МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ІМЕНІ ІГОРЯ СІКОРСЬКОГО»

Моніторинг мультисервісних мереж

КОМП'ЮТЕРНИЙ ПРАКТИКУМ

*Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для студентів, які навчаються за спеціальністю
121 «Інженерія програмного забезпечення»*

Київ
КПІ ім. Ігоря Сікорського
2020

Моніторинг мультисервісних мереж. Комп’ютерний практикум: навч. посіб. для студентів спеціальності 121 - «Інженерія програмного забезпечення» денної форми навчання / Укладач: Федорова Н.В.; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 10,6 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2020. – 105 с.

Гриф надано Методичною радою КПІ ім. Ігоря Сікорського (протокол №4 від 4.12.2020 р.) за поданням Вченої ради факультету (протокол №5 від 30.11.2020 р.)

Електронне мережне навчальне видання
МОНІТОРИНГ МУЛЬТИСЕРВІСНИХ МЕРЕЖ
Комп’ютерний практикум

Укладач: *Федорова Наталія Володимирівна, д. т. н.*

Відповідальний редактор: *Коваль О.В., к. т. н., доцент*

Рецензент: *Дичка І.А., д. т. н., професор*

Посібник розроблений на підставі робочої програми освітнього компоненту 2Ф-каталогу навчальної та професійної магістратури з дисципліни “Моніторинг мультисервісних мереж”, що призначений для якісної організації виконання лабораторних робіт студентами та розуміння роботи програм мережевого моніторингу, обсягом 27 годин.

Призначений для студентів, які навчаються за освітньою програмою «Інженерія програмного забезпечення інтелектуальних кібер-фізичних систем і веб-технологій» підготовки магістрів за спеціальністю 121 – «Інженерія програмного забезпечення» денної форми навчання.

Спрямований на формування у студентів умінь та набуття практичних навичок, пов’язаних із роботою програм для моніторингу мультисервісних мереж, оцінюванням складності та ефективності програм за допомогою сучасних засобів профілювання.

Забезпечує студентів необхідними теоретичними знаннями для опанування відповідної теми комп’ютерного практикуму та виконання завдань, запланованих впродовж семестру. Містить короткий теоретичний опис, методичні поради виконання комп’ютерних практикумів.

ЗМІСТ

Вступ

Одним з напрямків діяльності магістра за спеціальністю 121 «Інженерія програмного забезпечення» освітньої програми «Інженерія програмного забезпечення інтелектуальних кібер-фізичних систем і веб-технологій» є розуміння поняття мережевого моніторингу.

Для якісної та безперебійної роботи мережі адміністраторам доводиться невпинно за нею стежити. Моніторинг мережі – це складне завдання, яке потребує великих витрат сил та є життєво важливою частиною роботи мережевих адміністраторів. Моніторинг та аналіз трафіку необхідні для того, щоб ефективніше діагностувати та вирішувати проблеми, не доводячи мережеві сервіси до «простою» протягом тривалого часу. Сьогодні відомі програми моніторингу, орієнтовані на маршрутизатори й не орієнтовані на маршрутизатори; останні поділяються на активні і пасивні. Моніторинг, який вбудований в маршрутизатори і не вимагає додаткового встановлення програмного або апаратного забезпечення, називають основаним на маршрутизаторах. На противагу їм є моніторинг, що не ґрунтується на маршрутизаторах, але вимагає встановлення спеціального апаратного та програмного забезпечення. Мережевий моніторингу тісно пов'язаний зі завданнями забезпечення ефективного завантаження обладнання, безперебійної роботи мережі та запобіганням несанкціонованим атакам на мережу.

Для точної ідентифікації проблеми обов'язково використовуються дані одночасно з декількох програм. Виділяють програми для моніторингу мережі та програми для моніторингу послуг.

Тому завданням даного навчального посібника, відповідно до робочої навчальної програми курсу «Моніторинг мультисервісних мереж», є розгляд ряду програм для моніторингу, які використовуються службами моніторингу на профільних підприємствах для детектування можливих проблем на мережах та засвоєння студентами даних програм для моніторингу мультисервісних мереж, принципів їх дії та можливостей.

Загальний порядок виконання комп'ютерних практикумів:

- ознайомитися з теоретичними відомостями до відповідного комп'ютерного практикуму;
- сумлінно виконати отримане завдання;
- скласти протокол комп'ютерного практикуму;
- здати та захистити комп'ютерний практикум.

Вимоги до оформлення протоколів комп'ютерних практикумів

Протокол комп'ютерного практикуму охайно оформлюється у вигляді текстового файлу.

На титульному аркуші зверху з вирівнюванням по центру вказують назву університету, факультету та кафедри. Нижче під ними розміщують номер, назву комп'ютерного практикуму; ще нижче, з вирівнюванням вправо, вказують прізвище автора роботи, групу та прізвище викладача, який буде здійснювати перевірку роботи.

На наступних листах вказують мету роботи та розміщують результати відповідної роботи.

Для захисту комп'ютерного практикуму необхідно:

- надати протокол з результатами роботи;
- продемонструвати роботу програмного продукту;
- відповісти на запитання викладача.

Комп’ютерний практикум №1

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ TOTAL NETWORK MONITOR 2

Мета роботи – ознайомлення та отримання досвіду використання програми моніторингу Total Network Monitor 2.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Total Network Monitor 2 (TNM 2) - це програма для спостереження за роботою локальної мережі окремих комп'ютерів, мережевих і системних служб. У разі неполадок або непередбачених помилок Total Network Monitor сповістить вас і сформує докладний звіт. Ви завжди маєте можливість перевірити будь-який аспект роботи тієї чи іншої служби, сервера або файлової системи: FTP, POP/SMTP, HTTP, IMAP, Registry, Event Log, Service State і безліч інших.

Total Network Monitor може бути централізовано встановлений на Windows сервер. Всі типи мережевих вузлів можна відстежувати, включаючи комп'ютери, що працюють під Windows, Linux, Mac OS X, широкий діапазон мережевих пристроїв, бездротових точок доступу і пристроїв. Total Network Monitor може стежити за всім, що володіє IP адресою (див. рисунок 1.1) [1].

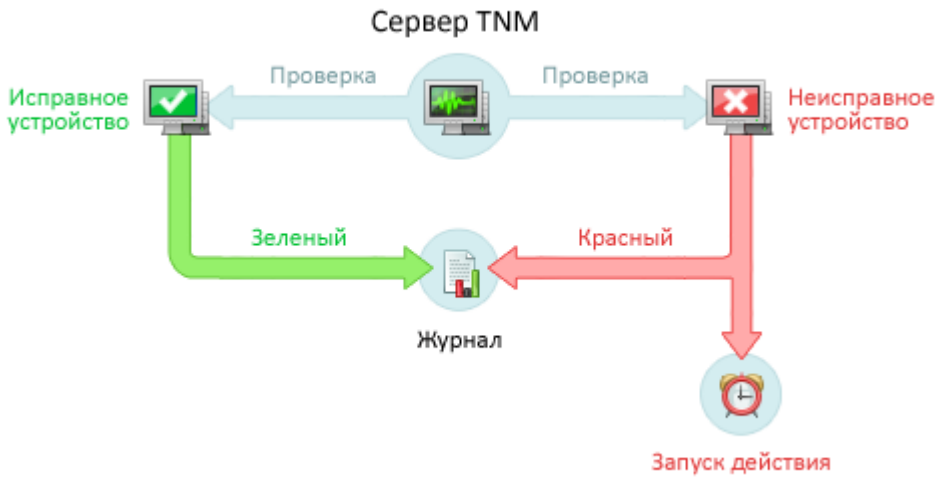


Рисунок 1.1 - Відстеження пристроїв з IP адресою

Ви створюєте Монітори - об'єкти, які періодично перевіряють той чи інший аспект роботи служби, сервера або файлової системи. Монітори гнучко налаштовуються і відображають стан мережі в реальному часі. При відхиленні будь-яких показників від норми, монітор виконує описаний заздалегідь сценарій дій: наприклад, звуковий сигнал, оповіщення по e-mail або IM з докладним описом події, перезавантаження віддаленого комп'ютера, запуск програми і т. п. Звернувшись до журналу моніторингу мережі, ви завжди можете побачити історію показань всіх моніторів і список виконаних дій.

Перевірки працездатності і проблем

Перевірки - зв'язок Total Network Monitor 2 із зовнішнім світом. Саме вони надають моніторам дані для аналізу. У TNM 2 для моніторингу мережі існує безліч перевірок для

будь яких випадків (див. рисунок 1.2). Запити по мережевих протоколах для моніторингу серверів, перевірка служб, журналу подій і ключів реєстру Windows, пошук рядка у файлі на віддаленому комп'ютері і багато іншого (таблиця 1.1) [1].

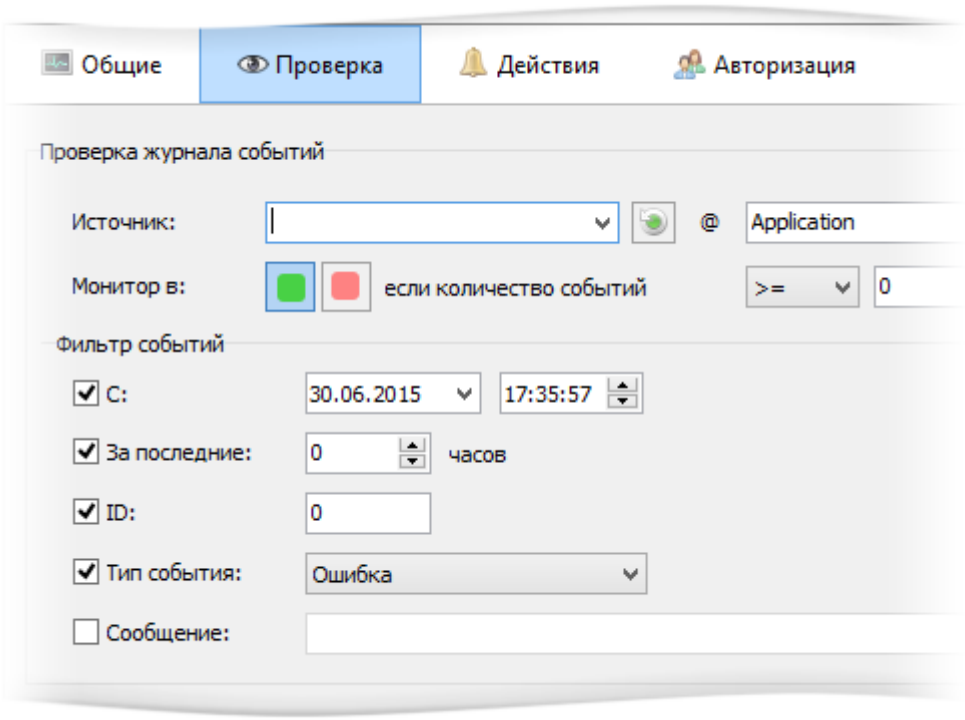


Рисунок 1.2 - Перевірки працездатності і проблем

Таблиця 1.1

Список перевірок		
Інтернет	Windows	Файлові
• ICMP • TCP • HTTP • FTP • SMTP • POP3 • IMAP • Telnet	• Журнал подій • Стан служби • Стан реєстру • Продуктивність системи	• Існування файлу • Розмір файлу • Порівняння файлів • Число файлів • CRC32 файлу • Вміст файлу • Місце на диску

Оповіщення та історія подій

Дії спрацьовують, як тільки що-небудь йде не за планом. Вони сповіщають вас, щоб ви могли вчасно все виправити (див. рисунок 1.3). Вони можуть надати першу допомогу в адмініструванні локальної мережі: перезавантажити службу або віддалений комп'ютер, запустити додаток, виконати скрипт (таблиця 1.2) [1]. А можуть і просто додати запис в окремий журнал.

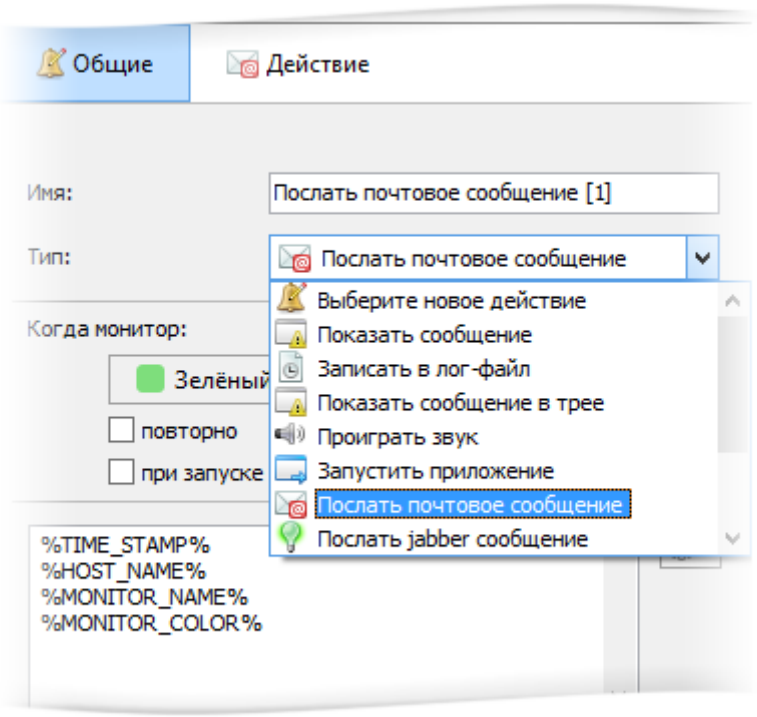


Рисунок 1.3 - Перевірки працездатності і проблем

Таблиця 1.2

Список перевірок		
Попередження	Оповіщення	Міра
• Вікно повідомлення • Повідомлення • Звуковий сигнал • Запис у файл	• E-mail • Jabber • Журнал подій	• Запустити додаток • Виконати скрипт • Перезапустити службу • Перезапустити комп'ютер

Всі виконані дії і всі зміни спостережуваних параметрів безперервно заносяться в журнал, формуючи наочну картину стану мережі.

Запис перевірок в журнал моніторів

Total Network Monitor 2 веде спостереження за всіма працюючими моніторами і записує необхідну інформацію про роботу перевірок. Будь-яка зміна стану монітора фіксується в журналі моніторів (див. рисунок 1.4) [1].

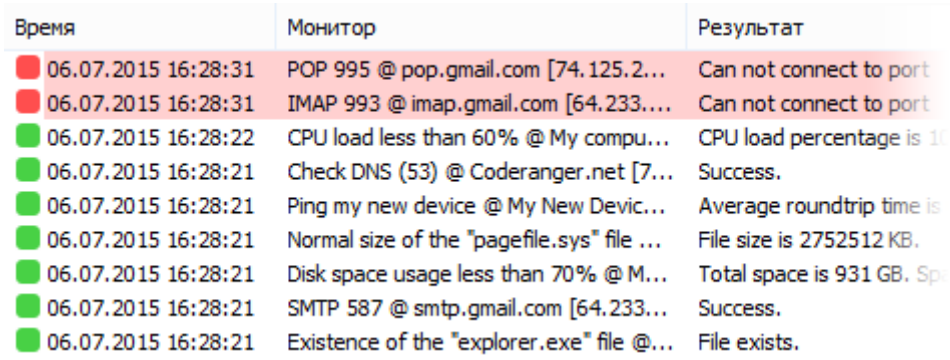


Рисунок 1.4 - Перевірки працездатності і проблем

Статистика та діаграма активності

Статистика включає в себе час запуску і останньої перевірки обраного монітора, загальна кількість і кількість зелених, червоних і чорних станів монітора. Окремим інструментом можна назвати діаграму активності, яка графічно відображає результати перевірки обраного монітора (див. рисунок 1.5) [1].

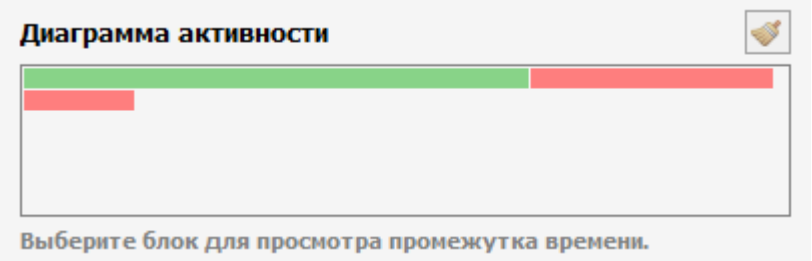


Рисунок 1.5 - Перевірки працездатності і проблем

Контроль дій в журналі

TNM 2 реєструє кожну виконану і невиконану дію в журналі дій, показуючи таймкод, а також ім'я та IP адресу цільового обладнання (див. рисунок 1.6) [1].

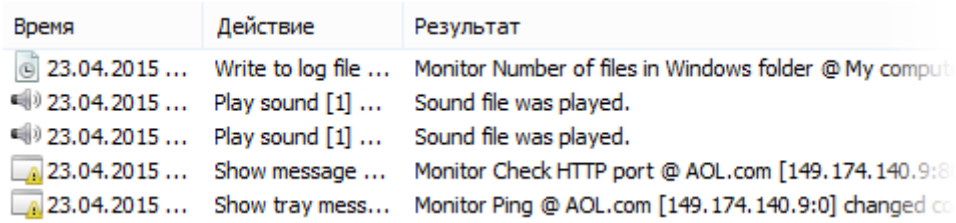


Рисунок 1.6 - Перевірки працездатності і проблем

З 2 серпня 2020 року подальша розробка та розповюдження Total Network Monitor 2 повністю зупинено. На зміну їй пройшов новий продукт - Network Olympus, який за всіма критеріями перевершує свого попередника, а також має більший потенціал до подальшого розвитку.

ПІДГОТОВКА ДО ВИКОНАННЯ КОМП'ЮТЕРНОГО ПРАКТИКУМУ №1

Перед виконанням комп'ютерного практикуму №1 рекомендується ознайомитись з основними принципами роботи програми моніторингу Total Network Monitor 2, що розглядається в курсі лекцій, а також допоміжній літературі [1].

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

Звіт з комп'ютерного практикуму №1 обов'язково повинен містити наступну інформацію:

- назва комп'ютерного практикуму;
- мета роботи;
- постановка завдання;
- відповіді.

ЗАВДАННЯ ДЛЯ ЗАХИСТУ КОМП'ЮТЕНОГО ПРАКТИКУМУ №1

1. Втановити програмний пакет Total Network Monitor 2 згідно [1].
2. Здійснити налаштувати Total Network Monitor 2 згідно [1].
3. Додати карту.
4. Додати пристрої.
5. Налаштувати сервіс.

Комп'ютерний практикум №2

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ OBSERVIUM

Мета роботи - ознайомлення та отримання досвіду використання програми моніторингу Observium.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Observium - це платформа автоматичного моніторингу мереж, що не потребує великих затрат та підтримує широкий спектр типів пристроїв, платформ і операційних систем, включаючи Cisco, Windows, Linux, HP, Juniper, Dell, FreeBSD, Brocade, Netscaler, NetApp і багато інших. Observium фокусується на наданні красивого і потужного, але простого і інтуїтивно зрозумілого інтерфейсу для моніторингу працездатності і стану мережі.

Программа професійно розроблена та підтримується командою досвідчених мережевих інженерів та системних адміністраторів. Observium - це платформа, спроектована та побудована її користувачами.

Observium Community - версія доступна безкоштовно для всіх, вона отримує оновлення та нові функції двічі на рік.

Observium Professional додає пріоритетний доступ до щоденних оновлень і нових функцій за невелику щорічну плату.

Широка підтримка пристроїв

Observium підтримує широкий спектр пристроїв і операційних систем, що охоплюють як стандартні, так і приватні MIB(Management Information Base - база даних інформації управління). В даний час підтримується більше 458 окремих типів ОС, включаючи автоматичне виявлення і побудову графіків показників пристроїв з сотень галузевих стандартних і приватних MIB.

Команда розробників Observium часто працює з постачальниками обладнання для розширення та тестування підтримки нових пристроїв (див. рисунок 2.1) [2].

Рисунок 2.1 - Підтримка пристроїв

Облік трафіку

Облік трафіку - це функція, доступна в професійному виданні, яка призначена для полегшення процесу відстеження та виставлення рахунків за використання смуги пропускання клієнтами (див. рисунок 2.2) [2]. Він самостійно опитує і зберігає вимірювання в своїх власних таблицях бази даних, щоб обійти традиційні циклічні обмеження. Він може бути запущений з різними інтервалами для основного опитувальника Observium, що дозволяє вести облік на основі інтервалів, відмінних від стандартних 5 хвилин.

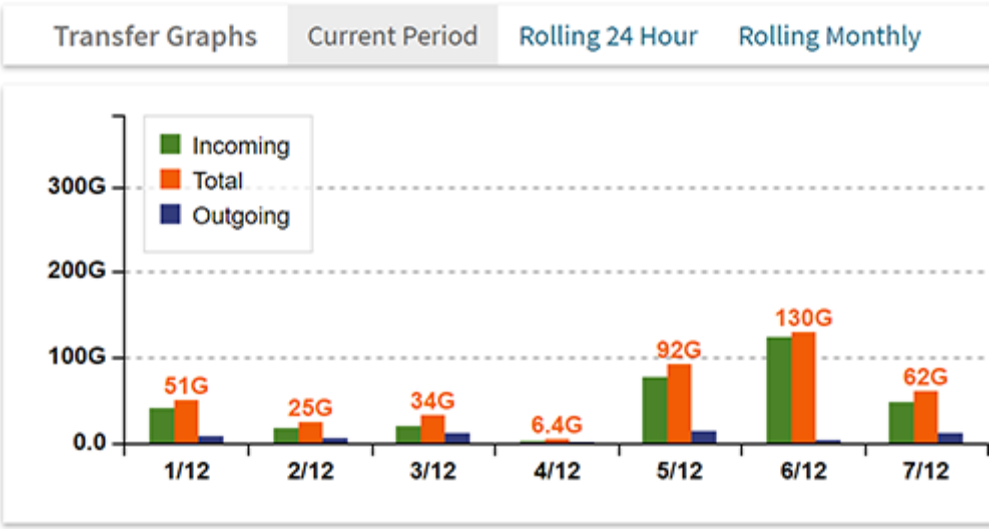


Рисунок 2.2 - Облік трафіку

Зовнішня інтеграція

Observium підтримує інтеграцію з рядом сторонніх додатків і можливість написання власних користувальницьких модулів додатків для збору даних з ваших додатків.

Інтеграція існує для collectd, munin, smokeping і RANCID, що дозволяє переглядати метрики і конфігураційні дані, зібрані цими інструментами в інтерфейсі Observium, допомагаючи оптимізувати діагностику і повсякденні операції (див. рисунок 2.3.) [2].

У програму вже включені збирачі даних для додатків Apache, BIND, DRBD, Memcached, MySQL, NFS та інші.

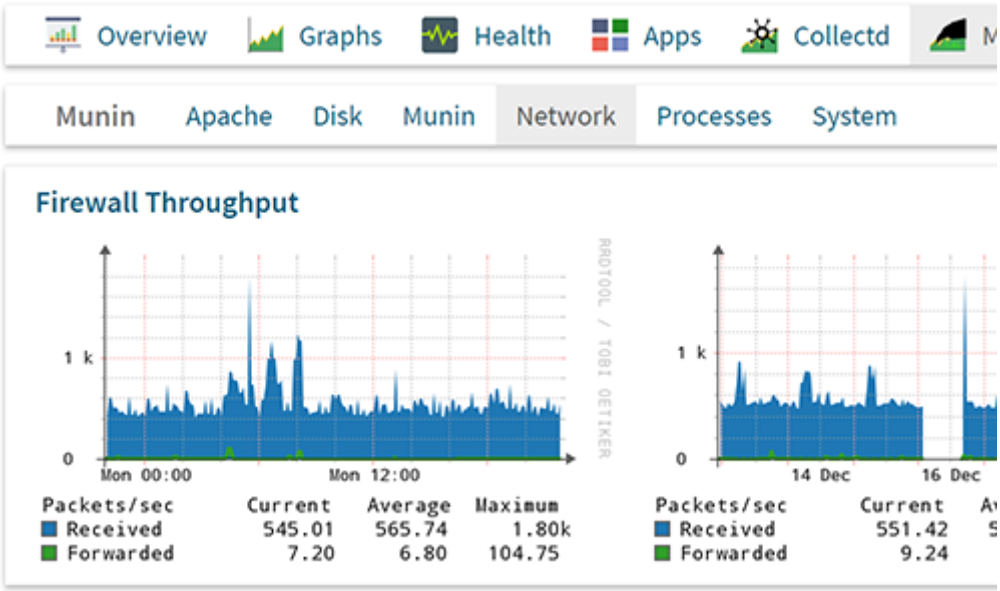


Рисунок 2.3 - Перегляд метрик та конфігурації

Порогове оповіщення

Система оповіщення Observium threshold дозволяє налаштовувати порогові значення і стани відмови для широкого спектру різних типів сутностей. Деякі типи підтримують автоматичний збір порогових значень з самого контрольованого пристрою (див. рисунок 2.4) [2].

Записи сповіщень автоматично створюються в процесі виявлення, щоб переконатися, що ваша система оповіщення знаходиться в актуальному стані з конфігурацією вашої мережевої інфраструктури, що допомагає зменшити кількість пропущених попереджень.

Тести можуть бути пов'язані з пристроями та об'єктами за допомогою гнучкої системи визначень асоціацій, а не попередньо встановлених шаблонів або ручних конфігурацій.

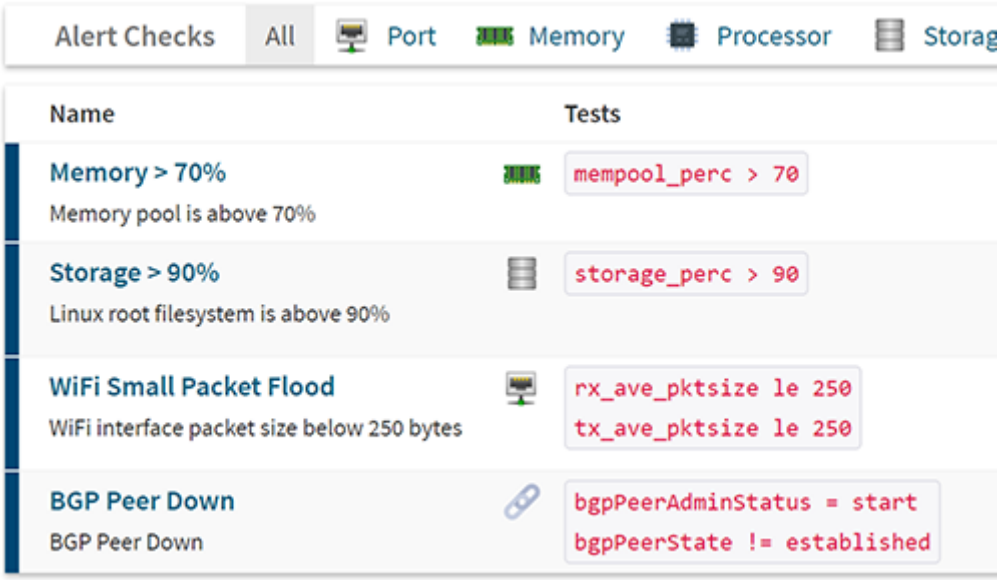


Рисунок 2.4 - Встановлення порогових значень

ПІДГОТОВКА ДО ВИКОНАННЯ КОМП'ЮТЕРНОГО ПРАКТИКУМУ №2

Перед виконанням комп'ютерного практикуму №2 рекомендується ознайомитись з принципами роботи програми моніторингу Observium, що розглядається в курсі лекцій, а також допоміжній літературі [2]. Розробити алгоритм розв'язання завдання. Провести обчислення і дослідження на ЕОМ. В Додатку А наведено хід роботи.

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

Звіт з комп'ютерного практикуму №2 обов'язково повинен містити наступну інформацію:

- назва комп'ютерного практикуму;
- мета роботи;
- постановка завдання і алгоритм його розв'язання;
- скріншоти;
- лістинг програми.

ЗАВДАННЯ ДЛЯ ЗАХИСТУ КОМП'ЮТЕНОГО ПРАКТИКУМУ №2

Завдання.

1. Втановити програмний пакет Observium.
2. Здійснити налаштувати Observium.
3. Додати карту.
4. Додати пристрої.
5. Налаштувати сервіс (Додаток А).

Примітка:

- Команди, що починаються " $ " означають, що вони повинні бути виконані з правами звичайного користувача - а не адміністратора.
- Команди, що починаються " # " означають, що ви повинні мати права адміністратор.
- Команди з більш специфічними підказками (наприклад " rtrx > "або "mysql>") означають що ви виконуєте їх або на віддаленому обладнанні, або в якійсь іншій програмі.

Комп'ютерний практикум №3

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ NAGIOS

ТЕОРЕТИЧНІ ВІДОМОСТІ

Мета роботи - ознайомлення та отримання досвіду використання програми моніторингу Nagios.

Система моніторингу Nagios [3] - це просунуте рішення для моніторингу, управління яке засноване на веб-інтерфейсі. Зазвичай, це первинна система моніторингу, в яку заведено основну масу обладнання, наприклад, мережі передачі даних.

Моніторинг Мережі

Коли мова заходить про інструменти мережевого моніторингу з відкритим вихідним кодом, найбільші світові організації звертаються до Nagios. Nagios відстежує мережу на наявність проблем, викликаних перевантаженими каналами передачі даних або мережевими з'єднаннями, а також відстежує маршрутизатори, комутатори та багато іншого. Легко контролюючи доступність, час безвідмовної роботи і час відгуку кожного вузла мережі, Nagios може надавати результати в різних візуальних уявленнях і звітах.

Виконує наступні цілі:

- Виступає як програмне Забезпечення Для Моніторингу Мережі
- Моніторинг Мережевого Трафіку
- Мережевий аналізатор

Моніторинг Серверів

Nagios відомий як найкраще програмне забезпечення для моніторингу серверів на ринку. Моніторинг серверів в Nagios спрощується завдяки гнучкості моніторингу ваших серверів, як за допомогою агентного, так і безагентного моніторингу. Він маючи понад 5000 різних доповнень, що допомагають в моніторингу серверів.

Виконує наступні цілі:

- Виступає як програмне Забезпечення Для Моніторингу Серверів
- Моніторинг Windows Server
- Моніторинг Серверів Linux

Моніторинг Додатків

Впровадження ефективного моніторингу додатків за допомогою Nagios дозволяє організаціям швидко виявляти проблеми додатків, служб або процесів і вживати заходів щодо усунення простоїв для користувачів додатків. Nagios надає інструменти для моніторингу додатків і стану додатків, включаючи додатки Windows, Linux, UNIX і веб-додатки.

Виконує наступні цілі:

- Надає інструменти Моніторингу Додатків
- Моніторинг Веб-Додатків
- Моніторинг Журналу Додатків

Для того щоб перейти у вікно моніторингу необхідно в меню обрати рядок «Problems», після чого в основному тілі будуть відображуватись Алерти. Нюанс роботи «Нагіос» такий, що програма робить запит в історію Алерту. Тому після серйозної аварії варто очікувати ці ж Алерти в цей же час наступної доби. Для перегляду IP сервера і додаткової інформації необхідно вибрати його.

Для кожного серверу надається інформація в форматі (див. рисунок 3.1) [3]:

- Host – ім’я серверу;
- Service – сервіс по якому сталася подія;
- Status – рівень важливості (критичність) Алерту;
- LastCheck – час, коли останнього оновлення інформації (час, коли було здійснено останній запит сервера);
- Duration – тривалість Алерту з моменту його появи в визначеному системою статусі;
- Status Information – поле помилки.

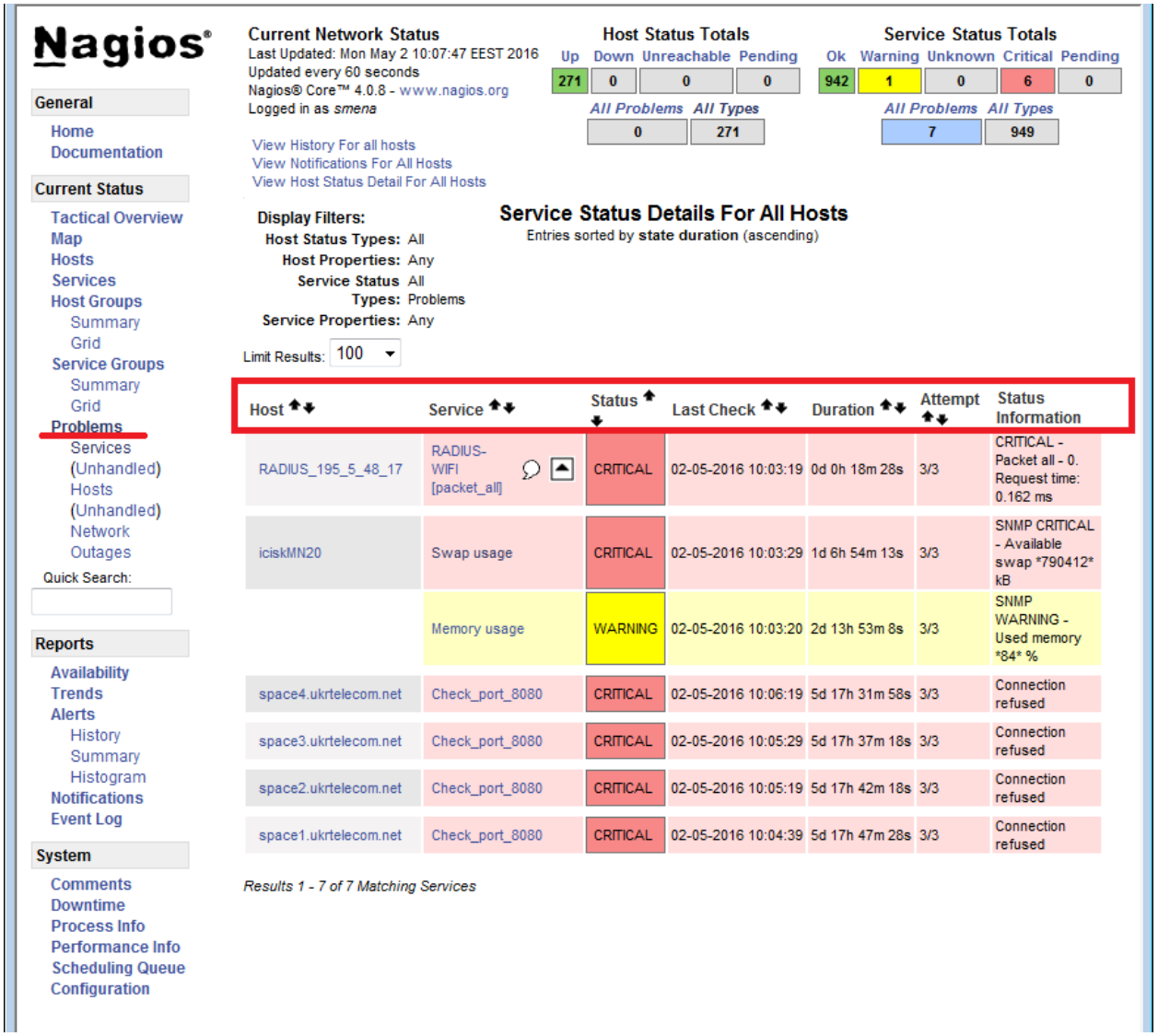


Рисунок 3.1 - Формат інформації для серверу

ПІДГОТОВКА ДО ВИКОНАННЯ КОМП'ЮТЕРНОГО ПРАКТИКУМУ №3

Перед виконанням комп'ютерного практикуму №3 рекомендується ознайомитись з принципами роботи програми моніторингу Nagios, що розглядається в курсі лекцій, а також допоміжній літературі [3]. Розробити алгоритм розв'язання завдання. Провести обчислення і дослідження на ЕОМ. В Додатку Б наведено хід роботи.

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

Звіт з комп'ютерного практикуму №3 обов'язково повинен містити наступну інформацію:

- назва комп'ютерного практикуму;
- мета роботи;
- постановка завдання і алгоритм його розв'язання;
- скріншоти;
- лістинг програми.

ЗАВДАННЯ ДЛЯ ЗАХИСТУ КОМП'ЮТЕНОГО ПРАКТИКУМУ №3

Завдання.

1. Втановити програмний пакет Nagios (Додаток Б).

2. Розробити сценарії автоматичного навантажувального тестування.

Необхідно для довільного унікального WEB ресурсу виконати навантажувальне тестування кількістю користувачів 50. Для цього необхідно запросити 2 довільні сторінки.

Результати тестування (середній час відповіді, максимальний час відповіді, кількість поламаних запитів) по кожній сторінці оформити у вигляді таблиці.

Навантажувальне тестування проводиться щоб отримати відповіді на наступні питання:

- *чи є bottlenecks (в пер. вузькі місця) в системі і виправити їх;*
- *визначити конфігурацію ІС (hardware) при якій система може обслуговувати скажімо 1000 online одночасних користувачів;*
- *визначити, скільки здатна обслужити онлайн користувачів конкретна зафіксована конфігурація ІС.*

У даному комп'ютерному приктикумі роботі необхідно дати відповідь на третє питання, зафіксувавши параметри обладнання, на якому буде проведено тестування.

Далі за допомогою спеціалізованих інструментів формується тест-план, де вказується деяке початкове число одночасних користувачів (скажімо 10). Після чого реалізується емуляція виконання обраного ключового сценарію для кожного з користувачів. Тести виконуються. Вимірюється максимально час відгуку по будь-якому з запитів до ІС. Критерієм зупинки є досягнення 3 секунд. У зворотному випадку, кількість користувачів збільшується з деяким кроком.

Знайдене число користувачів є результатом роботи тестів.

Після виконання навантажувальних тестів в даному комп'ютерному приктикумі необхідно специфікувати ціль інтеграційних тестів, обраний сценарій, інструмент тестування і привести наступну інформацію з тестовими коментарями:

- кількість користувачів яке здатна витримати задана тестова конфігурація;
- графік зміни часу відгуку від кількості користувачів. Прокоментувати результати, вказати на характер залежності.

3. Моніторинг програми під час проведення навантажувального тестування та зняття телеметрії.

Пропонується проводити моніторинг за наступними телеметричними параметрами (тобто знімати телеметрію з деякою частотою наприклад 5 секунд):

- чи запущено додаток (фіксується деякий URL і перевіряється його доступність);
- середній час тривалості запиту до сервера;
- розмір витраченої оперативної пам'яті додатком;
- утилізація процесорного часу додатком.

Комп'ютерний практикум №4

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ PRTG NETWORK MONITOR

Мета роботи - ознайомлення та отримання досвіду використання програми моніторингу PRTG Network Monitor.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Програмний компонент PRTG, сумісний з пристроями на базі ОС Windows, призначений для моніторингу мереж, використовується не тільки для сканування пристроїв, які в даний момент підключені до локальної мережі, але також може послужити відмінним помічником і у виявленні мережевих атак**.** Має наступні функції:

Інтегровані технології

PRTG контролює всю інфраструктуру та підтримує всі популярні технологій:

- SNMP: готові шаблони та індивідуальне налаштування моніторингу
- WMI та лічильники продуктивності Windows
- SSH: для Linux / Unix і macOS
- Аналіз трафіку через протоколи Flow або аналіз пакетів
- HTTP запити
- REST APIs повертають XML і JSON
- Пінг, SQL і багато іншого

Карти і панелі управління

Візуалізує стан вашої мережі, в реальному часі за допомогою карт (див. рисунок 4.1) [4].

Ви можете налаштувати зовнішній вигляд панелі управління за допомогою редактора карт, додати на панель всі елементи вашої мережі, використовуючи більш ніж 300 вбудованих графічних об'єктів, таких як іконки пристроїв і статусів, графіки, списки, рейтинги і багато іншого. Також можна створити свою Панель управління за допомогою налаштувань HTML, поділіться готовою карткою через унікальний URL всередині компанії, або навіть за межами вашої компанії.

Рисунок 4.1 - Карти і панелі управління

Гнучке оповіщення

PRTG попереджає вас, коли виявляє проблеми або незвичайні показники. PRTG включає в себе вбудовані технології оповіщення, такі як електронна пошта, push-повідомлення, або запуск HTTP-запитів. Завдяки нашим безкоштовним додаткам для Android і iOS, Push повідомлення будуть тримати вас в курсі подій, коли ви працюєте через

мобільні пристрої (див. рисунок 4.2) [4].

Ви можете адаптувати систему повідомлень відповідно до ваших потреб і відрегулювати періодичність повідомлень (щоб, наприклад, не отримувати оповіщення про події з низьким пріоритетом ночами), або уникайте великого потоку повідомлень і помилкових спрацьовувань за допомогою налаштування залежностей між сенсорами. Також можна використовувати PRTG API для створення власних повідомлень.

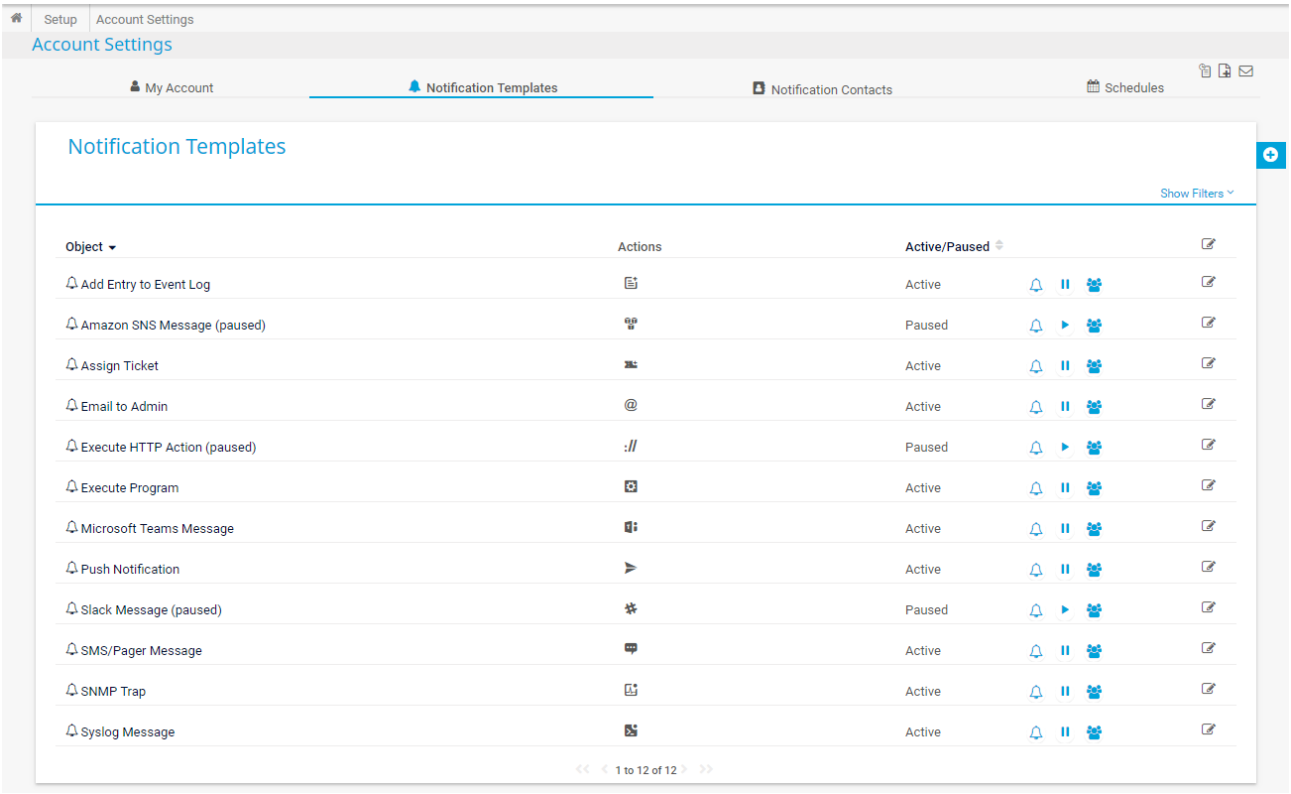


Рисунок 4.2 - Гнучке оповіщення

ПІДГОТОВКА ДО ВИКОНАННЯ КОМП'ЮТЕРНОГО ПРАКТИКУМУ №4

Перед виконанням комп'ютерного практикуму №4 рекомендується ознайомитись з принципами роботи програми моніторингу PRTG Network Monitor, що розглядається в курсі лекцій, а також допоміжній літературі [4]. Розробити алгоритм розв'язання завдання. Провести обчислення і дослідження на ЕОМ. В Додатку В наведено хід роботи.

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

Звіт з комп'ютерного практикуму №4 обов'язково повинен містити наступну інформацію:

- назва комп'ютерного практикуму;
- мета роботи;
- постановка завдання і алгоритм його розв'язання;
- скріншоти;
- лістинг програми.

ЗАВДАННЯ ДЛЯ ЗАХИСТУ КОМП'ЮТЕНОГО ПРАКТИКУМУ №4

Завдання.

1. Втановити програмний пакет PRTG Network Monitor.
2. Здійснити налаштувати PRTG Network Monitor.
3. Додати карту.
4. Додати пристрої.
5. Налаштувати сервіс.

Комп'ютерний практикум №5

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ KISMET

Мета роботи - ознайомлення та отримання досвіду використання програми моніторингу Kismet.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Вступ до Kismet

Kismet - це корисний open-source додаток для системних адміністраторів, який дозволяє всебічно аналізувати мережевий трафік, виявляти в ньому аномалії, запобігати збої і може бути використано з системами на базі *NIX/Windows/Cygwin/macOS. Kismet нерідко використовується саме для аналізу бездротових локальних мереж на основі стандарту 802.11 b (в тому числі, навіть мереж з прихованим SSID).

З його допомогою ви без зусиль знайдете некоректно сконфігуровані і навіть нелегально працюють точки доступу (які зловмисники використовують для перехоплення трафіку) та інші приховані пристрої, які можуть бути потенційно "шкідливі" для вашої мережі. Для цих цілей в додатку дуже добре опрацьована можливість виявлення різних типів мережевих атак-як на рівні мережі, так і на рівні каналів зв'язку. Як тільки одна або кілька атак будуть виявлені, Системний адміністратор отримає тривожний сигнал і зможе вжити заходів щодо усунення загрози.

Kismet - це детектор бездротової мережі і пристроїв, сніффер, інструмент wardriving і фреймворк WIDS (wireless intrusion detection).

Kismet працює з інтерфейсами Wi-Fi, Bluetooth-інтерфейсами, деякими апаратними засобами SDR (програмно-визначене радіо), такими як RTLSDR, та іншими спеціалізованими апаратними засобами захоплення.

Kismet працює на Linux, OSX і, в деякій мірі, Windows 10 під фреймворком WSL. У Linux він працює з більшістю карт Wi-Fi, інтерфейсів Bluetooth та інших апаратних пристроїв. У OSX він працює з вбудованими інтерфейсами Wi-Fi, а в Windows 10 він буде працювати з віддаленими захопленнями.

Компіляція або пакети?

Часто дистрибутиви відстають від випусків програмного забезпечення і можуть пропонувати більш старі - іноді значно старіші - пакети. Щоб отримати останню версію, ви можете або встановити Kismet з пакета в офіційних сховищах Kismet, або скомпілювати його з вихідного коду.

Якщо ви хочете внести зміни в код Kismet або встановлюєте дистрибутив, який наразі не підтримується офіційними пакетами Kismet, вам обов'язково потрібно буде скомпілювати його з вихідного коду.

Якщо ви встановлюєте систему з дуже обмеженими ресурсами, наприклад Raspberry Pi, вам може знадобитися розглянути або пакети, або створення крос - компіляційного середовища-Сучасний C++ може бути дуже ресурсомістким для компіляції, і Raspberry Pi 3 або Raspberry Pi 0 навряд чи зможуть успішно скомпілюватися спочатку. Офіційні пакети для цих середовищ побудовані на сервері Intel з емульованим середовищем pi docker, щоб подолати ці перешкоди.

ПІДГОТОВКА ДО ВИКОНАННЯ КОМП'ЮТЕРНОГО ПРАКТИКУМУ №5

Перед виконанням комп'ютерного практикуму №5 рекомендується ознайомитись з принципами роботи програми моніторингу Kismet, що розглядається в курсі лекцій, а також допоміжній літературі [5]. Розробити алгоритм розв'язання завдання. Провести обчислення і дослідження на ЕОМ. В Додатку 4 наведено хід роботи.

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

Звіт з комп'ютерного практикуму №5 обов'язково повинен містити наступну інформацію:

- назва комп'ютерного практикуму;
- мета роботи;
- постановка завдання і алгоритм його розв'язання;
- скріншоти;
- лістинг програми.

ЗАВДАННЯ ДЛЯ ЗАХИСТУ КОМП'ЮТЕНОГО ПРАКТИКУМУ №5

Завдання.

1. Втановити програмний пакет Kismet (Додаток Г).
2. Здійснити налаштувати Kismet (Додаток Г).
3. Додати карту.
4. Додати пристрої
5. Налаштувати сервіс.

Комп'ютерний практикум №6

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ WIRESHARK

Мета роботи - ознайомлення та отримання досвіду використання програми моніторингу Wireshark.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Що таке Wireshark?

Wireshark - це аналізатор мережевих пакетів. Аналізатор мережевих пакетів представляє захоплені пакетні дані якомога детально.

Ви можете уявити собі аналізатор мережевих пакетів як вимірювальний пристрій для вивчення того, що відбувається всередині мережевого кабелю, точно так само, як електрик використовує вольтметр для вивчення того, що відбувається всередині електричного кабелю (але на більш високому рівні, звичайно).

У минулому такі інструменти були або дуже дорогими, або патентованими, або і тим і іншим. Однак з появою Wireshark все змінилося. Wireshark - це програмний проект з відкритим вихідним кодом, випущений під ліцензією GNU General Public License (GPL). Ви можете вільно використовувати Wireshark на будь-якій кількості комп'ютерів, не турбуючись про ліцензійні ключі тощо. Крім того, весь вихідний код знаходиться у вільному доступі під GPL. Через це людям дуже легко додавати нові протоколи в Wireshark, або у вигляді плагінів, або вбудованих у вихідний код, і вони часто це роблять! Wireshark

доступний безкоштовно, з відкритим вихідним кодом і є одним з кращих аналізаторів пакетів, доступних сьогодні.

Ось кілька причин, чому люди використовують Wireshark:

- Мережеві адміністратори використовують його для усунення неполадок в мережі
- Інженери з мережевої безпеки використовують його для вивчення проблем безпеки
- QA інженери використовують його для перевірки мережевих додатків
- Розробники використовують його для налагодження реалізацій протоколів
- Люди використовують його для вивчення внутрішніх компонентів мережевого протоколу

Wireshark також може бути корисним у багатьох інших ситуаціях.

Функції

Нижче наведені деякі з численних функцій Wireshark:

- Доступ для UNIX і Windows.
- Захоплення пакетних даних з мережевого інтерфейсу у режимі реального часу.
- Відкриття файлів, що містять пакетні дані, захоплені за допомогою tcpdump/WinDump, Wireshark і багатьох інших програм захоплення пакетів.
- Імпорт пакетів з текстових файлів, що містять шістнадцяткові дампи пакетних даних
- Відображення пакетів з дуже докладною інформацією про протокол.
- Збереження захоплених пакетних даних.
- Експорт деяких або всіх пакетів в кілька форматів файлів захоплення.
- Фільтрування пакетів за багатьма критеріями.
- Пошук пакетів за багатьма критеріями.
- Створення різних статистичних даних.

Захоплення з різних мережевих носіїв

Wireshark може захоплювати трафік з багатьох різних типів мережевих носіїв, включаючи Ethernet, бездротову локальну мережу, Bluetooth, USB і багато іншого. Підтримувані типи носіїв можуть бути обмежені кількома факторами, включаючи апаратне забезпечення та операційну систему. Огляд підтримуваних типів носіїв можна знайти за посиланням [https://gitlab.com/wireshark/wireshark/wikis/CaptureSetup/NetworkMedia].

Імпорт файлів з багатьох інших програм захоплення

Wireshark може відкривати захоплення пакетів з великої кількості програм захоплення. Список вхідних форматів див. у розділі [Section 5.2.2, “Input File Formats”].

Експорт файлів для багатьох інших програм захоплення

Wireshark може зберігати захоплені пакети в багатьох форматах, включаючи ті, які використовуються іншими програмами захоплення. Список вихідних форматів див. у розділі [Section 5.3.2, “Output File Formats”].

ПІДГОТОВКА ДО ВИКОНАННЯ КОМП’ЮТЕРНОГО ПРАКТИКУМУ №6

Перед виконанням комп’ютерного практикуму №6 рекомендується ознайомитись з принципами роботи програми моніторингу Wireshark, що розглядається в курсі лекцій, а також допоміжній літературі [6]. Розробити алгоритм розв’язання завдання. Провести обчислення і дослідження на ЕОМ. В Додатку Д наведено хід роботи.

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

Звіт з комп’ютерного практикуму №6 обов’язково повинен містити наступну інформацію:

- назва комп’ютерного практикуму;
- мета роботи;
- постановка завдання і алгоритм його розв’язання;
- скріншоти;
- лістинг програми.

ЗАВДАННЯ ДЛЯ ЗАХИСТУ КОМП’ЮТЕНОГО ПРАКТИКУМУ №6

Завдання.

1. Втановити програмний пакет Wireshark (Додаток Д).
2. Здійснити налаштувати Wireshark (Додаток Д).
3. Додати карту.
4. Додати пристрої.
5. Налаштувати сервіс.

Додаткове завдання.

1. Перерахуйте будь-які 3 протоколи, які можуть бути відображені в стовпці Protocol (Протокол) при відключеному фільтрі пакетів. Скільки часу пройшло від моменту відправки повідомлення GET протоколу HTTP до отримання відповідного повідомлення OK? (За замовчуванням, значення поля Time (Час) у вікні списку являє собою час в секундах від початку трасування. Ви можете поміняти вид цього поля за вашим бажанням, вибравши в меню View (Вид) пункт Time Display Format (Формат відображення часу) і потім вказавши відповідне уявлення часу.)

2. Яка IP-адреса у сервера [gaia.cs.umass.edu] (також відомого як [www net.cs.umass.edu])? Яка адреса вашого комп'ютера?

3. Роздрукуйте повідомлення протоколу HTTP (GET і OK), отримані вами при відповіді на попереднє запитання. Для цього виберіть команду меню File ⇒ Print (Файл ⇒ Друк), встановіть перемикачі в положення selected Packet only (тільки обраний пакет) і print as displayed (друкувати у форматі відображення), відповідно, і потім натисніть кнопку OK.

Комп’ютерний практикум №7

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ NeDi

Мета роботи - ознайомлення та отримання досвіду використання програми моніторингу NeDi.

ТЕОРЕТИЧНІ ВІДОМОСТІ

NeDi-це повністю безкоштовне ПЗ, яке сканує мережу по MAC-адресами (також серед допустимих критеріїв пошуку є IP-адреси і DNS) і складає з них власну БД. Для роботи цей програмний продукт використовує веб-інтерфейс.

Таким чином, ви можете в режимі онлайн спостерігати за всіма фізичними пристроями і їх місцем розташування в рамках вашої локальної мережі (фактично, ви знайдете можливість вилучення даних про будь – якому мережевому вузлі-починаючи від його прошивки і закінчуючи конфігурацією).

Деякі професіонали задіють NeDi для пошуку пристроїв, які використовуються нелегально (наприклад, вкрадені). Для підключення до комутаторів або маршрутизаторів дане ПЗ використовує протоколи CDP/LLDP. Це дуже корисне, хоча і непросте в освоєнні рішення..

NeDi виявляє ваші мережеві пристрої та відстежує підключені кінцеві вузли. Він містить безліч додаткових функцій для управління корпоративними мережами: Intelligent topology awareness:

- Відображення / відстеження MAC-адрес
- Графік трафіку, помилок, відкидання і широкомовної передачі з пороговим попередженням
- Час безвідмовної роботи, BGP-вузлам і моніторингу стану інтерфейсу
- Кореляція повідомлень системного журналу і пасток з подіями виявлення
- Мережеві карти для документування та моніторингу інформаційних панелей
- Виявлення точок доступу Rouge і пошук зниклих пристроїв
- Велика звітність, починаючи від пристроїв, модулів, інтерфейсів і закінчуючи активами і вузлами.

Архітектура

Архітектуру NeDi можна розділити на наступні компоненти:

- Виявлення мережі (nedi.pl)
- Моніторинг (moni.pl, trap.pl і ще syslog.pl)
- Майстер-демон і список агентів для централізації розподілених екземплярів NeDi
- Виявлення вузлів для отримання відомостей про активи (зібраних за допомогою nodi.pl використання WMI і SSH)
- Модульний веб-інтерфейс, написаний на PHP і деяких javascript
- API-інтерфейс RESTful інтерфейс, написаний на PHP
- Головний файл налаштувань (nedi.conf)
- Залежності також вказані вище (наприклад, API розмовляє тільки з БД і потоком.pl використовує дані трафіку для створення графіків)
- NFDUMP може бути додатково інтегрований, так як інтерфейс може отримувати доступ до даних netflow і відображати їх

ПІДГОТОВКА ДО ВИКОНАННЯ КОМП'ЮТЕРНОГО ПРАКТИКУМУ №7

Перед виконанням комп'ютерного практикуму №7 рекомендується ознайомитись з принципами роботи програми моніторингу NeDi, що розглядається в курсі лекцій, а також допоміжній літературі [7]. Розробити алгоритм розв'язання завдання. Провести обчислення і дослідження на ЕОМ. В Додатку Е наведено хід роботи.

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

Звіт з комп'ютерного практикуму №7 обов'язково повинен містити наступну інформацію:

- назва комп'ютерного практикуму;
- мета роботи;
- постановка завдання і алгоритм його розв'язання;
- скріншоти;
- лістинг програми.

ЗАВДАННЯ ДЛЯ ЗАХИСТУ КОМП'ЮТЕНОГО ПРАКТИКУМУ №7

Завдання.

1. Втановити програмний пакет NeDi (Додаток Е).

2. Здійснити налаштувати NeDi (Додаток Е).
3. Додати карту.
4. Додати пристрої.
5. Налаштувати сервіс.

Комп'ютерний практикум №8

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ ZABBIX

Мета роботи - ознайомлення та отримання досвіду використання програми моніторингу Zabbix.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Zabbix був створений Олексієм Владишевим, і в теперішній час активно розробляється і підтримується компанією Zabbix SIA.

Zabbix - це рішення розподіленого моніторингу корпоративного класу з відкритими вихідними кодами.

Zabbix - це програмне забезпечення для моніторингу численних параметрів мережі, життєздатності та цілісності серверів. Zabbix використовує гнучкий механізм сповіщень, що дозволяє користувачам конфігурувати повідомлення засновані на e-mail практично для будь-якої події. Це дозволяє швидко реагувати на проблеми з серверами. Zabbix пропонує відмінні функції звітності та візуалізації даних засновані на даних історії. Це робить Zabbix ідеальним для планування потужності.

Zabbix підтримує і пуллери, і траппери. Всі звіти і статистика Zabbix, так само як і параметри налаштування, доступні через Веб інтерфейс. Веб інтерфейс гарантує, що стан вашої мережі і життєздатність ваших серверів буде доступно з будь-якого місця. Правильно налаштований, Zabbix може зіграти важливу роль в моніторингу IT інфраструктури. Це вірно і для маленьких організацій з декількома серверами і для великих організацій з безліччю серверів.

Zabbix безкоштовний. Zabbix написаний і поширюється під ліцензією GPL General Public License версії 2. Це означає, що його вихідний код поширюється і доступний для необмеженого кола осіб.

Можливості Zabbix

Zabbix - високо інтегроване рішення моніторингу мережі, яке пропонує безліч функцій в одному пакеті.

Збір даних

- перевірки доступності та продуктивності
- підтримка моніторингу з використанням SNMP (і траппери, і пуллери), IPMI, JMX, VMware
- користувальницькі перевірки
- збір бажаних даних за допомогою користувацьких інтервалів
- виконуються сервером / проксі та агентами

Гнучкі визначення порогів

- ви можете задавати дуже гнучкі пороги проблем, звані тригерами, посилаючись на значення з бази даних

Безліч налаштувань сповіщень

- відправку сповіщень можна налаштувати, використовуючи розклади ескалацій, одержувачів, типів оповіщень

- сповіщення можна зробити інформативними та корисними при використанні змінних макросів
- автоматичні дії, що включають в себе віддалені команди

Побудова графіків в режимі реального часу

- за допомогою вбудованого функціоналу побудови графіків відразу ж доступні графіки за спостережуваними елементами даних

Можливості Веб-моніторингу

- Zabbix може імітувати натискання мишкою на веб-сайті, перевірити функціонал і час відповіді

Широкі можливості візуалізації

- можливість створювати користувальницькі графіки, що дозволяє комбінувати безліч елементів даних в одному місці
- карти мережі
- Користувальницькі комплексні екрани і слайд-шоу на зразок зовнішнього вигляду ПАНЕЛІ
- звіти
- високорівневе (бізнес) представлення спостережуваних ресурсів

Зберігання даних історії

- дані записуються в базу даних
- історія, що налаштовується
- вбудована процедура очищення історії

Просте налаштування

- добавление наблюдаемых устройств узлами сети
- як тільки вузли мережі є в базі даних, вони готові до моніторингу
- застосування шаблонів до спостережуваних пристроїв

Використання шаблонів

- групування перевірок в шаблони
- шаблони можуть успадковуватися від інших шаблонів

Мережеве виявлення

- автоматичне виявлення мережевих пристроїв
- автоматична реєстрація агентів
- файлових систем, мережевих пристроїв і SNMP OID'ів

Швидкий Веб-інтерфейс

- Веб-інтерфейс, заснований на мові PHP
- доступний з будь-якого місця
- зручна навігація
- журнал аудиту

Zabbix API

- Zabbix API забезпечує програмований інтерфейс до Zabbix для масових маніпуляцій, для інтеграції стороннього програмного забезпечення та інших цілей.

Система прав доступу

- безпечна аутентифікація користувачів
- можливість обмеження доступу окремим користувачам до конкретних сторінок

Повнофункціональний і легко розширюваний агент

- розгортається на спостережуваних машинах
- можна розгорнути як на Linux, так і на Windows

Огляд Zabbix

АРХІТЕКТУРА

Zabbix складається з декількох основних програмних компонентів, функції яких викладені нижче.

СЕРВЕР

Zabbix сервер є основним компонентом, якому агенти повідомляють інформацію і статистику про доступність і цілісності. Сервер є головним сховищем, в якому зберігаються всі дані конфігурації, статистики, а також оперативні дані.

БАЗА ДАНИХ

Як така вся інформація про конфігурацію, а так само дані зібрані Zabbix, зберігаються в базі даних.

ВЕБ-ІНТЕРФЕЙС

Для легкого доступу до Zabbix з будь-якого місця і з будь-якої платформи, поставляється інтерфейс на основі Веб. Інтерфейс є частиною Zabbix сервера і зазвичай (але не обов'язково) працює на тому ж самій фізичній машині, що і сервер.

Проксі

Zabbix проксі може збирати дані про продуктивність і доступності від імені Zabbix сервера. Проксі є опціональною частиною Zabbix; однак він може бути корисним щоб розподілити навантаження одного Zabbix сервера.

АГЕНТ

Zabbix агенти розгортаються на спостережуваних системах для активного моніторингу за локальними ресурсами і додатками, і для відправки зібраних даних Zabbix серверу або проксі.

ПОТІК ДАНИХ

Крім того, важливо зробити крок назад і поглянути на весь потік даних в Zabbix. Для того щоб створити елемент даних, який буде збирати дані, ви повинні спочатку створити вузол мережі. Переміщаючись в інший кінець спектра Zabbix, у вас повинен бути елемент даних, щоб створити тригер. У вас повинен бути тригер, щоб створити дію. Таким чином, якщо ви хочете отримувати сповіщення про занадто високе завантаження процесора на сервері X, ви спочатку повинні створити запис про вузол мережі для Сервера X, потім елемент даних для спостереження за CPU, потім тригер, який спрацює, якщо завантаження CPU буде занадто високим, а потім дія яка відправить вам e-mail. Хоча може здатися, що потрібно занадто багато кроків, використання шаблонів значно спрощує процес. Однак, така побудова системи дозволяє створювати дуже гнучкі інсталяції.

ПІДГОТОВКА ДО ВИКОНАННЯ КОМП'ЮТЕРНОГО ПРАКТИКУМУ №8

Перед виконанням комп'ютерного практикуму №8 рекомендується ознайомитись з принципами роботи програми моніторингу Zabbix, що розглядається в курсі лекцій, а також допоміжній літературі [8]. Розробити алгоритм розв'язання завдання. Провести обчислення і дослідження на ЕОМ. В Додатку Ж наведено хід роботи.

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

Звіт з комп'ютерного практикуму №8 обов'язково повинен містити наступну інформацію:

- назва комп'ютерного практикуму;
- мета роботи;
- постановка завдання і алгоритм його розв'язання;
- скріншоти;
- лістинг програми.

ЗАВДАННЯ ДЛЯ ЗАХИСТУ КОМП'ЮТЕНОГО ПРАКТИКУМУ №8

Завдання.

1. Втановити програмний пакет Zabbix (Додаток Ж).

2. Здійснити налаштувати Zabbix (Додаток Ж).
3. Додати карту.
4. Додати пристрої.
5. Налаштувати сервіс.

Комп’ютерний практикум №9

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ NETWORK OLYMPUS

Мета роботи - ознайомлення та отримання досвіду використання програми моніторингу Network Olympus.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Програма працює як служба і має веб-інтерфейс, що дає набагато більшу гнучкість і зручність в роботі. Головна особливість – конструктор сценаріїв, що дозволяє відійти від виконання примітивних перевірок, які не дозволяють враховувати ті чи інші обставини роботи пристроїв. З його допомогою можна організовувати схеми моніторингу будь-якої складності, щоб точно виявляти проблеми і несправності, а також автоматизувати процес їх усунення.

В основі сценарію лежить сенсор, від якого можна вибудовувати логічні ланцюжки, які в залежності від успішності перевірки будуть генерувати різні оповіщення та дії, спрямовані на вирішення ваших завдань. Кожен елемент ланцюжка може бути відредагований в будь-який час і відразу застосується для всіх пристроїв, за якими закріплений сценарій. Вся мережева активність буде відслідковуватися за допомогою журналу активності і спеціальних звітів.

Якщо у Вас невелика мережа, то купувати ліцензію не знадобиться – програма буде працювати в **безкоштовному режимі**.

Моніторинг мережі

Моніторинг всіх компонентів корпоративної мережі є невід'ємною частиною ефективної стратегії будь-якої великої компанії. Досягнення мети у вигляді безперервної роботи мережі вимагає негайного вирішення будь-яких виникаючих проблем. Network Olympus надає найбільш повне і універсальне рішення для гнучкого моніторингу вашої корпоративної мережі і швидкого реагування на будь-яку потенційну проблему.

Сенсори для моніторингу. Сенсори є об'єктами, які можуть перевіряти продуктивність і працездатність мережевого пристрою.

Network Olympus підтримує більше 20 різних сенсорів, розділених на 3 групи: NetBase, WinBase і FileSystem.

1. Сенсори NetBase

Мережеві сенсори дозволяють Вам перевіряти доступність будь-яких мережевих протоколів, включаючи **TCP, HTTP, FTP, SMTP, POP, IMAP, TELNET**, і використовувати їх для моніторингу веб-сайтів (див. рисунок 9.1) [9].

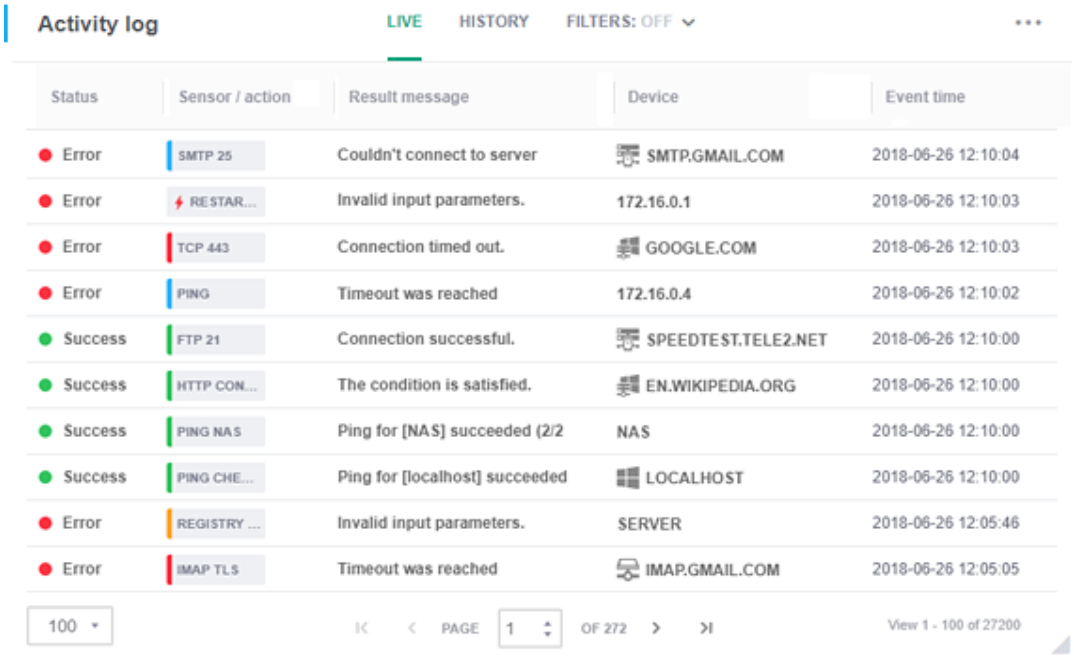


Рисунок 9.1 - Перевірка доступності мережевих протоколів

- Перевіряйте доступність серверів за допомогою необхідних протоколів, наприклад використовуючи сенсор **ICMP пінг**;
- Слідкуйте за працездатністю підтримуваних мережевих пристроїв;
- Слідкуйте за роботою веб-сайту, виконуючи регулярну перевірку веб-сторінки на певний текст.

2. Сенсори WinBase

За допомогою сенсорів WinBase ви можете виконувати моніторинг швидкодії систем Windows і виявляти потенційні загрози до того, як вони стануть реальними. Сенсори також дозволяють вам переконатися, що всі елементи системи працюють в штатному режимі.

Переконайтеся, що процесор не перевантажений за допомогою перевірки його завантаження сенсором **Завантаження ЦП (**див. рисунок 9.2) [9].

Слідкуйте за споживанням пам'яті та іншими значеннями, використовуючи **WMI сенсори**.

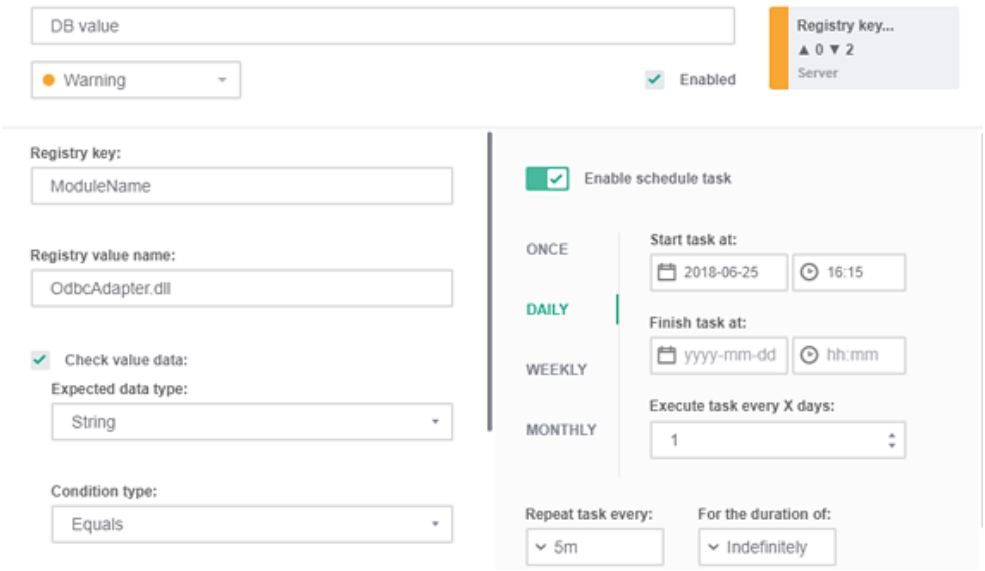


Рис. 9.2 - Перевірка завантаження сенсором

Використовуйте сенсор **Продуктивність Windows** оптимізований під ваші потреби.

3. Сенсори FileSystem

Не обмежуйте себе тільки мережевими перевірками; виконуйте **файлові перевірки на системах Windows** і отримаєте повідомлення, як тільки сенсор змінить свій стан (див. рисунок 9.3) [9].

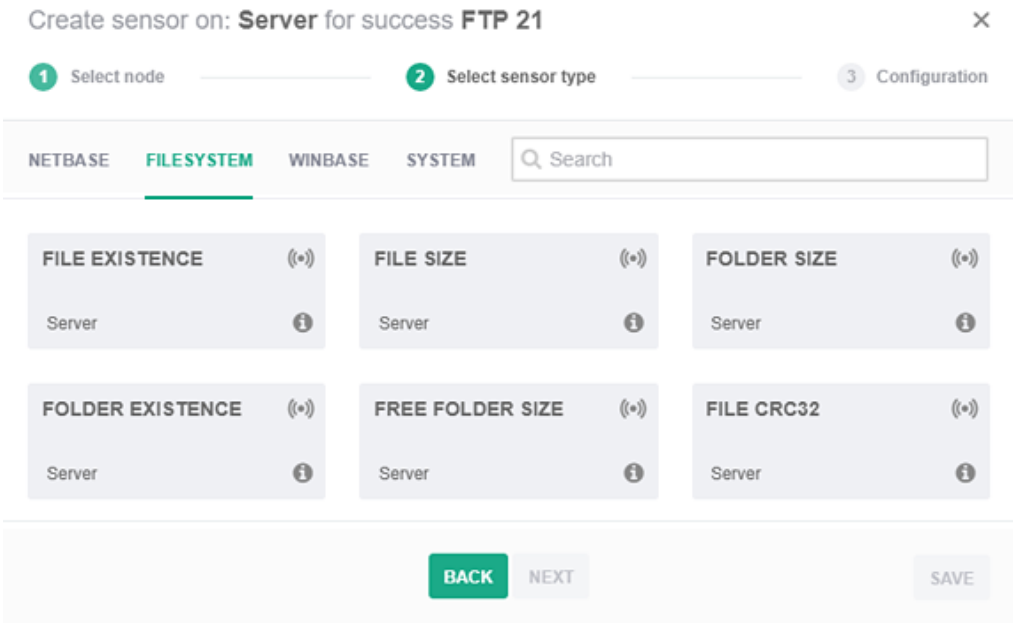


Рис. 9.3 - Файлова перевірка

- Відстежуйте, чи знаходиться файл в певній папці, стежте за його розміром і контрольною сумою CRC32, а також за багатьма іншими параметрами;
- Порівнюйте розміри файлів і їх вміст;
- Перевіряйте наявність папки, її розмір, обсяг вільного простору і т. д.

Карта мережі

Network Olympus підтримує широкий діапазон мережевих протоколів, служб і пристроїв, що дозволяє автоматично виявити кожен пристрій і дає можливість побудувати детальну карту вашої мережі. Карта мережі дозволяє візуалізувати інформацію як по одиночним мережевим вузлам, так і по груповим, таким як домени, робочі групи і підмережі (див. рисунок 9.4) [9].

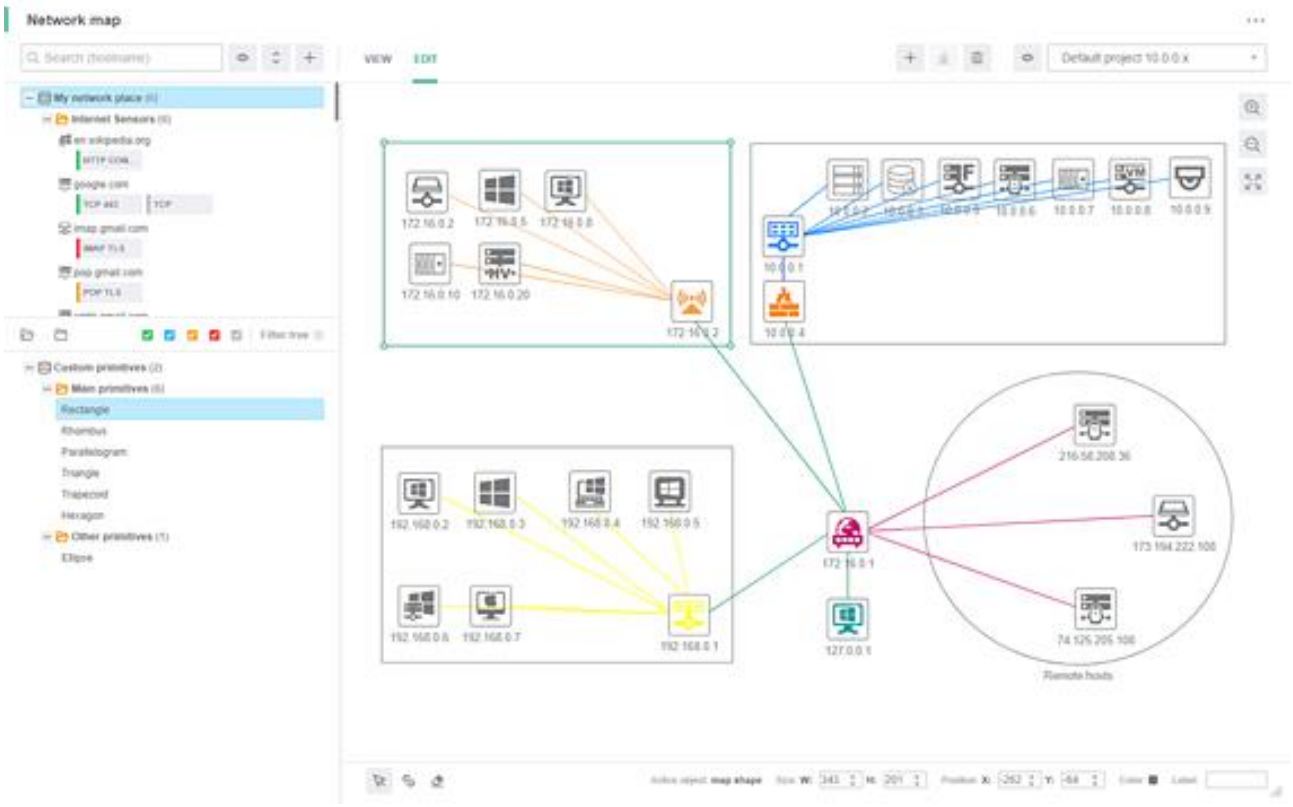


Рисунок 9.4 - Візуалізація мережі

Можливість створення карти мережі інтегрована в систему. За допомогою модуля карти мережі легко реалізувати багаторівневе управління і чіткий контроль як за всією мережевою інфраструктурою в цілому, так і за окремими пристроями.

Ви можете створити будь-яку кількість унікальних карт. Створюйте окремі карти для кожного поверху компанії, щоб співробітники мали доступ до тих пристроїв, які вони обслуговують.

Всі елементи управління інтуїтивно зрозумілі і складаються з простих меню і панелей управління.

Елементи карти мережі безпосередньо пов'язані з реальними пристроями і відображають їх статус в режимі реального часу. Вузли та зв'язки дозволяють мережевим адміністраторам з точністю відтворити топологію мережі своєї компанії. Карта може також містити додаткові візуальні елементи. Наприклад, стандартні геометричні форми можуть бути використані для позначення або поділу реальних і віртуальних пристроїв на групи.

Для зручності ви можете розташувати пристрої на схемі будівлі, карті світу або на діаграмі за допомогою додавання різних фонових зображень для кожної карти.

Моніторинг серверів

Network Olympus дозволяє виконувати моніторинг всієї мережевої інфраструктури за допомогою стандартного протоколу WMI. Час безперервної роботи і продуктивність серверів і мережевих пристроїв, служб і протоколів; пропускна здатність, використання мережі і її доступність, продуктивність і рух трафіку — все це відстежується і аналізується в режимі реального часу.

Безпомилковий **моніторинг серверів** - запорука успіху будь-якого великого бізнесу. У вашій мережі, швидше за все, є як мінімум декількох пристроїв, які постійно перевіряються. Коли результат моніторингу досягнутий, програма проінформує вас про це і повторить процедуру моніторингу.

Наші сенсори відстежують **продуктивність ваших серверів** і надають вам інформацію, необхідну для забезпечення успішної роботи системи. Процес гранично

простий: сенсори збирають дані, аналізують їх, оцінюють поточний стан системи і повідомляють користувача про будь-які проблеми.

Сенсори дозволяють виконувати широкий спектр завдань. В цілому сенсори відповідають за **моніторинг різних параметрів мережевих пристроїв**, таких як комп'ютери, сервери і різне мережеве обладнання. Принцип роботи сенсорів досить простий: кожен сенсор або кілька сенсорів призначаються мережевому пристрою і відстежують його параметри. Сенсори можуть бути призначені як на окремий пристрій, так і на цілу групу. Крім того, якщо в групі знаходяться підгрупи, сенсор буде прив'язаний до всіх пристроїв, що знаходяться в них.

Продуктивність серверів може бути критична. Якщо ваша компанія надає продукти або послуги онлайн, то низька продуктивність серверів, що вимагають апгрейда, може мати значний вплив на роботу. Постійний **моніторинг апаратної частини** HTTP-серверів дозволить вчасно відстежити і усунути подібні проблеми..

Поштові сервери містять багато конфіденційної інформації. У разі виникнення проблем, у співробітників, що відповідають за обслуговування сервера, повинно бути достатньо часу для виправлення помилки і захисту компанії від потенційних атак хакерів. Наше ПЗ для моніторингу серверів надає можливість відстежувати їх стан і відразу ж повідомляти вас у разі виявлення проблем. Network Olympus підтримує протоколи SMTP, POP, IMAP та інші.

Конструктор сценаріїв

Network Olympus представляє Конструктор сценаріїв: гнучкий і багатофункціональний інструмент, здатний вирішувати по-справжньому складні завдання моніторингу пристроїв. Конструктор сценаріїв дозволить вам піти від виконання елементарних перевірок, які не враховують певні аспекти роботи пристрою. З його допомогою ви можете організувати гнучкі схеми моніторингу для того, щоб точно визначити проблему або несправність, а також автоматизувати процес їх усунення.

Конструктор сценаріїв, як і самі сценарії, є ключовою особливістю Network Olympus і дозволяє повністю **автоматизувати управління мережею**. Оскільки конструктор сценаріїв націлений на полегшення рішень, прийнятих користувачами, його функціонал спрямований на вирішення двох основних завдань:

* автоматизація процесу віддаленого реагування на будь-які виникаючі проблеми в мережі;

* полегшення налаштування складних схем для діагностики проблем мережі.

Це надає практично необмежені можливості для **моніторингу в реальному часі**.

За допомогою конструктора сценаріїв ви можете створювати **сценарії з розгалуженою структурою**. Їх робота ґрунтується на сенсорах, що опитують пристрої, що дозволяє реалізувати **гнучкі схеми моніторингу**.

ПІДГОТОВКА ДО ВИКОНАННЯ КОМП’ЮТЕРНОГО ПРАКТИКУМУ №9

Перед виконанням комп’ютерного практикуму №9 рекомендується ознайомитись з принципами роботи програми моніторингу Network Olympus, що розглядається в курсі лекцій, а також допоміжній літературі [9]. Розробити алгоритм розв’язання завдання. Провести обчислення і дослідження на ЕОМ. В Додатку И наведено хід роботи.

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

Звіт з комп'ютерного практикуму №9 обов'язково повинен містити наступну інформацію:

- назва комп'ютерного практикуму;
- мета роботи;
- постановка завдання і алгоритм його розв'язання;
- скріншоти;
- лістинг програми.

ЗАВДАННЯ ДЛЯ ЗАХИСТУ КОМП'ЮТЕНОГО ПРАКТИКУМУ №9

Завдання.

1. Втановити програмний пакет Network Olympus (Додаток И).
2. Здійснити налаштувати Network Olympus (Додаток И).
3. Додати карту.
4. Додати пристрої.
5. Налаштувати сервіс.

Комп'ютерний практикум №10

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ CACTI

Мета роботи - ознайомлення та отримання досвіду використання програми моніторингу Cacti.

ТЕОРЕТИЧНІ ВІДОМОСТІ

Система моніторингу Cacti – це графічна система моніторингу, яка дозволяє контролювати обладнання та лінії зв'язку на різних рівнях мережі передачі даних.

Cacti складається з декількох складових, а саме:

- підсистема моніторингу в яку заведено всі існуючі сервери Служби моніторингу мережі/Прикладні системи (СММ).

Інтерфейс системи являє собою розмежований на дві основні області екрану (див. рисунок 10.1) [10]. Зліва розташовується «Дерево» з назвами послуг та серверів (1). В праві половині графічне відображення стану сервісів по обраній послузі (оновлення графіків відбувається кожні п'ять хвилин) (2).

Обрав один з сервісів є можливість розглянути його стан на різних часових проміжках, а також виділити і переглянути необхідну область на графіку за допомогою меню (праворуч від сервісу – виділено червоним прямокутником).

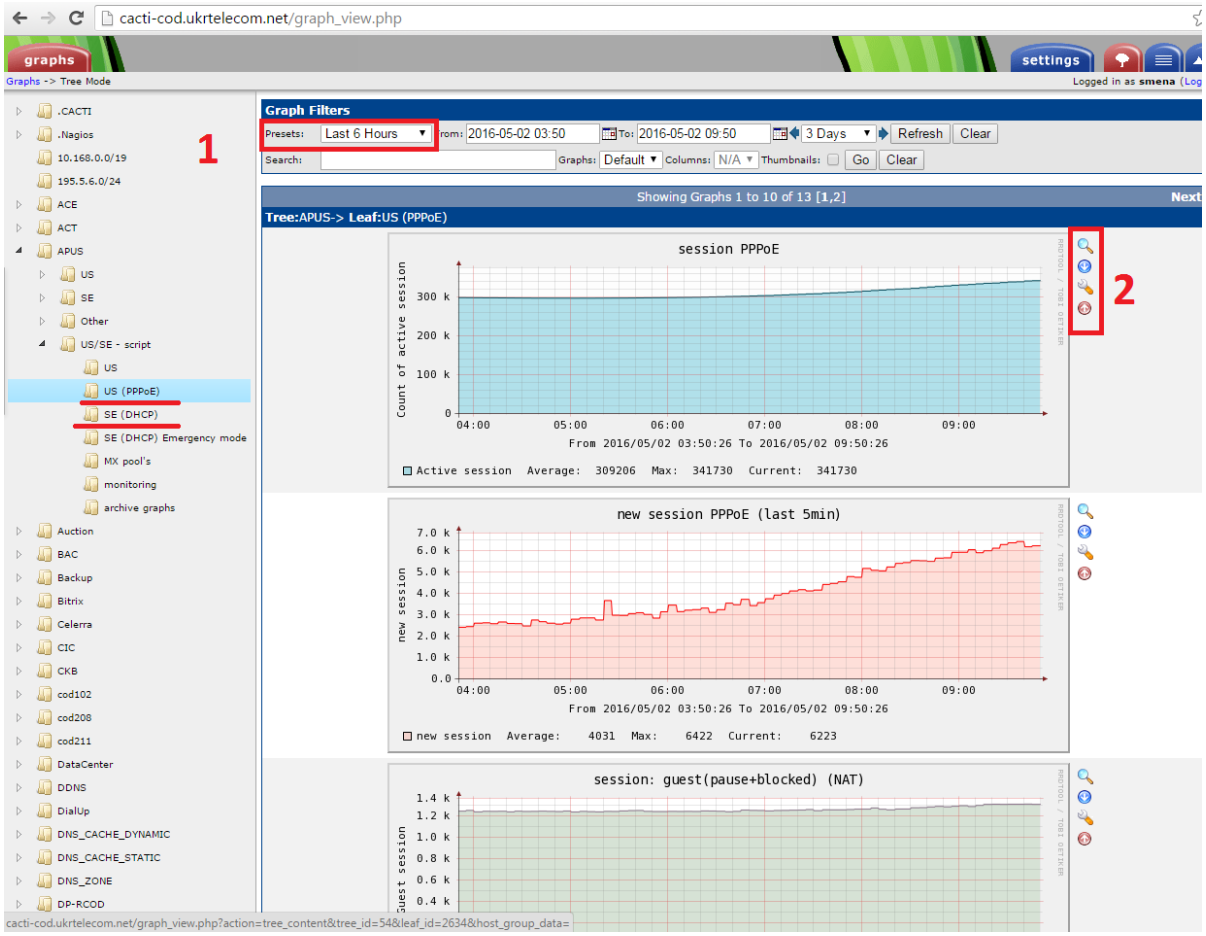


Рисунок 10.1 - Інтерфейс системи Cacti: моніторинг серверів Служби моніторингу мережі та Прикладних систем

- підсистема моніторингу, в яку заведено всі існуючі комутатори рівнів дистрибуції та агрегації, разом зі станом ліній зв'язку;
- підсистема моніторингу, в яку заведено всі існуючі сервери ядра мережі, центральних вузлів (ЦВ) та обладнання термінації.

ПІДГОТОВКА ДО ВИКОНАННЯ КОМП'ЮТЕРНОГО ПРАКТИКУМУ №10

Перед виконанням комп'ютерного практикуму №10 рекомендується ознайомитись з принципами роботи програми моніторингу Cacti, що розглядається в курсі лекцій, а також допоміжній літературі [10]. Розробити алгоритм розв'язання завдання. Провести обчислення і дослідження на ЕОМ. В Додатку К наведено додаткову інформацію.

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

Звіт з комп'ютерного практикуму №10 обов'язково повинен містити наступну інформацію:

- назва комп'ютерного практикуму;
- мета роботи;
- постановка завдання і алгоритм його розв'язання;
- скріншоти;
- лістинг програми.

ЗАВДАННЯ ДЛЯ ЗАХИСТУ КОМП'ЮТЕНОГО ПРАКТИКУМУ №10

Завдання.
1. Втановити програмний пакет Cacti (Додаток К).
2. Здійснити налаштувати Cacti (Додаток К).
3. Додати карту.
4. Додати пристрої.
5. Налаштувати сервіс.

Комп'ютерний практикум №11

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ CIC (CISCO INFO CENTRE)

Мета роботи - ознайомлення та отримання досвіду використання програми моніторингу CIC (Cisco info Centre).

ТЕОРЕТИЧНІ ВІДОМОСТІ

Cisco Info Center (CIC) являє собою повнофункціональне рішення для контролю стану великих мереж операторів зв'язку або підприємств, а також їх IT-інфраструктури. Рішення CIC забезпечує моніторинг відмов, локалізацію несправностей і управління рівнем якості послуг, що надаються в режимі реального часу. Впровадження CIC дозволяє операторам зосереджуватися на дійсно важливих подіях за рахунок різкого скорочення обсягу інформації, що надходить (з використанням розвинених засобів фільтрації подій) і можливості настроювання вікон для перегляду інформації про події. Рішення є гнучким, з повним підлаштуванням під конкретні потреби, клієнт-серверним додатком, яке забезпечує консолідацію, усуває дублікати, виконує фільтрацію і кореляційний аналіз повідомлень про відмови від різноманітних платформ управління і безпосередньо від мережевих пристроїв, що працюють за різними технологіями.

CIC збирає потоки подій або повідомлень з багатьох джерел і надає єдиний інтегрований погляд на поточний стан всіх систем, які знаходяться під його контролем. Він поширює інформацію про події серед операторів та адміністраторів, відповідальних за моніторинг послуг. Ця інформація може бути потім:

- призначена операторам – відповідальним виконавцям;
- передана системам підтримки користувачів (Help Desk);
- збережена в базі даних;
- передана віддаленій системі CIC за заданими правилами;
- використана в якості тригера для запуску автоматичної реакції на певні події.

CIC надає адміністратору єдину точку моніторингу різноманітних систем мережевого управління, додатків і протоколів. CIC не замінює платформи управління, він доповнює їх, забезпечуючи збір інформації про події, відмови і їх стан в масштабах всієї організації.

CIC пов'язує воєдино платформи управління технологічними і географічними доменами мережі. Інформація про стан мережевих елементів зберігається у високопродуктивній розподіленій базі даних безпосередньо в пам'яті серверів управління.

Ця інформація представляється зацікавленим операторам за допомогою індивідуально налаштованих фільтрів і уявлень. Для виконання інтелектуальної обробки поточного стану об'єктів управління можуть використовуватися вбудовані функції автоматизації CIC.

CIC є надбудовою над існуючими системами управління і додатками. Оскільки набуті навички роботи з системами управління використовуються на повну міру, час і витрати на розгортання CIC мінімальні.

Архітектура рішення Cisco Info Center

Cisco Info Center є багаторівневою розподіленою системою. Нижній рівень складають проби і монітори, які з одного боку отримують інформацію від мережевих елементів або інформаційних систем, а з іншого – передають попередньо оброблені дані компоненту Object Server. На нижньому рівні відбувається перетворення інформації, отриманої за різними протоколами, в канонічну форму, в якій дані зберігаються і обробляються компонентом Object Server. Верхній рівень рішення складають клієнтські програми (див. рисунок 11.1) [11].

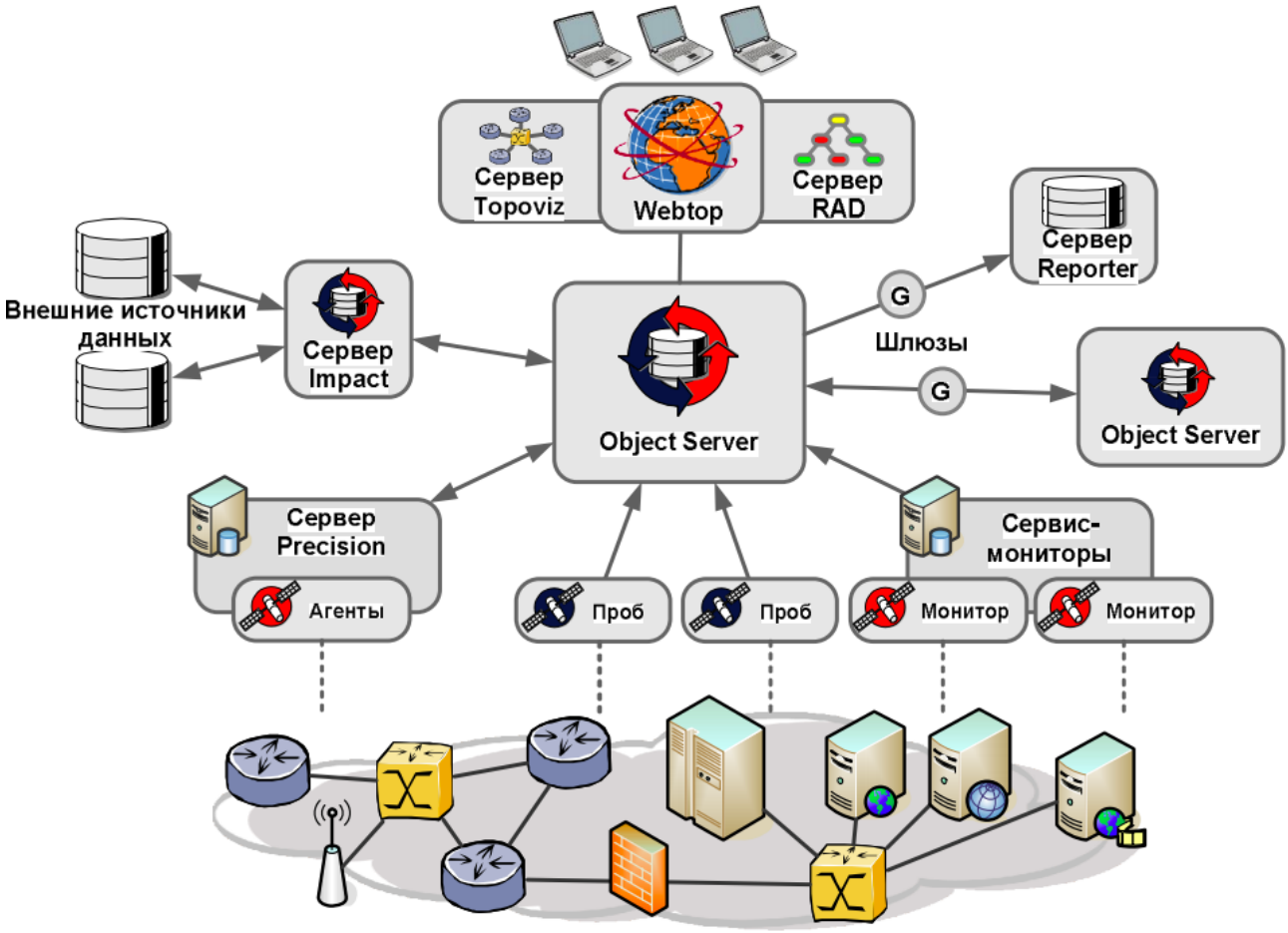


Рисунок 11.1 - Загальна архітектура рішення Cisco Info Center

Для интеграции элементов решения CIC используются шлюзы. Шлюзы обеспечивают односторонний или двусторонний механизм передачи данных компонентам CIC или элементам внешних информационных систем. Кроме того, шлюзы обеспечивают интеграцию компонентов CIC. Так, например, CIC может открыть обращение с описанием

неполадки в системе поддержки пользователей (Help Desk) или получить данные по клиенту из внешней базы даных.

Для інтеграції елементів рішення CIC використовуються шлюзи. Шлюзи забезпечують односторонній або двосторонній механізм передачі даних компонентам CIC або елементам зовнішніх інформаційних систем. Крім того, шлюзи забезпечують інтеграцію компонентів CIC. Так, наприклад, CIC може відкрити звернення з описом неполадки в системі підтримки користувачів (Help Desk) або отримати дані по клієнту із зовнішньої бази даних.

Ключові переваги Cisco Info Center

- Можливість контролю стану мереж, побудованих на обладнанні різних постачальників. Cisco Info Center отримує дані від різних пристроїв, перетворюючись в інтегрований центр обробки подій.
- Можливість управління як обладнанням, так і програмним забезпеченням. Можливості Cisco Info Center з інтеграції дозволяють створювати гнучкі комплекси відповідно до потреб замовника.
- Можливість поліпшення обслуговування клієнтів. Своєчасна реакція на проблемні ситуації дає можливість запропонувати новий рівень обслуговування клієнтів і впровадити проактивний похід до взаємодії з клієнтами.
- Можливість надання нових послуг. Web-технології Cisco Info Center дозволяють надавати клієнтам доступ до порталу і давати клієнту можливість контролювати події в його частині мережі.
- Правила кореляції подій, що налаштовуються, дозволяють зменшити кількість повідомлень, що вимагають обробки, в десятки і сотні разів, що істотно підвищує продуктивність праці персоналу Центру управління мережею.
- Управління бізнес-процесами. Універсальні проби дають можливість проводити моніторинг бізнес-процесів компанії і сповіщати зацікавлених осіб про збої.

Системні вимоги

Кількість і конфігурація серверів залежить від архітектури рішення (обраного набору додатків). Типові вимоги до серверів наведено в таблиці 11.1 [11].

Таблиця 11.1

Вимога	Опис
Мінімальний розмір оперативної пам'яті (ОЗУ)	Розмір ОЗУ залежить від конфігурації системи. Типова конфігурація, - 1ГБ.
Дисковий простір Solaris	Solaris, - 200МБ Windows 2000/XP – 70МБ Linux – 100МБ

Cisco Info Center поставляється у вигляді CD-ROM і доступний для завантаження по протоколу FTP через Інтернет.

Підтримувані платформи

Підтримувані операційні системи, на які можуть бути встановлені компоненти Cisco Info Center:

- Sun Solaris

- Microsoft Windows
- Linux

ПІДГОТОВКА ДО ВИКОНАННЯ КОМП'ЮТЕРНОГО ПРАКТИКУМУ №11

Перед виконанням комп'ютерного практикуму №11 рекомендується ознайомитись з принципами роботи програми моніторингу СІС, що розглядається в курсі лекцій, а також допоміжній літературі [11]. Розробити алгоритм розв'язання завдання. Провести обчислення і дослідження на ЕОМ. В Додатку Л наведено додатоку інформацію.

ВИМОГИ ДО ОФОРМЛЕННЯ ЗВІТУ

Звіт з комп'ютерного практикуму №11 обов'язково повинен містити наступну інформацію:

- назва комп'ютерного практикуму;
- мета роботи;
- постановка завдання і алгоритм його розв'язання;
- скріншоти;
- лістинг програми.

ЗАВДАННЯ ДЛЯ ЗАХИСТУ КОМП'ЮТЕНОГО ПРАКТИКУМУ №11

Завдання.

1. Втановити програмний пакет СІС (Додаток Л).
2. Здійснити налаштувати СІС (Додаток Л).
3. Додати карту.
4. Додати пристрої.
5. Налаштувати сервіс.

ПЕРЕЛІК ПОСИЛАНЬ

1. Документация Total Network Monitor / [Електроний ресурс] // https://www.softinventive.com/docs/TNM-docs-ru.pdf
2. Network monitoring with intuition / [Електроний ресурс] // https://www.observium.org/
3. The Industry Standard In IT Infrastructure Monitoring / [Електроний ресурс] // https://www.nagios.org
4. Мониторинг. Визуализация. Контроль / [Электронный ресурс] // https://www.ru.paessler.com/prtg
5. Kismet Wireless / [Електроний ресурс] // https://www.kismetwireless.net/
6. Wireshark Developer's Guide.Version 3.5.0 / [Електроний ресурс] // https://www.wireshark.org/docs/wsdg_html_chunked/
7. Rediscover your network! / [Електроний ресурс] // https://www.nedi.ch/
8. Программые и учебные файлы / [Электронный ресурс] // https://www.zabbix.com/documentation/ru/2.0/manual.
9. Network Olympus: Monitoring / [Електроний ресурс] // https://www.network-olympus.com/ru/monitoring/
10. Cacti® - The Complete RRDTool-based Graphing Solution / [Електроний ресурс] // https://www.cacti.net/what_is_cacti.php
11. Cisco Info Center. Решение для эффективного управления сетевыми отказами / [Электронный ресурс] // http://www.justogroup.ru/dokumentacija/cisco/upravlenie-i-monitoring/opisanie_cisco_infocenter.pdf

ДОДАТОК А

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ OBSERVIUM

Зайдіть на вашу віртуальну машину як Адмін. У ньому не повинно бути ніяких налаштованих пристроїв. Відредагуйте файл конфігурації для Observium, щоб «сказати» йому про вашу мережу

$ sudo editor /opt/observium/config.php

Тепер зробіть наступні зміни:
Знайдіть рядок:

$config['snmp']['community'] = array("public");

та змініть ‘public’ на ‘NetManage’ (НЕ “netmanage” и НЕ “NETMANAGE”),
так що рядок виглядає таким чином:

$config['snmp']['community'] = array("NetManage");

Також, додайте наступний рядок:

$config['autodiscovery']['xdp'] = TRUE;

Збережіть файл і вийдіть з редактора.
Додайте хост - ваш власний роутер
У web-інтерфейсі (http://observiumX.ws.nsrc.org), зайдіть в меню “Device ”, і натисніть “Add Device ” Ім'я хоста: rtrX.ws.nsrc.org версія SNMP: v2c [повинен бути вже обраний]
SNMP Community: ви можете залишити це поле порожнім, тому що ми вже налаштували його в config.php; Ви також можете ввести його: NetManage. Якщо все йде добре, ви повинні побачити кілька повідомлень типу:

Adding host rtrX.ws.nsrc.org community NetManage port 161
Trying v2c community NetManage ...
Device added (id = 1)

Ви можете зайти на сторінку пристрою в Observium, і побачити, що пристрій було справді додано: http://observiumX.ws.nsrc.org/devices/ Ви можете погратися з веб-інтерфейсом пару хвилин - але поки там немає ніяких даних, і якщо ви натиснете на пристрій (rtrx), Observium поскаржиться, що пристрій поки не було виявлено.
Ви може сказати Observium почати збір даних для цього пристрою, запустивши наступну команду:

$ cd /opt/observium
$ sudo ./poller.php -h all

Ми автоматизуємо цей процес надалі.
Скажіть Observium зробити сканування мережі і почати збір даних:

$ cd /opt/observium
$ sudo ./discovery.php -h all

Зверніть увагу на те, що в результаті з'явиться багато нової інформації! Ми запустимо збір даних знову вручну:

$ sudo ./poller.php -h all

Знову зайдіть на web-інтерфейс http://observiumX.ws.nsrc.org/ На що ви звернули увагу? Як, на вашу думку, зміг Observium виявити інші пристрої в мережі, і звідки він дізнався як з ними зв'язатися?

Активуйте завдання в cron. Зараз гарний час для налаштування того, щоб збір даних відбувався автоматично.

Кілька автоматичних завдань повинні бути додані в cron:

Створіть файл /etc/cron.d/observium:

$ sudo editor /etc/cron.d/observium

і скопіюйте наступні рядки:

```
33  */6  * * *  root   /opt/observium/discovery.php -h all >> /dev/null 2>&1
*/5 *    * * *  root   /opt/observium/discovery.php -h new >> /dev/null 2>&1
*/5 *    * * *   root   /opt/observium/poller-wrapper.py 1 >> /dev/null 2>&1
```

Пройде якийсь час перш ніж дані з'являться на графіках.

Поки ми чекаємо появи даних, ми можемо пройтися по інтерфейсу Зайдіть на http://observiumX.ws.nsrc.org/ Натисніть “Devices” у верхньому меню. Знайдіть роутер вашої групи в списку пристроїв, і натисніть на його ім'я. Ви потрапите на оглядову сторінку для пристрою. Зверніть увагу на те, що Observium автоматично знайшов велику кількість інформації про ваш роутер! Вгорі, під ім'ям роутера, ви побачите список вкладок, кожна з яких показує певну інформацію про ваш пристрій:

Overview | Graphs | Health | Ports | Routing | Inventory | Logs | Alerts

У вкладці “Graphs”, ви побачите всю інформацію, яка може бути показана у формі графіка: мережевий трафік, дисковий ввід / виведення, використання пам'яті і процесора, і т. д.

Ви також побачите вкладку “Health”, яка показує різну інформацію про те, як "залізо " пристрою себе почуває - якщо ця інформація доступна - таку як температуру, напругу, швидкість обертання вентиляторів, і т. д. Зауважте, що деяка інформація звідси також присутня на оглядовій сторінці для пристрою (на яку Ви потрапляєте при натисканні на ім'я пристрою).

Тепер ми подивися на вкладку порти “Ports”. Там ви знайдете зведення трафік на всіх портах, включаючи біти в секунду і пакети в секунду, швидкість порту, і тип з'єднання (Ethernet або інший тип). Зверніть увагу на те, що на всі елементи можна клікнути, і ви потрапите на відповідну сторінку для джерела даних.

Вкладка “Routing” покаже вам огляд працюючих протоколів роутингу. Якщо ви активували OSPF або BGP на роутерах, Ви отримаєте інформацію про активні сесії, сусідів, і іншу інформацію, що відноситься до протоколу.

Вкладка “Inventory” містить повний список модулів і серійних номерів для обладнання, встановленого на роутері. Це не буде працювати для всіх виробників.

У вкладці “Logs” ви побачите список подій для роутера: в зміни конфігурації, в статусі інтерфейсів, сервісів і т. д.

Зараз вкладка оповіщень “Alerts” порожня-надалі ми розберемося з цим.

Подивіться на функцію “Map” у вкладці “Ports”.

Це автоматично створена діаграма топології вашої мережі, як вона видно з точки

зору роутера. Це буде працювати тільки для пристроїв, що підтримують CDP / LLDP (Cisco, IOS,...) Ви можете активувати CDP / LLDP на ваших Linux серверах, встановивши ladvd (**sudo apt-get install ladvd**). Спробуйте додати пристрої під управлінням ОС Linux таким чином. Ця функція доступна, тільки якщо ви активувати автовиявлення.

Додайте місце розташування та контактну інформацію для вашого роутера. Якщо ви перейдете назад на оглядову сторінку роутера (перейдіть на Devices, натисніть на ім'я роутера), ви побачите, що Observium визначив платформу, операційну систему, і час роботи вашого пристрою.

Тепер, залогіньтесь на роутер за допомогою програми SSH і додайте наступну інформацію в конфігурацію по SNMP:

Встановіть місце розташування (використовуйте формат місто, країна, так що ваш хост з'явиться на оглядовій сторінці з географічною картою) Додайте контактну інформацію (адресу пошти або ім'я)

Ось як це зробити:

rtr8> enable
Password:
rtr8# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
rtr8(config)# snmp-server contact user@email.address
rtr8(config)# snmp-server location City, Country
rtr8(config)# exit
rtr8# write memory

Вам слід замінити “City, Country” на місто і країну, в якій ви знаходитесь). Наприклад:

Bloomington, Indiana

Thimphu, Bhutan і т. д.

Якщо ви почекаєте кілька хвилин(до 5), ви повинні побачити, що ця інформація автоматично з'явилося в оглядовій вкладці роутеру в OB-serviume.

Інтересу заради, домовтеся з вашими колегами в групі, і попросіть їх вибрати різні місто і країну для кожного роутера. Зачекайте поки Observium не пересканував пристрої, і подивіться на карту світу на головній сторінці Обсервиума (http://observiumX.ws.nsrc.org/)

Додавання опису інтерфейсу

Поки ви з'єднані з роутером, додайте псевдо-інтерфейс, щоб побачити, чи виявить його Observium:

rtr8(config)# interface loopback123
rtr8(config-if)# description A useless interface
rtr8(config-if)# exit
rtr8(config)# exit
rtr8# write memory

Ця інформація теж повинна з'явитися в Observiume через якийсь час - спробуйте знайти опис у вкладці **“Ports”**

Пошук за IP-адресою

На головній сторінці Observium, ви знайдете, в меню "огляд" вгорі сторінки, підменю **“Search”** з п'ятьма пунктами:

- IPv4 search -> http://observiumX.ws.nsrc.org/search/search=ipv4/
- IPv6 search -> http://observiumX.ws.nsrc.org/search/search=ipv6/
- MAC search -> http://observiumX.ws.nsrc.org/search/search=mac/
- ARP/NDP tables -> http://observiumX.ws.nsrc.org/search/search=arp/

Використовуючи пошук за таблицями IPv4 і ARP, спробуйте знайти IP адреси обладнання в класі:

- IP шлюзу (10.10.0.254)
- IP роутерів (10.10.X.254)
- IPs віртуальних машин (10.10.1.1, 10.10.5.17, і т. д...)

Спробуйте пошук IP вашого власного ноутбуку! Знайдіть його IP, а подивіться, чи можете ви його знайти в Observiume. Можете? Чому?

Додайте маршрутизатор

З пункту меню вгорі сторінки "Devices", виберіть "Add device". Заповнивши наступні поля:

Hostname: sw.ws.nsrc.org

Community: NetManage

Натисніть на “Add Host”. Через кілька секунд, Observium повинен додати маршрутизатор. Через кілька хвилин, повинні з'явитися його дані. Зверніть увагу на рядок "Ports" справа вгорі інтерфейсу. Чи Сказано там, що якісь порти не працюють? Які? Спробуйте натиснути на повідомлення “X down” щоб побачити, які порти неактивні на яких пристроях.

Відключимо невикористовувані порти

Знайдіть оглядову сторінку для "sw.ws.nsrc.org". Звідси, ви можете налаштувати пристрій (іконка "ключ" справа вгорі). З'явиться сторінка конфігурації пристрою. Натисніть на “Ports”, Ви отримаєте оглядову сторінку стану портів на маршрутизаторі. Знайдіть ті, які позначені як "вниз". Відзначте прапорець “Ignore” для цих портів, потім натисніть на “Save” під “Index”.

Якщо ви знову підете на головну сторінку: http://observiumX.ws.nsrc.org/

Observium більше не повинен виділяти ці порти.

Чи спробували ви додати вашу віртуальну машину? Інші віртуальні машини?

Інші цікаві речі:

- З верхнього меню, виберіть Devices - > All devices
- Знайдіть ваш роутер в списку, і натисніть на нього.
- Під зведенням графіків, ви побачите список інтерфейсів на роутері: Fa0/0, Fa0/1, Null0.
- Натисніть на Fa0/0.
- Натисніть на " Real Time”

Налаштування регіону на карті

Якщо хочете, ви можете поміняти частину світу, яку карта буде показувати при вході в Observium.

Знайдіть параметри для цього тут: http://www.observium.org/wiki/Configuration_Options#Map_overview_settings Зокрема, $config ['frontpage'] ['map'] ['region'] може бути встановлений в якусь країну або Регіон.\

Більше інформації може бути знайдено в https://developers.google.com/chart/interactive/docs/gallery/geochart

Параметр $ config ['frontpage'] ['map'] ['region'] може приймати декілька значення. Звідси:

https://developers.google.com/chart/interactive/docs/gallery/geochart

region: площа для презентації на карту (навколишні території теж будуть показані). Може бути одне з:

- 'world' - карта всього світу
- континент або під-континент задається кодом з 3-х цифр, наприклад, '011' для Західної Африки.
- Країна задається дво-літерним ISO 3166-1 alpha-2 кодом, наприклад 'AU' для Австралії.

- Штат у Сполучених Штатах Америки задається кодом ISO 3166-2: US,наприклад 'US-AL' для Алабами. Зверніть увагу, що параметр "resolution" повинен бути або 'provinces' або 'metros'.

Ви можете погратися з цими можливостями змінюючи параметр і перевантажуючи оглядову сторінку в Observiume.

ДОДАТОК Б

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ NAGIOS

Встановлення Nagios

Для початку на server01 необхідно встановити пакет nagios. Для цього введіть в терміналі:

sudo apt-get install nagios3 nagios-nrpe-plugin

Вам буде запропоновано ввести пароль для користувача nagiosadmin. Облікові записи користувача знаходяться в/etc/nagios3/htpasswd.users. Для зміни пароля користувача або додавання інших для виконання CGI скриптів Nagios використовуйте утиліту htpasswd, яка є частиною пакету apache2-utils. apache2-utils.

Наприклад, для зміни пароля користувача nagiosadmin введіть в термінал:

sudo htpasswd/etc/nagios3/htpasswd.users nagiosadmin

Для додавання користувача:

sudo htpasswd/etc/nagios3/htpasswd.users steve

Далі, на server02 встановіть пакет nagios-nrpe-server. У терміналі на server02 введіть:

sudo apt-get install nagios-nrpe-server

NRPE дозволяє виконувати локальні перевірки на віддаленому комп'ютері. Але існують і інші способи досягнення цієї мети, використовуючи інші плагіни Nagios, також як і інші способи перевірок.

Огляд конфігурації

Існує кілька каталогів, що містять конфігураційні файли Nagios а також файли перевірок.

• /etc/nagios3: містить конфігураційні файли для роботи демона nagios, CGI-файлів, хостів та ін.

• /etc/nagios-plugins: файли конфігурації для службових перевірок.

• /etc/nagios: містить конфігураційні файли на віддаленому
комп'ютері Nagios-nrpe-server.

• /usr/lib/nagios/plugins/: тут знаходяться бінарні перевірки. Для перегляду опцій перевірки використовуйте ключ-*h*.

Наприклад:

/usr/lib/Nagios/plugins/check_dhcp -h

Існує безліч перевірок Nagios, які можуть бути налаштовані для виконання на будь-якому комп'ютері. У цьому прикладі Nagios буде налаштований на перевірку дискового простору, служби DNS, а також групи користувачів MySQL. Перевірка DNS буде здійсняться на server02, а група комп'ютерів MySQL буде включати в себе як server01, так і server02.

На додаток до цього будуть наведені кілька термінів, які допоможуть вам полегшити Налаштування Nagios:

- Host: сервер, робоча станція, мережевий пристрій і т.д., який відстежується.

- Host Group: група подібних комп'ютерів. Наприклад ви можете згрупувати всі веб-сервери, файлові сервери і т. д.
- Service: служба, яка відстежується на комп'ютері. Наприклад HTTP, DNS, NFS і т. д.
- Група служб: дозволяє об'єднати кілька служб разом. Наприклад, це буде корисним для об'єднання декількох веб-серверів.
- Контакт: людина, яка буде повідомлена при будь-якій події. Nagios може бути налаштований на відправку email, SMS-повідомлень і т. д.

За замовчуванням Nagios налаштований на перевірку HTTP, дискового простору, SSH, поточних користувачів, процесів і стеження за рівнем завантаження на локальному комп'ютері (localhost). Nagios також виконує перевірку шлюзу за допомогою команди ping.

Налаштувати Nagios на безлічі комп'ютерів може бути досить складно. Почати краще з декількох комп'ютерів, одного або двох, налаштувати все оптимальним чином, а потім розширити налаштування для більшої кількості комп'ютерів.

Конфігурація

Для початку необхідно створити конфігураційний файл для server02. Якщо не вказано інше, виконайте всі ці команди на server01.

Введіть у терміналі:

conf.d/localhost_nagios2.cfg\/etc/nagios3/conf.d/server02.cfg

Примітка. У вищевказаному, а також наступному прикладі замініть "server01", "server02", 172.18.100.100 та 172.18.100.101 на ім'я та IP-адреси ваших серверів.

Далі відредагуйте файл /etc/nagios3 / conf.d/server02.cfg:

```
define host{
use                     generic-host ; Name of host template to use
host_name               server02
alias                   Server 02
address                 172.18.100.101
}

# check DNS service.
define service {
use                     generic-service
host_name               server02
service_description     DNS
check_command           check_dns!172.18.100.101
}
```

Перезавантажте демон nagios Для активації нових налаштувань:

sudo /etc/init.d/nagios3 restart

Тепер додамо службовий опис для перевірки MySQL шляхом додавання наступних рядків в/etc / nagios3 / conf.d/services_nagios2.cfg:

```
# check MySQL
servers.
define service {
hostgroup_name          mysql-servers
service_description     MySQL
```

```
check_command          check_mysql_cmdlinecred!nagios!secret!$HOSTADDRESS
use                    generic-service
notification_interval  0 ; set > 0 if you want to be renotified
}
```

Зараз повинні бути визначена група mysql-servers. Відредагуйте /etc/nagios3/conf.d/hostgroups_nagios2.cfg, додавши наступне:

```
# MySQL hostgroup. define hostgroup {
                hostgroup_name mysql-servers
                alias                MySQLservers
                members              localhost, server02
                }
```

Перевірка Nagios повинна пройти аутентифікацію в MySQL. Щоб додати користувача nagios до MySQL, введіть:

```
mysql -u root -p -e "create user nagios identified by 'secret';"
```

Примітка. Користувач nagios повинен бути присутнім на всіх комп'ютерах робочої групи серверів mysql-servers.

Перезавантажте nagios для перевірки сервера MySQL.

```
sudo /etc/init.d/nagios3 restart
```

Нарешті, необхідно налаштувати NRPE для перевірки дискового простору на server02. На server01 додамо службову перевірку в /etc/nagios3/conf.d/server02.cfg:

```
# NRPE disk check.
define service {
use                    generic-service
host_name              server02
service_description    nrpe-disk
check_command          check_nrpe_1arg!check_all_disks!172.18.100.101
}
```

Тепер на server02 відредагуємо /etc/nagios/nrpe.cfg:

```
allowed_hosts=172.18.100.100
```

А в рядок оголошення команди додамо:

```
command[check_all_disks]=/usr/lib/nagios/plugins/check_disk -w 20% -c 10% -e
```

В кінці перезавантажимо nagios-nrpe-server:

```
sudo /etc/init.d/nagios-nrpe-server restart
```

На server01 також потрібно перезавантажити nagios:

```
sudo /etc/init.d/nagios3 restart
```

Тепер ви повинні бачити ваші сервери і службові перевірки в файлах Nagios CGI.

Для доступу до них наберіть в рядку браузера http://server01/nagios3. Вам буде запропоновано ввести ім'я користувача та пароль для nagiosadmin.

ДОДАТОК В

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ PRTG NETWORK MONITOR

Приклад моніторигна серверної кімнати (див. рисунок В.1).

Рисунок В.1 - Карта (вид зверху)

В результаті настройки поточний стан датчиків буде видно на карті PRTG Network Monitor, буде можливо миттєве оповіщення відповідальних осіб про відхилення параметрів навколишнього середовища за допомогою SMS / e-mail, а також отримання періодичних звітів про стан навколишнього середовища в приміщенні і аудит аналізу даних за минулі проміжки часу.

Приклад повідомлення про затоплення серверної кімнати (див. рисунок В.2).

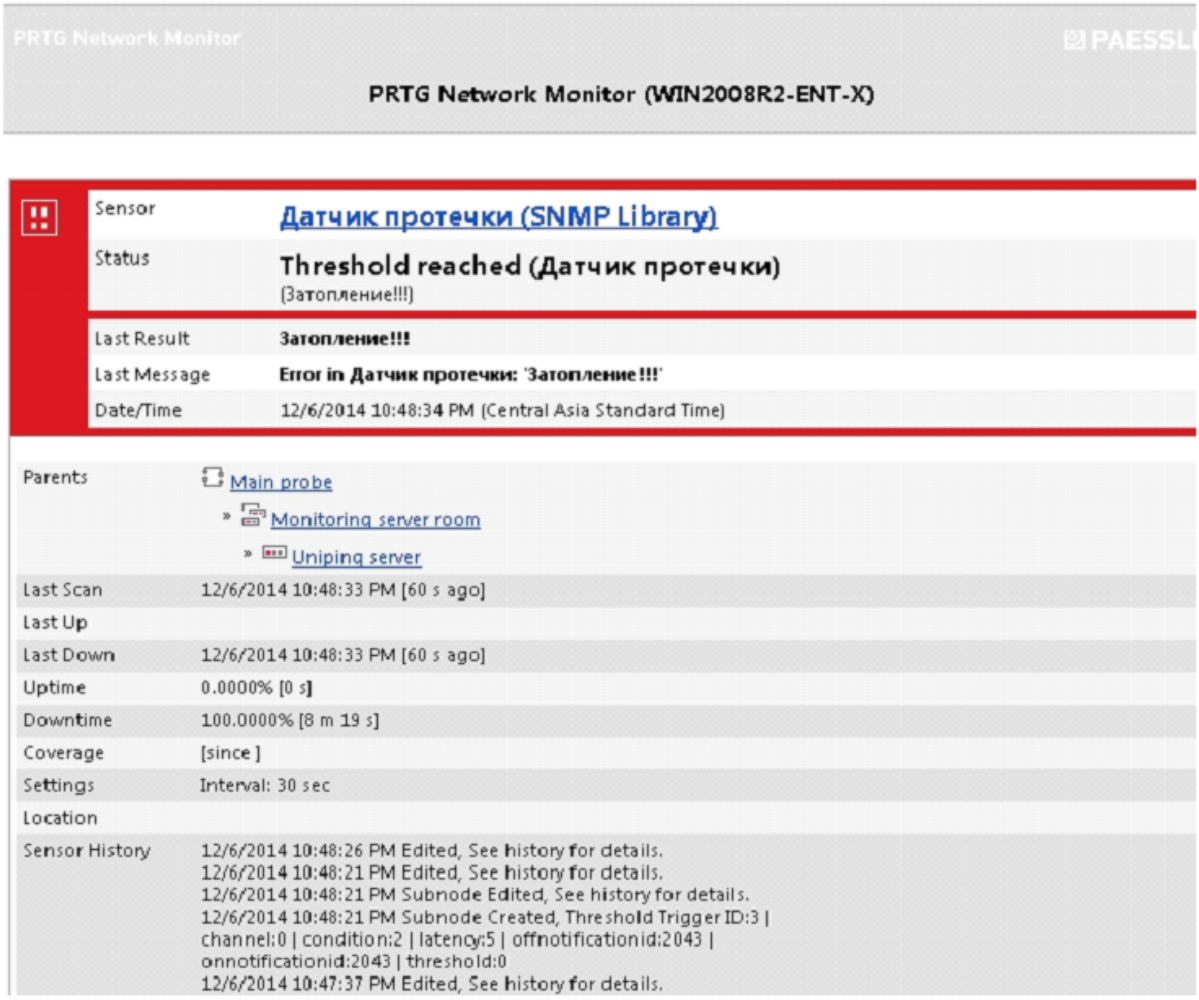


Рисунок В.2 - Повідомлення про затоплення серверної кімнати

Зведений звіт про стан серверної кімнати (графіки і дані) за місяць (див. рисунок В.3):

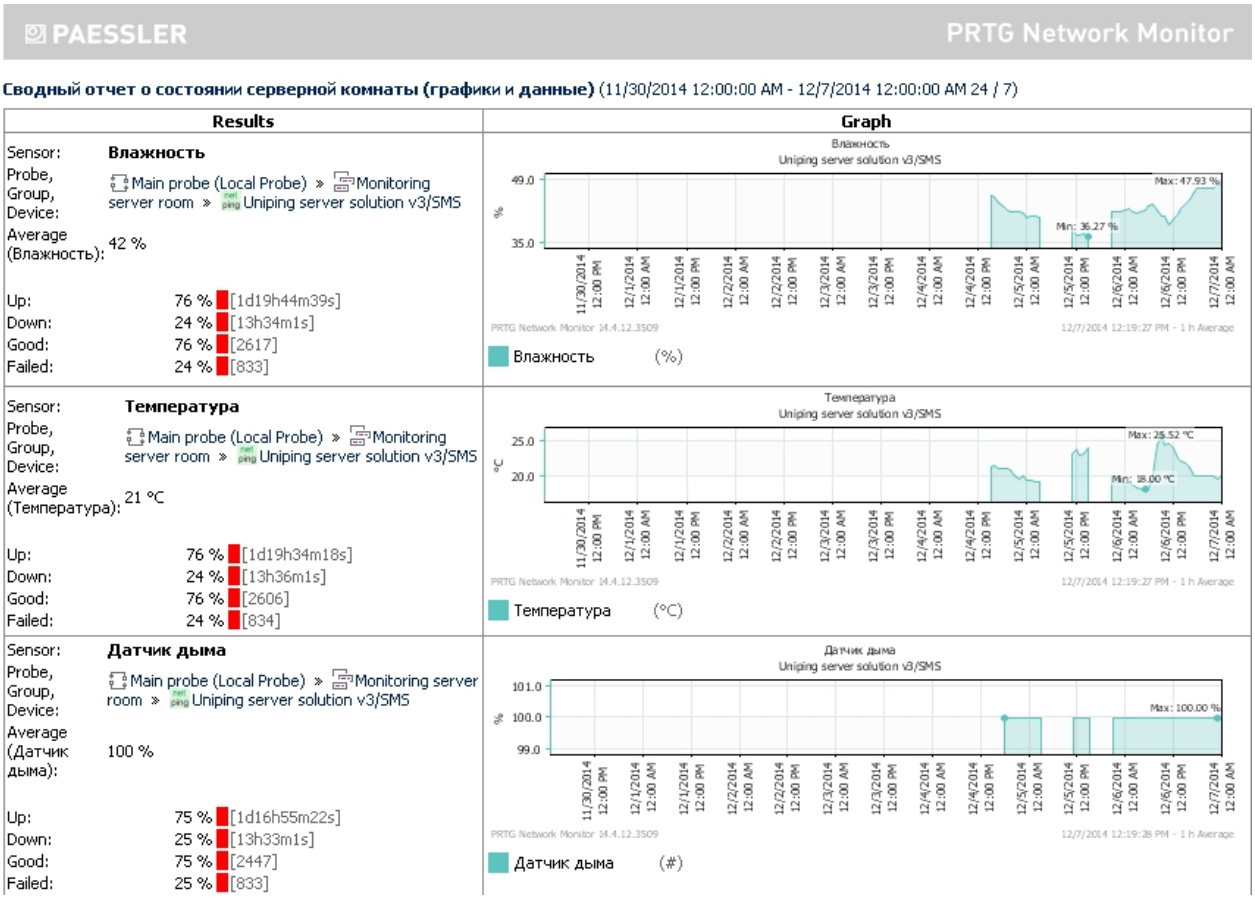


Рисунок В.3 - Звіт про стан серверної кімнати

Пристрій UniPing server solution v3 / SMS спільно з налагодженою системою моніторингу PRTG Network Monitor забезпечить контроль над температурою і вологістю в серверній кімнаті, запобігає виникненню пожежонебезпечної ситуації або виходу з ладу обладнання в результаті затоплення і забезпечить контроль доступу в закрите приміщення серверної кімнати або в шафу.

До переваг організації на основі такої схеми моніторингу можна віднести:

• наявність простої установки і налаштування апаратного забезпечення пристрою NetPing с датчиками;

• наявність швидкої і нескладної настройки PRTG Network Monitor;

• наявність докладної документації та технічної підтримки по UniPing server solution v3 / SMS і PRTG Network Monitor;

• стабільний контроль параметрів;

• миттєве отримання повідомлень за потребою декількома способами;

• побудова детальних звітів різної складності;

• наявність історії подій.

вимоги

Для реалізації роботи вище описаного прикладу моніторингу серверної кімнати на основі PRTG Network Monitor і UniPing server solution v3 / SMS необхідно:

• пристрій віддаленого моніторингу UniPing server solution v3 / SMS;

• термодатчик для вимірювання температури навколишнього повітря в серверній кімнаті;

•датчик вологості;

• датчик відкриття / закриття дверей;

• датчик протікання;

• датчик диму;

• розгорнута система моніторингу PRTG Network Monitor в локальній мережі.

Вважаємо, що всі датчики підключені до UniPing server solution v3 / SMS в відповідні інтерфейси і заздалегідь налаштовані.

Опис системи PRTG Network Monitor і керівництво користувача з встановлення та налаштування системи під час першого запуску можна знайти на офіційному сайті за адресою http://www.paessler.com/support/manuals.

Для установки і роботи PRTG Network Monitor v14 необхідно:

• ПК, сервер або віртуальна машина з CPU не раніше 2007 року випуску і мінімум 1GB RAM;

• Microsoft Windows 7 або новіша ОС (архітектура x86 або x64 біта); \

• Web-браузер Google Chrome v38 і вище (рекомендується), Firefox v33 і вище, Internet Explorer 10 або 11.

Більш детальна інформація по системним вимогам системи PRTG Network Monitor є за адресою: http://www.paessler.com/prtg/detailed-requirements.

Налаштування системи

Підключення до PRTG Network Monitor

Підключитися в браузері до web-інтерфейсу системи PRTG Network Monitor v14 і пройти авторизацію (див. рисунок В.4):

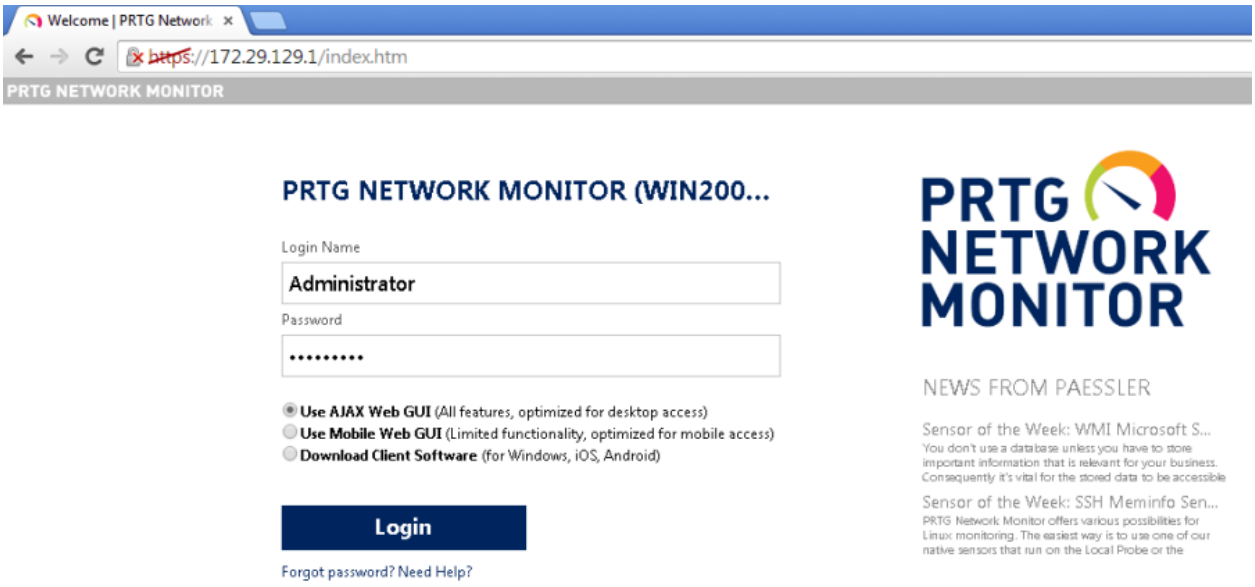


Рисунок В.4 - Підключення в браузері до web-інтерфейсу

В даному прикладі система PRTG Network Monitor встановлена на сервері з IP-адресою 172.29.129.1

Після авторизації з'явиться стартова сторінка системи PRTG, з якої необхідно почати налаштування моніторингу серверної кімнати (див. рисунок В.5):

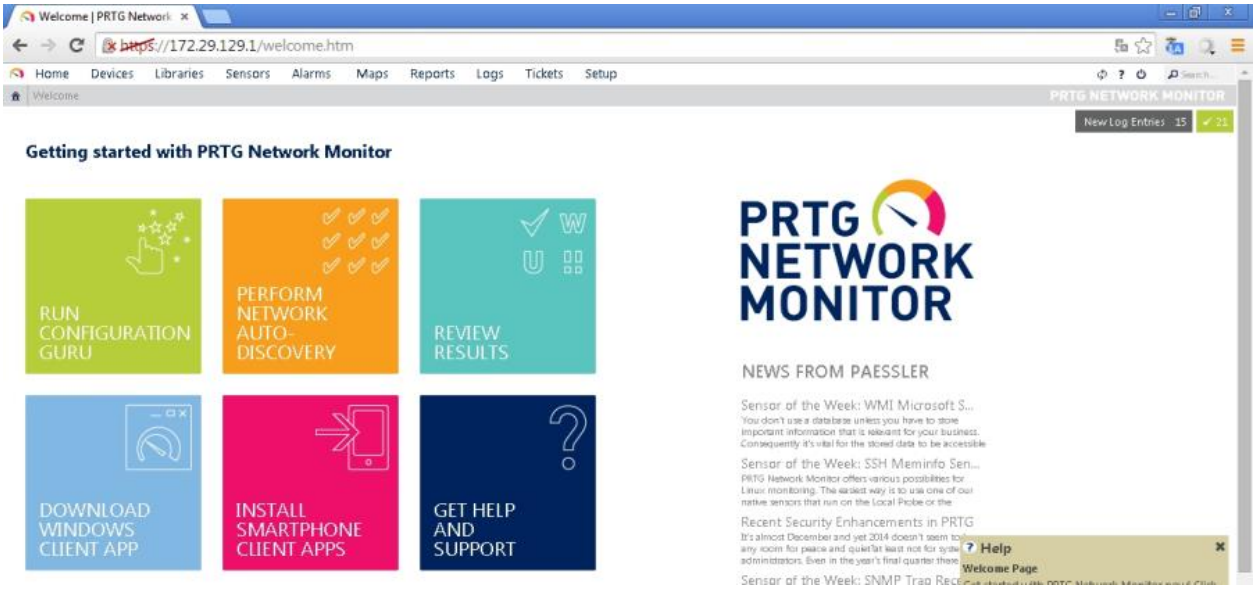


Рисунок В.5 - Стартова сторінка системи PRTG

Додавання пристрою UniPing server solution v3 / SMS в PRTG

Перед додаванням пристрою UniPing server solution v3 / SMS в PRTG необхідно підключити до нього всі наявні датчики і налаштувати його так, щоб на web-інтерфейсі пристрою відображалися всі значення. Перед додаванням самого пристрою UniPing server solution v3 / SMS в PRTG рекомендується додати групу для визначення ієрархічного порядку і загального функціоналу всіх пристроїв, що знаходяться в групі.

Щоб додати групу вручну необхідно перейти по вкладці «Devices», пункт меню «Add Group» (див. рисунок В.6):

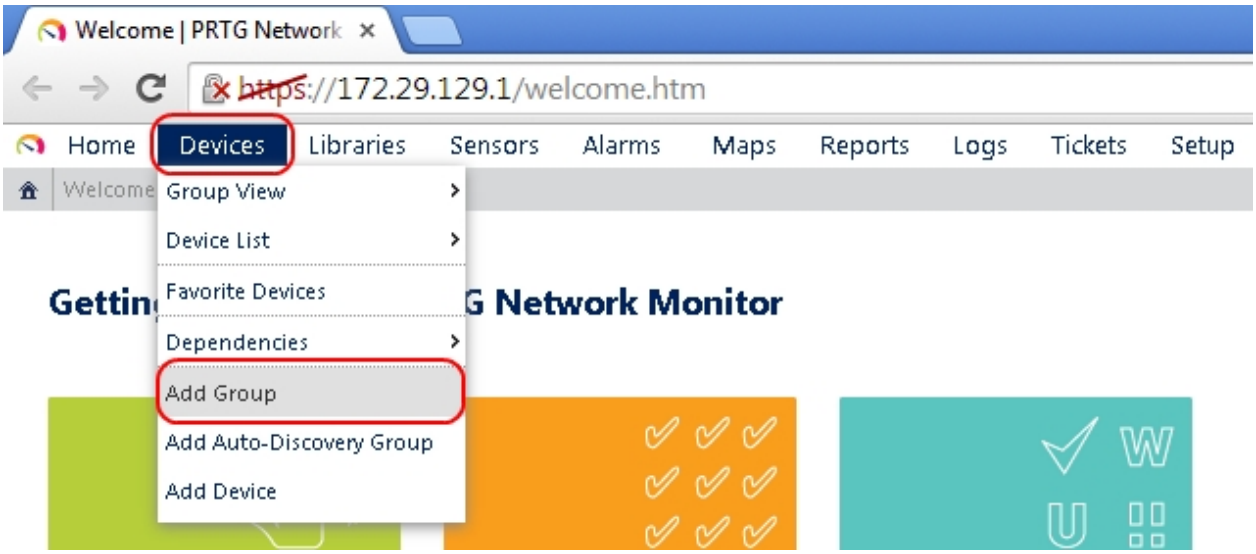


Рисунок В.6 - Вкладка «Devices», пункт меню «Add Group»

На сторінці «Add Group» вибрати «Main probe», в якому буде створена нова група для моніторингу серверної кімнати, і натиснути кнопку «Continue>» (див. рисунок В.7):

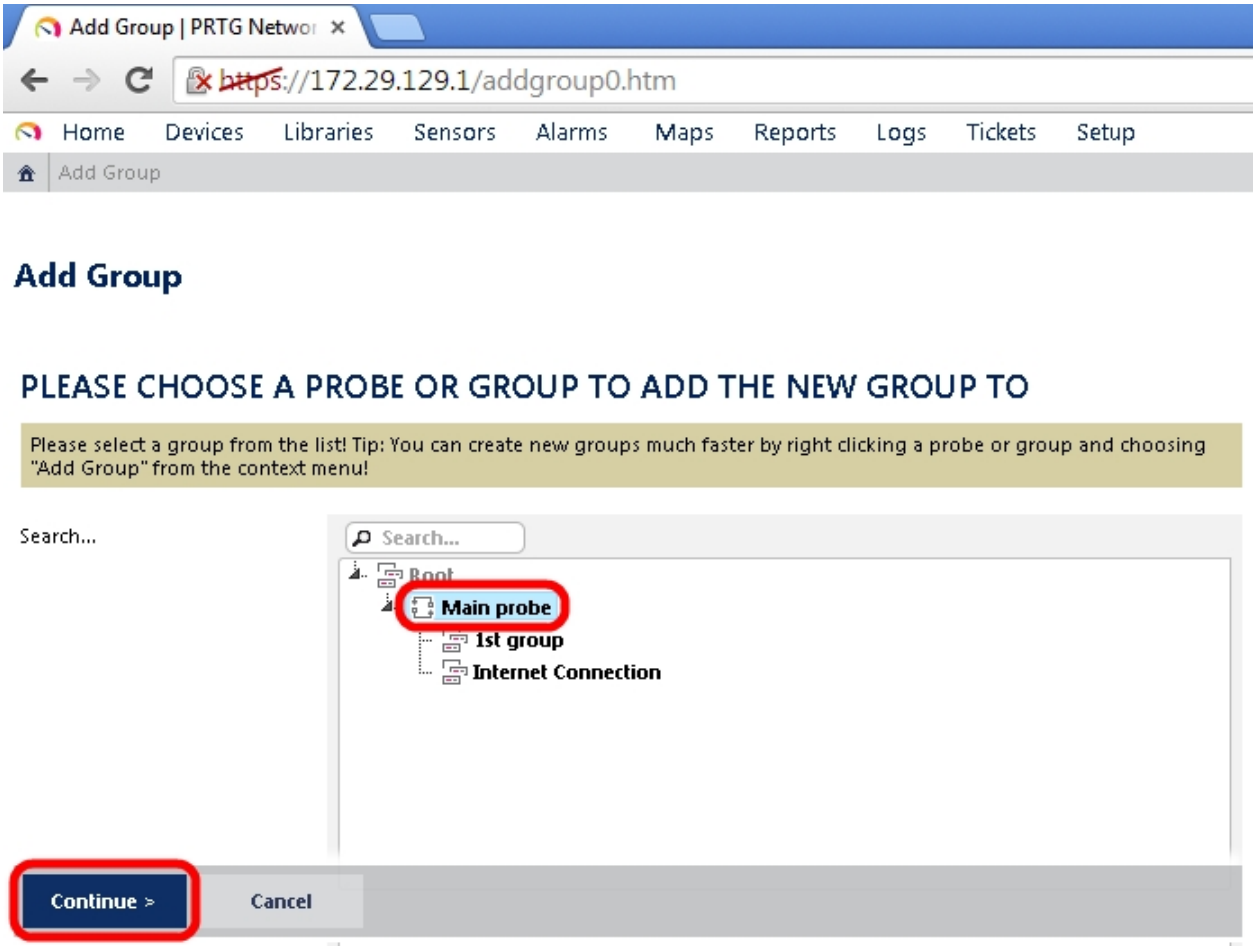


Рисунок В.7 - Сторінка «Add Group», пункт меню «Main probe»

Заповнити всі необхідні параметри на другому кроці створення нової групи, сторінка «Add Group to Group Main probe» (див. рисунок В.8):

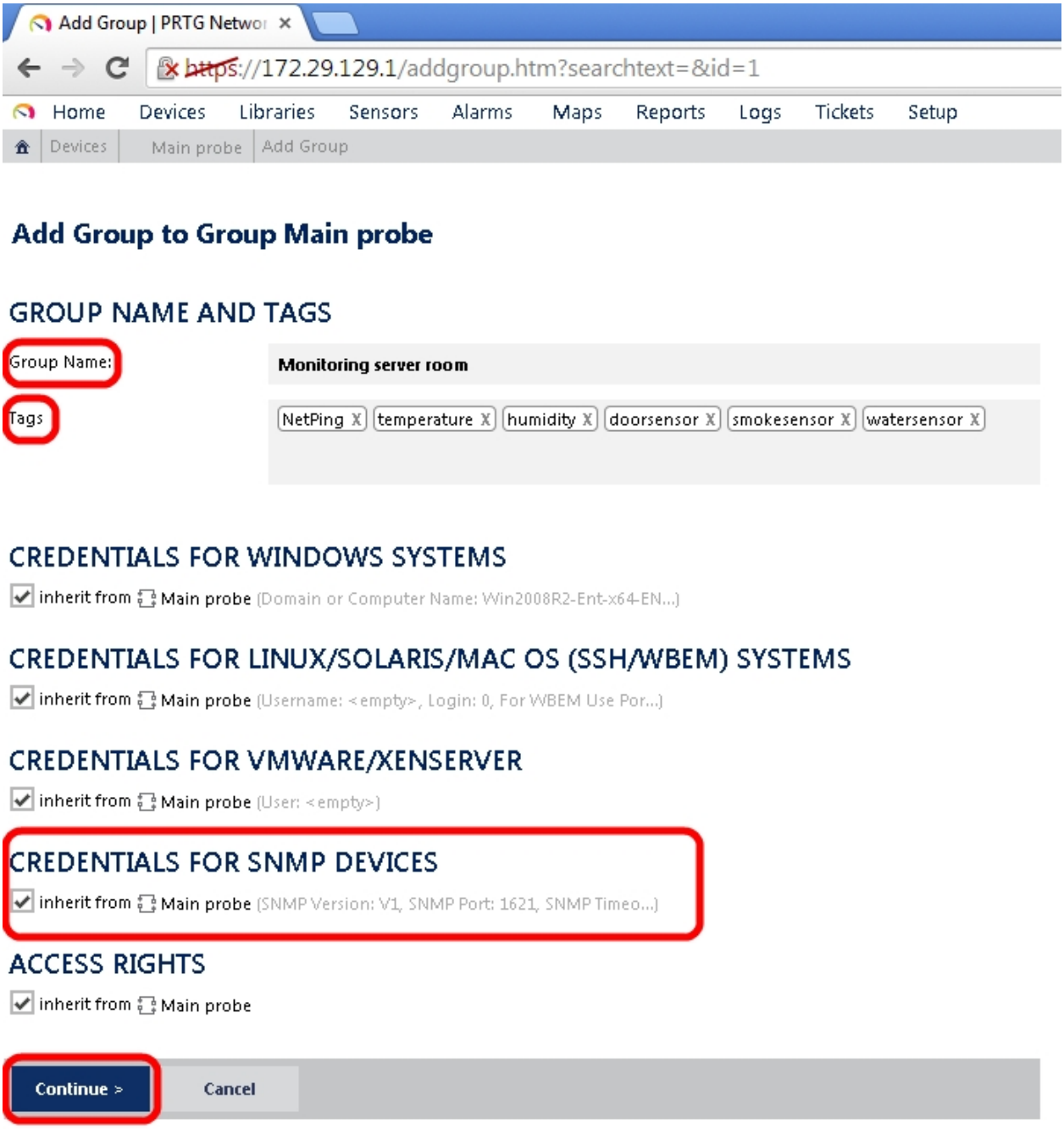


Рисунок В.8 - Сторінка «Add Group to Group Main probe»

де:

Group name - ім'я групи для ідентифікації. Ім'я буде відображатися за замовчуванням в дереві пристроїв і у всіх повідомленнях про помилки.

Tags - теги групують об'єкти в системі PRTG, а також дозволяють їх фільтрувати по цікавого функціоналу.

Credentials for SNMP devices - дані для підключення до пристроїв для моніторингу і управління по протоколу SNMP.

Для налаштування параметрів «Credentials for SNMP devices» необхідно або наслідувати параметри, сконфігуровані при першому запуску PRTG в конфігураторі Guru (http://www.paessler.com/support/video_tutorials/configuration-guru), установкою галочки «inherit from Main probe», або прибрати галочку «inherit from Main probe» і заповнити пропоновану форму відповідними параметрами, взятими з web-інтерфейсу пристрою UniPing server solution v3 / SMS (див. рисунок В.9):

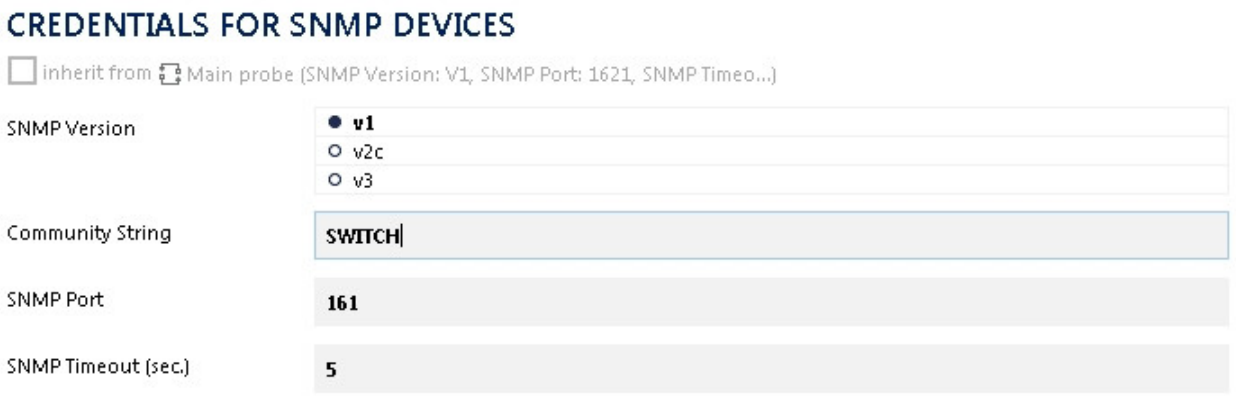


Рисунок В.9 - Налаштування параметрів «Credentials for SNMP devices»

Після завершення налаштування параметрів групи натисніть на кнопку «Continue>». Нова група «Monitoring server room» з'явиться на сторінці «Group room» (див. рисунок В.10):

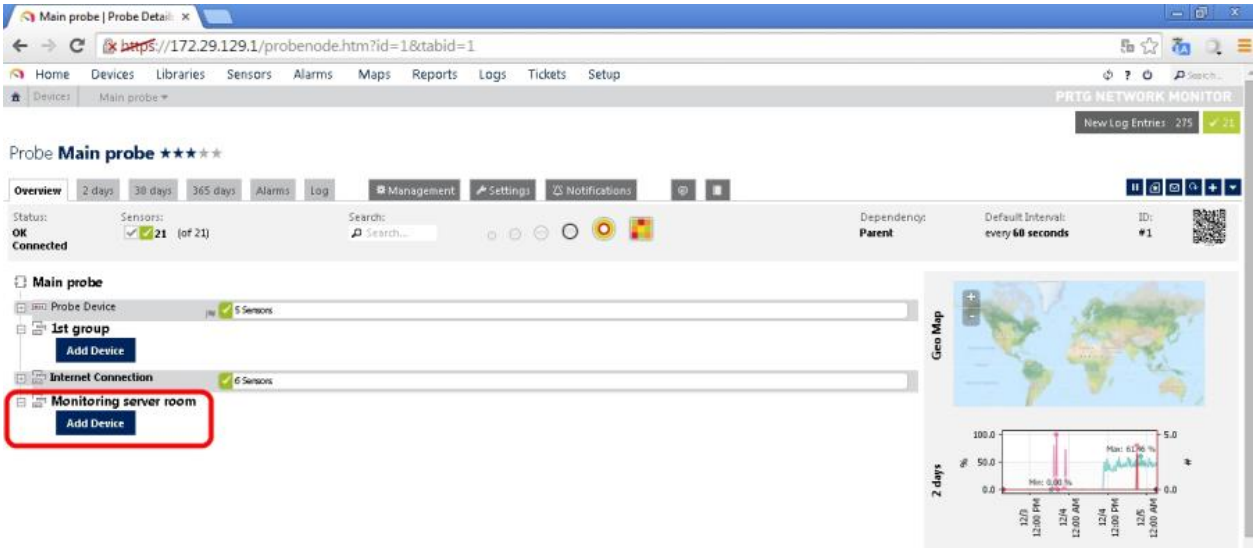


Рисунок В.10 - Група «Monitoring server room»

Далі натиснути на кнопку «Add Device», яка розташована під назвою групи «Monitoring server room», для додавання UniPing server solution v3 / SMS (див. рисунок В.11):

Рисунок В.12 - Додавання UniPing server solution v3 / SMS

Або можна додати новий пристрій через верхнє меню, вкладка «Devices», пункт контекстного меню «Add Device» (див. рисунок В.13):

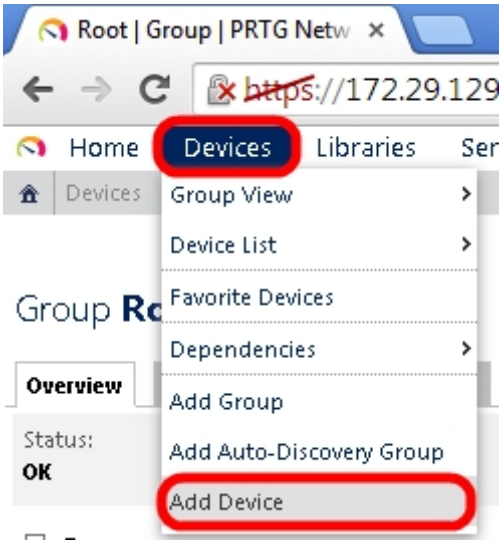


Рисунок В.13 - Вкладка «Devices», пункт контекстного меню «Add Device»

Процес додавання нового пристрою проходить в два етапи. Перший етап - на сторінці «Add devices» вибрати параметр «Add device to an existing group» і вказати вже заздалегідь створену групу «Monitoring server room» у доданому пристрою. Натиснути кнопку «Continue>» для переходу на другий етап настройки (див. рисунок В.14):

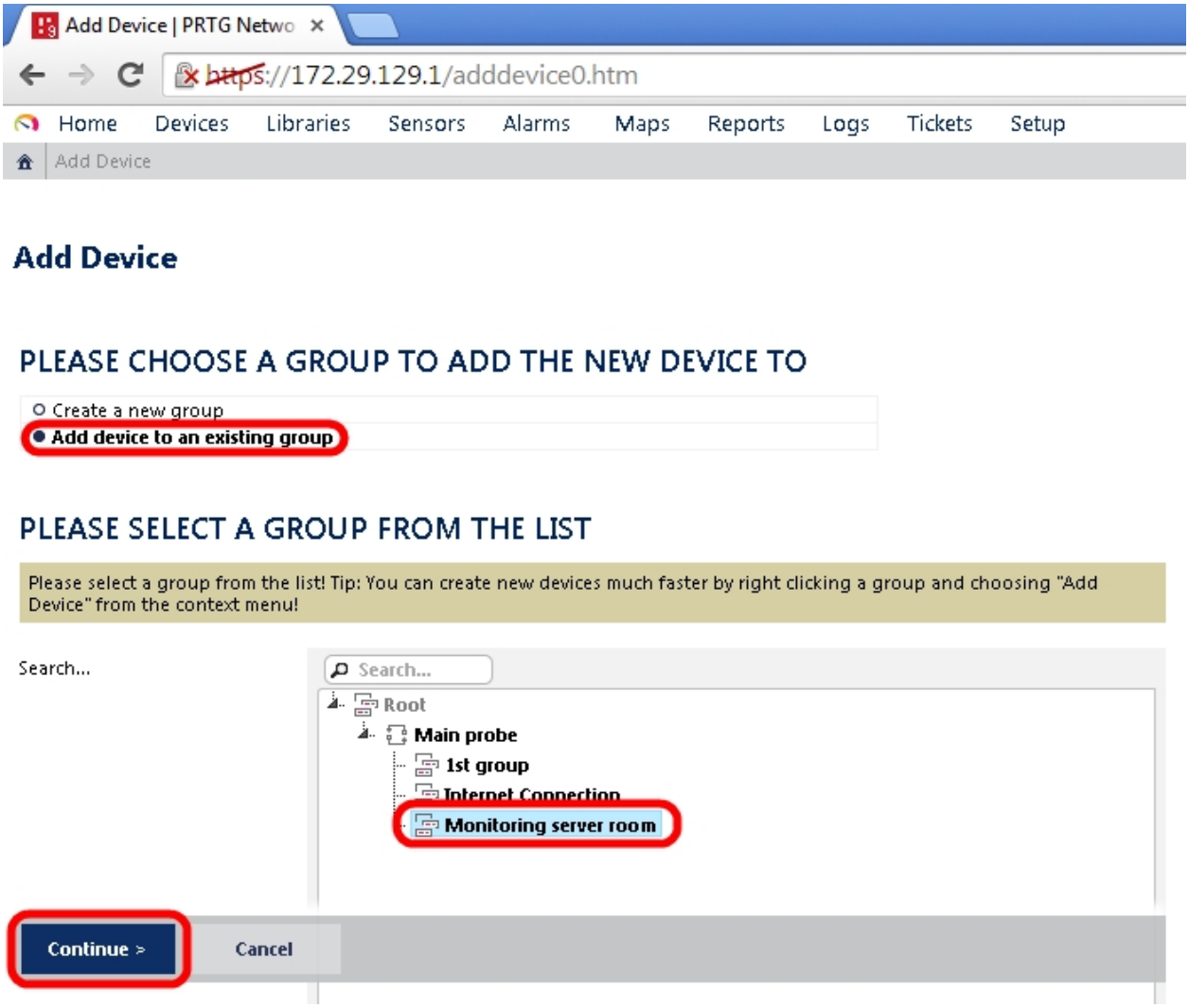


Рисунок В.14 - Параметр «Add device to an existing group»

Важливо: в даному прикладі показана настройка додавання нового пристрою від облікового запису PRTG System Administrator на головній ноді (master node). Для інших облікових записів, інтерфейсів або нод не всі зазначені в описі параметри можуть бути доступні.

На другому етапі на сторінці «Add Device to Group Monitoring server room» заповнити основні параметри, виділені червоним кольором (див. рисунок В.15):

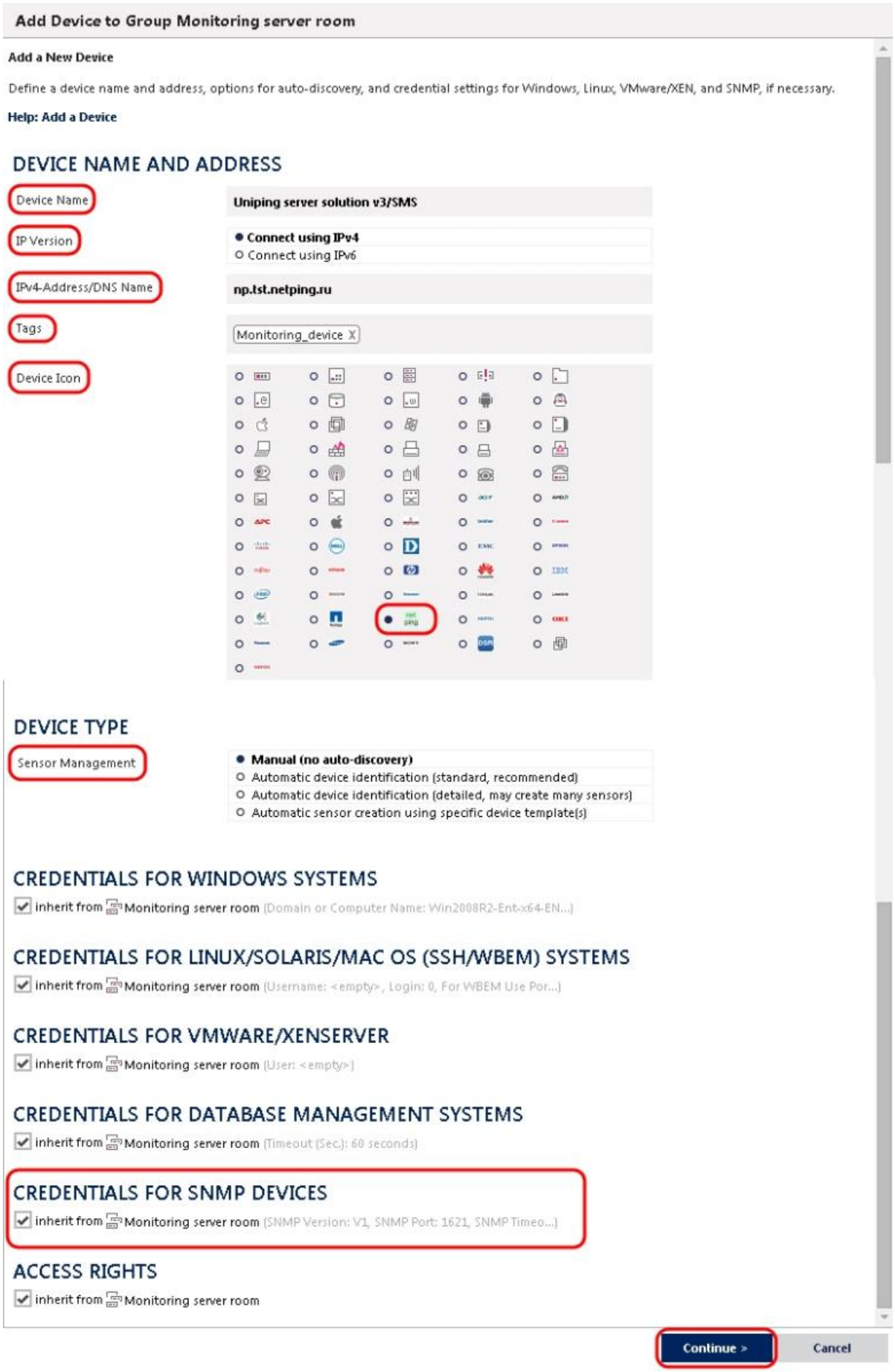


Рисунок В.15 - Сторінка «Add Device to Group Monitoring server room», заповнення основних параметрів

де:

Device Name - ім'я для ідентифікації пристрою. Ім'я буде відображатися за замовчуванням в дереві пристроїв і у всіх повідомленнях про помилки.

IP Version - вибір версії IP протоколу для підключення до нового пристрою.

IPv4-Address / DNSName - IP-адреса або DNS-ім'я нового пристрою.

Tags - теги групують об'єкти в системі PRTG, а також дозволяють їх фільтрувати по цікавого функціоналу.

Device Icon - вибір значка для пристрою зі списку. Значок буде відображатися в дереві пристроїв. При необхідності можна додати власний значок. Для цього файл значка потрібно покласти в папку шляхом: C: \ Program Files (x86) \ PRTG Network Monitor \ webroot \ icons \ devices \

Sensor Management - вибір типу виявлення пристрою. В даному прикладі буде розглянуто ручний режим додавання без автоматичного виявлення пристрою. Для більш детального вивчення режимів автоматичного виявлення і додаткових налаштувань рекомендуємо звернутися до статті «PRTG Manual: Add a Device» за адресою http://www.paessler.com/manuals/prtg/add_a_device.

Credentials for SNMP devices - дані для підключення до пристроїв для моніторингу і управління по протоколу SNMP. У прикладі параметри успадковуються від групи «Monitoring server room». Якщо необхідно вказати параметри, відмінні від успадкованих, необхідно зняти галочку «inherit from Monitoring server room».

Після натискання кнопки «Continue>» пристрій UniPing server solution v3 / SMS буде додано на сторінку «Group Root» (див. рисунок В.16).

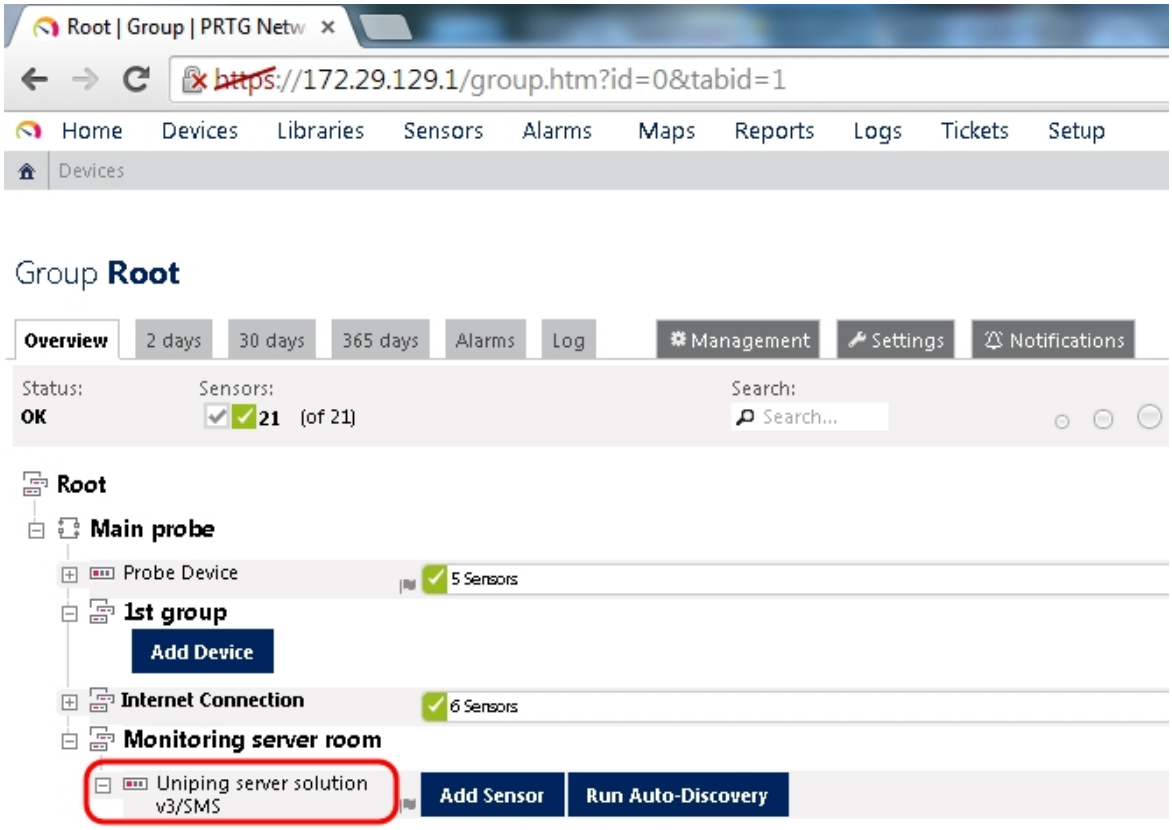


Рисунок В.16 - Пристрій UniPing server solution v3 / SMS буде додано на сторінку «Group Root»

Інформація щодо подальших необхідних налаштування дій та повідомлень, а також результатів моніторингу наведено: сайт http://www.netping.ru/Blog/primer-monitoringa-servernoj-komnaty-na-osnove-prtg-i-ustrojstv-netping

ДОДАТОК Г

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ KISMET

Встановлення Kismet

It is **strongly** recommended that Kismet never be run as root; instead use the Kismet suid-root installation method; when compiling from source it can be installed via: Установка Kismet.

Настійно рекомендується ніколи не запускати Kismet від імені root; замість цього використовуйте метод установки Kismet suid-root; при компіляції з вихідного коду він може бути встановлений через:

```
$ ./configure
$ make
$ sudo make suidinstall
```

Майже всі пакети Kismet також повинні підтримувати метод встановлення suid-root.

Це створить нову групу kismet і встановить інструменти захоплення, які потребують кореневого доступу як suid-root, але можуть бути запущені тільки користувачами в групі kismet.

Це дозволить будь-якому члену групи Kismet змінювати конфігурацію бездротових інтерфейсів в системі, але не дозволить Kismet працювати від імені root.

Запуск Kismet.

Kismet може бути запущений нормально з командного рядка і буде працювати в невеликій оболонці на основі ncurses, яка покаже самий останній висновок сервера і перенаправлення на веб-інтерфейс.

Kismet також може бути запущений як сервіс; зазвичай в цьому випадку ви також повинні передати --no-ncurses, щоб запобігти завантаженню оболонки ncurses.

Приклад сценарію systemd знаходиться в каталозі packaging/ systemd / джерела Kismet; якщо ви встановлюєте його з джерела, його можна скопіювати в файл / etc/systemd/system / kismet.service, і пакети повинні автоматично включати цей файл.

При запуску Kismet через systemd ви повинні встановити kismet як suidroot і використовувати systemctl edit kismet.service для установки наступних параметрів:

```
 [Service]
User=your-unprivileged-user
Group=kismet
```

Крім того, при використанні systemd (або будь-якої іншої системи сценаріїв запуску) вам необхідно буде обов'язково налаштувати Kismet для входу в Допустиме місце розташування. За замовчуванням Kismet реєструється в каталозі, з якого він запускається, що навряд чи буде допустимо при запуску з завантажувального скрипта.

Обов'язково поставте log_prefix=... у свій файл kismet_site.conf; наприклад

```
log_prefix=/home/kismet/logs
```

Якщо ви зіткнулися з помилками при запуску Kismet зі сценарію запуску, обов'язково перевірте journalctl -xe або свої системні журнали для отримання додаткової інформації.

Швидке Налаштування

Kismet має безліч конфігураційних ручок і опцій; але для найшвидшого способу змусити основи працювати:

1. Видаліть усі існуючі установки Kismet. Якщо ви встановили Kismet за допомогою пакета зі свого дистрибутива, видаліть його таким же чином; якщо ви скомпілювали його самостійно, обов'язково видаліть його

2. Встановіть залежності. Kismet потребує ряду бібліотек і заголовків розробки для компіляції; вони повинні бути доступні майже у всіх дистрибутивах.

- *Linux Ubuntu/Debian/Kali/Mint*

```
$ sudo apt install build-essential git libmicrohttpd-dev pkg-config zlib1g-dev libnl-3-dev libnl-genl-3-dev libcap-dev libpcap-dev libnm-dev libdw-dev libsqlite3-dev libprotobuf-dev libprotobuf-c-dev protobuf-compiler protobuf-c-compiler libsensors4-dev libusb-1.0-0-dev python3 python3-setuptools python3-protobuf python3-requests python3-numpy python3-serial python3-usb python3-dev librtlsdr0 libubertooth-dev libbtbb-dev
```

У деяких старих дистрибутивах libprotobuf-c-dev може називатися libprotobuf-c0-dev.

Для підтримки rtlsdr rtl_433 вам також знадобиться інструмент rtl_433 від https://github.com/merbanan/rtl_433 якщо інше не передбачено вашим дистрибутивом.

- *Linux Fedora (and related)*

```
$ sudo dnf install make automake gcc gcc-c++ kernel-devel git libmicrohttpd-devel pkg-config zlib-devel libnl3-devel libcap-devel libpcap-devel NetworkManager-libnm-devel libdwarf libdwarf-devel elfutils-devel libsqlite3x-devel protobuf-devel protobuf-c-devel protobuf-compiler protobuf-c-compiler lm_sensors-devel libusb-devel fftw-devel
```

Для OSX потрібен набір інструментів XCode з Apple store. Після установки вам потрібно буде запустити Xcode IDE хоча б один раз, щоб прийняти ліцензію; зробіть це перед використанням інструментів командного рядка.

Вам потрібно буде встановити інструмент brew з brew.sh. існують і інші менеджери пакетів для OSX; не соромтеся використовувати будь-який з них, у якого є необхідні пакети, але Brew, як відомо, працює.

Встановіть необхідні пакети через Brew:

```
% brew install pkg-config python3 libpcap protobuf protobuf-c pcre librtlsdr libbtbb ubertooth libusb
```

Попередження OSX libmicrohttpd в даний час остання версія libmicrohttpd (0.9.71), яка включена в Brew, мабуть, має значну проблему зупинки, яка завадить Kismet працювати належним чином. Це можна тимчасово обійти, переключившись на версію 0.9.63. На жаль, для цього потрібно кілька кроків через обмеження системи brew, які були введені в останніх версіях. Для цього також буде потрібно встановити кілька додаткових бібліотек та інструментів, необхідних для компіляції libmicrohttpd, так як він не зможе встановлюватися з попередньо скомпільованої пляшки.

```
% brew unlink libmicrohttpd
% git -C "/usr/local/Homebrew/Library/Taps/homebrew/homebrew-core" fetch --unshallow
% brew tap-new kismet/libmicrohttpd
% brew extract --version 0.9.63 libmicrohttpd kismet/libmicrohttpd
% brew install kismet/libmicrohttpd/libmicrohttpd@0.9.63
```

Клон Кісмет з git. Якщо ви ще не клонували Kismet раніше: Сподіваюся, Що цей обхідний шлях не знадобиться в майбутньому.

Сподіваюся, що цей обхідний шлях не знадобиться в майбутньому.

Якщо ви вже побудували Kismet з версією libmicrohttpd 0.9.71 на OSX, вам доведеться перекомпілювати Kismet.

Клон Кісмет з git. Якщо ви ще не клонували Kismet раніше: я сподіваюся, що цей обхідний шлях не знадобиться в майбутньому.

```
$ git clone https://www.kismetwireless.net/git/kismet.git
```

Якщо у вас вже є repo Kismet:

```
$ cd kismet
$ git pull
```

3. Запустіть configure. Це дозволить знайти всі особливості вашої системи і підготувати Kismet до компіляції. Якщо у вас є які-небудь відсутні залежності або несумісні версії бібліотек, вони з'являться тут.

Компакт-диск $ кісмет

```
$ cd kismet
$ ./configure
```

Зверніть увагу на резюме в кінці і стежте за будь-якими попередженнями! У зведенні будуть показані ключові функції і підняті попередження про відсутні залежності, які різко вплинуть на скомпільований Kismet.

Якщо ви компілюєте лише для платформи віддаленого захоплення, перевірте документи віддаленого захоплення для отримання додаткової інформації.

4. Скомпілюйте Kismet

```
$ make
```

Ви можете прискорити процес, додавши-j #, залежно від того, скільки процесорів у вас є. Для автоматичної компіляції на всіх доступних ядрах:

```
$ make -j$(nproc)
```

C++ використовує досить багато оперативної пам'яті для компіляції, тому в залежності від оперативної пам'яті, доступної у вашій системі, вам може знадобитися обмежити кількість процесів, які ви запускаєте одночасно.

5. Встановіть Kismet. Як правило, ви повинні встановити Kismet як suid-root; Kismet автоматично додасть групу і встановить двійкові файли захоплення відповідно.

При установці suid-root Kismet запустить двійкові файли, які керують каналами і інтерфейсами з необхідними привілеями, але збереже декодування пакетів і веб-інтерфейс без привілеїв root.

```
$ sudo make suidinstall
```

6. Додайте свого користувача до групи kismet (Linux)

```
$ sudo usermod -aG kismet $USER
```

Це дозволить додати поточного користувача, який увійшов в систему на kismet групу.

В OSX, Kismet встановлюється в групі staff, частиною якої є користувач за замовчуванням.

7. Вийдіть з системи і ввійдіть назад. Linux не оновлює групи до тих пір, поки ви не ввійдете в систему; якщо ви тільки що додали себе до групи Kismet, вам доведеться повторно увійти в систему.

8. Переконайтеся, що ви перебуваєте в групі Kismet:

```
$ groups
```

Якщо ви не входите в групу kismet, Вам слід повністю вийти з системи або перезавантажитися.

9. Тепер ви готові запустити Kismet! Наведіть його на свій мережевий інтерфейс... різні дистрибутиви (і версії ядра, і версії дистрибутива) називають інтерфейси по-різному; ваш інтерфейс може бути wlan0 або wlan1, або він може бути названий якось на зразок wlp0s1, або він може бути названий з використанням MAC-адреси карти і виглядати як wlx00c0ca8d7f2e.

Тепер ви можете запустити Kismet на Linux з чимось на зразок:

```
$ kismet -c wlan0
```

або на OSX:

```
$ kismet -c en1
```

або ж ви можете просто запустити Kismet, а потім використовувати новий веб-інтерфейс для вибору карти, яку ви хочете використовувати, просто запустивши її:

```
$ kismet
```

Ім'я вашого інтерфейсу буде відрізнятися залежно від вашого ядра, дистрибутива тощо; якщо ви сумніваєтеся, запустіть Kismet без певних джерел і виберіть один з варіантів "Джерела даних" у верхньому лівому меню веб-інтерфейсу.

Пам'ятайте, що до тих пір, поки ви не додасте джерело даних, Kismet не буде захоплювати ніяких пакетів!

При першому запуску KISMET ви повинні зайти в Kismet WebUI і встановити свій логін і пароль.

Цей логін буде збережений в конфігураційному файлі:~/.kismet/kismet_httpd.conf, який знаходиться в домашньому каталозі користувача, що запускає Kismet при установці в режимі suidroot. Це найкращий спосіб запуску Kismet.

Якщо ви запустите Kismet як або через sudo (або через скрипт запуску системи, де він працює від імені root), то він буде знаходитися в кореневому домашньому каталозі: /root/.kismet/kismet_httpd.conf

1. У браузері http://localhost:2501 (або Адреса сервера Кісмет працює на)

Якщо ви використовуєте Kismet на своєму ноутбуці (або іншій системі з браузером), ви можете побачити користувальницький інтерфейс Kismet за адресою http://localhost:2501-да.

Якщо ви використовуєте Kismet на Raspberry Pi, Wi-Fi Pineapple або іншому пристрої, вам потрібно буде вказати свій комп'ютер на адресу пристрою, на якому працює Kismet. Вам потрібно буде підключити систему під керуванням Kismet до дротового Ethernet, або їй потрібна друга карта Wi-Fi, налаштована для підключення до вашої мережі: ви не можете запустити Kismet і підключитися до мережі на одній і тій же карті Wi-Fi одночасно.

ДОДАТОК Д

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ WIRESHARK

Значно поглибити розуміння мережевих протоколів можна, якщо побачити їх в дії, поспостерігавши за послідовністю повідомлень, якими обмінюються два елементи протоколу, якщо вникнути в деталі роботи протоколу, змусивши його виконувати певні дії і спостерігати за цими діями і їх результатами. Таке можна здійснити або за допомогою модельованих сценаріїв, або в реальному мережевому середовищі, такому, як Інтернет. У лабораторних роботах цього курсу ви, використовуючи програму Wireshark, будете запускати мережеві додатки з різними сценаріями на вашому комп'ютері (або на комп'ютері, позиченому у друзів; повідомте нам, якщо у вас немає комп'ютера, де можна запустити Wireshark). Ви будете спостерігати, як мережеві протоколи вашого комп'ютера взаємодіють і обмінюються повідомленнями з об'єктами протоколу, що виконується в іншому місці мережі Інтернет. Таким чином, ви і ваш комп'ютер будете невід'ємною частиною цих «живих» лабораторних робіт. Ви будете спостерігати і вчитися на власному досвіді.

У цій першій лабораторній роботі ви познайомитеся з програмою Wireshark і виконаєте кілька простих дій по захопленню пакетів і спостереженню за ними. Основний інструмент для спостереження за повідомленнями, якими обмінюються елементи виконуваного протоколу, називається аналізатор пакетів (або сніффер). Як випливає з назви, він аналізує (перехоплює) повідомлення, які надсилаються або отримуються вашим комп'ютером; він також зазвичай зберігає та/або відображає вміст різних полів протоколу цих перехоплених повідомлень. Аналізатор пакетів є пасивною програмою. Він тільки стежить за повідомленнями, відправленими і отриманими додатками і протоколами, запущеними на вашому комп'ютері, але сам ніколи не відправляє пакети. Отримані пакети теж ніколи явно не адресуються аналізатору. Він просто отримує копію цих пакетів.

На рис. 1 показана структура аналізатора пакетів. У правій частині рис.1 знаходяться протоколи (в даному випадку, інтернет-протоколи) і додатки (наприклад, веб-браузер або FTP-клієнт), які зазвичай працюють на вашому комп'ютері. Аналізатор пакетів (в пунктирному прямокутнику) є доповненням до звичайного програмного забезпечення вашого комп'ютера і складається з двох частин.

Бібліотека захоплення пакетів отримує копію кожного кадру канального рівня, який відправляється або отримується комп'ютером. Згадаймо, що повідомлення, якими обмінюються протоколи більш високого рівня, такі як HTTP, FTP, TCP, UDP, DNS або IP, в кінцевому рахунку, укладені в кадри канального рівня, які передаються через фізичний носій, такий, як кабель Ethernet. На рисунку Д.1 показано припущення, що фізичним носієм є Ethernet, і тому всі протоколи верхніх рівнів, в кінцевому рахунку, інкапсулюються в кадр Ethernet. Захоплення всіх кадрів канального рівня, таким чином, дає всі повідомлення, відправлені/отримані всіма протоколами і додатками, що виконуються на вашому комп'ютері.

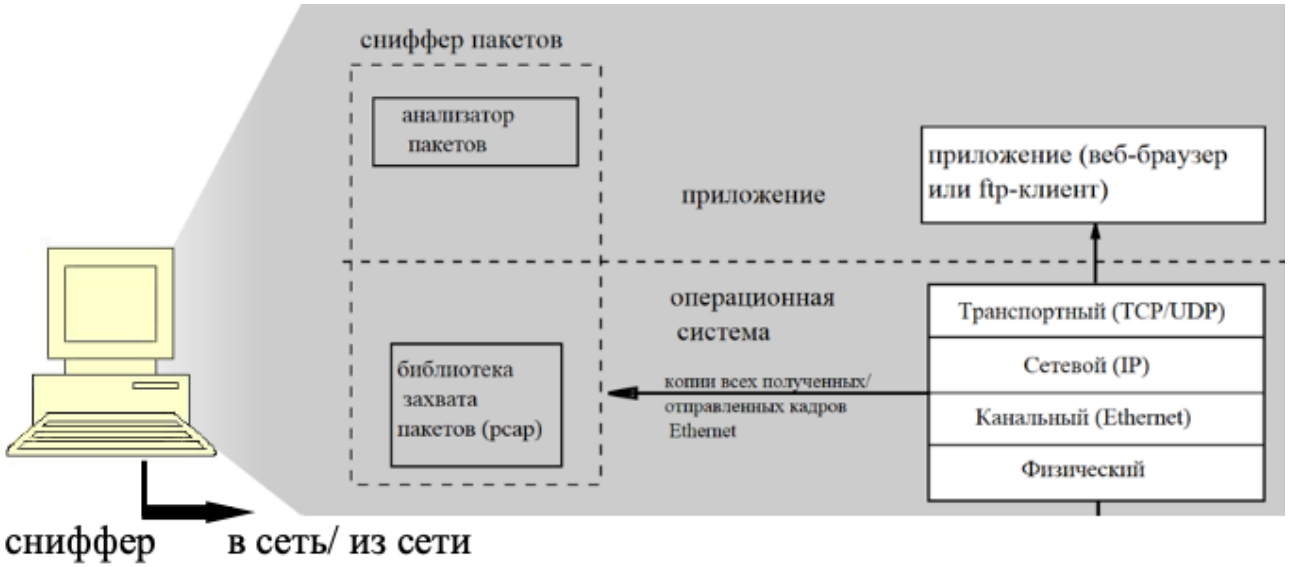


Рисунок Д.1 - Структура аналізатора пакетів

Другим компонентом є аналізатор пакетів, який відображає вміст усіх полів у протокольному повідомленні. Щоб зробити це, аналізатор пакетів повинен "розуміти" структуру всіх повідомлень, якими обмінюються протоколи. Наприклад, припустимо, що ми хочемо відобразити різні поля в повідомленнях, якими обмінюється протокол HTTP на рисунку Д.2. Аналізатор пакетів розуміє формат Ethernet-кадрів, і тому може ідентифікувати IP-дейтаграми всередині кадру Ethernet. Він також розуміє формат IP-дейтаграми, так що він може витягти сегмент TCP з IP - дейтаграми. І, нарешті, він розуміє структуру сегмента TCP, тому він може отримати повідомлення HTTP, що міститься в сегменті TCP. Нарешті, він розуміє протокол HTTP і тому, наприклад, знає, що перші байти повідомлення HTTP будуть містити рядок GET, POST або HEAD, як показано на рисунку Д.3 у тексті.

Ми будемо використовувати аналізатор пакетів Wireshark [wireshark.org] у цих лабораторних роботах, який дозволить нам відображати вміст повідомлень, переданих / отриманих протоколами на різних рівнях стека протоколів. (З технічної точки зору, Wireshark-це аналізатор пакетів, який використовує бібліотеку захоплення пакетів у вашому комп'ютері). Це безкоштовна програма, яка підтримує роботу в операційних системах Windows, Linux / Unix і OS X. Це ідеальний аналізатор для наших лабораторних – він стабільний, має велику базу користувачів і добре документовану підтримку, яка включає в себе керівництво користувача [wireshark.org/docs/wsug_html_chunked/], сторінки електронного посібника [wireshark.org/docs/man-pages/] і докладний список поширених запитань [wireshark.org/faq.html], багатий функціонал, що включає в себе можливість аналізувати сотні протоколів, і добре продуманий інтерфейс користувача. Він працює на комп'ютерах, використовуючи протоколи Ethernet, PPP і SLIP, 802,11 та багато інших технологій канального рівня (якщо середовище, в якому він працює, дозволяє Wireshark це робити).

Завантаження Wireshark

Щоб запустити Wireshark, вам потрібен комп'ютер, який підтримує як Wireshark, так і одну з бібліотек – libpcap або WinPCap. Бібліотека libpcap, якщо вона ще не присутня у вашій операційній системі, встановлюється разом з Wireshark. Список підтримуваних операційних систем представлений на сторінці завантаження [wireshark.org/download.html].

Для завантаження та встановлення Wireshark:

1. Перейдіть за посиланням [wireshark.org/download.html].

2. Завантажте інсталяційний файл для вашої системи та встановіть Wireshark на комп'ютер.

Якщо у вас виникають складнощі з установкою і запуском Wireshark, зверніться до розділу Wireshark FAQ і ви знайдете багато корисної інформації.

Запуск Wireshark

При запуску програми Wireshark, ви побачите головне вікно, як показано нижче:

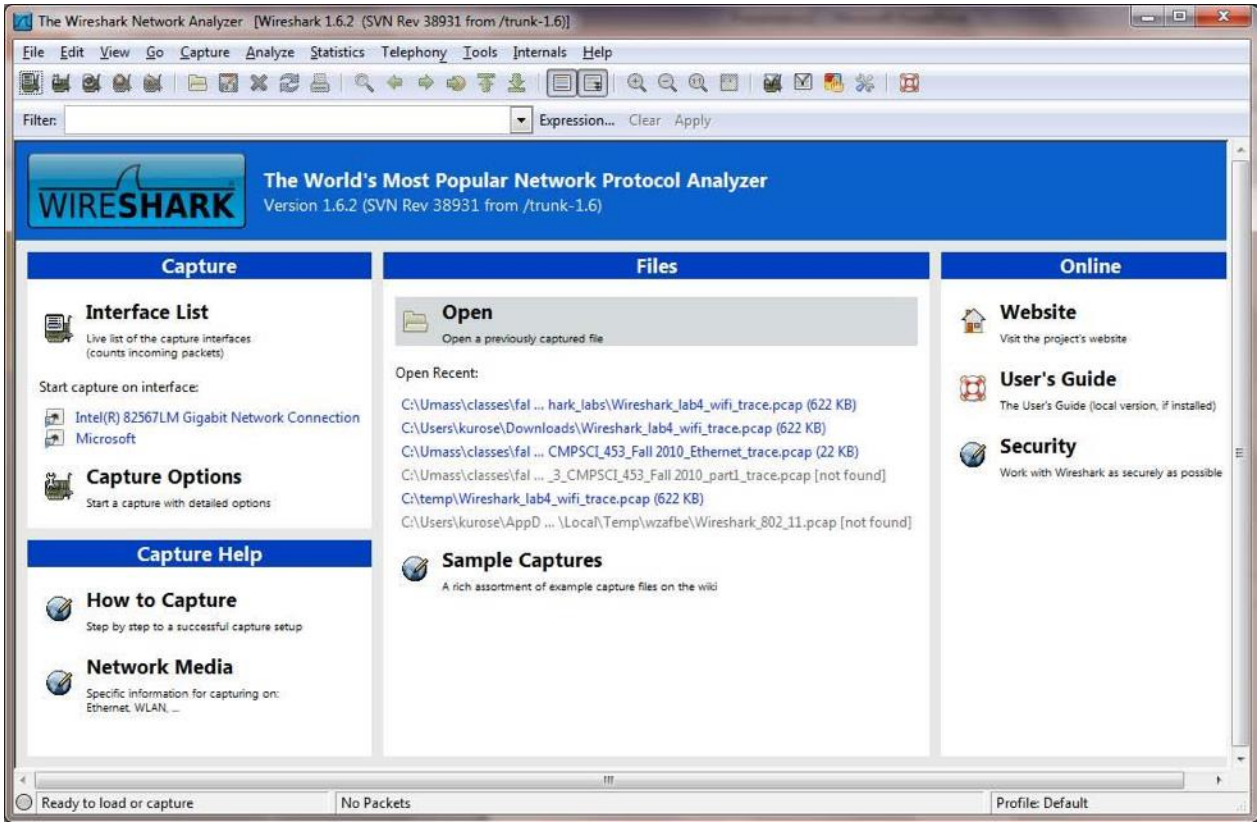


Рисунок Д.2 - Головне вікно програми Wireshark

У лівій верхній частині вікна ви побачите список інтерфейсів (Interface list), в якому представлені всі наявні на вашому комп'ютері мережеві інтерфейси. Після того, як ви виберете інтерфейс, Wireshark буде перехоплювати всі пакети, що проходять через нього. У прикладі вище ми бачимо два інтерфейси: Ethernet-інтерфейс (Gigabit network Connection) і бездротовий інтерфейс (Microsoft).

Якщо ви виберете один з інтерфейсів, щоб почати перехоплення пакетів (тобто дасте команду для Wireshark почати перехоплення пакетів на цьому інтерфейсі), з'явиться вікно (подібне до того, що ви бачите нижче), що показує інформацію про перехоплені пакети. Зупинити захоплення пакетів ви можете, використовуючи команду Stop (Стоп) в меню Capture (Захоплення).

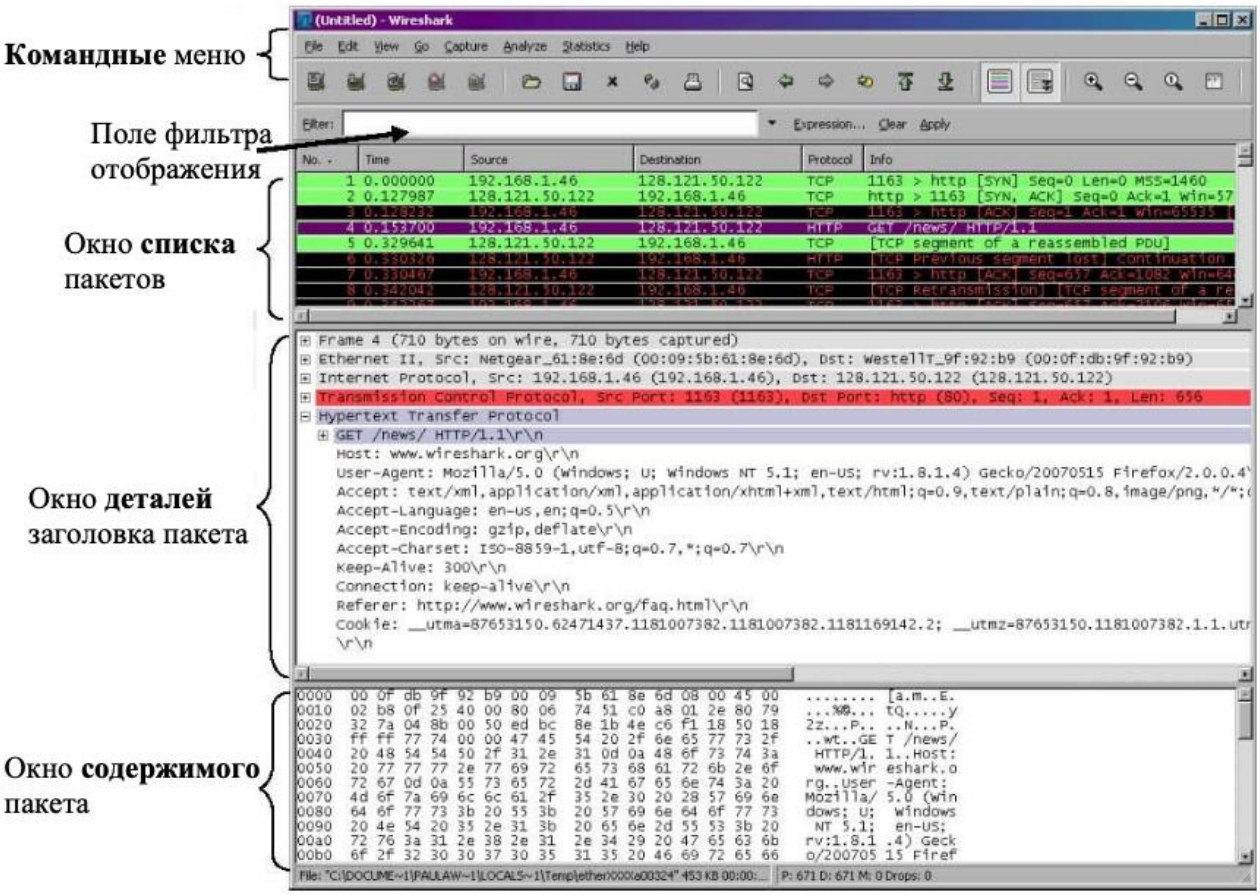


Рисунок Д.3 - Графічний інтерфейс користувача програми Wireshark під час захоплення та аналізу пакетів

Інтерфейс Wireshark містить п'ять основних областей:

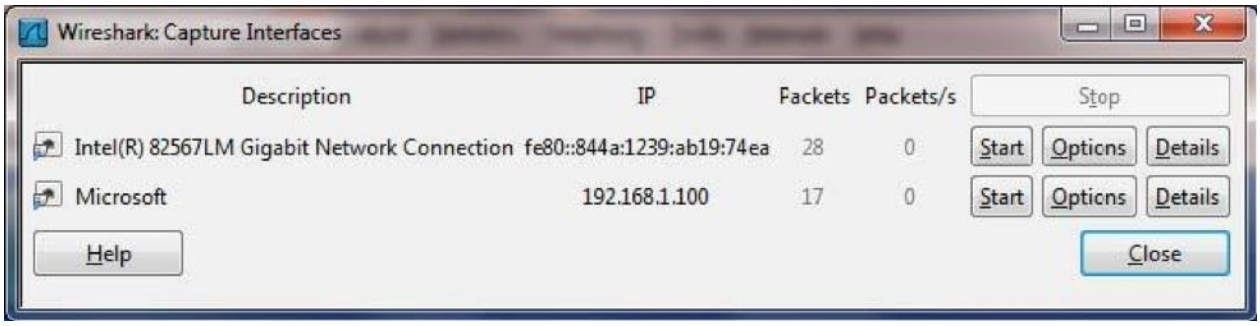
- Командні меню являють собою стандартні спадні меню, розташовані вгорі вікна. Зараз нас цікавлять меню File (Файл) і Capture (Захоплення). Меню File (Файл) призначене для збереження захоплених пакетів, для відкриття файлу з уже збереженими даними пакетів, а також для виходу з програми. Команди в меню Capture (Захоплення) дозволяють почати захоплення пакетів.
- Вікно списку пакетів порядково відображає інформацію по кожному захопленому пакету, включаючи номер пакета (присвоюється тут в програмі, а не міститься ні в якому заголовку) час, коли пакет був перехоплений, адреси джерела і приймача, тип протоколу а також спеціальну інформацію, що відноситься до протоколу. Список пакетів можна відсортувати за будь-яким з цих полів простим натисканням на ім'я відповідного стовпця. У полі тип протоколу відображається верхній рівень протоколу, тобто протокол, який є або вихідним, або кінцевим для конкретного пакета.
- У вікні деталей заголовку пакета відображається докладна інформація про пакет, обраний у попередньому вікні (рядок з цим пакетом підсвічений). (Щоб вибрати пакет у вікні списку, просто наведіть вказівник миші на відповідний рядок і натисніть ліву кнопку миші). Сюди включена інформація про кадр Ethernet (вважаємо, що пакет проходив через інтерфейс Ethernet) і про IP-дейтаграму, що міститься в пакеті. Обсяг інформації, що відображається в цьому вікні можна зменшувати або збільшувати, згортаючи або розгортаючи групу рядків, використовуючи значки плюс мінус зліва в рядку.
- Вікно вмісту пакета відображає все, що міститься в захопленому пакеті, в шістнадцятковому форматі і в форматі ASCII.
- Вгорі графічного вікна користувача, безпосередньо під командним меню знаходиться поле фільтра відображення, в яке може бути введено ім'я протоколу або щось

ще, щоб відфільтрувати інформацію, що відображається у вікні списку пакетів (і, отже, в двох наступних за ним вікнах). У наведеному нижче прикладі, ми будемо використовувати це поле, щоб Wireshark приховав (не відображав) всі пакети, крім тих, які відповідають повідомленням протоколу HTTP.

Пробний запуск Wireshark

Найкращий спосіб для вивчення нового програмного забезпечення – спробувати його в дії! Ми будемо вважати, що ваш комп'ютер підключений до Інтернету через провідний інтерфейс Ethernet. Ми рекомендуємо вам для першої лабораторної роботи використовувати саме Ethernet-з'єднання, а не бездротовий зв'язок. Виконайте наступне:

1. Запустіть ваш улюблений браузер, і в ньому відкриється домашня сторінка.
2. Запустіть програму Wireshark. Ви побачите початкове вікно, показане на рис.2. Програма ще не почала захоплювати пакети. Щоб почати роботу, виберіть в меню Capture (Захоплення) команду Interfaces (Інтерфейси). Відкриється вікно Wireshark: Capture Interfaces (Wireshark: Інтерфейси для захоплення), показане на рисунку Д.4.



Рисунку Д.4 - Вікно вибору інтерфейсу Wireshark: Capture Interfaces

Ви побачите список всіх інтерфейсів вашого комп'ютера, а також поточне число пакетів, що пройшли через інтерфейси. Натисніть кнопку Start (Запуск) поруч з тим інтерфейсом, який хочете аналізувати (в нашому випадку Gigabit Network Connection). Почнеться захоплення пакетів – програма Wireshark тепер перехоплює всі пакети, отримані або відправлені вашим комп'ютером!

Як тільки ви почнете захоплення пакетів, з'явиться вікно, подібне показаному на рис. 3. В ньому відображаються перехоплені пакети. Вибравши в меню Capture (Захоплення) команду Stop (Стоп), ви можете зупинити захоплення пакетів. Але не зупиняйте поки процес. Давайте перехопимо що-небудь цікаве. Щоб зробити це, ми повинні будемо відтворити мережевий трафік. Скористаємося веб-браузером, який використовує протокол HTTP, який ми будемо детально вивчати, щоб завантажити контент з веб-сайту.

Не завершуючи роботу Wireshark, введіть в браузері адресу [http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html].

Після того, як ваш браузер відобразив сторінку INTRO-wireshark-file1.html (рядок з поздоровленням), зупиніть захоплення пакетів, вибравши в меню Capture (Захоплення) команду Stop (Стоп). Вікно Wireshark тепер має виглядати так само, як показано на рис. 3. Тепер у вас є реальні дані по пакетам, якими обмінювався ваш комп'ютер з іншим об'єктом мережі! HTTP-повідомлення обміну з веб-сервером gaia.cs.umass.edu повинні бути десь у списку захоплених пакетів. Але там присутній також безліч інших типів пакетів (бачите різні типи в поле Protocol (Протокол). Навіть якщо крім завантаження веб-сторінки ви більше нічого не робили, все одно на вашому комп'ютері працює безліч інших протоколів, прихованих від очей. Ми поговоримо про них пізніше, а поки потрібно просто пам'ятати, що в мережі відбувається завжди набагато більше подій, ніж помітно!

Для того щоб відобразити сторінку, ваш браузер зв'язується з HTTP-сервером за адресою gaia.cs.umass.edu і обмінюється HTTP-повідомленнями з сервером, щоб

завантажити цю сторінку. Кадри Ethernet, що містять ці http-повідомлення (а також всі інші кадри, що проходять через адаптер Ethernet) будуть перехоплені програмою Wireshark.

3. Вкажіть значення http (всі імена протоколів в Wireshark пишуться в нижньому регістрі) в поле фільтра відображення. Потім натисніть кнопку Apply (Застосувати) (праворуч від цього поля). Це призведе до того, що у вікні списку пакетів відображатимуться лише HTTP-повідомлення.

4. Знайдіть повідомлення GET протоколу HTTP, відправлене з вашого комп'ютера на HTTP-сервер [gaia.cs.umass.edu] (шукайте його у вікні списку захоплених пакетів (див. рис. 3)), що містить також введену вами адресу [gaia.cs.umass.edu]. Коли ви виділите знайдений рядок з повідомленням HTTP GET, то у вікні деталей заголовків з'явиться інформація по заголовках кадру Ethernet, IP-дейтаграм, сегмента TCP і повідомлення HTTP 2. Користуючись кнопками + і - в лівій частині вікна, ви можете за бажанням згортати або розгортати рядки. Згорніть, наприклад, інформацію про кадр і протоколи Ethernet, IP і TCP, а розгорнутою залиште ту, що відноситься до протоколу HTTP. Тепер вікно вашої програми Wireshark має виглядати приблизно так, як показано на рисунку Д.5.

5. Завершіть роботу Wireshark.

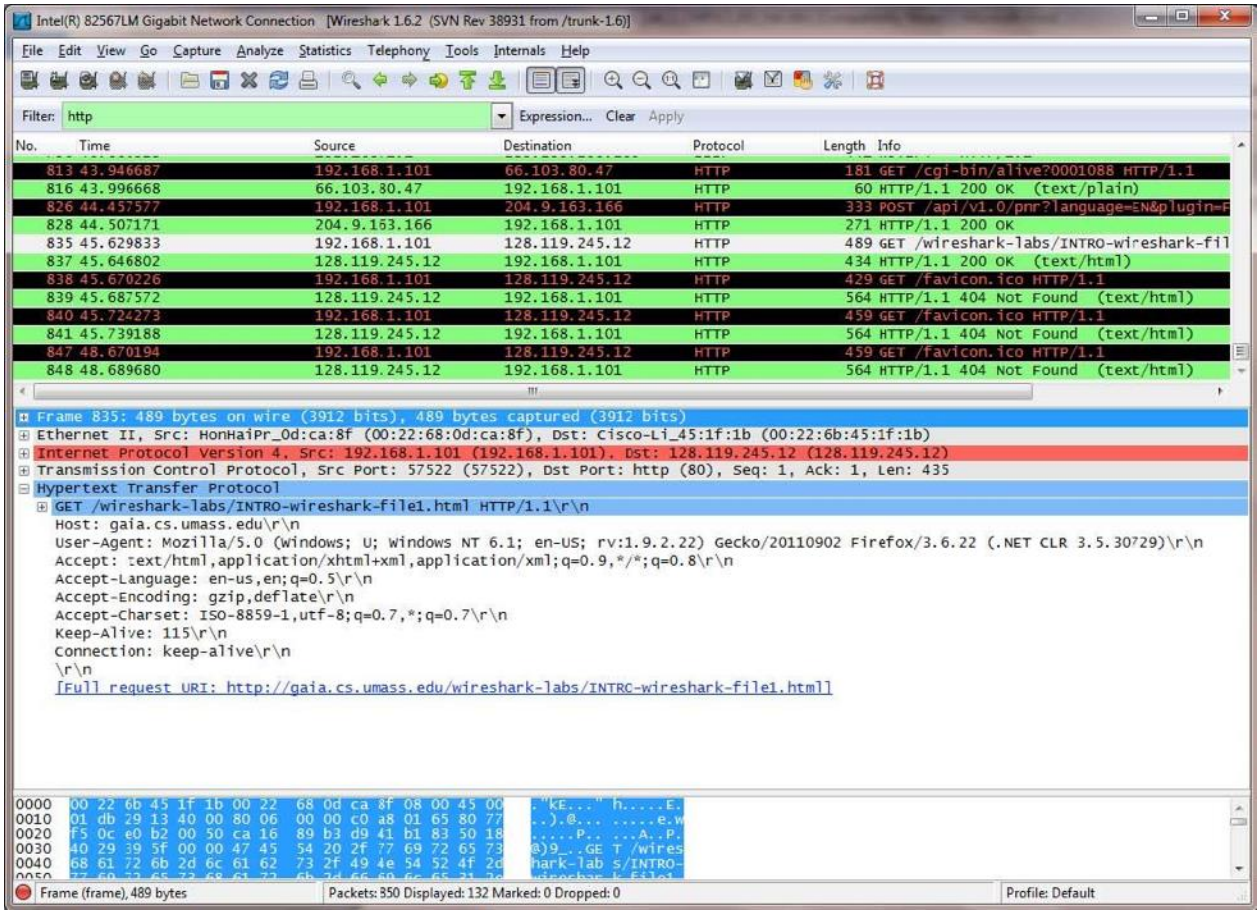


Рисунок Д.5 - Вікно програми Wireshark після кроку 4

ДОДАТОК Е

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ NeDi

Інструкція по установці

Сайт NeDi надає всю необхідну інформацію для успішної установки. Загальна процедура з деякими посиланнями на зовнішню документацію:

http://www.nedi.ch/installation

Специфічна інформація для ОС:

http://www.nedi.ch/installation/freebsd

http://www.nedi.ch/installation/os-x

http://www.nedi.ch/installation/suse-installation

ДОДАТОК Ж

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ ZABBIX

Встановлення Zabbix. 8:00:10

1. Скопіюйте з [flash] і встановіть додаток: VMware-player-5.0.1-894247.exe
2. Скопіюйте з [flash] і розпакуйте архів готового рішення Zabbix_2.0_x86_64.x86_64-2.0.9.vmx.tar, наприклад, за допомогою 7-Zip.
3. Запустіть програму VMware player.
4. Відкрийте в VMware player готове рішення zabbix.

Готове рішення Zabbix засноване на Linux OpenSUSE. Образ містить налаштований Zabbix сервер, що працює з базою даних MySQL, також доступний і веб-інтерфейс.

Встановлене готове рішення Zabbix має наступні паролі:

Система:

root:zabbix

zabbix:zabbix

База даних:

root:zabbix

zabbix:zabbix

Веб-інтерфейс Zabbix:

Admin:zabbix

5. Після завантаження системи введіть в поле login: zabbix, в поле password zabbix – рисунки Ж1 і Ж.2.

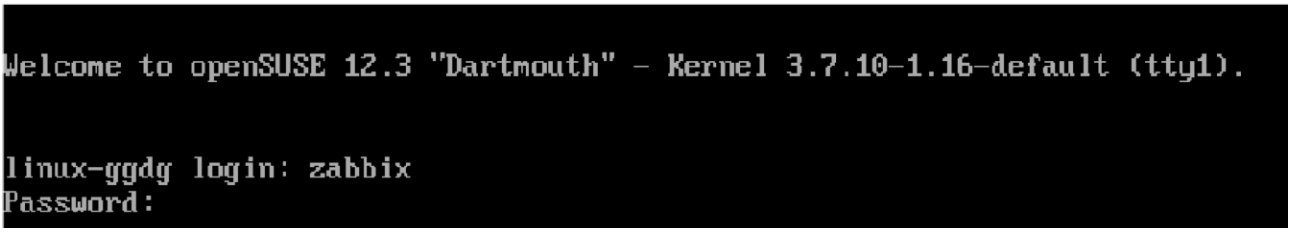


Рисунок Ж.1 - Вхід в систему

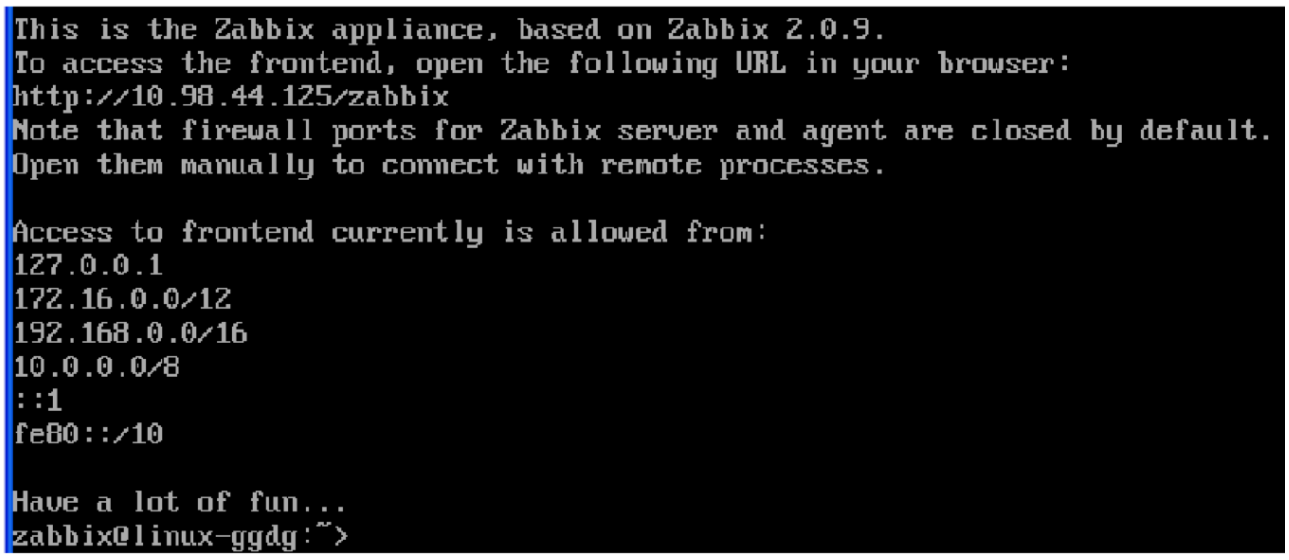


Рисунок Ж.2 - Вхід в систему

6. Увійдіть в систему як root: у командному рядку введіть su на запит Password введіть zabbix.

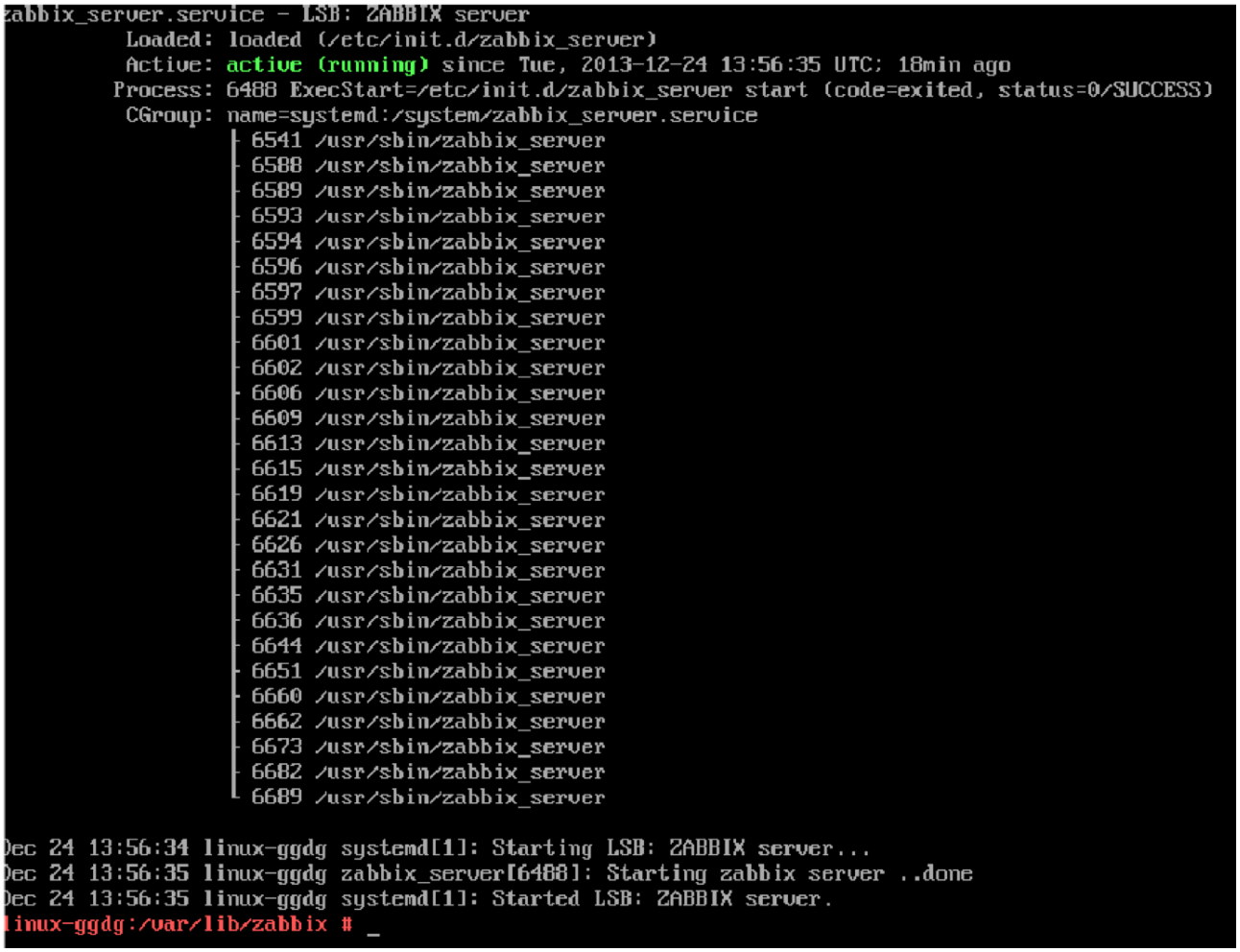


Рисунок Ж.3 - Перевірка сервера

7. Перевірте роботу Zabbix-сервера (див. рисунок Ж.3) у командному рядку введіть:

service zabbix_server status

У представленій конфігурації Zabbix сервер спостерігає за деякими базовими параметрами самого себе за допомогою локально встановленого агента.

7. Перевірте роботу Zabbix-сервера див. рисунок Ж.4) у командному рядку введіть:

service zabbix_agentd status

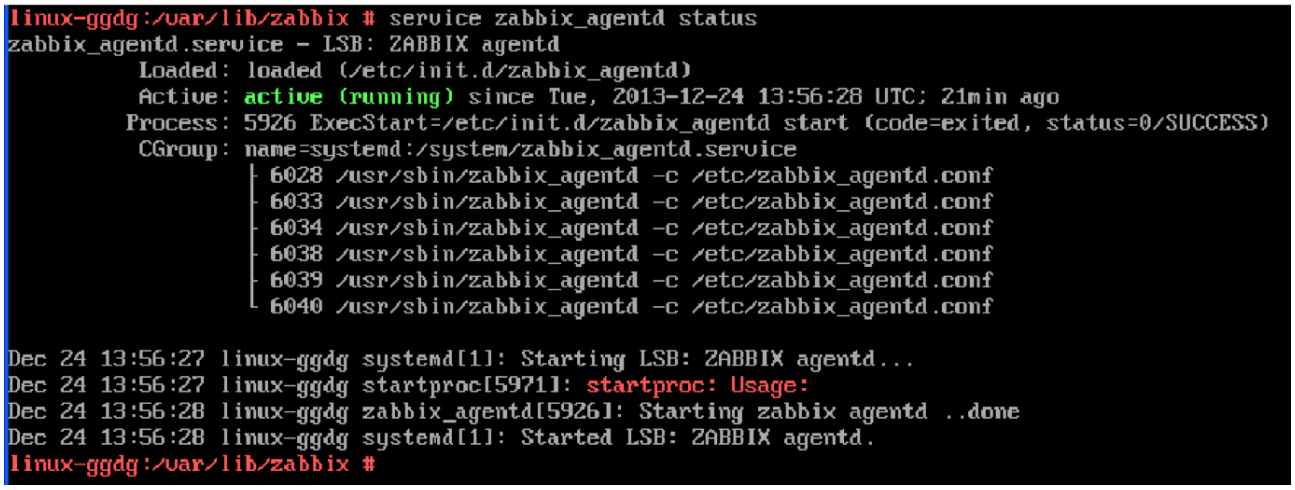


Рисунок Ж.4 - Перевірка агента

Для більш простого доступу Zabbix з будь-якого місця і з будь-якої платформи, поставляється веб-інтерфейс. Для доступу до веб-інтерфейсу треба знати ip-адресу.

8. Подивіться призначену серверу ip-адресу (рис. Д.7.5): у командному рядку введіть команду ifconfig

На рисунку Ж.5 це адреса 10.98.44.125. У вас буде інша адреса.

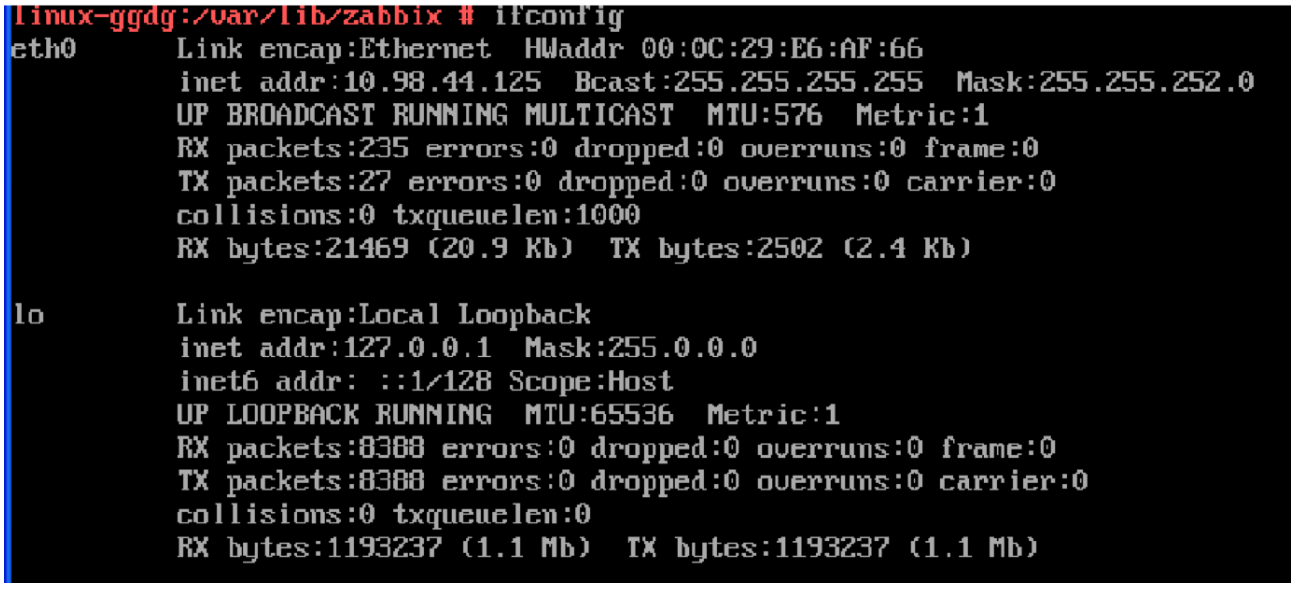


Рисунок Ж.5 - Перевірка ip-адреси

9. Відкрийте веб-інтерфейс Zabbix-а: для цього запустіть браузер і в адресному рядку введіть: http://10.98.44.125/zabbix

Де замість 10.98.44.125 призначена вашій віртуальній системі ip-адреса (див. рисунок Ж.5).

10. Це екран "Привітання" в Zabbix (див. рисунок Ж.6). Введіть Ім'я користувача Admin з паролем zabbix для входу під Супер-Адміністратором Zabbix.

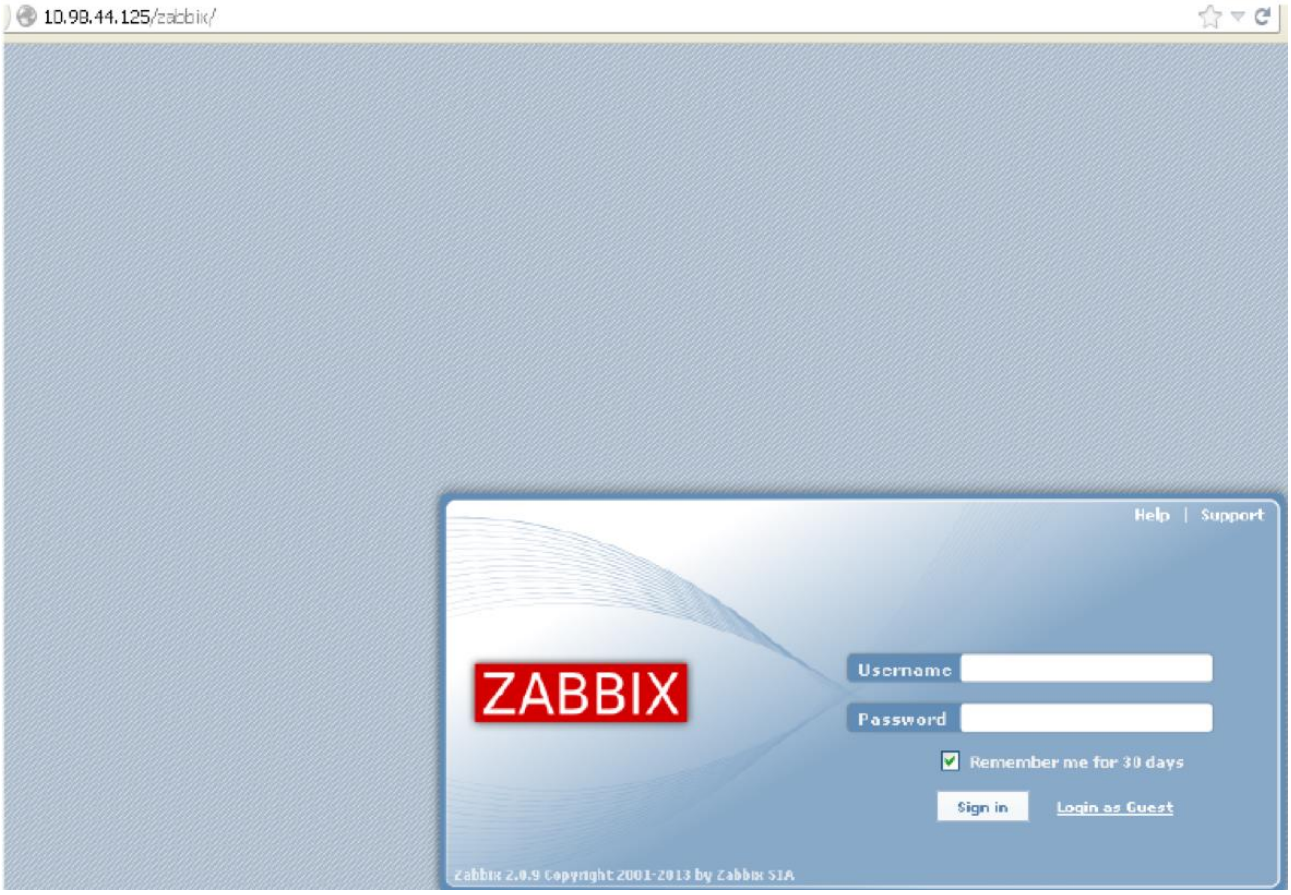


Рисунок Ж.6 - Привітання

11. Встановіть мову: у правому куті виберіть profile, у списку language виберіть Russian, натисніть Save.

12. Виберіть Моніторинг, Панель. Зробіть знімок екрана (див. рисунок Ж.7).

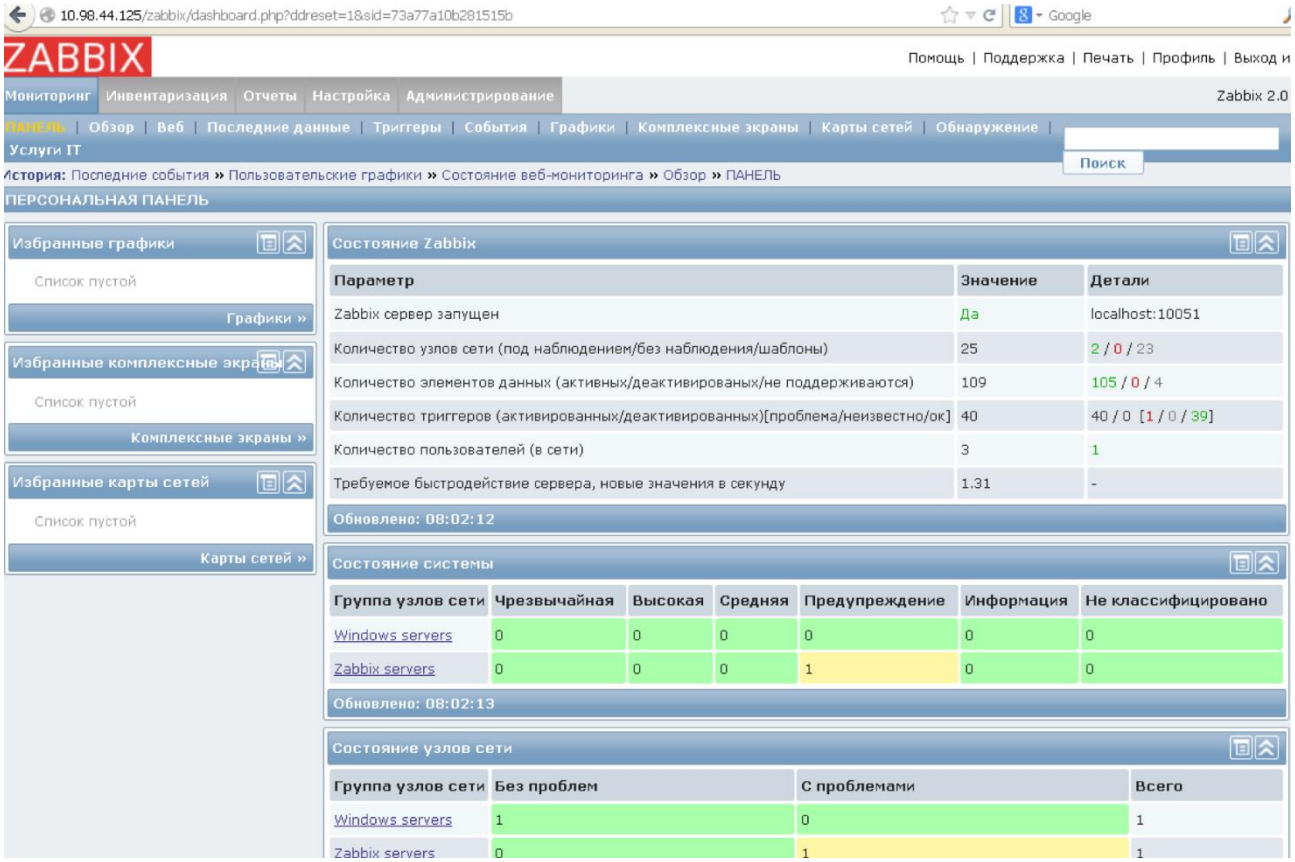


Рисунок Ж.7 - Моніторинг, панель

Агент. 9:00:34

Zabbix агенти розгортаються на спостережуваних активних моніторингах локальних ресурсів і додатками (статистика жорстких дисків, пам'яті, процесорів і т.д.).

Агент збирає локальну оперативну інформацію і відправляє дані Zabbix серверу для подальшої обробки. У разі проблем (таких як робочий жорсткий диск заповнений або впав процес сервісу) Zabbix сервер може швидко повідомити адміністраторів конкретного сервера, який сповістив про помилку.

Zabbix агенти безпечні, використовують нативні системні виклики для збору інформації.

Zabbix агенти можуть виконувати пасивні і активні перевірки.

У разі пасивної перевірки агент відповідає на запит даних. Zabbix сервер (або проксі) запитує дані, наприклад, завантаження ЦПУ, і Zabbix повертає результат.

Активні вимоги вимагають більш складної обробки. Агент спочатку список отримує елементи даних для незалежної обробки від Zabbix сервера. Далі він буде періодично відправляти нові значення серверу.

Незалежно від цього моніторингу пасивних або активних перевірок налаштовується вибір відповідного типу елемента даних. Zabbix агент обробляє елементи типу 'Zabbix агент' або 'Zabbix агент (активний)'.

Zabbix агент підтримується на:

Linux
IBM AIX
FreeBSD
NetBSD
OpenBSD
HP-UX
Mac OS X
Солярис

Windows: 2000, Server 2003, XP, Vista, Server 2008, 7

13. Створіть на диску c: вашого комп'ютера (не пропонуйте машини!) Каталог c: / zabbix

14. Скопіюйте [flash] файл zabbix_agentd.exe в каталог c: / zabbix

15. Скопіюйте [flash] конфігураційний файл zabbix_agentd.conf в корінь диска c:

16. Відредагуйте файл c: / zabbix_agentd.conf за нижченаведеним прикладом.

Замість 10.98.44.125 введіть IP-адресу Вашого Zabbix-сервера (пункт 8).

Это файл конфигурации для демона агента Zabbix (Windows)

Чтобы получить дополнительную информацию о Zabbix, перейдите на http://www.zabbix.com

############ ОБЩИЕ ПАРАМЕТРЫ #################

Параметр: LogFile

Имя файла журнала.

Если не установлен, используется журнал событий Windows.

#

Обязательно: нет

По умолчанию:

LogFile =

LogFile = c: \ zabbix_agentd.log

Параметр: LogFileSize

Максимальный размер файла журнала в МБ.

0 - отключить автоматическую ротацию логов.

#

Обязательно: нет

Диапазон: 0-1024

По умолчанию:

LogFileSize = 1

Вариант: DebugLevel

Определяет уровень отладки

0 - без отладки

1 - критическая информация

2 - информация об ошибке

3 - предупреждения

4 - для отладки (выдает много информации)

#

Обязательно: нет

Диапазон: 0-4

По умолчанию:

DebugLevel = 3

Вариант: SourceIP

Исходный IP-адрес для исходящих соединений.

#

Обязательно: нет

По умолчанию:

SourceIP =

Вариант: EnableRemoteCommands

Разрешены ли удаленные команды от Zabbix сервера.

0 - не допускается

1 - разрешено

#

Обязательно: нет

По умолчанию:

EnableRemoteCommands = 0

Вариант: LogRemoteCommands
Включить регистрацию выполненных команд оболочки как предупреждений.
0 - отключен
1 - включен
#
Обязательно: нет
По умолчанию:
LogRemoteCommands = 0
Пассивные проверки, связанные
Вариант: Сервер
Список разделенных запятыми IP-адресов (или имен хостов) Zabbix серверов.
Входящие соединения будут приниматься только от хостов, перечисленных здесь.
Пробелы не допускаются.
Если поддержка IPv6 включена, то '127.0.0.1', ':: 127.0.0.1', ':: ffff: 127.0.0.1' обрабатываются одинаково.
#
Обязательно: нет
По умолчанию:
Сервер =
Сервер = 10.98.44.125
Вариант: ListenPort
Агент будет прослушивать этот порт на предмет подключений с сервера.
#
Обязательно: нет
Диапазон: 1024-32767
По умолчанию:
ListenPort = 10050
Вариант: ListenIP
Список IP-адресов, разделенных запятыми, которые должен прослушивать агент.
Первый IP-адрес отправляется Zabbix серверу при подключении к нему для получения списка активных проверок.
#
Обязательно: нет
По умолчанию:
ListenIP = 0.0.0.0
Вариант: StartAgents
Количество предварительно форкованных экземпляров zabbix_agentd, обрабатывающих пассивные проверки.
Если установлено значение 0, пассивные проверки отключаются, и агент не будет прослушивать ни один TCP-порт.
#
Обязательно: нет
Диапазон: 0-100
По умолчанию:
StartAgents = 3
Активные проверки, связанные
Вариант: ServerActive
Список пар IP: порт (или имя хоста: порт) через запятую Zabbix серверов для активных проверок.
Если порт не указан, используется порт по умолчанию.
Адреса IPv6 должны быть заключены в квадратные скобки, если указан порт для этого хоста.
Если порт не указан, квадратные скобки для адресов IPv6 не обязательны.

Если этот параметр не указан, активные проверки отключены.
Пример: ServerActive = 127.0.0.1: 20051, zabbix.domain, [:: 1]: 30051, :: 1, [12fc :: 1]
#
# Обязательно: нет
# По умолчанию:
# ServerActive =
ServerActive = 10.98.44.125
Вариант: имя хоста
Уникальное имя хоста с учетом регистра.
Требуется для активных проверок и должно соответствовать имени хоста, настроенному на сервере.
Значение получается из HostnameItem, если не определено.
#
Обязательно: нет
По умолчанию:
Имя хоста =
Вариант: HostnameItem
Элемент, используемый для генерации имени хоста, если он не определен.
Игнорируется, если имя хоста определено.
#
# Обязательно: нет
# По умолчанию:
HostnameItem = system.hostname
Вариант: RefreshActiveChecks
Как часто обновляется список активных проверок, в секундах.
#
Обязательно: нет
Диапазон: 60-3600
По умолчанию:
RefreshActiveChecks = 120
Вариант: BufferSend
Не хранить данные в буфере дольше N секунд.
#
Обязательно: нет
Диапазон: 1-3600
По умолчанию:
BufferSend = 5
Параметр: BufferSize
Максимальное количество значений в буфере памяти. Агент пришлет
все собранные данные на Zabbix сервер или прокси, если буфер заполнен.
#
Обязательно: нет
Диапазон: 2-65535
По умолчанию:
BufferSize = 100
Параметр: MaxLinesPerSecond
Максимальное количество новых строк, которые агент будет отправлять в секунду на Zabbix Server
или прокси-серверы обрабатывают активные проверки 'log', 'logrt' и 'eventlog'.
Указанное значение будет заменено параметром maxlines,
предоставляется в ключах элементов 'log', 'logrt' или 'eventlog'.
#
Обязательно: нет

Диапазон: 1-1000
По умолчанию:
MaxLinesPerSecond = 100
############ РАСШИРЕННЫЕ ПАРАМЕТРЫ #################
Вариант: Псевдоним
Устанавливает псевдоним для параметра. Может быть полезно заменить длинное и сложное имя параметра на меньшее и более простое.
Например, если вы хотите получить информацию об использовании файла подкачки в процентах от сервера,
вы можете использовать параметр "perf_counter [\ Paging File (_Total) \% Usage]", или вы можете определить псевдоним, добавив следующую строку в файл конфигурации
Alias = pg_usage: perf_counter [\ Файл подкачки (_Total) \% использования]
После этого вы можете использовать имя параметра "pg_usage" для получения той же информации.
Вы можете указать столько записей «Псевдонимов», сколько захотите.
Псевдонимы не могут использоваться для параметров, определенных в записях файла конфигурации "PerfCounter".
#
Обязательно: нет
Диапазон:
По умолчанию:
Вариант: Тайм-аут
Тратьте на обработку не более Timeout секунд
#
Обязательно: нет
Диапазон: 1-30
По умолчанию:
Тайм-аут = 3
Вариант: PerfCounter
Синтаксис: <имя_параметра>, "<perf_counter_path>", <период>
Определяет новый параметр <имя_параметра>, который является средним значением для системного счетчика производительности <perf_counter_path> за указанный период времени <period> (в секундах).
Например, если вы хотите получать среднее количество прерываний процессора в секунду за последнюю минуту, вы можете определить новый параметр «прерывания» следующим образом:
PerfCounter = прерывания, "\ Processor (0) \ Interrupts / sec", 60
Обратите внимание на двойные кавычки вокруг пути счетчика производительности.
Образцы для расчета среднего значения будут браться каждую секунду.
Вы можете запустить "typeperf -qx", чтобы получить список всех счетчиков производительности, доступных в Windows.
#
Обязательно: нет
Диапазон:
По умолчанию:
Вариант: включить
Вы можете включать отдельные файлы в файл конфигурации.
#
Обязательно: нет
По умолчанию:
Включить =
Включить = c: \ zabbix \ zabbix_agentd.userparams.conf

####### ОПРЕДЕЛЕННЫЕ ПОЛЬЗОВАТЕЛЕМ ПАРАМЕТРЫ МОНИТОРИНГА #######

Параметр: UnsafeUserParameters

Разрешить передачу всех символов в качестве аргументов определяемым пользователем параметрам.

0 - не разрешать

1 - разрешить

#

Обязательно: нет

Диапазон: 0-1

По умолчанию:

UnsafeUserParameters = 0

Параметр: UserParameter

Определяемый пользователем параметр для мониторинга. Может быть несколько параметров, определяемых пользователем.

Формат: UserParameter = <ключ>, <команда оболочки>

#

Обязательно: нет

По умолчанию:

UserParameter =

17. Встановіть як агента сервіс Windows. Введіть

c: \ zabbix \ zabbix_agentd.exe –установить

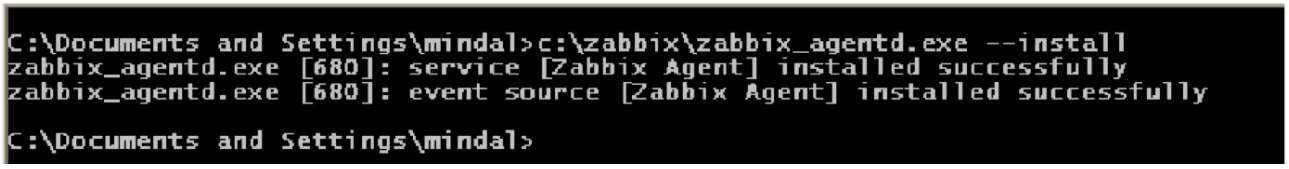


Рисунок Ж.8 - Установка як агента сервіс Windows

18. Зробіть знімок екрана (див. рисунок Ж.8).

19. Тепер ви можете використовувати панель управління для запуску агента як сервісу. Відкрийте Панель управління, Адміністрування, Служби, вибрати Zabbix agent, Запустити

Користувач. 10:01:12

20. Для перегляду інформації про користувачів перейдіть в Адміністрування? Користувачі і виберіть Користувачі в випадаючому меню.

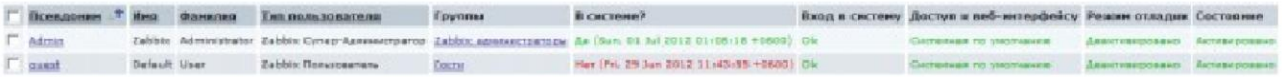


Рисунок Ж.9 - Користувачі

Спочатку в Zabbix тільки два встановлених користувача.

Користувач 'Admin' це суперкористувач Zabbix, який має всі привілеї.

Користувач 'Guest' це спеціальний користувач за замовчуванням. Якщо користувач не увійшов в систему, тоді він отримає доступ з привілеями користувача "guest". За замовчуванням, "guest" не має дозволів на об'єкти Zabbix.

21. Щоб додати нового користувача, натисніть Створити користувача. Введіть свою ПІБ.

22. У діалозі створення користувача переконайтеся, що користувач належить хоча б одній групі користувачів, наприклад 'Мережеві адміністратори'.

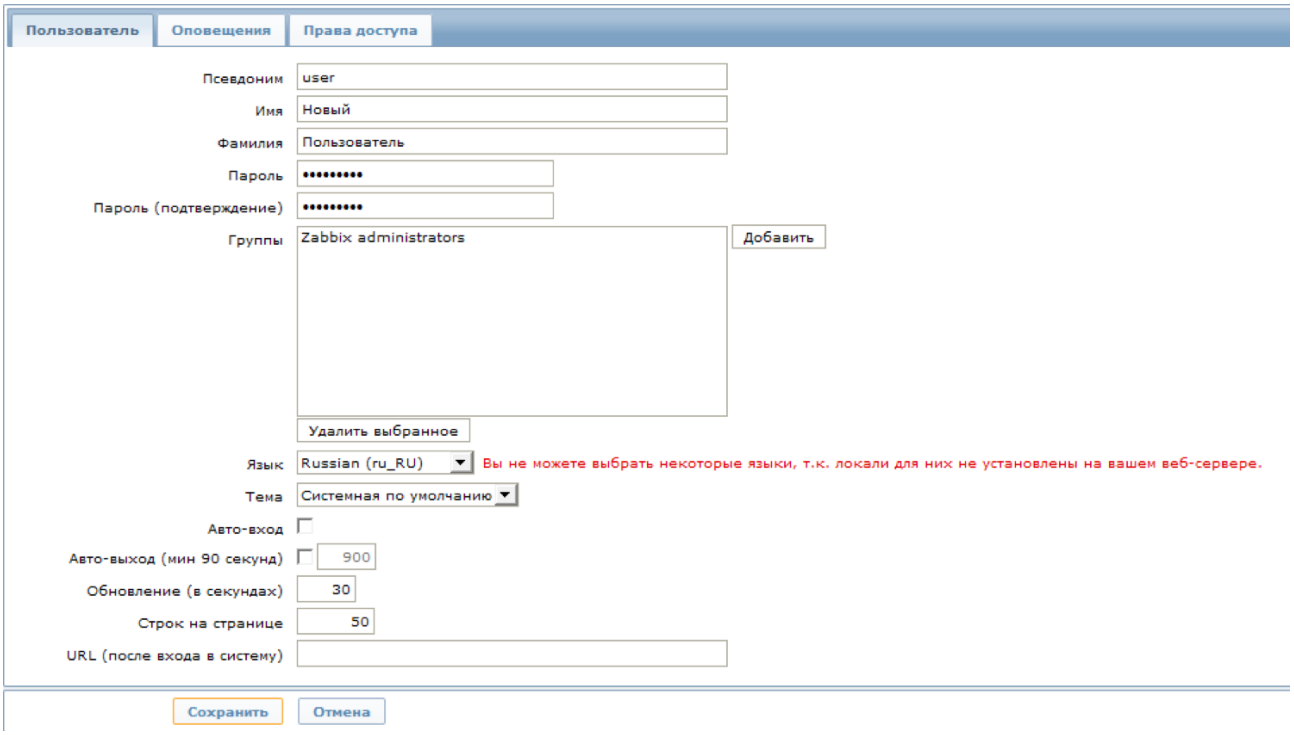


Рисунок Ж.10 - Створення користувача

23. За замовчуванням у нових користувачів немає встановлених способів оповіщення (методів відправки повідомлень). Для створення його перейдіть на закладку 'Способи оповіщення' і натисніть Додати.

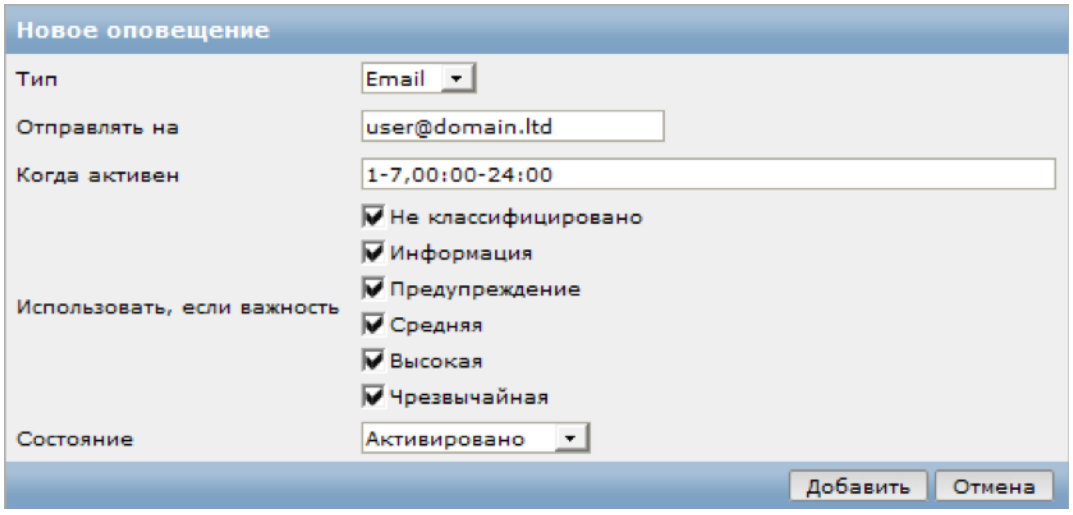


Рисунок Ж.11 - Оповіщення

24. У цьому спливаючому вікні введіть для користувача e-mail адресу.

25. Натисніть Додати, потім Зберегти у властивостях користувача. Новий користувач з'явиться в списку користувачів.

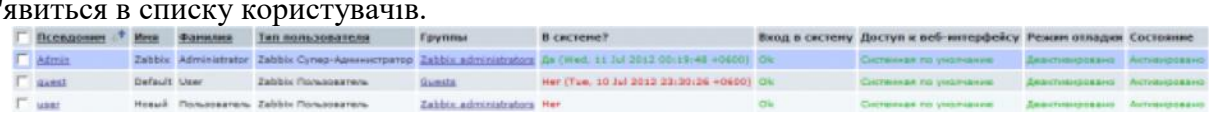


Рисунок Ж.12 - Новий користувач

26. Зробіть знімок екрана.

Додавання прав доступу

За замовчуванням, новий користувач не має прав.

27. Для надання йому прав натисніть на ім'я групи в колонці Групи (в даному випадку - 'Network administrators'). У цій формі властивостей групи перейдіть на закладку Права.

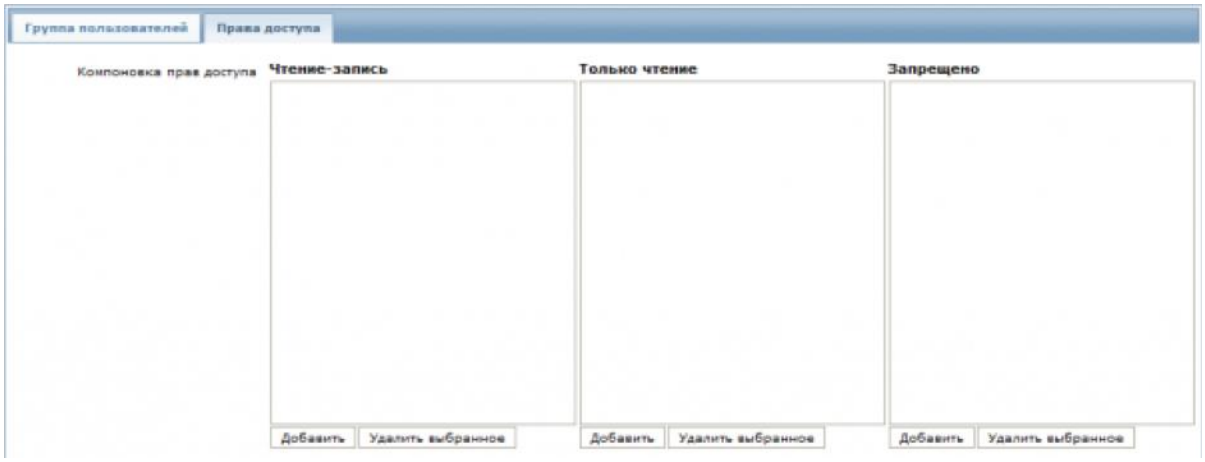


Рисунок Ж.13 - Права

28. Цей користувач повинен мати доступ лише для читання групи Windows servers, тому натисніть Додати нижче блоку значень Тільки читання.

Рисунок Ж.14 - Права

У цьому спливаючому вікні виберіть 'Windows servers' і потім натисніть Вибрати. Windows servers повинні відображатися у відповідному полі. У формі властивостей групи користувачів, натисніть Зберегти.

29. Тепер увійдіть під створеним користувачем.

Новий вузол. 11:05:07

Вузол мережі в Zabbix - є сутністю мережі (фізичної, віртуальної), яку ви хочете спостерігати. Визначення того, що може бути "вузлом мережі" в Zabbix дуже гнучке. Він може бути фізичним сервером, мережевим світчем, віртуальному машиною або яким-небудь додатком.

Додавання вузла мережі

30. Інформація про налаштовані вузли мережі в Zabbix доступна в Налаштування? Вузли мережі. Існує вже один попередньо встановлений вузол мережі, який називається 'Zabbix server', але ми хочемо додати ще один вузол мережі.

31. Щоб додати новий вузол мережі, натисніть Створити. Ця дія покажемо нам форму настройки вузла мережі.

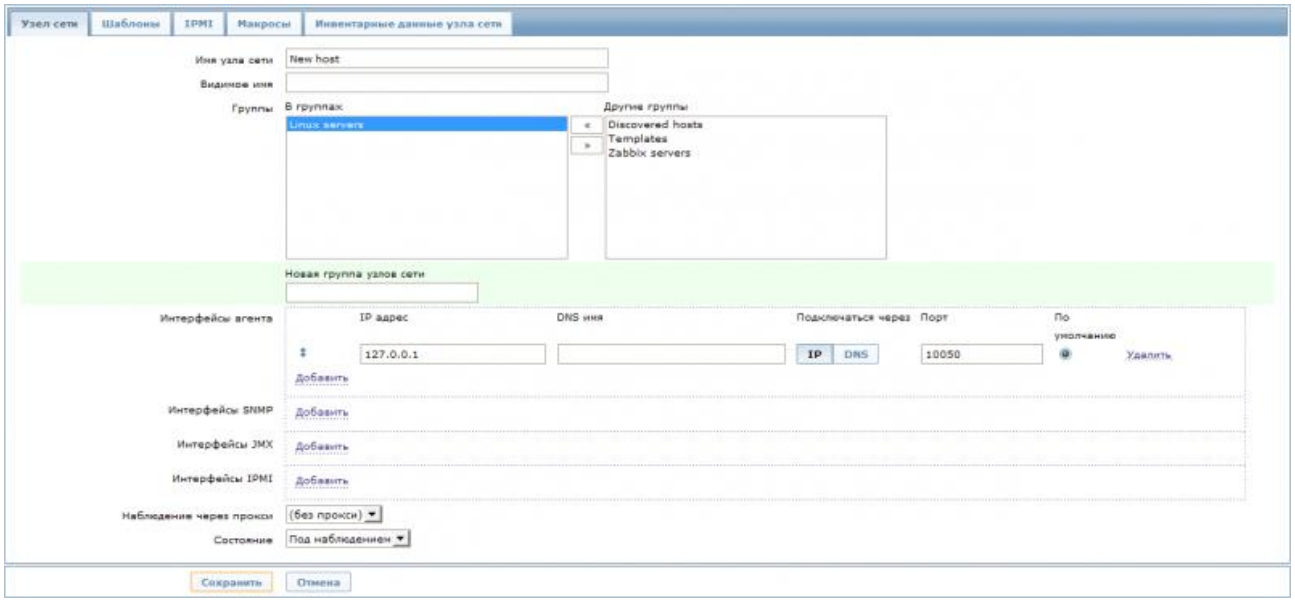


Рисунок Ж.15 - Створення вузла

32. У формі введіть мінімум:

Ім'я вузла мережі

Введіть ім'я вузла мережі. Допускаються число-літерні символи, пробіли і підкреслення, наприклад, GMC

Група

Виберіть одну або кілька груп зі списку праворуч і натисніть", щоб перемістити їх в список 'В групах'. Наприклад, Windows servers

Всі права доступу призначаються на групи вузлів мережі, не індивідуально вузлам мережі. Тому вузол мережі повинен належати хоча б одній групі.

IP адреса

Введіть IP адресу вузла мережі. Наприклад, 19.98.44.122. Чому?

32. У командному рядку вашого комп'ютера (не віртуальної машини!) вводимо команду ipconfig (див. рисунок Ж.16).

```
Настройка протокола IP для Windows

VMware Network Adapter VMnet8 - Ethernet адаптер:

        DNS-суффикс этого подключения . . :
        IP-адрес  . . . . . . . . . . . . : 192.168.86.1
        Маска подсети . . . . . . . . . . : 255.255.255.0
        Основной шлюз . . . . . . . . . . :

VMware Network Adapter VMnet1 - Ethernet адаптер:

        DNS-суффикс этого подключения . . :
        IP-адрес  . . . . . . . . . . . . : 192.168.174.1
        Маска подсети . . . . . . . . . . : 255.255.255.0
        Основной шлюз . . . . . . . . . . :

Подключение по локальной сети - Ethernet адаптер:

        DNS-суффикс этого подключения . . : beeline
        IP-адрес  . . . . . . . . . . . . : 10.98.44.122
        Маска подсети . . . . . . . . . . : 255.255.252.0
        Основной шлюз . . . . . . . . . . : 10.98.44.1
```

Рисунок Ж.16 - Перевірка ip-адреси

Інші опції підійдуть нам на даний момент за замовчуванням.

33. Коли завершите, натисніть на Зберегти. Ваш новий вузол мережі повинно бути видно в списку вузлів мережі.

Якщо іконка Z в колонці Доступність червона, то це означає що є якась помилка зі зв'язком - помістіть курсор мишки над цією іконкою і ви побачите спливаючу підказку про помилку. Якщо іконка сіра, значить стан поки не оновився. Перевірте чи запущений Zabbix сервер і спробуйте оновити сторінку трохи пізніше.

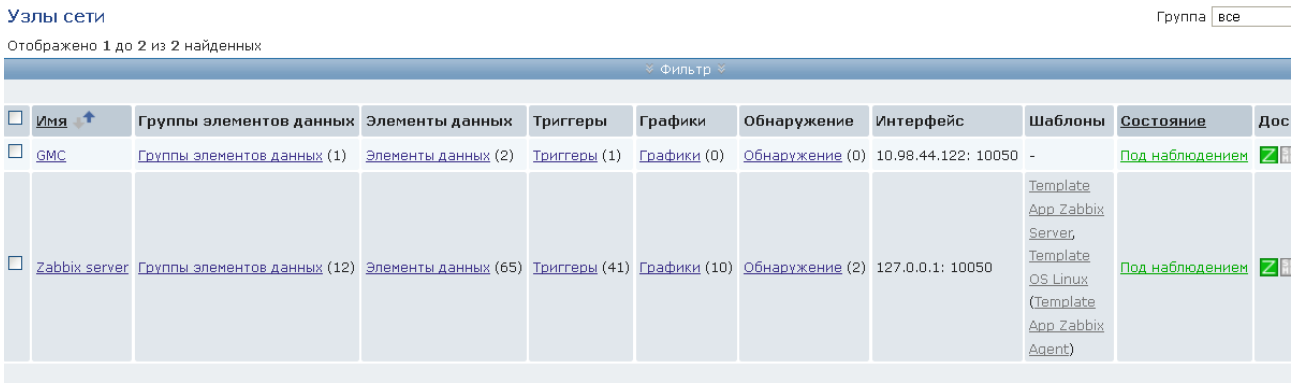


Рисунок Ж.17 - Новий вузол

34. Зробіть знімок екрана.

Новий елемент даних. 12:10:05

Елементи даних лежать в основі збору даних в Zabbix. Без елементів даних, немає даних - тому що тільки елемент даних визначає одну метрику або які дані збираються з вузла мережі.

Всі елементи даних групуються навколо вузлів мережі.

35. Саме тому для налаштування прикладу елемента даних перейдемо в Налаштування ? Вузли мережі і знайдемо 'Новий вузол мережі', який ми створили.

36. Посилання Елементи даних в рядку з 'Новим вузлом мережі' повинно відображати кількість рівну '0'. Натисніть на це посилання, і потім натисніть на Створити елемент даних. Це покаже нам форму визначення елемента даних.

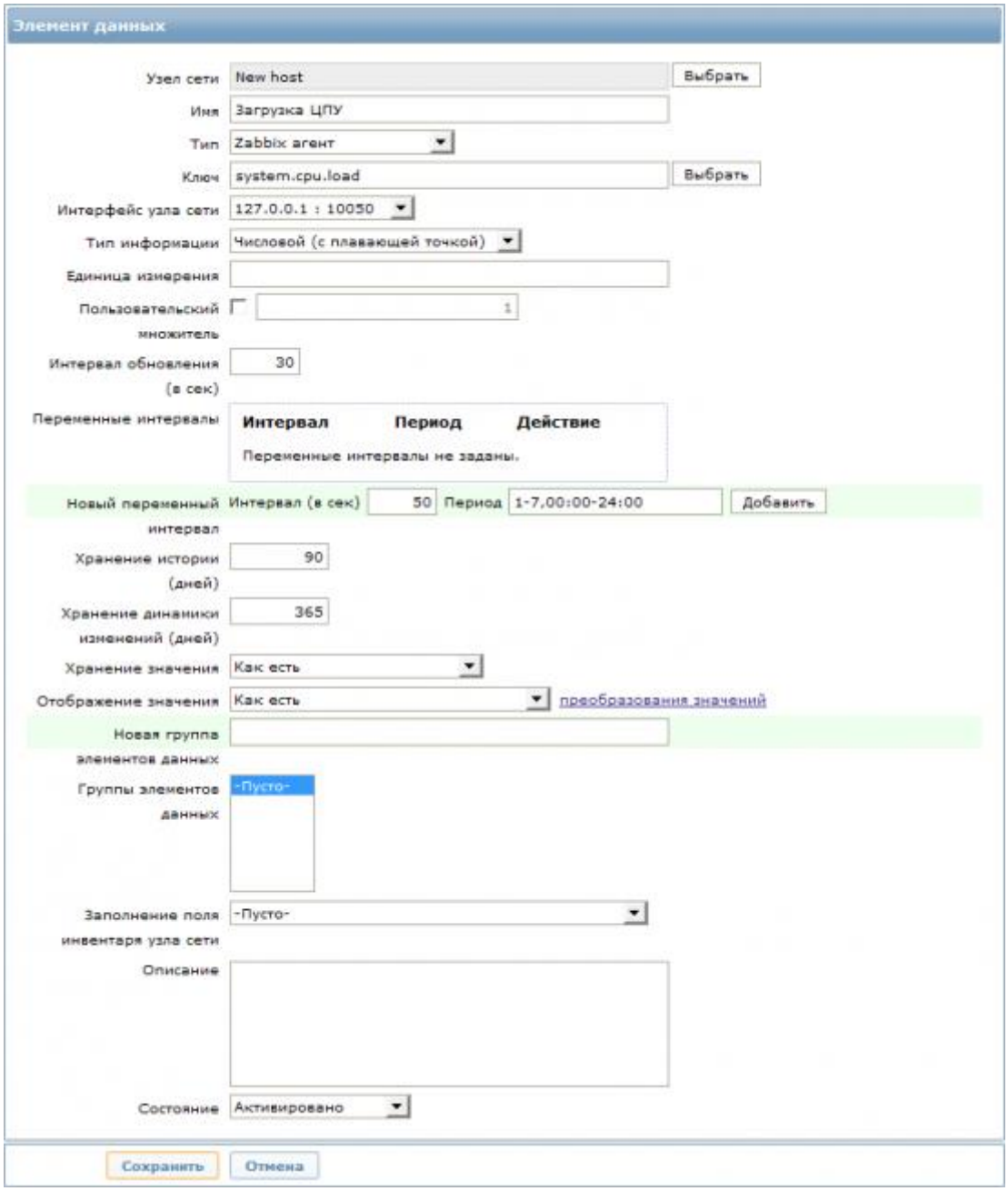


Рисунок Ж.18 - Елемент даних

37. Введіть необхідну інформацію, для нашого прикладу елемента даних:

Ім'я

Введіть значення Завантаження ЦПУ. Це буде видимим ім'ям елемента даних в списках і в інших місцях.

Ключ

Введіть значення system.cpu.load

Це формальне ім'я елемента даних, яке ідентифікує тип інформації, яка буде збиратися. Цей ключ є лише одним з зумовлених ключів, які йдуть з Zabbix агентом.

Тип інформації

Тут виберіть Дробове число. Цей атрибут визначає формат очікуваних даних.

Інші опції підійдуть нам на даний момент за замовчуванням.

38. Коли завершите, натисніть на Зберегти. Новий елемент даних повинен з'явиться в списку елементів даних. Натисніть на Деталі вище списку, щоб переглянути, що саме було зроблено.

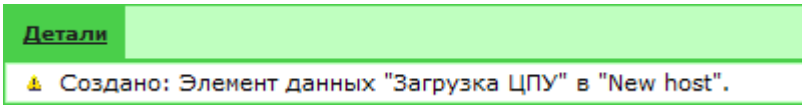


Рисунок Ж.19 - Новий елемент даних

Перегляд даних

З елементом даних все зрозуміло, вам може бути цікаво чи є насправді збір даних.

39. Для цього перейдіть в Моніторинг? Останні дані, натисніть на + до - інше - і перевірте чи є там ваш елемент даних і чи відображаються дані.

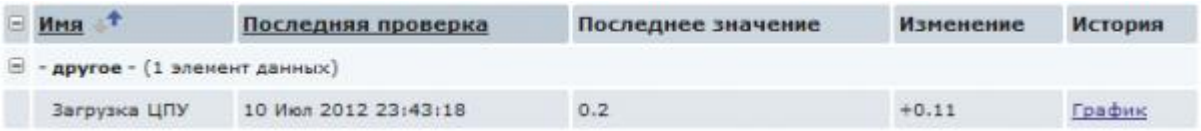


Рисунок Ж.20 - Перегляд даних

З урахуванням сказаного, отримання перших даних може зайняти до 60 секунд. Це час, за замовчуванням, як часто сервер читає зміни конфігурації і забирає нові елементи даних для обробки.

Якщо ви не бачите значення в колонці 'Змінений', то можливо до теперішнього часу було отримано тільки одне значення. Зачекайте 30 секунд поки прийде інше значення.

Якщо ви не бачите інформації про елемент даних як в скріншоті, переконайтеся що:

ви вказали поля 'Ключ' і 'Тип інформації' в елементі даних так само як на скріншоті

агент і сервер запущені

стан вузла мережі 'Спостерігається' і його іконка доступності зелена

виберіть вузол мережі у списку вузлів мережі, елемент даних активний

40. Зробіть знімок екрана.

Графіки

З елементом даних працюючим якийсь час, прийшов час побачити щось візуальне. Прості графіки доступні для будь-якого спостережуваного числового елемента даних без будь-яких додаткових налаштувань. Ці графіки створюються в режимі реального часу.

41. Для перегляду графіка, перейдіть до Моніторинг? Останні дані і натисніть на посилання 'Графік' у цьому елементі даних.

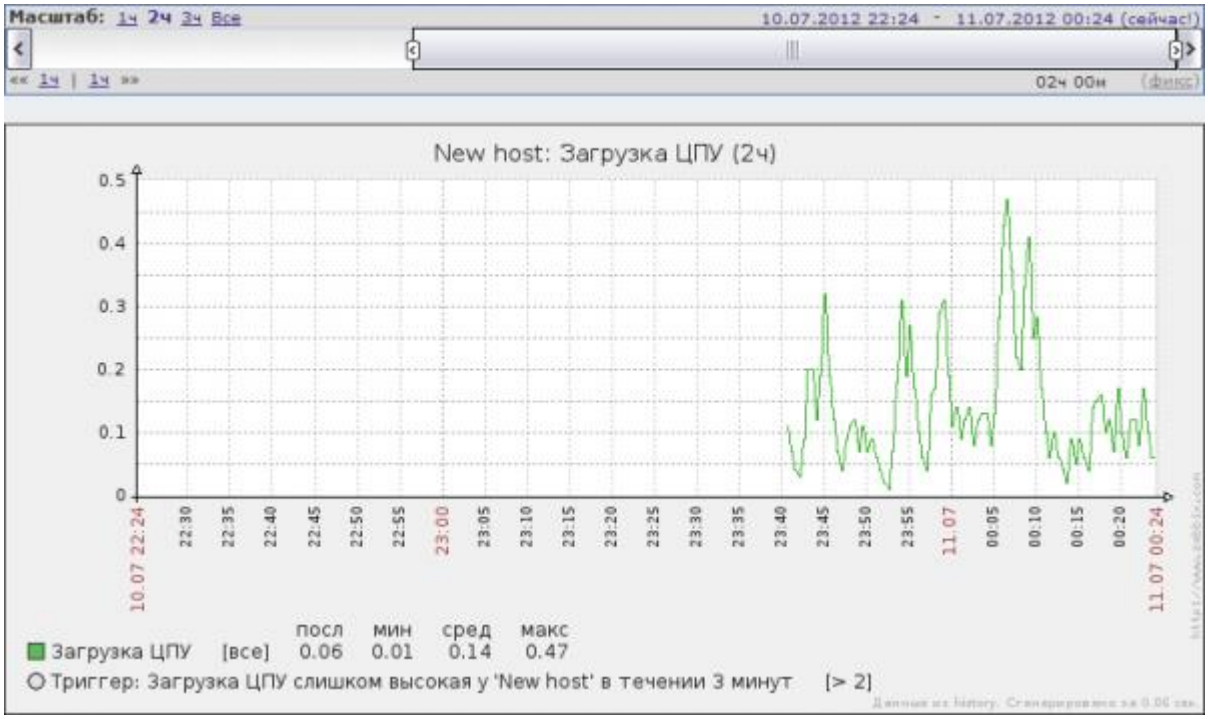


Рисунок Ж.21 -. Графік

42. Зробіть знімок екрана.

Новий тригер. 13:02:45

Елементи даних тільки збирають дані. Для автоматичної оцінки даних, що приходять, нам потрібно встановити тригери. Тригер містить вираз, який визначає поріг прийнятного рівня для даних.

Якщо цей рівень буде перевищувати дані, що прийшли, тригер буде "загорятися" або перейде в стан 'Проблема' - даючи зрозуміти, що щось сталося і може зажадати уваги. Якщо рівень стане знову прийнятним, то тригер повернеться в стан 'Ок'.

Додавання тригера

43. Щоб налаштувати тригер для нашого елемента даних, перейдіть до Налаштування? Вузли мережі, знайдіть 'Новий вузол мережі' і далі натисніть на Тригери і потім на Створити тригер. Нам буде показана форма визначення тригера.

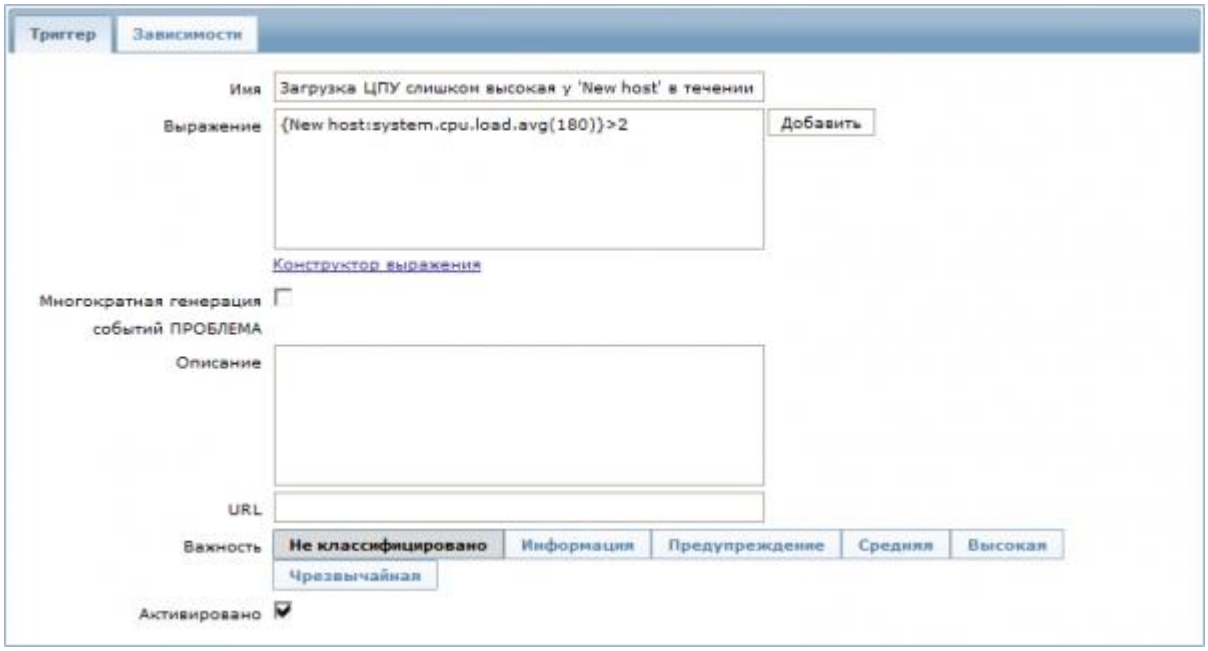


Рисунок Ж.22 - Створення тригера

44. Введіть тут необхідну інформацію для нашого тригера:

Ім'я

Введіть значення Завантаження ЦПУ занадто висока у 'GMC' протягом 3 хвилин. Це буде ім'я тригера, яке буде відображатися в списках і в інших місцях.

Вираження

Введіть: {GMC:system.cpu.load.avg(180)}>2

Де GMC ім'я вузла мережі з пункту 32.

Це вираз тригера. Переконайтеся, що вираз введено вірно, аж до останнього символу. Тут ключ елемента даних (system.cpu.load) використовується для посилання на елемент даних. По простому даний вислів говорить, що проблема з'являється при перевищенні порога, коли значення середнього завантаження ЦПУ за 3 хвилини перевищує 2.

45. Коли завершите, натисніть на Зберегти. Цей новий тригер повинен з'явитися в списку тригерів.

Перегляд стану тригера

З доданим тригером, ви можливо захочете подивитися його стан.

46. Для цього, перейдіть в Моніторинг ? Тригери. Через 3 хвилини або близько того (врешті-решт ми задавали оцінити середнє за 3 хвилини) повинен з'явитися тут, імовірно з миготливим зеленим 'ОК' в колонці 'Стан'.

Миготіння вказує на недавню зміну стан тригера, яке мало місце за останні 30 хвилин.

Якщо там блимає червоним 'ПРОБЛЕМА', тоді очевидно завантаження ЦПУ перевищило рівень порога, який ви встановили в тригері.

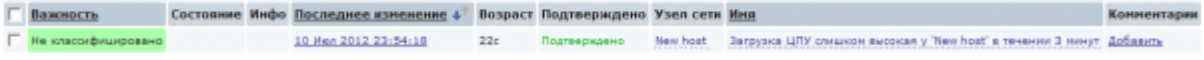


Рисунок Ж.23 - Перегляд стану тригера

ДОДАТОК И

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ NETWORK OLYMPUS

Основне завдання програми - моніторинг мережі. Він має на увазі безліч перевірок різних типів для пристроїв в мережі і реагування відповідно до результатів цих перевірок.

Для реалізації перевірок використовуються сенсори, які відслідковують певні аспекти роботи пристроїв. Кожен сенсор збирає і аналізує інформацію про пристрій, потім оцінює поточний стан на основі призначених для користувача налаштувань і, в якщо буде потреба, оповіщає про можливі проблеми.

Рисунок И.1

Кожен сенсор може здійснювати моніторинг одного вузла дерева мережі. Таким чином, сенсор може бути прив'язаний до пристрою або до групи.

Якщо сенсор прив'язаний до групи, то він буде виконувати моніторинг та відображатися для кожного з пристроїв в цій групі. Такий механізм зручно застосовувати, якщо певний сценарій моніторингу підходить для декількох пристроїв.

Так, щоб приступити до моніторингу чергового пристрою, досить включити його в групу, до якої вже прив'язані необхідні сенсори.

Рисунок И.2

Якщо група має підгрупи, то дія сенсору розповсюджується для всіх пристроїв, що входять во внутрішні підгрупи.

Рисунок И.3

Запуск сенсора може здійснюватися трьома способами вручну:

Запуск сенсора вручну призводить до його однократному негайного запуску.

Запустити сенсор одноразово можна з його контекстного меню в різних віджети, наприклад: в Дереві мережі, в Списку сенсорів і т.д.

За розкладом:

Використовується Планувальник завдань. Може бути налаштований при створенні або редагуванні сенсора на кроці конфігурації.

За результатами виконання іншого сенсора:

Для більш ефективного виявлення проблем можна формувати логічні ланцюжки сценарію.

З їх допомогою за результатами виконання сенсора можна виконувати дії і розсилати оповіщення, а також запускати інші сенсори.

Інформація щодо створення сенсорів, налаштування дій та повідомлень, а також результатів моніторингу наведено: сайт https://www.network-olympus.com/files/Network-Olympus-docs-RU.pdf

ДОДАТОК К

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ CACTI

Cacti-це повноцінний інтерфейс RRDTool, він зберігає всю необхідну інформацію для створення графіків і заповнення їх даними в базі даних MySQL. Інтерфейс повністю управляється PHP. Поряд з можливістю підтримувати графіки, джерела даних і циклічні архіви в базі даних, cacti обробляє збір даних. Існує також підтримка SNMP для тих, хто використовується для створення графіків трафіку за допомогою MRTG.

Джерела даних

Для обробки збору даних ви можете згодувати cacti шляху до будь-якого зовнішнього скрипту / команді разом з будь-якими даними, які користувач повинен буде "заповнити", а потім cacti збере ці дані в cron-завданні і заповнить базу даних MySQL/циклічні архіви.

Також можуть бути створені джерела даних, що відповідають фактичним даним на графіку. Наприклад, якщо користувач хоче побудувати графік часу пінгу для хоста, ви можете створити джерело даних, використовуючи скрипт, який пінгує хост і повертає його значення в мілісекундах. Після визначення параметрів RRDTool, таких як спосіб зберігання даних, ви зможете визначити будь-яку додаткову інформацію, необхідну джерелу Введення даних, наприклад, хост для пінгу в цьому випадку. Після створення джерела даних він автоматично підтримується з інтервалом в 5 хвилин.

Діаграми

Після визначення одного або декількох джерел даних можна створити графік RRDTool з використанням цих даних. Cacti дозволяє створювати практично будь-які мислимі графи RRDTool, використовуючи всі стандартні типи графів RRDTool і функції консолідації. Область вибору кольору і функція автоматичного заповнення тексту також допомагають у створенні графіків, щоб полегшити цей процес.

Ви не тільки можете створювати графіки на основі RRDTool в cacti, але і є багато способів їх відображення. Поряд зі стандартним "поданням списку" і "режим попереднього перегляду", який нагадує інтерфейс rrdtool 14all, існує "подання", яке дозволяє поміщати графіки в ієрархічне дерево для організаційних цілей.

Управління користувачами

Завдяки безлічі функцій cacti, в нього вбудований користувальницький інструмент управління, що дозволяє додавати користувачів і надавати їм права на певні області cacti. Це дозволить комусь створити деяких користувачів, які можуть змінювати параметри графіки, тоді як інші можуть лише переглядати графіки. Кожен користувач також підтримує свої власні налаштування, коли справа доходить до перегляду графіків.

Шаблон

Cacti здатний масштабуватися до великої кількості джерел даних і графіків за допомогою шаблонів. Це дозволяє створити єдиний шаблон графіка або джерела даних, який визначає будь-який пов'язаний з ним графік або джерело даних. Шаблони хостів дозволяють визначити можливості хоста, щоб cacti міг опитувати його для отримання інформації при додаванні нового хоста (див. рисунок К.1).

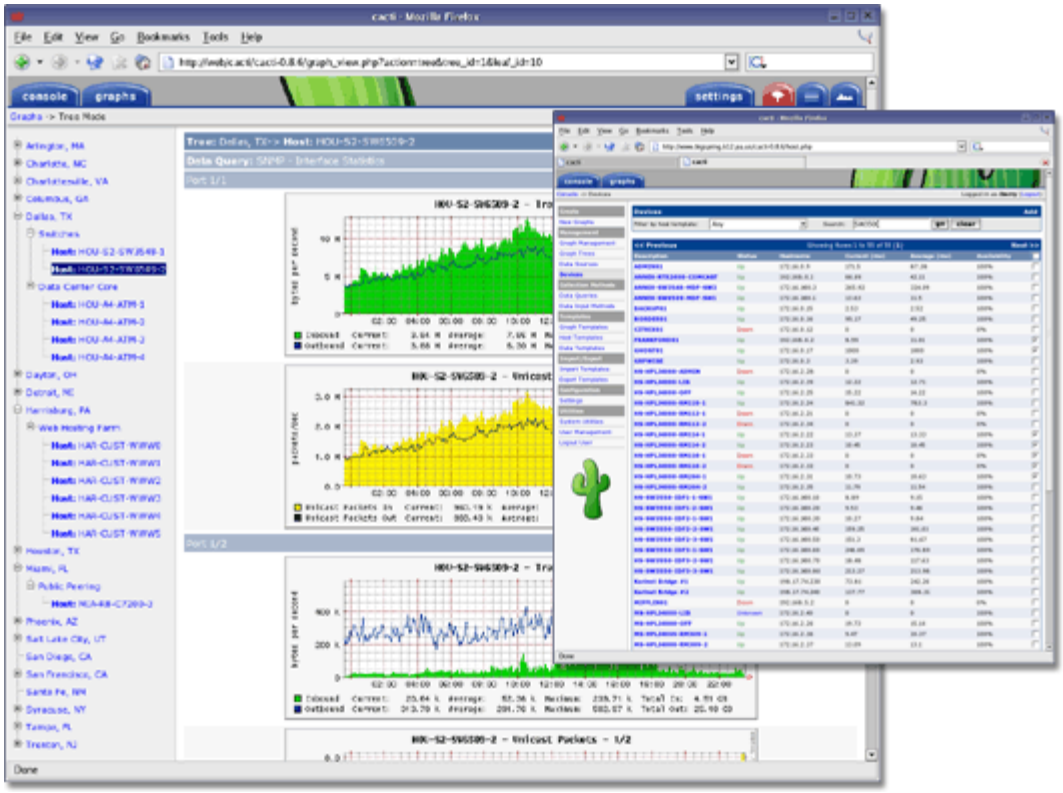


Рисунок К.1 Приклад роботи

Особливості:

- Діаграми

Необмежена кількість елементів графіка може бути визначена для кожного графіка опціонально з використанням CDEF або джерел даних з cacti.

Автоматичне групування елементів графіка GPRINT в область, стек і лінію для швидкого повторного секвенування елементів графіка.

Підтримка автоматичного заповнення, щоб переконатися, що текст легенди графіка вирівнюється.

Графічними даними можна маніпулювати за допомогою математичних функцій CDEF, вбудованих в RRDTool. Ці функції CDEF можуть бути визначені в cacti і можуть використовуватися глобально на кожному графіку.

Підтримка всіх типів графічних елементів RRDTool, включаючи область, стек, лінію, GPRINT, коментар, VRULE і HRULE.

- Джерела даних

Можна створювати джерела даних, що використовують функції RRDTool "create"і " update". Кожен джерело даних може бути використаний для збору локальних або віддалених даних і поміщений на графік.

Підтримує файли RRD з декількома джерелами даних і може використовувати файл RRD, що зберігається в будь-якому місці локальної файлової системи.

Налаштування round robin archive (RRA) можна налаштувати, надавши користувачеві можливість збирати дані на нестандартних тимчасових інтервалах при зберіганні різних обсягів даних.

- Збір даних

Містить механізм "введення даних", який дозволяє користувачам визначати користувацькі сценарії, які можуть бути використані для збору даних. Кожен сценарій може містити аргументи, які повинні бути введені для кожного джерела даних, створеного за допомогою сценарію (наприклад, IP-адреса).

Вбудована підтримка SNMP, яка може використовувати php-snmp, ucd-snmp або net-snmp.

Можливість вилучення даних за допомогою SNMP або скрипта з індексом. Прикладом цього може бути заповнення списку IP-інтерфейсами або змонтованими розділами на сервері.

Інтеграція з шаблонами графів може бути визначена таким чином, щоб забезпечити створення графів в один клік для хостів.

Для виконання сценаріїв, вилучення SNMP-даних і оновлення файлів RRD надається опитувальник на основі PHP.

- Шаблон

Шаблони графіків дозволяють групувати загальні графіки за допомогою шаблонів. Кожне поле для нормального графіка може бути шаблонізовано або задано на основі кожного графіка.

Шаблони джерел даних дозволяють групувати загальні типи джерел даних за допомогою шаблонів. Кожне поле для звичайного джерела даних може бути шаблонізовано або задано на основі кожного джерела даних.

Шаблони вузлів-це група шаблонів графів і джерел даних, які дозволяють визначати загальні типи вузлів. При створенні хоста він автоматично приймає властивості свого шаблону.

- Відображення Графіків

Деревоподібне представлення дозволяє користувачам створювати "ієрархії графів" і розміщувати графіки на дереві. Це простий спосіб управління організації великої кількості графіків.

Подання списку містить заголовок кожного графіка в одному великому списку, який пов'язує Користувача з реальним графіком.

У режимі попереднього перегляду всі графіки відображаються в одному великому форматі списку. Це схоже на представлення за замовчуванням для сценарію 14all cgi для RRDTool/MRTG.

- Управління користувачами

Управління на основі користувачів дозволяє адміністраторам створювати користувачів і призначати різні рівні дозволів для інтерфейсу cacti.

Дозволи можуть бути вказані на кожному графіку для кожного користувача, що робить Кактуси придатними для ситуацій спільного розташування.

Кожен користувач може зберегти свої власні налаштування графіка для різних переваг перегляду.

ДОДАТОК Л

ПРОГРАМА ДЛЯ МОНІТОРИНГУ МЕРЕЖІ CIC (CISCO INFO CENTRE)

Компоненти Cisco Info Center

CIC/Object Server

Object Server є основним елементом архітектури рішення Cisco Info Center. Він забезпечує функції консолідації, обробки і зберігання даних, що надходять у вигляді потоку повідомлень від проби і моніторів, які, в свою чергу, збирають дані від мережевих елементів та інформаційних систем. Невід'ємною частиною Object Server є база даних, яка знаходиться безпосередньо в пам'яті працюючого сервера, на якому встановлено додаток. Це дозволяє значно прискорити обробку аварійних повідомлень.

Object Server виконує наступні функції:

- отримує повідомлення про відмови з різних джерел, об'єднує їх, призводить до єдиного формату;
- видаляє дублікати подій;
- виконує фільтрацію подій;
- здійснює попередній кореляційний аналіз подій;
- автоматично передає управління зовнішнім програмам по настанні критично важливих подій;
- надає інформацію про відмови іншим програмам і компонентів системи управління.

Object Server має відкриту модульну архітектуру, що дозволяє розширювати можливості системи в міру зміни функціональних вимог до неї.

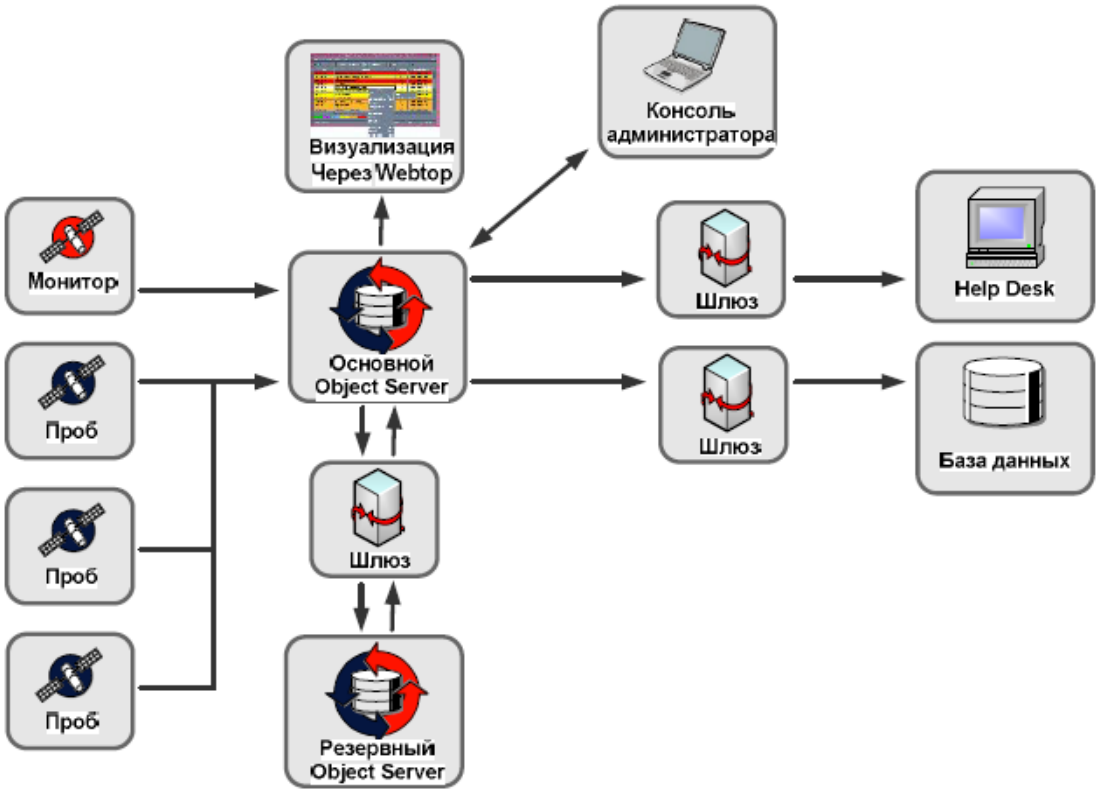


Рисунок Л.1 - Архітектура програмного модуля Object Server

Гнучка архітектура Object Server дозволяє створювати отказоустойчивую систему контролю стану мережі, а також реалізовувати різні схеми впровадження рішення для територіально-розподілених організацій з одним або декількома центрами управління.

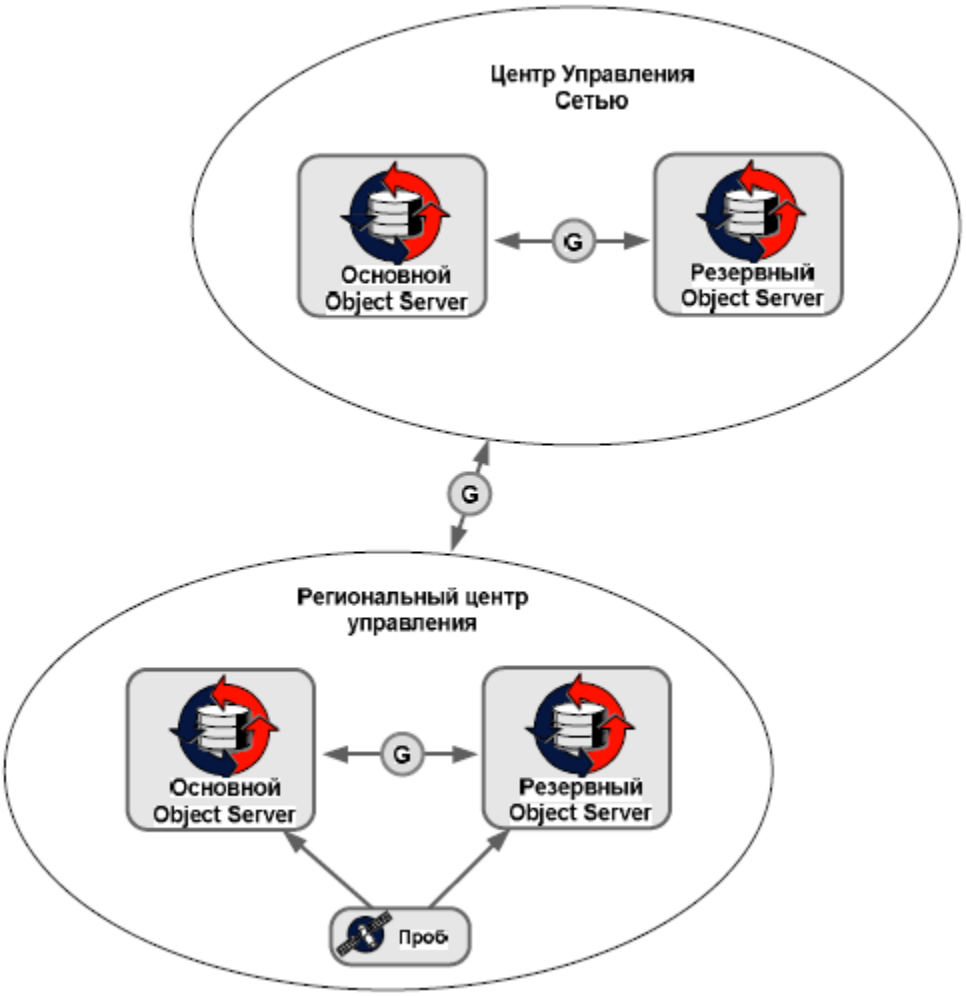


Рисунок Л.2 - Відмовостійка архітектура Object Server

Проби

Для інтеграції з обладнанням і іншими системами управління CIC використовуються програмні модулі - проби. В архітектурі CIC розрізняються спеціалізовані проби, які працюють виключно з певним видом пристроїв або з певною системою управління, і універсальні проби, які можуть бути налаштовані на взаємодія з пристроями, що підтримують протокол, за яким працює проб.

Наприклад, для інтеграції з системою управління HP OpenView використовується проб, файли конфігурації якого налаштовані на взаємодію з HP OpenView, тому при установці такого проба зусилля на його конфігурація є мінімальними.

Універсальні проби - це проби, які працюють з певною групою протоколів, наприклад, Telnet. Універсальні проби поставляються без попередньої настройки і можуть бути налаштовані для взаємодії з будь-яким пристроєм або системою, які працюють з тією ж групою протоколів, що і проб. Проби (їх перелік) вибираються в Залежно від структури мережі і завдань, які ставляться перед CIC. Проби можуть встановлюватися в міру необхідності, при цьому не потрібно серйозно змінювати конфігурацію всього комплексу Cisco Info Center.

На даний момент існує понад 400 готових проби для CIC, що дає можливість

впровадити рішення в найкоротші терміни без значних витрат.

CIC / Webtop

Додаток CIC Webtop забезпечує доступ до Cisco Info Center з використанням web-браузера. Webtop надає інформацію про відмови у вигляді карт, гістограм, кругових діаграм і списків подій, які надаються користувачам з використанням засобів HTML і Java. CIC Webtop підтримує аутентифікацію користувачів і дозволяє розмежовувати права доступу для різних груп користувачів. Для кожного користувача або групи користувачів можна налаштувати свій власний web-інтерфейс.

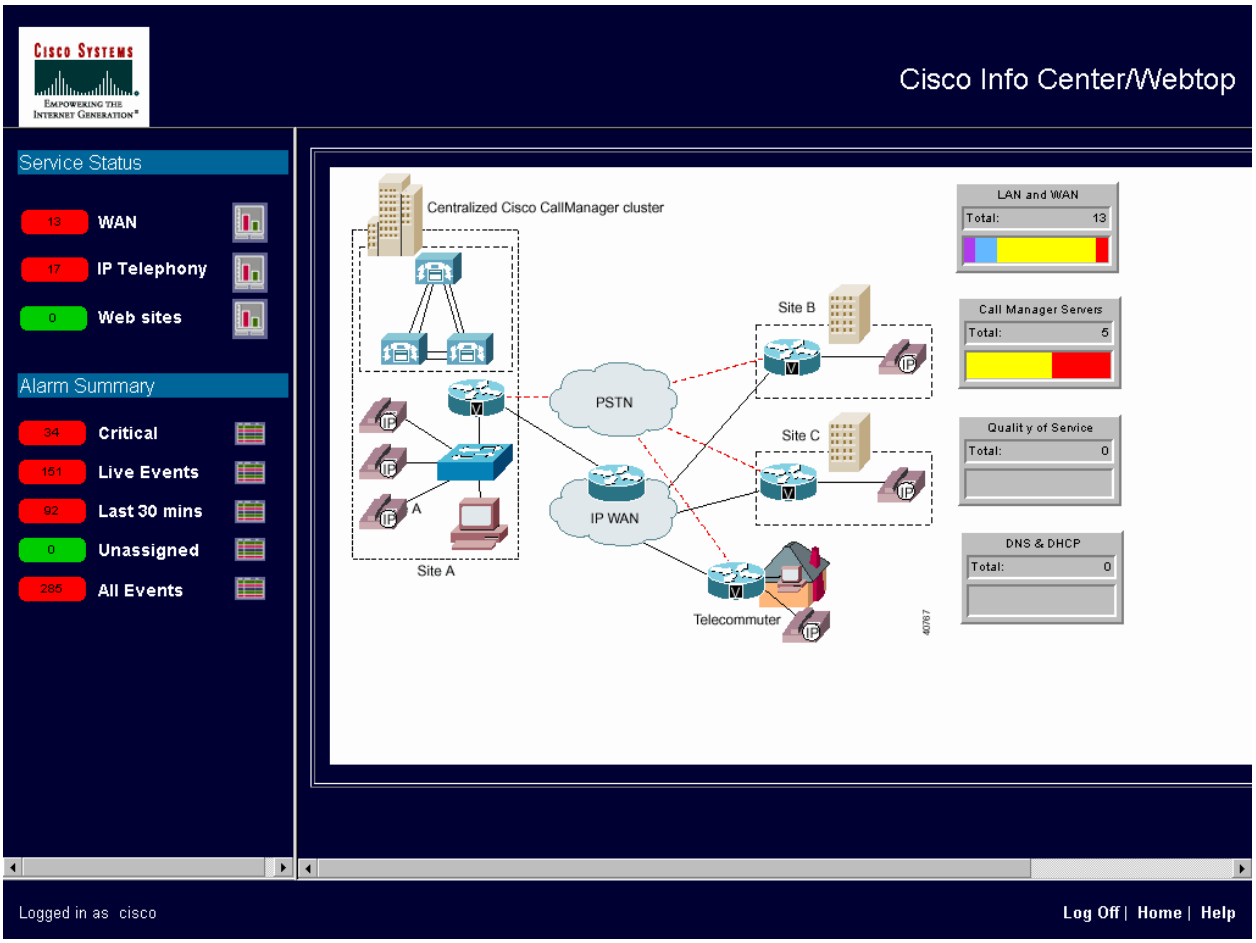


Рисунок Л.3 - Приклад узагальненого відображення сегмента мережі

Гнучкість технології Webtop дозволяє створювати самі різні уявлення даних про поточний стан мережевих елементів і додатків. Високорівнева карта може містити агреговані дані про стан мережі в регіоні або місті, в той час як низькорівневі карти можуть відображати стан обладнання, розміщеного на поверсі або в шафі серверної.

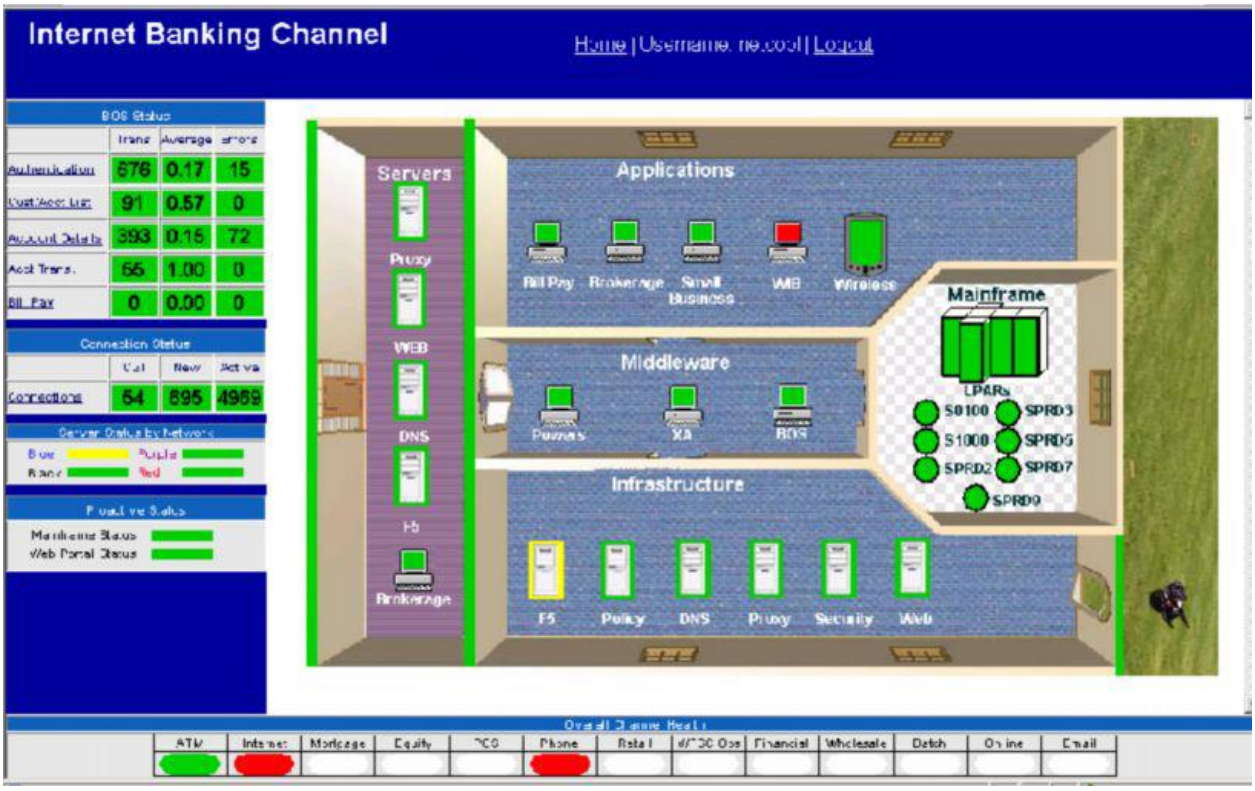


Рисунок Л.4 - Приклад відображення стану додатків з прив'язкою до плану приміщення

Використання Web-технологій дозволяє швидко виконувати локалізацію інтерфейсу.

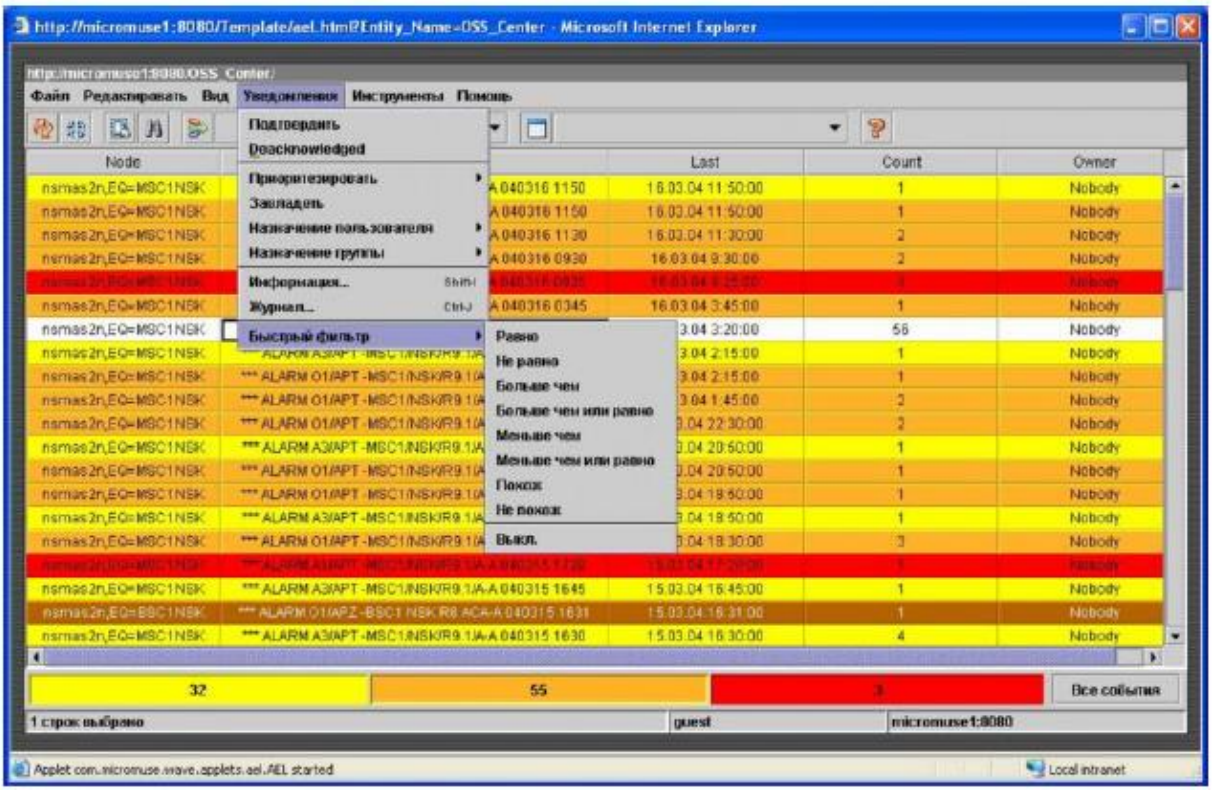


Рисунок Л.5 - Приклад локалізованого вікна виведення аварійних повідомлень

CIC / Impact

Додаток Impact є інтегруючим компонентом рішення Cisco Info Center. Impact може використовуватися для автоматизації завдань управління повідомленнями, проведення кореляційного аналізу і заповнення полів повідомлень даними від інших систем.

Даний модуль є ланкою, що забезпечує інтеграцію компонентів Cisco Info Center і продуктів сторонніх виробників.

Додаток Impact діє як односпрямований або двонаправлений інтерфейс між статичною інформацією, що зберігається в призначених для користувача базах даних, і інформацією про відмови, що зберігаються в базі даних Object Server. Основними діями, які можуть бути зроблені під час вступу події в Object Server, є доповнення повідомлення інформацією про клієнта і що надається йому послуги, аналіз впливу події на послугу, проведення більш детального кореляційного аналізу і обробка події з залученням інформації про топології мережі, даних по інвентаризації або іншої інформації бізнес-рівня.

Доповнення даних

При отриманні події додаток Impact витягує із зовнішньої бази даних (наприклад, інвентарної бази даних) додаткову інформацію, вносить її в поля повідомлення та повертає повідомлення в базу даних Object Server. Інформація із зовнішньої бази даних, отримана Impact, дозволяє проаналізувати:

- яка послуга постраждала;
- які клієнти постраждали;
- яка угоду про якість обслуговування по цій послузі з цими клієнтами.

Наприклад, Impact може використовуватися для визначення того, на роботу якого саме клієнта вплинуло відключення каналу зв'язку.

Отримане подія може нести недостатню інформацію для з'ясування ступеня його вплив на функціонування послуг. Impact може проводити складний кореляційний аналіз, щоб більш точно визначити важливість неполадки.

Кореляційний аналіз

За допомогою Impact можна змінити пріоритет події відповідно до бізнес-правилами.

Наприклад, якщо подія, пов'язана з пріоритетним клієнтом або послугою, не підтверджене оператором протягом п'яти хвилин, ступінь його важливості піднімається до критичної - 'Critical'.

Impact може виділяти з ряду подій, які були відіслані мережевими пристроями або додатками, першопричину відмови. Відомості про всіх інших подіях, крім першопричини, можуть бути придушені і не виводитися оператору, що різко скорочує кількість повідомлень, що підлягають аналізу, та прискорює процес усунення збоїв.

Правила кореляції можуть створюватися або змінюватися за допомогою вбудованого редактора, що дозволяє виробляти підстроювання системи під зміни мережевого оточення без істотних тимчасових затримок.

Оповіщення

Інформація про відмову може бути передана з використанням електронної пошти, SMS або каналів зв'язку з центром управління більш високого рівня. механізми передачі оповіщень є частиною функціональності Impact.

Взаємодія із зовнішніми програмами

Відповідно до заданих правил обробки повідомлення додаток Impact може взаємодіяти із зовнішніми програмами. Наприклад, Impact дозволяє створити звернення в системі типу Help Desk. При роботі Impact в режимі двунаправленного інтерфейсу повідомлення про відмову може бути видалено з бази даних Object Server по фактом закриття звернення.

CIC / NetManager IP

Додаток CIC / NetManager IP забезпечує візуалізацію структури складних мереж і полегшує розуміння впливу аварійних ситуацій на мережу. Можливості програми по визначенню першопричин відмов забезпечують операторам центру управління можливість сфокусуватися на усунення причини відмови, а не наслідків. При цьому наслідки відмови можуть бути придушені або ж відображені в окремому вікні.

Надання оператору короткої і коректної інформації про відмови дозволяє зменшити час локалізації збою в десятки разів.

CIC / NetManager IP забезпечує наступні основні функції:

- автоматичне визначення і побудова моделі мережі;
- візуалізація мережі;
- визначення першопричини відмови (Root Cause Analysis; RCA);
- побудова інвентарних звітів по обладнанню, яке було знайдено в процесі побудови моделі мережі.

NetManager IP аналізує мережу за допомогою спеціалізованих агентів, використовуючи при це складні алгоритми для визначення структури і топології мережі. результати аналізу використовуються для моделювання мережі і побудови графічного представлення мережі. Для взаємодії з пристроями NetManager IP використовує протоколи ICMP і SNMP.

Використання протоколу SNMP дозволяє взаємодіяти не тільки з пристроями виробництва Cisco Systems, а й з будь-якими іншими пристроями, що підтримують цей

Протокол.

При інтеграції з Object Server функціональні можливості NetManager IP надають можливість виконувати глибокий кореляційний аналіз і пошук першопричин відмов рамках всього комплексу Cisco Info Center.

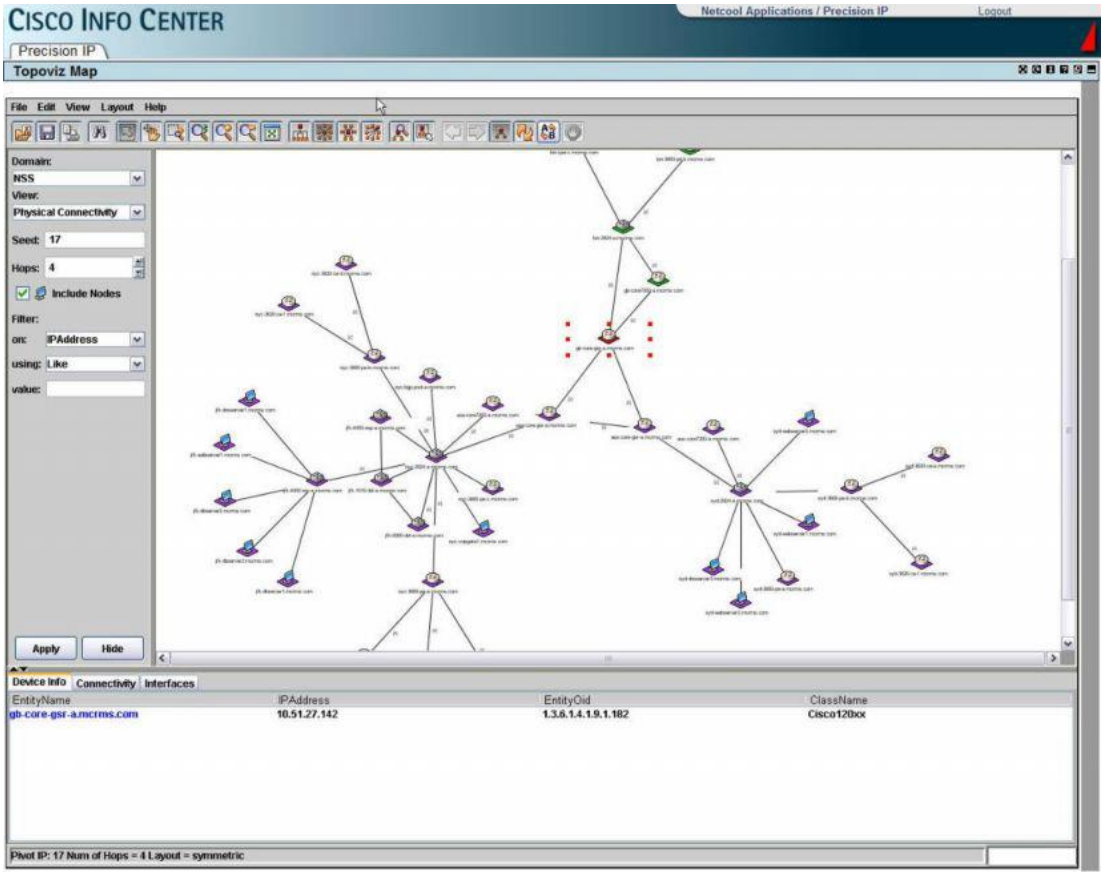


Рисунок Л.6 - Приклад подання сегмента мережі, побудованого за допомогою NetManager IP

Для роботи з даними NetManager IP необхідно встановити сервер TopViz, який входить в комплект поставки продукту CIC / NetManager IP і забезпечує можливість підключення за допомогою Web-браузера. Інтерфейс продукту дозволяє переглядати різні рівні мережі, проводити відображення тільки мережевих елементів певних типів, а також проводити пошук мережевого обладнання.

Сервіс-монітори

Сервіс-монітори є комплекс програм, які забезпечує можливість перевірки працездатності додатків в режимі реального часу.

Кожен монітор проводить моніторинг одного сервісу / додатки.

Сервіс-монітори контролюють сервіси і додатки, емулюючи роботу користувача.

Наприклад, для перевірки Web-сервера, монітор HTTP тестує доступність web-сторінки подібно живій людині і вимірює параметри доступності. Дані, які були отримані і збережені монітором, відображають доступність даної сторінки оператору і можуть бути використані в подальшому для отримання графічних звітів по швидкодії сервісів. Результати вимірювань також пересилаються компоненту Object Server для подальшої обробки та оповіщення про аварійні ситуації.

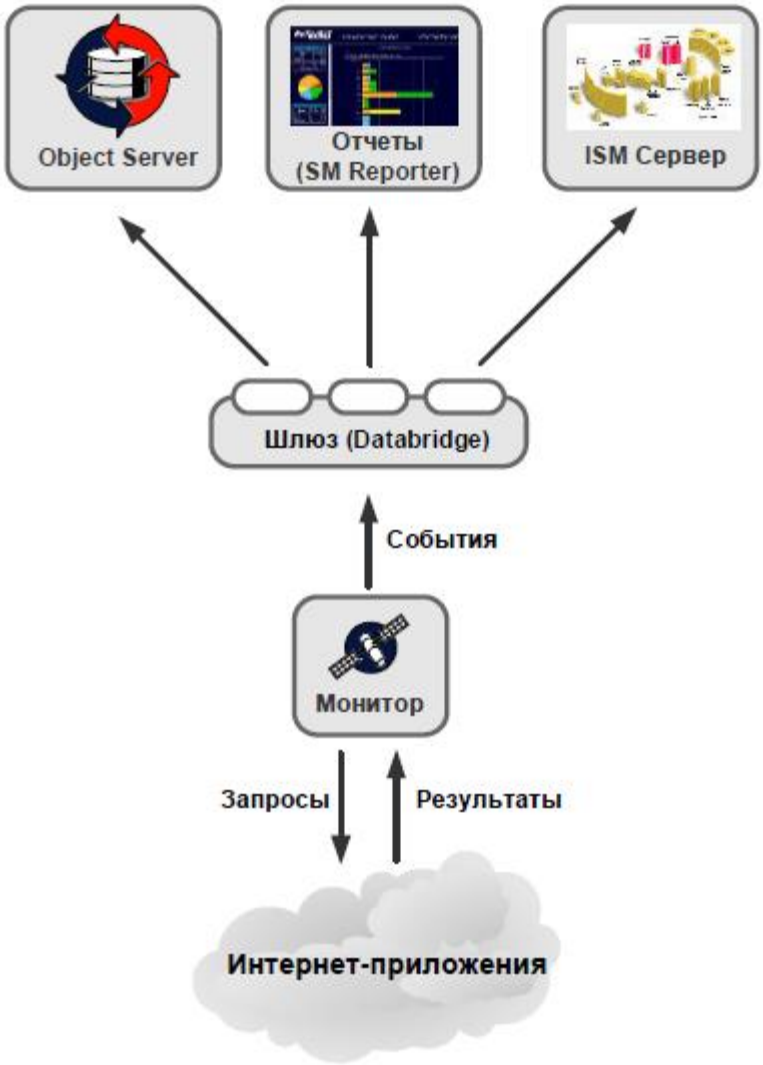


Рисунок Л.7 - Схема інтеграції сервіс-моніторів з CIC

Перелік моніторів, покривають значну частину Інтернет-додатків. Особливої уваги заслуговує монітор TRANSX, який забезпечує можливість моніторингу складних транзакцій. Наприклад, дія буде називатися успішним в разі, якщо додаток отримало файл з використанням засобів віддаленого доступу, опрацювало та зберегло цей файл з використанням протоколу FTP на файловому сервері і відправило поштове повідомлення про результат обробки. Монітор TRANSX дозволяє виробляти моніторинг виконання послідовності, тестуючи основні сервіси (Dial-UP, FTP, SMTP) і видавати аварійне повідомлення в разі, якщо дана послідовність перестав виконана.

Таблиця Л.1 - Неповний перелік додатків, контрольованих моніторами

Группа сервис-мониторов	Перечень протоколов и приложений, которые могут контролироваться
Мониторинг Интернет-сервисов (Internet Service Monitors; ISM)	Cisco SLA, DHCP, Dial-UP, DNS, FTP, HTTP, HTTPS, ICMP (ping), IMAP4, LDAP, NTP, POP3, RADIUS, RPING, RTSP, SMTP, SNMP, RCP Port, TFTP, TRANSX (монитор транзакций), WAM (монитор приложений Windows), WMS (монитор протокола Windows media streaming)
Мониторинг приложений (Application Service Monitors; ASM))	Oracle, Microsoft IIS/SQL/Exchange, Apache, IBM WebSphere, BEA Weblogic, Lotus Notes/Domino, SAP R/3
Мониторинг операционных систем (System Service Monitors; SSM)	Windows, Solaris, Linux, HP-UX, Tru64
Мониторинг мобильных услуг (Wireless Service Monitors; WSM)	SMS, WAP, MMS

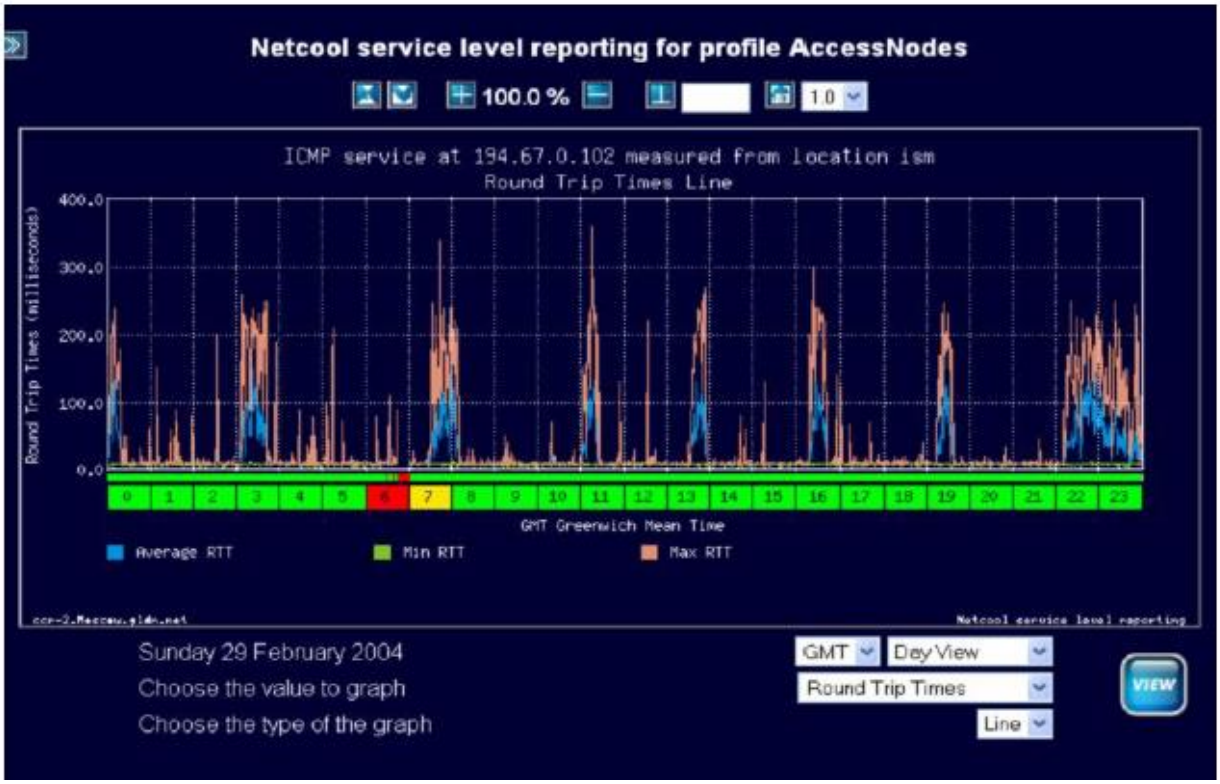


Рисунок Л.8 - Приклад звіту роботи ISM. Монітор ICMP

CIC / BSM

Додаток CIC / Business Service Manager (CIC / BSM) надає якісне і кількісний опис послуг і визначає їх взаємну залежність від існуючих мережевих пристроїв, додатків, а також від параметрів якості функціонування мережі.

Для реалізації цих вимог CIC / BSM містить формалізований опис моделі послуги, а також методи отримання інформації і процедури її аналізу для визначення впливу, що чиниться подіями різних типів на процес надання послуги.

CIC / BSM дозволяє робити моніторинг стану процесу надання послуг, взаємодіючи з додатком Object Server. При спільному використанні з додатком CIC / Impact компонент CIC / BSM дозволяє створювати складні правила для аналізу впливу проблемних ситуацій в мережі на комплексні послуги.

CIC / BSM забезпечує наступні базові функції:

- Формалізований опис послуг, що надаються, контроль параметрів процесів і додатків, обчислення індикаторів рівня сервісу, а також опис способу і частоти вимірювань значень індикаторів;
- Формування і ескалація повідомлень в разі виходу значень контрольованих індикаторів рівня сервісу за встановлених межі;
- Візуальне уявлення каталогу (моделі) сервісів з наданням статусної інформації про стан і параметри сервісу даного виду;
- Формування даних для угоди SLA (Service Level Agreement), що фіксує якісний і кількісний опис сервісів і визначального взаємну відповідальність постачальника послуг і клієнта;
- Формалізований опис структури звітів та вимог до змісту звітів і / або інших документів, частота і / або умови генерації певних документів.

CIC / BSM здатний здійснювати моніторинг SLA на підставі тимчасових інтервалів, кількості інцидентів і кумулятивних параметрів.

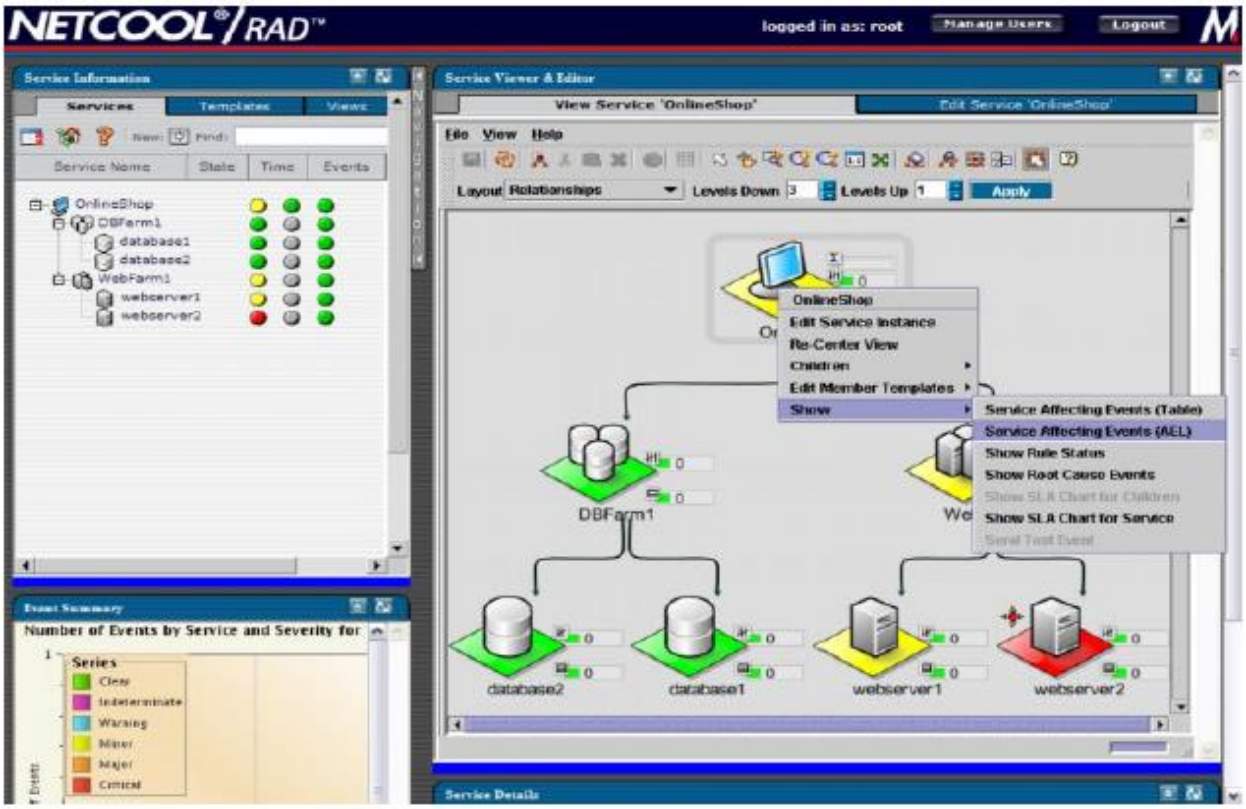


Рисунок Л.9 - Процес моделювання послуги в CIC/BSM

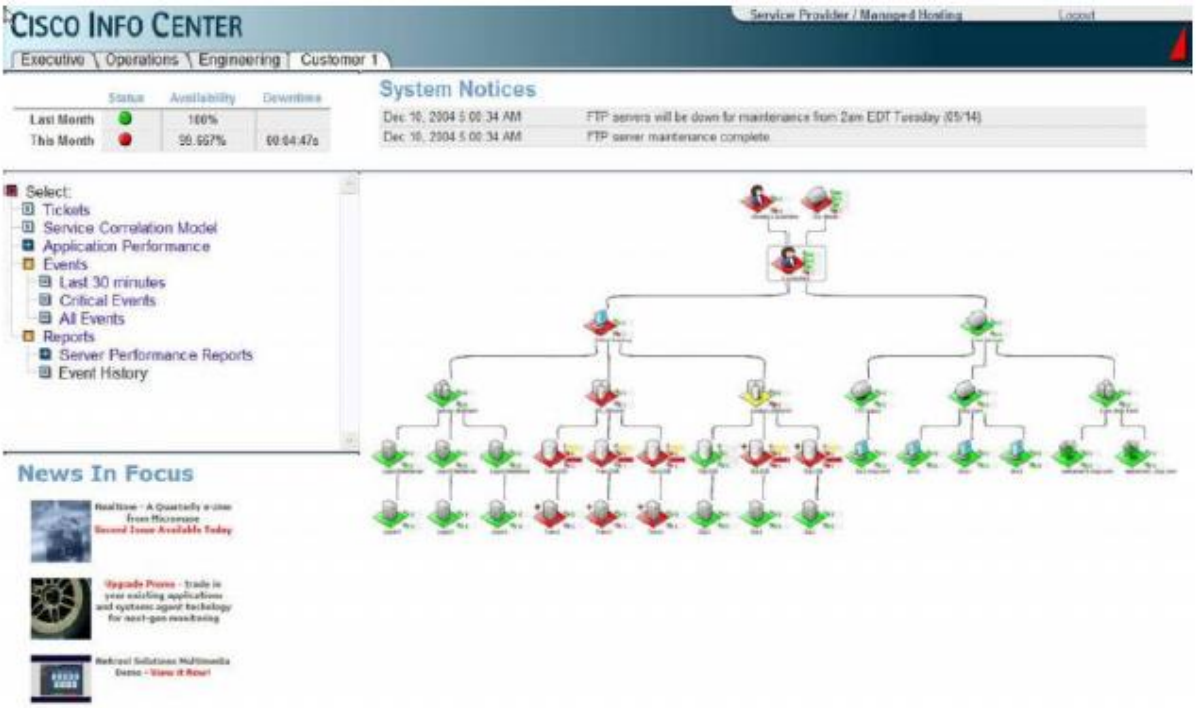


Рисунок Л.10 - Відображення першопричини непрацездатності послуги в BSM

CIC / Reporter

Додаток Reporter виконує функції генерування хронологічних звітів про події та збої і надання доступу до цих звітів з використанням web інтерфейсу. Додаток Reporter може інтегруватися з іншими додатками, які не входять до складу рішення Cisco Info Center, і відображати дані в одному інтерфейсі. Наприклад, статистичні дані з системи Help Desk можуть бути пов'язані з даними по збоїв і відображені в рамках одного звіту для простеження взаємозв'язку.

Reporter є клієнт-серверним додатком. До його складу входять Сервер і шлюз для взаємодії з компонентом Object Server. Шлюз пересилає події з бази даних Object Server в хронологічну базу даних подій Сервера. Сервер витягає інформацію з бази даних і генерує звіти за запитом оператора та / або по розкладом за звітний період. Графічні засоби програми включають в себе будівник звітів, консоль оператора для перегляду звітів і інтерфейс адміністратора для управління користувачами, ресурсами, розкладами і т.д. Перегляд звітів забезпечується з використанням Web-браузера.

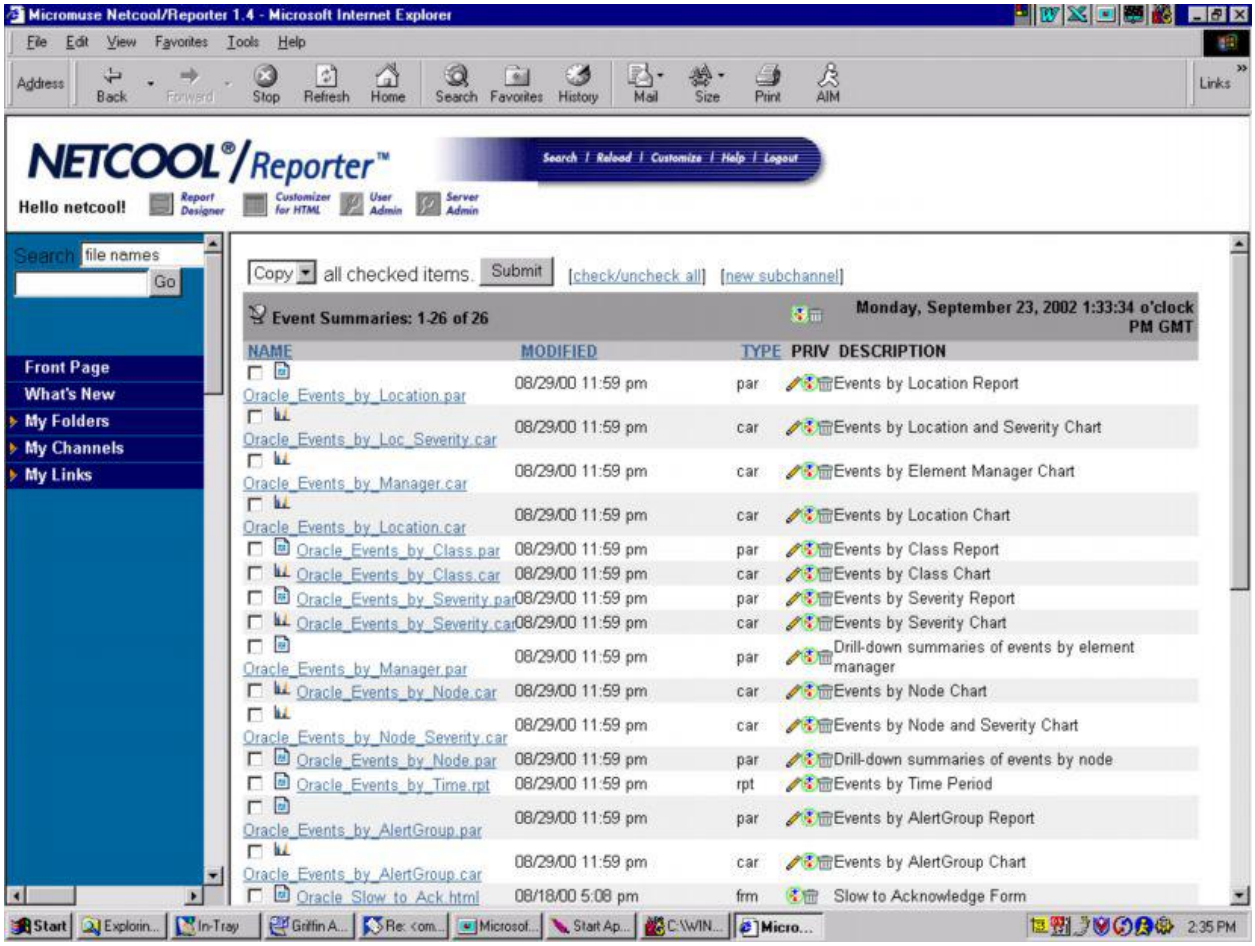


Рисунок Л.11 - Перелік звітів Reporter, доступних для перегляду

Додаток Reporter надає набір готових звітів, включаючи зведення подій для діагностики відмов і управління SLA.

Узагальнюючи дані про події за ключовими ознаками (місцезнаходження вузлів, клас подій, різні ідентифікатори), Reporter дозволяє виявляти об'єкти мережевої інфраструктури, що вимагають уваги персоналу.

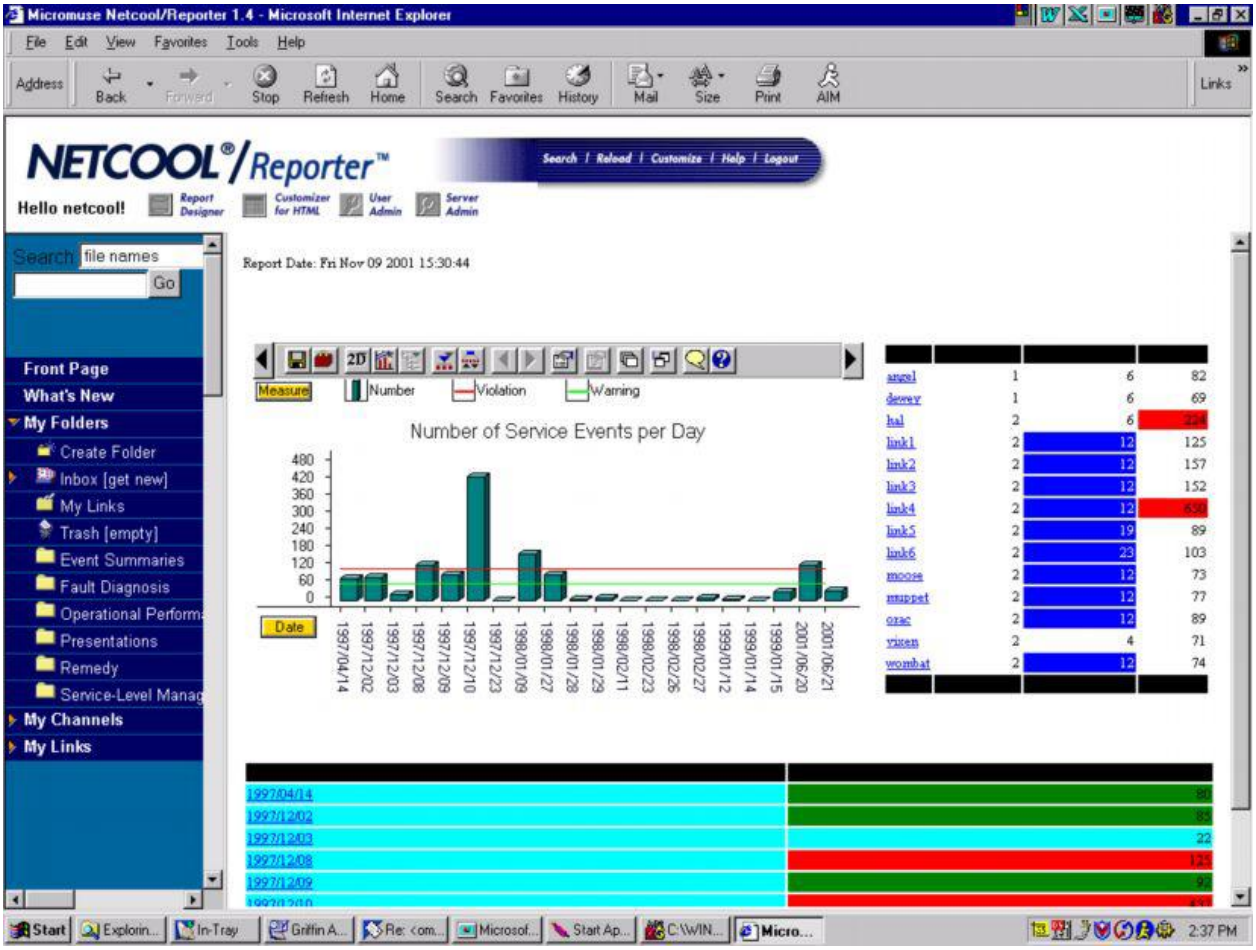


Рисунок Л.12 - Приклади звітів в Reporter

CIC / Portal

Додаток CIC / Portal являє собою незалежну платформу, яка дозволяє організувати захищений доступ до інтерактивних web-додатків, впровадити функцію єдиної реєстрації (SSO - Single Sign-On) з централізованим контролем доступу користувачів до додатків.

CIC / Portal дозволяє створювати будь-яку кількість інтерактивних web-додатків на web-сторінках порталу з можливістю завдання різних прав доступу для користувачів або груп користувачів.

У середовищі Cisco Info Center портал дозволяє відображати дані додатків ISM, Reporter, Webtop, BSM і NetManager (TopoViz). Гнучкі засоби інтеграції дозволяють додати в портал вже використовуються в організації програми, але, тим самим, організувати єдину точку доступу до інформаційних ресурсів.

Рисунок Л.13 - Єдина точка доступу до інформації: CIC/Portal