SIEM monitor - Analiza performansi

Helena Zečević, SW-6/2014
Luka Maletin, SW-7/2014
Aleksandar Nikolić, SW-25/2014

Stres testovi

Za stres testove koristili smo alat *Gatling*, koji omogućava automatizaciju slanja velikog broja HTTP zahteva i analizu performansi izvršavanja zahteva. Test scenariji se pišu u programskom jeziku *Scala*. Za naše potrebe napravili smo dva scenarija koji pokrivaju osnovne funkcionalnosti našeg sistema:

1. Slanje logova od strane agenata,
2. Slanje upita od strane operatera.

Oba scenarija su izvršavana za 100, 1000 i 10000 konkurentnih zahteva. Sažeti rezultati testiranja prikazani su u tabelama 1 i 2, dok se detaljniji rezultati mogu pogledati u izgenerisanim izveštajima.

Tabela 1. Vremena odziva (ms) prilikom slanja logova (simulacija agenata).

Broj zahteva	Najmanje vreme	Najveće vreme	Prosečno vreme
100	13	151	51
1k	11	336	62
10k	11	3844	574

Tabela 2. Vremena odziva (*ms*) prilikom slanja upita (simulacija operatera).
Broj logova u sistemu je 49k.

Broj zahteva	Najmanje vreme	Najveće vreme	Prosečno vreme
100	57	231	153
1k	34	3217	731
10k	35	20268	8979

Rezultati pokazuju da sistem radi zadovoljavajuće čak i kad je u pitanju neočekivano veliko opterećenje. Performanse su naročito dobre u simulaciji agenata, gde je očekivani broj agenata u realnom sistemu nekoliko stotina do nekoliko hiljada. Ukoliko bi postojala potreba za još većim brojem agenata, imalo bi smisla razdvojiti sistem na podsisteme sa zasebnim SIEM centrima.

Vreme odziva pretrage logova raste očekivano brže sa porastom broja zahteva, medjutim očekivani broj korisnika je ipak samo nekoliko desetina.

Potrošnja resursa

S obzirom da je SIEM centar implementiran u vidu *Spring Boot* aplikacije, za analizu potrošnje resursa računara koristili smo *Spring Boot Admin*, koji se oslanja na *Spring Boot Actuator*.
Analizom različitih metrika kao najvažniju izdvojili smo zauzeće memorije. Prilikom mirovanja aplikacija zauzima oko 200 MB. Zauzeće prilikom velikog broja konkurentnih zahteva (korišćen *Gatling*) prikazano je u tabelama 3 i 4.

Tabela 3. Zauzeće memorije (MB) prilikom slanja logova.

Broj zahteva	Zauzeće memorije
100	317
1k	583
10k	469

Tabela 4. Zauzeće memorije (MB) prilikom slanja upita.

Broj zahteva	Zauzeće memorije
100	275
1k	436
10k	731

Iz ovoga zaključujemo da sistem ne zahteva mnogo memorije, i da može da radi sa 2 GB koji su alocirani za JVM sa podrazumevanom konfiguracijom.
Što se tiče prostora na disku, trenutnih 66k logova zauzima 400 MB. To u ovom trenutku nije problem, ali bi sistem svakako trebalo proširiti funkcionalnostima za brisanje starih logova.