УДК 004.415.5
В. Стеблик, У. Поливана
Тернопільський національний технічний університет імені Івана Пулюя

МЕРЕЖЕВИЙ МОНІТОРИНГ ЯК ЗАСІБ АНАЛІЗУ ІНФОРМАЦІЙНИХ ПРОЦЕСІВ У ЛОКАЛЬНІЙ І ГЛОБАЛЬНІЙ МЕРЕЖІ

UDC 004.415.5
V. Steblyk, U. Polyvana
(Ternopil Ivan Puluj National Technical University, Ukraine)

NETWORK MONITORING AS A WAY TO ANALYZE INFORMATION PROCESSES IN LOCAL AND GLOBAL NETWORK

Мережевий моніторинг в інформаційній структурі охоплює малі компанії та великі дата-центри. Моніторинг використовується, щоб системні адміністратори могли розрахувати спожитий трафік, стан безпеки мережі, а також були сповіщені про поломки та проблеми в інфраструктурі.

Раніше роль моніторингу здійснювали системні адміністратори, а інформацію про стан систем зберігались в неспеціалізованих програмах, або взагалі не зберігались. Практичний досвід роботи був єдиною інформацією про дану систему.

В теперішній час появилась велика кількість спеціалізованих систем моніторингу, які аналізують стан, оцінюють, збирають інформацію, а також обробляють її при необхідності.

Основною задачею системи моніторингу є представлення актуальної інформації для аналізу стану IT-інфраструктури і швидкого знаходження неполадок та їх оперативне усунення. Системи моніторингу дозволяють вчасно помітити зменшення продуктивності, відслідковувати дії користувачів в локальній комп'ютерній мережі та трафік з глобальної мережі. Постійний моніторинг дозволяє запобігти простою в роботі, підтримувати всі сервіси в активному робочому стані та дає можливість модернізації для покращення рівня якості. При виникненні проблеми в мережі відбувається надходження сповіщень-розсилок певним спеціалістам.

При відсутньому зв'язку з вузлом або елементом мережі, може використовуватись один з трьох типів систем моніторингу:

Базові системи моніторингу зазвичай працюють з протоколом ICMP. Стан елементів мережі проводиться періодично. Надається інформація про доступ та час відповіді.

Розширені системи моніторингу використовують протоколи, такі як SNMP, CDP, SSH. Завдяки їм, системи можуть отримувати практично всю інформацію про пристрої в мережі.

Системи моніторингу з активним контролем мають можливість керувати мережевими пристроями. За допомогою автоматичних сценаріїв, в цих системах можна побудувати алгоритм певних подій процедури.

При виборі, розробці чи розгортанні систем моніторингу спочатку потрібно визначити які об'єкти будуть відслідковуватись, а також критичні події і показники, які будуть надходити в сповіщеннях.

Літератури

1. Network Monitoring Fundamentals and Standards – [Електронний ресурс]. – Режим доступу: https://www.cse.wustl.edu/~jain/cis788-97/ftp/net_monitoring.pdf
2. Класифікаційні ознаки об'єктів інформаційно-моніторингових систем на основі моделі OSI – [Електронний ресурс]. – Режим доступу: http://stratcom.co.ua/klasifikatsijni-oznaki-ob-yektiv-informatsijno-monitoringovih-sistem-na-osnovi-modeli-osi/
3. Т. Лобур, О. Мацюк, Ю. Шилінська-Лобур Аналіз моніторингу трафіку в комп'ютерних мережах – [Електронний ресурс] – Режим доступу: http://elartu.tntu.edu.ua/handle/123456789/7840