Graylog: jedno okno na logi z całej firmy

Poziom: podstawy **Dotyczy: Graylog 7.1** **Czas: ~15 min**

Ta strona otwiera książkę o Graylogu: skąd wziął się pomysł zbierania logów w jednym miejscu, dlaczego akurat Graylog i co czeka na kolejnych stronach.

Skróty użyte na tej stronie (3)

Skrót	Co znaczy
IT	Information Technology: dział albo praca związana z komputerami i infrastrukturą firmy
RFC	Request for Comments: oficjalny dokument opisujący standard internetowy, na przykład sposób działania danego protokołu; w ITIL także Request for Change, czyli wniosek o zmianę
SSH	Secure Shell: szyfrowane zdalne logowanie do serwera

Skąd się wzięło

> **Pojęcie: syslog.** Standardowy sposób, w jaki systemy uniksowe i urządzenia sieciowe zapisują i przesyłają dalej komunikaty o zdarzeniach: kto się zalogował, jaki proces się uruchomił, którą regułę firewalla zastosowano. Syslog nie jest programem, tylko formatem i protokołem, więc rozumie go niemal każdy system i każde urządzenie sieciowe od czterdziestu lat.

Napisał go Eric Allman na początku lat osiemdziesiątych na Uniwersytecie Kalifornijskim w Berkeley, jako część swojego programu Sendmail do obsługi poczty elektronicznej. Sendmail potrzebował sposobu na zapisywanie własnych komunikatów o błędach, a Allman zaprojektował go na tyle uniwersalnie, że inne programy zaczęły z niego korzystać przy okazji. Format okazał się na tyle użyteczny, że stał się nieformalnym standardem całego Uniksa, a później doczekał się oficjalnej specyfikacji w RFC 3164, a następnie w nowszym, bardziej ustrukturyzowanym RFC 5424.

Syslog rozwiązuje jednak tylko połowę problemu: mówi, jak log ma wyglądać i jak go wysłać, ale nie mówi, gdzie go szukać ani jak go przeszukiwać. Administrator dziesięciu czy stu serwerów, z których każdy pisze własny plik `/var/log/messages`, wciąż musi wiedzieć, na który serwer się

zalogować, zanim zada jakiekolwiek pytanie. Tę drugą połowę, przeszukiwalny magazyn i wygodny interfejs nad surowym strumieniem syslogowym, dopisała dopiero kolejna generacja narzędzi.

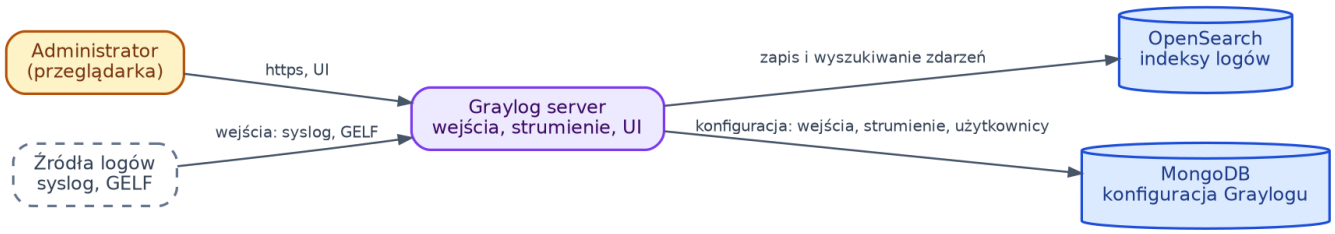
> **Pojęcie: Graylog.** Serwer centralnego logowania z własnym interfejsem webowym: przyjmuje zdarzenia z wielu źródeł naraz, indeksuje je w silniku wyszukiwania i pozwala budować zapytania, pulpity i alerty bez logowania się na żaden z monitorowanych serwerów. Graylog nie zastępuje syslogu, tylko dokłada mu drugą połowę: miejsce, w którym wszystkie te komunikaty w końcu się spotykają.

Graylog napisał Lennart Koopmann, programista z Hamburga, który zaczął projekt jako prywatną inicjatywę pod nazwą Torch około 2009 i 2010 roku, pracując wtedy w serwisie społecznościowym XING. Projekt szybko przerósł status hobby: w 2012 roku powstała spółka, w 2013 roku produkt przyjął nazwę Graylog, a w 2014 roku firma przeniosła się do Houston w Teksasie, gdzie działa do dziś jako Graylog, Inc. Od 2016 roku obok darmowej wersji Open istnieje płatna wersja Enterprise z dodatkowymi funkcjami, do których jeszcze wrócimy.

Silnikiem wyszukiwania pod spodem był przez lata Elasticsearch. W styczniu 2021 roku firma Elastic zmieniła licencję Elasticsearch na taką, która przestała być wolnym oprogramowaniem w rozumieniu społeczności open source, więc Amazon odpowiedział własnym forkiem sprzed zmiany licencji, nazwanym OpenSearch. Graylog poszedł tą samą drogą: od wersji 5.0 z 2022 roku OpenSearch jest domyślnym i docelowym silnikiem, a stary Elasticsearch traktowany jest jako ścieżka do migracji, nie jako cel sam w sobie.

Jak to działa w jednym obrazku

Graylog sam w sobie nie przechowuje logów. To warstwa aplikacyjna, która przyjmuje zdarzenia na wejściach, przepuszcza je przez reguły klasyfikujące, a samo przechowywanie i przeszukiwanie oddaje silnikowi OpenSearch. Własną konfigurację, czyli kto ma jakie konto i jak nazywają się wejścia oraz reguły, trzyma osobno, w bazie MongoDB.



Graylog przyjmuje logi ze źródeł, zapisuje i przeszukuje je w OpenSearch, a swoją konfigurację trzyma w MongoDB (kliknięcie otwiera pełny rozmiar)

Dlaczego Zielona

> **Z ŻYCIA WZIĘTE**
>
> Piątek, 15:40. Ktoś skasował plik `cennik_2026_Q4.xlsx` z udziału `\\fs01\Ksiegowosc`, a nikt nie przyznaje się do winy. Tomek, drugi tydzień w pracy, dostaje zadanie „sprawdź w logach, kto to zrobił". Zanim w firmie stanął Graylog, oznaczało to piętnaście osobnych sesji SSH i piętnaście różnych `grep` po plikach `/var/log`, z których część i tak już zdążyła się zrotować i zniknąć.

Zespół IT Zielonej długo radził sobie z logami tak, jak radzi sobie większość małych firm: każdy serwer trzymał swoje zdarzenia lokalnie, a przeszukanie czegokolwiek ponad jedną maszynę oznaczało ręczne kopiowanie plików albo, gorzej, logowanie się po kolei wszędzie tam, gdzie problem mógł zostawić ślad. Przy piętnastu serwerach produkcyjnych i dwóch administratorach ta metoda przestała się skalować na długo przed tym, zanim ktokolwiek zdążył to świadomie zauważyć.

Graylog zmienia to jednym mechanizmem: każdy serwer i każda aplikacja, opisane osobno na stronie Wysyłka logów z hostów, wysyłają swoje zdarzenia od razu, w chwili ich powstania, do jednego centralnego miejsca. Tomek zamiast piętnastu sesji SSH wpisuje jedno zapytanie w przeglądarce i w kilka sekund ma odpowiedź, z którego konta i o której godzinie plik zniknął, niezależnie od tego, na którym z piętnastu serwerów zdarzenie faktycznie powstało.

Mapa tej książki

Książka o Graylogu składa się z dziesięciu stron: od instalacji, przez codzienne wyszukiwanie, po kopię zapasową i aktualizację.

Strona	Na jakie pytanie odpowiada
Graylog: jedno okno na logi z całej firmy	Skąd wziął się Graylog i po co go mamy
Instalacja Grayloga w Dockerze: Graylog, MongoDB i OpenSearch	Jak postawić trzy kontenery i połączyć je w jeden działający system
Graylog: logowanie kontem z Active Directory	Jak podłączyć logowanie przez LDAP i co z tego jest darmowe, a co płatne
Po co centralne logowanie i jak to działa	Jaki problem w ogóle rozwiązuje centralne logowanie, niezależnie od narzędzia
Graylog: wejścia, strumienie, wyszukiwanie	Jak Graylog klasyfikuje i przeszukuje przychodzące zdarzenia

Strona	Na jakie pytanie odpowiada
Wysyłka logów z hostów	Jak skonfigurować rsyslog, journald i Windows, żeby logi w ogóle dotarły
Kopia zapasowa i aktualizacja Grayloga	Jak bezpiecznie zrobić backup trzech baz naraz i podnieść wersję
Graylog: codzienna praca z logami	Jak szukać, dzielić logi na strumienie z retencją, budować panele i alerty z powiadomieniem e-mail oraz reguły potoku
Graylog: przeprowadzka z docker01 na log01	Jak przenieść Grayloga na własny serwer bez zmian na hostach i z planem powrotu
Graylog: częste problemy	Co robić, gdy brakuje logów, czas jest przesunięty, dysk OpenSearch się zapełnił albo pola zniknęły

Powiązane: Po co centralne logowanie i jak to działa · Architektura Zabbixa: serwer, proxy, agent, frontend

Źródła: en.wikipedia.org/wiki/Graylog · graylog.org, sekcja „About" i historia firmy · RFC 5424 (The Syslog Protocol) · go2docs.graylog.org, „Upgrading to OpenSearch"

Revision #23
Created 2026-09-28 16:57:53 UTC by Tomasz Konieczny
Updated 2026-10-26 14:15:28 UTC by Tomasz Konieczny