УДК 004.4
О. Гуменюк
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

АНАЛІЗ РОБОТИ СТАНДАРТУ ЖУРНАЛЮВАННЯ SYSLOG

UDC 004.4
O. Humeniuk

ANALYSIS OF THE OPERATION OF THE SYSLOG JOURNALING STANDARD

Syslog – це стандарт для надсилання та отримання повідомлень у певному форматі від різних мережевих пристроїв. Повідомлення включають тимчасові мітки, повідомлення про події, серйозність, IP-адреси хостів, діагностику та багато іншого. Що стосується вбудованого рівня серйозності, то він може передавати повідомлення в діапазоні від рівня 0 – аварійний, рівня 5 – попередження, нестабільність системи, критичний та рівнів 6 та 7 – інформаційний та налагоджувальний.

Більше того, Syslog є відкритим. Syslog був розроблений для моніторингу мережевих пристроїв і систем з метою надсилання повідомлень при виникненні будь-яких проблем з функціонуванням, він також відправляє попередження про заздалегідь попереджені події та відстежує підозрілу активність через журнал змін/журнал подій мережевих пристроїв, що беруть участь.

Протокол Syslog був спочатку написаний Еріком Оллманом і визначений RFC 3164. Повідомлення надсилаються через IP-мережі на збирачі повідомлень про події або сервери syslog. Syslog використовує для зв'язку протокол User Datagram Protocol (UDP), порт 514. Хоча сервери syslog не надсилають підтвердження отримання повідомлень. З 2009 року syslog стандартизовано IETF в RFC 5424.

Для своєї роботи Syslog використовує наступні компоненти:

- Прослуховувач Syslog – збирає та обробляє дані syslog, надіслані через UDP порт 514. Однак отримання підтвердження не передбачено, і надходження повідомлень не гарантується;
- база даних – сервери syslog потребують бази даних для зберігання величезної кількості даних для швидкого доступу;
- програмне забезпечення для керування та фільтрації - оскільки обсяг даних може бути величезним, пошук певних записів у журналі може зайняти занадто багато часу. Сервер syslog потребує допомоги для автоматизації роботи, а також для фільтрації для перегляду певних повідомлень журналу. Наприклад, він може отримувати повідомлення на основі певних параметрів, таких як критична подія або ім'я пристрою. Ви також можете використовувати фільтр, щоб не бачити певних типів записів за допомогою правила Negative Filter. Якщо ви бажаєте, ви можете показати всі критичні повідомлення журналу від брандмауера.

У стандарті Syslog існує три різні рівні, а саме:

- зміст Syslog (інформація, що міститься в повідомленні про подію);
- додаток Syslog (генерує, інтерпретує, маршрутизує та зберігає повідомлення);
- транспорт Syslog (передає повідомлення).

Сигнали тривоги можуть бути налаштовані на відправлення повідомлень через SMS, спливаючі повідомлення, електронну пошту, HTTP та багато іншого. Оскільки процес автоматизований, IT-команда отримає негайне повідомлення про раптову відмову будь-якого з пристроїв.

Сервери Syslog використовуються для надсилання даних діагностики та моніторингу. Потім ці дані можуть бути проаналізовані для моніторингу системи, обслуговування мережі тощо. Оскільки протокол Syslog підтримується широким спектром пристроїв, вони можуть зручно реєструвати інформацію на сервері Syslog.

Ці дані можна аналізувати визначення поведінки систем. Крім того, журнали вважаються надійним джерелом даних для розуміння поточної статистики системи та прогнозування тенденцій. Не кажучи вже про те, що журнали використовуються для таких дій, як усунення несправностей або відхилення системи після збою.

Література

1. What is Syslog. 2017. URL: https://www.paessler.com/it-explained/syslog.
2. Syslog message formats. 2018. URL: https://support.oneidentity.com/kb/4282913/syslog-message-formats.
3. SYSLOG Over TCP. 2022. URL: https://docs.citrix.com/en-us/citrix-adc/current-release/system/audit-logging/reliable-syslog.html.