Часову зону UTC +2:00 (Київський час).

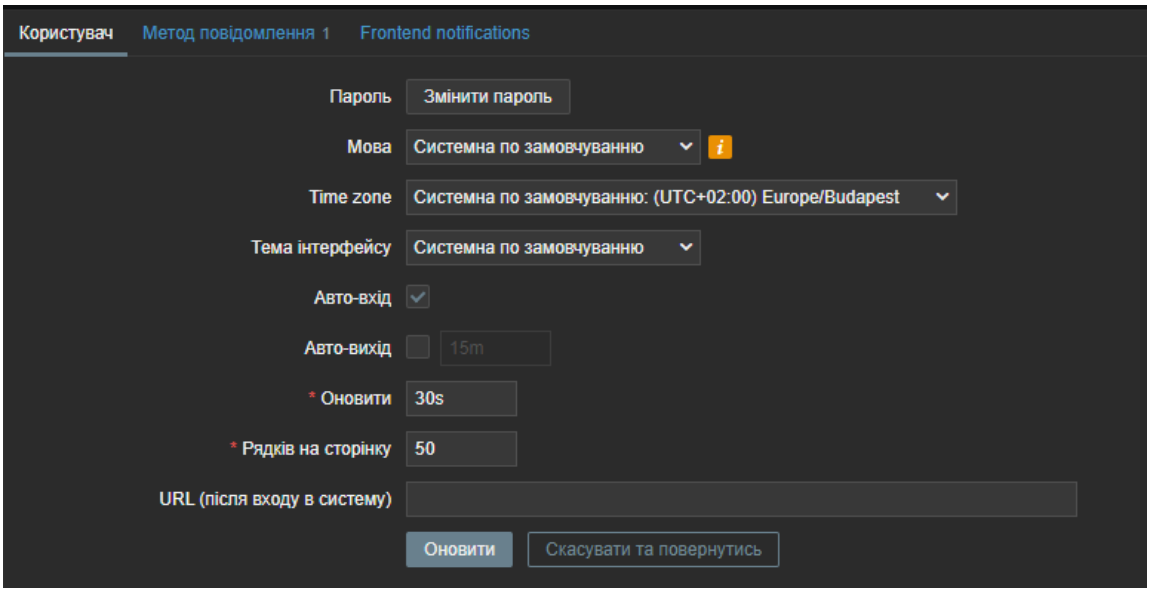

Рисунок 4.15 – Основні параметри конфігурації

Підключення до бази даних: У процесі установки система автоматично створила та підключила базу даних MySQL для зберігання інформації про

моніторинг. Перевірено конфігурації підключення до бази даних через веб-інтерфейс.

4.3. Додавання вузлів мережі до **Zabbix**

В рамках реалізації моніторингової системи в навчального закладу, було використано рішення на базі Zabbix 7.0, що дозволяє централізовано контролювати роботу різних пристроїв і серверів в мережі навчального закладу.

Загальний список груп вузлів мережі:

Applications: MicroTik 3011 router.

Databases: WinSRV.

Discovered hosts: WinSRV.

Hypervisors: Proxmox.

IP cam: Camera21, Camera44, Camera201, Camera203, Camera204, Camera205, Camera206, Camera207, Camera208, Camera209, Camera210, Camera211, Camera212, Camera213, Camera214, Camera215, VideoReg, Video_reg.

Linux servers: Proxmox.

Virtual machines: Proxmox.

Wi-Fi: AccountingDepartmentVPU21, CableWireProcessing, Director, ElectronicEngineer, EnglishKab9, Hurtovzhytok-1-1, Kab-14, Kab07, Kab12, Kab13, Kab17, Kab19, Kab20, Kab22, Kab23, Kab26, Kab27, Kab28, Kab33, Kab43, Kab47, Kab53, LaboratoryShipElectrical, Library, MastersRoom, Methodist, Polygraphy, PrimalCommission, Psychologist, SeniorMaster, SeniorMasterElectrician, soc_robota, Teachers, TechnologyElectricalWorks, Tenda.

Zabbix servers: Zabbix server.

Основою моніторингу були наступні критичні компоненти інфраструктури:

4.3.1. **Маршрутизатори**

Основною точкою доступу та управління мережею навчального закладу є MicroTik 3011 router, який виконує роль маршрутизатора і дозволяє організувати ефективний контроль трафіку і підключень у мережі. Маршрутизатор є ключовим елементом мережі, тому його стан, продуктивність та навантаження ретельно моніторяться за допомогою Zabbix.

4.3.2. **Wi-Fi мережі**

У навчального закладу діє велика кількість точок доступу Wi-Fi, що забезпечують підключення як для співробітників, так і для студентів. До моніторингу підключено 35 Wi-Fi вузлів, таких як:

AccountingDepartmentVPU21

CableWireProcessing

Director

Kab (різні кабінети) і багато інших.

Кожна з цих точок моніториться з метою забезпечення безперебійного інтернет-з'єднання, нагляду за навантаженням та забезпечення захищеності від можливих атак.

4.3.3. Сервери

Одним з основних серверів, які використовуються в інфраструктурі, є Windows Server 2022 (в групі під іменем WinSRV). Він виконує роль файлового, поштового або ж базового серверного рішення для навчального закладу. Zabbix контролює ключові параметри роботи сервера, включаючи навантаження на процесор, використання оперативної пам'яті, стан дисків та мережеву активність.

Також до моніторингу підключено Zabbix server, який є центральним вузлом для збору всіх даних і сповіщень від усіх інших елементів мережі. Це

рішення дозволяє адміністратору оперативно отримувати інформацію про всі критичні події у мережі.

4.3.4. **IP камери та відеореєстратор**

Мережа навчального закладу також включає в себе систему відеоспостереження. Було додано 18 IP-камер, серед яких:

Camera21

Camera44

Camera201 *до* ***Camera215***

VideoReg *та* ***Video_reg.***

Ці камери разом із відеореєстратором забезпечують відеоспостереження за периметром та внутрішніми приміщеннями навчального закладу. Система моніторингу дозволяє відстежувати стан підключення кожної з камер, а також забезпечує контроль доступності відеореєстратора, що є критично важливим для безпеки закладу.

4.3.5. **Proxmox сервер**

Інфраструктура навчального закладу також включає в себе віртуалізаційну платформу на базі **Proxmox**, яка дозволяє керувати віртуальними машинами, такими як **Windows Server** або **Zabbix server**. Моніторинг Proxmox дозволяє отримувати інформацію про стан гіпервізора, ресурси віртуальних машин, навантаження на процесор та інші показники.

Моніторингова система в навчального закладу на базі Zabbix 7.0 забезпечує контроль за ключовими компонентами інфраструктури, такими як маршрутизатори (MicroTik 3011 router), Wi-Fi вузли, сервери (Windows Server 2022, Zabbix server), IP-камери та відеореєстратор, а також платформа віртуалізації Proxmox. Це рішення дозволяє швидко реагувати на будь-які проблеми у мережі та забезпечує безперебійну роботу всіх важливих систем закладу.

Вже успішно додано та налаштувано всі важливі вузли мережі в системі моніторингу Zabbix на базі наявної інфраструктури навчального закладу. Нижче наведений опис декількох вузлів мережі:

AccountingDepartmentVPU21

Вузол був доданий до моніторингу з використанням шаблону ICMP Ping для контролю його доступності.

Вузол включений до групи Wi-Fi, що відповідає його призначенню як точки доступу в мережі Wi-Fi закладу.

Вказано DNS-ім'я AccountingDepartmentVPU21 для забезпечення моніторингу через агент на порту 10050.

Camera201

IP-камера Camera201 була додана до групи IP cam і налаштована для моніторингу через шаблон ICMP Ping.

Для моніторингу камери використовується її IP-адреса 192.168.100.201. Підключення відбувається через агент на порту 10050.

Це дозволяє системі відстежувати доступність камери та оперативно реагувати на можливі збої.

Kab53

Wi-Fi точка доступу Kab53 була налаштована і додана до групи Wi-Fi.

Вузол моніториться через шаблон ICMP Ping для перевірки його доступності.

Вказано DNS-ім'я Kab53.vpu21.local з підключенням через агент на порту 10050.

MicroTik 3011 router

Маршрутизатор MicroTik 3011 router налаштований для моніторингу за допомогою SNMP, з використанням шаблону MikroTik RB3011UiAS-RM by SNMP.

Включений до групи Applications, що дозволяє відстежувати його роботу та мережеву активність.

Для SNMP підключення використовується IP-адреса 192.168.111.1 з портом 161.

VideoReg

Відеореєстратор VideoReg був доданий для моніторингу за допомогою шаблону ICMP Ping для перевірки доступності.

Вузол додано до групи IP cam, яка включає всі пристрої відеоспостереження.

Для моніторингу використовується IP-адреса 192.168.100.200, що підключається через агент на стандартному порту 10050.

WinSRV

Сервер WinSRV був налаштований для моніторингу з використанням шаблону Windows by Zabbix agent, що дозволяє збирати інформацію про стан операційної системи Windows.

Вузол додано до групи Discovered hosts, оскільки він був автоматично виявлений системою Zabbix.

Використовується IP-адреса 192.168.111.2 з підключенням через Zabbix агент на порту 10050.

Ці вузли мережі вже налаштовані для постійного моніторингу, і система Zabbix забезпечує контроль за їх доступністю, роботою, та можливими збоями. Завдяки цьому, будь-які проблеми з мережевим обладнанням чи точками доступу можуть бути швидко виявлені і вирішені.

4.4. Додавання карт мережі до **Zabbix**

4.4.1. Загальні відомості мережі в навчального закладу

Мережа в навчального закладу є важливою складовою інфраструктури закладу, яка забезпечує безперебійну роботу освітніх і адміністративних процесів. Основною метою мережі є підтримка надійного з'єднання для викладачів, студентів, адміністрації та технічного персоналу. Мережа охоплює

як внутрішні системи (сервери, локальні мережі), так і зовнішні (підключення до інтернету), що робить її важливим компонентом для виконання навчальних та управлінських завдань.

Основні компоненти мережі включають:

Маршрутизатори і комутатори, що розподіляють мережевий трафік між підключеними пристроями.

Точки доступу Wi-Fi для забезпечення бездротового з'єднання в аудиторіях, гуртожитках і адміністративних приміщеннях.

Сервери, які забезпечують зберігання даних, роботу внутрішніх додатків та контроль доступу до мережі.

Система відеоспостереження, яка інтегрована в загальну мережу і контролює важливі зони закладу, такі як входи, адміністративні приміщення та навчальні корпуси.

Основні завдання мережі:

– Постійний контроль працездатності обладнання і своєчасне виявлення проблем дозволяє швидко реагувати на збої і забезпечувати безперервність освітнього процесу.

– Мережа забезпечує захист інформації від несанкціонованого доступу за допомогою налаштувань безпеки, включаючи фільтрування доступу та шифрування даних.

– Важливою метою є забезпечення високої пропускної здатності мережі для підтримки навчальних і адміністративних процесів. Це особливо критично під час масових заходів, таких як онлайн-лекції, вебінари або дистанційне навчання.

4.4.2. Основні проблеми мережі в навчального закладу:

Перевантаження мережі в години пік, коли одночасно велика кількість користувачів підключається до системи для роботи або навчання.

Стара інфраструктура в деяких корпусах, що вимагає модернізації для забезпечення більш стабільного з'єднання та швидшого доступу до інтернету.

Фізичні обмеження, такі як товсті стіни підвалів і старих будівель, що можуть впливати на якість сигналу Wi-Fi та інших бездротових підключень.

Мережа навчального закладу структурована за принципом розподілених сегментів, що дозволяє легко масштабувати і модернізувати її відповідно до потреб навчального закладу. Завдяки постійному моніторингу в системі Zabbix, адміністратори можуть відстежувати всі ключові параметри мережі і вчасно вирішувати проблеми, що виникають.

Це дозволяє забезпечувати ефективну роботу як навчального процесу, так і адміністративних служб, підтримуючи високий рівень комфорту для всіх користувачів мережі.

4.4.3. Створення карт мережі в навчального закладу

Нижче наведено опис кожної суб карти та головної карти мережі навчального закладу:

4.4.3.1. Geo

Ця карта відображає географічну структуру мережі закладу та дозволяє відстежувати фізичне розташування всіх пристроїв у реальному часі. Це спрощує адміністрування та швидке реагування на збої. Основні компоненти:

Геолокаційні точки для кожного пристрою.

Візуалізація мережевих з'єднань для спрощеного управління мережею.

Основні призначення:

– Точне відстеження місцезнаходження пристроїв у великих будівлях, таких як гуртожитки та навчальні корпуси.

– Виявлення проблем з підключенням або доступністю пристроїв залежно від їхнього розташування.

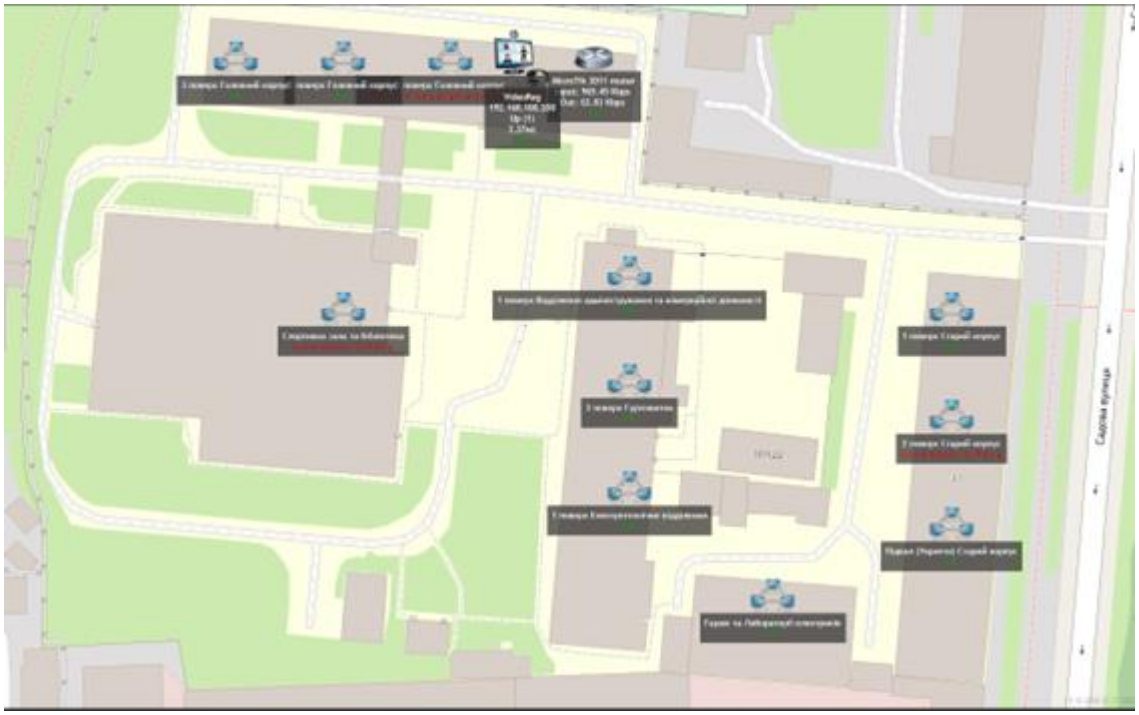

Рисунок 4.24 – Geo

4.4.3.2. **Головний корпус**

4.4.3.2.1. **1 поверх**

Ця карта покриває перший поверх головного корпусу, який включає навчальні класи, адміністративні приміщення та комп'ютерні лабораторії. Мережа складається з таких елементів:

Комп'ютери та ноутбуки для навчальних цілей: пристрої підключені до внутрішньої локальної мережі для доступу до освітніх ресурсів.

Комутатори для розподілу з'єднань між навчальними кабінетами.

Основні виклики:

– Підтримка стабільного підключення під час проведення занять з використанням інтернету.

– Запобігання перевантаженню мережі в години навчальних занять, коли велика кількість студентів одночасно користується навчальними матеріалами онлайн.

– Забезпечення надійності внутрішньої мережі для проведення лабораторних робіт та тестування.

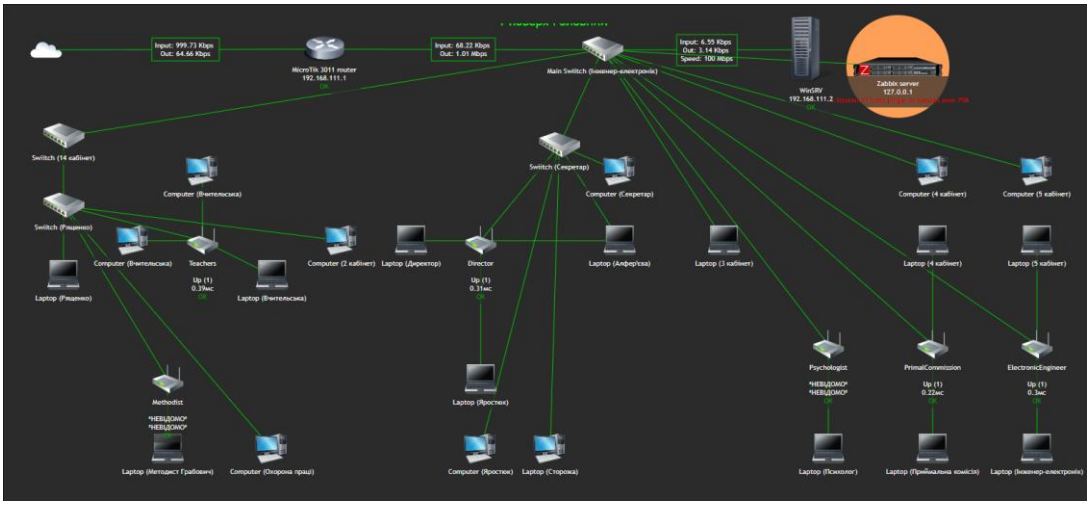

Рисунок 4.17 – 1 поверх Головний корпус

4.4.3.2.2. **2 поверх**

Ця карта відображає мережеву інфраструктуру другого поверху головного корпусу, де розташовані комп'ютерні класи та кабінети для дистанційного навчання. Основні компоненти:

Локальна мережа для підключення студентських робочих станцій.

Точки доступу до Wi-Fi, що забезпечують бездротовий інтернет-зв'язок для викладачів і студентів.

Основні призначення:

– Підтримка стабільного з'єднання для онлайн-навчання.

– Підтримка високої пропускної здатності під час проведення масових заходів, таких як онлайн-курси або вебінари.

– Виявлення та усунення проблем із підключенням, що можуть виникати через одночасне використання великої кількості пристроїв.

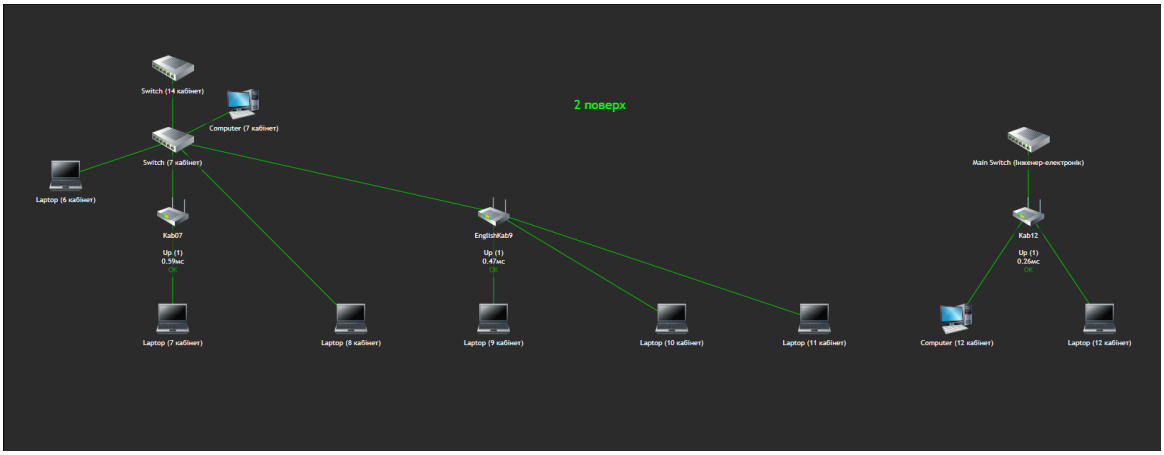

Рисунок 4.20 – 2 поверх Головний корпус

4.4.3.2.3. **3 поверх**

На третій поверх головного корпусу припадає значна частина мережевих з'єднань, зокрема для адміністративних та освітніх цілей. Основні елементи:

Комп'ютерні класи для дистанційного навчання.

Мережеве обладнання для підключення комп'ютерів та ноутбуків до локальної мережі.

Основні призначення:

– Підтримка стабільної роботи мережі для проведення дистанційних занять та онлайн-лекцій.

– Моніторинг якості інтернет-з'єднання для забезпечення безперебійної роботи викладачів та студентів.

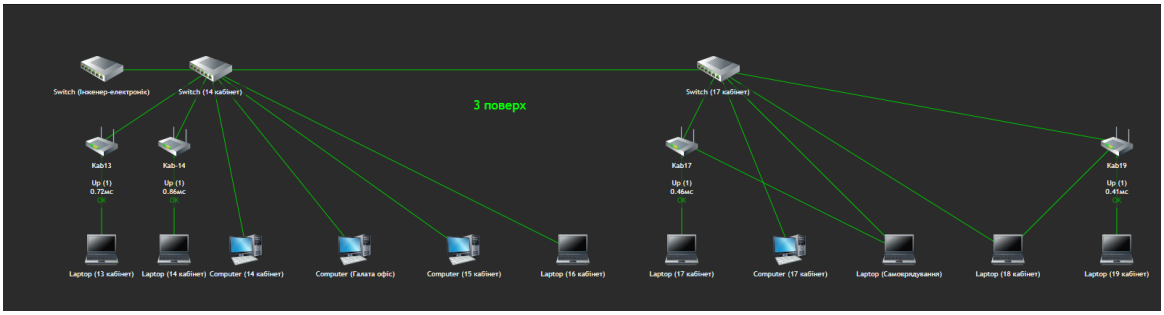

Рисунок 4.23 – 3 поверх Головний корпус

4.4.3.3. Старий корпус

4.4.3.3.1. 1 поверх

Мережа на цій карті охоплює перший поверх старого корпусу, де розташовані старі аудиторії та адміністративні приміщення. Основні елементи:

Старе мережеве обладнання, яке потребує регулярного моніторингу для виявлення потенційних збоїв.

Підключення до загальної мережі через кілька ключових комутаторів.

Основні призначення:

– Підтримка стабільної роботи мережі в умовах застарілої інфраструктури.

– Потреба в регулярному моніторингу та обслуговуванні обладнання для уникнення збоїв.

– Забезпечення ефективної роботи мережі для адміністративного персоналу, що працює в цьому корпусі.

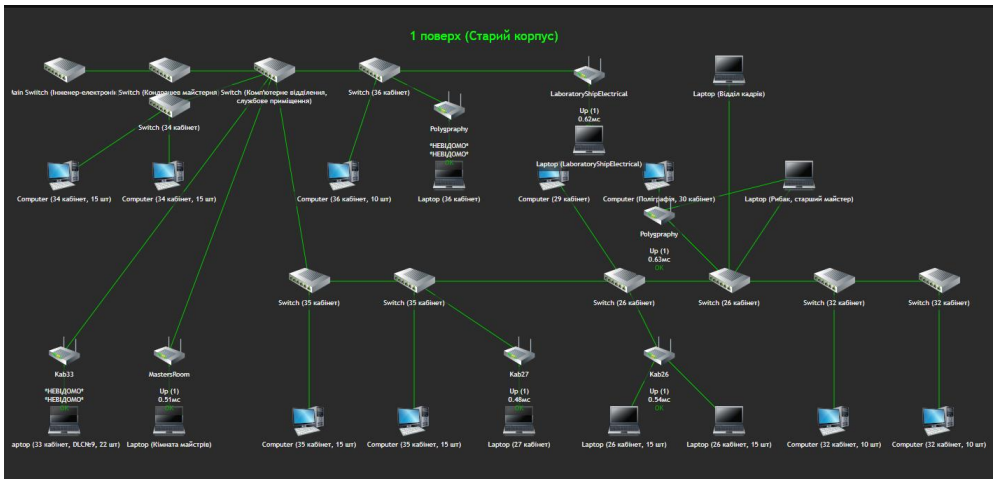

Рисунок 4.19 – 1 поверх Старий корпус

4.4.3.3.2. **2 поверх**

Ця карта представляє мережеву інфраструктуру другого поверху старого корпусу. Основні елементи мережі включають:

Підключення комп'ютерних класів через комутатори до основної мережі.

Підтримка Wi-Fi з'єднання для студентів і викладачів.

Основні призначення:

– Вирішення проблем із доступом до мережі, які можуть виникати через старе обладнання та фізичні умови будівлі (товсті стіни).

– Потреба в модернізації інфраструктури для забезпечення більш стабільного та швидкого підключення до мережі.

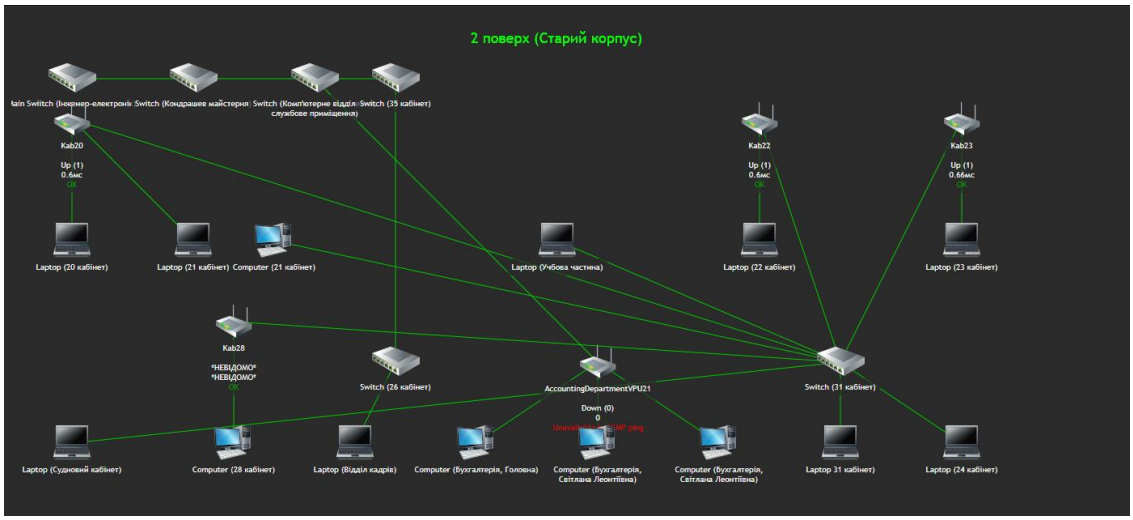

Рисунок 4.22 – 2 поверх Старий корпус

4.4.3.3.3. **Підвал (Укриття)**

Ця карта представляє мережу підвального приміщення старого корпусу, де розташовані укриття. Основні елементи:

Мережеві комутатори, які забезпечують підключення пристроїв у технічних приміщеннях.

Основні призначення:

– Відстеження стабільності з'єднання в умовах підвального розташування та товстих стін.

– Забезпечення безперебійної роботи обладнання у випадку надзвичайних ситуацій або евакуації.

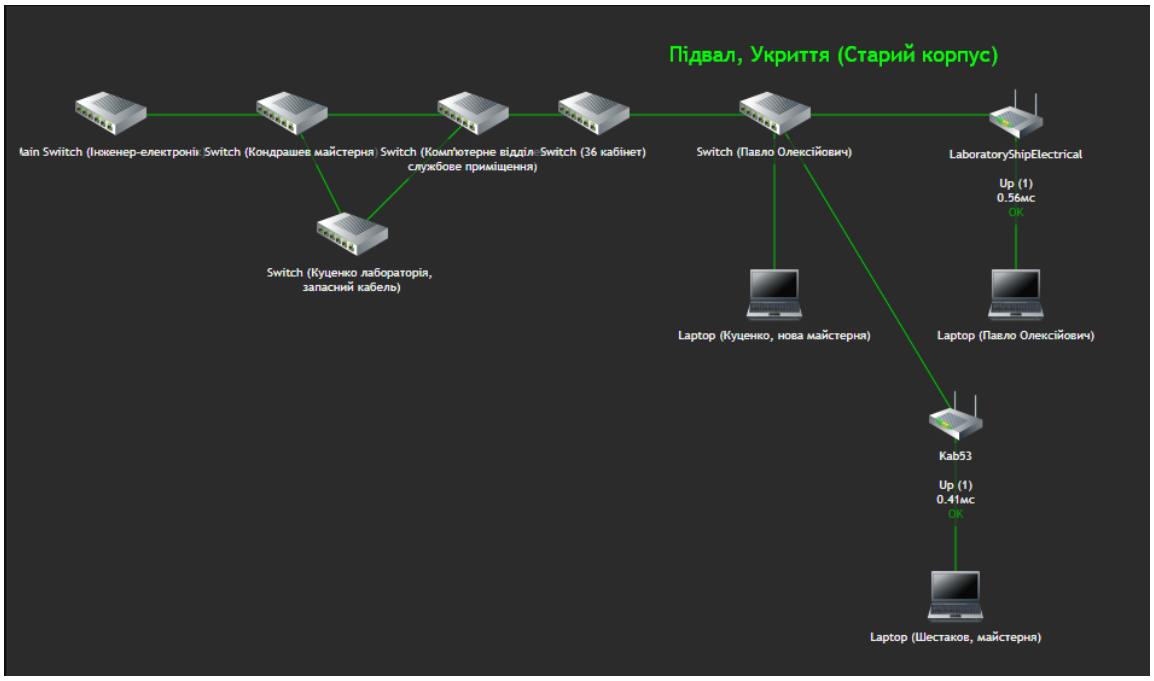

Рисунок 4.27 – Підвал (Укриття) Старий корпус

4.4.3.4. Відділення адміністративної та комерційної діяльності

4.4.3.4.1. 1 поверх

Ця карта відображає мережеву інфраструктуру, що охоплює адміністративні відділи та кабінети для обслуговування студентів і викладачів на першому поверсі. Основними мережевими елементами є:

Маршрутизатори та комутатори для розподілу інтернет-з'єднання між офісними приміщеннями.

Сервери для внутрішньої обробки даних: на цьому рівні встановлені сервери, що обробляють запити співробітників адміністративного відділення.

Основні призначення:

– Забезпечення безперебійної роботи сервера в години пік.

– Підтримка стабільного з'єднання під час обробки великих обсягів інформації, включаючи облік студентів і ведення документації.

– Відсутність збоїв у з'єднанні під час проведення адміністративних нарад чи заходів, що вимагають відеозв'язку.

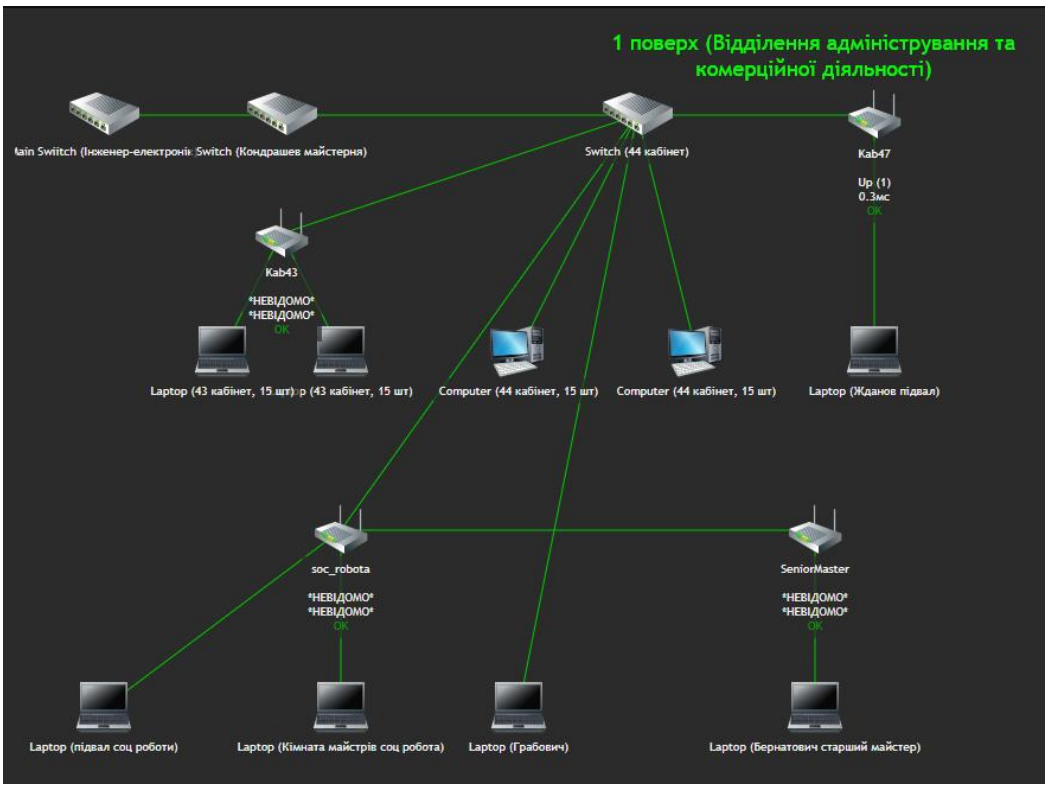

Рисунок 4.16 – 1 поверх (Відділення адміністрування та комерційної діяльності)

4.4.3.4.2. **2 поверх (Гуртожиток)**

Мережа на другому поверсі гуртожитку включає точки доступу Wi-Fi та підключення до загальної мережі закладу. Основні компоненти:

Wi-Fi точки доступу, які забезпечують підключення студентів до інтернету в кімнатах.

Мережеві комутатори, що об'єднують інтернет-підключення на поверхах гуртожитку.

Основні призначення:

– Забезпечення надійного підключення до інтернету для великої кількості студентів, що проживають на поверсі.

– Вирішення проблем із перевантаженням мережі в години пік.

– Постійний моніторинг якості зв'язку та виявлення потенційних збоїв у мережі.

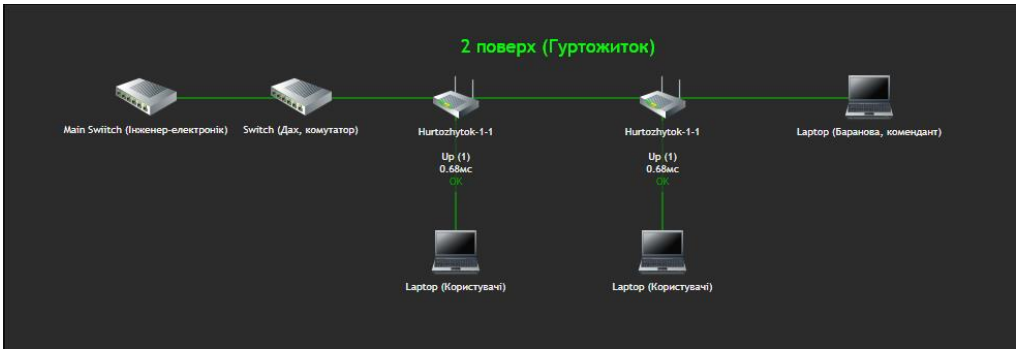

Рисунок 4.21 – 2 поверх Гуртожиток

4.4.3.5. Електротехнічне відділення

4.4.3.5.1. 1 поверх

Ця карта відображає мережеву структуру, яка обслуговує електротехнічне відділення навчального закладу. На цьому рівні підключені:

– **Комп'ютери та спеціалізоване обладнання для проведення практичних занять.**

– **Мережеві комутатори**, що забезпечують підключення навчальних лабораторій до загальної мережі.

Основні призначення:

– Підтримка безперебійного доступу до інтернету для проведення досліджень та лабораторних робіт.

– Забезпечення надійності мережі під час використання спеціалізованого навчального обладнання.

– Виявлення можливих проблем з доступністю обладнання та своєчасне їх вирішення для безперервного навчального процесу.

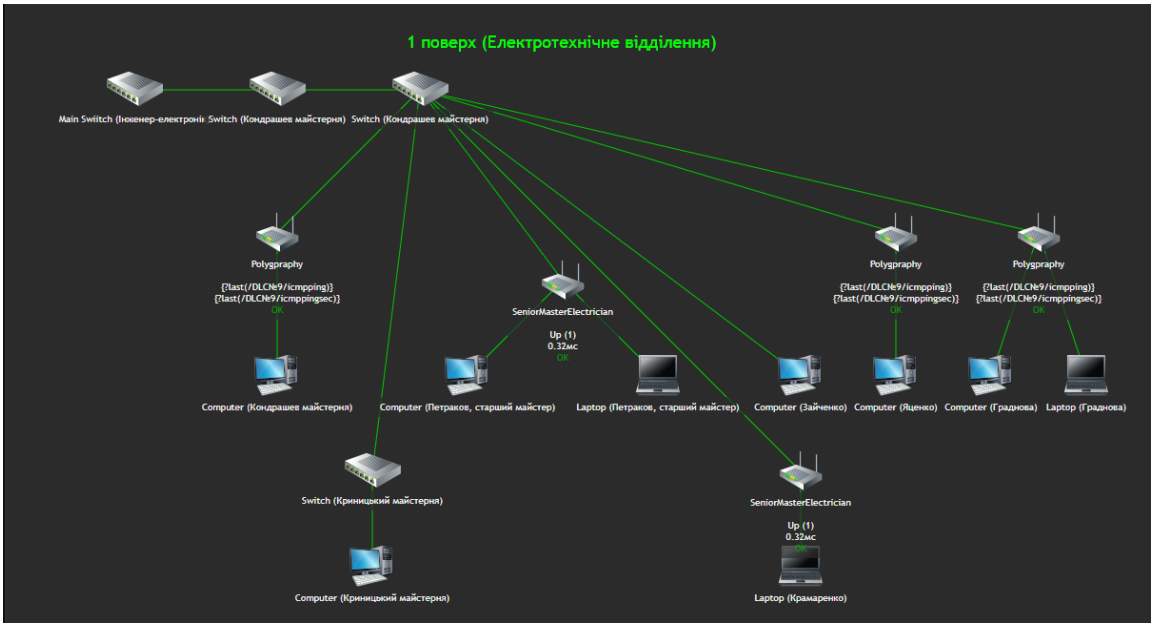

Рисунок 4.18 – 1 поверх Електротехнічне відділення

4.4.3.6. Гараж та Лабораторії електриків

Ця карта охоплює мережеву інфраструктуру гаражів і навчальних лабораторій електриків. Основні елементи:

Підключення спеціалізованого навчального обладнання до мережі.

Мережеві комутатори для об'єднання різних частин лабораторій.

Основні призначення:

– Забезпечення надійного підключення навчального обладнання для проведення практичних занять.

– Моніторинг технічного стану обладнання для запобігання збоїв у навчальному процесі.

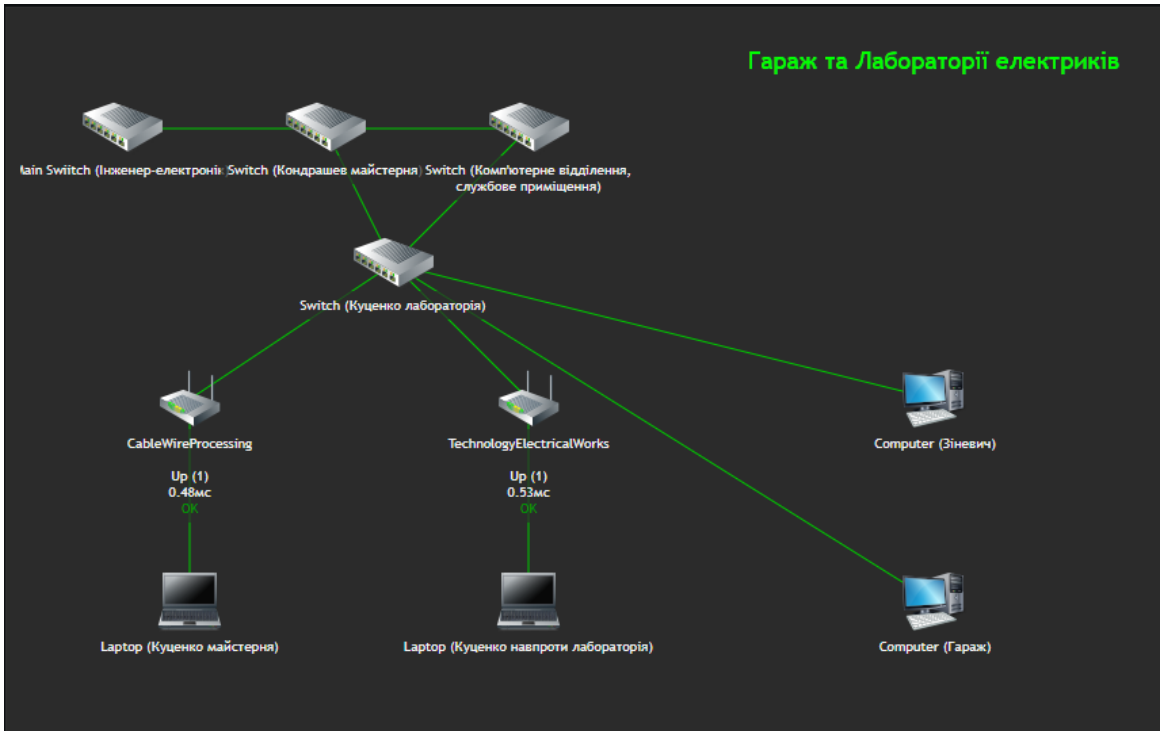

Рисунок 4.26 – Гараж та Лабораторії електриків

4.4.3.7. Спортивна зала та бібліотека

Мережа спортивної зали та бібліотеки включає:

Wi-Fi зони покриття, які забезпечують доступ до інтернету в цих приміщеннях.

Комп'ютери в бібліотеці, підключені до локальної мережі для доступу до освітніх ресурсів.

Основні призначення:

– Забезпечення стабільного покриття Wi-Fi на великій площі спортивної зали.

– Підтримка надійного підключення в бібліотеці для забезпечення доступу до ресурсів.

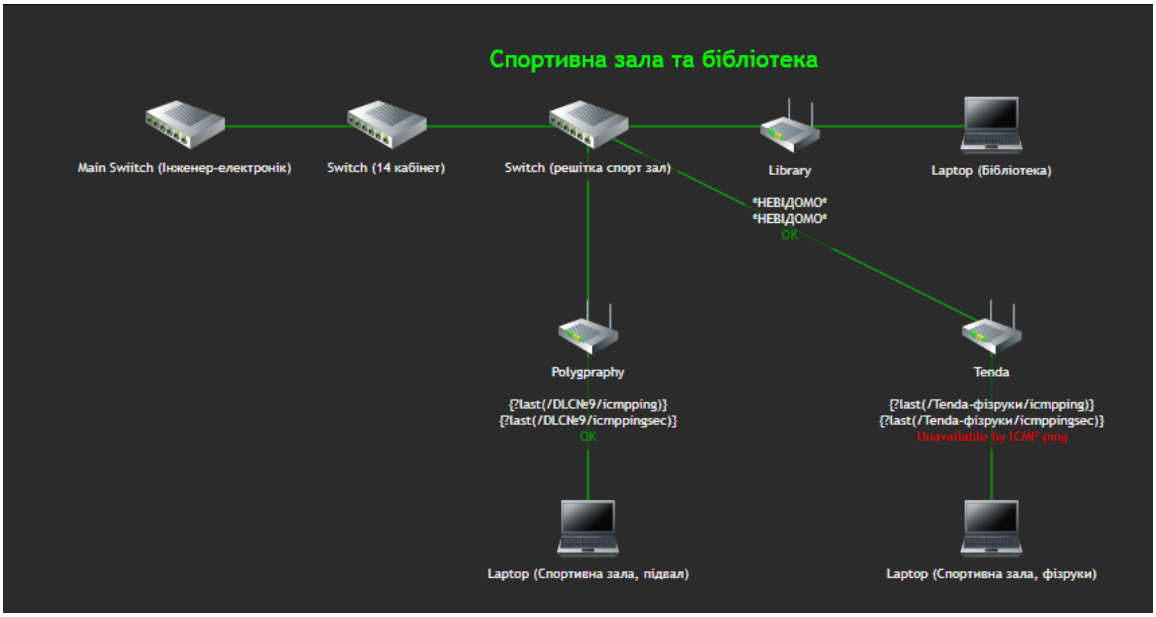

Рисунок 4.28 – Спортивна зала та бібліотека

4.4.3.8. **VideoCam**

Ця карта охоплює мережу відеоспостереження, зокрема всі камери, розташовані на території навчального закладу. Основні елементи включають:

Відеокамери для моніторингу внутрішньої та зовнішньої частини будівель.

Системи зберігання відеоданих для запису та архівування відеопотоків.

Основні призначення:

– Забезпечення безперебійної роботи системи відеоспостереження, особливо в критичних зонах, таких як вхідні двері та важливі адміністративні приміщення.

– Моніторинг якості відеопотоку та вирішення проблем із передачею даних через мережу.

Рисунок 4.25 – VideoCam

Ці карти детально відображають структуру мережі в навчального закладу, що дозволяє швидко виявляти та усувати проблеми, забезпечуючи ефективну роботу всієї мережі.

Карта **Geo** є основною картою мережевої інфраструктури навчального закладу, на яку приєднуються всі субкарти, що представляють різні частини мережі закладу (навчальні корпуси, гуртожитки, бібліотека, укриття тощо). Ця карта надає загальний огляд мережі і дозволяє адміністратору швидко перейти до кожного сегменту для детального моніторингу.

Основні функції карти Geo:

– Відображення **географічного розташування всіх пристроїв** мережі: кожен маршрутизатор, комутатор, сервер, комп'ютер або Wi-Fi точка доступу має своє місце на карті.

– **Субкарти**, такі як карти окремих поверхів чи спеціалізованих відділень, інтегровані у карту **Geo**, що дозволяє переміщатися між різними частинами мережі.

– **Інтерактивні функції**: за допомогою карти можна **перевірити стан кожного пристрою**.

Натиснувши на будь-який комп'ютер, маршрутизатор або інший пристрій, можна:

– **Пропінгувати** пристрій, щоб перевірити його доступність у мережі.

– Переглянути, чи є доступ до інтернету.

– Переглянути **швидкість інтернет-з'єднання** для кожного пристрою в реальному часі, що допомагає виявляти проблеми з підключенням або затримками.

Карта **Geo** виступає як централізований вузол для адміністрування мережі, дозволяючи швидко аналізувати ситуацію, виявляти неполадки та здійснювати базові дії з обслуговування пристроїв.

Карта **VideoCam** містить всі **камери відеоспостереження** та **відеореєстратор**, який відповідає за запис та збереження відеопотоків. Ця карта дозволяє моніторити стан системи відеоспостереження, що розміщена по всій території навчального закладу.

Основні функції карти VideoCam:

– **Відображення всіх камер спостереження** та їх географічне розташування на території закладу: камери встановлені як на входах у будівлі, так і в стратегічно важливих зонах (навчальні приміщення, адміністративні кабінети, зовнішні периметри).

– **Відеореєстратор**, який отримує дані від камер і зберігає відеозаписи. Це дозволяє переглядати історію подій і забезпечувати безпеку в режимі реального часу.

Інтерактивні можливості для кожної камери:

– При натисканні на камеру можна **перевірити її стан**: чи є вона активною, чи є з'єднання з відеореєстратором.

– **Пропінгувати камеру**, щоб перевірити її доступність в мережі.

– Переглянути **швидкість інтернет-з'єднання** для кожної камери, що важливо для оцінки якості відеопотоку та можливих затримок або перебоїв у передачі даних.

– Карта **VideoCam** дозволяє адміністраторам постійно контролювати роботу системи відеоспостереження та швидко реагувати на будь-які проблеми, що можуть виникати з камерами або відеореєстратором.

– **Швидкість інтернету** та доступність до мережі відображаються на кожному пристрої, що дозволяє точно оцінювати якість підключення та виявляти проблеми на кожному етапі роботи мережі.

4.5. Система оповіщення в Telegram

4.5.1. Загальні відомості оповіщення через Telegram

Оповіщення через Telegram у системі Zabbix є ефективним способом забезпечення швидкого інформування про будь-які проблеми в мережі чи на сервері. Використання Telegram як каналу для сповіщень має кілька ключових переваг:

– Замість електронної пошти чи SMS, які можуть затримуватися, повідомлення в Telegram приходять майже миттєво.

– Ви можете отримувати сповіщення на смартфон або комп'ютер, що дає можливість швидко реагувати на проблеми.

– Користувач може легко переглядати стан пристрою, пінгувати його або перевіряти доступність в інтернеті, натиснувши на відповідний елемент у повідомленні.

– Можливість налаштувати надсилання сповіщень кільком користувачам або групі в Telegram, що спрощує колективне адміністрування.

– Telegram є безкоштовним додатком, який працює на всіх платформах, і не вимагає додаткових витрат на обслуговування.

Ця система оповіщення дозволяє системним адміністраторам бути в курсі подій і проблем в мережі, навіть якщо вони не знаходяться безпосередньо біля комп'ютера. Це значно спрощує реагування на інциденти і допомагає підтримувати стабільну роботу інфраструктури.

4.5.2. Реалізація системи оповіщення через Telegram

Для налаштування оповіщень через Telegram я виконав наступні дії:

Крок 1: Створення Telegram-бота

Для початку було створено Telegram-бота для надсилання повідомлень. Зайшовши у Telegram, знайдено бота BotFather, через якого надіслано команду /newbot. Після виконання декількох кроків отримано токен для бота, який використано для налаштування з'єднання між Zabbix і Telegram.

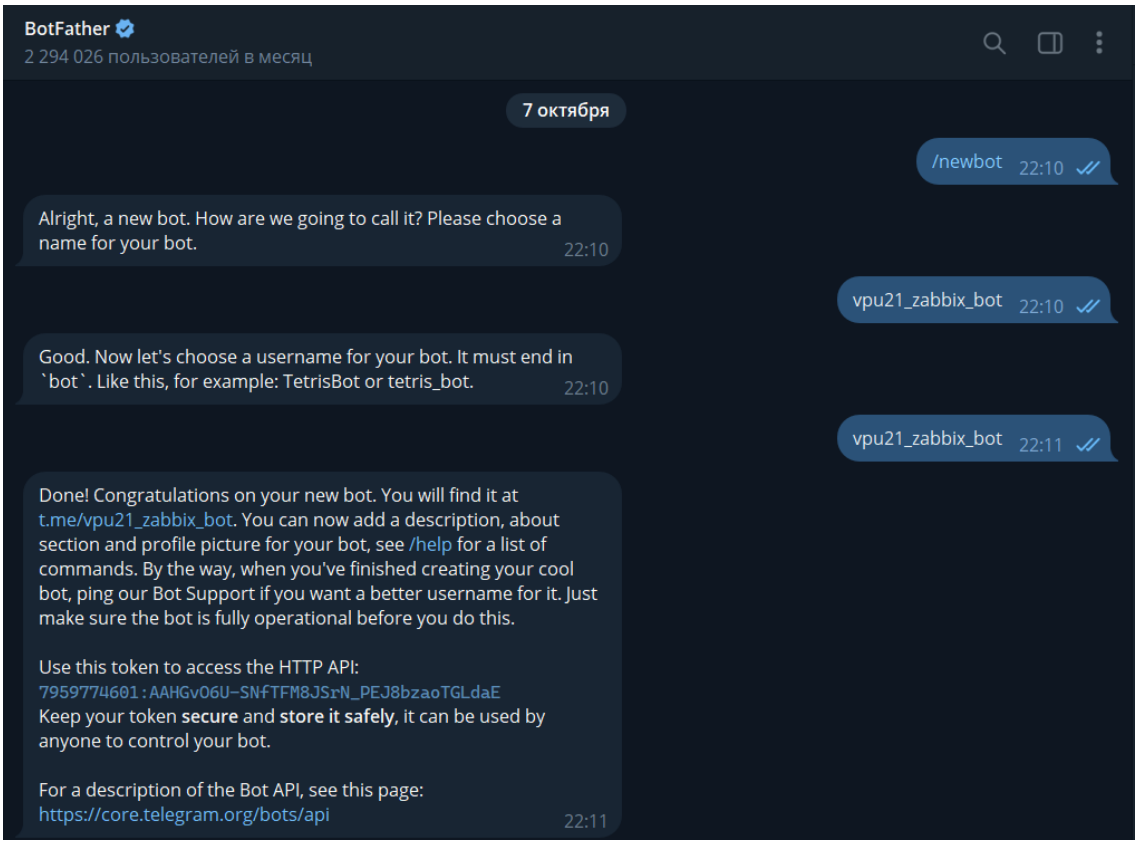

Рисунок 4.29 – Створення Telegram-бота

Крок 2: Отримання chat_id

Для отримання chat_id використано бота @getmy_idbot, який надав унікальний ідентифікатор після відправки повідомлення. Цей chat_id необхідний для надсилання повідомлень конкретному користувачеві.

Створено Telegram-бота через @BotFather, виконавши такі дії:

Зверненося до @BotFather, відправлено команду `/newbot`, обрано ім'я бота, і отримано унікальний токен доступу:

Токен: `7959774601:AAHGvO6U-SNfTFM8JSrN_PEJ8bzaoTGeenaE`.

Цей токен дозволяє використовувати API для взаємодії з ботом і інтеграції його в інші системи. Він працює як ключ для доступу до функцій бота, таких як відправка повідомлень, отримання подій та багато іншого. Він унікальний, тому для конфіденційності було прийнято рішення змінити токен.

Для отримання ID чату використано @getmy_idbot, який надав ID групового чату, куди був доданий бот:

ID чату: `-1002446115139`.

Префікс `-100` свідчить про те, що це груповий чат або канал. Цей ID необхідний для того, щоб бот міг надсилати повідомлення чи сповіщення в конкретний чат.

Також через @getmy_idbot отримано ID користувача:

ID користувача: 658815041.

Цей унікальний ідентифікатор потрібен, щоб бот взаємодіяв з конкретним користувачем, наприклад, відправляв йому особисті повідомлення або відповідав на його дії в чаті.

Тепер Telegram-бот повністю готовий для інтеграції з системами моніторингу, такими як Zabbix, або для інших автоматизованих завдань. Можна використовувати цей бот для надсилання сповіщень про важливі події або зміни в системі, що дозволить оперативно реагувати на проблеми чи ситуації.

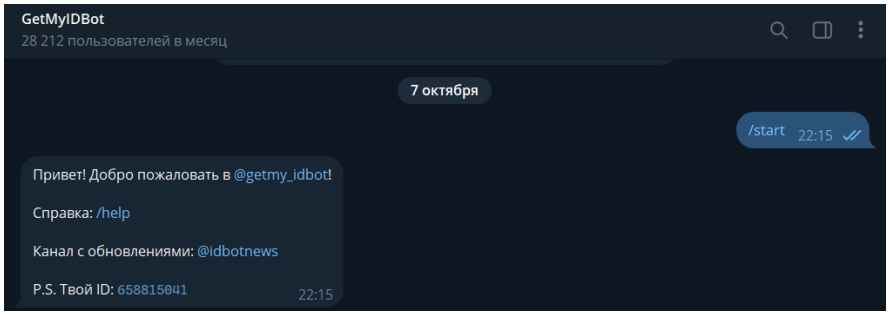

Рисунок 4.30 – Отримання chat_id

Крок 3: Створення групи та додавання телеграм бота та адміністраторів

Для зручного інформування створено групу в Telegram під назвою vpu21_zabbix_bot, куди додано:

Створеного Telegram-бота.

Адміністраторів, які відповідальні за моніторинг і підтримку мережі.

Це дозволяє всім членам групи отримувати сповіщення одночасно, що сприяє швидшому реагуванню на будь-які проблеми в мережі. Усі сповіщення, що надходять через Zabbix, тепер автоматично з'являються в групі, де кожен адміністратор може взаємодіяти з повідомленням, перевіряти стан мережевих пристроїв або виконувати інші необхідні дії.

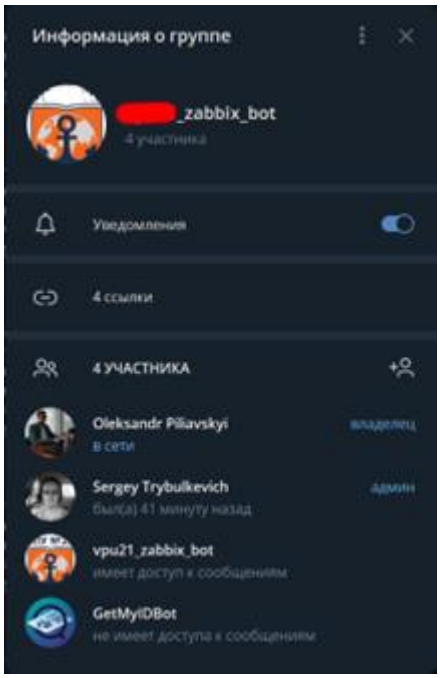

Рисунок 4.31 – Створення групи в Telegram

Крок 4: Активація Telegram в Zabbix

Після налаштування медіа типу для Telegram переконанося, що він був активований у системі. У налаштуваннях медіа типів Telegram показувався як Webhook із статусом Активовано, що підтверджує правильну інтеграцію.

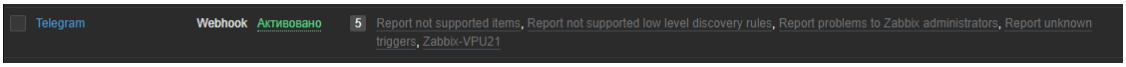

Рисунок 4.32 – Активація Telegram в Zabbix

Крок 6: Налаштування Trigger actions

Для автоматичного надсилання повідомлень через Telegram при спрацюванні тригерів у Zabbix налаштовано дії у розділі Trigger actions.

У розділі Trigger actions я створено кілька дій для різних вузлів мережі (сервери, бази даних, віртуальні машини, IP-камери, Wi-Fi тощо). Це дозволяє отримувати детальні сповіщення про проблеми з конкретними частинами інфраструктури, що допомагає швидко реагувати на будь-які збої. Наприклад, сповіщення були налаштовані для таких умов:

Linux servers: Надсилання сповіщень групі адміністраторів через всі методи, включаючи Telegram.

Zabbix servers та Virtual machines: Надсилання повідомлень безпосередньо через Telegram групі адміністраторів.

Wi-Fi та IP камери: Сповіщення про проблеми з доступом до цих сегментів мережі.

Кожна дія налаштована так, що коли спрацьовує тригер на будь-якому з цих вузлів, повідомлення одразу надсилаються до групи vpu21_zabbix_bot, де адміністратори можуть переглядати деталі та відповідно реагувати.

Це завершальний етап у налаштуванні системи оповіщень через Telegram, і він забезпечує ефективне управління інфраструктурою та своєчасне реагування на будь-які інциденти.

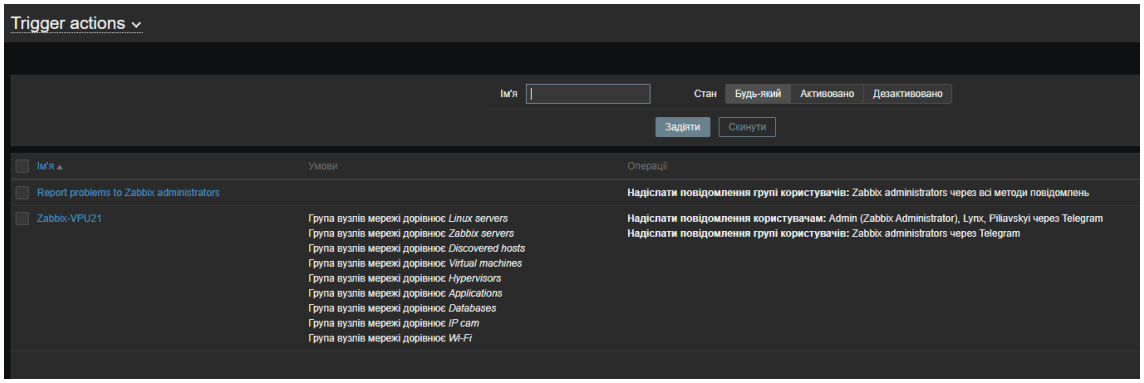

Рисунок 4.33 – Налаштування Trigger actions

Крок 7: Тестування

Після завершення налаштувань проведено тестування системи оповіщення, викликавши помилку на одному з роутерів. Сповіщення надійшло в Telegram із вказаною інформацією про проблему, що дозволило оперативно її вирішити.

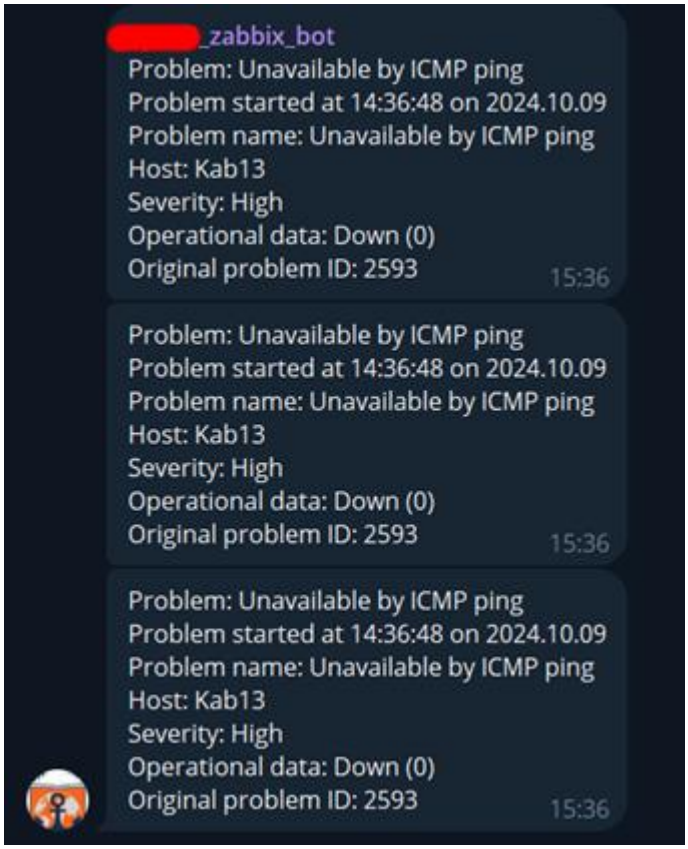

Рисунок 4.34 – Тестування системи оповіщення

Було проведено аналіз переваг налаштованої системи:

– Сповіщення в Telegram надходять миттєво, що дозволяє оперативно реагувати на критичні події.

– Telegram доступний на всіх пристроях, що забезпечує отримання повідомлень навіть за відсутності біля комп'ютера.

– Сповіщення дають змогу одразу виконувати необхідні дії, як-от пропінгувати пристрій або перевірити доступ до інтернету.

– Система дозволяє налаштувати сповіщення для різних груп користувачів або підсистем.

– Всі повідомлення зберігаються в Telegram, що полегшує відстеження історії подій та вирішення проблем у мережі.

Таким чином, реалізація системи оповіщень через Telegram у Zabbix значно підвищила ефективність моніторингу та управління мережевими пристроями в інфраструктурі.

4.6. Інтеграція VPN на базі L2TP **IPSec**

Інтеграція L2TP VPN стала важливим кроком у розвитку інфраструктури навчального закладу, оскільки вона забезпечила надійний і безпечний доступ до внутрішніх ресурсів, сприяючи ефективній роботі як адміністративного персоналу, так і викладачів.

4.6.1. Етапи налаштування VPN на базі L2TP

Налаштування серверної частини на MikroTik 3011

Увійшовши до інтерфейсу MikroTik через WinBox, використано IP-адресу маршрутизатора (192.168.111.1).

Перейдено до меню PPP, де створено новий профіль для VPN-сервера.

Вибрано тип з'єднання L2TP Server та активовано його, поставивши галочку на "Enable L2TP Server".

Створення користувачів для VPN

У меню PPP додано нового користувача для L2TP з унікальним логіном і паролем.

Наприклад, для адміністративного доступу використано логін "admin".

Призначено внутрішню IP-адресу, яка буде використовуватися під час VPN-з'єднання. Це дозволяє контролювати доступ до різних сегментів мережі.

Налаштування IPSec для захисту з'єднання

Для забезпечення шифрування VPN-з'єднань увімкнено підтримку **IPSec**.

У меню IP > IPsec > Peers створено новий запис із параметрами шифрування, використовуючи алгоритми AES та SHA1 для захисту з'єднання.

Вказано Pre-shared Key для забезпечення надійного з'єднання.

Додавання правил фільтрації трафіку

Налаштовано правила Firewall для обмеження доступу лише авторизованих користувачів до внутрішньої мережі через L2TP.

Створено правило для дозволу трафіку з внутрішньої IP-адреси VPN до всіх необхідних служб і підмереж.

Тестування та впровадження

Після завершення налаштувань проведено тестування через віддалене з'єднання з VPN через L2TP на різних клієнтах (Windows та мобільні пристрої).

Після успішного тестування впроваджено систему для співробітників і адміністрації навчального закладу, що дозволяє безпечно підключатися до внутрішньої мережі закладу з будь-якого місця.

Результат Інтеграція L2TP VPN

Інтеграція L2TP VPN на маршрутизаторі MikroTik 3011 дозволила створити надійне та захищене з'єднання, яке використовується адміністраторами та викладачами навчального закладу для роботи з

внутрішніми серверами та іншими ресурсами закладу. Це рішення забезпечує можливість віддаленої роботи, що стало критично важливим для забезпечення безперервного функціонування навчального процесу та адміністративної діяльності.

Завдяки впровадженню L2TP VPN, співробітники отримали доступ до ресурсів мережі закладу з будь-якого місця, де є Інтернет-з'єднання, що значно підвищило гнучкість роботи та дозволило вирішувати завдання, не прив'язуючись до фізичного місця перебування. Це з'єднання захищене за допомогою шифрування, що гарантує безпеку переданих даних і запобігає можливим загрозам кібербезпеки.

					172.4397ст3.КР.ПЗ.Р5			
Змн.	*Арк.*	*№ документу*	*Підпис*	*Дата*				
Розробник		Пілявський О. І.			ОХОРОНА ПРАЦІ	*Літ.*	*Арк.*	*Аркушів*
Консультант		Тубальцев А. М.					78	
Н. контр.		Добрінова Л. П.				НУК імені адмірала Макарова		
Керівник		Трибулькевич С. Л.						
Зав. каф.		Рябенький В. М.						

РОЗДІЛ 5. ОХОРОНА ПРАЦІ

Охорона праці являє собою комплекс правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних, а також лікувально-профілактичних заходів і засобів, що спрямовані на підтримання здоров'я і працездатності людини в процесі її трудової діяльності.

Основною метою системи управління охороною праці є забезпечення безпеки та збереження здоров'я працівників під час виконання ними робочих завдань. Для досягнення цієї мети реалізуються різні управлінські функції, що являють собою взаємопов'язані заходи, які здійснюються суб'єктом управління з метою впливу на об'єкт управління.

Об'єктом управління в системі охорони праці є робота функціональних служб і структурних підрозділів, відповідальних керівників і технічного персоналу підприємства, спрямована на забезпечення безпечних, нешкідливих та комфортних умов праці на робочих місцях, виробничих ділянках, цехах та на підприємстві в цілому.

Основна мета впровадження системи управління охороною праці полягає в тому, щоб сприяти виконанню вимог, що дозволяють усунути або звести до мінімуму небезпечні і шкідливі фактори виробничого середовища, ізолювати персонал від джерел небезпеки, застосовувати засоби, що запобігають виникненню небезпечних ситуацій, підвищувати технічну безпеку і створювати належні санітарно-гігієнічні та ергономічні умови праці.

Система управління охороною праці передбачає визначення конкретних кількісних показників роботи виробничих підрозділів, підтримка яких на відповідному рівні забезпечує досягнення основної мети — створення безпечних і нешкідливих умов праці.

Відповідно до статті 18 Закону України «Про охорону праці», працівники зобов'язані знати та дотримуватися вимог нормативних актів, що стосуються

охорони праці, дотримуватися правил експлуатації машин, механізмів, устаткування та інших засобів виробництва, користуватися засобами колективного й індивідуального захисту, а також своєчасно проходити попередні й періодичні медичні огляди.

Дія Закону «Про охорону праці» поширюється на всі підприємства, установи та організації незалежно від форм власності і видів їхньої діяльності, а також на всіх працюючих осіб, залучених до трудової діяльності на цих підприємствах. Для забезпечення належної охорони праці активно впроваджуються науково-технічні досягнення, зокрема автоматизація небезпечних і шкідливих виробничих процесів, застосування нових безпечних матеріалів, конструктивних рішень та сучасних засобів захисту. Окрім цього, збереження здоров'я працівників допомагає зменшити витрати на виплату лікарняних листів та гарантує високу продуктивність праці. Таким чином, охорона здоров'я працівників сприяє збереженню майбутнього держави.

5.1. Аналіз небезпечних і шкідливих факторів, що впливають на людину при розробці системи

5.1.1. У приміщеннях, де передбачено розробку, виготовлення та тестування системи, можуть виникати такі небезпечні та шкідливі фактори:

– підвищений ризик ураження електричним струмом;

– підвищена пожежна небезпека;

– шкідливе електромагнітне випромінювання;

– тривала робота за комп'ютером;

– недостатній рівень освітленості.

Одним із найбільш поширених небезпечних виробничих факторів є електричний струм. Його вплив на живу тканину організму людини має різні форми і проявляється як термічний, електролітичний, механічний і біологічний ефекти.

Термічний ефект струму викликає опіки окремих частин тіла та нагрівання до високих температур органів, розташованих на шляху проходження струму, що може призвести до серйозних функціональних порушень. Електролітична дія струму полягає в розкладанні органічних рідин, у тому числі крові, з порушенням їхнього фізико-хімічного складу. Механічна дія струму призводить до розшарування і розриву тканин тіла внаслідок електродинамічного ефекту, а також миттєвого вибухоподібного утворення пари з рідин.

Біологічний ефект струму проявляється у вигляді подразнення та порушення життєдіяльності живих тканин організму і порушення внутрішніх біологічних процесів.

Допустимим вважається струм, при якому людина може самостійно відірватися від електричного кола. Його значення залежить від часу проходження струму через тіло людини: при тривалості понад 10 секунд допустимий струм складає 2 мА, а при короткочасному впливі (менше 1 секунди) — 6 мА. Струм, при якому потерпілий не може самостійно звільнитися від струмопровідних частин, називається «струмом, що не відпускає», і його величина складає від 10 до 20 мА. Змінний струм небезпечніший за постійний, але при високих напругах постійний струм може становити більшу небезпеку.

Пожежі на територіях, де знаходяться підприємства, часто виникають через порушення технологічних процесів, що є досить поширеним явищем. Для запобігання пожежам існують спеціальні нормативні документи, такі як ДСТ 12.1.004-76 «Пожежна безпека» та ДСТ 12.1.010-76 «Вибухобезпека». Тривала робота за комп'ютером також може суттєво вплинути на здоров'я людини, особливо в таких аспектах, як:

– погіршення зору через тривалу роботу за комп'ютером. Як зазначалося раніше, тривала робота з комп'ютером негативно впливає на очі. З'являються

нові терміни, які описують захворювання очей, спричинені тривалою роботою за монітором;

– дисплейна хвороба, яка полягає в порушенні акомодації очей через перенапруження війкового м'яза;

– синдром сухого ока, який виникає через порушення зволоження передньої частини ока (рогівки) слізною рідиною. У нормі людина здійснює більше 20 моргань за хвилину, що забезпечує постійне зволоження та очищення ока. Тривала робота за комп'ютером може призвести до виникнення міопії (короткозорості), далекозорості та навіть глаукоми. Особливо це стосується низькоякісних моніторів із низькою роздільною здатністю;

– захворювання кистей рук. Тривала робота з клавіатурою може стати причиною нервово-м'язових розладів. Пальці, кисті рук та передпліччя виконують основну частину механічної роботи при роботі з комп'ютером. Хоча фізичне навантаження зазвичай невелике, тривалість такої роботи негативно впливає на суглоби;

– захворювання нервової системи. Головний біль є однією з найпоширеніших скарг при тривалій роботі за комп'ютером. Хронічна напруга, постійне перенапруження м'язів обличчя та черепа можуть стати причиною цих симптомів;

– зниження уваги і складнощі з концентрацією. Хронічна втома, що виникає через роботу з комп'ютером, може супроводжуватися шумом у вухах, запамороченням та нудотою. У таких випадках слід звернутися до лікаря і тимчасово припинити роботу з комп'ютером;

– порушення опорно-рухової системи. Тривала робота за комп'ютером може призвести до викривлення хребта або сколіозу, особливо в дітей, у яких хребетний стовп легко деформується. У дорослих можуть виникати грижі міжхребцевих дисків, що спричиняють здавлювання нервових закінчень і радикуліт. Основною причиною цього є неправильна поза під час роботи.

Окрім цих проблем, тривале перебування за комп'ютером може спричинити гастрити, виразки шлунка, простатит і навіть безсоння.

5.1.2. Освітленість робочого місця є одним з основних факторів, що впливають на ефективність праці. Раціональне освітлення є необхідним для забезпечення продуктивності та безпеки праці, а також для попередження нещасних випадків і перевтоми працівників. Недостатнє освітлення може спричинити порушення зору, нервову напругу та втому.

Освітлення виробничих приміщень — це один із головних факторів зовнішнього виробничого середовища, що впливає на працівників під час їхньої роботи. Тільки за умови належного освітлення робочих місць можна забезпечити безпеку та високу продуктивність праці.

Низький рівень освітлення та нерівномірний розподіл світла призводять до перевтоми зору, зниження продуктивності праці та можливих нещасних випадків на робочих місцях. Відповідно до чинних норм, рівень освітленості робочих місць має відповідати будівельним нормам та правилам ДБН В 2 5-28-2006.

5.2. Природне освітлення

Природне освітлення — це процес освітлення приміщень за рахунок природного денного світла, яке проникає через вікна та інші світлові отвори в зовнішніх конструкціях будівлі.

Виробничі приміщення мають бути обладнані світловими прорізами, які забезпечують належний рівень природного освітлення. В окремих випадках, таких як проектування конференц-залів, архівів, кіносховищ, підприємств побутового обслуговування, а також коридорів та складських приміщень, дозволяється відсутність природного освітлення.

Природне освітлення класифікується за напрямом проникнення світла в приміщення. Бокове освітлення забезпечується через вікна, розташовані на

стінах будівлі, верхнє — через спеціальні світлові ліхтарі або отвори в стелі, а комбіноване поєднує обидва ці типи освітлення.

Бокове освітлення може бути одностороннім (світло надходить через вікна на одній із зовнішніх стін приміщення) або двостороннім (світло проникає через вікна, розташовані на двох протилежних стінах). Природне освітлення є нестабільним, оскільки його інтенсивність змінюється в залежності від часу доби і пори року. Для його кількісної оцінки використовується коефіцієнт природної освітленості, який визначає відносну освітленість приміщення при природному освітленні.

5.3. Штучне освітлення

Штучне освітлення — це система освітлення приміщень за допомогою штучних джерел світла, таких як електричні лампи різних типів (газорозрядні, лампи розжарювання тощо).

Залежно від конструкції, штучне освітлення поділяється на загальне, місцеве та комбіноване. Загальне освітлення забезпечує рівномірне освітлення приміщення або його зон. Місцеве освітлення додається до загального і використовується для підсвічування окремих робочих місць. Комбіноване освітлення поєднує загальне і місцеве освітлення для створення оптимальних умов освітленості.

Функціонально штучне освітлення може бути робочим, аварійним, охоронним та черговим. Робоче освітлення призначене для забезпечення належних умов зорової діяльності під час виконання роботи, проходу працівників і руху транспорту. Воно має відповідати нормованим показникам освітленості та яскравості у приміщеннях. Для приміщень з різними умовами природного освітлення може бути передбачено роздільне керування освітленням різних зон.

Аварійне освітлення поділяється на освітлення безпеки, яке дозволяє продовжувати роботу під час аварій, та евакуаційне, призначене для безпечної евакуації при відключенні основного освітлення. Аварійні світильники підключаються до окремої електромережі.

Чергове освітлення застосовується в приміщеннях, а охоронне — на територіях підприємств для їх освітлення в нічний час або в неробочі години. Частина світильників робочого або аварійного освітлення може використовуватися для забезпечення чергового освітлення, підтримуючи мінімальний рівень освітленості для чергових працівників.

Джерела штучного освітлення включають:

– лампи розжарювання (загального призначення);

– газорозрядні лампи (високого та низького тиску);

– люмінесцентні лампи низького тиску для освітлення опалюваних приміщень;

– дугові ртутні лампи високого тиску для освітлення високих виробничих приміщень та зовнішніх територій;

– металогалогенні лампи для освітлення територій та приміщень із підвищеними вимогами до освітленості (наприклад, зборка електроніки);

– натрієві лампи високого тиску для приміщень, де виконуються роботи низької точності (грубі роботи);

– світлодіодні лампи для загального та спеціалізованого освітлення.

Методи розрахунку штучного освітлення включають:

– метод коефіцієнта світлового потоку для розрахунку рівномірного загального освітлення горизонтальних поверхонь без затінення;

– точковий метод;

– метод питомої потужності для приблизних розрахунків.

Робоче освітлення забезпечує нормальні зорові умови для виконання робіт і переміщення працівників, підтримуючи освітленість і яскравість на відповідному рівні.

5.4. Заходи щодо техніки безпеки

5.4.1. Забезпечення електробезпеки

Електробезпека на робочому місці забезпечується конструкцією електроустаткування, яке має відповідати умовам експлуатації і захищати працівників від контакту зі струмопровідними частинами. Технічні засоби захисту, а також організаційні заходи забезпечують безпечні умови праці.

Конструкція електрообладнання має гарантувати захист від впливу зовнішніх факторів, таких як проникнення сторонніх предметів або вологи. Організаційні заходи електробезпеки включають навчання персоналу, проведення інструктажів та регулярні медичні огляди для допуску до роботи. Працівники мають дотримуватися особливих вимог при роботі з частинами, що знаходяться під напругою.

5.4.2. Заходи щодо пожежної безпеки

Заходи пожежної безпеки поділяються на організаційні, технічні, режимні та експлуатаційні.

Організаційні заходи включають правильну експлуатацію машин і обладнання, підтримання чистоти на території підприємства, регулярні інструктажі з пожежної безпеки, створення добровільних пожежних дружин та протипожежних комісій. Технічні заходи передбачають дотримання правил і норм пожежної безпеки під час проектування будівель, проведення електропроводки, встановлення вентиляції та освітлення.

Режимні заходи включають заборону паління у невстановлених місцях, проведення зварювальних та інших вогневих робіт у пожежонебезпечних приміщеннях.

Експлуатаційні заходи передбачають своєчасні профілактичні огляди, ремонти та випробування обладнання для підтримання його в належному стані.

5.4.3. Заходи щодо техніки безпеки при роботі з ПК

Для забезпечення безпеки під час роботи з персональними комп'ютерами необхідно дотримуватися таких рекомендацій:

– встановлювати обмеження на час роботи для осіб з захворюваннями опорно-рухового апарату, очей, а також для вагітних жінок;

– використовувати монітори з високою роздільною здатністю і великим екраном (не менше 15 дюймів);

– вибирати відеоадаптери з частотою оновлення зображення не менше 72 Гц, краще — 85 Гц і вище;

– застосовувати поляризаційні фільтри для моніторів, щоб зменшити шкідливе випромінювання і мерехтіння зображення;

– сидіти не ближче ніж за 70 см від екрана монітора;

– розташовувати робоче місце біля вікна таким чином, щоб кут між вікном і екраном становив не менше 90 градусів для уникнення відблисків, а при необхідності — зашторювати вікно;

– не розміщувати монітор безпосередньо під джерелом освітлення;

– стежити за тим, щоб освітленість робочого місця не перевищувала 2/3 від загальної освітленості приміщення;

– при розташуванні кількох комп'ютерів у кімнаті відстань між ними повинна бути не менше 1,2 метра;

– облаштовувати робочі місця таким чином, щоб уникати незручних пози і тривалого статичного навантаження на тіло;

– загальний час роботи за комп'ютером не повинен перевищувати 50% робочого дня (для дорослих — не більше 4 годин, для дітей — не більше 2 годин);

– робити перерви по 15 хвилин кожні 2 години роботи, а при інтенсивній роботі — кожну годину або навіть півгодини;

– стежити за тим, щоб лінія руки в області зап'ястя залишалася прямою під час роботи, руки були розслаблені, а пальці трохи зігнуті;

– удари по клавішах мають бути легкими, щоб не напружувати руки;

– використовувати підлокітники для підтримки рук як під час роботи з клавіатурою, так і з мишею;

– у разі виникнення напруження або спазмів у м'язах слід припинити роботу і виконати кілька вправ для розслаблення;

– регулювати висоту стільця так, щоб стегна були паралельні підлозі, а ноги твердо стояли на підлозі;

– під час роботи намагатися зберігати природний вигин тіла в поясниці, уникати сутулості і напруги в шиї;

– регулярно виконувати вправи для очей;

– забезпечувати однаковий колір поверхонь столу, клавіатури і корпусу комп'ютера для уникнення відблисків;

– при можливості працювати в режимі «темні символи на світлому фоні»;

– підтримувати відносну вологість повітря не менше 40% для зменшення впливу електростатичного поля;

– розміщувати обладнання комп'ютера на відстані 60-90 см від робочого місця.

Під час виконання цієї частини проекту було розроблено рекомендації щодо захисту від шкідливих впливів під час роботи, забезпечення електробезпеки, пожежної безпеки, а також заходів для мінімізації впливу електромагнітного випромінювання та роботи з ПК.

ВИСНОВКИ

У даному дипломному проекті проведено впровадження системи моніторингу для мережі навчального закладу з використанням програмного забезпечення Zabbix 7.0. Було виконано аналіз сучасних систем моніторингу, зокрема таких як Cacti, Nagios, Icinga, Nedi, Ntop, Zabbix, Observium та The Dude, та обрано найоптимальніше рішення для навчального закладу. Основними перевагами Zabbix стали його масштабованість, підтримка різних типів моніторингу та можливість інтеграції з системами оповіщення через Telegram.

У рамках проєкту було розгорнуто віртуальні машини на сервері Proxmox, налаштовано моніторинг ключових вузлів мережі, таких як маршрутизатори, сервери, IP-камери та точки доступу Wi-Fi, що дозволяє централізовано контролювати їх роботу. Також було створено карти мережі, що дозволяють наочно відстежувати стан кожного вузла і швидко реагувати на потенційні проблеми.

Система оповіщення в Telegram забезпечує миттєве інформування про будь-які збої або критичні ситуації, що значно підвищує ефективність роботи системного адміністратора та дозволяє мінімізувати час на реагування.

Загалом, впроваджена система моніторингу мережі навчального закладу значно спрощує адміністрування, забезпечує безперебійну роботу обладнання та своєчасне вирішення проблем, що виникають у мережі, підвищуючи стабільність і безпеку інфраструктури закладу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Proxmox VE Administration Guide. Proxmox VE. URL: https://pve.proxmox.com/pve-docs/pve-admin-guide.html (date of access: 18.11.2024).

2. Zabbix Manual. Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution. URL: https://www.zabbix.com/documentation/current/en/manual (date of access: 18.11.2024).

3. Telegram Bot API. Telegram APIs. URL: https://core.telegram.org/bots/api (date of access: 18.11.2024).

4. Manual:TOC - MikroTik Wiki. MikroTik Wiki. URL: https://wiki.mikrotik.com/Manual:TOC (date of access: 18.11.2024).

5. Статті. Інтернет-магазин Wi-Fi обладнання ТехноТрейд. URL: https://www.technotrade.com.ua/articles (дата звернення: 18.11.2024).

ДОДАТОК А

Налаштування маршрутизатору

```
# 2024-11-27 11:52:08 by RouterOS 7.14
# software id = CKDQ-TM1F
#
# model = RB3011UiAS
# serial number = HGF09Z0EP33
/interface bridge
add admin-mac=D4:01:C3:A9:78:5D auto-mac=no comment=defconf fast-
forward=no \
    name=bridge
/interface pppoe-client
add add-default-route=yes disabled=no interface=ether1 name=pppoe-
vpu21 \
    use-peer-dns=yes user=vpu-21
/interface list
add comment=defconf name=WAN
add comment=defconf name=LAN
add name=VPN
/ip firewall layer7-protocol
add name=DHCP_req regexp="\\\\x35\\\\x01\\\\x03"
add name=DHCP_disc regexp="\\\\x35\\\\x01\\\\x01"
add name=DHCP_off regexp="\\\\x35\\\\x01\\\\x02"
/ip pool
add name=default-dhcp ranges=192.168.111.50-192.168.111.254
add name=VPN ranges=10.0.0.10-10.0.0.254
/ip dhcp-server
add address-pool=default-dhcp bootp-support=none interface=bridge
lease-time=\
    10m name=defconf server-address=192.168.111.1
/port
set 0 name=serial0
/ppp profile
add interface-list=VPN local-address=10.0.0.1 name=VPN remote-
address=VPN
/snmp community
add addresses=::/0 name=vpu21
/interface bridge port
add bridge=bridge comment=defconf interface=ether2
add bridge=bridge comment=defconf interface=ether3
add bridge=bridge comment=defconf interface=ether4
add bridge=bridge comment=defconf interface=ether5
add bridge=bridge comment=defconf interface=ether6
add bridge=bridge comment=defconf interface=ether7
add bridge=bridge comment=defconf interface=ether8
add bridge=bridge comment=defconf interface=ether9
add bridge=bridge comment=defconf interface=ether10
add bridge=bridge comment=defconf interface=sfp1
/interface bridge settings
set allow-fast-path=no use-ip-firewall=yes
/ip neighbor discovery-settings
set discover-interface-list=LAN
/interface l2tp-server server
set default-profile=VPN enabled=yes use-ipsec=yes
/interface list member
add comment=defconf interface=bridge list=LAN
add comment=defconf interface=ether1 list=WAN
```

```
add interface=pppoe-vpu21 list=WAN
/ip address
add address=192.168.111.1/24 interface=bridge network=192.168.111.0
add address=192.168.100.1/24 interface=bridge network=192.168.100.0
/ip arp
add address=192.168.111.126 interface=bridge mac-
address=28:EE:52:D6:92:43
add address=192.168.111.151 interface=bridge mac-
address=74:FE:CE:47:47:EB
/ip dhcp-client
add comment=defconf disabled=yes interface=ether1
/ip dhcp-server alert
add disabled=no interface=bridge on-alert=alien_DHCP valid-server=\
    D4:01:C3:A9:78:5D
/ip dhcp-server lease
add address=192.168.111.120 client-id=1:bc:24:11:28:d6:9 mac-
address=\
    BC:24:11:28:D6:09 server=defconf
/ip dhcp-server network
add address=192.168.111.0/24 comment=defconf dns-
server=192.168.111.1 domain=\
    vpu21.local gateway=192.168.111.1 netmask=24
/ip dns
set allow-remote-requests=yes cache-max-ttl=1d cache-size=4096KiB
/ip dns static
add address=192.168.88.1 comment=defconf name=router.lan
add address=192.168.111.120 name=Zabbix.vpu21.local
/ip firewall filter
add action=drop chain=input dst-port=53 in-interface-list=WAN
protocol=udp
add action=log chain=input comment=dhcp-req disabled=yes dst-port=67
\
    layer7-protocol=DHCP_req protocol=udp src-mac-
address=28:EE:52:D6:92:43
add action=log chain=input comment=dhcp-disc disabled=yes dst-
port=67 \
    layer7-protocol=DHCP_disc protocol=udp src-mac-
address=28:EE:52:D6:92:43
add action=log chain=output comment=dhcp-off disabled=yes dst-
port=68 \
    layer7-protocol=DHCP_off protocol=udp
add action=accept chain=input in-interface-list=VPN
add action=accept chain=input dst-port=1701,500,4500 in-interface-
list=WAN \
    protocol=udp src-port=""
add action=accept chain=input comment=\
    "defconf: accept established,related,untracked" connection-
state=\
    established,related,untracked
add action=drop chain=input comment="defconf: drop invalid"
connection-state=\
    invalid
add action=accept chain=input comment="defconf: accept ICMP"
protocol=icmp
add action=accept chain=input comment=\
    "defconf: accept to local loopback (for CAPsMAN)" dst-
address=127.0.0.1
add action=drop chain=forward comment=\
    "defconf: drop all from WAN not DSTNATed" connection-nat-
state=!dstnat \
    connection-state=new in-interface-list=WAN
add action=drop chain=input comment="defconf: drop all not coming
from LAN" \
```

```
    in-interface-list=!LAN
add action=accept chain=forward comment="defconf: accept in ipsec
policy" \
    ipsec-policy=in,ipsec
add action=accept chain=forward comment="defconf: accept out ipsec
policy" \
    ipsec-policy=out,ipsec
add action=fasttrack-connection chain=forward comment="defconf:
fasttrack" \
    connection-state=established,related hw-offload=yes
add action=accept chain=forward comment=\
    "defconf: accept established,related, untracked" connection-
state=\
    established,related,untracked
add action=drop chain=forward comment="defconf: drop invalid" \
    connection-state=invalid
add action=accept chain=input in-interface-list=WAN protocol=ipsec-
esp
/ip firewall mangle
add action=change-mss chain=postrouting comment="MSS correction"
new-mss=\
    clamp-to-pmtu out-interface=all-ppp passthrough=yes protocol=tcp
\
    tcp-flags=syn
/ip firewall nat
add action=masquerade chain=srcnat comment="defconf: masquerade" \
    ipsec-policy=out,none out-interface-list=WAN
add action=masquerade chain=srcnat dst-address=192.168.100.0/24 src-
address=\
    192.168.111.0/24
/ipv6 firewall address-list
add address=::/128 comment="defconf: unspecified address"
list=bad_ipv6
add address=::1/128 comment="defconf: lo" list=bad_ipv6
add address=fec0::/10 comment="defconf: site-local" list=bad_ipv6
add address=::ffff:0.0.0.0/96 comment="defconf: ipv4-mapped"
list=bad_ipv6
add address=::/96 comment="defconf: ipv4 compat" list=bad_ipv6
add address=100::/64 comment="defconf: discard only " list=bad_ipv6
add address=2001:db8::/32 comment="defconf: documentation"
list=bad_ipv6
add address=2001:10::/28 comment="defconf: ORCHID" list=bad_ipv6
add address=3ffe::/16 comment="defconf: 6bone" list=bad_ipv6
/ipv6 firewall filter
add action=accept chain=input comment=\
    "defconf: accept established,related,untracked" connection-
state=\
    established,related,untracked
add action=drop chain=input comment="defconf: drop invalid"
connection-state=\
    invalid
add action=accept chain=input comment="defconf: accept ICMPv6"
protocol=\
    icmpv6
add action=accept chain=input comment="defconf: accept UDP
traceroute" \
    dst-port=33434-33534 protocol=udp
add action=accept chain=input comment=\
    "defconf: accept DHCPv6-Client prefix delegation." dst-port=546
protocol=\
    udp src-address=fe80::/10
add action=accept chain=input comment="defconf: accept IKE" dst-
port=500,4500 \
```

```
    protocol=udp
add action=accept chain=input comment="defconf: accept ipsec AH"
protocol=\
    ipsec-ah
add action=accept chain=input comment="defconf: accept ipsec ESP"
protocol=\
    ipsec-esp
add action=accept chain=input comment=\
    "defconf: accept all that matches ipsec policy" ipsec-
policy=in,ipsec
add action=drop chain=input comment=\
    "defconf: drop everything else not coming from LAN" in-
interface-list=\
    !LAN
add action=accept chain=forward comment=\
    "defconf: accept established,related,untracked" connection-
state=\
    established,related,untracked
add action=drop chain=forward comment="defconf: drop invalid" \
    connection-state=invalid
add action=drop chain=forward comment=\
    "defconf: drop packets with bad src ipv6" src-address-
list=bad_ipv6
add action=drop chain=forward comment=\
    "defconf: drop packets with bad dst ipv6" dst-address-
list=bad_ipv6
add action=drop chain=forward comment="defconf: rfc4890 drop hop-
limit=1" \
    hop-limit=equal:1 protocol=icmpv6
add action=accept chain=forward comment="defconf: accept ICMPv6"
protocol=\
    icmpv6
add action=accept chain=forward comment="defconf: accept HIP"
protocol=139
add action=accept chain=forward comment="defconf: accept IKE" dst-
port=\
    500,4500 protocol=udp
add action=accept chain=forward comment="defconf: accept ipsec AH"
protocol=\
    ipsec-ah
add action=accept chain=forward comment="defconf: accept ipsec ESP"
protocol=\
    ipsec-esp
add action=accept chain=forward comment=\
    "defconf: accept all that matches ipsec policy" ipsec-
policy=in,ipsec
add action=drop chain=forward comment=\
    "defconf: drop everything else not coming from LAN" in-
interface-list=\
    !LAN
/ppp secret
add name=Lynx profile=VPN
add name=Pilyavskyi profile=VPN
/snmp
set enabled=yes
/system clock
set time-zone-name=Europe/Kiev
/system note
set show-at-login=no
/system routerboard settings
set enter-setup-on=delete-key
/system scheduler
add disabled=yes interval=5m name=schedule1 on-event=\
```

```
    "/system script run  DHCP2DNS_FULLUPDATE" policy=read,write,test
\
    start-date=2024-10-05 start-time=18:26:45
/system script
add dont-require-permissions=no name=alien_DHCP owner=Lynx policy=\
    read,write,test source=":log info \"Allert. Found alien DHCP\""
add dont-require-permissions=no name=DHCP2DNS_FULLUPDATE owner=Lynx
policy=\
    read,write,test source="# Here are three linked system
scripts.\r\
    \n# The first one creates a new static DNS records,\r\
    \n# the second one cleans up orphaned records,\r\
    \n# and the third one resolves loadbalancer IP addresses from
hostnames in\
    \_port forwarding rules.\r\
    \n/system script run DHCP2DNS_CLEANUP\r\
    \n\r\
    \n# DHCP2DNS_FULLUPDATE\r\
    \n\r\
    \n:foreach lease in=[/ip dhcp-server lease find] do={    \r\
    \n    :local hostName [/ip dhcp-server lease get \$lease host-
name]\r\
    \n    :local leaseStatus [/ip dhcp-server lease get \$lease
status]\r\
    \n\r\
    \n    # Skip if hostName is empty or lease is not active\r\
    \n    :if ( ( [ :len \$hostName ] > 0 ) and (\$leaseStatus =
\"bound\") ) \
    do={\r\
    \n\r\
    \n        :local ipAddress [/ip dhcp-server lease get \$lease
address]\r\
    \n        :local ttl [/ip dhcp-server lease get \$lease expires-
after]\r\
    \n        \r\
    \n        :local networkId [/ip dhcp-server network find where
\$ipAddress\
    \_in address]\r\
    \n        :local domainName [/ip dhcp-server network get
\$networkId domai\
    n]\r\
    \n        :local fqdn \"\$hostName.\$domainName\"\r\
    \n\r\
    \n        # Remove any existing DNS entries with the same
hostname and #DH\
    CP comment\r\
    \n        :foreach oldRecord in=[/ip dns static find where
name=\$fqdn and\
    \_comment=\"#DHCP\"] do={\r\
    \n            :log info \"Removing old DNS entry for \$fqdn with
IP [/ip d\
    ns static get \$oldRecord address]\"\r\
    \n            /ip dns static remove \$oldRecord\r\
    \n        }\r\
    \n\r\
    \n        # Add a new DNS entry with the #DHCP comment\r\
    \n        :log info \"Creating DNS entry for \$fqdn with IP
\$ipAddress\"\
    \r\
    \n        /ip dns static add address=\$ipAddress name=\$fqdn
ttl=\$ttl com\
    ment=\"#DHCP\" disabled=no\r\
    \n    }\r\
```

```
    \n}"
add dont-require-permissions=no name=DHCP2DNS_CLEANUP owner=Lynx
policy=\
    read,write,test source="/# DHCP2DNS_CLEANUP\r\
    \n\r\
    \n# Remove static DNS entries that are no longer in the DHCP
lease list\r\
    \n:foreach dnsRecord in=[/ip dns static find where
comment~\"#DHCP\"] do={\
    \r\
    \n\r\
    \n    :local dnsName [/ip dns static get \$dnsRecord name]\r\
    \n    :local dnsTTL [/ip dns static get \$dnsRecord ttl]\r\
    \n    :local dnsAddress [/ip dns static get \$dnsRecord
address]\r\
    \n    \r\
    \n    :local found false\r\
    \n\r\
    \n    :log info \"Checking DNS entry: \$dnsName with IP
\$dnsAddress and T\
    TL \$dnsTTL\"\r\
    \n\r\
    \n    # Check if the DNS name exists in the DHCP lease list\r\
    \n    :foreach lease in=[/ip dhcp-server lease find] do={\r\
    \n        :local hostName [/ip dhcp-server lease get \$lease
host-name]\r\
    \n        :local ipAddress [/ip dhcp-server lease get \$lease
address]\r\
    \n        :local ttl [/ip dhcp-server lease get \$lease expires-
after]\r\
    \n        \r\
    \n        # Validate hostname and IP address are not empty\r\
    \n        :if ([:len \$hostName] > 0 and [:len \$ipAddress] > 0)
do={\r\
    \n\r\
    \n            # Find the corresponding network for the lease's
IP address\
    \r\
    \n            :local networkId [/ip dhcp-server network find
where \$ipAdd\
    ress in address]\r\
    \n\r\
    \n            # Ensure networkId is valid\r\
    \n            :if ([:len \$networkId] > 0) do={\r\
    \n                :local domainName [/ip dhcp-server network get
\$network\
    Id domain]\r\
    \n                :local fqdn \"\$hostName.\$domainName\"\r\
    \n\r\
    \n                :log info \"Comparing FQDN \$fqdn with DNS
entry \$dnsNa\
    me\"\r\
    \n\r\
    \n                :if (\$fqdn = \$dnsName) do={\r\
    \n                    :set found true\r\
    \n                    \r\
    \n                    # Update TTL if it's different\r\
    \n                    :if (\$dnsTTL != \$ttl) do={\r\
    \n                        :log info \"Updating TTL for \$dnsName
from \$dn\
    sTTL to \$ttl\"\r\
    \n                        /ip dns static set \$dnsRecord
ttl=\$ttl\r\
```

```
    \n                    } else={\r\
    \n                        :log info \"TTL for \$dnsName is
already up-to-d\
    ate\"\r\
    \n                    }\r\
    \n\r\
    \n                    :break\r\
    \n                }\r\
    \n            } else={\r\
    \n                :log warning \"No network found for IP
\$ipAddress, skip\
    ping this lease entry\"\r\
    \n            }\r\
    \n        } else={\r\
    \n            :log warning \"Invalid hostName or ipAddress,
skipping this \
    lease entry\"\r\
    \n        }\r\
    \n    }\r\
    \n\r\
    \n    # If not found, remove the DNS static entry\r\
    \n    :if (!\$found) do={\r\
    \n        :log info \"Removing stale DNS entry: \$dnsName with
IP \$dnsAdd\
    ress\"\r\
    \n        /ip dns static remove \$dnsRecord\r\
    \n    }\r\
    \n}"
/tool mac-server
set allowed-interface-list=LAN
/tool mac-server mac-winbox
set allowed-interface-list=LAN
```

ДОДАТОК Б

Налаштування Zabbix

Конфігурація вузлів


```
{
    "zabbix_export": {
        "version": "7.0",
        "host_groups": [
            {
                "uuid": "a571c0d144b14fd4a87a9d9b2aa9fcd6",
                "name": "Applications"
            },
            {
                "uuid": "f2481361f99448eea617b7b1d4765566",
                "name": "Discovered hosts"
            },
            {
                "uuid": "4b9bc90514354d9db34145f68d8f3736",
                "name": "IP cam"
            },
            {
                "uuid": "dc579cd7a1a34222933f24f52a68bcd8",
                "name": "Linux servers"
            },
            {
                "uuid": "137f19e6e2dc4219b33553b812627bc2",
                "name": "Virtual machines"
            },
            {
                "uuid": "bf880e08a6a84800af5afcdcf0381a82",
                "name": "Wi-Fi"
            },
            {
                "uuid": "6f6799aa69e844b4b3918f779f2abf08",
                "name": "Zabbix servers"
            }
        ],
        "hosts": [
            {
                "host": "192.168.111.1",
                "name": "MicroTik 3011 router",
                "templates": [
                    {
                        "name": "MikroTik RB3011UiAS-RM by SNMP"
                    }
                ],
                "groups": [
                    {
                        "name": "Applications"
                    }
                ],
                "interfaces": [
                    {
                        "type": "SNMP",
                        "ip": "192.168.111.1",
```

```
                            "port": "161",
                            "details": {
                                "community": "{$SNMP_COMMUNITY}"
                            },
                            "interface_ref": "if1"
                        }
                    ],
                    "inventory": {
                        "name": "MikroTik",
                        "os": "7.14",
                        "serialno_a": "HGF09Z0EP33",
                        "location_lat": "46.956505",
                        "location_lon": "32.000980",
                        "model": "RouterOS RB3011UiAS"
                    },
                    "inventory_mode": "AUTOMATIC"
                },
                {
                    "host": "AccountingDepartmentVPU21",
                    "name": "AccountingDepartmentVPU21",
                    "templates": [
                        {
                            "name": "ICMP Ping"
                        }
                    ],
                    "groups": [
                        {
                            "name": "Wi-Fi"
                        }
                    ],
                    "interfaces": [
                        {
                            "useip": "NO",
                            "ip": "",
                            "dns":
"AccountingDepartmentVPU21.vpu21.local",
                            "interface_ref": "if1"
                        }
                    ],
                    "inventory_mode": "DISABLED"
                },
                {
                    "host": "CableWireProcessing",
                    "name": "CableWireProcessing",
                    "templates": [
                        {
                            "name": "ICMP Ping"
                        }
                    ],
                    "groups": [
                        {
                            "name": "Wi-Fi"
                        }
                    ],
                    "interfaces": [
                        {
                            "useip": "NO",
                            "ip": "",
                            "dns": "CableWireProcessing.vpu21.local",
                            "interface_ref": "if1"
                        }
                    ],
                    "inventory_mode": "DISABLED"
```

```
    },
    {
        "host": "Camera21",
        "name": "Camera21",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "IP cam"
            }
        ],
        "interfaces": [
            {
                "ip": "192.168.100.21",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Camera44",
        "name": "Camera44",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "IP cam"
            }
        ],
        "interfaces": [
            {
                "ip": "192.168.111.44",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Camera201",
        "name": "Camera201",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "IP cam"
            }
        ],
        "interfaces": [
            {
                "ip": "192.168.100.201",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
```

```
    },
    {
        "host": "Camera203",
        "name": "Camera203",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "IP cam"
            }
        ],
        "interfaces": [
            {
                "ip": "192.168.100.203",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Camera204",
        "name": "Camera204",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "IP cam"
            }
        ],
        "interfaces": [
            {
                "ip": "192.168.100.204",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Camera205",
        "name": "Camera205",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "IP cam"
            }
        ],
        "interfaces": [
            {
                "ip": "192.168.100.205",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
```

```
    },
    {
        "host": "Camera206",
        "name": "Camera206",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "IP cam"
            }
        ],
        "interfaces": [
            {
                "ip": "192.168.100.206",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Camera207",
        "name": "Camera207",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "IP cam"
            }
        ],
        "interfaces": [
            {
                "ip": "192.168.100.207",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Camera208",
        "name": "Camera208",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "IP cam"
            }
        ],
        "interfaces": [
            {
                "ip": "192.168.100.208",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
```

```
    },
    {
        "host": "Camera209",
        "name": "Camera209",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "IP cam"
            }
        ],
        "interfaces": [
            {
                "ip": "192.168.100.209",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Camera210",
        "name": "Camera210",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "IP cam"
            }
        ],
        "interfaces": [
            {
                "ip": "192.168.100.210",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Camera211",
        "name": "Camera211",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "IP cam"
            }
        ],
        "interfaces": [
            {
                "ip": "192.168.100.211",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
```

```
    },
    {
        "host": "Camera212",
        "name": "Camera212",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "IP cam"
            }
        ],
        "interfaces": [
            {
                "ip": "192.168.100.212",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Camera213",
        "name": "Camera213",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "IP cam"
            }
        ],
        "interfaces": [
            {
                "ip": "192.168.100.213",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Camera214",
        "name": "Camera214",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "IP cam"
            }
        ],
        "interfaces": [
            {
                "ip": "192.168.100.214",
                "interface_ref": "if1"
            }
        ],
        "inventory": {
```

```
            "url_a": "http://192.168.111.8"
        }
    },
    {
        "host": "Camera215",
        "name": "Camera215",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "IP cam"
            }
        ],
        "interfaces": [
            {
                "ip": "192.168.100.215",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Director",
        "name": "Director",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "Wi-Fi"
            }
        ],
        "interfaces": [
            {
                "useip": "NO",
                "ip": "",
                "dns": "Director.vpu21.local",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "ElectronicEngineer",
        "name": "ElectronicEngineer",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "Wi-Fi"
            }
        ],
        "interfaces": [
            {
                "useip": "NO",
```

```
                "ip": "",
                "dns": "ElectronicEngineer",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "EnglishKab9",
        "name": "EnglishKab9",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "Wi-Fi"
            }
        ],
        "interfaces": [
            {
                "useip": "NO",
                "ip": "",
                "dns": "EnglishKab9.vpu21.local",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Hurtozhytok-1-1",
        "name": "Hurtozhytok-1-1",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "Wi-Fi"
            }
        ],
        "interfaces": [
            {
                "useip": "NO",
                "ip": "",
                "dns": "Hurtozhytok-1-1.vpu21.local",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Kab-14",
        "name": "Kab-14",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
```

```
                "name": "Wi-Fi"
            }
        ],
        "interfaces": [
            {
                "useip": "NO",
                "ip": "",
                "dns": "Kab-14.vpu21.local",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Kab07",
        "name": "Kab07",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "Wi-Fi"
            }
        ],
        "interfaces": [
            {
                "useip": "NO",
                "ip": "",
                "dns": "Kab07.vpu21.local",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Kab12",
        "name": "Kab12",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "Wi-Fi"
            }
        ],
        "interfaces": [
            {
                "useip": "NO",
                "ip": "",
                "dns": "Kab12.vpu21.local",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Kab13",
        "name": "Kab13",
        "templates": [
```

```
                {
                    "name": "ICMP Ping"
                }
            ],
            "groups": [
                {
                    "name": "Wi-Fi"
                }
            ],
            "interfaces": [
                {
                    "useip": "NO",
                    "ip": "",
                    "dns": "Kab13.vpu21.local",
                    "interface_ref": "if1"
                }
            ],
            "inventory_mode": "DISABLED"
        },
        {
            "host": "Kab17",
            "name": "Kab17",
            "templates": [
                {
                    "name": "ICMP Ping"
                }
            ],
            "groups": [
                {
                    "name": "Wi-Fi"
                }
            ],
            "interfaces": [
                {
                    "useip": "NO",
                    "ip": "",
                    "dns": "Kab17.vpu21.local",
                    "interface_ref": "if1"
                }
            ],
            "inventory_mode": "DISABLED"
        },
        {
            "host": "Kab19",
            "name": "Kab19",
            "templates": [
                {
                    "name": "ICMP Ping"
                }
            ],
            "groups": [
                {
                    "name": "Wi-Fi"
                }
            ],
            "interfaces": [
                {
                    "useip": "NO",
                    "ip": "",
                    "dns": "Kab19.vpu21.local",
                    "interface_ref": "if1"
                }
            ],
```

```
            "inventory_mode": "DISABLED"
        },
        {
            "host": "Kab20",
            "name": "Kab20",
            "templates": [
                {
                    "name": "ICMP Ping"
                }
            ],
            "groups": [
                {
                    "name": "Wi-Fi"
                }
            ],
            "interfaces": [
                {
                    "useip": "NO",
                    "ip": "",
                    "dns": "Kab20.vpu21.local",
                    "interface_ref": "if1"
                }
            ],
            "inventory_mode": "DISABLED"
        },
        {
            "host": "Kab22",
            "name": "Kab22",
            "templates": [
                {
                    "name": "ICMP Ping"
                }
            ],
            "groups": [
                {
                    "name": "Wi-Fi"
                }
            ],
            "interfaces": [
                {
                    "useip": "NO",
                    "ip": "",
                    "dns": "Kab22.vpu21.local",
                    "interface_ref": "if1"
                }
            ],
            "inventory_mode": "DISABLED"
        },
        {
            "host": "Kab23",
            "name": "Kab23",
            "templates": [
                {
                    "name": "ICMP Ping"
                }
            ],
            "groups": [
                {
                    "name": "Wi-Fi"
                }
            ],
            "interfaces": [
                {
```

```
                "useip": "NO",
                "ip": "",
                "dns": "Kab23.vpu21.local",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Kab26",
        "name": "Kab26",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "Wi-Fi"
            }
        ],
        "interfaces": [
            {
                "useip": "NO",
                "ip": "",
                "dns": "Kab26.vpu21.local",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Kab27",
        "name": "Kab27",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "Wi-Fi"
            }
        ],
        "interfaces": [
            {
                "useip": "NO",
                "ip": "",
                "dns": "Kab27.vpu21.local",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Kab28",
        "name": "Kab28",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
```

```
            {
                "name": "Wi-Fi"
            }
        ],
        "interfaces": [
            {
                "useip": "NO",
                "ip": "",
                "dns": "linux-500ff5a3be20.vpu21.local",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Kab33",
        "name": "Kab33",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "Wi-Fi"
            }
        ],
        "interfaces": [
            {
                "useip": "NO",
                "ip": "",
                "dns": "Kab33.vpu21.local",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Kab47",
        "name": "Kab47",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "Wi-Fi"
            }
        ],
        "interfaces": [
            {
                "useip": "NO",
                "ip": "",
                "dns": "Kab47.vpu21.local",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Kab53",
        "name": "Kab53",
```

```
                    "templates": [
                        {
                            "name": "ICMP Ping"
                        }
                    ],
                    "groups": [
                        {
                            "name": "Wi-Fi"
                        }
                    ],
                    "interfaces": [
                        {
                            "useip": "NO",
                            "ip": "",
                            "dns": "Kab53.vpu21.local",
                            "interface_ref": "if1"
                        }
                    ],
                    "inventory_mode": "DISABLED"
                },
                {
                    "host": "LaboratoryShipElectrical",
                    "name": "LaboratoryShipElectrical",
                    "templates": [
                        {
                            "name": "ICMP Ping"
                        }
                    ],
                    "groups": [
                        {
                            "name": "Wi-Fi"
                        }
                    ],
                    "interfaces": [
                        {
                            "useip": "NO",
                            "ip": "",
                            "dns":
"LaboratoryShipElectrical.vpu21.local",
                            "interface_ref": "if1"
                        }
                    ],
                    "inventory_mode": "DISABLED"
                },
                {
                    "host": "Library",
                    "name": "Library",
                    "templates": [
                        {
                            "name": "ICMP Ping"
                        }
                    ],
                    "groups": [
                        {
                            "name": "Wi-Fi"
                        }
                    ],
                    "interfaces": [
                        {
                            "useip": "NO",
                            "ip": "",
                            "dns": "Library.vpu21.local",
                            "interface_ref": "if1"
```

```
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "MastersRoom",
        "name": "MastersRoom",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "Wi-Fi"
            }
        ],
        "interfaces": [
            {
                "useip": "NO",
                "ip": "",
                "dns": "MastersRoom.vpu21.local",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Methodist",
        "name": "Methodist",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "Wi-Fi"
            }
        ],
        "interfaces": [
            {
                "useip": "NO",
                "ip": "",
                "dns": "Methodist.vpu21.local",
                "interface_ref": "if1"
            }
        ],
        "inventory_mode": "DISABLED"
    },
    {
        "host": "Polygpraphy",
        "name": "Polygpraphy",
        "templates": [
            {
                "name": "ICMP Ping"
            }
        ],
        "groups": [
            {
                "name": "Wi-Fi"
            }
        ],
```

```
            "interfaces": [
                {
                    "useip": "NO",
                    "ip": "",
                    "dns": "Polygpraphy.vpu21.local",
                    "interface_ref": "if1"
                }
            ],
            "inventory_mode": "DISABLED"
        },
        {
            "host": "PrimalCommission",
            "name": "PrimalCommission",
            "templates": [
                {
                    "name": "ICMP Ping"
                }
            ],
            "groups": [
                {
                    "name": "Wi-Fi"
                }
            ],
            "interfaces": [
                {
                    "useip": "NO",
                    "ip": "",
                    "dns": "PrimalCommission.vpu21.local",
                    "interface_ref": "if1"
                }
            ],
            "inventory_mode": "DISABLED"
        },
        {
            "host": "Proxmox",
            "name": "Proxmox",
            "templates": [
                {
                    "name": "Linux by Zabbix agent"
                },
                {
                    "name": "Proxmox VE by HTTP"
                }
            ],
            "groups": [
                {
                    "name": "Linux servers"
                },
                {
                    "name": "Virtual machines"
                }
            ],
            "interfaces": [
                {
                    "ip": "192.168.111.3",
                    "interface_ref": "if1"
                }
            ],
            "macros": [
                {
                    "macro": "{$PVE.TOKEN.ID}",
                    "value": "Zabbix@pam!monitiring",
```

```
                        "description": "API tokens allow stateless
access to most parts of the REST API by another system, software or
API client."
                    },
                    {
                        "macro": "{$PVE.TOKEN.SECRET}",
                        "value": "94fbad50-413e-470a-b913-
3d5e82638fba",
                        "description": "Secret key."
                    },
                    {
                        "macro": "{$PVE.URL.HOST}",
                        "value": "192.168.111.3",
                        "description": "The hostname or IP address
of the Proxmox VE API host."
                    }
                ],
                "inventory_mode": "DISABLED"
            },
            {
                "host": "Psychologist",
                "name": "Psychologist",
                "templates": [
                    {
                        "name": "ICMP Ping"
                    }
                ],
                "groups": [
                    {
                        "name": "Wi-Fi"
                    }
                ],
                "interfaces": [
                    {
                        "useip": "NO",
                        "ip": "",
                        "dns": "Psychologist.vpu21.local",
                        "interface_ref": "if1"
                    }
                ],
                "inventory_mode": "DISABLED"
            },
            {
                "host": "SeniorMasterElectrician",
                "name": "SeniorMasterElectrician",
                "templates": [
                    {
                        "name": "ICMP Ping"
                    }
                ],
                "groups": [
                    {
                        "name": "Wi-Fi"
                    }
                ],
                "interfaces": [
                    {
                        "useip": "NO",
                        "ip": "",
                        "dns":
"SeniorMasterElectrician.vpu21.local",
                        "interface_ref": "if1"
                    }
```

```
                    ],
                    "inventory_mode": "DISABLED"
                },
                {
                    "host": "Teachers",
                    "name": "Teachers",
                    "templates": [
                        {
                            "name": "ICMP Ping"
                        }
                    ],
                    "groups": [
                        {
                            "name": "Wi-Fi"
                        }
                    ],
                    "interfaces": [
                        {
                            "useip": "NO",
                            "ip": "",
                            "dns": "Teachers.vpu21.local",
                            "interface_ref": "if1"
                        }
                    ],
                    "inventory_mode": "DISABLED"
                },
                {
                    "host": "TechnologyElectricalWorks",
                    "name": "TechnologyElectricalWorks",
                    "templates": [
                        {
                            "name": "ICMP Ping"
                        }
                    ],
                    "groups": [
                        {
                            "name": "Wi-Fi"
                        }
                    ],
                    "interfaces": [
                        {
                            "useip": "NO",
                            "ip": "",
                            "dns":
"TechnologyElectricalWorks.vpu21.local",
                            "interface_ref": "if1"
                        }
                    ],
                    "inventory_mode": "DISABLED"
                },
                {
                    "host": "Tenda",
                    "name": "Tenda",
                    "templates": [
                        {
                            "name": "ICMP Ping"
                        }
                    ],
                    "groups": [
                        {
                            "name": "Wi-Fi"
                        }
                    ],
```

```
            "interfaces": [
                {
                    "useip": "NO",
                    "ip": "",
                    "dns": "Tenda.vpu21.local",
                    "interface_ref": "if1"
                }
            ],
            "inventory_mode": "DISABLED"
        },
        {
            "host": "VideoReg",
            "name": "VideoReg",
            "templates": [
                {
                    "name": "ICMP Ping"
                }
            ],
            "groups": [
                {
                    "name": "IP cam"
                }
            ],
            "interfaces": [
                {
                    "ip": "192.168.100.200",
                    "interface_ref": "if1"
                }
            ],
            "inventory_mode": "DISABLED"
        },
        {
            "host": "Video_reg",
            "name": "Video_reg",
            "templates": [
                {
                    "name": "ICMP Ping"
                }
            ],
            "groups": [
                {
                    "name": "IP cam"
                }
            ],
            "interfaces": [
                {
                    "ip": "192.168.100.10",
                    "interface_ref": "if1"
                }
            ],
            "inventory_mode": "DISABLED"
        },
        {
            "host": "WinSRV",
            "name": "WinSRV",
            "templates": [
                {
                    "name": "Windows by Zabbix agent"
                }
            ],
            "groups": [
                {
                    "name": "Discovered hosts"
```

```
                    }
                ],
                "interfaces": [
                    {
                        "ip": "192.168.111.2",
                        "interface_ref": "if1"
                    }
                ],
                "inventory_mode": "DISABLED"
            },
            {
                "host": "Zabbix server",
                "name": "Zabbix server",
                "templates": [
                    {
                        "name": "Linux by Zabbix agent"
                    },
                    {
                        "name": "Zabbix server health"
                    }
                ],
                "groups": [
                    {
                        "name": "Zabbix servers"
                    }
                ],
                "interfaces": [
                    {
                        "interface_ref": "if1"
                    }
                ],
                "inventory": {
                    "name": "appliance",
                    "os": "Linux version 4.18.0-
553.16.1.el8_10.x86_64 (mockbuild@x64-builder02.almalinux.org) (gcc
version 8.5.0 20210514 (Red Hat 8.5.0-2",
                    "location_lat": "46.956505",
                    "location_lon": "32.000980"
                },
                "inventory_mode": "AUTOMATIC"
            }
        ]
    }
}
```