CARNET

Splunk Free

CERT.hr-PUBDOC-2021-8-404

CERT.hr

Sadržaj

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument vlasništvo je Nacionalnog CERT–a. Namijenjen je javnoj objavi te se svatko smije njime koristiti i na njega se pozivati, ali isključivo u izvornom obliku, bez izmjena, uz obvezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima povreda je autorskih prava CARNET-a, a sve navedeno u skladu je sa zakonskim odredbama Republike Hrvatske.

1 Uvod

Kako bi se osigurala dostupnost i sigurnost bilo kojeg složenijeg IT sustava, potrebno je taj sustav kontinuirano nadzirati. Za kvalitetan nadzor IT sustava, potrebno je prikupljati dnevnike (engl. *logs*) koji se generiraju na razini uređaja i pojedinih aplikacija te razne druge metrike poput postotka korištenosti radne memorije nekog poslužitelja i broja HTTP zahtjeva po sekundi koji pristiže na određenu web aplikaciju. Takvi podaci su neophodni pri otklanjanju problema u radu te su također iznimno bitni u kontekstu sigurnosti. Pomoću takvih podataka, administratori primjerice mogu nadzirati tko pristupa kojem sustavu, kako to utječe na sustav i događa li se nešto neočekivano.

Danas svaki uređaj, operacijski sustav i aplikacija generiraju dnevnike i druge podatke za nadzor te kod velikih IT sustava, analiza tih podataka može biti izrazito zahtjevna. Uobičajeno je da mali broj administratora održava stotine poslužitelja raznih vrsta te da oni redovito moraju otkrivati uzrok nekog problema koji se nalazi u jednoj od brojnih komponenti tog sustava. Iako je moguće otkriti uzrok problema čitanjem jednog po jednog zapisa dnevnika, taj proces je izrazito dugotrajan te je na taj način teško vidjeti širu sliku.

Tvrtka *Splunk* pruža rješenje za ovaj problem softverom *Splunk Free,* koji služi za centraliziranu pohranu zapisa, njihovu pretragu, analizu i vizualizaciju. *Splunk* kao tvrtka nudi još brojna druga rješenja, no fokus ovog dokumenta je softver *Splunk Free*.

Bitno je odmah napomenuti da je tehnički *Splunk Free* zapravo isti softver kao i *Splunk Enterprise*, samo s drugom licencom i ograničenim funkcionalnostima. Zato, kod pretrage dokumentacije, dokumentacija za *Splunk Enterprise* ujedno je i dokumentacija za *Splunk Free*.

Splunk Enterprise se može besplatno preuzeti i koristiti bez licence 60 dana, a nakon isteka probnog perioda, potrebno je ili kupiti licencu ili aktivirati besplatnu licencu, čime *Splunk Enterprise* postaje *Splunk Free*. Alternativno, moguće je preuzeti *Splunk Enterprise* i odmah promijeniti licencu u *Splunk Free*.

U usporedbi sa *Splunk Enterprise* licencom, *Splunk Free* ima određena ograničenja, od kojih su najvažnija sljedeća:

- moguće je prikupljati (indeksirati) samo do 500MB podataka dnevno;
- alarmi (slanje poruka administratorima nakon određenog događaja) nisu dostupni;
- nema funkcionalnosti za korisnike/uloge s različitim dozvolama (moguće je koristiti isključivo administratorsko sučelje);
- nije moguća distribuirana implementacija *Splunka*, tj. dostupan je samo tzv. *single-instance deployment*, implementacija *Splunka* na jednom poslužitelju;
- *Splunk* neće moći prosljeđivati podatke drugim aplikacijama.

Postoje dva načina na koje *Splunk Free* može prikupljati podatke od uređaja i aplikacija. *Splunk Free* može:

- samostalno prikupljati podatke od različitih sustava (primjerice putem protokola poput SNMP-a) ili
- se na sustav čije zapise prikupljamo može instalirati pomoćni alat, tzv. *Splunk forwarder*, koji će lokalno prikupljati podatke i slati ih na centralni poslužitelj gdje je instaliran *Splunk Free*.

Splunk Free, glavna centralna komponenta koji služi za prikupljanje i analizu podataka, dostupan je za operacijske sustave Windows, macOS i Linux. *Splunk forwarder*, čija je svrha prikupljanje i prosljeđivanje podataka *Splunku Free*, moguće je instalirati na veliki broj različitih operacijskih sustava, uključujući Windows, macOS, Linux, Solaris i FreeBSD. *Splunk Forwarder* instaliran na jednom operacijskom sustavu (npr. Linux) može bez problema slati podatke *Splunku Free* koji je instaliran na drugom operacijskom sustavu (npr. Windows).

Ovaj dokument će opisati:

- osnovni postupak instalacije i konfiguracije *Splunka Free* na jednom poslužitelju te *Splunk Forwardera* na drugom poslužitelju,
- osnovno pretraživanje, analizu i vizualizaciju prikupljenih podataka.

Splunk Free i *Splunk forwarder* bit će instalirani na poslužitelje s operacijskim sustavom Windows Server 2019, no instalacija, konfiguracija i korištenje su većinom isti neovisno o platformi.

2 Instalacija alata *Splunk Free*

Ovo poglavlje je podijeljeno na dva dijela:

- instalacija alata *Splunk Free i*
- instalacija alata *Splunk Universal Forwarder*

Alat *Splunk Free* bit će instaliran na jedno računalo, a alat *Splunk Universal Forwarder* na drugo računalo, na istoj mreži.

2.1 Instalacija alata *Splunk Free*

Splunk Enterprise sustav se u složenijim okolinama može razdvojiti na više elemenata, kao što su *indexer* i *search head.* Kod takvih implementacija, svaki element sustava (svaka *Splunk* instanca) se specijalizira za obavljanje jednog zadataka, tako da primjerice jedna instanca obavlja samo pretragu i analizu (*search head*), dok druga obavlja samo primanje podataka i pohranu (*indexer*).

Kao što je napomenuto u uvodu, za razliku od *Splunka Enterprise*, nije moguće distribuirano implementirati *Splunk Free*. Drugim riječima, *Splunk Free* je moguće instalirati samo na jednom poslužitelju koji će tada obavljati i pohranu i analizu podataka (tzv. *single-instance deployment*).

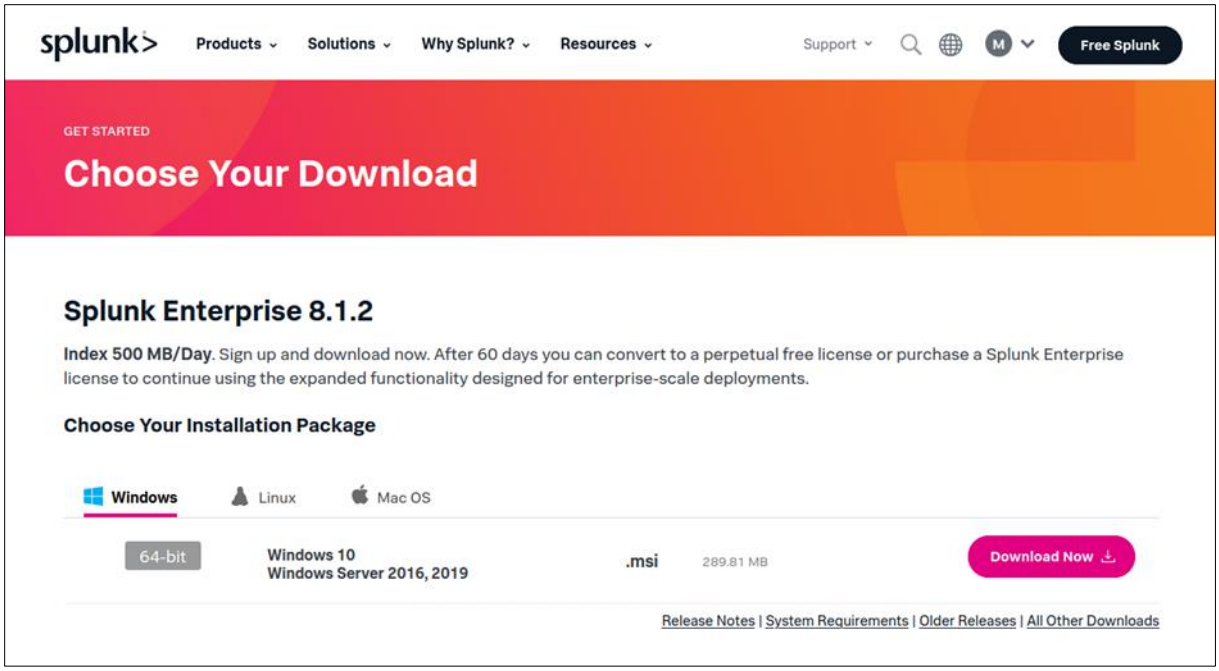
Službeni preporučeni minimalni zahtjevi na računalo za *single-instance deployment* su:

- x86 64 procesorska arhitektura;
- 12 fizičkih CPU jezgri, odnosno 24 virtualne CPU jezgre s taktom od 2GHz ili više;
- 12 GB RAM-a;
- 1 Gb/s mrežno sučelje.

Još jedan bitan faktor je podatkovni prostor, no to prvenstveno ovisi o količini prikupljenih zapisa te o trajanju čuvanja pohranjenih podataka.

Ovi službeni zahtjevi namijenjeni su produkcijskim okruženjima, no *Splunk Free* može funkcionirati i s manje resursa. Za svrhu ovog dokumenta te za svrhu učenja *Splunka Free*, dovoljno je računalo s dvije CPU jezgre, 4 GB RAM-a i 40 GB podatkovnog prostora.

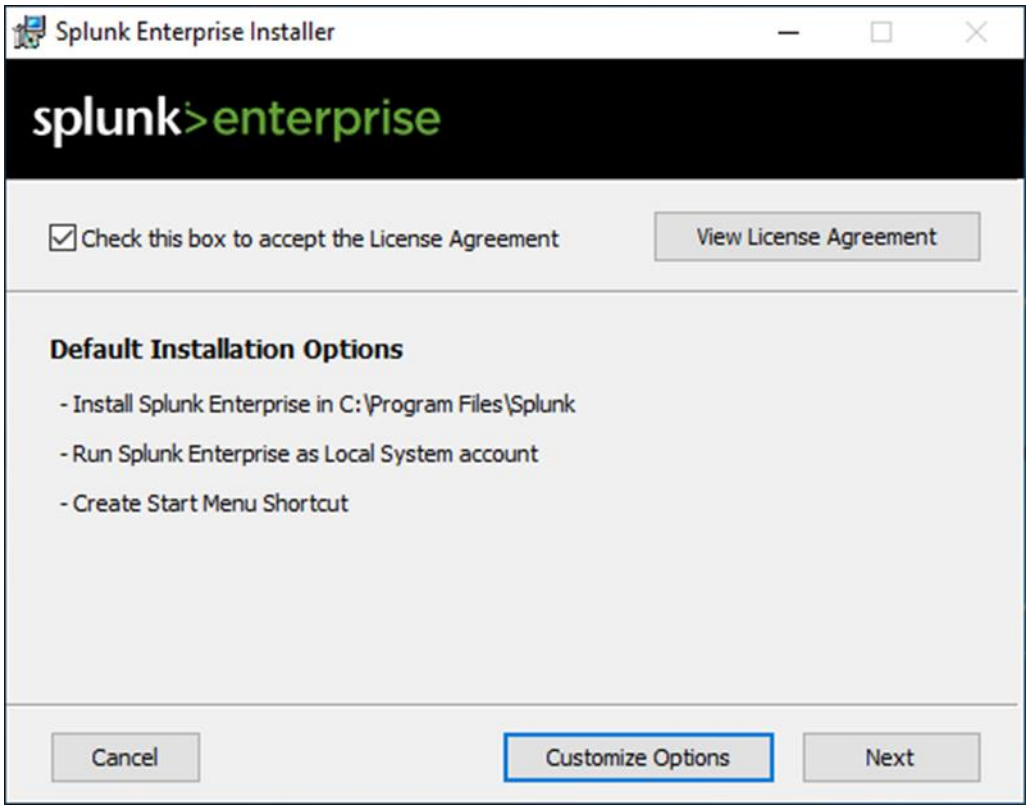
Prije početka instalacije, treba se besplatno registrirati na službenim *Splunk* web stranicama. Nakon registracije treba preuzeti instalacijsku datoteku za *Splunk Enterprise* (to je ujedno i instalacijska datoteka za *Splunk Free*). Kako ćemo instalirati *Splunk* na Windows poslužitelj, odabiremo MSI datoteku.



Slika 1 – Izbornik *Splunk Enterprise* verzija na službenim *Splunk* stranicama

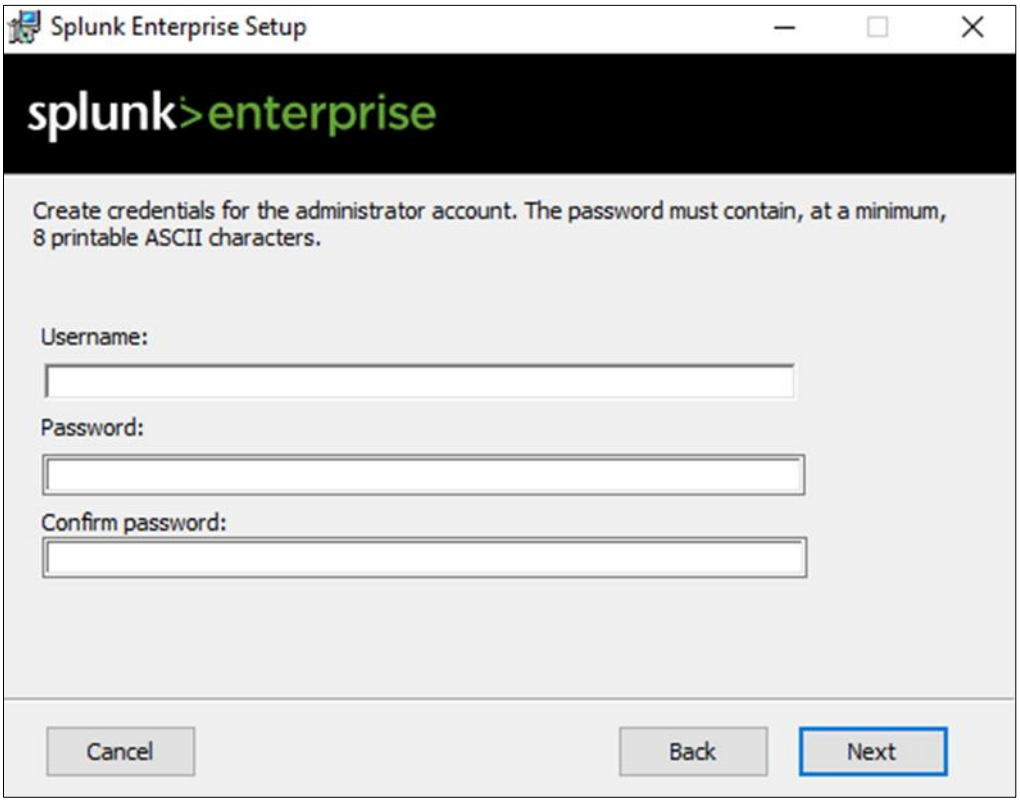
Za vrijeme pisanja ovog dokumenta, najnovija *Splunk Enterprise* odnosno *Splunk Free* verzija bila je 8.1.2. Postupak instalacije za buduće verzije može varirati, no načelno razlike ne bi smjele biti značajne.

Nakon preuzimanja, instalacijsku datoteku treba pokrenuti. Instalacijski alat će pitati gdje na poslužitelju treba instalirati *Splunk Enterprise* i pod kojim korisničkim računom, no za svrhu osnovne instalacije to nije potrebno mijenjati. Jedino je bitno odabrati gornji potvrdni okvir (engl. *checkbox*) s kojim potvrđujemo da se slažemo s uvjetima korištenja, te kliknuti *Next*.



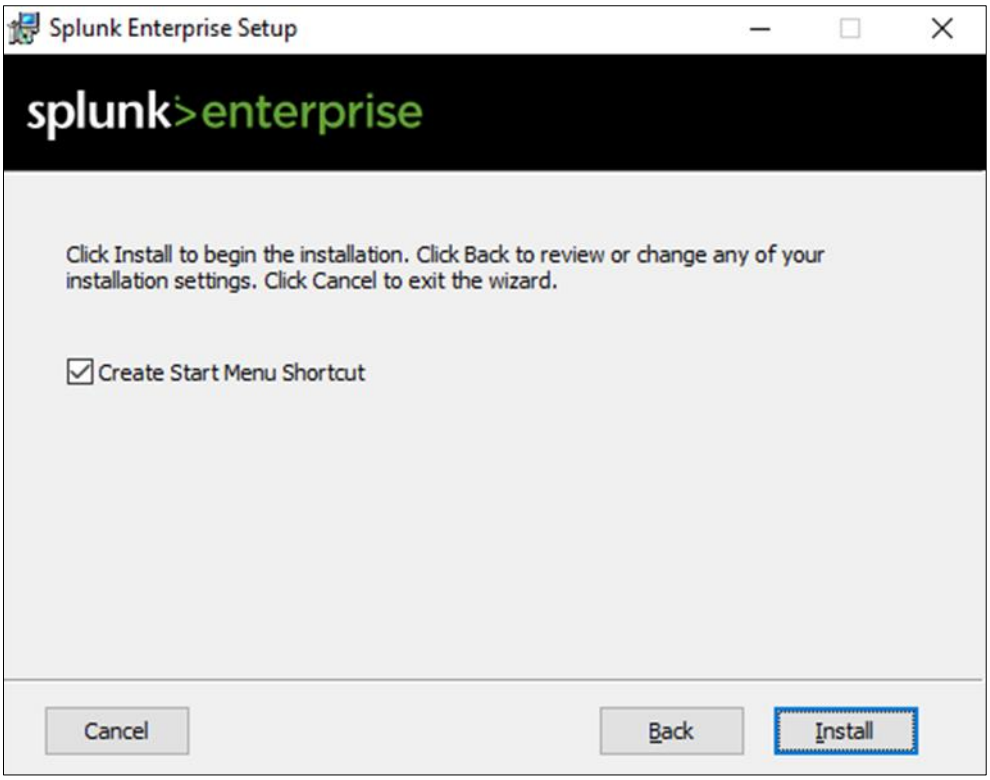
Slika 2 – Prvi korak instalacije

U idućem koraku (prikazanom na slici 3) potrebno je definirati administratorski korisnički račun kojim se kasnije pristupa sučelju *Splunk-a* nakon završetka instalacije.



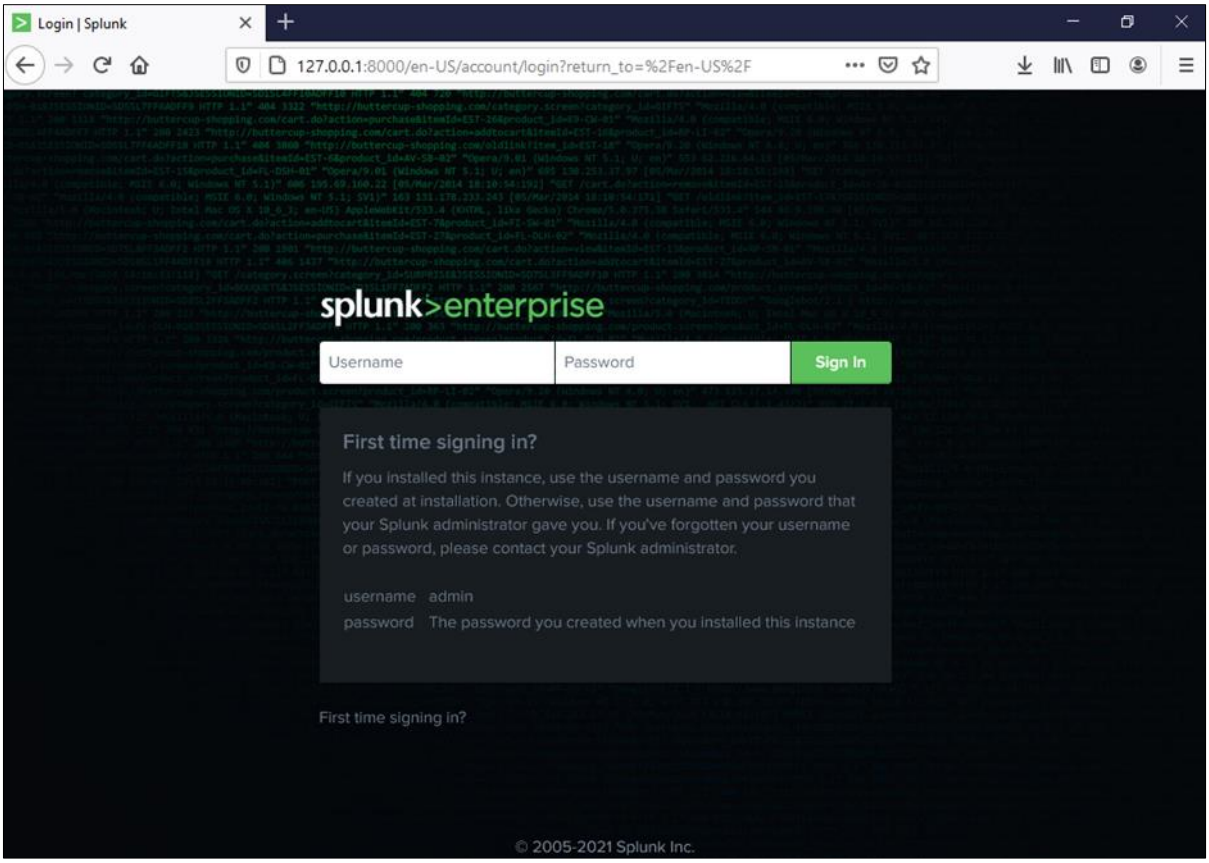
Slika 3 – Unos imena i lozinke administratorskog korisničkog računa

Idući korak instalacije samo pita želimo li prečicu za pokretanje *Splunka*. Dovoljno je započeti instalaciju klikom na *Install*.



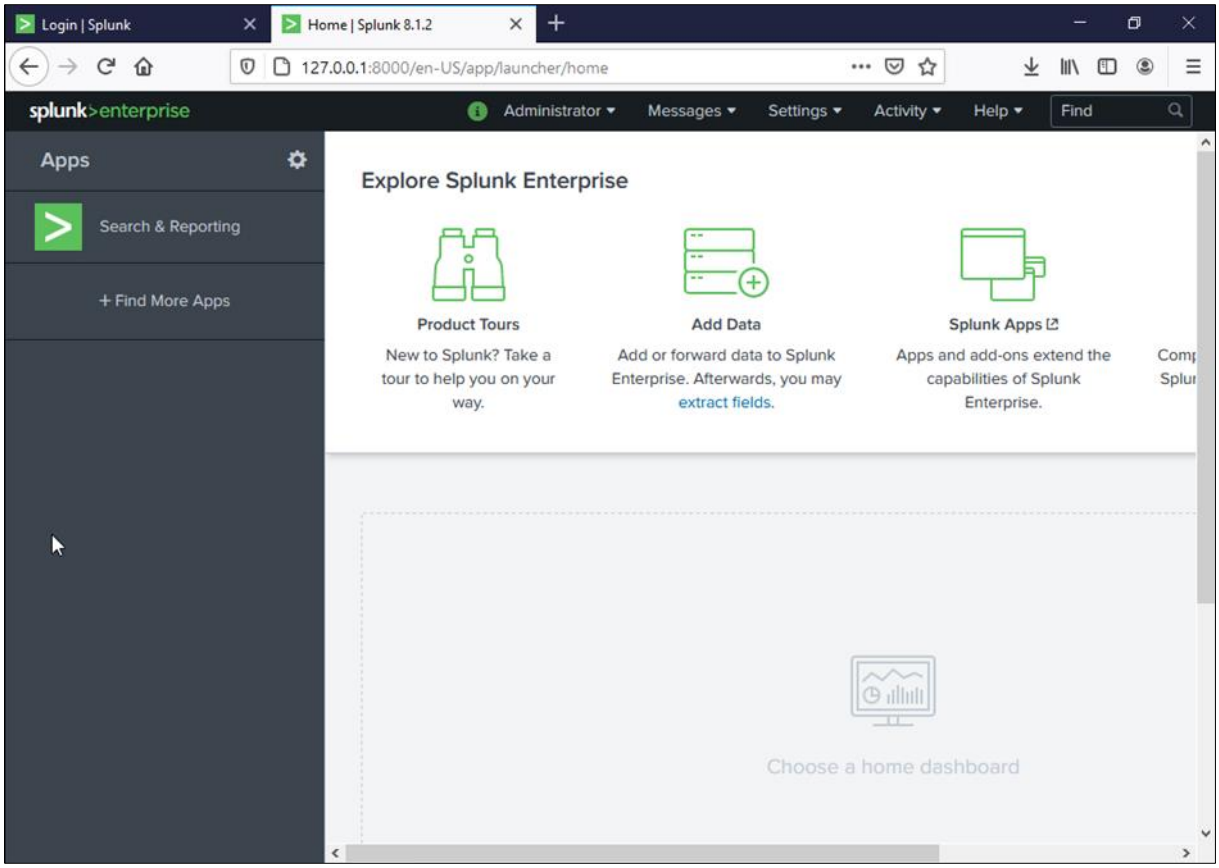
Slika 4 – Završni izbornik prije početka instalacije

Nakon završetka instalacije, automatski će se otvoriti lokalni web preglednik koji će otvoriti adresu *Splunk* sučelja. U slučaju da se to nije dogodilo, web sučelju se može pristupiti s računala na kojem smo odradili instalaciju na URL-u: http://127.0.0.1:8000/



Slika 5 – Obrazac za prijavu u *Splunk* web sučelje

Treba unijeti podatke za administratorski korisnički račun koje smo naveli tijekom instalacije. Nakon uspješne prijave, otvara se korisničko sučelje.



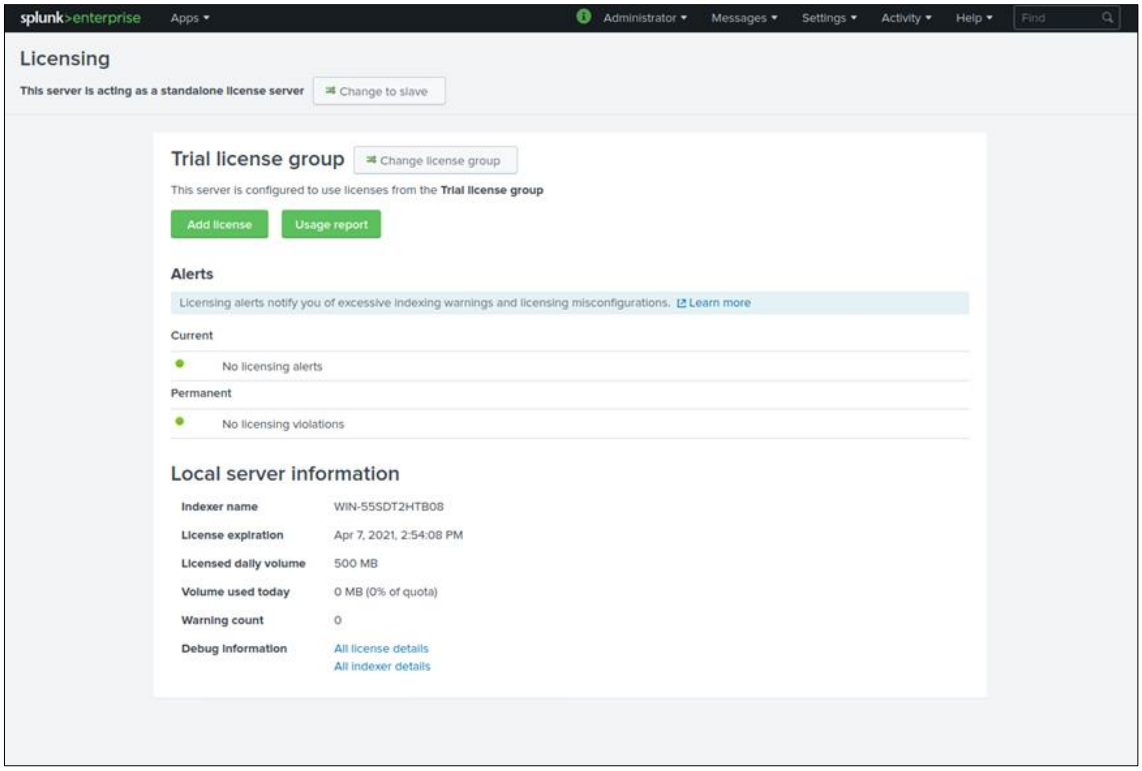
Slika 6 – *Splunk* korisničko sučelje

Početna konfiguracija vatrozida (engl. *firewall*) na operacijskom sustavu Windows Server 2019 zabranjuje udaljen pristupi na TCP priključak (engl. *port*) 8000 na kojemu *Splunk* web sučelje očekuje veze. Za udaljeni pristup *Splunk* web sučelju potrebno je konfigurirati vatrozid tako da dopušta spajanje na taj priključak. Iz sigurnosnih razloga, poželjno je preko vatrozida dopustiti pristup *Splunk* web sučelju isključivo s IP adresa administratora.

Također, u konfiguraciji vatrozida je potrebno omogućiti i komunikaciju *Splunk Forwader* agenata s centralnim *Splunk Free* poslužiteljem. Ta komunikacija se podrazumijevano (engl. *default*) ostvaruje preko TCP priključka 9997. U ovom primjeru je na poslužitelju gdje je *Splunk Free* instaliran u vatrozidu dopušteno spajanje i na taj priključak.

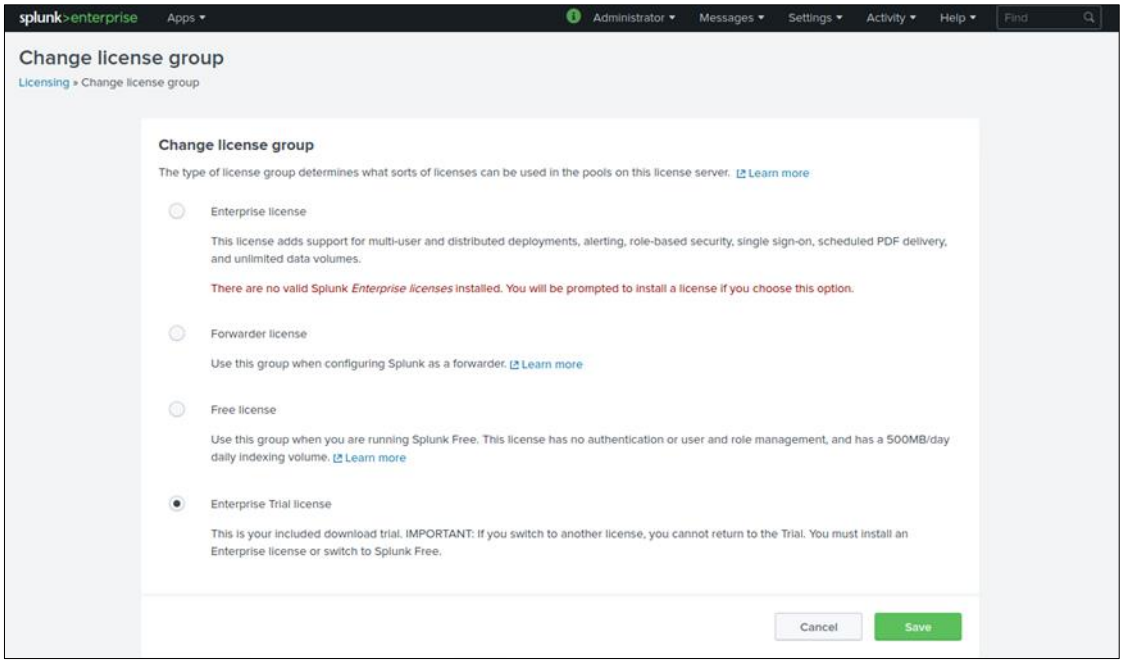
Sada je kroz instalaciju *Splunka* zapravo aktiviran probni period (engl. *trial*) *Splunk Enterprise* licence. Nakon isteka probnog perioda, *Splunk* će se automatski prebaciti na *Splunk Free* licencu čime će se ograničiti funkcionalnosti nabrojane u uvodu ovog dokumenta.

Moguće je i prije isteka probnog perioda prebaciti se na *Splunk Free* licencu. To ostvarujemo putem *Splunkovog* web sučelja. Potrebno je prijaviti se s administratorskim korisničkim računom, te odabrati *Settings* → *Licensing*. Na sučelju prikazanom na slici 7, potrebno je odabrati *Change license group*.



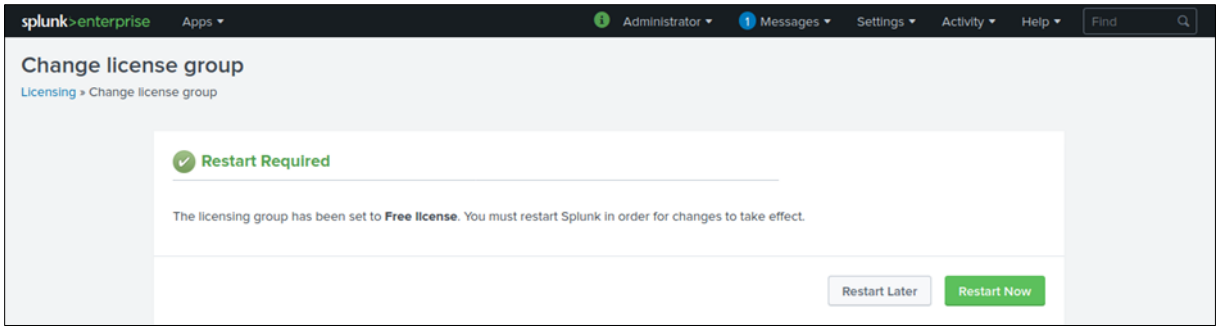
Slika 7 – Konfiguracija licenci na *Splunk* sučelju

Na sučelju prikazanom na slici 8, potrebno je odabrati *Free license* te kliknuti *Save*.



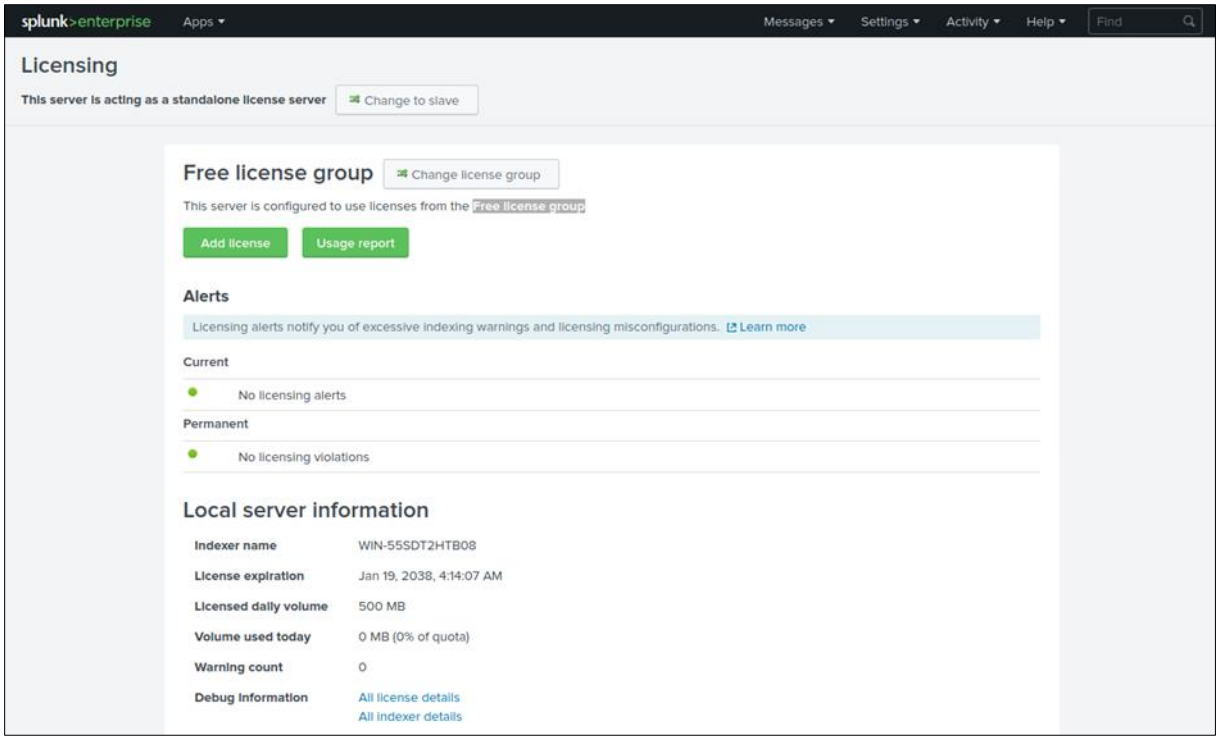
Slika 8 – Izbornik promjene licenci na *Splunk* sučelju

Za promjenu licence potrebno je ponovo pokrenuti *Splunk* servis. Idući prozor nas pita želimo li to učiniti odmah. Za ponovno pokretanje odmah treba odabrati *Restart Now*.



Slika 9 – Prozor ponovnog pokretanja *Splunk* servisa nakon promjene licence

Nakon ponovnog pokretanja i prijave, ako u sučelju ponovo odaberemo *Settings* → *Licensing*, trebalo bi sada pisati da je konfigurirana licenca *Free license group*, što potvrđuje uspješno prebacivanje na besplatnu licencu, odnosno na *Splunk Free*.



Slika 10 – Potvrda uspješnog prebacivanja *Splunk Enterprise* u *Splunk Free*

2.2 Instalacija alata *Splunk universal forwarder*

U uvodu je već spomenuto kako *Splunk forwarder* služi za prosljeđivanje podataka centralnom *Splunk Free* servisu. Zapravo postoje tri vrste *forwardera*: *universal*, *heavy* i *light forwarder*. *Heavy* i *light* inačice *forwardera* su zapravo puni *Splunk Enterprise* servisi s određenim funkcionalnostima isključenim. *Splunk Universal Forwader* je program namijenjen isključivo prosljeđivanju podataka, te se preporučuje korištenje *Universal Forwardera*, osim ako nisu potrebne napredne funkcionalnosti cijelog *Splunk* servisa.

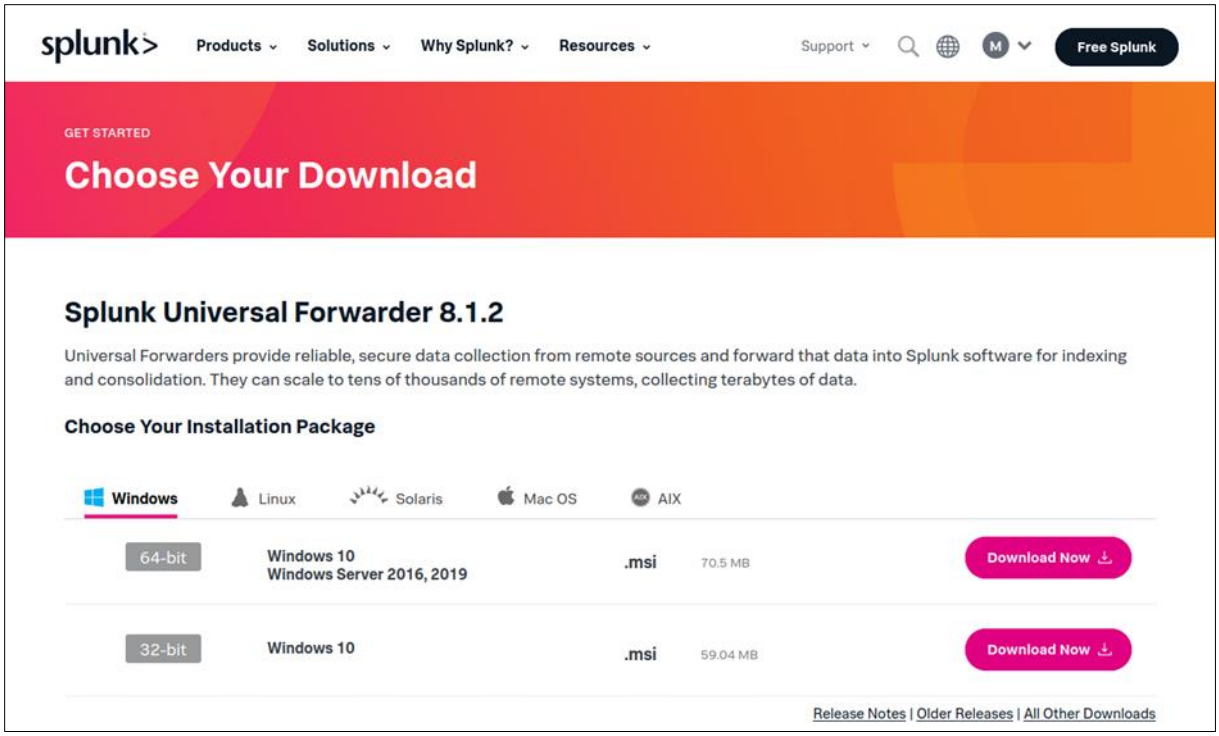
Prije instalacije bilo kojeg *Splunk forwadera* na uređaj s kojega želimo prikupljati podatke, treba odlučiti je li nam uopće potreban *forwader*. Iako je uobičajena preporuka da se koristi forwader, ponekada to nije potrebno. Primjerice, ako samo trebamo prikupljati osnovne podatke s nekog mrežnog uređaja, onda može biti dovoljno konfigurirati prikupljanje podataka putem SNMP-a ili udaljeno slanje *syslog* dnevnika na centralni *Splunk* poslužitelj. No u većini uobičajenih slučajeva – prikupljanje dnevnika Windows i Linux poslužitelja, prikupljanje dnevnika aplikacija, prikupljanje metrika poput postotka korištenosti RAM-a ili broja HTTP zahtjeva po sekundi – preporučuje se korištenje *forwardera*.

Također, korištenje *forwadera* ima dodatne prednosti. *Splunk Universal Forwarder* prati koje zapise je uspješno proslijedio. U slučaju da se prekine komunikacija između *forwardera* i centralnog *Splunk* servisa, *forwarder* će zapamtiti koji zapisi nisu uspješno poslani, te će ih proslijediti nakon ponovne uspostave komunikacije. S ovim načinom rada zapisi se puno teže mogu izgubiti. *Splunk Universal Forwarder* također može pokretati razne skripte ili programe, te može njihove izlazne informacije prosljeđivati kao zapise ili metrike.

U ovom će poglavlju biti opisana instalacija *Splunk Universal Forwardera* na poslužitelj s operacijskim sustavom *Windows Server 2019*. Taj poslužitelj je odvojen od poslužitelja na kojega je upravo instaliran *Splunk Free*, ali se nalazi na istoj mreži. Prvi poslužitelj (*Splunk Free*) je centralno mjesto prikupljanja i analize podataka, dok je drugi poslužitelj (*Splunk forwarder*) predmet nadzora.

Kao što je objašnjeno u uvodu, *Splunk Universal Forwarder* može se instalirati i na računala s drugim operacijskim sustava, uključujući Windows, macOS, Linux, Solaris i FreeBSD. Proces konfiguracije *Universal Forwadera* je u načelu isti (iste je parametre potrebno konfigurirati), no za Windows je dostupna instalacija i konfiguracija kroz grafičko sučelje, dok je na drugim operacijskim sustavima u pravilu ekvivalentan postupak potrebno napraviti kroz sučelje naredbene linije (engl. *command line interface*, CLI) i konfiguracijsku datoteku. Za *Splunk* početnike lakše je prvo instalirati *forwarder* na Windows računala koja trebaju biti pod nadzorom, pa onda kada proces instalacije i konfiguracije *forwadera* bude načelno jasan, isto napraviti i na računalima s drugim operacijskim sustavima.

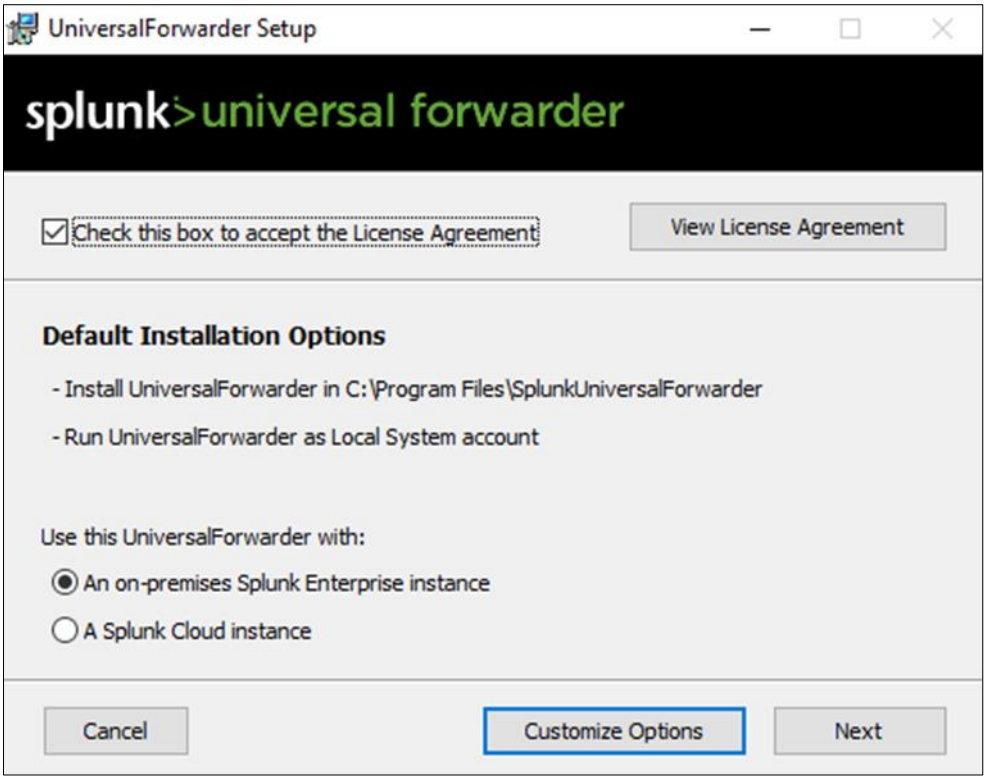
Za instalaciju *Splunk Universal Forwardera* potrebno je najprije preuzeti instalacijsku datoteku. Moguće je pristupiti stranicama za preuzimanje *forwardera* putem istog korisničkog računa kojega smo koristili u prijašnjim koracima. S obzirom na to da u ovom primjeru koristimo operacijski sustav Windows Server 2019, odabiremo odgovarajuću MSI instalacijsku datoteku.



Slika 11 – Izbornik *Splunk Universal Forwarder* verzija na službenim *Splunk* stranicama

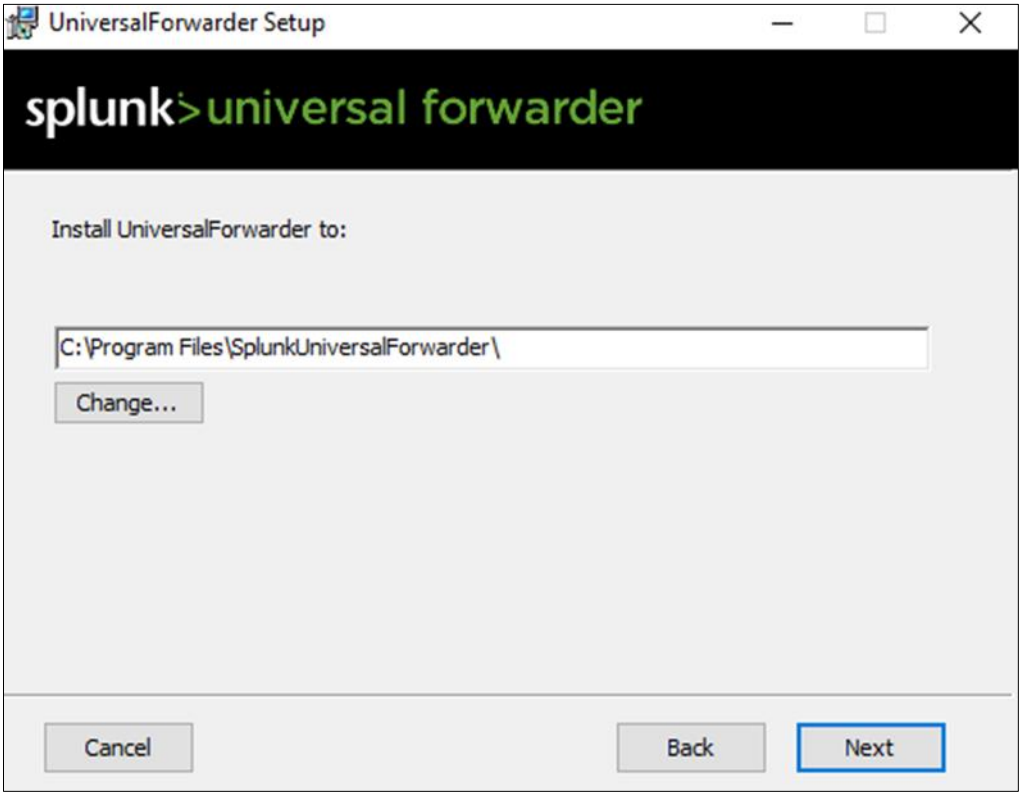
Nakon preuzimanja MSI datoteke, potrebno ju je samo pokrenuti. Na slici 12 prikazan je prvi izbornik nakon pokretanja instalacije. Ovdje je potrebno u gornjem potvrdnom okviru prihvatiti uvjete korištenja, te niže odabrati *on-premises* tip instalacije.

Zatim treba odabrati *Customize Options* (a ne *Next*) kako bismo kroz grafičko sučelje odmah konfigurirali parametre *forwadera*.



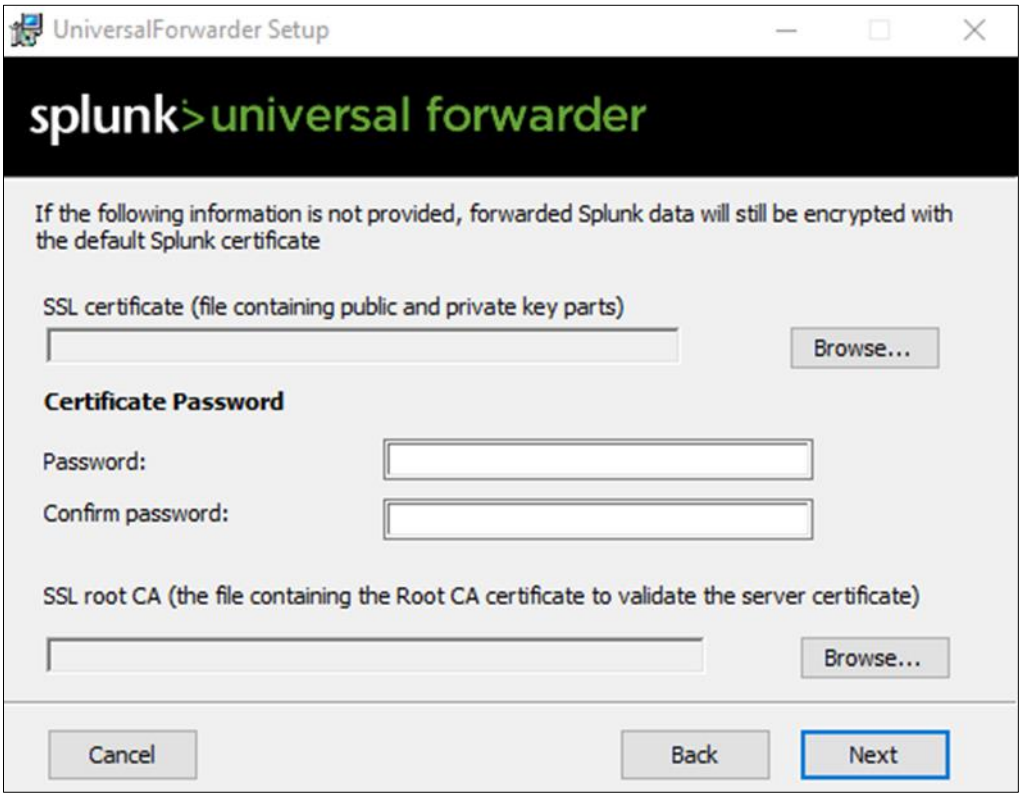
Slika 12 – Početni prozor *Splunk Universal Forwarder* instalacije

Idući korak instalacije pita gdje treba instalirati *Forwarder*. Dovoljno je unijeti putanju (ili ostaviti zadanu putanju) pa odabrati *Next*.



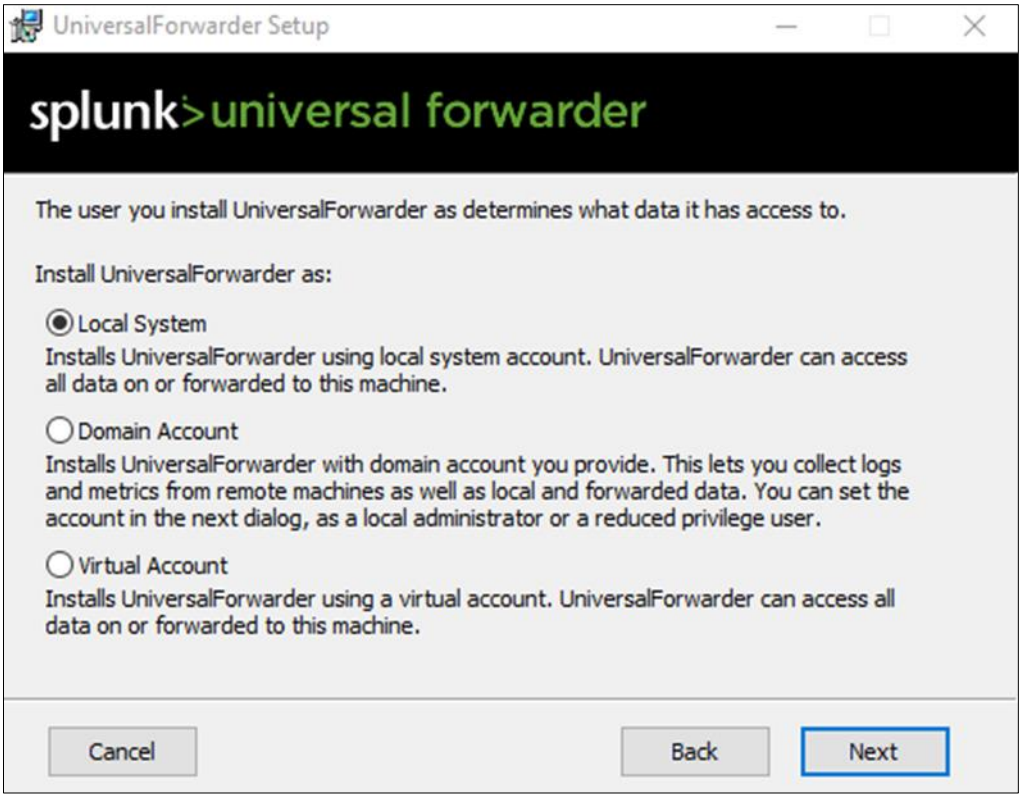
Slika 13 – Odabir instalacijske putanje

Na prozoru prikazanom na slici 14 instalacija pita želimo li koristiti vlastite SSL certifikate. Za višu razinu sigurnosti bilo bi bolje konfigurirati vlastite certifikate, no za jednostavniju instalaciju, moguće je sva prikazana polja ostaviti prazna, pa odabrati *Next*.



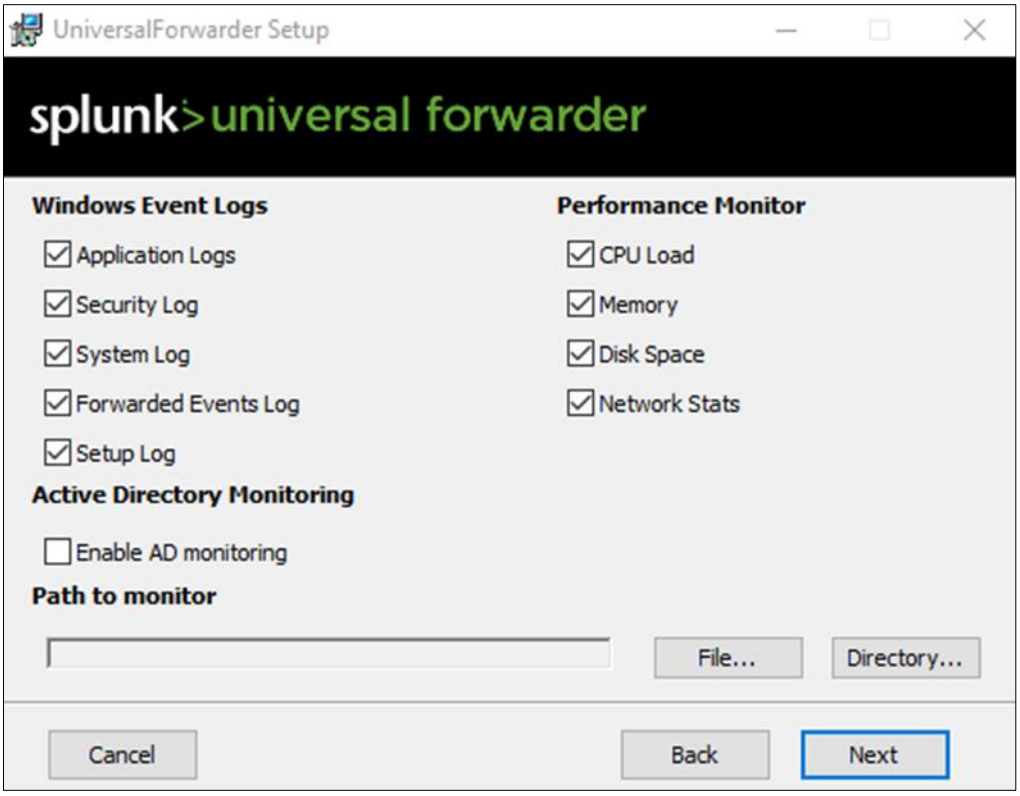
Slika 14 – konfiguracija SSL certifikata

U idućem koraku biramo korisnički račun pod kojim će se *Forwarder* instalirati. U složenijim okruženjima, npr. u mrežama gdje se koristi *Active Directory*, ima smisla odabrati domenski korisnički račun koji ima sva potrebna prava, no u jednostavnijim okruženjima kao u ovom primjeru dovoljno je odabrati korisnički račun *Local System* i pritisnuti *Next*.



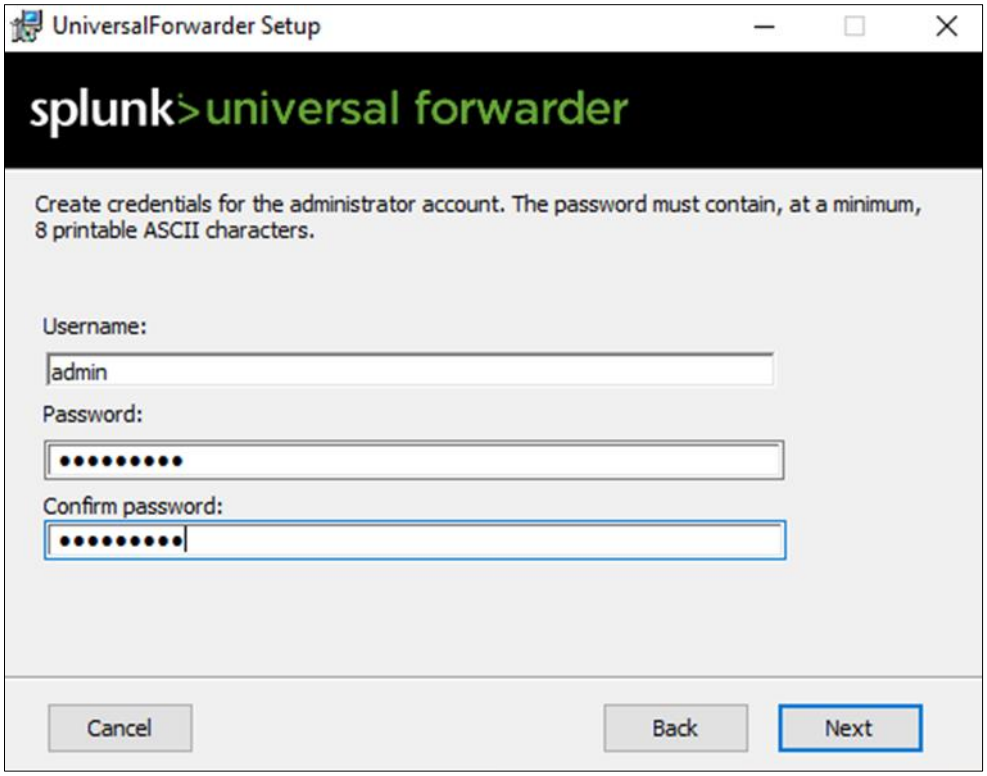
Slika 15 – Odabir korisničkog računa pod kojim će se instalirati *Forwarder*

Na prozoru prikazanom na slici 16 instalacija pita koje Windows dnevnike i metrike treba prosljeđivati. U ovom primjeru odabrani su svi Windows dnevnici (engl. *Windows Event Logs*) i sve ponuđene metrike performansi (CPU, RAM, disk, mreža). Sve postavke *forwardera* mogu se promijeniti i nakon završetka instalacije, no lakše ih je konfigurirati odmah tijekom instalacije kroz grafičko sučelje. Nakon što su odabrani podaci za nadzor i prosljeđivanje, treba pritisnuti *Next*.



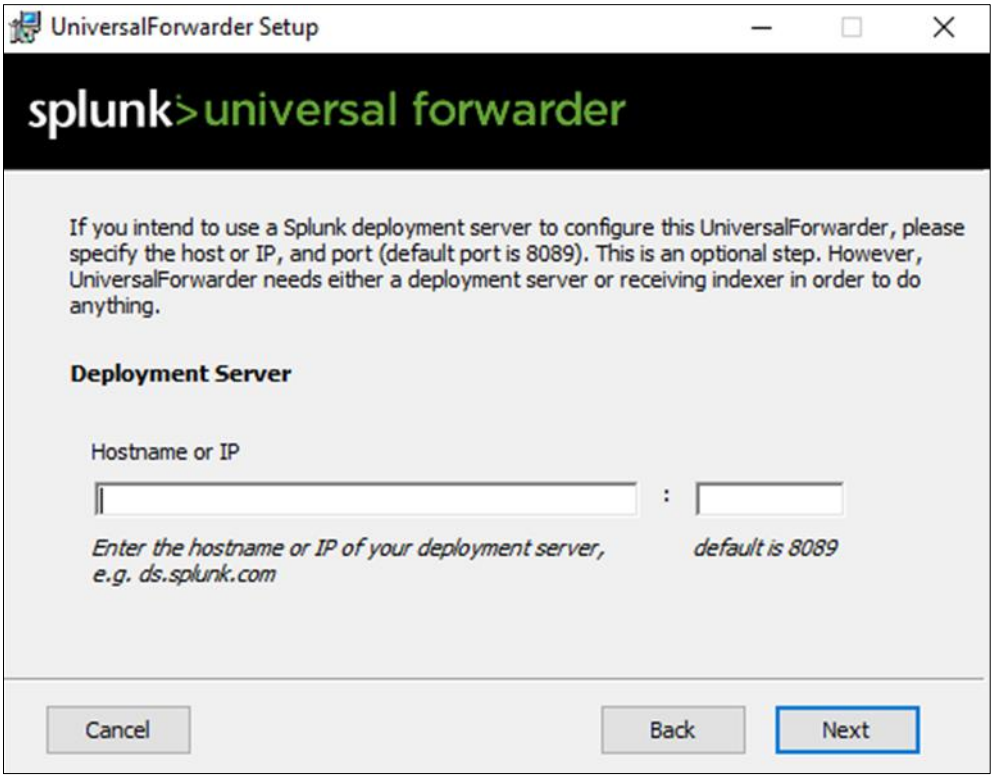
Slika 16 – Odabir podataka koje će *Forwarder* prosljeđivati

U idućem koraku potrebno je unijeti korisničko ime i lozinku koji će se koristiti za eventualno naknadno administriranje *Splunk Forwardera*.



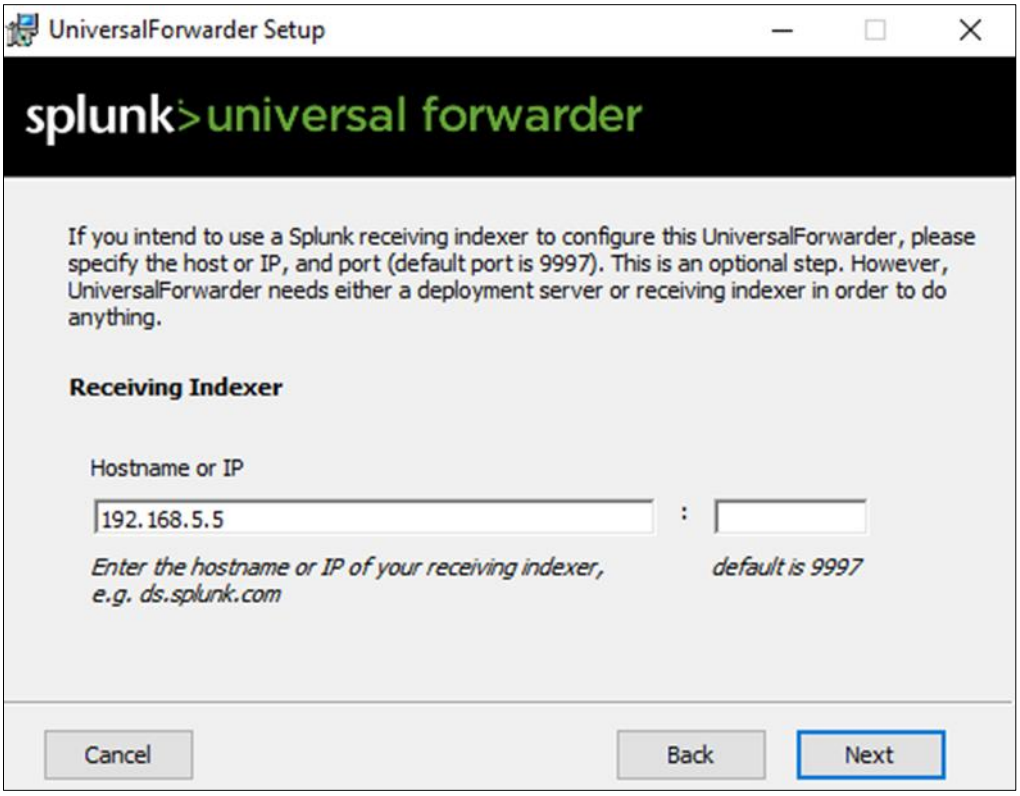
Slika 17 – Unos imena i lozinke korisničkog računa za administriranje *Splunk Forwardera*

U idućem koraku, prikazanom na slici 18, *forwarder* instalacija pita gdje se nalazi *Deployment server*. To je napredni način rada *Splunka* putem kojeg se lako može administrirati veliki broj *Forwardera*. Za osnovnu instalaciju *forwardera* dovoljno je ostaviti sva polja prazna i pritisnuti *Next*.



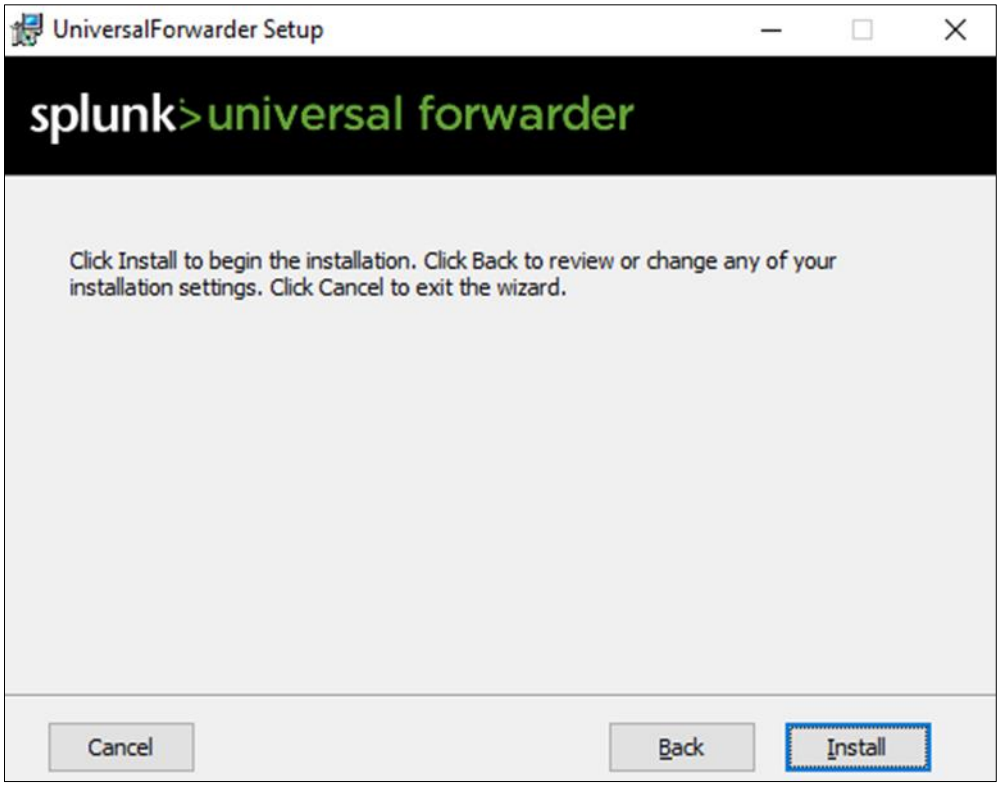
Slika 18 – Unos IP adrese *Splunk Deployment* instance

Kako ne koristimo *Deployment Server,* potrebno je *forwarderu* reći gdje će prosljeđivati zapise. Na koraku prikazanom na slici 19 potrebno je unijeti IP adresu glavne *Splunk Free* instance koju smo instalirali u prijašnjim koracima. U našem je slučaju to IP adresa *192.168.5.5*. Zadani priključak (engl. *default port*) ne treba mijenjati, pa to polje ostavljamo prazno.



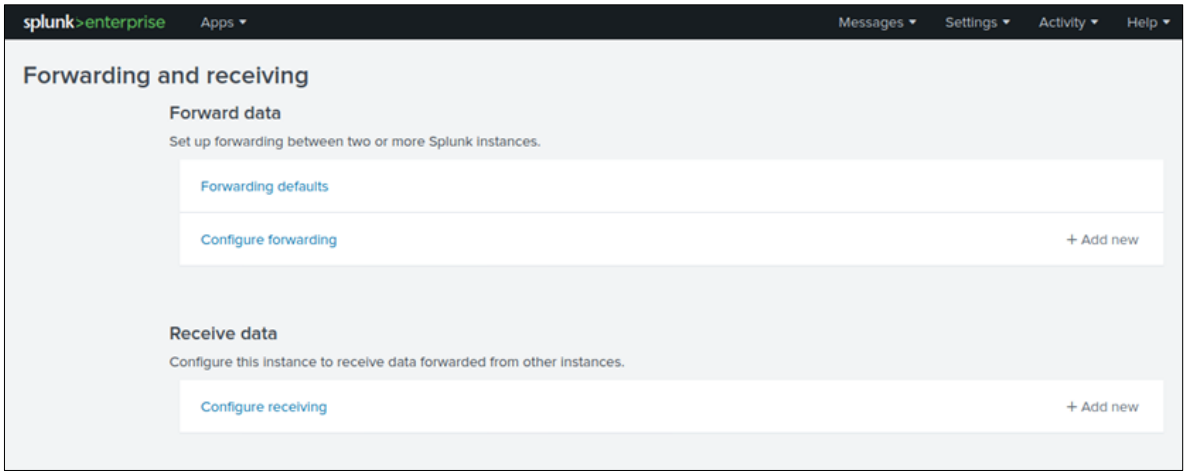
Slika 19 – Unos IP adrese centralne *Splunk Free* instance

Na zadnjem koraku je potrebno samo pritisnuti *Install*.



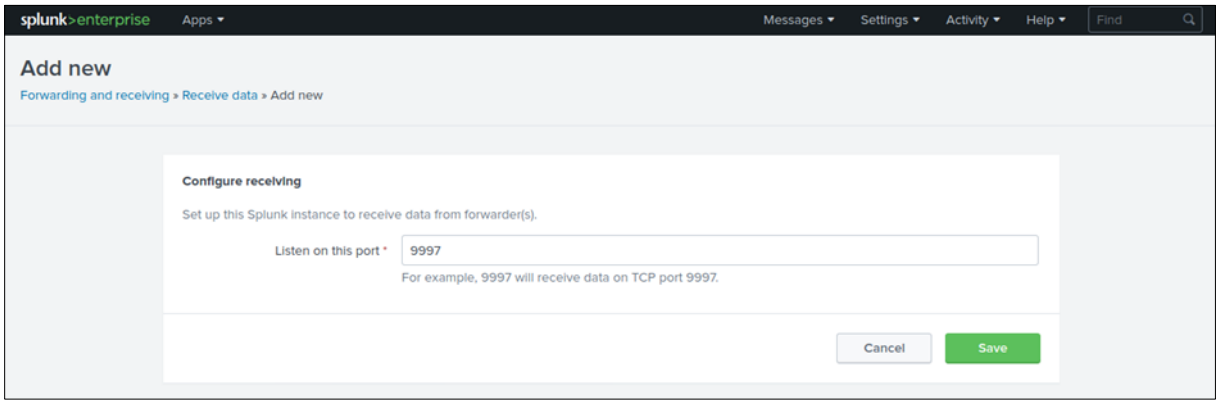
Slika 20 – Završni korak prije početka *Splunk Universal Forwarder* instalacije

Nakon što se *Splunk Universal Forwarder* instalira, potrebno je na *Splunk Free* korisničkom sučelju omogućiti primanje zapisa. To se ostvaruje otvaranjem *Settings* → *Forwarding and receiving*. Na izborniku prikazanom na slici 21, potrebno je desno na polju *Configure receiving* odabrati *+ Add new*. Otvoriti će se novi prozor.



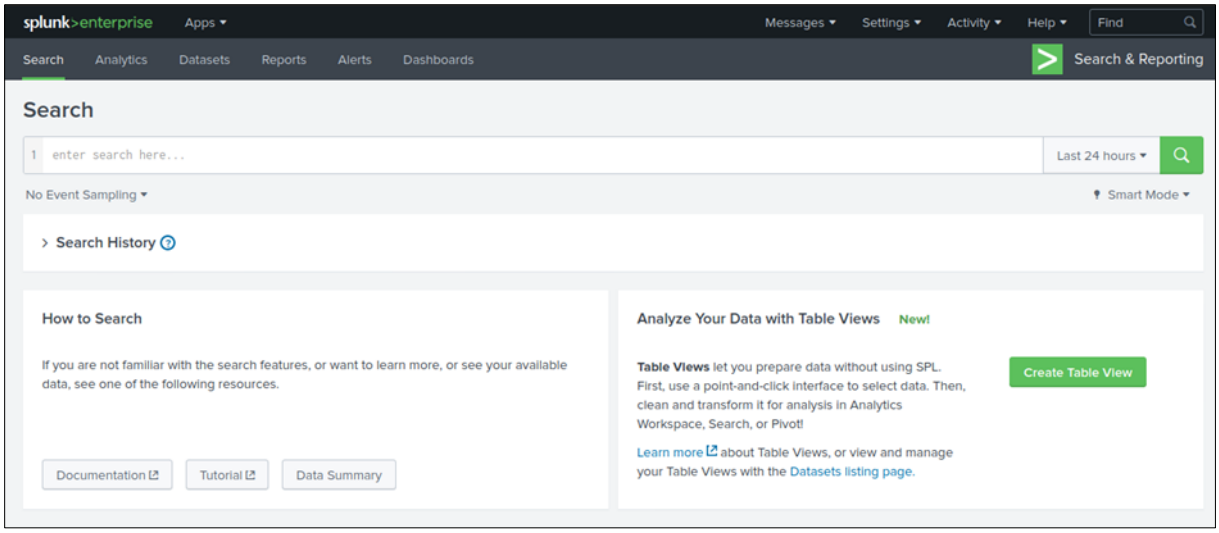
Slika 21 – Konfiguracija dohvata zapisa na *Splunk Free* instanci

Kako smo *Forwardera* konfigurirali da šalje zapise na zadani TCP priključak 9997, potrebno ga je ovdje navesti te pritisnuti *Save*.



Slika 22 – Dodavanje TCP priključka za primanje udaljenih zapisa na *Splunk Free* instanci

Sada bi bilo dobro provjeriti stanje aktivnih *forwardera*, tj. koji sve *forwarderi* šalju podatke na *Splunk Free*. Kako bismo to provjerili, na *Splunk Free* sučelju, na vrhu ekrana treba odabrati *Apps*, pa *Search & reporting*. Otvoriti će se glavni prozor pretrage zapisa.

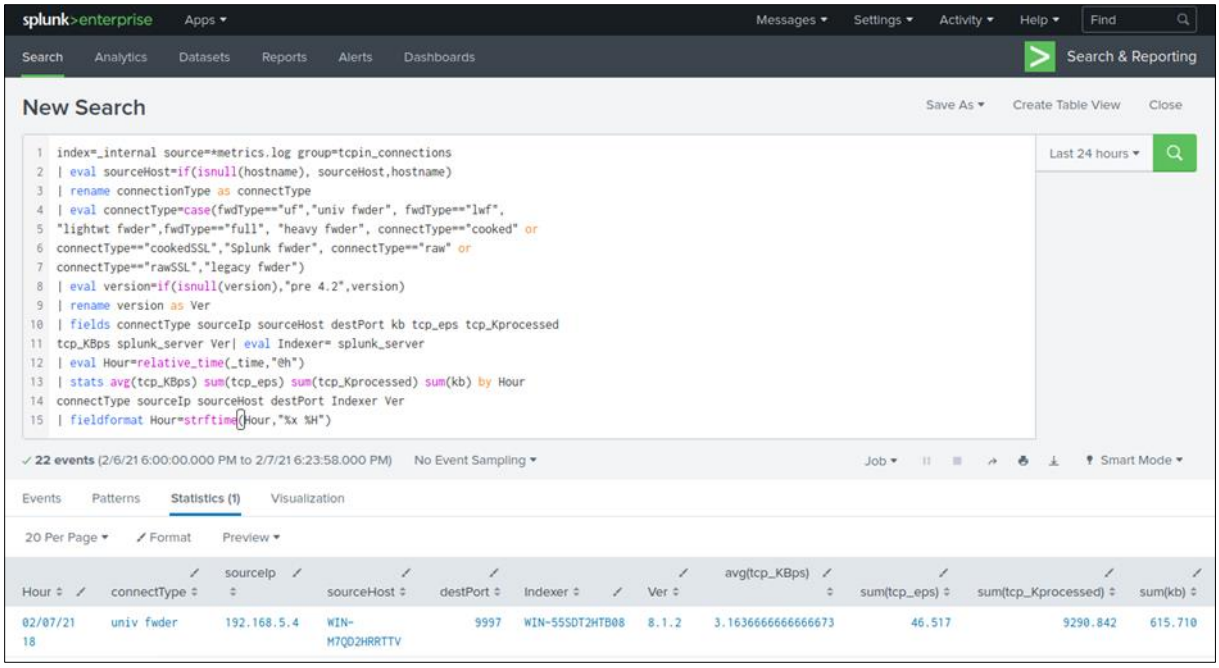


Slika 23 – Glavni prozor pretrage na *Splunk Free* sučelju

Na prozoru prikazanom na slici 23 vidimo glavno polje pretrage zapisa. U *Splunk Free* bazi podataka se nalaze i podaci o spojenim *forwarderima*, pa je kroz sučelje za pretragu moguće vidjeti je li novo instalirani *forwarder* aktivan. Kako bismo to vidjeli, u *Search* polje treba unijeti sljedeći upit za pretragu:

```
index=_internal source=*metrics.log group=tcpin_connections
| eval sourceHost=if(isnull(hostname), sourceHost,hostname)
| rename connectionType as connectType
| eval connectType=case(fwdType=="uf","univ fwder", fwdType=="lwf", "lightwt
fwder",fwdType=="full", "heavy fwder", connectType=="cooked" or
connectType=="cookedSSL","Splunk fwder", connectType=="raw" or
connectType=="rawSSL","legacy fwder")
| eval version=if(isnull(version),"pre 4.2",version)
| rename version as Ver
| fields connectType sourceIp sourceHost destPort kb tcp_eps tcp_Kprocessed
tcp_KBps splunk_server Ver| eval Indexer= splunk_server
| eval Hour=relative_time(_time,"@h")
| stats avg(tcp_KBps) sum(tcp_eps) sum(tcp_Kprocessed) sum(kb) by Hour connectType
sourceIp sourceHost destPort Indexer Ver
| fieldformat Hour=strftime(Hour,"%x %H")
```

Za sada je cilj samo otkriti koji su *forwarderi* spojeni, nije potrebno razumjeti ovaj složeni upit (sljedeće poglavlje objašnjava kako formirati upite). U ovom slučaju nas samo zanimaju izlazne vrijednosti ovog upita, koje su prikazane na slici 24.



Slika 24 – Prikaz upita vezanog za *Splunk Forwardere*

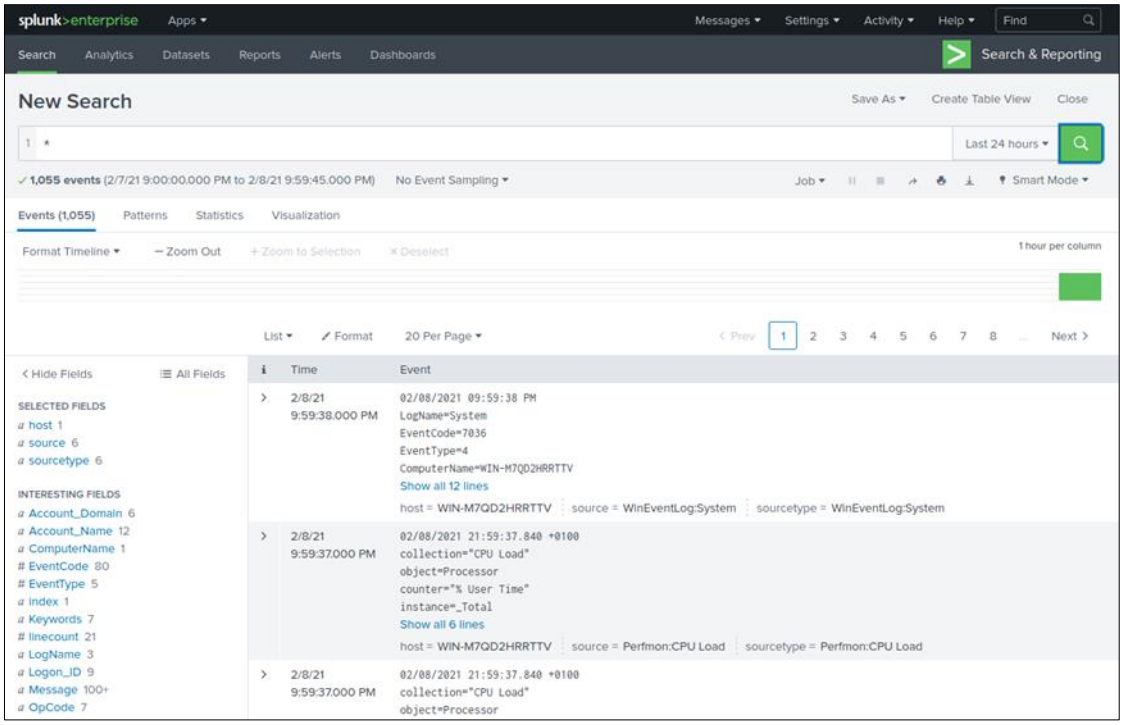
Na slici 24 vidimo da je naš upit vratio jedan rezultat. Pronašao je naš aktivni *Splunk Universal Forwarder* instaliran.

na IP adresi *192.168.5.4* na poslužitelju imena *WIN-M7QD2HRRTTV*, verzije *8.1.2*. To potvrđuje da je instalacija *Splunk Universal Forwardera* uspješno završila.

Još je korisno provjeriti prosljeđuje li *forwarder* uspješno zapise. To je lako provjeriti na istoj stranici u *Splunk* sučelju, gdje u polje pretrage umjesto prikazanog upita treba upisati samo „*" (znak zvjezdice, bez navodnika). Taj upit traži od *Splunka* da prikaže sve zapise koje ima.

Na slici 25 prikazani su rezultati upita. Vidimo da su dostupni razni zapisi prikupljeni s poslužitelja imena *WIN-M7QD2HRRTTV*, što je trenutno jedini instalirani *forwarder* čije smo informacije vidjeli na slici 24.

Ovime je potvrđeno da su *Splunk Free* i udaljeni *Splunk Universal Forwarder* uspješno instalirani te da prikupljanje zapisa radi.



Slika 25 – Prikaz *Splunk* upita koji prikazuje sve zapise

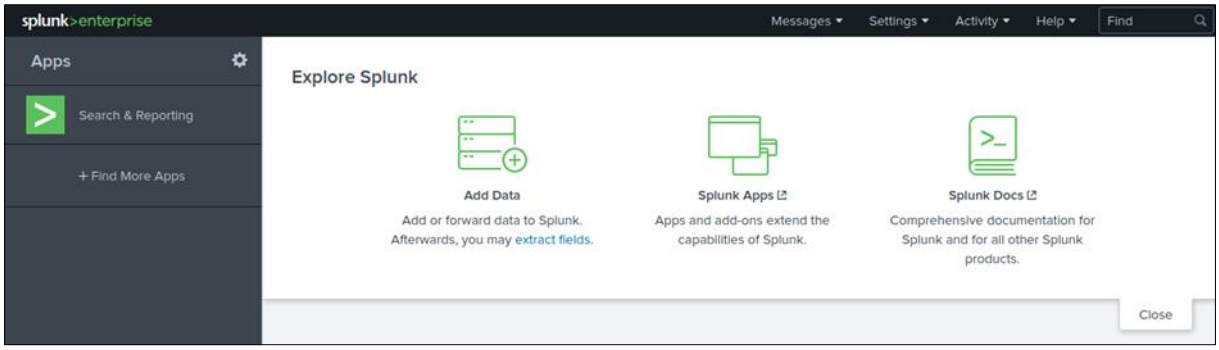
3 Osnovno korištenje alata *Splunk Free*

Svrha ovog poglavlja je demonstrirati osnove pretraživanja, analize i vizualizacije prikupljenih podataka u alatu *Splunk Free*. Prethodno instalirani *forwarder* već šalje dnevnike i metrike s Windows sustava na kojeg je instaliran, no to je i dalje relativno mala količina podataka sa samo jednog računala koja ne odgovara razmjeru podataka iz stvarnih IT sustava.

Kako bi ovo poglavlje kvalitetnije demonstriralo funkcionalnosti alata *Splunk Free*, prvo ćemo u bazu podataka učitati dodatne podatke koje ćemo zatim pretraživati, analizirati i vizualizirati. Službene *Splunk* stranice nude prethodno generirane zapise prigodne za učenje koje ćemo koristiti u ovom poglavlju.

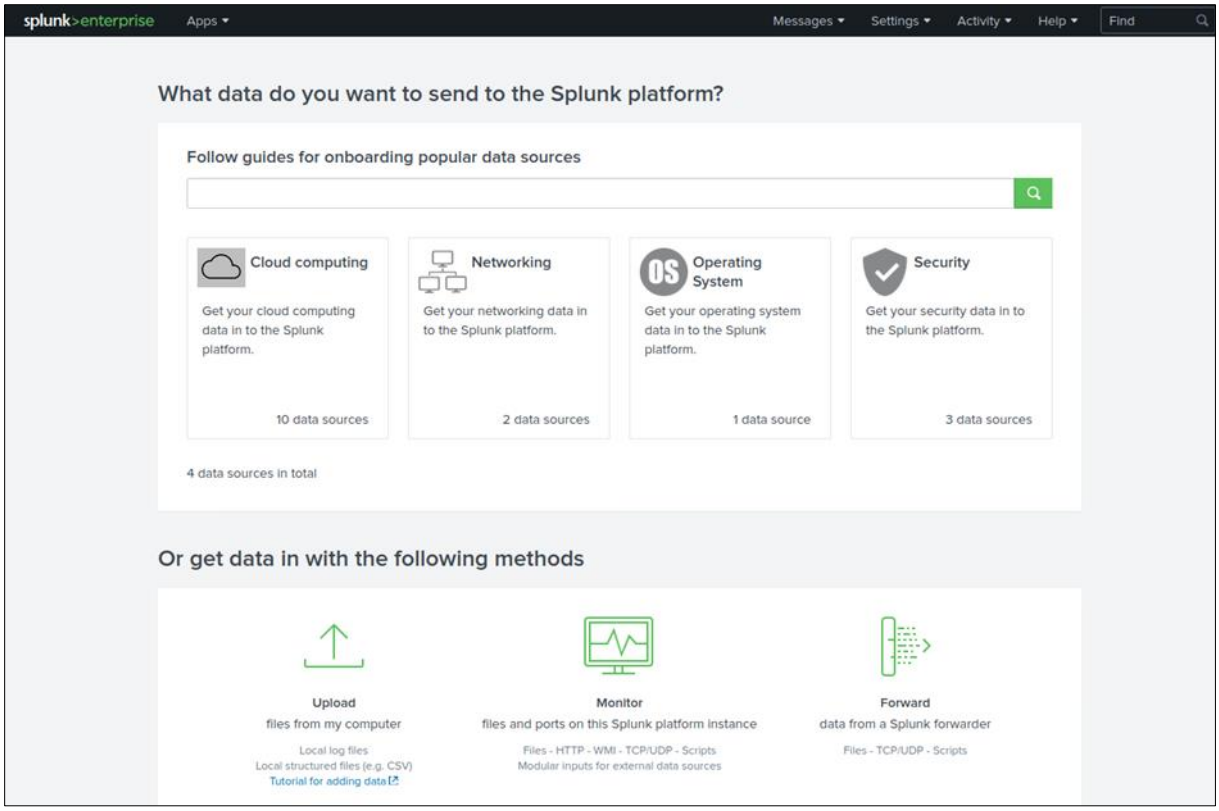
Najprije je potrebno preuzeti potrebne datoteke putem web preglednika: *tutorialdata.zip* i *Prices.csv.zip*. Te dvije datoteke su u ZIP formatu, nije ih još potrebno raspakirati. Datoteka *tutorialdata.zip* treba ostati u ZIP formatu, a datoteku *Prices.csv.zip* ćemo koristiti u kasnijem primjeru.

Idući je korak učitati datoteku *tutorialdata.zip* u *Splunk Free*. Na početnoj stranici *Splunk* sučelja (dostupnoj pritiskom na S*plunk Enterprise* logo) treba odabrati *Add Data*.



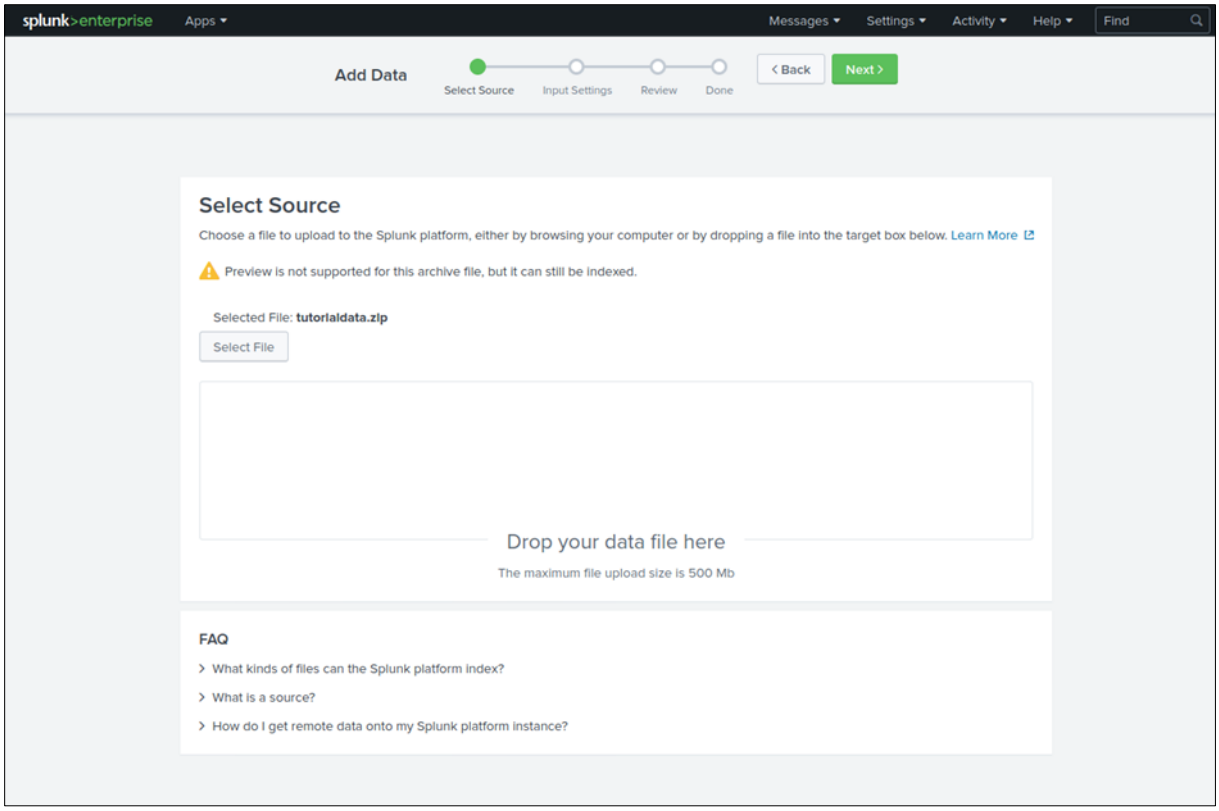
Slika 26 – *Splunk Free* početna stranica

Otvorit će se prozor prikazan na slici 27. Kako želimo unijeti zapise iz datoteke, treba odabrati *Upload*.



Slika 27 – Izbornik za dodavanje podataka

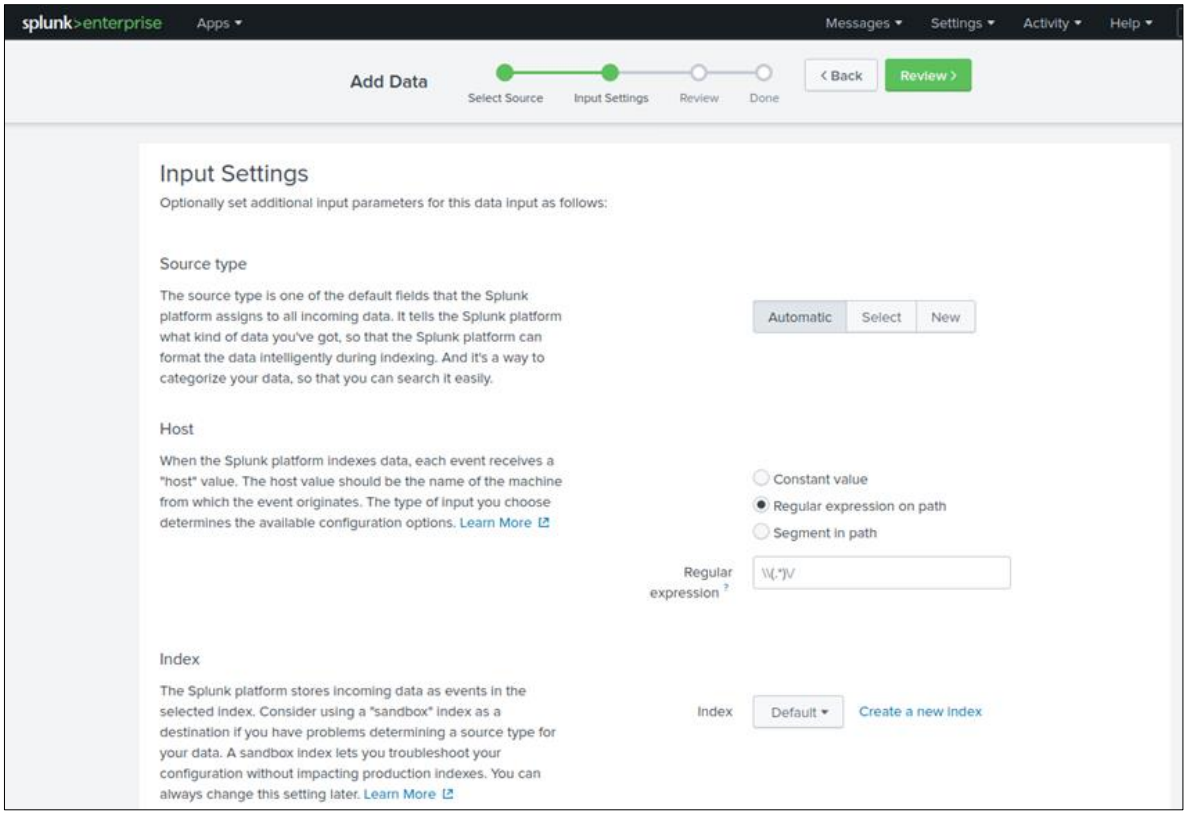
Na prozoru prikazanom na slici 28, potrebno je odabrati *Select File* te odabrati datoteku *tutorialdata.zip*. Nakon odabira, na vrhu prozora treba odabrati *Next*.



Slika 28 – Prozor za unos datoteka

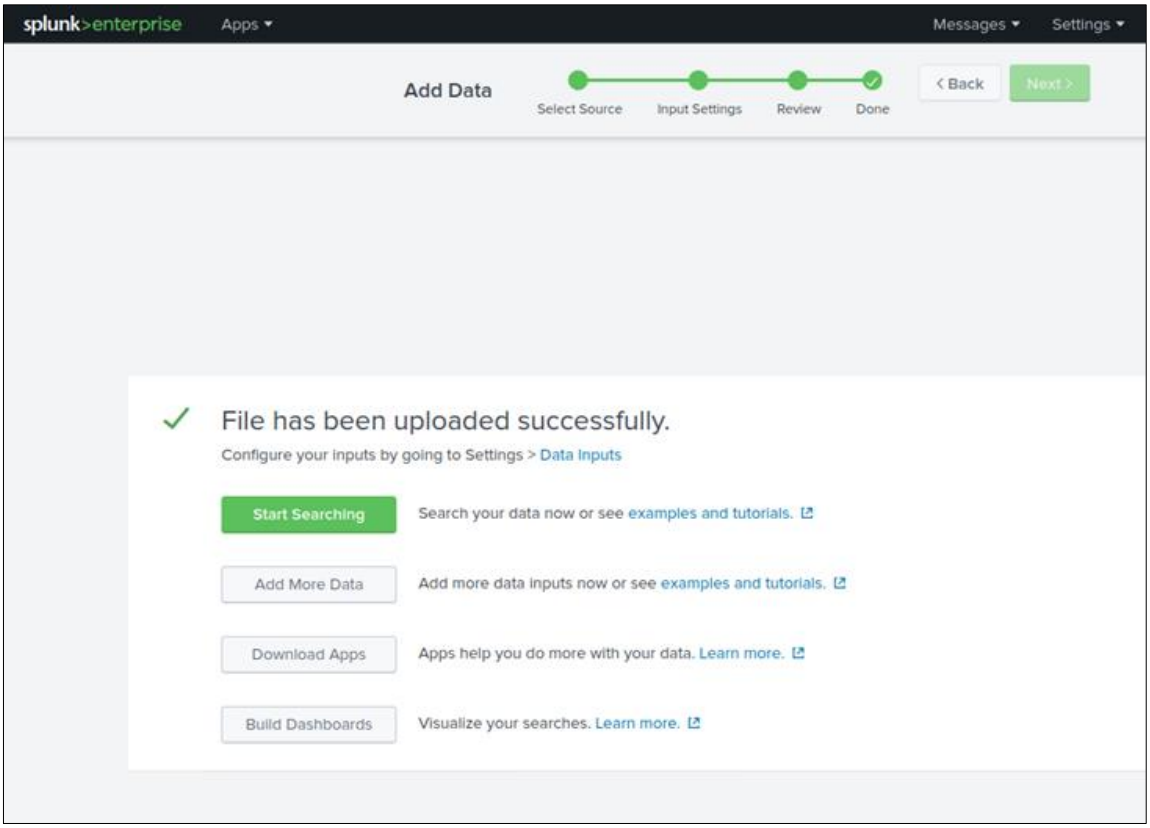
Slika 29 prikazuje idući korak, odnosno konfiguraciju podataka koje unosimo. Kako se u ZIP datoteci nalazi nekoliko datoteka s podacima s više različitih računala, potrebno je *Splunku* objasniti kako na temelju putanje razlikovati koji podaci dolaze s kojeg računala.

Ovdje pod *Host* treba odabrati *Regular Expression on path*, te u polju ispod upisati „\\(.*)\/" (bez navodnika). Na taj se način u ZIP datoteci koju učitavamo za svaku sadržanu datoteku izdvaja dio putanje koji označava računalo s kojega dolaze podaci. Nakon što je to uneseno, pri vrhu ekrana treba odabrati *Review*. Prikazat će se sažetak našeg izbora gdje treba samo odabrati *Submit*.



Slika 29 – Konfiguracija podataka za unos

Slika 30 prikazuje prozor koji korisniku potvrđuje uspješan unos datoteke.



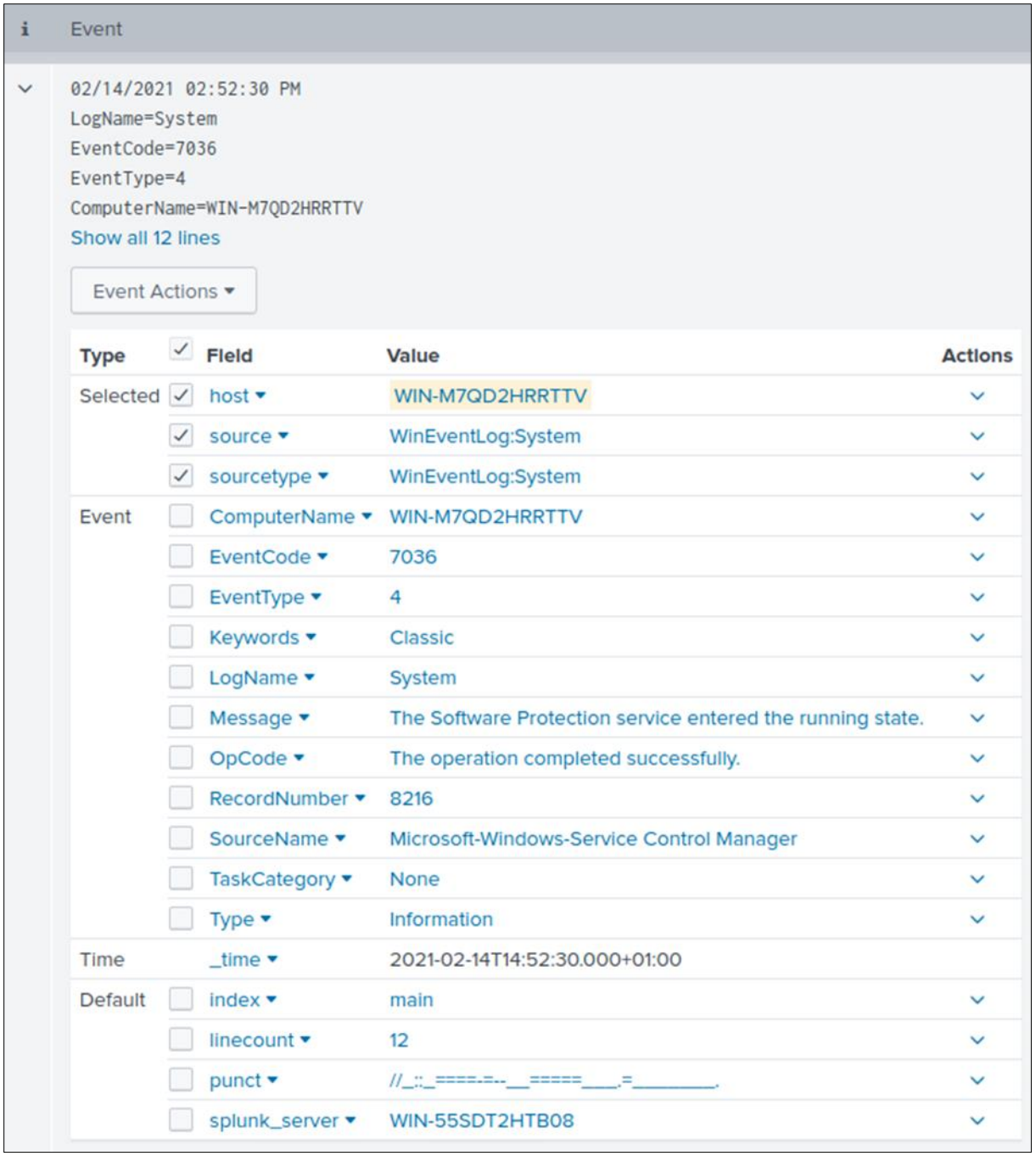
Slika 30 – Prikaz uspješnog unosa statičke datoteke

Nakon što smo uspješno unijeli zapise, sljedeći korak je njihova pretraga. Važna *Splunk* funkcionalnost koju treba razumjeti prije pretrage je indeksiranje polja (eng. *field*). Svaki zapis kojega *Splunk* primi može se podijeliti u niz polja, gdje svako polje ima ime i vrijednost. Korištenjem tih polja možemo znatno brže i lakše filtrirati željene zapise.

Prikažimo to u primjeru – pogledajmo jedan zapis od našeg *forwardera* (prikazan i na slici 31):

```
02/14/2021 02:52:30 PM
LogName=System
EventCode=7036
EventType=4
ComputerName=WIN-M7QD2HRRTTV
SourceName=Microsoft-Windows-Service Control Manager
Type=Information
RecordNumber=8216
Keywords=Classic
TaskCategory=None
OpCode=The operation completed successfully.
Message=The Software Protection service entered the running state.
```

Vidimo da ovaj zapis ima niz polja s imenima i vrijednostima. Kod poznatih tipova zapisa, *Splunk* će automatski detektirati i izdvojiti polja. Ovaj se proces zove *field extraction*. Kod manje poznatih formata zapisa moguće je i definirati vlastita pravila za izdvajanje polja.



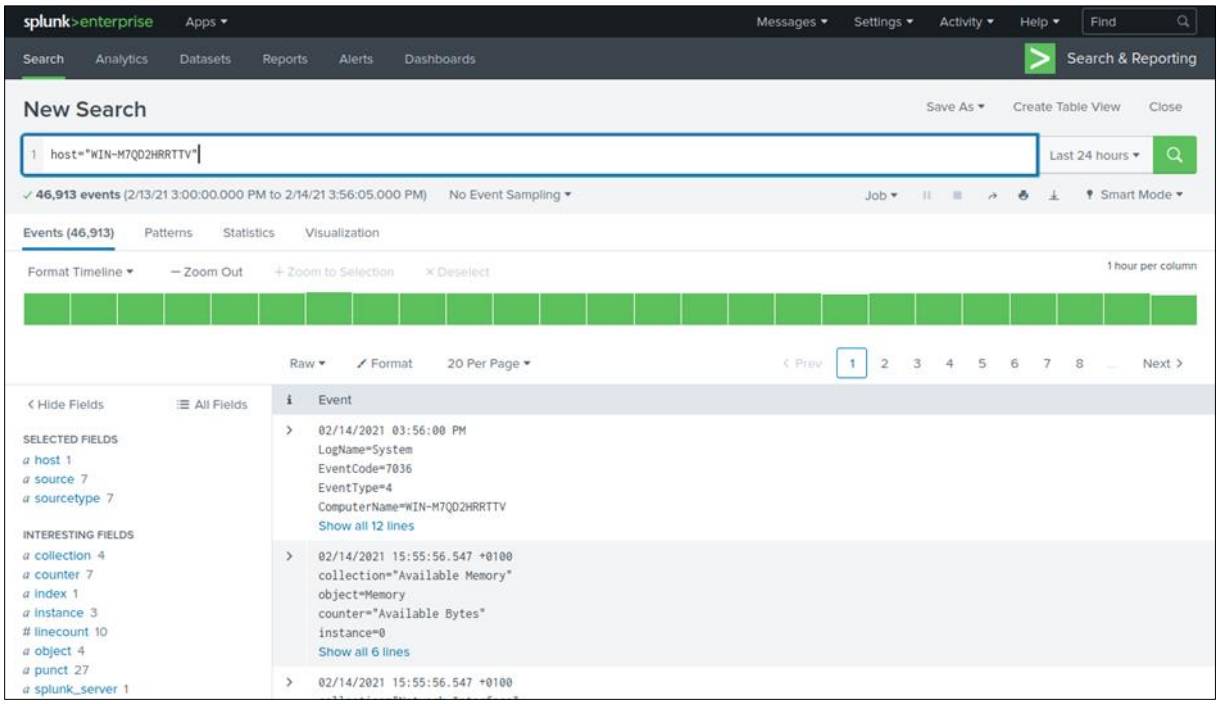
Slika 31 – Prikaz ekstrahiranih polja jednog zapisa

Kako je *Splunk* uspješno izdvojio sva polja zapisa, ta se polja onda mogu koristiti za pretragu i analizu. *Splunk* je također i dodao neka polja koja se ne nalaze u originalnom zapisu poput *host* i *source*.

U prethodnom smo poglavlju za provjeru unijeli upit „*“ koji vraća sve zapise koje je *Splunk* primio. Ovako širok upit nije prikladan za analizu zapisa – bilo bi bolje dodati još neke kriterije za pretragu. Primjerice, moguće je pretražiti zapise po računalu koje je poslalo zapis. U ovom primjeru, računalo na koje je instaliran *Splunk Forwarder* zove se *WIN-M7QD2HRRTTV*, pa u polje pretrage na *Splunk* korisničkom sučelju treba upisati:

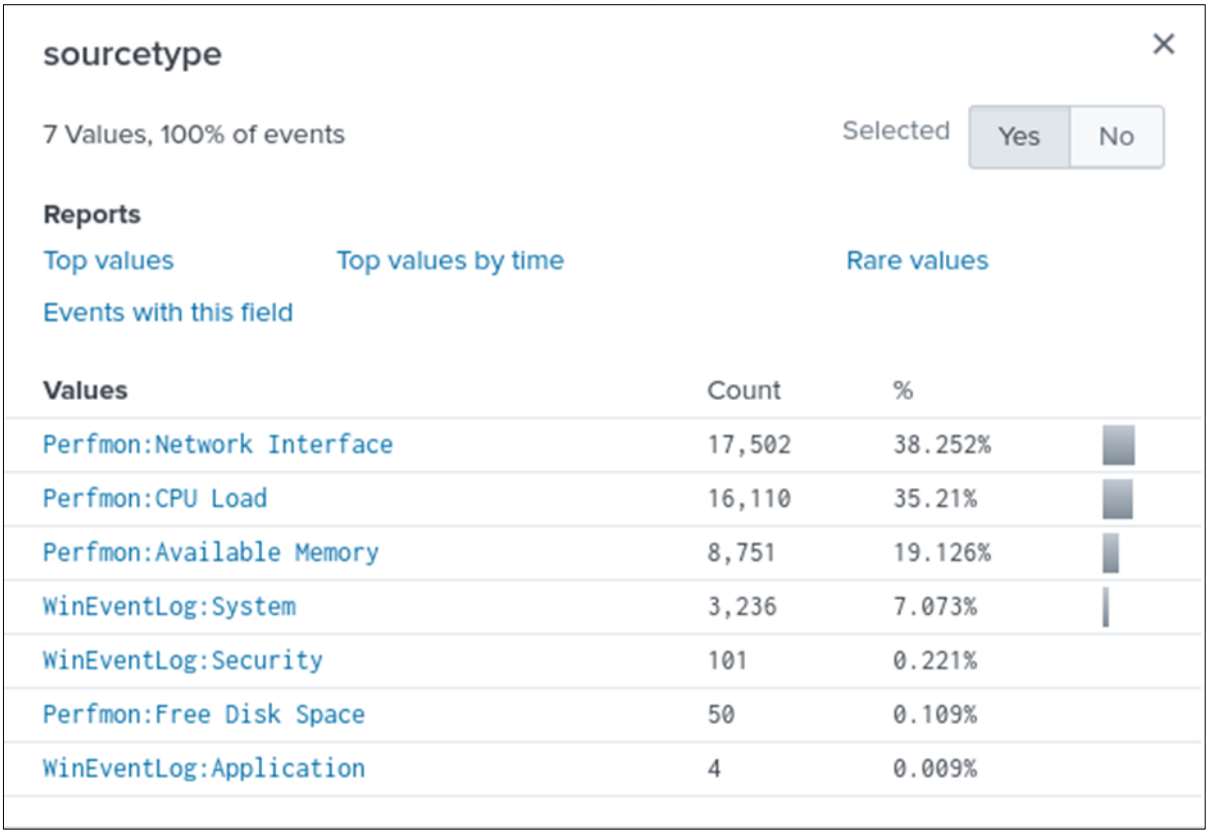
```
host="WIN-M7QD2HRRTTV"
```

Rezultati tog upita prikazani su na slici 32. U prikazu rezultata pretrage, lijevo se nalazi natpis *Selected fields*. Tamo je vidljivo koja je polja *Splunk* prepoznao u rezultatima upita te koliko različitih jedinstvenih vrijednosti imaju. Primjerice, može se vidjeti da je polje *host* u rezultatima upita imalo samo jednu jedinstvenu vrijednost, što je i logično jer je upit tražio samo zapise s jednog računala. S druge strane, polje *sourcetype* ima više vrijednosti, jer su s tog računala prikupljeni zapisi iz više različitih vrsta izvora.



Slika 32 – Prikaz upita koji vraća sve zapise s određenog poslužitelja

Pritiskom na polje *sourcetype* prikazat će se informacije o broju zapisa te vrste (kao što je prikazano na slici 33).



Slika 33 – Prikaz svih vrijednosti „sourcetype" polja u rezultatima *Splunk* upita

Možemo dodatno suziti naš upit da prikaže zapise s određenog računala, no samo sa zadanim tipom. Unesimo sljedeći upit:

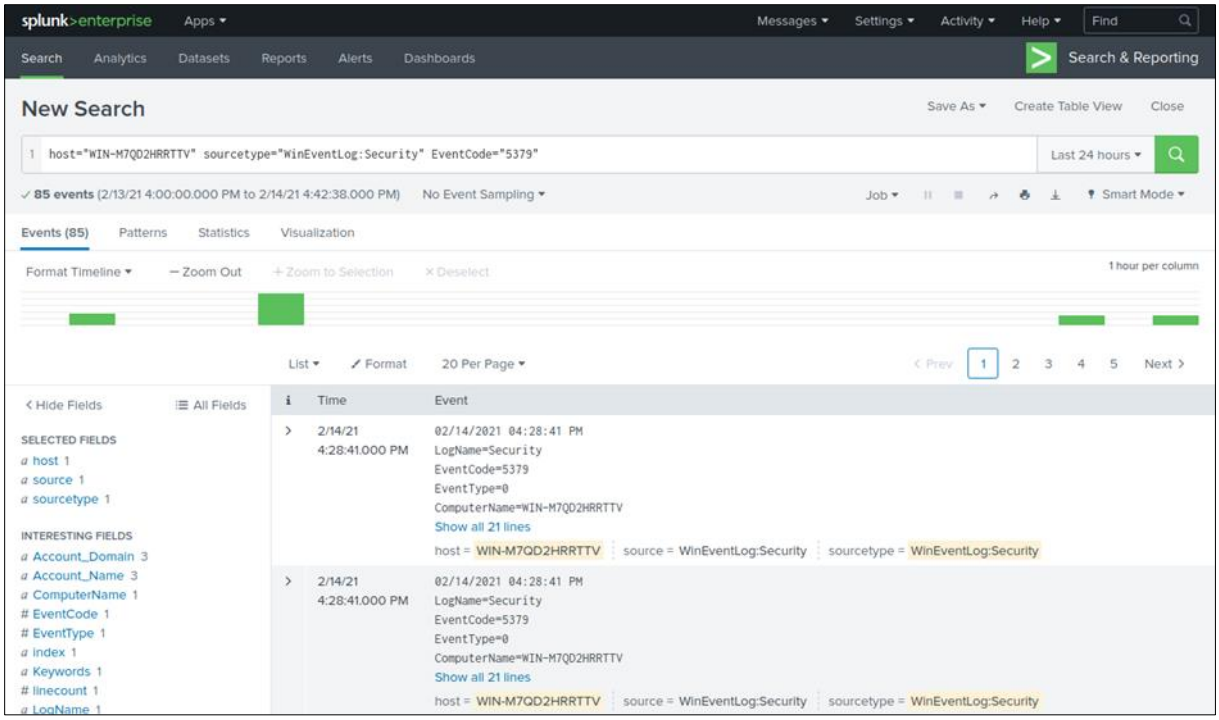
```
host="WIN-M7QD2HRRTTV" sourcetype="WinEventLog:Security"
```

Ovim smo upitom dodatno suzili pretragu na zapise sigurnosnih dnevnika (engl. *security logs*) s određenog poslužitelja.

Ako tražimo specifičnu vrstu događaja, možemo dodatno suziti upit:

```
host="WIN-M7QD2HRRTTV" sourcetype="WinEventLog:Security" EventCode="5379"
```

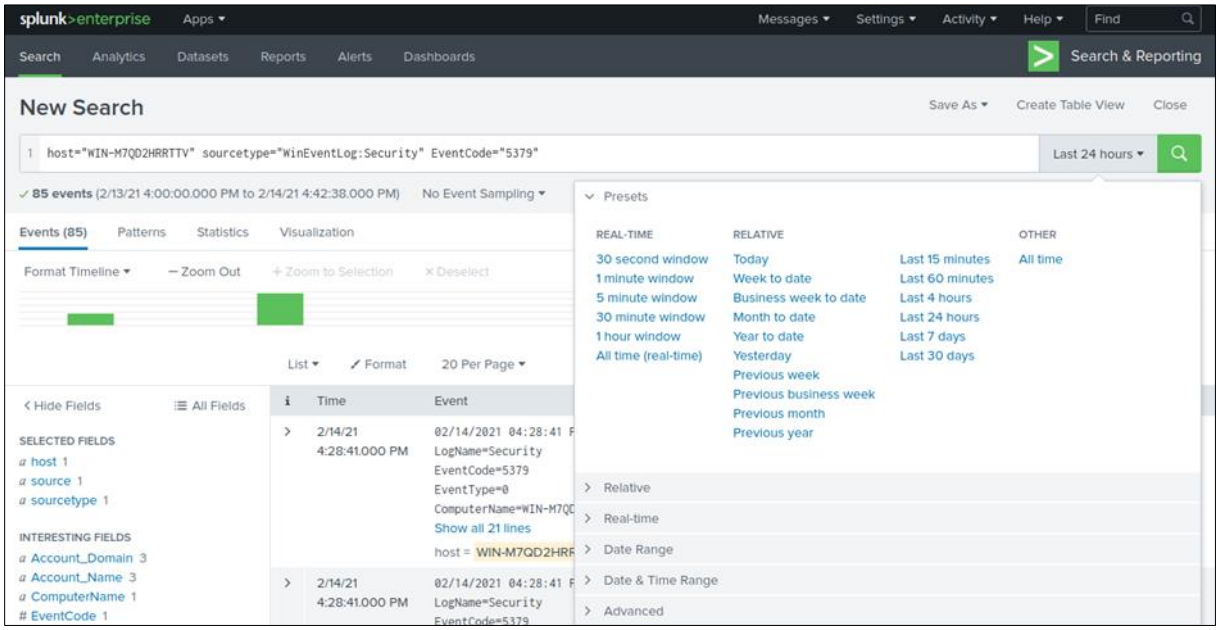
Ovim upitom tražimo sigurnosne dnevnike s određenog računala s kodom vrste događaja „5379".



Slika 34 – Prikaz specifičnog upita

Bitno je napomenuti da se svakom upitu može dodijeliti i vremenski raspon. Svi naši dosadašnji upiti bili su fiksirani na zadnjih 24 sata, s čime smo iz rezultata uklonili sve zapise starije od jednog dana.

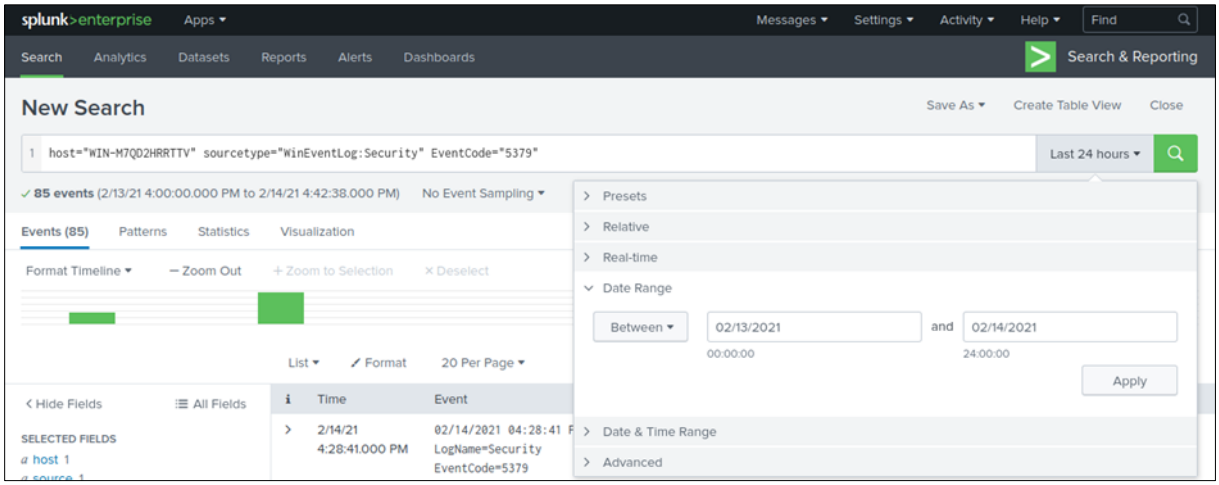
Vremenski raspon upita može se lako mijenjati tipkom koja je desno od polja pretrage, a u kojoj piše trenutno odabrani vremenski raspon (npr. *Last 24 hours*).



Slika 35 – Prikaz izbora vremenskog raspona upita

Splunk nudi već gotove izbornike za promjenu vremenskog raspona, no korisno je znati da se raspon može definirati od i do određenog vremenskog perioda.

To je korisno izabrati ako pretražujemo zapise za događaj za koji znamo da se dogodio primjerice „prošli četvrtak ili petak".

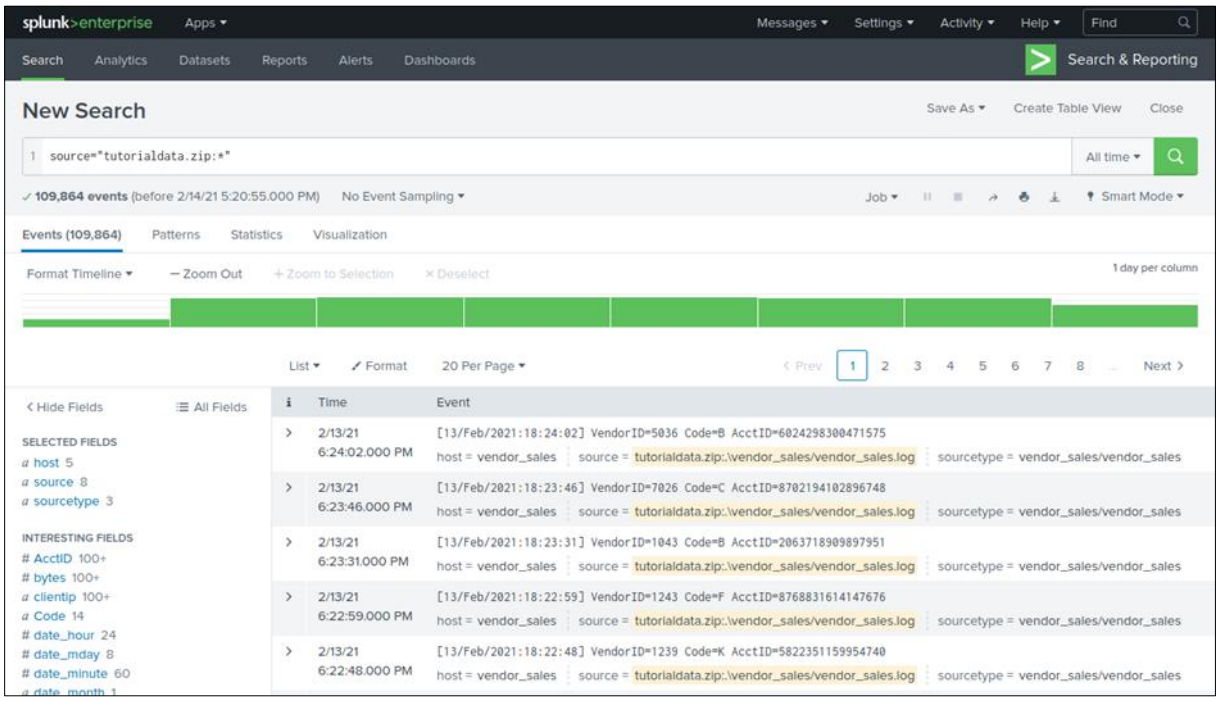


Slika 36 – Prikaz odabira specifičnog vremenskog raspona upita

Na početku ovog poglavlja smo u *Splunk* dodali zapise iz datoteke *tutorialdata.zip*. Pogledajmo što se nalazi u tim zapisima.

Kako smo zapise za demonstraciju unijeli ručno kroz datoteku, možemo kroz *Splunk* upit zatražiti samo te zapise. U polje pretrage upišite sljedeće i za vremenski raspon odaberite *All time*:

```
source="tutorialdata.zip:*"
```



Slika 37 – Prikaz upita za pretragu zapisa iz ZIP datoteke

Bitno je napomenuti da će datumi i vremena zapisa sadržanih u datoteci *tutorialdata.zip* ovisiti o vremenu kada smo tu datoteku preuzeli. Na *Splunkovoj* web stranici se sadržaj datoteke *tutorialdata.zip* svakodnevno mijenja tako da sadržani zapisi počinju na datum tjedan dana prije preuzimanja datoteke. To je napravljeno kako bi učenje pretraživanja pomoću tih podataka bilo lakše, tj. kako bi se mogla koristiti pretraga zapisa iz zadnjih 24 sata ili zadnjih tjedan dana.

Zapisi iz datoteke *tutorialdata.zip* su zapravo zapisi poslužitelja fiktivne tvrtke *Buttercupgames*.

Ako pogledamo koja je polja *Splunk* izdvojio iz ovih zapisa, vidimo da jedno polje ima ime `categoryId`. *Splunk* je automatski prepoznao to polje kao parametar u zapisima URL-ova. Suzimo naš upit da prikaže samo zapise s određenom kategorijom:

```
source="tutorialdata.zip:*" categoryId=SPORTS
```

Bitno je napomenuti da se pretrage mogu provoditi i na poljima koja nisu izdvojena, tj. na dijelovima drugih polja. Ako primjer *Splunk* ne prepozna polje `categoryId` (unutar polja URL-a), i dalje možemo tražiti zapise s određenom kategorijom pomoću upita:

```
source="tutorialdata.zip:*" "categoryid=sports"
```

Razliku između zadnja dva upita je u tome što u je donjem upitu drugi dio obuhvaćen u navodnike. S tim upitom *Splunku* kažemo da ne traži određeno polje po vrijednosti, već da nam prikaže zapis ako se traženi izraz nalazi bilo gdje u zapisu, primjerice kao dio nekog polja (dio URL-a u ovom slučaju).

Unesimo sljedeća dva upita:

```
categoryId=SPORTS
```

```
source="tutorialdata.zip:*" categoryId=SPORTS
```

Vidimo da ta dva upita daju jednake rezultate. Razlog tome je što polje `categoryId` ne postoji ni u jednom drugom tipu zapisa koji se trenutno nalaze na *Splunku*, te smo samo s tim upitom automatski iz rezultata uklonili sve zapise koji su pristigli primjerice s našeg *forwardera* instaliranog na Windows poslužitelju.

Kako su ovi fiktivni zapisi jednim dijelom dnevnici web poslužitelja, vidimo da *Splunk* već ima izdvojeno polje vrijednosti statusnog koda HTTP odgovora poslužitelja. Ako želimo popisati sve zapise gdje je poslužitelj odgovorio statusnim kodom 200 (koji označava uspješan odgovor), upisujemo sljedeći upit:

```
status=200
```

Ako želimo da upit vrati sve zapise gdje HTTP statusni kod nije bio 200, upisujemo sljedeće:

```
status!=200
```

U zapisima se također nalazi polje `action`, još jedan parametar kojega je *Splunk* prepoznao iz URL-a, a koji opisuje koju je radnju korisnik obavljao na web stranicama tvrtke.

Jedna takva radnja je kupnja, pa pregledajmo sve zapise gdje su korisnici uspješno kupili određeni artikl.

```
status=200 action=purchase
```

Suprotno tome, pogledajmo zapise gdje su korisnici pokušali kupiti nešto, no gdje kupnja nije uspjela:

```
status!=200 action=purchase
```

Bitno je spomenuti kako *Splunk* implicitno dodaje logički operator `AND` između dijelova upita. Gornji upiti *Splunku* kažu da prikaže sve zapise koji imaju obje spomenute vrijednosti. Isti upit se može formulirati na sljedeći način:

```
status=200 AND action=purchase
```

Drugim riječima, ako u upit ne napišemo `AND`, *Splunk* će ga automatski dodati. *Splunk* podržava i ostale logičke operatore, no njih je potrebno izričito navesti u upitu. Ako želimo upit koji vraća sve kupnje ili radnje dodavanja artikla u košaricu, možemo pokušati upisati sljedeći upit:

```
action=addtocart action=purchase
```

Vidimo da gornji upit ne vraća nikakve rezultate. Razlog tome je što u našim podacima svaki zapis ima samo jednu akciju (`action`), a ne više njih. Gornjim upitom smo od pretrage tražili zapise koji sadrže i jedno i drugo, a takvih zapisa nema. Promijenimo upit u sljedeće:

```
action=addtocart OR action=purchase
```

U rezultatima sada vidimo zapise koji sadržavaju jednu ili drugu akciju. Dodatno proširimo upit da nam vrati sve uspješno odrađene akcije kupnje ili dodavanje artikla u košaricu:

```
status=200 AND (action=addtocart OR action=purchase)
```

U gornjem upitu vidimo primjer grupiranja pomoću zagrada. Upitom tražimo sve zapise kupnje ili dodavanja u košaricu koji su bili uspješni (HTTP statusni kod 200).

Možemo i znak „*“ (zvjezdica) koristiti umjesto vrijednosti polja. U nižem upitu pretražujemo sve akcije koje je korisnik na određenoj IP adresi pokušao napraviti:

```
clientip=182.236.164.11 AND action=*
```

Ovim upitom tražimo sve zapise koje je generirao korisnik na IP adresi *182.236.164.11*, bez obzira na to kakvu je akciju pokušao napraviti. Ovime ne vidimo svu komunikaciju koju je korisnik imao s web poslužiteljima, već vidimo samo one zapise za koje znamo da je korisnik pokušao odraditi neku akciju (bez obzira na to koja je to akcija bila), jer ti zapisi imaju parametar `action` u URL-u.

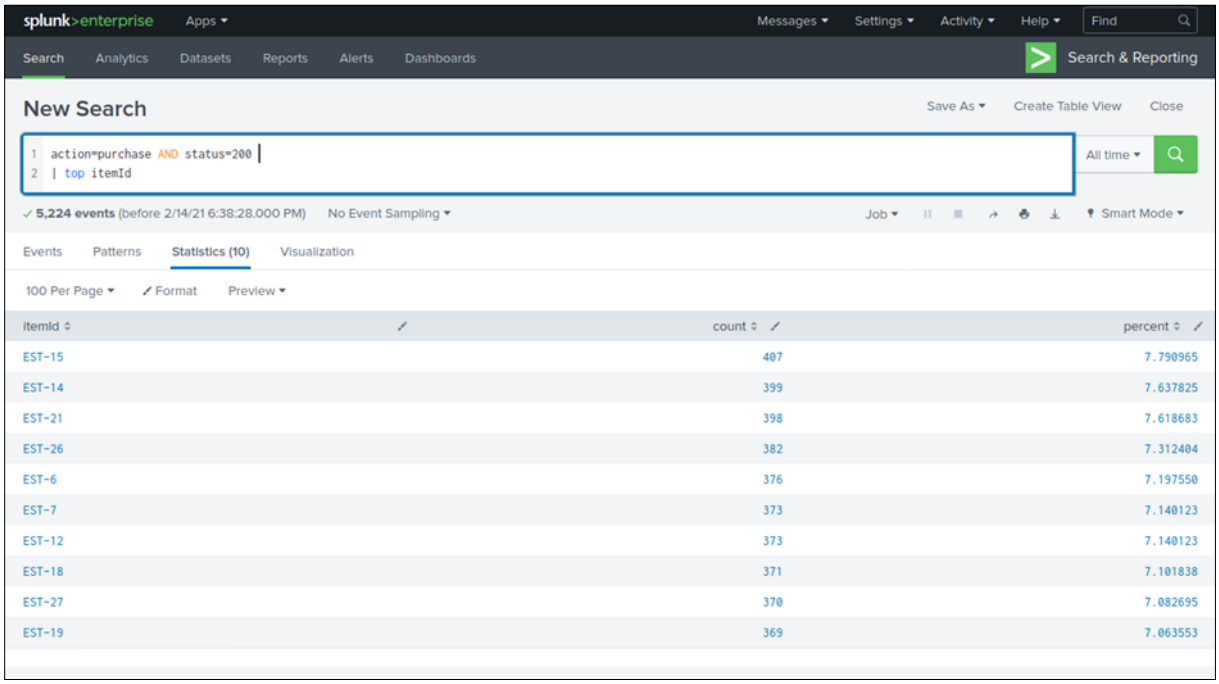
Do sada smo demonstrirali kako se zapisi pretražuju, no bitno je demonstrirati i kako analizirati te vizualizirati rezultate pretrage. *Splunk* pretraga ima funkcionalnost operatora za spajanje, tzv. *pipe operator* sličan istoimenom operatoru u Unix ljuskama

(engl. *shell*). Putem ovog operatora, izlazne informacije jedne pretrage postaju ulazne informacije druge pretrage ili funkcije. Prikažimo to na sljedećem primjeru.

Ako želimo prikazati sve uspješne kupnje, te vizualizirati koji su artikli bili kupovani, možemo koristiti *Splunkovu* funkciju *top*. U polje pretrage unesite sljedeće:

```
action=purchase AND status=200

| top itemId
```



Slika 38 – Tablični prikaz kupljenih artikla

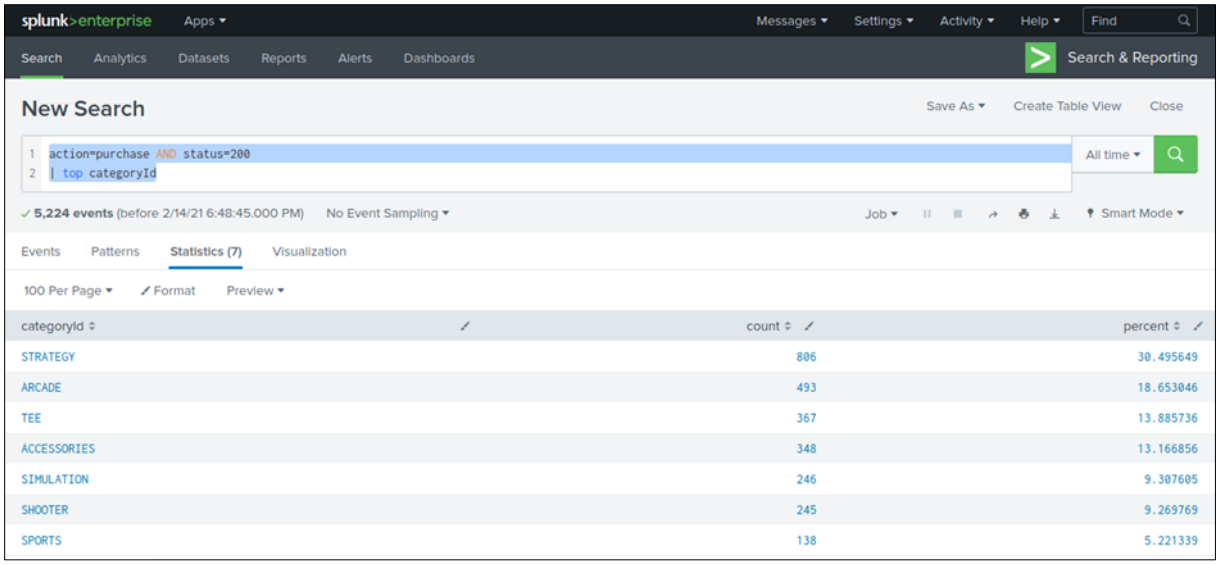
Vidimo da je *Splunk* pretražio sve zapise uspješne kupnje, te nam je pomoću *top* funkcije prikazao kojih 10 artikala su najčešće bili kupovani. Funkcija je automatski prebrojila kupnje po artiklu i prikazala ih u tablici.

Primijetimo na slici 38 da naš upit nije vezan za određeno vremensko razdoblje, dakle rezultati koje vidimo su generirani na temelju svih zapisa koje *Splunk* ima. Ako želimo istu tablicu no samo za određeni vremenski period, potrebno je suziti vremenski raspon pretrage na željeno vrijeme, na isti način kao i za bilo koju pretragu (pomoću izbornika desno od polja pretrage).

Ako želimo sličan upit, no nevezan za određene artikle već za kategorije, u polje pretrage upisujemo sljedeće:

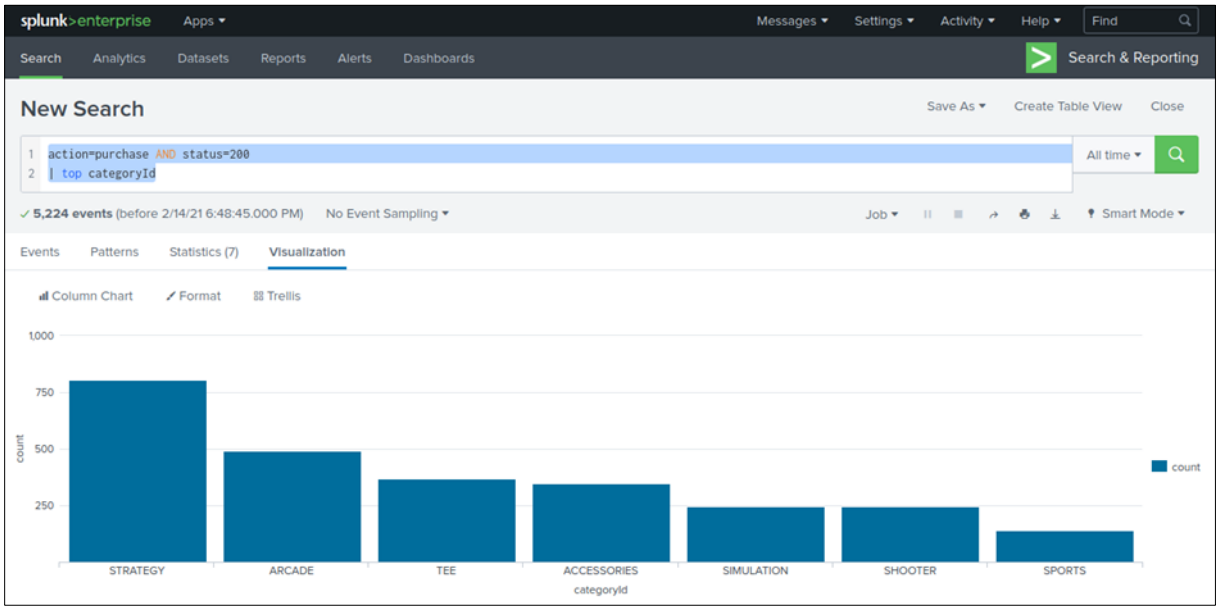
```
action=purchase AND status=200
| top categoryId
```

Upit prikazan na slici 39 prikazuje sortirani broj kupnji po kategoriji.



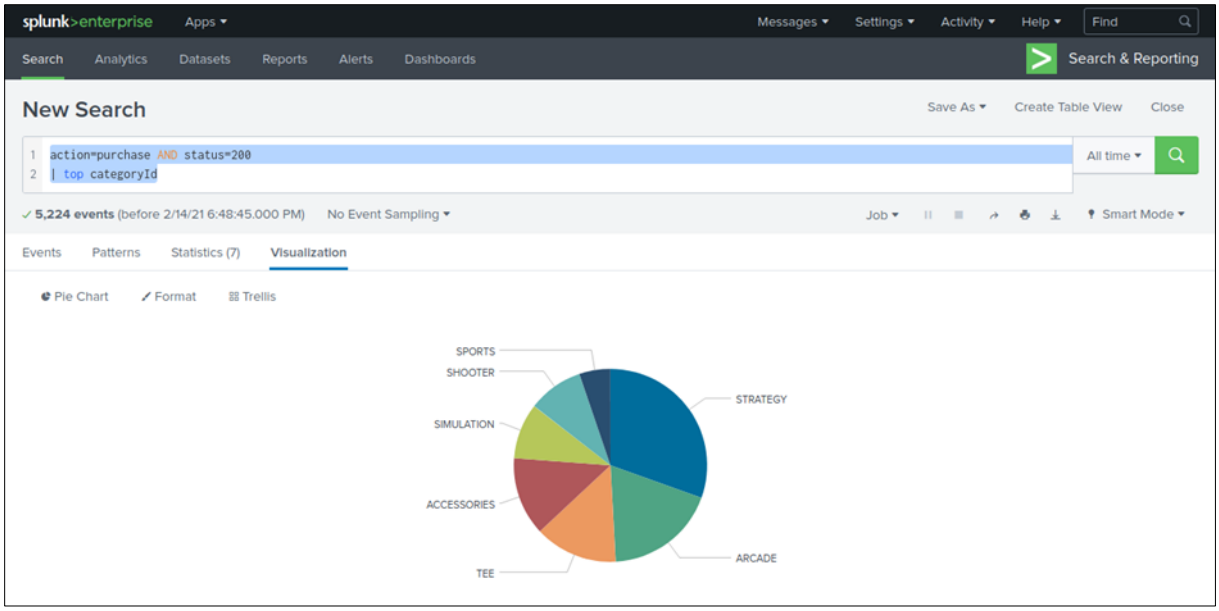
Slika 39 – Tablični prikaz kupnji po kategoriji

Ako ne želimo tablicu već vizualni prikaz, na sučelju ispod polja upita treba odabrati *Visualization*. Prikazat će se iste informacije, no vizualizirane grafom.



Slika 40 – Vizualni prikaz kupnji po kategoriji

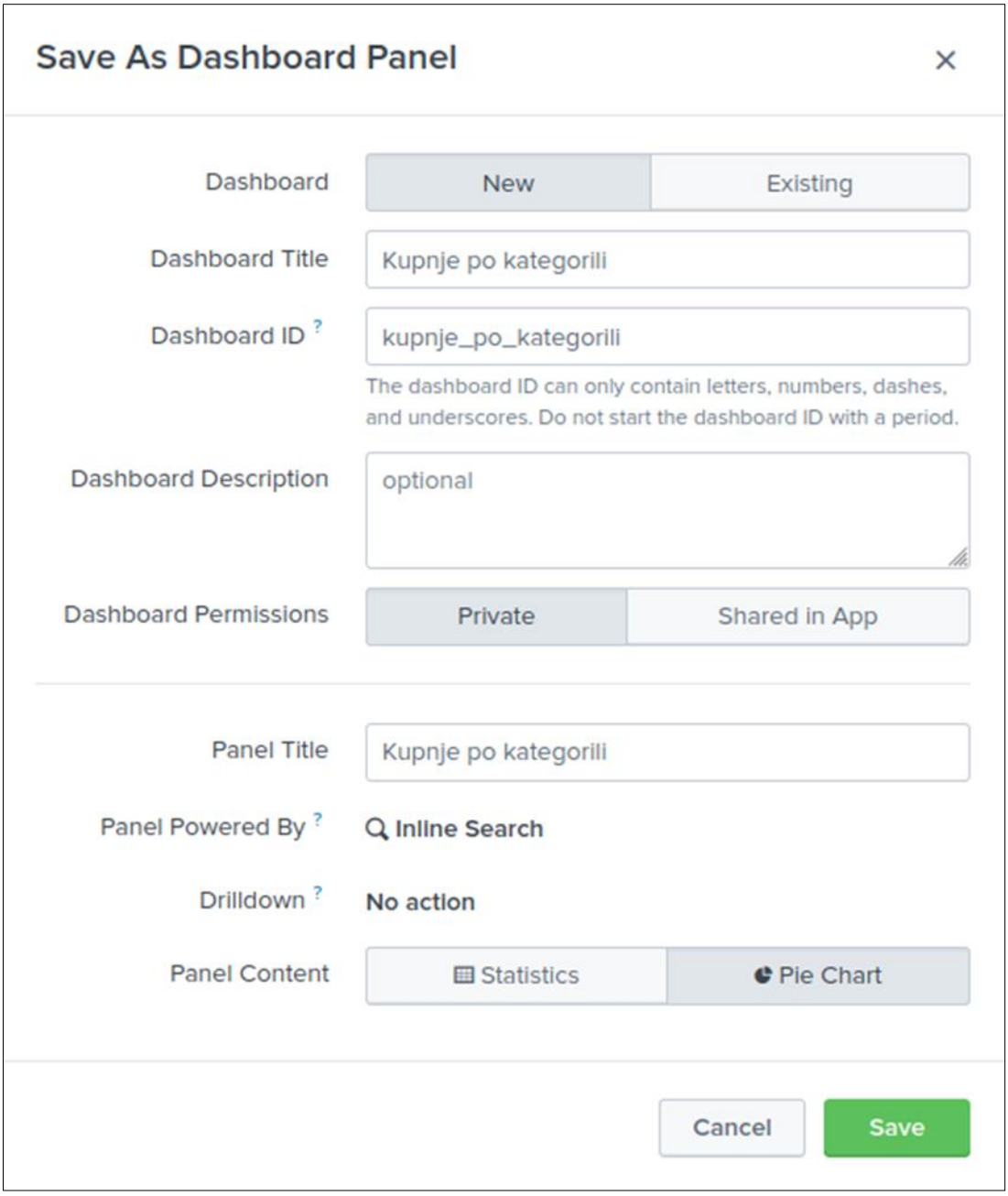
Vrsta vizualizacije se lako mijenja. Ove informacije je bolje predstaviti u kružnom grafu (engl. *pie chart*). Pritiskom na *Column Chart*, te odabirom *Pie Chart* promijenit će se tip vizualizacije.



Slika 41 – Vizualni prikaz kupnji po kategoriji u obliku kružnog grafa

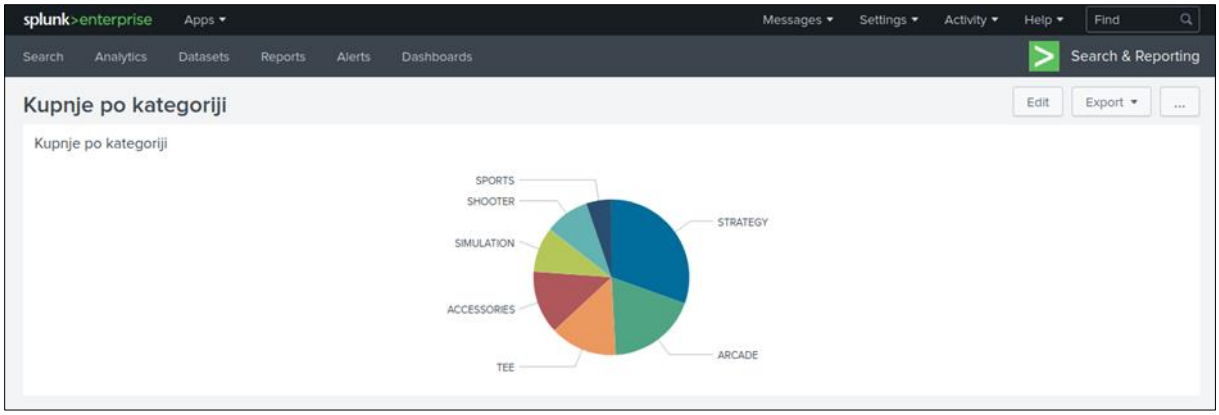
Ovu pretragu i njen graf možemo spremiti za lako ponovno izvršavanje kasnije. Pri vrhu prozora odaberite *Save As*, te *Dashboard Panel*.

U izborniku prikazanom na slici 42, unesite ime, pri dnu odaberite *Pie Chart* te pritisnite *Save*.



Slika 42 – Izbornik pohrane pretrage i njene vizualizacije

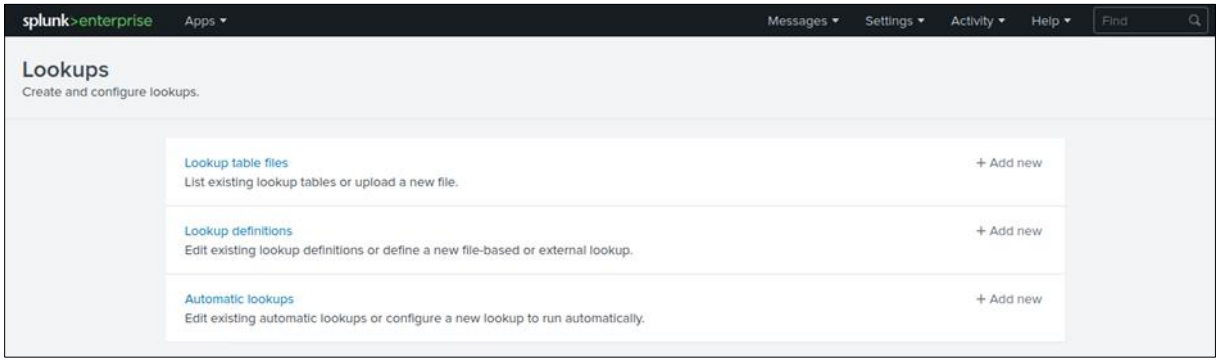
Pretraga i njena vizualizacija sada su spremljeni te se lako mogu ponovno izvršiti navigacijom na *Dashboards* te odabirom imena unesenog tijekom spremanja.



Slika 43 – Prikaz spremljenog kružnog grafa

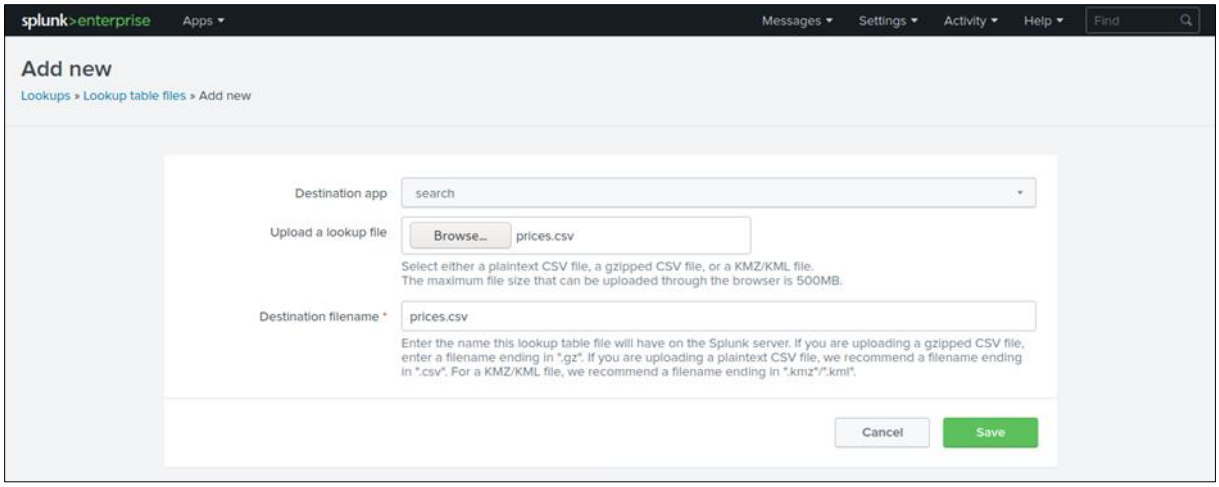
U idućem ćemo primjeru prikazati *Splunk* funkcionalnost zvanu *field lookups*. Ova funkcionalnost nam omogućuje zamjenu raznih vrijednosti s nekim drugim vrijednostima koje su praktičnije za analizu. Primjerice, ako naš upit ili graf prikazuje šifru određenog artikla, bilo bi jasnije umjesto šifre prikazati puno ime artikla.

Za to će nam biti potrebna druga preuzeta datoteka naziva *Prices.csv.zip*. Raspakirajte ovu ZIP datoteku i na *Splunk* korisničkom sučelju otvorite *Settings* → *Lookups*.



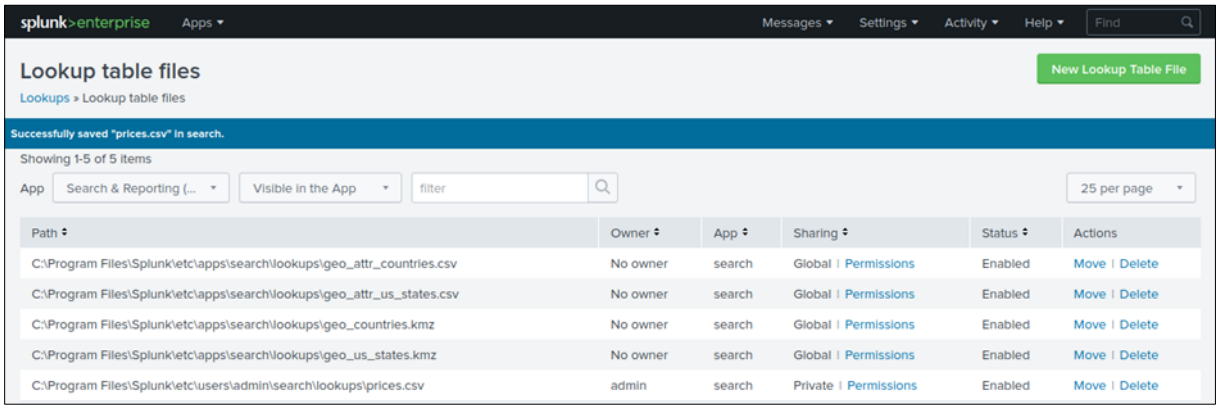
Slika 44 – Prikaz konfiguracijskog izbornika *lookup* datoteka na *Splunk* korisničkom sučelju

Desno na polju *Lookup table files* odaberite *Add new*. Na izborniku prikazanom na slici 45, odaberite raspakiranu datoteku *prices.cvs* te unesite isto ime u polje *Destination filename*. Nakon toga, pritisnite *Save*.



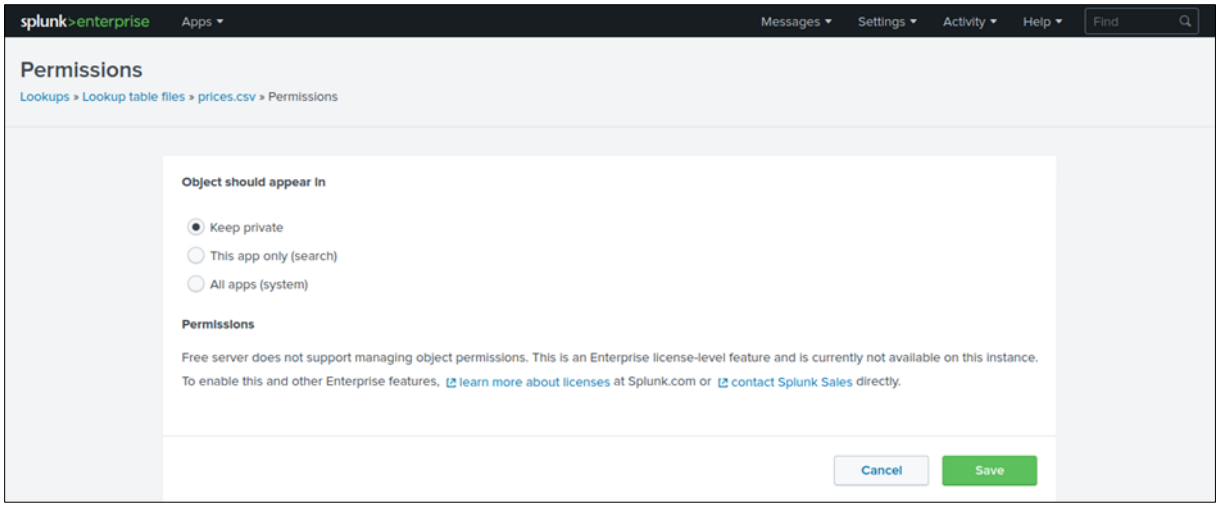
Slika 45 – Prikaz izbornika dodavanja *lookup* datoteke na *Splunk* korisničkom sučelju

Nakon što se datoteka pohrani, otvoriti će se prozor gdje se prikazuju sve datoteke tog tipa.



Slika 46 – Prikaz svih pohranjenih *lookup* datoteka

Još je potrebno omogućiti pristup ovoj datoteci iz svih dijelova *Splunka*. Naša datoteka je na slici prikazana zadnja u nizu. Na njenom redu je potrebno odabrati *Permissions*. Otvoriti će se novi prozor. Na prozoru prikazanom na slici 47, odaberite *All Apps* te pritisnite *Save*.

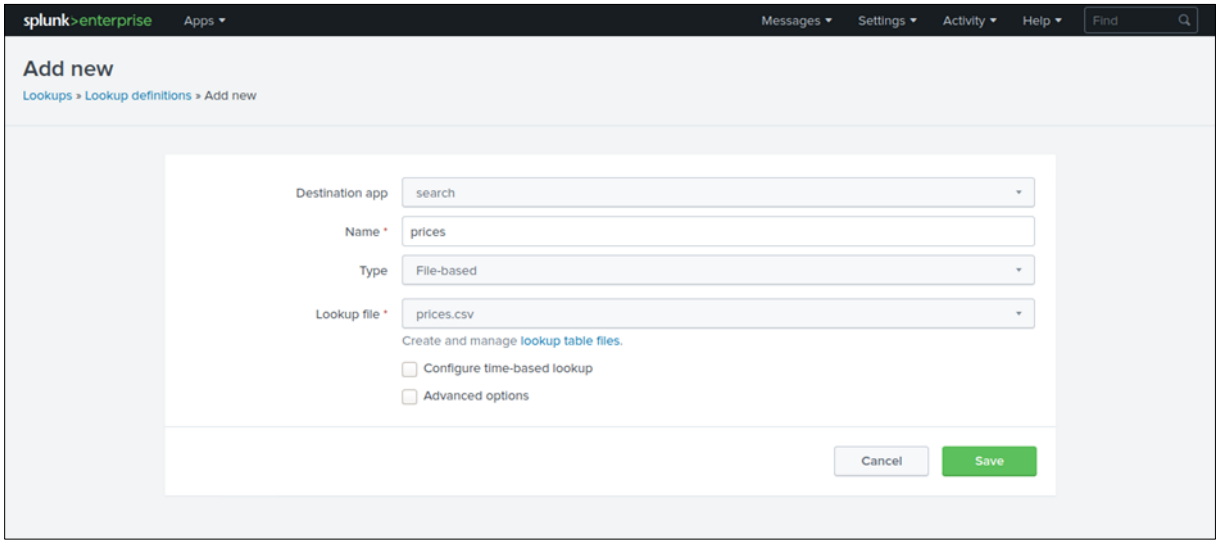


Slika 47 – Prikaz sučelja za izmjenu dozvola *lookup* datoteke

Nakon toga, potrebno je definirati *lookup* funkcionalnost. Trenutno *Splunk* ima našu datoteku, no potrebno mu je reći kako i kada ju treba koristiti.

Na *Splunk* korisničkom sučelju, ponovo otvorite *Settings* → *Lookups*, no ovaj put desno na polju *Lookup definitions* odaberite *Add new*.

Za ime definicije unesite *prices* te niže na *Lookup file* polju odaberite našu datoteku *prices.csv*. Pritisnite *Save*. Naša definicija je sada pohranjena i može se koristiti.



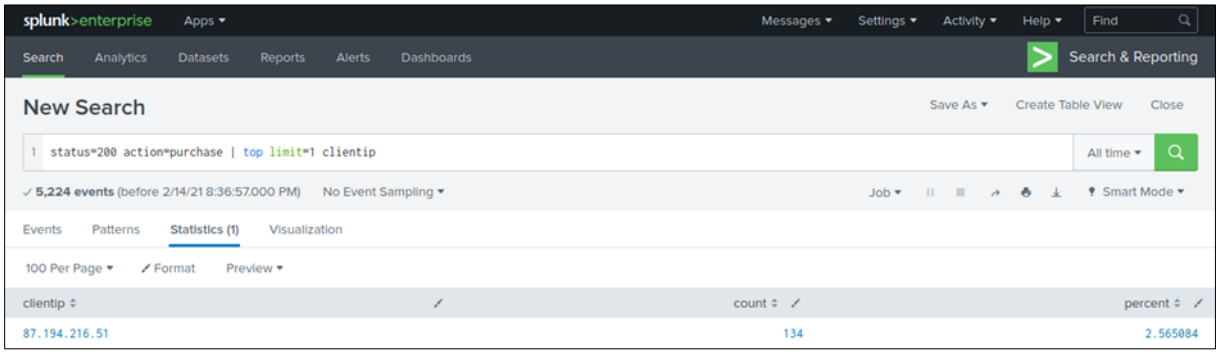
Slika 48 – Prikaz dodavanje nove *lookup* definicije

Pretpostavimo da imamo zadatak saznati koji korisnik je kupio najviše artikala i kojih. U sljedećem primjeru ćemo prikazati kako to otkriti. Koristiti ćemo već spomenutu *lookup* funkcionalnost zajedno sa *subsearch* funkcionalnosti.

Subsearch je funkcionalnost gdje rezultate jedne pretrage možemo staviti kao argument neke druge pretrage, slično prethodno spomenutom *pipe* operatoru.

Prvo je potrebno definirati upit kojim ćemo otkriti koji je korisnik napravio najviše uspješnih kupnji. U glavno polje pretrage upisujemo sljedeći upit:

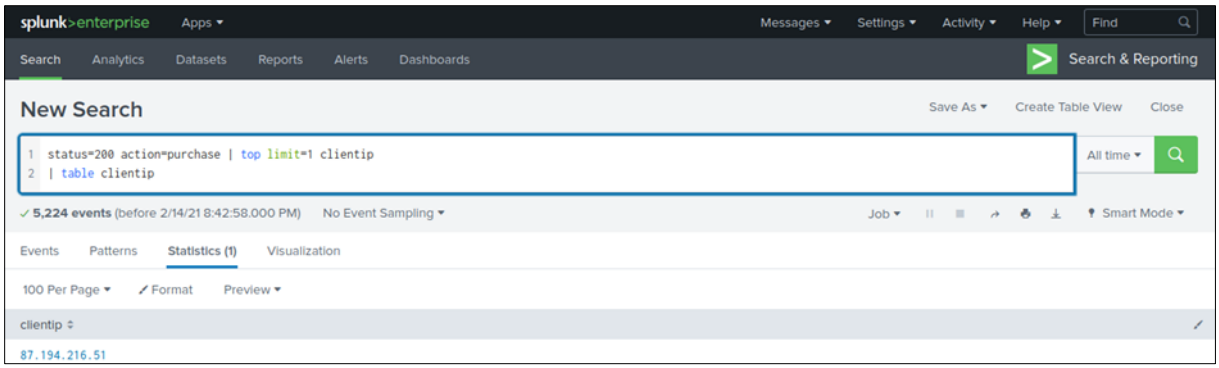
```
status=200 action=purchase | top limit=1 clientip
```



Slika 49 – Prikaz upita gdje tražimo korisnika s najviše uspješnih kupnji

Upit je vrlo sličan onima koje smo već koristili. Primijetimo argument `limit=1` funkcije *top*. Pomoću njega smo funkciji *top* rekli da prikaže samo jednu vrijednost korisnika (IP adrese) s najvećim brojem kupnji umjesto najviših 10. Također vidimo da je upit vratio više stupaca u tablici, no mi želimo samo IP adresu, pa na kraj gornjeg upita dodajemo naredbu *table* samo s argumentom `clientip`:

```
status=200 action=purchase | top limit=1 clientip
| table clientip
```



Slika 50 – Prikaz upita gdje tražimo samo IP adresu korisnika s najviše uspješnih kupnji

Iduće je potrebno otkriti što je sve taj korisnik kupovao. Bez korištenja *subsearch* funkcionalnosti, to možemo otkriti sljedećim upitom:

```
status=200 action=purchase 87.194.216.51
```

U ovom je trenutku gornji upit dovoljan, no možda se uskoro pojavi neki drugi korisnik koji kupi više proizvoda. Bolje bi bilo koristiti *subsearch* funkcionalnost koja će izlaz prvog upita ovog primjera staviti kao argument drugog upita. Upišite sljedeće:

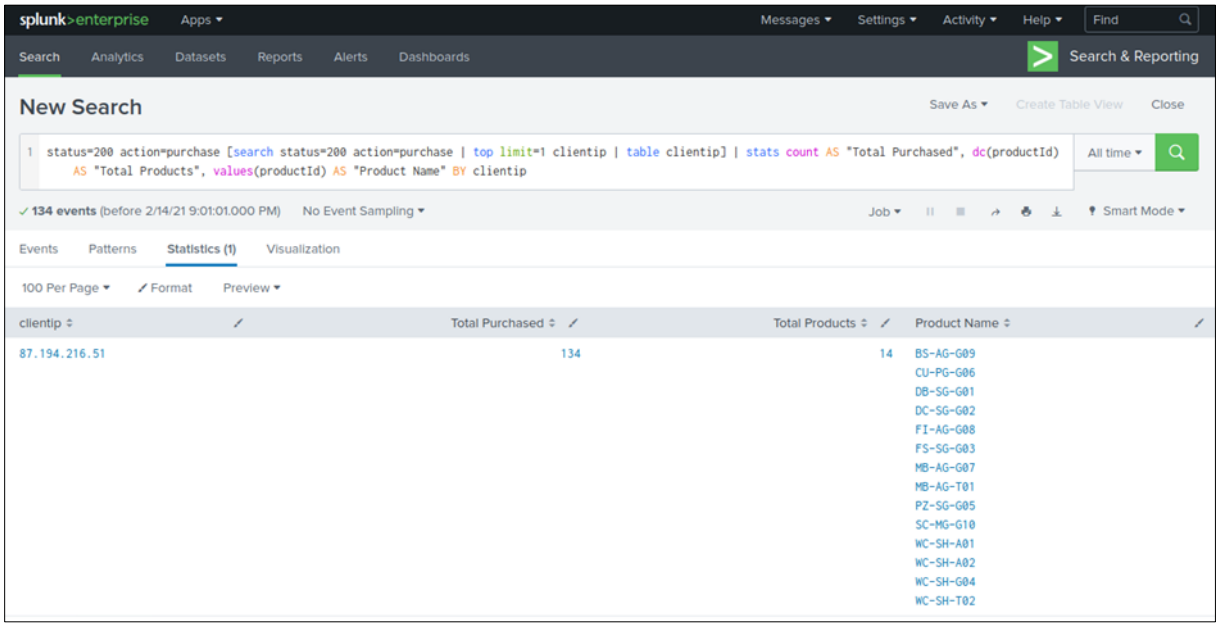
```
status=200 action=purchase
[search status=200 action=purchase | top limit=1 clientip | table clientip]
```

Uglatim zagradama smo rezultat jednog upita ugradili kao argument drugog upita. Vidimo da su rezultati zadnja dva upita trenutno isti, no samo će upit koji koristi *subsearch* biti

ispravan i ubuduće ako se promijeni korisnik koji je kupio najviše proizvoda. Također, sada kada smo zapisali upit pomoću *subsearch* funkcionalnosti, možemo mijenjati i vremenski period pretrage.

Sada je potrebno analizirati koje je artikle taj korisnik kupovao. Za to ćemo koristiti funkciju *stats*, koja se može koristiti za izračun statistika. Upišite sljedeći upit:

```
status=200 action=purchase
[search status=200 action=purchase | top limit=1 clientip | table clientip]
| stats count AS "Total Purchased", dc(productId) AS "Total Products",
values(productId) AS "Product Name" BY clientip
```



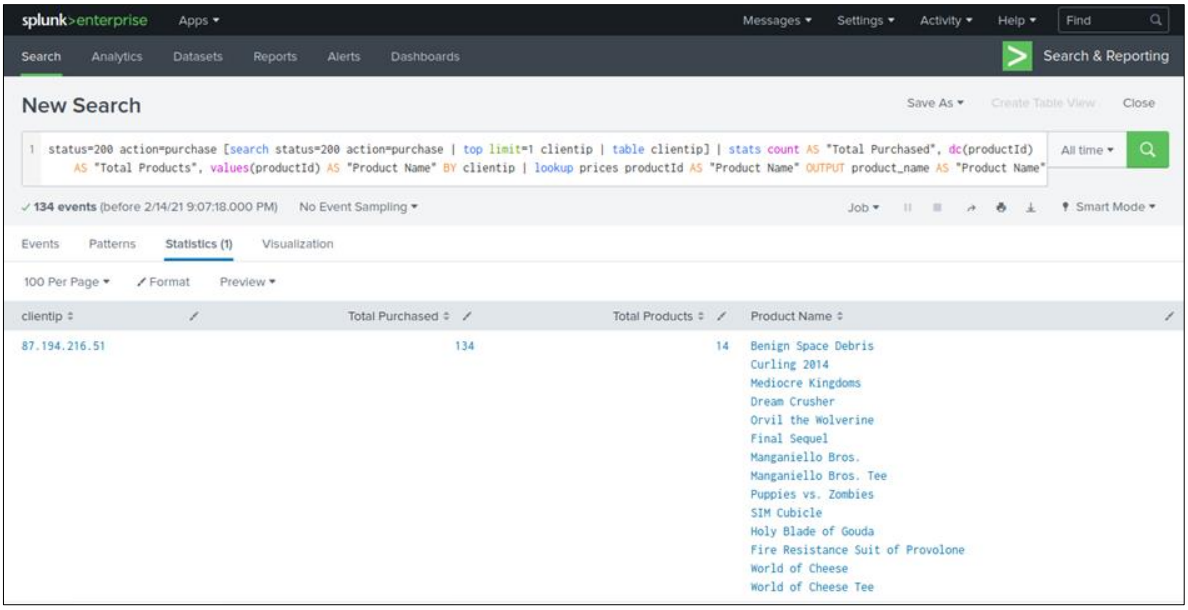
Slika 51 – Prikaz upita gdje tražimo sve kupljene artikle od klijenta s najvećim brojem kupnji

Naš *subsearch* je pronašao najboljeg kupca, glavna pretraga je filtrirala samo njegove kupnje, te nam je *stats* funkcija prikazala sveukupni broj kupnji (pomoću funkcije `count`), broj različitih proizvoda (pomoću funkcije `dc`, engl. *distinct count,* za brojanje jedinstvenih vrijednosti) i šifre kupljenih artikla. Ključnom riječi `AS` stupci izlazne tablice su preimenovani.

Malo je nezgodno što su u zapisima spomenute samo šifre artikla, a ne njihova imena. Kako bismo zamijenili ove šifre s pravim imenima artikla, koristiti ćemo prethodno učitanu *lookup* datoteku. Na kraj gornjeg upita, pozovimo funkciju *lookup*:

```
status=200 action=purchase
[search status=200 action=purchase | top limit=1 clientip | table clientip] | stats
count AS "Total Purchased", dc(productId) AS "Total Products", values(productId) AS
"Product Name" BY clientip
| lookup prices productId AS "Product Name" OUTPUT product_name AS "Product Name"
```

Na slici 52 vidimo da smo funkcijom *lookup* zamijenili šifre artikla s pravim imenima, onako kako je to definirano u datoteci *prices.csv*.

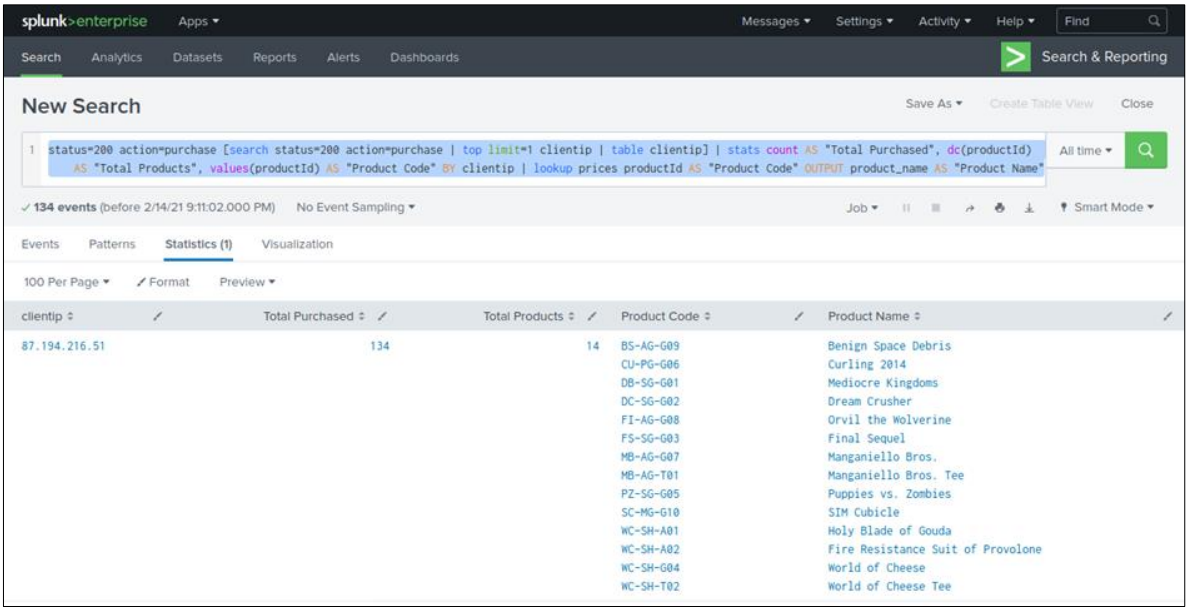


Slika 52 – Primjer *lookup* upita s kojim mijenjamo dio izlaznih vrijednosti u druge vrijednosti

Ako želimo prikazati isti upit no ostaviti kodove artikla, potrebno je malo izmijeniti upit:

```
status=200 action=purchase
[search status=200 action=purchase | top limit=1 clientip | table clientip] | stats count AS "Total Purchased", dc(productId) AS "Total Products", values(productId) AS "Product Code" BY clientip
| lookup prices productId AS "Product Code" OUTPUT product_name AS "Product Name"
```

Na slici 53 vidimo iste rezultate, samo što je ovaj put *lookup* funkcija dodala ime artikla u tablicu.



Slika 53 – Primjer *lookup* upita kojim dodajemo informacije o šifri proizvoda izlaznoj tablici

Detaljni opisi svih funkcija pretraga i primjeri njihove primjene mogu se pronaći u službenoj *Splunk* dokumentaciji.

4 Zaključak

Splunk Free je moćan alat za centralno prikupljanje, pretragu, analizu i vizualizaciju zapisa poput dnevnika (engl. *logs*) i raznih metrika.

Splunk podržava i brojne dodatke (tzv. *Splunk Apps*) koji mu proširuju mogućnosti. Primjerice, postoje dodatci koji:

- pružaju bolju integraciju s Cisco mrežnom opremom;
- automatski kreiraju nadzorne ploče (engl. *dashboard*) za različite scenarije;
- mogu poslati notifikaciju na *Slack* ili *Microsoft Teams.*

Sve aplikacije i dodatke moguće je pronaći na službenim *Splunk* stranicama.

U ovom je dokumentu opisano kako instalirati *Splunk Enterprise*, kako ga prebaciti na *Splunk Free* licencu, kako instalirati *Splunk Universal Forwarder* te kako koristiti osnovne funkcionalnosti *Splunka Free*. *Splunk Free* pruža brojne funkcionalnosti, no u produkcijskom okruženju, neka ograničenja *Splunka Free* mogu biti ozbiljan nedostatak.

Primjerice, za manja okruženja, ograničenje od 500MB prikupljenih podataka dnevno te nedostatak alarma/notifikacija možda nije problem. No kada to okruženje naraste, gotovo je sigurno da će količina podataka premašiti to ograničenje te da će alarmi postati nezaobilazna funkcionalnost. U toj će situaciji biti potrebno prijeći na *Splunk Enterprise* licencu koja nije besplatna, već ima nekoliko različitih modela plaćanja (ovisno o količini unesenih podataka, broju jezgri i slično).

Alternativno, postoje i drugi sustavi koji pružaju funkcionalnosti slične *Splunku Free* i *Enterprise*. Jedna od najpopularnijih alternativa je tzv. ELK *stack*, kombinacija tri paketa slobodnog softvera (engl. *free and open source software*): *Elasticsearch*, *Logstash* i *Kibana*. I *Splunk* i ELK *stack* su relativno veliki, složeni sustavi, tako da im se funkcionalnosti ne preklapaju u potpunosti, no načelno, oba sustava služe za rješavanje istog problema (centralizirano prikupljanje, pretraga, analiza i vizualizacija podataka).

Uz ELK *stack*, popularni su i Graylog (koji je specijaliziran za centralno prikupljanje i analizu dnevnika) te Prometheus zajedno s Grafanom (koji su specijalizirani za prikupljanje i analizu metrika poput postotka korištenosti CPU-a ili broja HTTP zahtjeva po sekundi). Kao i ELK *stack*, *Graylog*, *Prometheus* i *Grafana* također imaju slobodnu licencu (engl. *free and open source software*).