Олександр Яценко,
Асистент кафедри комп'ютерних наук та інформаційних технологій,
sas@zu.edu.ua
(Житомирський державний університет імені Івана Франка)

ОГЛЯД ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ АНАЛІЗУ РОБОТИ МЕРЕЖІ

Використання корпоративних мереж дозволяє оптимізувати роботу, надаючи спільний доступ до серверних програм, ресурсів і обладнання, а також за рахунок прискорення обміну інформацією і даними між співробітниками. Таким чином, ефективність всього підприємства безпосередньо залежить від ефективності роботи його корпоративної мережі.

Однією з основних особливостей планування і подальшого розвитку корпоративної мережі компанії є аналіз характеристик мережевого підключення, заснований на періодичному моніторингу роботи мережі. Оцінка індивідуальних особливостей роботи локальної мережі може проводитися як на основі реальних експериментальних даних, так і з використанням процесу моделювання фізичних величин і механізмів.

Мережевий моніторинг тісно пов'язаний із забезпеченням ефективного завантаження обладнання, безперебійною роботою мережі та запобіганням несанкціонованим атакам.

Для обліку і планування зростання мережевого трафіку, аналізу характеристик мережевого підключення доцільно використовувати спеціальні засоби його моніторингу. Програмне забезпечення для моніторингу мережі є незамінним помічником для кожного системного адміністратора. Воно дозволяє вчасно реагувати на аномальну діяльність в мережі, бути в курсі всіх мережевих процесів і, таким чином, автоматизувати частину рутинної діяльності адміністратора: в першу чергу ту, що пов'язана з безпекою мережі.

Network Olympus [1] працює як служба та має веб-інтерфейс, що дає набагато більше гнучкості і зручності в роботі. Головною особливістю даного програмного продукту є конструктор скриптів, який дає можливість відійти від виконання примітивних перевірок, що не враховують всі особливості роботи

пристроїв мережі. З допомогою *Network Olympus* можна організувати схеми моніторингу будь-якої складності з метою точного виявлення проблем, а також автоматизувати процес їх усунення. *Network Olympus* постійно сканує мережу, відшукуючи доступні пристрої і створюючи візуальну карту мережевої інфраструктури, що показує підмережі, домени, робочі групи та окремі вузли; безперервно збирає і реєструє інформацію про мережу, відстежує її працездатність, перевіряє наявність сервісів. Адміністратори мережі можуть отримувати доступ до повних журналів або переглядати статистику про роботу мережі або будь-якої з її складових;

Плюсами *Network Olympus* є:

- дружній інтерфейс та простота налаштування;
- наявність конструктору сценаріїв;
- наявність датчиків, що дозволяють дізнатися про мережеві послуги, пристрої та умови їх експлуатації;
- наявність безкоштовної ліцензії для мережі, кількість пристроїв в якій менше 10 («зайві» пристрої будуть відображатися в сховищі як неактивні);
- наявність ліцензії для мереж різних розмірів, наявність знижок для навчальних закладів.

Мінусами, на нашу думку, є: установка лише під Windows та відсутність багатокористувацького режиму.

Ще одним досить поширеним додатком для моніторингу роботи мережі є *Observium* [2]. *Observium* – платформа моніторингу мережі з автоматичним реагуванням, що не вимагає додаткового обслуговування. В основі її роботи лежить використання протоколу SNMP, що дозволяє не лише досліджувати стан мережі будь-якого масштабу в режимі реального часу, але і аналізувати рівень її продуктивності. *Observium* покращує видимість мережевої інфраструктури, автоматично збираючи та відображаючи інформацію про служби та протоколи, допомагає оптимізувати планування потенціалу та відновлення інцидентів, надаючи довгостроковий збір мережевих показників та інтуїтивно зрозуміле візуальне представлення зібраних даних.

Плюси платформи *Observium*:

- інтуїтивно-зрозумілий інтерфейс;
- підтримує широкий спектр типів пристроїв, платформ та операційних систем (Cisco, Windows, Linux, HP, Juniper, Dell, FreeBSD, Brocade, Netscaler, NetApp та ін.);
- можливість налаштування різних варіантів конфігурації, починаючи від діапазонів для автовизначення до даних протоколу управління мережею (SNMP), що необхідний для збору мережевої інформації;
- може представити звіти, що генеруються за допомогою аналізу журналу подій, у графічному вигляді, наочно демонструючи слабкі сторони мережі.

Недоліки: не має підтримки мобільних пристроїв; досить складна в установці; обмежена безкоштовна версія (необмежена за кількістю пристроїв, але має значні обмеження за функціональними можливостями).

Програма *PRTG Network Monitor* [3] сумісна з пристроями на базі Windows та призначена для моніторингу мережі. Вона може бути використана не тільки для сканування пристроїв, що час підключені до локальної мережі, а й може служити для виявлення мережевих атак. Серед найкорисніших мережевих сервісів PRTG: перевірка пакетів, аналіз і збереження статистичних даних, перегляд мережевої карти в режимі реального часу, збір технічних параметрів про пристрої, підключені до мережі, аналіз рівня навантаження на мережеве обладнання. Програма, завдяки інтуїтивно зрозумілому графічному інтерфейсу, зручна у використанні. При необхідності системний адміністратор може отримати віддалений доступ до програми через веб-сервер.

До плюсів програми *PRTG Network Monitor* можна віднести: велику кількість функцій; налаштовуванні панелі; гнучкий моніторинг.

Мінуси: висока вартість (безкоштовна ліцензія лише на 30 днів); відсутність окремої бази даних та групових сенсорів.

Професійним рішенням для моніторингу роботи корпоративних комп’ютерних мереж на основі web-інтерфейсу є *Nagios*. Використання *Nagios* дає можливість віддалено регулювати навантаження на складові мережі,

слідкувати за об’ємом вільної пам’яті в базах даних, слідкувати за фізичними складовими мережного обладнання тощо. У випадку знаходження мережних аномалій програма автоматично відправляє повідомлення адміністратору мережі.

Плюсами даного програмного рішення є: висока гнучкість, наявність шаблонів, інтеграція з іншими пристроями, наявність розроблених виробником on-line уроків; можливість передавати керування конфігурацією моніторингу, системними налаштуваннями кінцевим користувачам.

Мінусами програми *Nagios*, на нашу думку, можна вважати високу вартість ліцензії (безкоштовна версія доступна впродовж 60 днів) складне налаштування та використанні (що вирішується з допомогою розробленої виробником документації та великому інтернет-співтовариству).

Крім розглянутого вище пропрієтарного програмного забезпечення для моніторингу роботи локальних корпоративних мереж існує велика кількість вільного ПЗ. Наприклад, Kismet, WireShark, NeDi, Zabbix та ін. Всі вони мають свої переваги та недоліки. На нашу думку найбільшим мінусом для більшості вільного ПЗ є відсутність оновлень та погана сумісність як з операційними системами так і з технічними пристроями.

Проаналізувавши зазначене вище, однозначно вибрати найкращу програму практично неможливо. Однак, на нашу думку, найбільш підходящою для використанні в локальних корпоративних мережах є Network Olympus. Для роботи з цією програмою непотрібно додаткового навчання, має велику кількість ліцензій для мереж різного розміру, її функціоналу достатньо для контролю практично всіх подій, що відбуваються в мережі.

Список використаних джерел та літератури

1. Network Olympus / [Електроний ресурс] // https://www.network-olympus.com/ (дата звернення: 16.05.2022).

2. Network monitoring with intuition / [Електроний ресурс] // https://www.observium.org/ (дата звернення: 16.05.2022).

3. Monitor. Visualize. Relax / [Електроний ресурс] // https://www.paessler.com/prtg (дата звернення: 16.05.2022).

4. The Industry Standard In IT Infrastructure Monitoring / [Електроний ресурс] // https://www.nagios.org (дата звернення: 16.05.2022).