https://orcid.org/0000-0002-9639-3544
https://orcid.org/0000-0001-8205-6806

УДК 004.457

О.Є. КОВАЛЕНКО[*], К.В. КУЗНЮК[*]

СИСТЕМИ МОНІТОРИНГУ КОМП'ЮТЕРНИХ МЕРЕЖ

[*]Національний університет біоресурсів і природокористування України, м. Київ, Україна

Анотація. *Засоби моніторингу є важливою складовою інфраструктури мережі й забезпечує автоматизацію процесів адміністрування мереж. Ефективність використання системи моніторингу є окремим показником якості комп'ютерної мережі і залежить від заданих налаштувань і сценаріїв її використання. Основні характеристики та параметри, які слід дослідити та врахувати при розгортанні системи моніторингу комп'ютерної мережі: масштабованість мережі; передбачення оновлення наявної системи після розгортання; необхідний рівень комплексності моніторингу мережі; функціональність сервісу. Інструменти керування та моніторингу мережі повинні містити такі ключові функції: деталізована аналітика, сумісність, режим спрощеного огляду, сповіщення, налаштування облікових записів та інтерфейсу. Деталізована аналітика та звіти – основа моніторингу мережі. Обраний інструмент повинен здійснювати оцінку продуктивності роботи мережі, обробляючи параметри швидкодії та латентності мережі. Сумісність дозволяє взаємодіяти з різними компонентами IT-інфраструктури. Широкий спектр сумісності забезпечує більшу різноманітність характеристик елементів та більшу адаптивність сервісу до реальних умов конкретного підприємства. Сповіщення системи моніторингу повинні бути миттєвими та надсилатися щоразу при перевищенні порогового значення показника або відключенні пристрою. Системи моніторингу дозволяють редагувати тип, рівень критичності сповіщення, а також створювати категорії та шаблони моніторингу. Облікові записи є важливим аспектом, зокрема, для віддаленої роботи. Інтерфейс користувача важливий для організації процесу роботи з системою моніторингу комп'ютерної мережі з точки зору продуктивності. Вдало організований інтерфейс пришвидшує взаємодію людини-адміністратора чи людини-оператора з інформацією щодо поточного стану системи. Важливою характеристикою інтерфейсу є адаптивність відображення на пристроях різних типів: смартфон, планшет, комп'ютер тощо.*
Ключові слова: *комп'ютерна мережа, засоби керування та моніторингу мережі, функціональність комп'ютерної мережі.*

Abstract. *Monitoring tools are an important component of network infrastructure and provide automation of network administration processes. The effectiveness of using a monitoring system is a specific indicator of the computer network quality and it depends on the specified settings and scenarios of its use. The main characteristics and parameters that should be investigated and taken into account when deploying a computer network monitoring system are network scalability, the anticipation of updating the existing system after the deployment, the required level of network monitoring complexity, and service functionality. Network management and monitoring tools should include the following key features: detailed analytics, compatibility, simplified overview mode, notifications, and account and interface settings. Detailed analytics and reports are the foundation of network monitoring. The chosen tool should evaluate network performance by processing parameters of network speed and latency. Compatibility allows you to interact with various components of the IT infrastructure. A wide range of compatibility provides a greater variety of characteristics of elements and greater adaptability of the service to the real conditions of a particular enterprise. Alerts from the monitoring system must be instantaneous and sent whenever a threshold value is exceeded or a device is disabled. Monitoring systems allow you to edit the type and severity level of an alert, as well as create monitoring categories and templates. Accounts are an important aspect, particularly for remote work. The user interface is important for organizing the process of working with a com-*

puter network monitoring system from the point of view of efficiency. A well-organized interface speeds up the interaction of an administrator or an operator with information about the current state of the system. An important characteristic of the interface is the adaptability of display on different types of devices: smartphones, tablets, computers, etc.
Keywords: *computer network, network management and monitoring tools, computer network functionality.*

DOI: 10.34121/1028-9763-2023-1-50-59

1. Вступ

Високопродуктивна комп'ютерна мережа (КМ) є базовим компонентом для функціонування IT-інфраструктури сучасних підприємств та організацій. Ефективне функціонування КМ забезпечує безперебійну підтримку бізнес-процесів та комунікацій між різними підрозділами компанії, а також із клієнтами та партнерами.

Моніторинг комп'ютерної мережі – важливий аспект мережевого адміністрування [1–3]. Впровадження новітніх комп'ютерних технологій, зокрема, технологій інтернету речей та мережевої віртуалізації, потребують відстеження стану різних фізичних і віртуальних пристроїв в організації. Задля відстеження доступності, продуктивності та використання пропускної здатності в комп'ютерній мережі рекомендується використовувати програмне забезпечення для моніторингу мережі. Засоби керування та моніторингу мережею (ЗКММ) (network management and monitoring tools – NMMT) – це хмарні програмні платформи, які під'єднані до мережевих компонентів та інших IT-систем для вимірювання параметрів їх параметрів та створення аналітичних звітів про топологію, продуктивність і стан мережі. Таким чином адміністратор має змогу швидко, навіть віддалено, втрутитися. Інструменти керування та моніторингу мережі повинні містити такі ключові функції: деталізована аналітика, сумісність, режим спрощеного огляду, сповіщення, налаштування облікових записів та інтерфейсу.

Метою статті є дослідження засобів розширення функціональних можливостей системи моніторингу комп'ютерної мережі на основі аналізу сфери застосування та потреб використання комп'ютерної мережі.

2. Завдання засобів керування та моніторингу мереж

Основними завданнями ЗККМ є.

Оптимізація пропускної здатності мережі. Адміністратори мережі можуть відстежувати, як різні пристрої, користувачі, програми та хости використовують доступну пропускну здатність мережі. Вони можуть застосовувати політики для оптимізації використання пропускної здатності для кожного суб'єкта, щоб зменшити загальний тиск на мережу.

Покращення продуктивності додатків. Залежно від потреб адміністратори можуть визначити, які додатки працюють добре й потребують іншої конфігурації мережевої інфраструктури. Вони можуть вирівняти налаштування мережі таким чином, щоб покращити продуктивність програми.

Посилення безпеки. У процесі керування мережею та моніторингу можна виявляти аномалії в реальному часі. У деяких випадках ці аномалії вказують на підозрілу поведінку користувача або шкідливе програмне забезпечення, яке порушило периметр мережі.

Зменшення витрат. Стейкхолдери мережевої інфраструктури можуть стежити за ефективністю інвестицій у розвиток мережі, продуктивністю додатків і відповідними результатами діяльності, щоб виявити неефективне використання мережевого середовища. Усунувши цю неефективність, можна заощадити кошти.

Необмежена масштабованість. Належне керування мережею сприятиме стандартизації підключених кінцевих точок, користувачів і мережевих компонентів. Ця стандарти-

зація полегшує масштабування корпоративних мереж за потреби та розгортання мережевих політик без фрагментації.

3. Основні функції засобів керування та моніторингу мереж

Можна виділити п’ять ключових функцій, на які повинні мати ЗККМ [4].

1. Детальна аналітика. Аналітика та дані звітів є основою моніторингу мережі. Інструмент, який використовується, має оцінювати продуктивність мережі за такими ключовими показниками, як затримки та швидкість. Він також має генерувати інформацію про місцезнаходження та особливості пристрою з точним відображенням трендів. Залежно від мережевого середовища повинна існувати можливість вибрати та створити свої аналітичні запити.

2. Широка сумісність. Інструмент має бути сумісним з якомога більшою різноманітністю мереж і компонентів IT-інфраструктури. Це включає програмні додатки та апаратні мережеві пристрої (наприклад, фізичний брандмауер або пристрій безпеки). Крім того, ви повинні мати можливість відстежувати підключення до мережі та стан підключення в режимі реального часу для віртуальних машин, наданих провідними постачальниками, такими як VMware.

3. Спрощені інформаційні панелі. Інформаційні панелі – засіб для перегляду інформації про стан мережі та її продуктивність. Хоча звіти з даними можуть бути довгими та детальними, інформаційні панелі мають стисло відображати інформацію для розуміння з першого погляду. Інтелектуальна візуалізація даних відображає найрелевантнішу та негайну інформацію у зрозумілому форматі природною мовою.

4. Настроювані сповіщення. ЗККМ має надсилати сповіщення щоразу, коли відбувається незвичайна мережева подія, перевищено порогове значення або відключення пристрою. Ви повинні налаштувати сповіщення, щоб отримувати лише ту інформацію, яку ви хочете. Крім того, ви повинні мати можливість налаштувати спеціальні канали сповіщень, такі як електронна пошта, SMS і push-сповіщення. Це допоможе зменшити шум сповіщення й надавати лише цінні дані.

5. Декілька інтерфейсів користувача. Важлива функція для сучасних підприємств. IT-фахівцям може знадобитися відстежувати та перевіряти мережі під час руху, навіть коли вони знаходяться поза робочими станціями. Оскільки все більше організацій переходять на віддалену та гібридну роботу в довгостроковій перспективі, численні інтерфейси користувача дозволяють IT-фахівцям використовувати свої смартфони та планшети для керування мережевими операціями з будь-якого місця.

3. Характеристики засобів керування та моніторингу мереж

Велика кількість різноманітних ЗККМ на ринку засобів обслуговування мереж потребує визначення переліку та оцінювання їх характеристик для вирішення специфічних задач керування цільовою мережею.

Характеристики ЗККМ для аналізу застосовності їх засобів можна поділити на
– функціональні;
– технологічні;
– експлуатаційні;
– архітектурні;
– комерційні.

До функціональних характеристик відносяться:
– засоби інформування про події;
– ведення системного журналу;
– відстеження тенденцій;

– прогнозування тенденцій;
– розподілений моніторинг;
– відображення зв'язності мережі;
– управління доступом.
До технологічних характеристик відносяться:
– платформа реалізації;
– технологія та метод зберігання даних;
– підтримувані мережеві протоколи (IPv4, IPv6, SNMP тощо);
– використання компілятора інформаційної бази керування (MIB);
– автоматичний пошук.
До експлуатаційних характеристик відносяться:
– оснащення;
– наявність та можливості веб-застосунку;
– масштаб керованої мережі.
До архітектурних характеристик відносяться:
– агентна / безагентна;
– вбудовування компонентів (plugin);
– логічне групування.
До комерційних характеристик відносяться:
– умови використання;
– дата поточного оновлення;
– частота оновлення версій;
– підтримка з боку розробника.
Формально запропонований набір характеристик представляється кортежем

$$C = \langle F, T, E, A, S \rangle, \quad (1)$$

де C – набір характеристик ЗККМ, F – множина функціональних характеристик, T – множина технологічних характеристик, E – множина експлуатаційних характеристик, A – множина архітектурних характеристик, S – множина комерційних характеристик.

4. Методика вибору ЗККМ

Існує велика кількість різноманітних ЗККМ [4], що ускладнює процес їх вибору для конкретних потреб цільового використання. Кожна організація, а, отже, кожна мережа має різні вимоги до ЗККМ. Щоб якомога повніше задовольнити різноманітні вимоги, розроблено безліч рекомендацій, зокрема, вони представлені у роботах [4–7]. На основі запропонованого переліку характеристик ЗККМ можна забезпечити обґрунтований вибір потрібного варіанта.

Групування характеристик за моделлю (1) дозволяє дати кардинальні оцінки варіантів на основі використання вагових коефіцієнтів для різних груп. З практичної точки зору, з більш ніж сорока ЗККМ, представлених у [5], пропонується обрати ті, що мають оновлення не пізніше, ніж річної давнини або оновлюються не рідше ніж щороку. Крім того, з точки зору доступності, обираються ЗККМ, що поширюються безкоштовно. Після застосування такого фільтру для порівняння залишаються сім ЗККМ: NetXMS, OpenNMS, Zabbix, Checkmk, Cacti, Netdisco, Nagios. Серед зазначених ЗККМ обираємо такі, що забезпечують відстеження та прогнозування тенденцій, а саме: OpenNMS, Zabbix, Checkmk, Cacti. Розглянемо більш детально їх характеристики.

4.1. OpenNMS

У міру того, як межі корпоративних мереж розширюються за рахунок збільшення кількості пристроїв, процесів, служб і місць, зростають і проблеми розподіленого моніторингу. Сильно розподілені мережі викликають такі проблеми, як безпека, конфіденційність, доступність і затримка, які ускладнюють моніторинг, збір і обробку великих обсягів даних.

ЗККМ OpenNMS [8] дозволяє здійснювати ефективний моніторинг і керування в розподілених мережевих середовищах на основі:

• розподіленого збору даних для моніторингу систем і мереж, не доступних іншим чином;

• моніторингу цифрового досвіду (DEM) з різних точок зору для кращого розуміння конкретних умов;

• динамічного масштабування для адаптації до мінливих умов мережі та обсягів даних, зібраних для обробки та зберігання;

• візуалізації даних і кореляції попереджень для кращого розуміння зібраних даних і скорочення часу реагування;

• налаштування для цільового унікального моніторингу, робочого процесу та потреб персоналу.

Компоненти OpenNMS та зв’язки між ними показано на рис. 1.

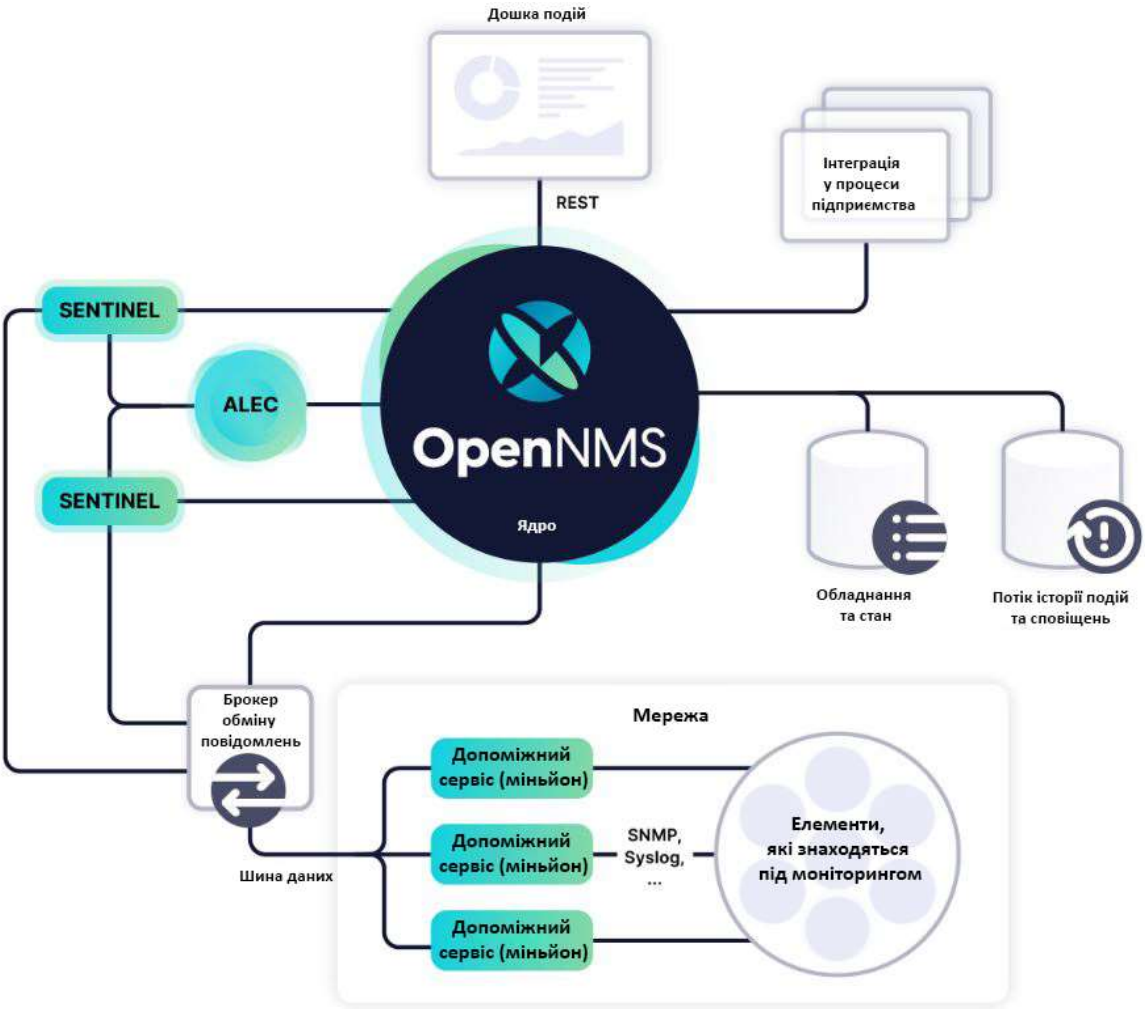

Рисунок 1 – Компоненти OpenNMS

До інфраструктури, служб і програм, розташованих на віддалених сайтах у великих розподілених корпоративних мережах, може бути складно, а то й неможливо отримати доступ і контролювати їх із центрального розташування, такого як центр обробки даних або хмара. Конкретні проблеми можуть бути пов'язані з налаштуваннями брандмауерів, трансляцією мережевих адрес (NAT), перекриттям діапазонів IP-адрес і заблокованих середовищ. Платформа моніторингу мережі повинна бути розгорнута в розподіленій конфігурації, щоб забезпечити доступ до систем і мереж, які в іншому випадку були б не доступні, зберігаючи централізовану логіку моніторингу для полегшення роботи та адміністрування.

OpenNMS забезпечує повний моніторинг несправностей, продуктивності та трафіка, а також генерацію попереджень для всієї мережі з одного центру керування.

Здійснюючи моніторинг з використанням багатьох протоколів від SNMP до Netflow і gRPC тощо, OpenNMS збирає дані про пристрої, інтерфейси та служби, які визначаються під час налаштування. Він запускає сигнали тривоги, коли виявляє проблему, і зберігає зібрані показники для аналізу тенденції, кращого управління потужністю та оптимізації мережі.

Minion діє як очі та вуха OpenNMS, розширюючи його охоплення, щоб він міг

• працювати за брандмауером і NAT;

• обробляти адресні простори, що накладаються, за допомогою окремого міньйона в кожному просторі;

• забезпечити стійке розгортання з кількома міньйонами на місце;

• масштабування горизонтального надсилання для потоку, пасток та повідомлень системного журналу з кількома міньйонами на місце;

• масштабування потокової обробки за допомогою OpenNMS Sentinel.

OpenNMS написаний мовою Java і використовує сховища даних на основі СУБД або JRobin, або RRDTool, або Apache Cassandra, або PostgreSQL.

4.2. Zabbix

Zabbix надає багато способів моніторингу різних аспектів мережевої IT-інфраструктури та майже всього, що можна підключити до нього [9, 10]. Її можна охарактеризувати як напівроздільну систему моніторингу з централізованим управлінням. Хоча багато установок мають єдину центральну систему, можна використовувати розподілений моніторинг із проксі-серверами, і більшість установок використовуватимуть агенти Zabbix. Компоненти архітектури Zabbix представлені на рис. 2.

Сервер Zabbix безпосередньо контролює кілька пристроїв, але віддалене розташування відокремлено брандмауером, тому легше збирати дані через Zabbix проксі. Zabbix проксі та Zabbix агенти, як і сервер, написані мовою C.

Центральним об'єктом є база даних Zabbix, яка підтримує кілька серверних модулів. Під час запуску кожного компонента на окремій машині і сервер Zabbix, і веб-інтерфейс Zabbix потребують доступу до бази даних Zabbix, а веб-інтерфейс Zabbix потребує доступу до сервера Zabbix для відображення статусу сервера та деяких додаткових функцій.

Хоча допускається запуск усіх трьох серверних компонентів на одному комп'ютері, але рекомендується розділити їх. Наприклад, скористатися виділеними високопродуктивною базою даних або веб-сервером.

Загалом контрольовані пристрої не впливають на відстежувані параметри. Управління конфігурацією є централізованим. Такий підхід збільшує вплив навіть однієї неправильно налаштованої системи, що може вивести з ладу всю систему моніторингу у цілому.

Сервер Zabbix, написаний мовою C, і веб-інтерфейс Zabbix, написаний мовою PHP, можуть знаходитися на одній машині або на іншому сервері.

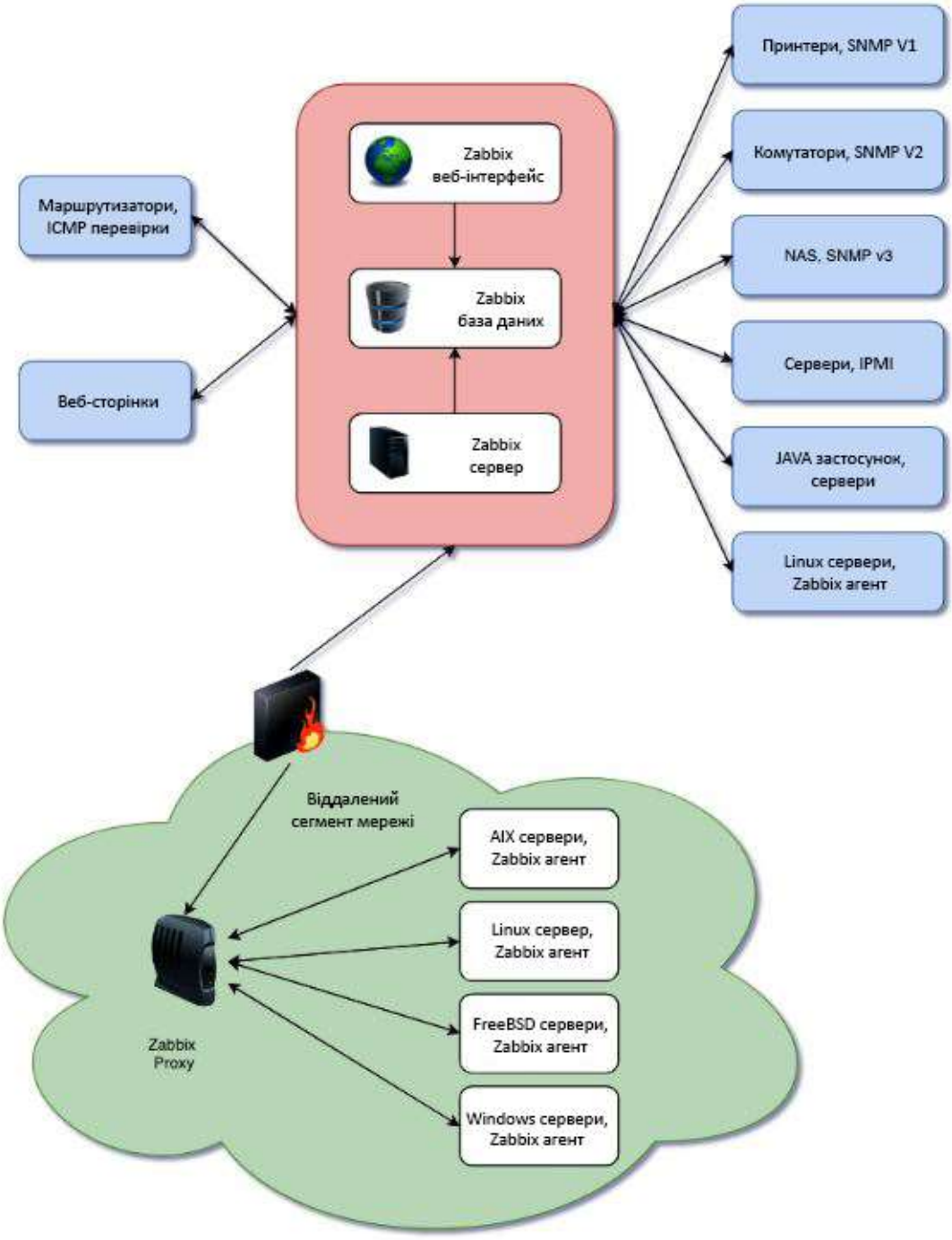

Рисунок 2 – Компоненти OpenNMS

4.3. Checkmk

Checkmk – комплексне рішення для моніторингу серверів, додатків, мереж, хмарних інфраструктур, контейнерів, сховищ, баз даних і сенсорів. Він має широкий набір функцій керування і моніторингу для масштабованих мережевих IT-середовищ [11].

Checkmk забезпечує три типи IT-моніторингу:

• Моніторинг, орієнтований на стан через порогові значення, які визначають «справність» пристрою чи програми.

• Моніторинг, орієнтований на показники, який дозволяє записувати та аналізувати параметри часових рядів за підтримки системи графічного відображення на основі HTML5. Також доступна інтеграція із плагіном Grafana [12].

• Моніторинг на основі журналів і подій, у якому можна відфільтрувати ключові події та запустити дії на основі цих подій.

Для забезпечення найширшого моніторингу Checkmk може використовувати понад 1700 плагінів у кожній редакції. Усі вони ліцензовані відповідно до GPLv2. Ці плагіни підтримуються як частина продукту і регулярно доповнюються додатковими плагінами або розширеннями. Також можливе підключення існуючих плагінів Nagios [13].

Щоб спростити налаштування та роботу, усі компоненти Checkmk постачаються повністю інтегрованими. Конфігурація на основі правил, а також високий ступінь автоматизації значно прискорюють робочі процеси, що включають:

– автоматичне виявлення хостів (за можливості);

– автоматичне виявлення послуг;

– автоматичне налаштування плагінів за допомогою попередньо налаштованих порогів і правил;

– автоматичне оновлення агентів через функцію CEE (Common Execution Environment);

– автоматичну та динамічну конфігурацію, яка дає змогу відстежувати нестійкі служби із тривалістю всього кілька секунд, наприклад, у середовищі Kubernetes (починаючи з CEE v1.6);

– автоматичне виявлення тегів і міток із таких джерел, як Kubernetes, AWS і Azure (починаючи з CEE v1.6).

Checkmk часто використовується у дуже великих розподілених середовищах, де відстежується велика кількість сайтів. Це можливо, зокрема, тому що мікроядро Checkmk споживає набагато менше ресурсів процесора, ніж, наприклад, Nagios, і тому пропонує значно вищу продуктивність на тому самому обладнанні. Крім того, неперсистентні дані зберігаються в оперативній пам'яті, що значно скорочує час доступу [14]. На рис. 3 представлена архітектура Checkmk [15].

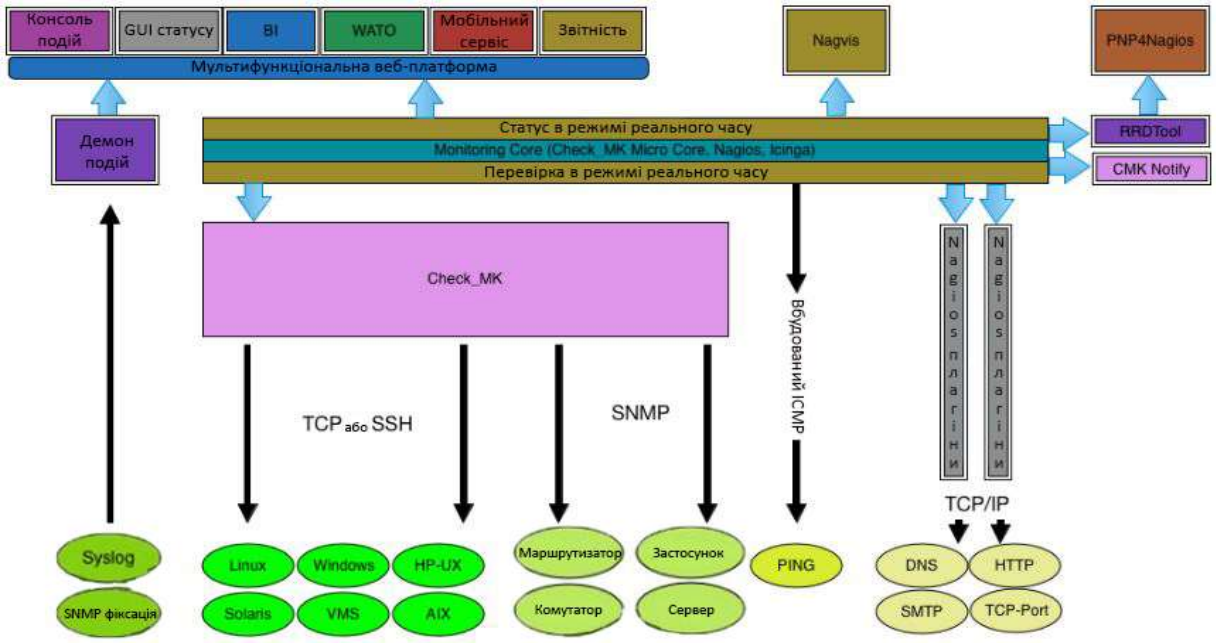

Рисунок 3 – Архітектура Checkmk

Checkmk написаний мовами Python та C++ і використовує набір утиліт RRDtool для роботи з кільцевою базою даних RRD (Round-Robin Database) [16].

4.4. Cacti

Cacti – це веб-орієнтований фреймворк із відкритим вихідним кодом [17] для управління конфігурацією, моніторингу, аналізу продуктивності та помилок мережі. Cacti дозволяє користувачеві опитувати служби через заздалегідь визначені проміжки часу та графічно представляти отримані дані. Завдяки використанню плагінів Cacti розширюється для охоплення всіх категорій операційного керування FCAPS (fault, configuration, accounting, performance, security). Зазвичай він використовується для побудови часових рядів даних метрик, таких як навантаження центрального процесора і використання пропускної здатності мережі. Загальним використанням є моніторинг мережевого трафіка шляхом опитування мережевого комутатора або інтерфейсу маршрутизатора через простий протокол керування мережею (SNMP). Архітектура фреймворку Cacti представлена на рис. 4.

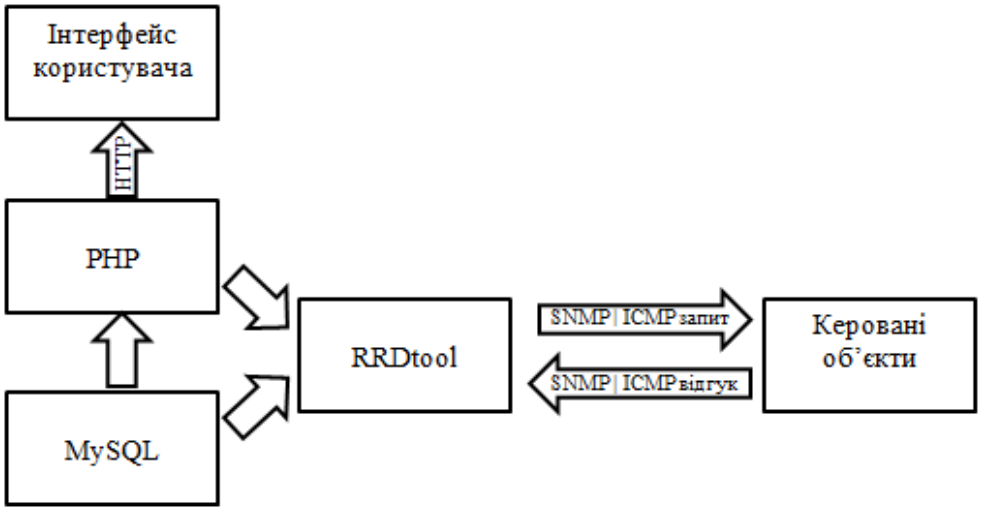

Рисунок 4 – Архітектура Cacti

Cacti підтримує моделі безпеки користувачів і груп користувачів і підтримує управління доступом на основі ролей (Role Based Access Control – RBAC) для доступу не лише до даних моніторингу, але й до різних областей інтерфейсу користувача. Базові користувачі можуть бути визначені локально або отримані з LDAP, Active Directory та інших протоколів через базову автентифікацію Apache та Nginx, яка включає постачальників єдиного входу (Single Sign-On – SSO). Інфраструктуру Cacti можна розширити за допомогою плагінів, які перетворюють Cacti з чистого рішення для створення графіків часових рядів у надійну платформу моніторингу продуктивності, керування помилками та конфігурацією. Cacti Group підтримує набір плагінів на GitHub, які надають такі можливості.

Cacti написаний мовою PHP як зовнішній застосунок, що використовує набір утиліт RRDtool для збереження файлів даних моніторингу і підтримує роботу з СУБД MySQL, MariaDB.

5. Висновки

Розглянуті засоби керування та моніторингу мережі допомагають досягати цілей керування за адекватною та передбачуваною ціною без шкоди для продуктивності. Підприємства повинні проводити попередні ретельні дослідження для оцінки своїх унікальних потреб щодо керування мережевою інфраструктурою. Цей вибір ґрунтується на п’яти функціона-

льних характеристиках, які визначають ефективність того чи іншого засобу керування та моніторингу мережі.

На вибір ЗККМ також можуть впливати архітектура системи, мови розробки, використовувані технології збереження даних та їх обробки. Архітектура на основі розширень із використанням плагінів дозволяє більш точно налаштувати ЗККМ під вирішення конкретних задач моніторингу, але потребує більш кваліфікованого персоналу. Безагентна модель знімає проблему доступності контрольованих активів мережі.

СПИСОК ДЖЕРЕЛ

1. Ratan V., Li K.F. NetFlow: Network Monitoring and Intelligence Gathering / F. Xhafa, L. Barolli, F. Amato (eds.). Advances on P2P, Parallel, Grid, Cloud and Internet Computing. 3PGCIC 2016. *Lecture Notes on Data Engineering and Communications Technologies*. 2017. Vol. 1. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-49109-7_83.
2. Tawalbeh L. Network Management. *The NICE Cyber Security Framework*. 2020. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-41987-5_5.
3. Кузнюк К.В., Коваленко О.Є. Дослідження технологій та розроблення засобів розширення функціональності систем моніторингу комп'ютерних мереж. *Інформаційні технології: економіка, техніка, освіта:* Зб. матеріалів XIII міжнар. наук.-практ. конф. молодих вчених‘2022” (м. Київ, 26–27 жовтня 2022 р.). Київ: НУБіП України, 2022. С. 135.
4. Chiradeep BasuMallick. Top 10 Network Management and Monitoring Tools in 2022. URL: https://www.spiceworks.com/tech/networking/articles/best-network-monitoring-tools.
5. Comparison of network monitoring systems. URL: https://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems.
6. How to choose the right network monitoring solution. URL: https://www.paessler.com/learn/whitepapers/selection-criteria.
7. Tittel E., Lindros K. How to select the best network monitoring tool. 2017. URL: https://www.techtarget.com/searchnetworking/feature/How-to-select-the-best-network-monitoring-tool.
8. What is OpenNMS? URL: https://www.opennms.com/platform.
9. Zabbix features and architecture. URL: https://subscription.packtpub.com/book/cloud-and-networking/9781789340266/1/ch01lvl1sec04/zabbix-features-and-architecture.
10. Zabbix Manual. URL: https://www.zabbix.com/documentation/current/en/manual.
11. Checkmk provides features for every need. URL: https://checkmk.com/product/features.
12. Mueller Ch. Grafana Data Source Plugin. 2023. URL: https://github.com/tribe29/grafana-checkmk-datasource.
13. Nagios Plugins. URL: https://www.nagios.org/downloads/nagios-plugins/.
14. Papiernik M. How To Monitor Server Health with Checkmk on Ubuntu 18.04. 2020. April 16. URL: https://www.digitalocean.com/community/tutorials/how-to-monitor-server-health-with-checkmk-on-ubuntu-18-04.
15. Check_MK Architecture. URL: https://check-mk-documentation.readthedocs.io/en/latest/cmkarchitecture.html.
16. About RRDtool. URL: https://oss.oetiker.ch/rrdtool/.
17. What is Cacti? The Cacti Group, Inc. URL: https://www.cacti.net/info/cacti.

Стаття надійшла до редакції 13.02.2023