Тема 4. Системні журнали. Перегляд подій системного журналу

Системний журнал (syslog – system log) – стандарт відправки та реєстрації повідомлень про події, що відбуваються в системі (тобто створення подійних журналів), що використовується в комп'ютерних мережах, що працюють за протоколом IP. Терміном «syslog» називають як стандартизований мережевий протокол syslog, так і програмне забезпечення (додаток, бібліотеку), яке займається відправкою та отриманням системних повідомлень.

Вперше стандарт реалізований на платформі BSD Еріком Оллманом як частина проекту Sendmail, згодом, завдяки простоті та масштабованості, набув широкого поширення на Unix- та Linux-платформах і реалізований у багатьох мережевих пристроях.

Стандартом передбачається, що джерела формують прості текстові повідомлення про події, що відбуваються в них, і передають їх на обробку серверу Syslog («syslogd», «syslog daemon» або «syslog server»), використовуючи один із мережевих протоколів сімейства IP (UDP або TCP). Формування повідомлень про події та їх передача відбувається за певними правилами, які називають протоколом Syslog. Як правило, повідомлення має невеликий розмір (до 1024 байт) і відсилається у відкритому вигляді. Тим не менш, при використанні спеціальних засобів (таких як Stunnel, sslio або sslwrap), можливе шифрування повідомлень і відправлення їх по протоколу SSL/TLS.

Оскільки джерела повідомлень та сервер Syslog можуть розташовуватися на різних машинах, це дозволяє організувати збирання та зберігання повідомлень від великої кількості географічно рознесених різнорідних джерел в єдиному сховищі (репозиторії), що надзвичайно важливо для адміністраторів мереж, які можуть і не мати фізичного доступу відразу до всіх пристроїв та комп'ютерів у мережі.

Також сервери Syslog, як правило, можуть не тільки реєструвати повідомлення, але й пересилати їх іншим серверам Syslog, ґрунтуючись на рівні важливості повідомлення (Severity) та категорії сформованого повідомлення

суб'єкта (Facility), що дозволяє організувати, наприклад, ієрархічну систему сховищ. А це може допомогти, наприклад, зменшити час реакції персоналу на критичні події. Припустимо, що існує якась велика мережа, що складається з кількох сегментів. У кожному сегменті є свій сервер Syslog, який отримує повідомлення лише від джерел всередині свого сегменту. Якщо ці низові сервери налаштувати так, щоб вони пересилали повідомлення критичного рівня важливості і вище на один загальний головний сервер, адміністратору мережі, що контролює через нього всю мережу, буде легше відстежити виникнення критичної ситуації, оскільки таких повідомлень небагато і вони не потонуть у потоці потрібних але менш важливих повідомлень.

Поточна версія протоколу Syslog пропонує вдосконалений формат повідомлень, що дозволяє використовувати точну позначку часу створення повідомлення та здійснювати надійну ідентифікацію джерела повідомлення, а також застосовувати кодування UTF-8 для тексту повідомлення, що дозволяє вирішити проблему інтернаціоналізації. Необов'язкові додаткові поля (структуровані дані) можуть використовуватися для передачі різної інформації, наприклад, про похибку локального годинника джерела повідомлення та точність їх синхронізації із зовнішнім годинником точного часу, про мову, якою написано повідомлення, і т. д. Через скасування прив'язки до конкретного транспорту протокол Syslog може використовувати будь-який з описаних в окремих RFC механізмів доставки повідомлень, але перевага надається транспортам TLS.

Довгий час syslog використовувався як стандарт де-факто без формальних специфікацій, через що існувало безліч реалізацій, деякі з яких були несумісні один з одним. Перші кроки щодо вирішення цієї проблеми були зроблені в 2001 році – протокол syslog був описаний в RFC 3164. Формальна специфікація, стандартизація вмісту повідомлень і механізм їх передачі були випущені в 2005 році.

Інформаційний RFC 3164 «The BSD Syslog Protocol» (Протокол BSD Syslog), що вийшов у серпні 2001 року, описав стан, що склався на момент

публікації. В результаті проведеної роботи з аналізу існуючих реалізацій було визначено місце та значимість протоколу Syslog в інформаційних системах, формалізовано структуру повідомлень, розглянуто базові моделі розгортання та сформульовано можливі проблеми безпеки. Як транспортний механізм був заявлений UDP (порт 514) з сімейства IPv4, а також введені деякі обмеження, пов'язані з використанням цього транспорту.

У листопаді 2001 року вийшов RFC 3195 «Reliable Delivery for Syslog» (Гарантована доставка для Syslog), в якому пропонувалося рішення, що дозволяє підвищити надійність протоколу Syslog за рахунок застосування певної реалізації каркасів BEEP як носія повідомлень та використання TCP (порт 601) із сімейства IPv4 як транспорт.

Березень 2009 ознаменувався виходом цілої групи RFC, що запропонували досить серйозні вдосконалення протоколу Syslog.

RFC 5424 «The Syslog Protocol» (Протокол Syslog), по-перше, постулював, що в якості механізму доставки повідомлень може бути використаний будь-який транспорт, і тому з опису протоколу були виключені визначення транспортних механізмів і, відповідно, опис обмежень і проблем безпеки, безпосередньо пов'язані з конкретним транспортом. По-друге, запропонував новий формат повідомлення, що передбачає наявність у тілі повідомлення, крім заголовка та тексту, ще й структурованих даних, елементи яких або безпосередньо зареєстровані в IANA, або управління ними делегується підприємствам, які зареєстрували в IANA свій особистий номер відповідно до SMIv2. Крім того, новий формат повідомлення дозволяє з більшою точністю локалізувати джерело та час створення повідомлення. По-третє, продовжуючи процес інтернаціоналізації, запропонував використовувати для тексту повідомлення кодування UTF-8 як краще.

RFC 5425 «Transport Layer Security (TLS) Transport Mapping for Syslog» (Механізм доставки для Syslog, що забезпечує безпеку на транспортному рівні (TLS)) описав застосування механізму TLS для доставки повідомлень з

використанням TCP (порт 6514) з сімейства IPv4/v6 як транспорту, його обмеження та проблеми безпеки.

RFC 5426 «Transmission of Syslog Messages over UDP» (Передача повідомлень Syslog через UDP) описав механізм доставки повідомлень, що не використовує TLS, за допомогою UDP (порт 514) з сімейства IPv4/v6 в якості транспорту, його обмеження та проблеми безпеки.

RFC 5427 «Textual Conventions for Syslog Management» (Текстові угоди для управління Syslog) задав набір текстових угод, що описують важливість (Severity) та категорію (Facility) повідомлень Syslog у форматі MIB, щоб інші модулі MIB могли їх використовувати в процесі визначення керованих об'єктів.

В жовтні 2009 року побачила світ ще одна група RFC, яка зв'язує управління об'єктами з протоколом Syslog.

RFC 5674 «Alarms in Syslog» (Аварійні сигнали в Syslog) відкрив шлях до використання бази аварійних сигналів IETF (Alarm MIB) у повідомленнях Syslog.

Завдання, розв'язувані RFC 5675 «Sapping Simple Network Management Protocol (SNMP) Notifications to SYSLOG Messages» (Механізм трансляції повідомлень протоколу простого управління мережами (SNMP) у повідомлення Syslog) і RFC 5676 Protocol (SNMP) Notifications» (Визначення керованих об'єктів для механізму трансляції повідомлень Syslog в повідомлення протоколу простого управління мережами (SNMP)), зрозумілі з назв документів.

RFC 5848 «Signed Syslog Messages» (Підписані повідомлення Syslog), що вийшов у травні 2010 року, описав застосування криптографічного підпису в повідомленнях Syslog.

В жовтні 2010 року вийшов RFC 6012 «Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog» (Механізм доставки для Syslog, що забезпечує безпеку датаграм на транспортному рівні (DTLS)), що запропонував застосування механізму TLS для доставки повідомлень з використанням UDP (порт 651) із сімейства IPv4/v6 як транспорт, його обмеження та проблеми безпеки.

RFC 6587 «Transmission of Syslog Messages over TCP» (Передача повідомлень Syslog через TCP), що вийшов у квітні 2012 року, описав сформовані механізми доставки повідомлень, які не використовують TLS, за допомогою TCP із сімейства IPv4/v6 як транспорт, їх обмеження та проблеми безпеки.

Syslog виступає центральним сховищем для журналів з різних джерел. Для досягнення цієї мети сервери Syslog складаються з декількох компонентів, включаючи:

- слухач Syslog – слухач збирає та обробляє дані syslog, надіслані через UDP порт 514. Однак отримання підтвердження не передбачено, і надходження повідомлень не гарантується;
- база даних – сервери yslog 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.

У стандарті Syslog існує три різні рівні, а саме:

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

Крім того, програми можуть бути налаштовані на надсилання повідомлень у декілька пунктів призначення. Існують також сигнали тривоги, які забезпечують миттєве повідомлення про такі події, як:

- апаратні помилки;

– збої у роботі додатків;
– втрата контакту;
– неправильна конфігурація.

Крім того, 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.

Для перегляду системних журналів на даний момент існує велика кількість програмного забезпечення під різні операційні системи.