بسمه تعالی

آموزش فنی نصب و پیکربندی Splunk (بخش دوم)

فهرست مطالب

۱ مقدمه

با توجه به تولید انبوه داده‌های خام با انواع مختلف در فضای مجازی، دسته‌بندی و استخراج مضامین خاص از آن‌ها، در دنیای امروز اهمیت ویژه‌ای پیدا کرده است. نرم‌افزار Splunk محصول اصلی شرکت Splunk می باشد که برای این هدف گسترش داده شده است. این شرکت در سال ۲۰۰۳ میلادی شروع به کار کرده و تمرکز اصلی آن در تولید محصولات Big Data و SIEM است که این موضوع تمایز اصلی محصول این شرکت با سایر رقبا می‌باشد. این نرم‌افزار جست‌وجو و تحلیل داده و انواع داده‌ای مختلف را از برنامه کاربردی، سرویس‌دهنده یا دستگاه‌های شبکه، به‌صورت بی‌درنگ امکان‌پذیر می‌نماید. این داده‌ها می‌توانند داده‌های پیغام، هشدار، اسکریپت، تنظیمات، لاگ‌ها و هر نوع معیاری در هر مکانی باشند.

Splunk در دو نسخه آزمایشی و شرکتی موجود است. در نسخه آزمایشی[۱] که رایگان است، مجموع داده‌ای که می‌توان به‌صورت روزانه import کرد، محدود به ۵۰۰ مگابایت می‌شود و بعضی امکانات مانند Alerting/monitoring را ندارد. این نسخه در یک محیط غیرتجاری و با ویژگی‌های محدود مورد استفاده قرار می‌گیرد. علاوه بر این، می‌توان با نصب و استفاده از افزونه‌های مختلف روی Splunk Enterprise که اکثراً به صورت رایگان ارائه می‌شوند، از این نرم‌افزار، به‌عنوان یک نرم‌افزار مانیتورینگ استفاده کرد. به‌عنوان مثال Splunk DBConnect، یک افزونه بانک اطلاعاتی SQL است که اجازه می‌دهد اطلاعات بانک اطلاعاتی با پرس‌وجوهای Splunk یکپارچه شوند.

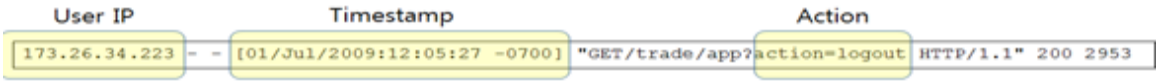
اصلی‌ترین مفهوم در Splunk رخداد[۲] می‌باشد. رخداد، هر رکوردی است که در یک فایل لاگ ثبت می‌شود. هر رخداد شامل موارد برچسب زمانی ایجاد رخداد و همچنین اطلاعاتی درباره اتفاقات روی سیستم است. هر رخداد، مرتبط با چند فیلد ازجمله برچسب زمانی، نوع منبع و میزبان[۳] می‌باشد. نوع رخداد نیز روشی است که به کاربر اجازه می‌دهد تا رخدادهای یکسان را طبقه‌بندی نماید و جست‌وجوهای بامعنا را بسته به نیاز خود تعریف کند. شکل ۱ نمونه‌ای از رخداد را نشان می‌دهد.

---

[۱] Trial

[۲] Event

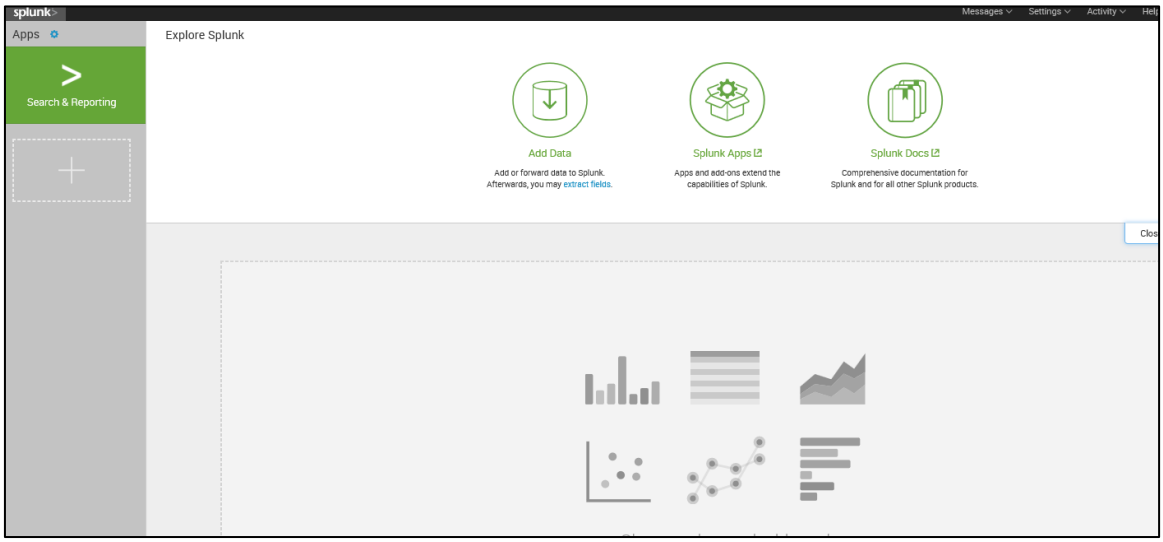
[۳] Host



شکل ۱ نمونه ای از رخداد

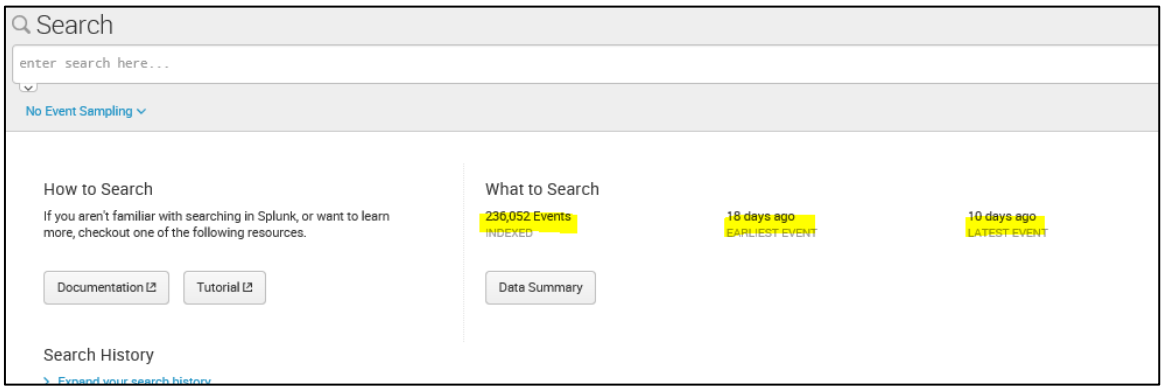
۲ نمای کلی نرم‌افزار

بعد از ورود به Splunk نمای اصلی مانند شکل ۲ است. در این صفحه یک منو با دسترسی سریع وجود دارد. به‌عنوان مثال، می‌توانیم از Add Data داده‌ای را اضافه نماییم، با Splunk apps نرم‌افزارهای مرتبط را اضافه کنیم، با Splunk docs مستندات مرتبط با این Splunk را مشاهده کنیم، و یا می‌توانیم داشبوردهایی که قبلاً تعریف نموده‌ایم را مشاهده نماییم. در هر کدام از صفحات چنان‌چه بخواهیم به صفحه‌ی Home بازگردیم، لازم است روی لوگوی Splunk کلیک کنیم.



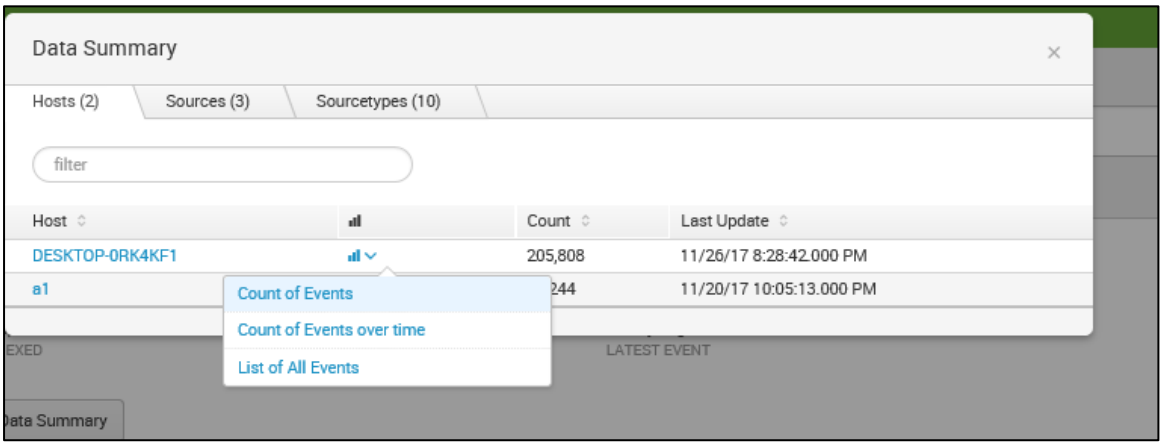
شکل ۲ نمای کلی از صفحه اصلی

چنان‌چه Search & Reporting را انتخاب کنیم، وارد صفحه جست‌وجو (شکل ۳) می‌شویم. در این صفحه با وارد کردن عبارت جست‌وجو، اطلاعات کلی از تعداد رخدادها و اولین و آخرین زمان روی دادن آن‌ها، نمایش داده می‌شود. این موارد در شکل ۳ مشخص شده است.



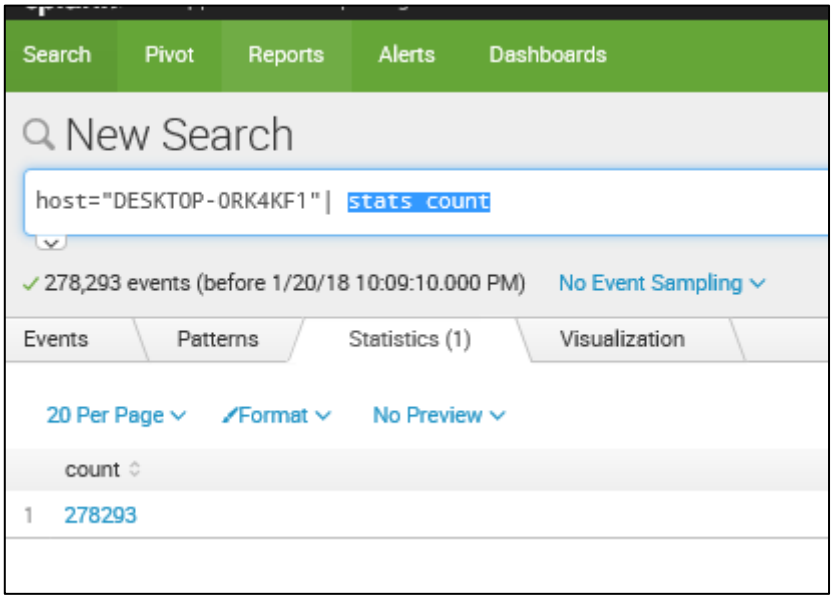
شکل ۳ نمای کلی از صفحه جست‌وجو

چنان‌چه بر روی دکمه Data summary کلیک کنیم، پنجره جدیدی مطابق شکل ٤ باز می‌شود که دارای سه برگه با نام‌های Hosts، Sources و Sourcetypes می‌باشد. در هر برگه اطلاعات مرتبط نشان داده می‌شود.



شکل ٤ نمای پنجره Data summary

عبارات با رنگ آبی در شکل ٤، لینکی برای جست‌وجوی بیشتر هستند. به‌عنوان مثال، می‌توان بر حسب تعداد رخدادها یک جست‌وجو داشت. در این شکل چنان‌چه بر روی Count of Events کلیک کنیم، پنجره جست‌وجو مطابق شکل ۵ باز می‌شود. عبارت stats count را به‌عنوان عبارت جست‌وجو وارد می‌کنیم و در خروجی تعداد رخدادها بر روی host را خواهیم داشت.



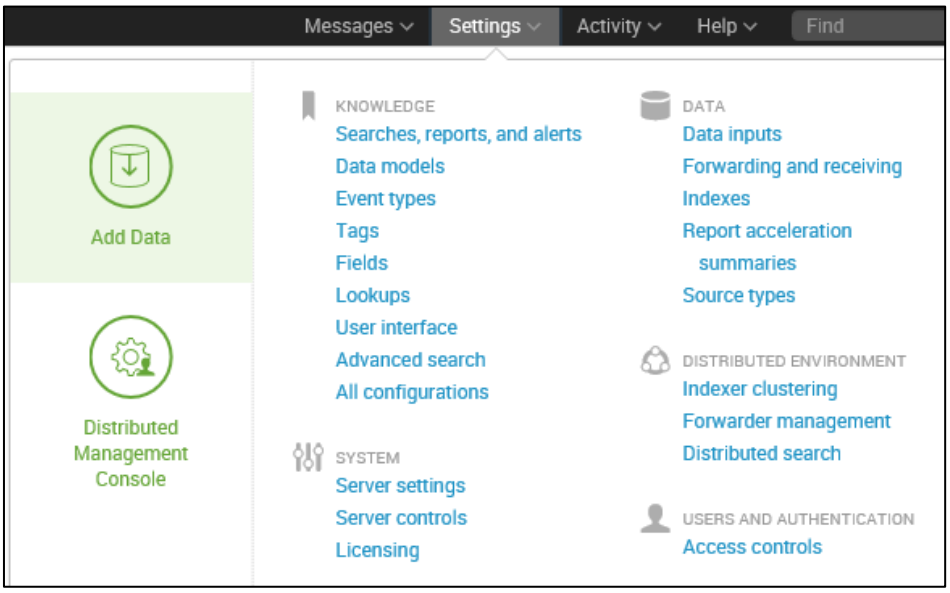
شکل ۵ پنجره جست‌وجو

۳ انتقال داده[۴]

برای انتقال داده به نرم‌افزار نیاز به منبع داده[۵] است که این منبع، داده ورودی می‌باشد. Splunk Enterprise جریان داده را شاخص‌گذاری می‌کند و آن را به مجموعه‌ای از رخدادها تبدیل می‌نماید. اگر Splunk Enterprise داشته باشیم، داده می‌تواند به عنوان نمایه‌ساز[۶] بر روی همان ماشین (داده محلی) و یا بر روی ماشین دیگری باشد (داده از راه دور). اگر Splunk Cloud داشته باشیم، داده بر روی شبکه مشترک قرار دارد و می‌توان آن را به Splunk Cloud فرستاد. همچنین می‌توان از طریق شبکه یا با نصب Splunk forwarderها، داده از راه دور را بر روی میزبان‌هایی که داده را تولید می‌نمایند، دریافت نمود.

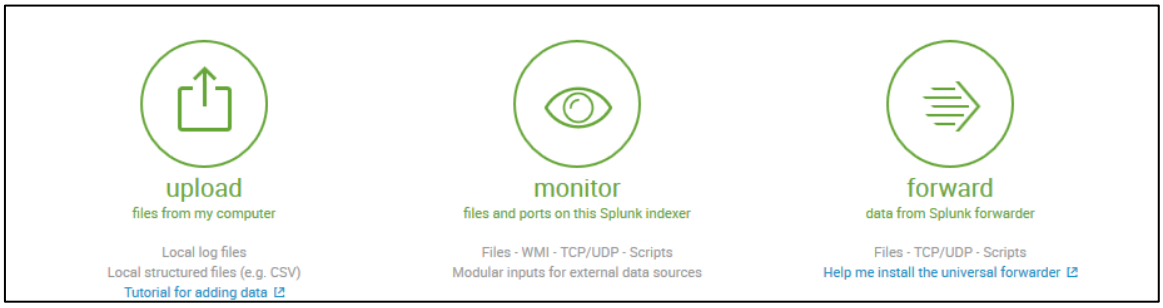
برای انتقال داده مطابق شکل ٦ از سربرگ Settings گزینه Add Data را انتخاب می‌کنیم. در این صفحه مطابق شکل ۷ سه گزینه خواهیم داشت.

[۴] Import
[۵] Data source
[۶] Indexer



شکل ٦ نمایش منو

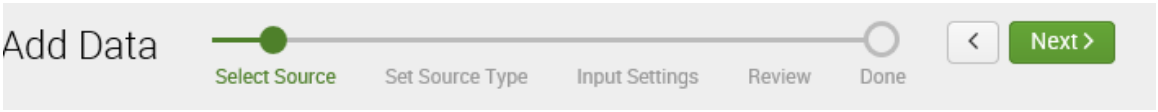
گزینه upload برای اضافه‌کردن یک فایل یا آرشیو فایل از روی کامپیوتر به‌صورت آفلاین و برای شاخص گذاری است. گزینه monitor اجازه مانیتور کردن یک یا چند فایل، دایرکتوری، جریان شبکه، لاگ‌های رخداد، معیارهای کارآیی، و یا هر نوع داده‌ای که Splunk Enterprise دسترسی به آن دارد، را می‌دهد. گزینه forward نیز اجازه دریافت داده از forwarderها به صورت بی‌درنگ را به Splunk می‌دهد. در ادامه این گزینه‌ها بیشتر توضیح داده می‌شوند.



شکل ٧ زیر منوها

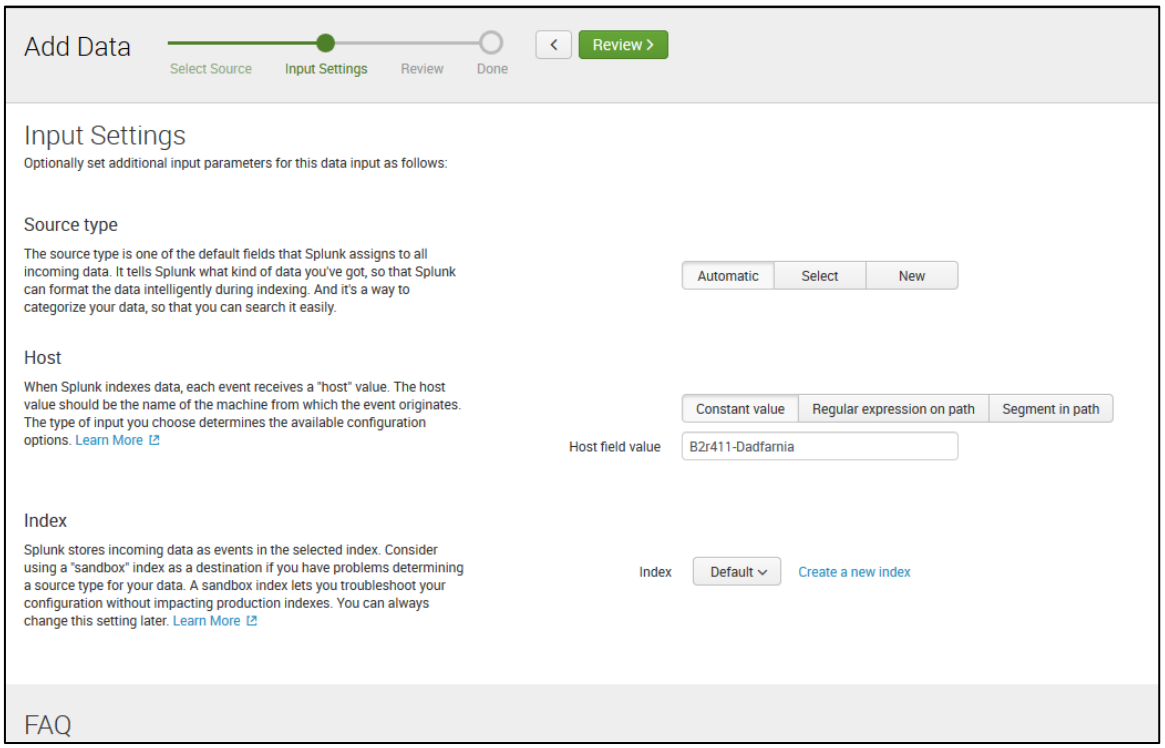
۳-۱ گزینه upload

برای اضافه‌کردن فایل از روی کامپیوتر، گزینه upload را انتخاب می‌کنیم. این عملیات، مطابق شکل ۸، شامل سه مرحله اصلی می‌باشد.



شکل ۸ مراحل اضافه نمودن فایل ورودی

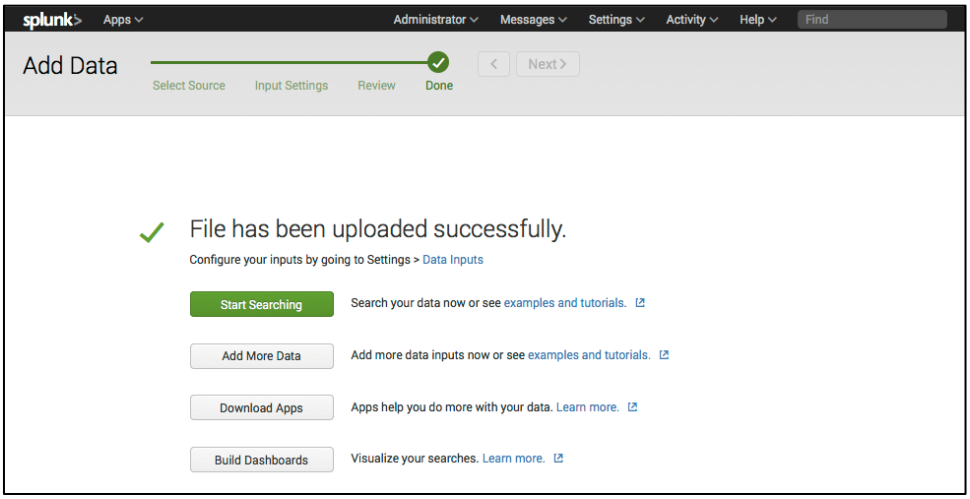
- در مرحله اول (Select Source) دکمه select file را انتخاب کرده و فایل مورد نظر را به‌عنوان ورودی به آن می‌دهیم. می‌توان فایل لاگ ویندوز را از مسیر C:\Windows\WindowsUpdate.log به‌عنوان ورودی به آن داد و یا در صورت نیاز از آدرس http://docs.Splunk.com/images/Tutorial/tutorialdata.zip داده تستی دانلود کرد. چنان‌چه نرم‌افزار Splunk، نوع داده این منبع را بشناسد، مرحله Set Source Type را نخواهیم دید.
- در مرحله دوم (Set Source Type) نوع منبع را انتخاب می‌کنیم، که نشان می‌دهد داده از چه نوعی است. نوع داده در حالت پیش‌فرض data است. Source Typeها می‌توانند برای تعریف قوانین برای رخدادها به‌کار روند. در واقع Splunk تشخیص می‌دهد که نوع داده چیست و بنابراین می‌تواند آن را به‌صورت مناسب شاخص‌گذاری نماید. انواع داده‌ای متفاوت برای پایگاه‌داده، سیستم‌عامل، شبکه، امنیت و غیره وجود دارد.
- در مرحله سوم (Input Setting) شکل ۹ را خواهیم داشت که تنظیمات ورودی Source type، Host و Index را انتخاب می‌کنیم. در قسمت Source type چنان‌چه Automatic انتخاب شود، نرم‌افزار نوع داده این منبع را به‌صورت خودکار تشخیص می‌دهد. در این قسمت می‌توان نوع ورودی پیش‌فرض یا تعریف شده را انتخاب یا ایجاد نمود. Splunk هنگام شاخص‌گذاری داده، به هر رخداد یک مقدار Host می‌دهد که باید نام ماشین ایجاد کننده رخدادها باشد. در قسمت Index می‌توان شاخص‌های پیش‌فرض یا تعریف شده را انتخاب و یا شاخصی را ایجاد نمود. در بخش‌های بعدی در مورد نوع ورودی‌ها و شاخص‌ها توضیح داده می‌شود.



شکل ۹ مرحله سوم

- در مرحله چهارم انتخاب‌های قبلی نشان داده شده و می‌توانیم آن را تأیید نماییم.

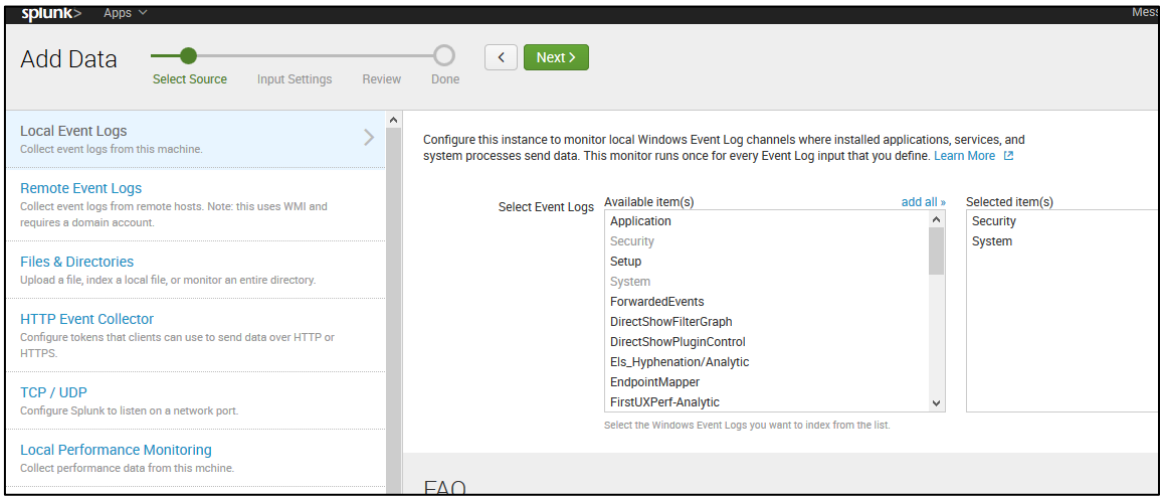
پس از آن شکل ۱۰ نمایش داده می‌شود که با کلیک بر روی Start Searching می‌توان داده را در محیط جست‌وجو دید، و یا با کلیک بر روی Add More Data می‌توان داده‌های بیشتری را اضافه نمود.



شکل ۱۰ مرحله چهارم

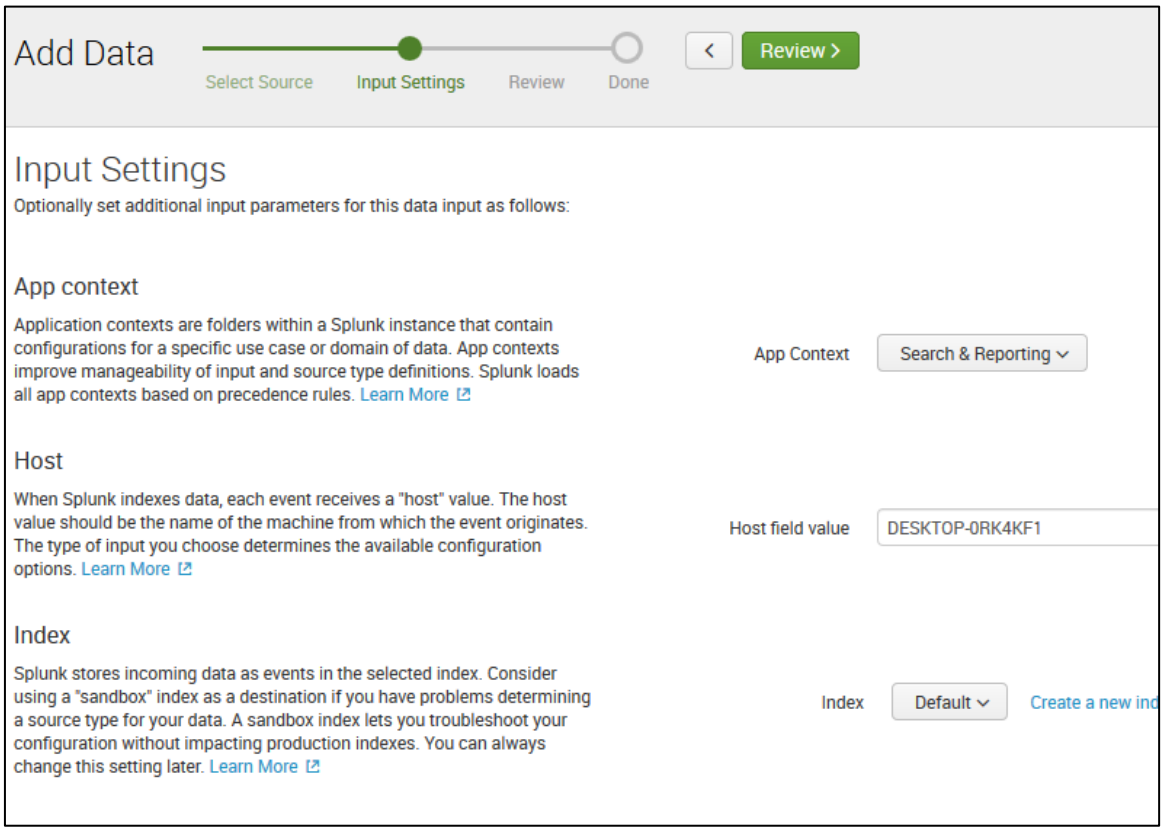
۲-۳ گزینه monitor

این گزینه برای مانیتور کردن منابع موجود می‌باشد. با انتخاب این گزینه صفحه‌ای باز می‌شود که در این صفحه می‌توانیم نوع داده‌ای که می‌خواهیم مانیتور شود را مشخص نماییم. ورودی‌های پیش‌فرض در ابتدای صفحه، و در ادامه ورودی‌های فوروارد شده و هر نوع داده ماژولار لیست شده‌اند. در این صفحه بسته به نسخه Splunk (Splunk Enterprise یا Splunk Cloud) و پلت‌فرمی‌که Splunk بر روی آن اجرا می‌شود، نوع‌های داده‌ای که می‌توانیم مانیتور کنیم را نمایش می‌دهد. به‌عنوان مثال، چنان‌چه گزینه Local Evnet Logs را انتخاب نماییم، لاگ‌های گرفته شده از این ماشین را نمایش می‌دهد. در این صفحه می‌توان نوع لاگ‌های رخداد را انتخاب کرد. مطابق شکل ۱۱، security و system و سپس دکمه next را انتخاب کردیم.



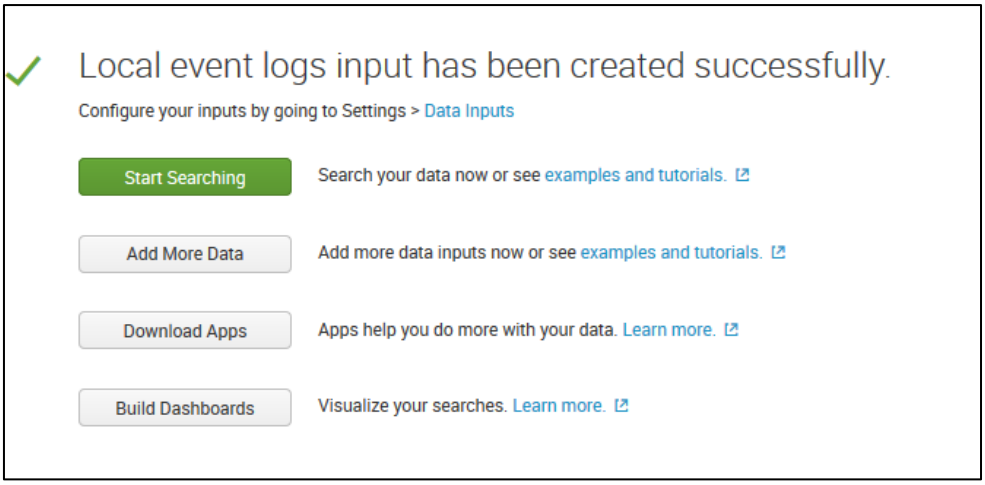
شکل ۱۱ انتخاب لاگ‌های رخداد

در صفحه بعدی که مطابق شکل ۱۲ نمایش داده می‌شود، محتوای داده، میزبان و شاخص مورد نظر را انتخاب کرده و به مرحله بعد می‌رویم که تأیید و بازبینی انتخاب‌ها انجام می‌شود.



شکل ۱۲ تنظیمات ورودی برای مانیتور کردن

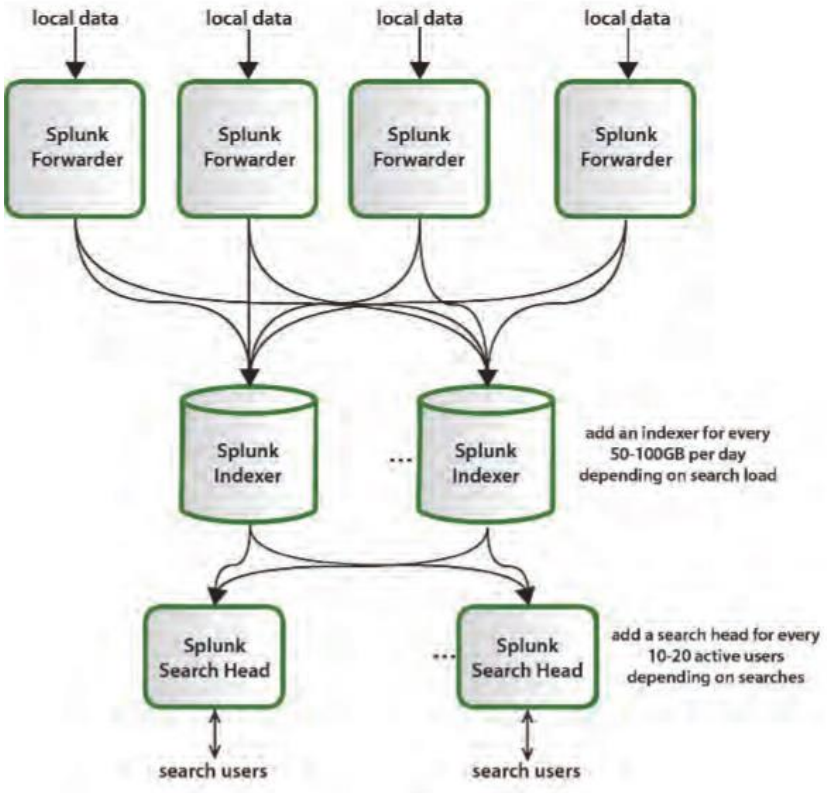
در نهایت مطابق شکل ۱۳ پیغام می‌دهد که لاگ‌های رخداد را به‌صورت موفقیت‌آمیز ایجاد نموده است. چنان چه دکمه Start Searching را فشار دهیم، وارد صفحه جست‌وجو شده و لاگ‌های ویندوز نمایش داده می‌شود. اگر پنجره Source Types را باز کنیم دو نوع ورودی WinEventLog:Security و WinEventLog:System به مجموعه قبلی اضافه شده است.



شکل ۱۳ ایجاد لاگ‌های رخداد

۳-۳ گزینه forward

فورواردرها داده را می‌گیرند و به Splunk شما برای شاخص‌گذاری می‌فرستند. با توجه به این‌که فورواردرها منابع محدودی را در اختیار می‌گیرند، اثر کمی بر پایین آوردن کارایی سرویس‌دهنده‌ای دارند که اطلاعات را جمع‌آوری می‌کند. علاوه بر این، می‌توان بر روی همه دسکتاپ‌های ویندوزی کاربران، فورواردر را نصب نمود تا بتوان لاگ‌های مختلف داشت و برای بدافزار یا موارد دیگر بررسی کرد. نمونه ای از Splunk که داده را از یک یا چند فورواردر دریافت می‌کند، دریافت‌کننده[۷] نامیده می‌شود. دریافت‌کننده، اغلب یک Splunk indexer است، اما می‌تواند یک فورواردر دیگر نیز باشد. شکل ۱٤ چهار فورواردر را نشان می‌دهد که داده را به دو دریافت‌کننده (نمایه‌ساز) می‌فرستند. در ادامه داده را شاخص‌گذاری می‌کند و آن را برای جست‌وجو موجود می‌سازد.



شکل ۱٤ مثالی از فورواردر و نمایه‌ساز

[۷] Receiver

۳-۳-۱ انواع forwarder

به‌طور کلی سه نوع forwarder وجود دارد:

- Universal forwarder

وقتی داده‌ای که می‌خواهیم جمع‌آوری کنیم، مستقیماً بر روی سرویس‌دهنده‌ای که Splunk روی آن نصب شده است قرار نداشته باشد، Splunk Universal Forwarder می‌تواند بر روی سرویس‌دهنده از راه دور نصب شود و داده را به سمت Splunk Enterprise، Splunk Light یا Splunk Cloud هدایت نماید. Universal forwarder شبیه به سرویس‌دهنده Splunk است و تنها ماژول‌هایی را شامل می‌شود که برای فوروارد کردن داده ضروری هستند، و به‌صورت جداگانه بسته قابل نصب موجود می‌باشند.

- Heavy forwarder

یک نمونه کامل از Splunk Enterprise است که می‌تواند علاوه بر فوروارد کردن، داده را شاخص‌گذاری کند، جست‌وجو کند و تغییر دهد. Heavy forwarder ویژگی‌هایی دارد که برای کاهش کاربرد منابع سیستم غیرفعال شده است.

- Light forwarder

یک نمونه کامل از Splunk Enterprise می‌باشد که ویژگی‌هایی بیشتری از آن، نسبت به Heavy forwarder، برای کاهش کاربرد منابع سیستم غیرفعال شده است.

بهترین ابزار برای فرستادن داده به نمایه‌سازها Universal forwarder می‌باشد. تنها محدودیت آن این است که فقط داده خام را فوروارد می‌کند و برای فرستادن داده‌های برمبنای رخداد[۸] به نمایه‌سازها باید از Heavy forwarder استفاده نمود. مزیت بزرگ Heavy forwarder نسبت به دو فورواردر دیگر این است که می‌توان داده را به‌صورت محلی شاخص‌گذاری کرده و به یک شاخص دیگر فوروارد کرد. اما شاخص‌گذاری محلی به‌صورت پیش‌فرض غیرفعال بوده و لازم است به‌صورت دستی و یا با ویرایش فایل outputs.conf این قابلیت را فعال کرد. جدول زیر شباهت‌ها و تفاوت‌های این سه فورواردر را نشان می‌دهد.

---

۸ Event-based

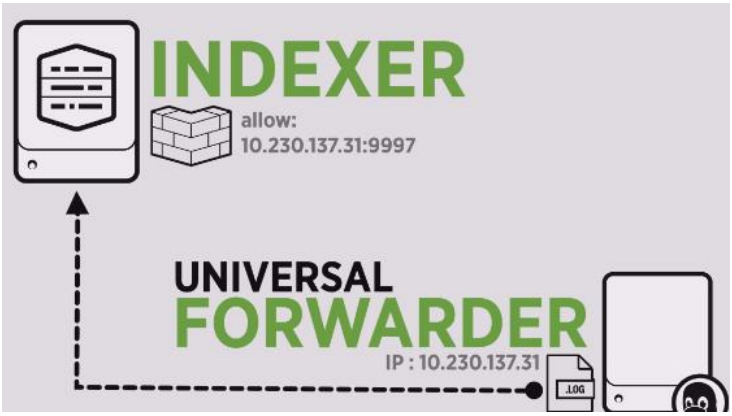
جدول ۱ مقایسه فورواردرهای مختلف در Splunk

Features and capabilities	Universal forwarder	Light forwarder	Heavy forwarder
Type of Splunk Enterprise instance	Dedicated executable	Full Splunk Enterprise, with most features disabled	Full Splunk Enterprise, with some features disabled
Footprint (memory, CPU load)	Smallest	Small	Medium-to-large (depending on enabled features)
Bundles Python?	No	Yes	Yes
Handles data inputs?	All types (but scripted inputs might require Python installation)	All types	All types
Forwards to Splunk Enterprise?	Yes	Yes	Yes
Forwards to 3rd party systems?	Yes	Yes	Yes
Serves as intermediate forwarder?	Yes	Yes	Yes
Indexer acknowledgment (guaranteed delivery)?	Optional	Optional (version 4.2 and later)	Optional (version 4.2 and later)
Load balancing?	Yes	Yes	Yes
Data cloning?	Yes	Yes	Yes
Per-event filtering?	No	No	Yes
Event routing?	No	No	Yes
Event parsing?	Sometimes	No	Yes
Local indexing?	No	No	Optional, by setting `indexAndForward` attribute in `outputs.conf`

Searching/alerting?	No	No	Optional
Splunk Web?	No	No	Optional

۳-۳-۲ تنظیمات لازم برای forward

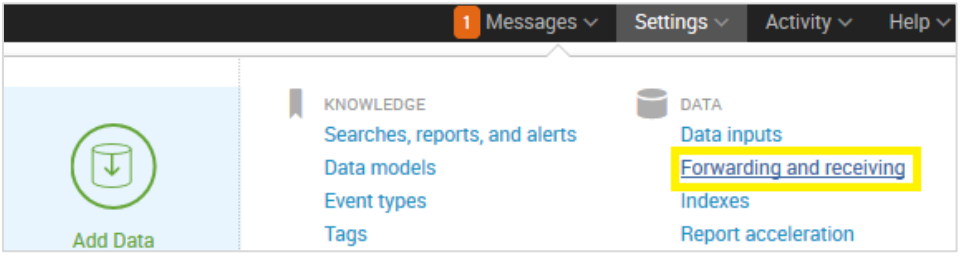
فرض کنید بخواهیم سناریوی شکل ۱۵ را انجام دهیم؛ یعنی داده‌هایی از میزبان 10.230.137.31 را از پورت ۹۹۹۷ دریافت کرده و در سرویس‌دهنده Splunk یا نمایه‌ساز خود ثبت نماییم. در این حالت لازم است تنظیمات لازم بر روی نمایه‌ساز و فورواردر را انجام دهیم.



شکل ۱۵ مثالی از یک سناریو

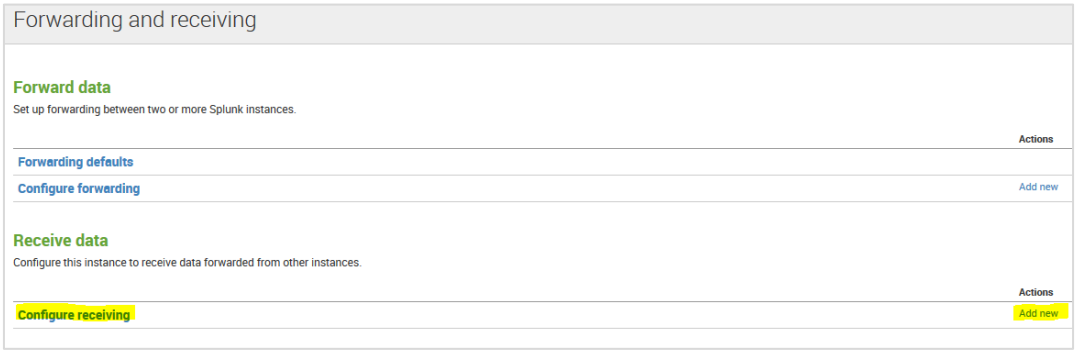
۳-۳-۲-۱ تنظیم نمایه‌ساز

برای تنظیم نمایه‌ساز در Splunk گزینه Forwarding and receiving را مطابق شکل ۱۶ از منوی Settings بخش data انتخاب می‌کنیم.



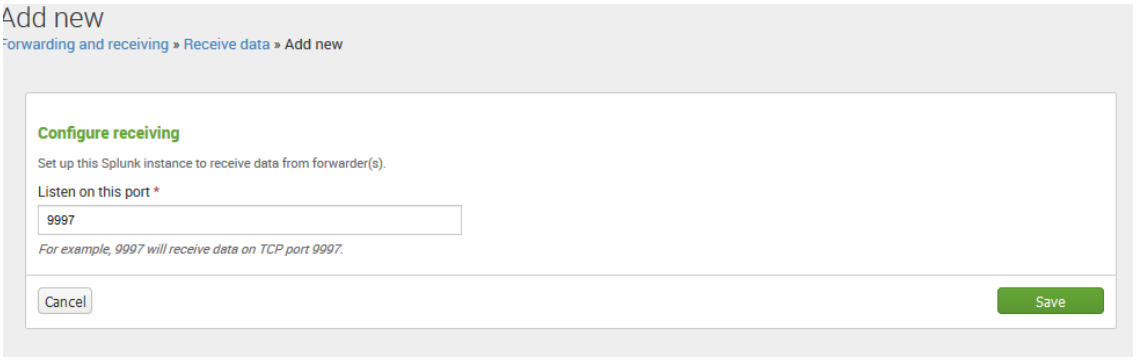
شکل ۱۶ تنظیمات دریافت کننده

سپس در صفحه نشان داده شده (شکل ۱۷) از قسمت Receive data بر روی Add new کلیک می‌کنیم.



شکل ۱۷ تنظیم دریافت‌کننده

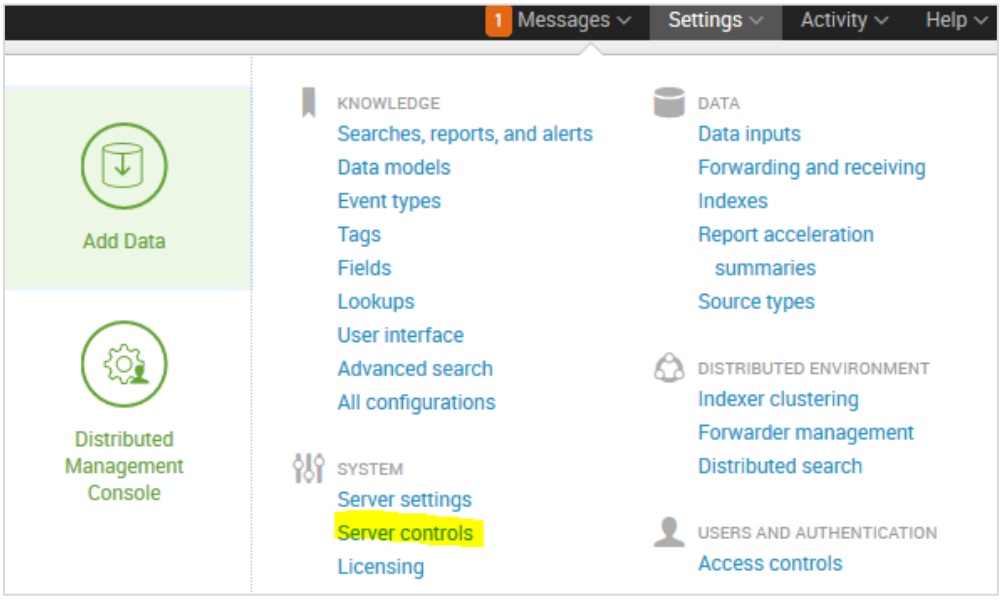
در صفحه باز شده (شکل ۱۸)، پورت ۹۹۹۷ را به‌عنوان پورت دریافت‌کننده وارد می‌نماییم.



شکل ۱۸ تعریف پورت برای دریافت‌کننده

در صفحه بعد نشان می‌دهد که پورت به‌عنوان دریافت‌کننده ثبت شده است و می‌توان آن را حذف یا غیرفعال نمود.

در ادامه لازم است که Splunk را راه‌اندازی مجدد کنیم. برای این منظور از گزینه Settings قسمت SYSTEM، لینک Server controls (شکل ۱۹) را انتخاب می‌نماییم و از آنجا دکمه Restart Splunk را فشار می‌دهیم.



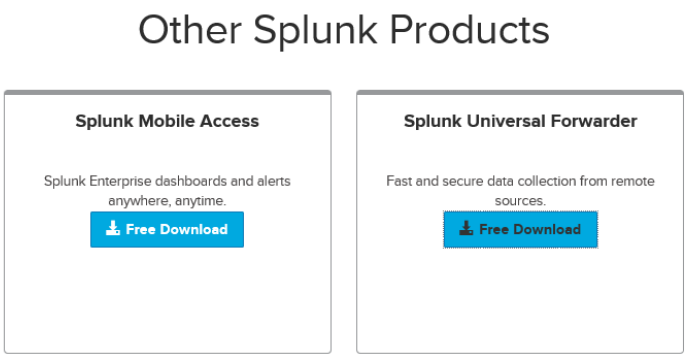
شکل ۱۹ زیر منوی لازم برای راه‌اندازی مجدد نرم افزار

۳-۳-۲-۲ تنظیم فورواردر

بعد از انجام تنظیمات نمایه‌ساز، لازم است تنظیمات مربوط به فورواردرها را نیز انجام دهیم. همان‌طور که گفتیم سه نوع فورواردر داریم که در ادامه به تنظیمات مربوط به آن‌ها اشاره می‌شود.

- Universal forwarder

برای این منظور در سایت Splunk به آدرس splunk.com وارد می‌شویم. گزینه Free Splunk و سپس Splunk Universal Forwarder را مطابق شکل ۲۰ انتخاب کرده و آن را بسته به پلت‌فرمی‌که فورواردر دارد دانلود می‌نماییم.



شکل ۲۰ دانلود Universal Forwarder

در ادامه مطابق شکل ۲۱ فایلی که دانلود کردیم را حالت فشرده خارج کرده و درون دایرکتوری Opt می‌ریزیم.

شکل ۲۱ باز کردن فایل دانلود شده از حالت فشرده

سپس وارد دایرکتوری splunkforwarder/bin می‌شویم و دستورات زیر را وارد می‌کنیم.

$ sudo ./splunk start –accept-license

$ sudo ./splunk enable boot-start

کاربر admin سیستم را ویرایش می‌کنیم و کلمه عبور آن را با دستور زیر از changeme (کلمه عبور پیش فرض) به goodpass تغییر می‌دهیم.

$ sudo ./splunk edit user admin –password goodpass –role admin –auth admin:changeme

برای این‌که اطلاعات به سرویس‌دهنده فوروارد شود دستور زیر را وارد می‌نماییم. در این دستور با auth– نام کاربری و کلمه عبور را وارد کرده و اطلاعات را به سرویس‌دهنده Splunk می‌فرستیم.

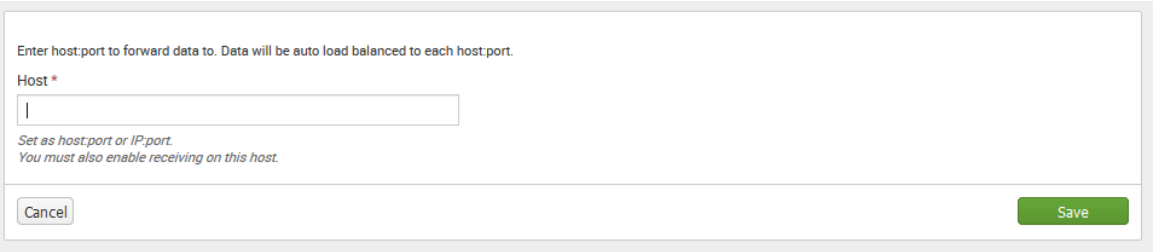
$ sudo ./splunk add forward-server 174.129.144.22:9997 –auth admin:goodpass

$ sudo ./splunk add monitor /opt/log/www1/

چنان‌چه مجدداً به Splunk وارد شویم و قسمت Data Summary را مشاهده نماییم، در تب Hosts میزبان 10.230.137.31 اضافه شده است.

- Heavy forwarder

چنان‌چه بخواهیم Heavy forwarding را با Splunk تنظیم نماییم، در شکل ۱۷ بر روی گزینه Add new در قسمت Configure forwarding کلیک می‌نماییم. در این حالت شکل ۲۲ را خواهیم داشت که لازم است نام میزبان یا IP دریافت‌کننده Splunk را وارد نماییم. به‌عنوان مثال ممکن است receivingserver.com:9997 را وارد نمایید. برای پیاده‌سازی load-balanced forwarding می‌توان چندین میزبان را با علامت کاما مشخص نمود. برای این‌که شاخص‌گذاری محلی را فعال نماییم، در شکل ۱۷ گزینه Forwarding defaults را انتخاب و دکمه yes را می‌زنیم.



شکل ۲۲ تنظیم سرویس‌دهنده دریافت‌کننده

اگر بخواهیم از طریق CLI این کار را انجام دهیم، به آدرس $SPLUNK_HOME/bin/ می‌رویم و دستور زیر را وارد می‌نماییم.

Splunk enable app SplunkForwarder -auth <username>:<password>

در ادامه Splunk را ریست می‌کنیم. برای این‌که اطلاعات را از فورواردر به دریافت‌کننده بفرستیم دستور زیر را وارد می‌نماییم.

Splunk add forward-server <host>:<port> -auth <username>:<password>

- Light forwarder

به آدرس $SPLUNK_HOME/bin/ می رویم و دستور زیر را وارد می نماییم و در ادامه Splunk را ریست می نماییم.

Splunk enable app SplunkLightForwarder -auth <username>:<password>

برای این‌که عملیات فوروارد را شروع کنیم مطابق حالات قبل دستور زیر را وارد می‌نماییم.

Splunk add forward-server <host>:<port> -auth <username>:<password>

چنان‌چه بخواهیم عملیات فوروارد کردن را متوقف کنیم، دستور زیر را وارد می‌نماییم.

Splunk remove forward-server <host>:<port> -auth <username>:<password>

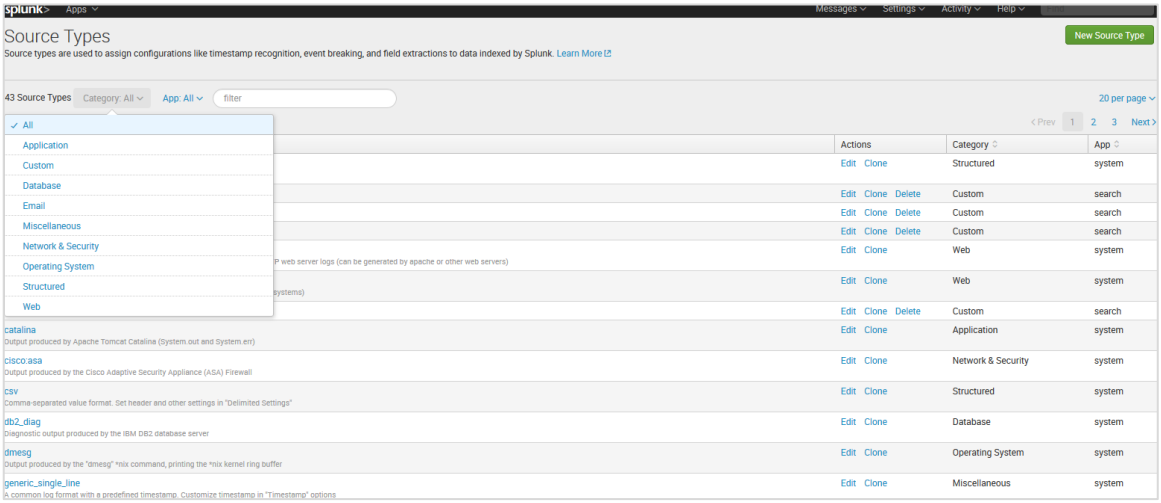
اگر عملیات فوروارد را متوقف کنیم، همچنان به‌عنوان فورواردر ثبت می‌شود. برای این‌که در Splunk Enterprise به عنوان فورواردر ثبت نشود از دستور disable استفاده می‌کنیم.

Splunk disable app SplunkForwarder -auth <username>:<password>

در صورتی که اطلاعات کافی داشته باشیم می‌توانیم با تغییر فایل outputs.conf، عملیات فوروارد کردن را انجام دهیم.

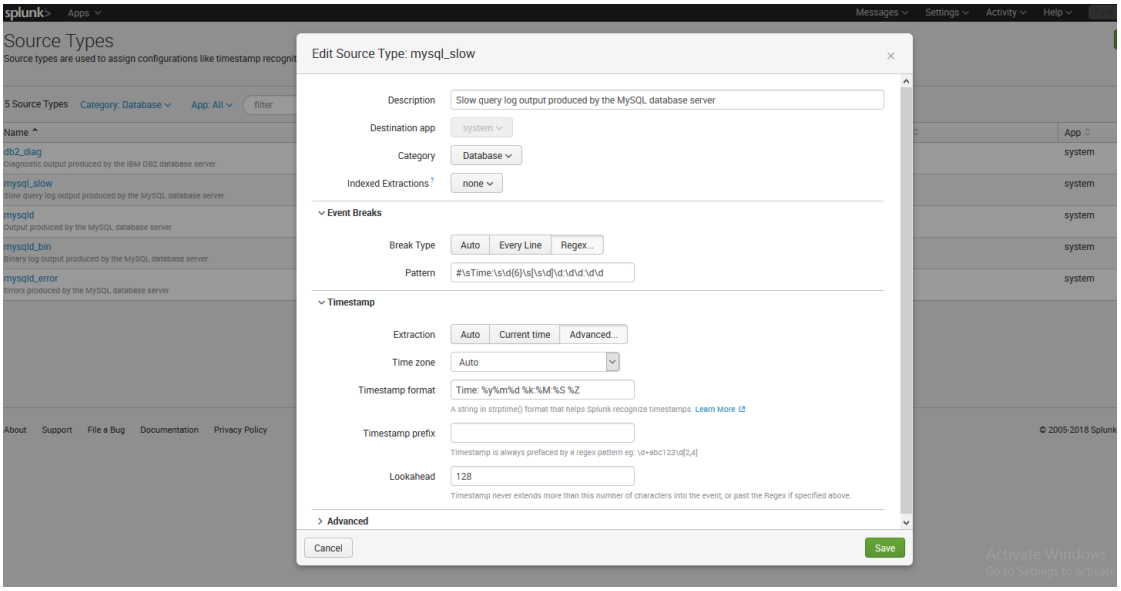
٤ مشاهده، ایجاد و حذف انواع داده

در نرم‌افزار Splunk، از منوی Settings قسمت Data لینک Source Types، مطابق شکل ۲۳، می‌توان همه انواع داده‌ای تعریف شده معمول را مشاهده کرد. می‌توان با کلیک بر روی ستون‌های "Name"، "Category" و "App" محتوای جدول را مرتب کرد.



شکل ۲۳ صفحه انواع داده‌ای

برای دیدن محتوای داده‌ای که به یک طبقه‌بندی خاص تعلق دارد، دکمه Category را از بالای صفحه انتخاب کرده و می‌توانیم نوع طبقه‌بندی داده که به آن تعلق دارد را انتخاب کنیم. این نوع داده‌ای می‌تواند ایمیل، بانک اطلاعاتی، برنامه کاربردی، سیستم‌عامل، شبکه و غیره باشد.



شکل ٢٤ ویرایش نوع داده

چنان‌چه Edit را انتخاب نماییم، می‌توانیم مطابق شکل ۲٤ نوع داده ای را ویرایش نماییم. می‌توانیم توضیحات دلخواه، محتوای برنامه، نوع طبقه‌بندی، فرمت استخراج‌کردن[۹] شاخص‌ها، و فرمت برچسب زمانی را به نوع داده اضافه نماییم. در این‌جا می‌توانیم انواع داده‌ای که تعریف نموده‌ایم را در صورت نیاز حذف کنیم. چند نمونه از انواع داده‌ای و محتوای آن‌ها در جدول ۲ نشان داده شده است. همان‌طور که مشخص است داده‌های خام متفاوت خواهند بود. Splunk با این انواع داده‌ای آشنا می‌باشد و نحوه شاخص‌گذاری آن را می‌تواند به صورت خودکار انجام دهد.

جدول ۲ چند نمونه از انواع داده‌ای تعریف‌شده در نرم‌افزار

Source type name	Origin	Examples
access_combined	NCSA combined format http web server logs (can be generated by apache or other web servers)	`10.1.1.43 - webdev [08/Aug/2005:13:18:16 -0700] "GET / HTTP/1.0" 200 0442 "-" "check_http/1.10 (nagios-plugins 1.4)"`
access_combined_wcookie	NCSA combined format http web server logs (can be generated by apache or other web servers), with cookie field added at end	`"66.249.66.102.1124471045570513" 59.92.110.121 - - [19/Aug/2005:10:04:07 -0700] "GET /themes/Splunk_com/images/logo_Splunk.png HTTP/1.1" 200 994 "http://www.Splunk.org/index.php/docs" "Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.7.8) Gecko/20050524 Fedora/1.0.4-4 Firefox/1.0.4" "61.3.110.148.1124404439914689"`
access_common	NCSA common format http web server logs (can be generated by apache or other web servers)	`10.1.1.140 - - [16/May/2005:15:01:52 -0700] "GET /themes/ComBeta/images/bullet.png HTTP/1.1" 404 304`
cisco_syslog	Standard Cisco syslog produced by all Cisco network devices including PIX firewalls, routers, ACS, etc., usually	`Sep 14 10:51:11 stage-test.Splunk.com Aug 24 2005 00:08:49: %PIX-2-106001: Inbound TCP connection denied from IP_addr/port to IP_addr/port flags TCP_flags on interface int_name Inbound TCP connection denied from 144.1.10.222/9876 to`

[۹] Extract

	via remote syslog to a central log host	`10.0.253.252/6161 flags SYN on interface outside`
db2_diag	Standard IBM DB2 database administrative and error log	`2005-07-01-14.08.15.304000-420 I27231H328 LEVEL: Event PID : 2120 TID : 4760 PROC : db2fmp.exe INSTANCE: DB2 NODE : 000 FUNCTION: DB2 UDB, Automatic Table Maintenance, db2HmonEvalStats, probe:900 STOP : Automatic Runstats: evaluation has finished on database TRADEDB`
linux_messages_syslog	Standard linux syslog (/var/log/messages on most platforms)	`Aug 19 10:04:28 db1 sshd(pam_unix)[15979]: session opened for user root by (uid=0)`
linux_secure	Linux securelog	`Aug 18 16:19:27 db1 sshd[29330]: Accepted publickey for root from ::ffff:10.2.1.5 port 40892 ssh2`
mysqld_error	Standard mysql error log	`050818 16:19:29 InnoDB: Started; log sequence number 0 43644 /usr/libexec/mysqld: ready for connections. Version: '4.1.10a-log' socket: '/var/lib/mysql/mysql.sock' port: 3306 Source distribution`
mysqld	Standard MySQL query log; also matches the MySQL binary log following conversion to text	`53 Query SELECT xar_dd_itemid, xar_dd_propid, xar_dd_value FROM xar_dynamic_data WHERE xar_dd_propid IN (27) AND xar_dd_itemid = 2`
sendmail_syslog	Standard Sendmail MTA log reported via the Unix/Linux syslog facility	`Aug 6 04:03:32 nmrjl00 sendmail[5200]: q64F01Vr001110: to=root, ctladdr=root (0/0), delay=00:00:01, xdelay=00:00:00, mailer=relay, min=00026, relay=[101.0.0.1] [101.0.0.1], dsn=2.0.0, stat=Sent (v00F3HmX004301 Message accepted for delivery)`
websphere_activity	Websphere activity log, also often referred to as the service log	`---------- -- ComponentId: Application Server ProcessId: 2580 ThreadId: 0000001c ThreadName: Non-deferrable Alarm : 3 SourceId: com.ibm.ws.channel.framework.impl. WSChannelFrameworkImpl ClassName: MethodName: Manufacturer: IBM Product: WebSphere Version: Platform 6.0 [BASE 6.0.1.0 o0510.18] ServerName: nd6Cell01\was1Node01\TradeServer1`

		TimeStamp: 2005-07-01 13:04:55.187000000 UnitOfWork: Severity: 3 Category: AUDIT PrimaryMessage: CHFW0020I: The Transport Channel Service has stopped the Chain labeled SOAPAcceptorChain2 ExtendedMessage: ----------

همچنین می‌توانیم در فایل props.conf نیز تغییرات لازم را برای تغییر نوع داده‌ای انجام دهیم. در واقع این فایل که در آدرس $SPLUNK_HOME/etc/system/local/ قرار دارد، تنظیمات داده را مشخص می‌کند. به عنوان مثال برای تعریف نوع داده‌ای access_combined می‌توان دستورات زیر را به فایل props.conf اضافه کرد.

```
[access_combined]
pulldown_type = true
maxDist = 28
MAX_TIMESTAMP_LOOKAHEAD = 128
REPORT-access = access-extractions
SHOULD_LINEMERGE = False
TIME_PREFIX = \[
category = Web
description = National Center for Supercomputing Applications (NCSA) combined fo
rmat HTTP web server logs (can be generated by apache or other web servers)

[source::/opt/weblogs/apache.log]
sourcetype = iis
```

۵ مشاهده، ایجاد و حذف شاخص

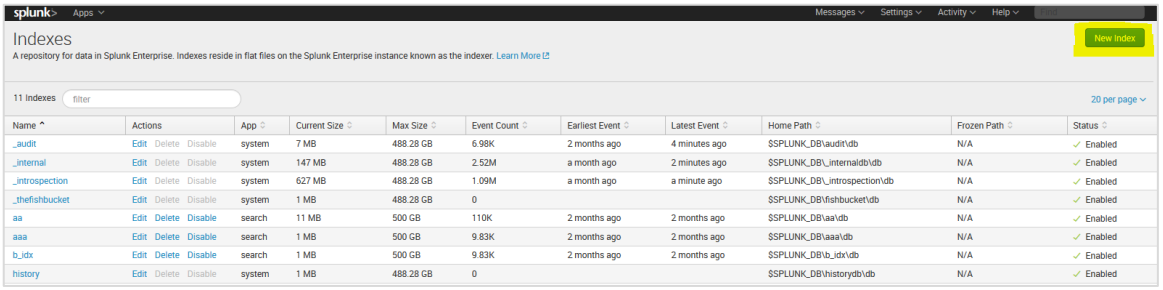
شاخص‌ها در حجم زیاد داده از اهمیت بالایی برخوردار می‌باشند و معمولاً بر روی بانک‌های اطلاعاتی با هدف افزایش کارایی و افزایش سرعت دسترسی به داده مورد نظر تعریف می‌شوند. Splunk ادعا می‌کند که اگر ماشینی داده‌ای را تولید کند، این نرم‌افزار می‌تواند آن را شاخص‌گذاری نماید[۱۰]. در Splunk مواردی که در جدول ۳ نشان داده شده است، همیشه شاخص‌گذاری می‌شوند.

[۱۰] www.Splunk.com

جدول ۳ فیلدهای Splunk که همیشه شاخص‌گذاری می‌شوند

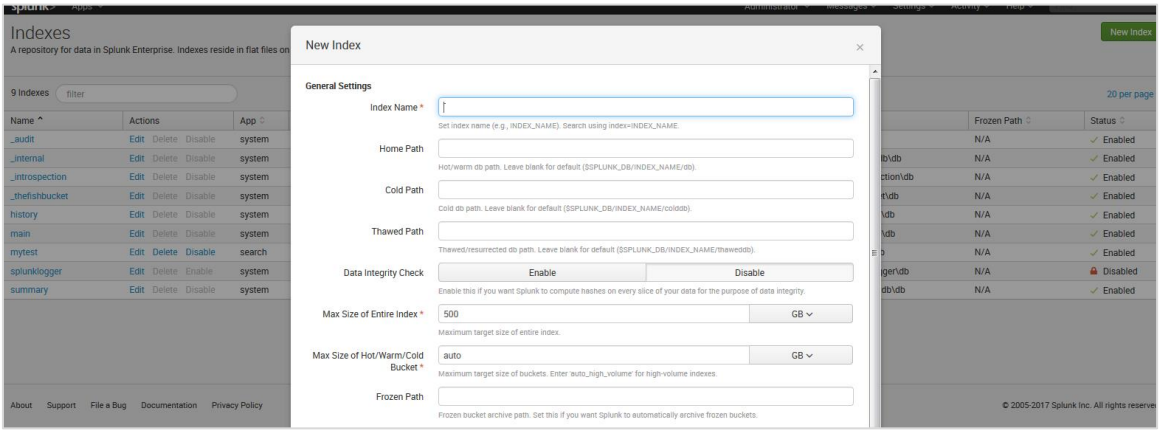
Field	Answers the question	Examples
source	Where did the data come from?	files (/var/log/), scripts (myscript.bat), net-work feeds (UDP:514)
sourcetype	What kind of data is it?	access_combined, syslog
host	Which host or machine did the data come from?	webserver01, cisco_ router
_time	When did the event happen?	Sat Mar 31 02:16:57 2012

در نرم‌افزار Splunk، از منوی Settings لینک indexes می‌توان همه شاخص‌ها را مشاهده کرد که در شکل ۲۵ نشان داده شده است.



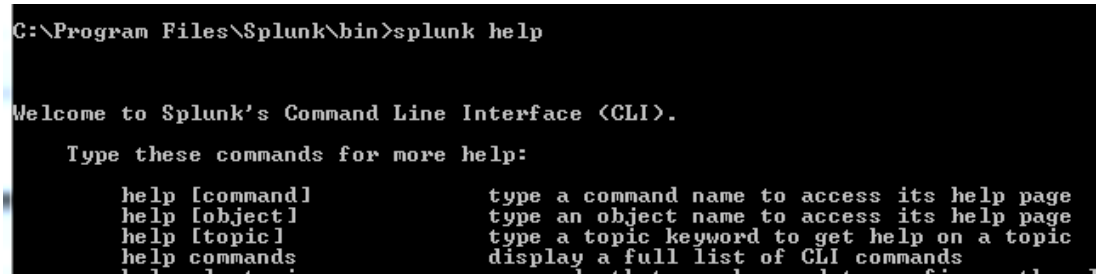
شکل ۲۵ صفحه شاخص‌ها

چنان‌چه دکمه New Index را در شکل ۲۵ فشار دهیم، صفحه‌ای باز می‌شود که می‌توان در آن شاخص جدیدی را تعریف نمود. این صفحه مطابق شکل ۲۶ می‌باشد.



شکل ۲۶ صفحه ایجاد شاخص جدید

چنان‌چه شاخص جدید تعریف نماییم، یک فایل جدید در مسیر %Splunk%\var\lib\Splunk با نامی‌که مشخص نموده‌ایم ایجاد می‌شود. برای حذف شاخص غیرضروری می‌توان از منوی Settings لینک Indexes برای حذف شاخص مورد نظر اقدام نمود که در این صورت از کاربر تأیید می‌گیرد و پیغام می‌دهد که این داده غیرقابل برگشت است. در این صورت فولدری که اشاره نمودیم در مسیر %Splunk%\var\lib\Splunk را حذف می‌نماید. می‌توان این کار را نیز به‌صورت دستورالعمل Command Line Interface (CLI) در Splunk انجام داد. برای این منظور cmd را در ویندوز اجرا می‌کنیم و به قسمت %Splunk%\bin می‌رویم. چنان‌چه دستور splunk help را وارد نماییم، شکل ۲۷ را خواهیم داشت:



شکل ۲۷ خروجی دستور Splunk help

مطابق شکل ۲۸ با دستور Splunk clean eventdata می‌توان کل اطلاعات شاخص‌ها را حذف نمود. دستور Splunk start و Splunk stop نیز برای شروع سرویس و متوقف‌کردن سرویس Splunk می‌باشد.

```
C:\Program Files\Splunk\bin>splunk clean eventdata
This action will permanently erase all events from ALL indexes; it cannot be un
one.
Are you sure you want to continue [y/n]? y
Cleaning database _audit.
Cleaning database _internal.
Cleaning database _introspection.
Cleaning database _thefishbucket.
Cleaning database history.
Cleaning database main.
Cleaning database mytest.
Cleaning database summary.
Disabled database 'splunklogger': will not clean.
```

شکل ۲۸ خروجی دستور Splunk clean eventdata

چنان‌چه بخواهیم اطلاعات شاخص خاصی را حذف نماییم، دستور زیر را وارد می‌کنیم.

Splunk clean eventdata -index <index_name>

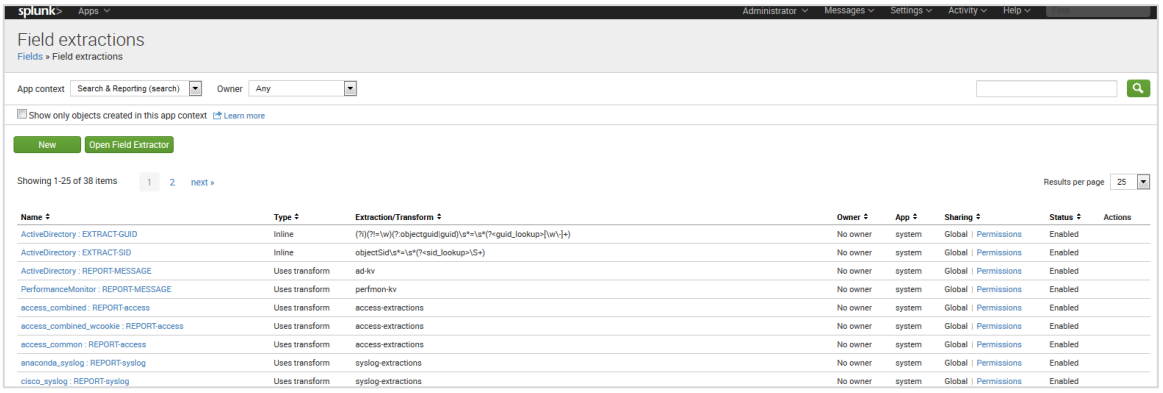
چنان‌چه بخواهیم اطلاعات شاخص خاصی را فعال و یا غیرفعال نماییم، از دستورات زیر استفاده می‌کنیم.

Splunk enable index <index_name>

Splunk disable index <index_name>

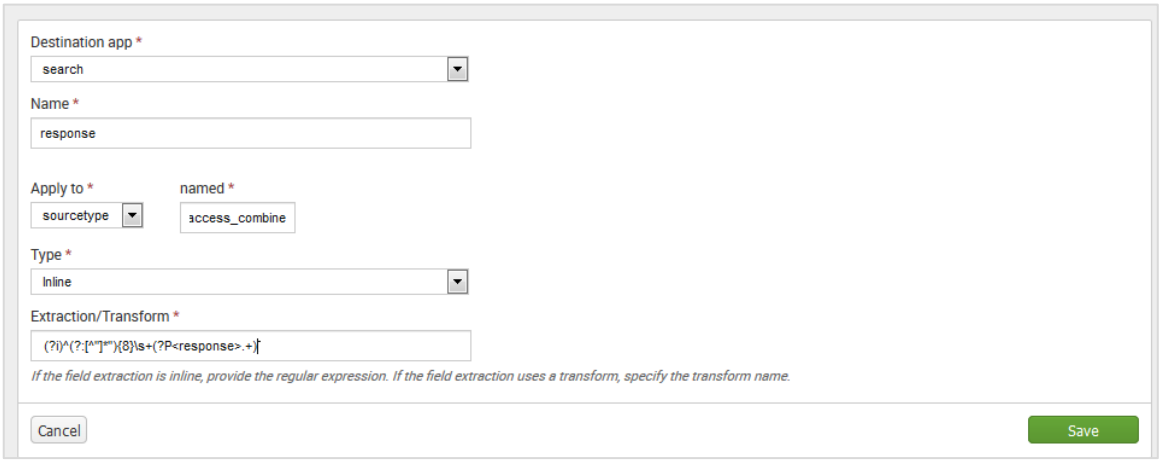
٦ مشاهده، ایجاد و حذف فیلدها

چنان‌چه از منوی Settings لینک Fileds و سپس Field Extraction را انتخاب کنیم، شکل ۲۹ را خواهیم داشت. در این صفحه می‌توان فیلدهای تعریف شده را مشاهده کرد.



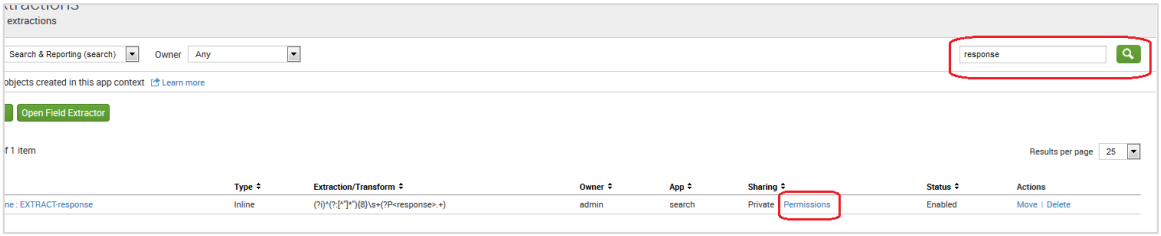
شکل ۲۹ انواع فیلدهای تعریف‌شده

همچنین می‌توان در صورت لزوم فیلدهای بیشتری را تعریف کرد. برای این کار دکمه new را انتخاب می‌کنیم. فیلد response را به‌صورت شکل ۳۰ تعریف نمودیم و بعد از فشار دادن دکمه Save این فیلد به فیلدهای موجود اضافه می‌شود.



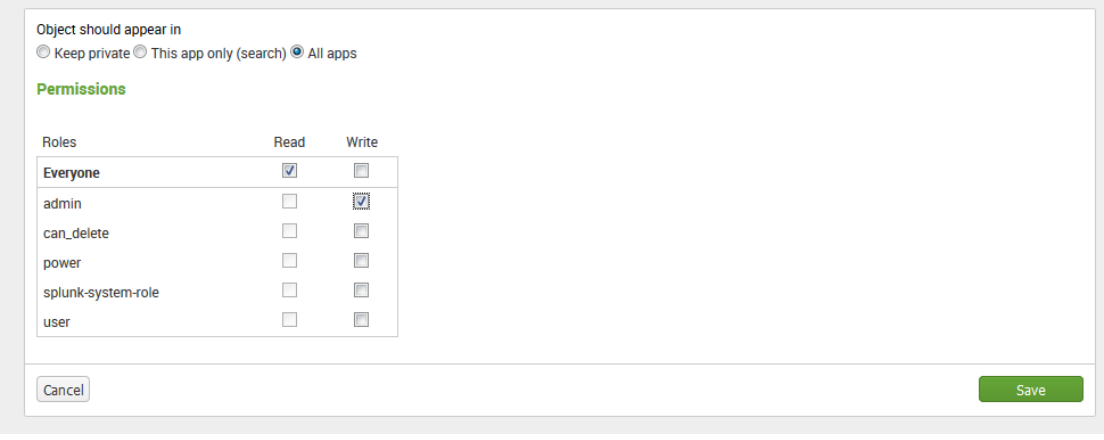
شکل ۳۰ تعریف فیلد جدید

فیلد مورد نظر را جست‌وجو می‌کنیم و با توجه به شکل ۳۱ از نتایج نمایش داده شده، لینک permission را انتخاب می‌نماییم.



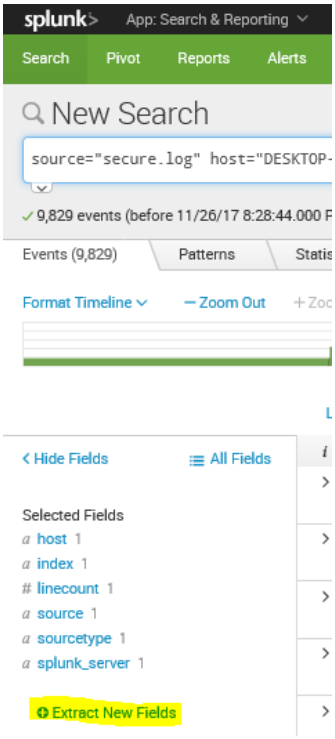
شکل ۳۱ انتخاب لینک permission

در این قسمت مطابق شکل ۳۲ دسترسی‌های لازم را به همه کاربران و کاربر admin سیستم می‌دهیم و دکمه Save را فشار می‌دهیم. بعد از آن این فیلد در فهرست فیلدهای کاربر و درقسمت datasource ای که تعیین کردیم نمایش داده می‌شود.



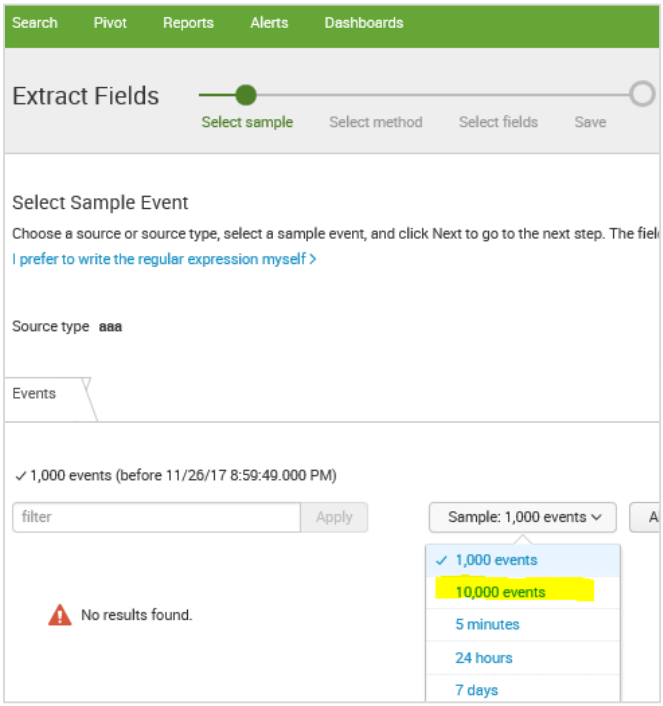
شکل ۳۲ انتخاب دسترسی های لازم به کاربران

علاوه بر روش بالا می‌توان مطابق شکل ۳۳ با فشار دادن لینک extract New Fields فیلدهای جدید تعریف نمود که دارای الگوی خاص مورد نظر ما باشند.



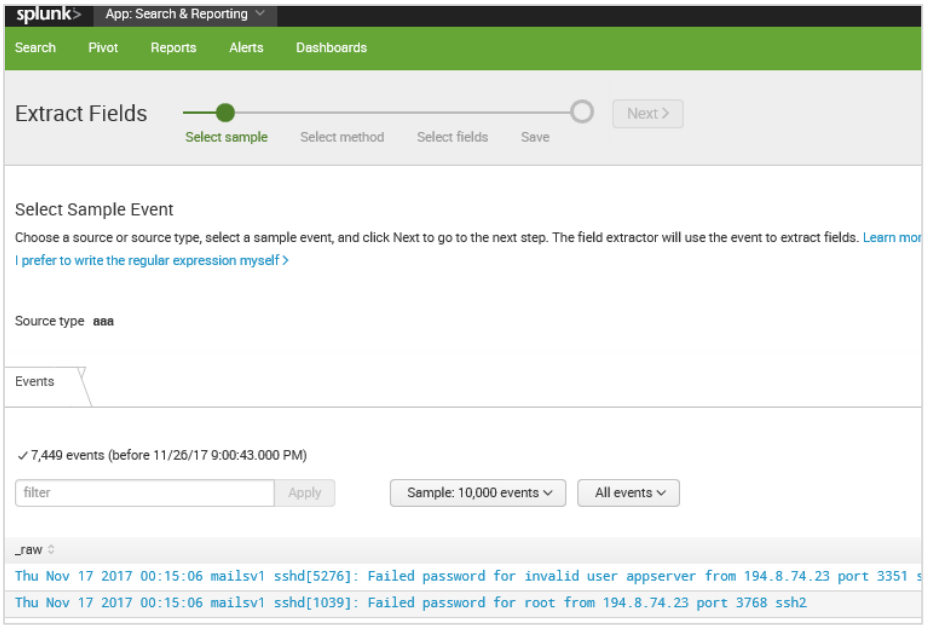
شکل ۳۳ روش تعریف فیلد جدید

از دکمه Sample می‌توان تعداد نمونه‌هایی که می‌خواهیم بررسی کنیم را انتخاب نماییم. می‌توانیم برای این‌که تعداد بیشتری رکورد داشته باشیم، گزینه ۱۰۰۰۰ رخداد را مطابق شکل ۳٤ انتخاب نماییم.



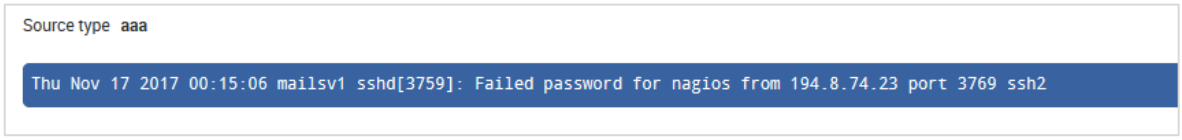
شکل ۳٤ انتخاب تعداد رکوردها برای تعریف فیلد جدید

که در این صورت شکل ۳۵ را خواهیم داشت.



شکل ۳۵ نمایش رکوردها برای تعریف فیلد جدید

بر روی یکی از نتایج حاصل‌شده که می‌خواهیم فیلد جدید تعریف نماییم، کلیک می‌کنیم که در این صورت این عبارت در بالای صفحه به صورت شکل ۳٦ نمایش داده می‌شود.

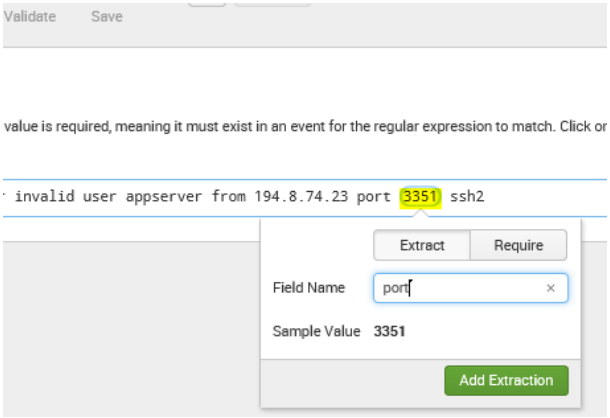


شکل ۳۶ نمایش رکوردی که می‌خواهیم فیلد جدید بر روی آن تعریف نماییم

با توجه به شکل ۳۷ چنان‌چه بخواهیم یک عبارت را برای جست‌وجو تهیه کنیم دکمه Regular Expression را می‌زنیم. اما اگر عبارتی را بخواهیم که قابل جدا کردن با کاما، فاصله خالی و غیره باشد دکمه Delimiters را انتخاب می‌کنیم.

شکل ۳۷ تعریف عبارت فیلد جدید

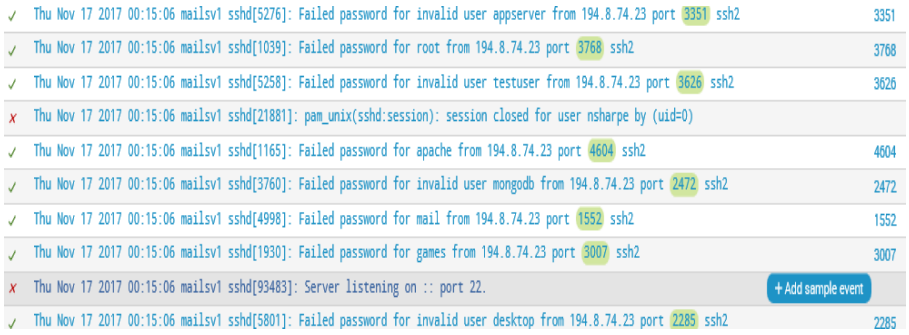
به‌عنوان مثال اگر بخواهیم شماره پورت را به‌عنوان فیلد تعریف نماییم، بر روی این شماره کلیک کرده تا پنجره جدیدی مطابق شکل ۳۸ باز شود. در این پنجره یک نام برای فیلد مورد نظر انتخاب می‌نماییم.



شکل ۳۸ تعریف شماره پورت به عنوان فیلد جدید

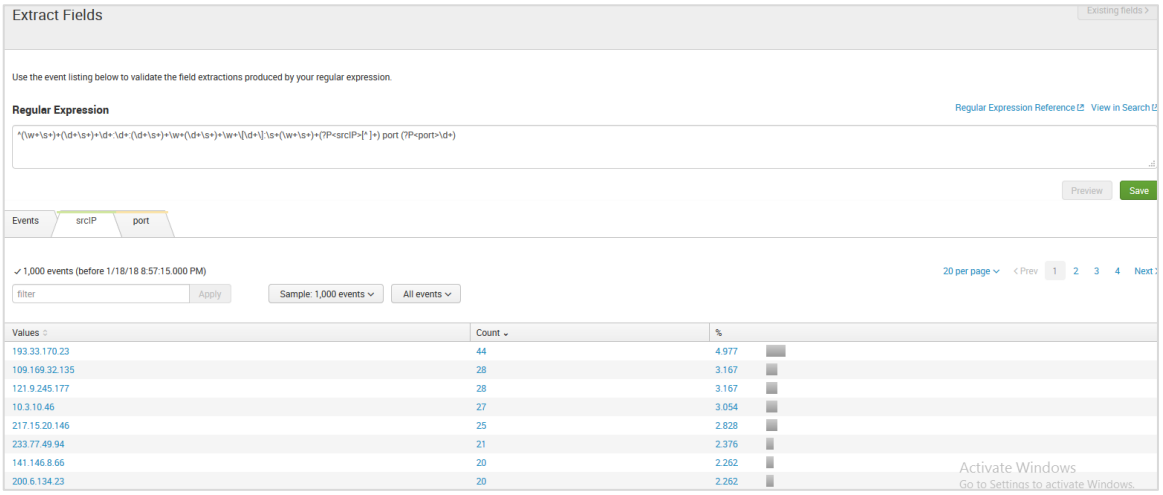
چنان‌چه بخواهیم عبارت دیگری را نیز به فیلد اضافه نماییم (یعنی با عبارت قبلی همه پورت‌ها اضافه نشده اند و لازم است ساختارهای بیشتری تعریف نماییم)، می‌توانیم مطابق شکل ۳۹ روی دکمه Add sample

event کلیک کنیم تا عبارت به بالای صفحه اضافه شود و از آنجا روی شماره پورت کلیک می‌کنیم تا به فیلد ما اضافه گردد.



شکل ۳۹ تعریف ساختار جدید برای فیلد جدید شماره پورت

چنان‌چه دکمه Show Regular Expression را فشار دهیم، عبارت تولید شده در بالای صفحه مطابق شکل ٤٠ نشان داده می‌شود. با توجه به فیلدهای تعریف‌شده دو سربرگ در صفحه ایجاد می‌شود که مقادیر مختلف برای این پارامترها در یک جدول نشان داده شده است.



شکل ٤٠ عبارات تعریف شده، تعداد و درصد تکرار آن‌ها در کل داده‌ها

۷ جست‌وجو

پس از شاخص‌گذاری، لازم است بر روی داده جست‌وجو و تحلیل انجام دهیم. این عمل جست‌وجو با زبان پردازشی جست‌وجو (SPL[۱۱]) انجام می‌پذیرد. صفحه اصلی جست‌وجو در Splunk مطابق شکل ٤١ از دو قسمت اصلی تشکیل شده است.

شکل ٤١ نمایش صفحه اصلی بعد از جست‌وجو

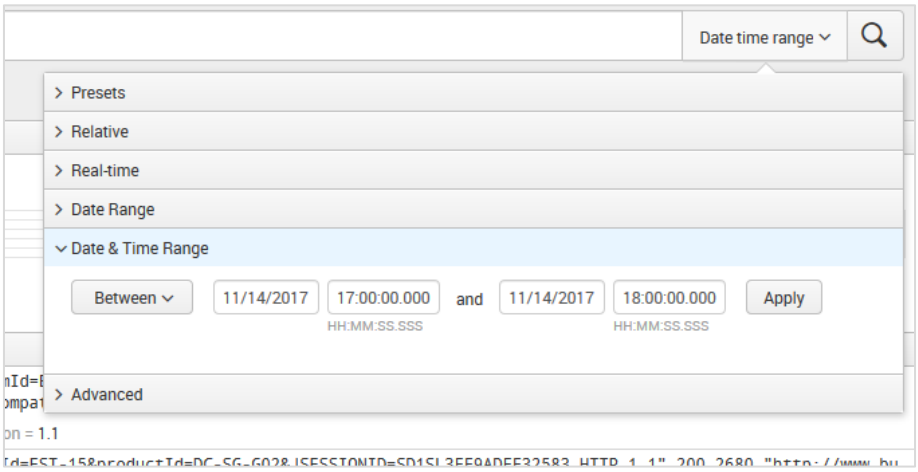
بالای صفحه در قسمت New Search می‌توان عبارت مورد نظر برای جست‌وجو را نوشت و با دکمه ذره‌بین عمل جست‌وجو را انجام داد. در قسمت پایین صفحه نیز نتایج جست‌وجو نمایش داده می‌شود.

برای جست‌وجو می‌توان بازه زمانی مورد نظر برای جست‌وجو را از قسمت بالا و راست صفحه تعیین نمود. چنان‌چه بر روی آن کلیک کنیم (به‌صورت پیش‌فرض all time انتخاب شده است)، صفحه‌ای مطابق شکل ٤٢ را خواهیم داشت که می‌توان بازه زمانی را به‌صورت پیشرفته تعیین نمود.

علاوه بر این می‌توان روش جست‌وجو را از نوع fast, verbose و یا smart تعیین نمود. روش fast همان‌طور که از نام آن مشخص است، یک روش جست‌وجوی سریع می‌باشد (معمولاً سریع‌ترین روش است)، چون فقط از فیلدهای پیش‌فرض استفاده می‌نماید. روش verbose زمان طولانی را برای جست‌وجو لازم دارد، زیرا

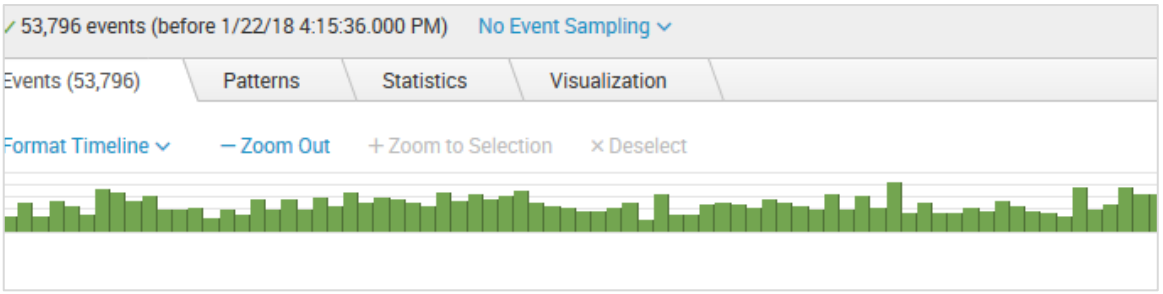
[۱۱] Search Processing Language

همه فیلدهایی که می‌تواند را پیدا می‌کند. روش smart (روش پیش‌فرض) می‌تواند بسته به فعال یا غیرفعال کردن فیلد، شبیه دو روش ذکر شده verbose و smart در نظر گرفته شود.



شکل ٤٢ نمایش صفحه بازه زمانی جست‌وجو

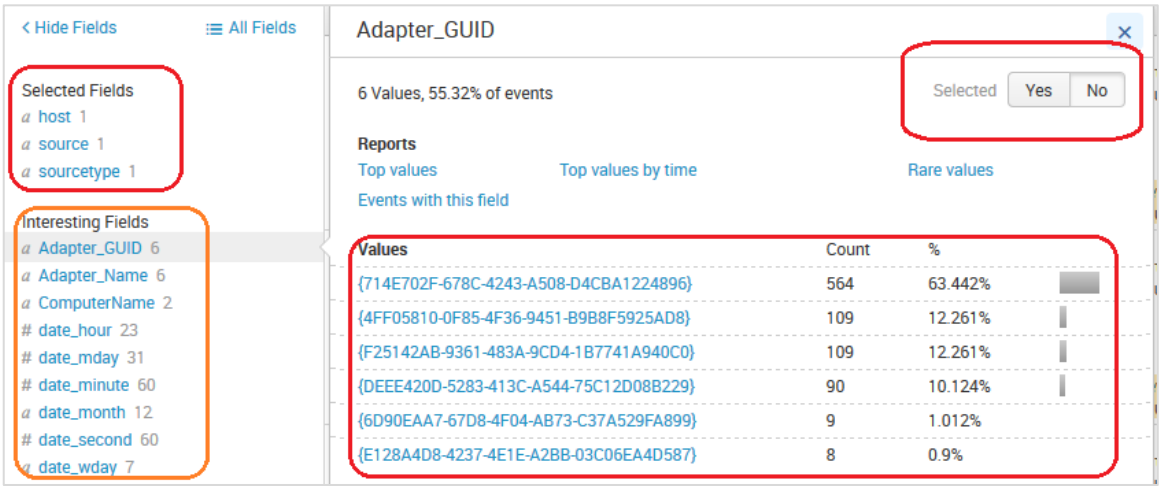
بعد از جست‌وجو نتایج در پایین صفحه نمایش داده می‌شود. در برگه‌ی events در پرانتز تعداد رخدادهایی که با این جست‌وجو اتفاق افتاده است نشان داده می‌شود (دراینجا ٥٣٧٩٦). همچنین در قسمت وسط صفحه یک نمودار نمایش داده می‌شود که بیان‌گر تعداد دفعاتی است که رخداد در فاصله زمانی که انتخاب کردیم اتفاق افتاده است. چنان‌چه بر روی هر یک از مستطیل‌های سبز رنگ کلیک کنیم می‌توانیم جزئیات بیشتر در فاصله زمانی کوتاه‌تر را مشاهده کنیم.



شکل ٤٣ نمایش تعداد تکرار رخدادها در بازه زمانی جست‌وجو

در قسمت سمت چپ چند فیلد به‌صورت پیش‌فرض در Selected Fields وجود دارد و فیلدهای دیگر در Interesting Fields آورده شده است، که عدد روبروی آن بیان‌گر تعداد مقادیر مختلفی است که برای یک فیلد در رخدادها وجود دارد. با کلیک بر روی هر کدام از فیلدها می‌توان مقادیر متفاوت را در ستون Values دید. همچنین در این جدول تعداد و درصد تکرار این مقدار، برای فیلد مورد نظر نشان داده می‌شود. به‌عنوان مثال

چنان‌چه بر روی فیلد Adapter_GUID مطابق شکل ٤٤ کلیک کنیم، ٦ مقدار متفاوت برای این فیلد وجود دارد که به ازای هر مقدار، تعداد تکرار و درصد تکرار آن مقدار نشان داده شده است.



شکل ٤٤ نمایش صفحه مشخصات فیلد

چنان‌چه در قسمت سمت راست بالای صفحه (Selected) گزینه Yes انتخاب شود، این فیلد به قسمت Selected Fields اضافه می‌شود که انتخاب آن در جست‌وجوهای بعدی در صورت نیاز برای بررسی آسانتر می‌باشد.

در اینجا می‌توان گزارش‌هایی را برای فیلد مورد نظر گزارش نمود. به‌عنوان مثال چنان‌چه Top values را انتخاب کنیم، بیشترین مقدار گزارش شده برای فیلد به صورت نمودار در برگه‌ی VIisualization نشان داده می‌شود، که درواقع Splunk به‌صورت خودکار مقدار"|top limit=20 NAME_FIELD" را به انتهای عبارت جست‌وجو اضافه می‌نماید (با علامت پایپ) که NAME_FIELD نام فیلد انتخاب شده و limit به معنی بیشترین مقادیر برای فیلد مورد نظر (حداقل ٢٠) می‌باشد. اگر Top values by Time انتخاب شود، مقدار "|timechart count by NAME_FIELD limit=10" به انتهای عبارت جست‌وجو اضافه می‌شود که خروجی آن یک نمودار است که در زمان‌های مختلف تکرار آن فیلد را در رخداد نشان می‌دهد.

۱-۷ عبارات مورد جست‌وجو

جست‌وجو در Splunk بر مبنای لغت می‌باشد. یعنی اگر لغت fail را جست‌وجو کنیم و در لاگ‌ها failure داشته باشیم، در خروجی نشان داده نمی‌شود. به همین منظور لازم است عبارت *fail را جست‌وجو کنیم. علاوه براین، این جست‌وجو به حروف بزرگ و کوچک حساس نمی‌باشد. برای عبارت ترکیبی جست‌وجو

نیز می‌توان از OR و AND استفاده نمود. جدول ٤ دستورات جست‌وجو را نشان می‌دهد. این دستورات شامل دستورات محاسباتی، منطقی و غیره می‌باشند. در ادامه این بخش با چند مثال توضیح داده می‌شود.

جدول ٤ دستورات جست‌وجو

Purpose of Command	What it Does	Actual Commands

Filter	Reduces results to a smaller set.	`search`
		`where`
		`dedup`
		`head`
		`tail`

Sort	Orders the results and can also be used to limit the number of results.	`sort`
Group	Puts those results like members together in groups to better see patterns in the data.	`transaction`

Report	Takes results of a search and summarizes them for a report.	`top / rare`
		`stats`
		`chart`
		`timechart`

Other	Included in this group are those that allow you to filter out fields, modify fields, or add fields to your results.	`fields`
		`replace`
		`eval`
		`rex`
		`lookup`

۲-۷ مثال‌هایی برای جست‌وجو

مثال اول) دستور زیر را درنظر بگیرید:

fail* password| stats count by port|sort -count| where count>7

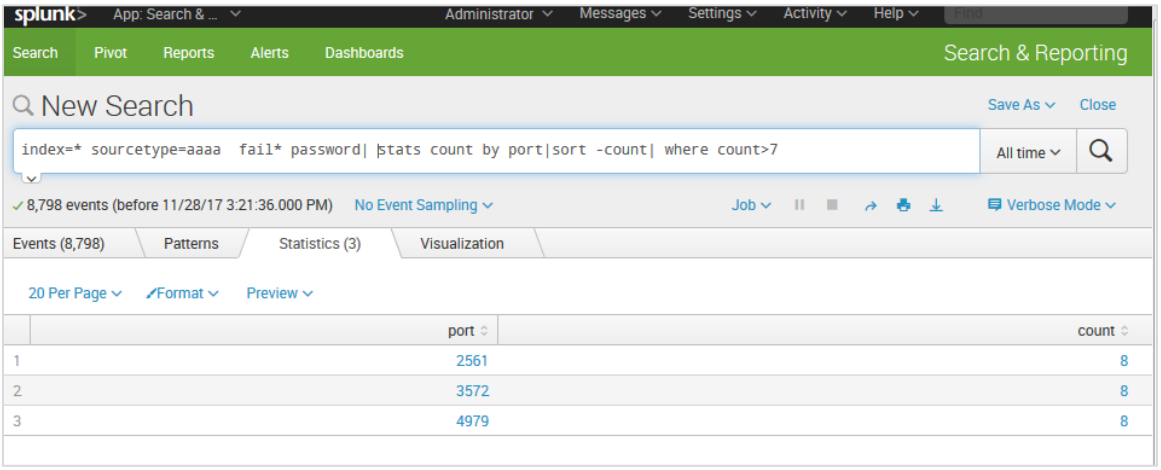
چنانچه دستور بالا را اجرا کنیم، خروجی مطابق شکل ٤٥ خواهیم داشت. قسمت های مختلف این دستور که با علامت پایپ جدا شده‌اند، هر کدام معانی زیر را دارد.

۱. دستور fail* password عباراتی را پیدا می‌کند که ابتدای آن کلمه با fail شروع می‌شود و بعد از آن لغت password وجود دارد.

۲. دستور stats count by port | با توجه به فیلد پورت که تعریف نمودیم گروه‌بندی می‌کند و تعداد آن را نمایش می‌دهد.

۳. دستور sort –count مقادیر count را به صورت نزولی مرتب می‌نماید. چنانچه علامت – را در دستور ننویسیم، عبارت به صورت صعودی مرتب می‌شود.

٤. دستور where count>7 |خروجی‌هایی را بر می‌گرداند که تعداد آن‌ها بالاتر از ۷ باشد.



شکل ٤٥ جست‌وجوی عبارت

مثال دوم) دستور زیر را درنظر بگیرید:

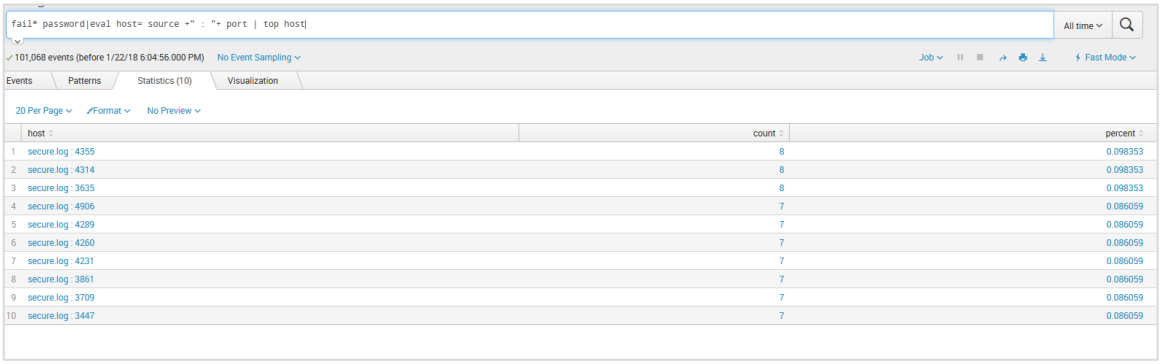
fail* password| top port

دستور top به‌صورت پیش‌فرض ۱۰ مقدار با بیشترین تکرار را به‌ترتیب نزولی برای فیلدهای مشخص برمی‌گرداند. بنابراین خروجی این دستور با fail* password| top 10 port برابر است. در واقع این دستور در جاهایی که پسورد اشتباه وارد شده است، ۱۰ پورت با بالاترین تکرار را برمی‌گرداند. چنانچه برگه‌ی virtualization را باز کنیم این ۱۰ پورت و تکرار آن‌ها را در یک نمودار به ما نشان می دهد.

مثال سوم) دستور زیر را درنظر بگیرید:

fail* password|eval host= source +" : "+ port | top host

دستور eval در واقع از ترکیب دو فیلد source و port عبارت جدیدی به نام host می‌سازد و بیشترین تکرار آن را برمی‌گرداند. شکل ٤٦ خروجی این عبارت را نشان می‌دهد.



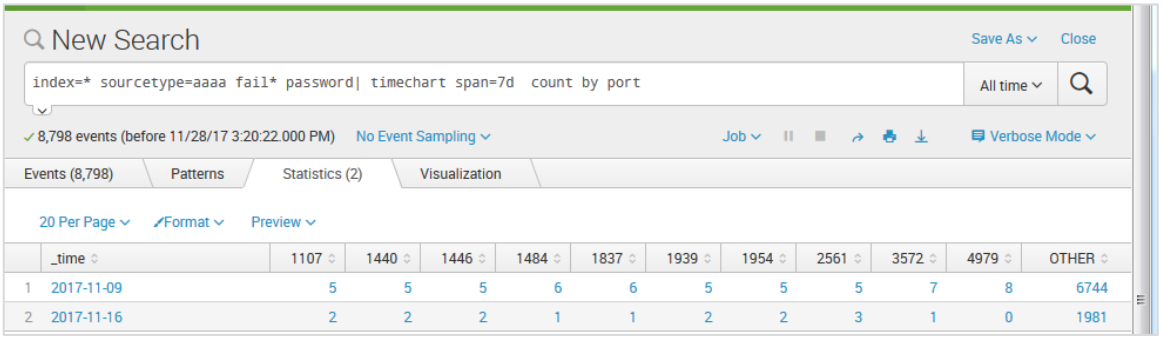
شکل ٤٦ جست‌وجوی عبارت

برای نام‌گذاری ستون از عبارت rename old-field-name as new-field-name استفاده می‌کنیم. بنابراین می توانیم با اضافه‌کردن دستور rename host as host:port | نام ستون host را به host:port تغییر دهیم.

مثال چهارم) دستور زیر را در نظر بگیرید:

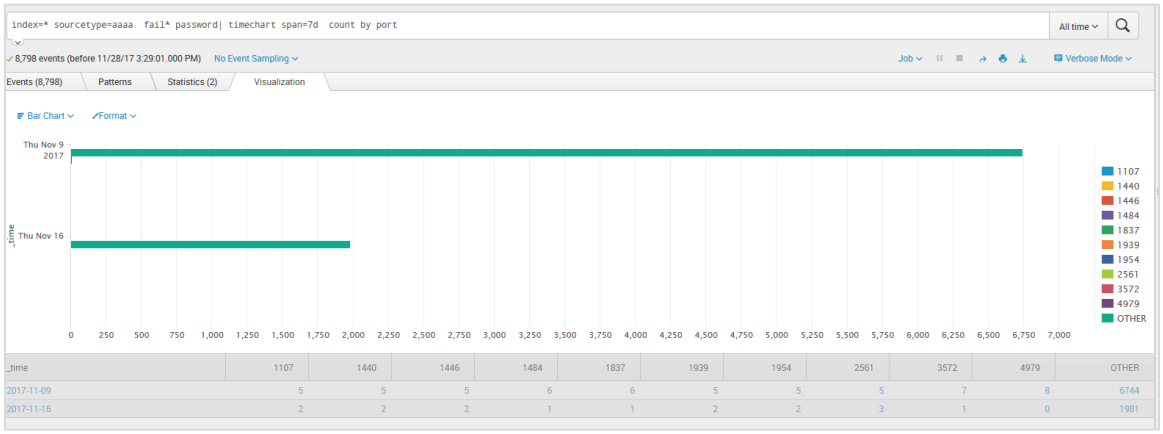
fail* password| timechart span=7d count by port

این دستور، در رخدادهایی که عبارت fail* password آمده، در فاصله زمانی ۷ روزه تعداد کل پورت‌های مختلف را شمرده و گروه‌بندی می‌نماید. تصویر ٤٧ نتایج را به‌صورت جدولی در برگه‌ی Statistics نمایش می‌دهد.

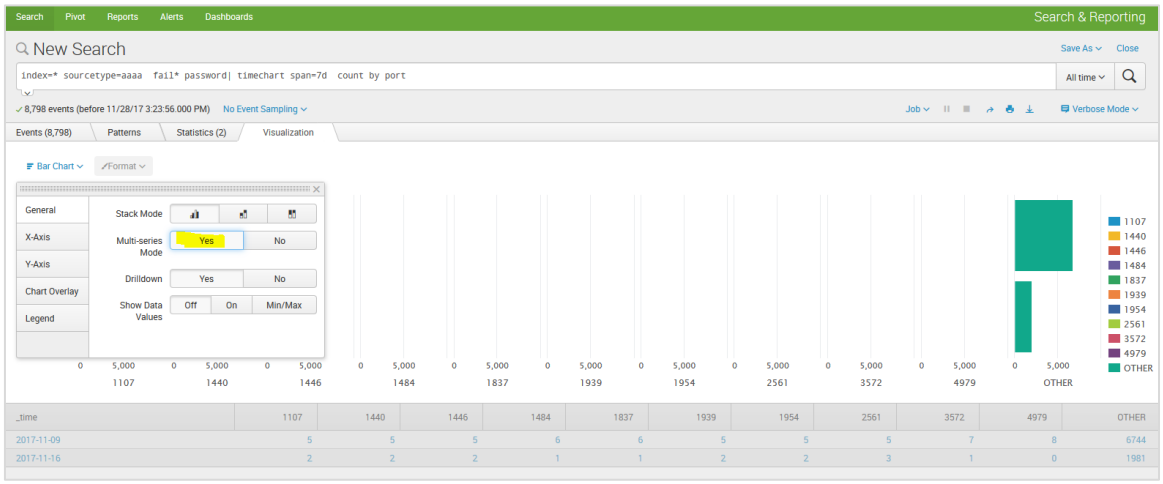


شکل ٤٧ جست‌وجوی عبارت

تصویر ٤٨ نتایج را به‌صورت گرافیکی در برگه‌ی Visualization نشان می‌دهد. می‌توان فرمت نتایج را مطابق شکل ٤٨ (ب) تغییر داد.



(الف)



(ب)

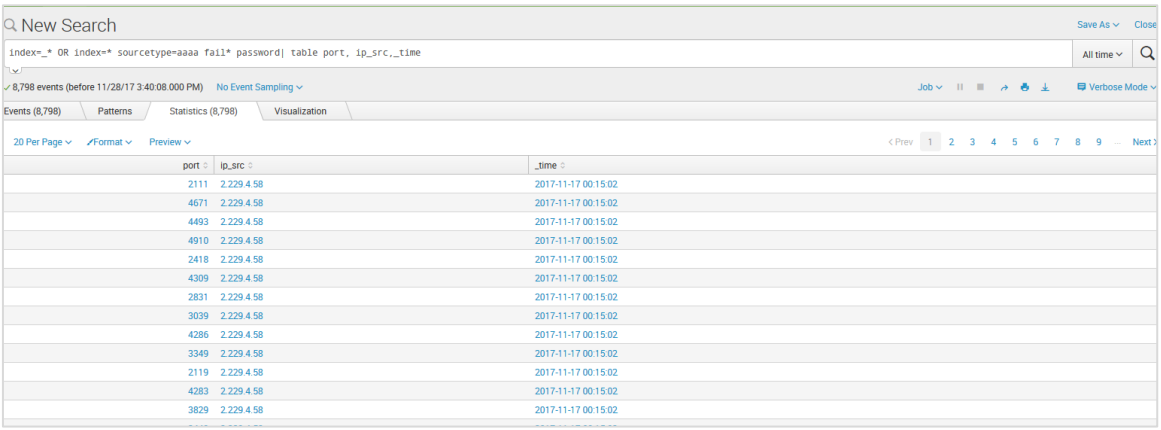
شکل ۴۸ جست‌وجوی عبارت

مثال پنجم) فیلد دیگری بنام ip_src را مانند port (بخش ٦) برای پورت‌ها تعریف کرده و دستور زیر را وارد می‌نماییم:

fail* password| table port, ip_src, _time

این دستور در قالب جدول اطلاعات پورت، ip و همچنین زمان ثبت‌شده رخدادهایی که عبارت fail* password دارند را نشان می‌دهد. در واقع این ipها در قسمت ورود به سیستم بیشترین تکرار ورود را با کلمه

عبور اشتباه انجام داده‌اند، که این می‌تواند برای تحلیل در حمله جست‌وجوی کورکورانه[۱۲] مورد استفاده قرار گیرد. نتایج در شکل ۴۹ نشان داده شده است.



شکل ۴۹ جست‌وجوی عبارت

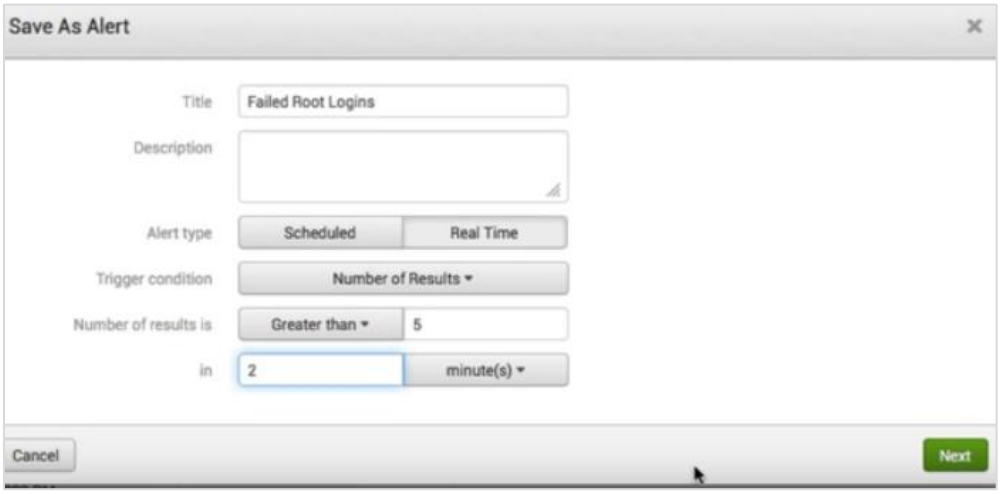
۸ ایجاد هشدار[۱۳]

هشدار برای این هست که بتوانیم یک اتفاق خاص را مانیتور کرده و به آن پاسخ دهیم. در واقع با تنظیم هشدار، وقتی اتفاق خاصی بیفتد Splunk به ما اطلاع می‌دهد. هشدار از یک جست‌وجوی ضبط‌شده برای رخدادها در زمان بی‌درنگ یا بر اساس برنامه‌ریزی استفاده می‌کند.

به‌عنوان مثال دستور failed password for root را در مستطیل جست‌وجو وارد می‌کنیم. سپس گزینه Save As > Alert را فشار می‌دهیم. در اینجا می‌توانیم هشدار را به صورت برنامه‌ریزی شده scheduled برای اجرا در زمان‌های مشخص و یا به‌صورت بی‌درنگ تعریف نماییم. در مستطیل trigger condition شرط مورد نظر را وارد می‌نماییم. به‌عنوان مثال می‌توانیم مشخص نماییم که زمانی که تعداد نتایج در ۲ دقیقه بیشتر از ۸ شود هشدار دهد. شکل ۵۰ نمایی صفحه هشدار را نشان می‌دهد.

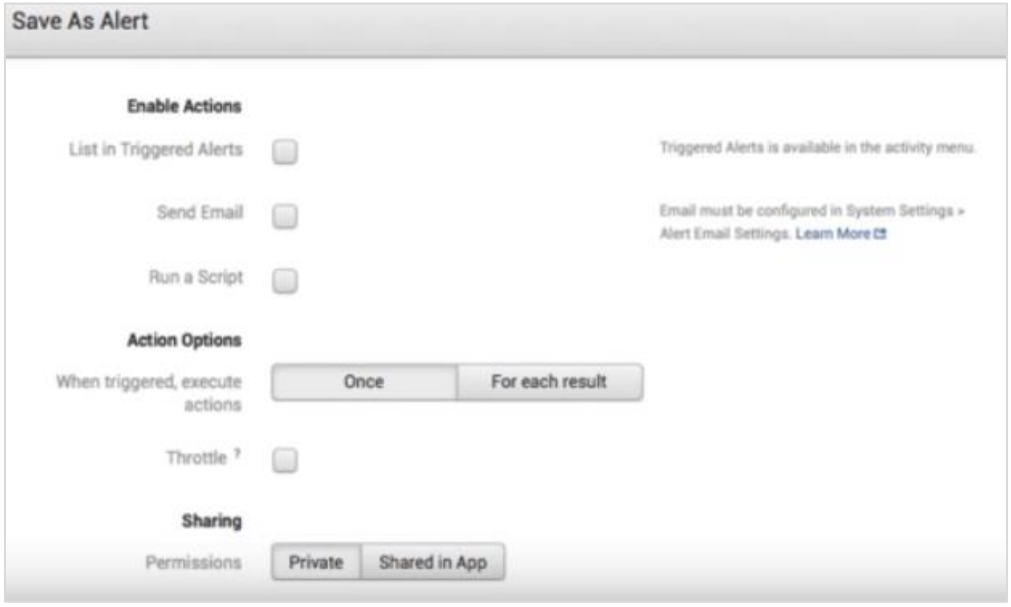
[۱۲] Brute force

[۱۳] Alert



شکل ۵۰ صفحه هشدار

بعد از ایجاد هشدار مشخص می‌نماییم که وقتی شرط تعریف‌شده در مرحله قبل محقق شود، چگونه به اطلاع فرد رسانده شود. به‌عنوان مثال می‌تواند به فرد ایمیل بزند و یا یک اسکریپتی اجرا کند. نمای این صفحه در شکل ۵۱ نشان داده شده است.



شکل ۵۱ صفحه هشدار

۹ منابع

[1] http://docs.splunk.com
[2] http://www.learnsplunk.com
[3] Diakun, Josh, Paul R. Johnson, and Derek Mock. *Splunk Operational Intelligence Cookbook*. Packt Publishing Ltd, 2016.
[4] Sigman, Betsy Page, and Erickson Delgado. *Splunk Essentials*. Packt Publishing Ltd, 2016.
[5] Miller, James. *Mastering Splunk*. Packt Publishing Ltd, 2014.