بسمه تعالی

آموزش فنی نصب و پیکربندی Splunk

(بخش نخست)

فهرست مطالب

1 مقدمه

داده‌های تولید شده توسط ماشین، یکی از پیچیده‌ترین و باارزش‌ترین مباحث مربوط به داده‌های حجیم[1] است، که دارای رشد بسیار سریعی هستند. از داده‌های ماشینی می‌توان اطلاعات ارزشمندی مانند فهرست کاملی از تراکنش‌های کاربران، رفتار مشتریان، رفتار ماشین، تهدیدهای امنیتی، فعالیت‌های مجرمانه و غیره را به‌دست آورد. شغل شما هر چیزی که باشد Splunk می‌تواند داده‌های ماشینی شما را برایتان تفسیر کرده و اطلاعات سودمندی را به شما ارائه دهد. این همان چیزی است که تیم Splunk آن را هوش عملیاتی می‌نامند. هوش عملیاتی به شما درکی از هر آنچه که در سراسر سیستم فناوری اطلاعات و ساختار تکنولوژی شما در حال رخ دادن است، به صورت زمان حقیقی[2]، می‌دهد تا بتوانید آگاهانه تصمیم بگیرید.

سازمان Splunk در سال 2003 میلادی در سانفرانسیسکو تأسیس شد. این سازمان، تولیدکننده‌ی نرم‌افزاری به همین نام است که وظیفه‌ی آن جستجو، نظارت، و تحلیل داده‌های ماشینی توسط یک واسط به سبک وب[3] است. در اوایل سال 2016 میلادی، Splunk بیش از ده هزار مشتری داشت.

- ✓ شما می‌توانید تمام سؤالات خود را که مربوط به Splunk هستند، در فروم رسمی این سازمان در آدرس https://answers.splunk.com/index.html مطرح و در اسرع وقت پاسخ خود را دریافت نمایید.
- ✓ بااستفاده از لینک https://docs.splunk.com/Splexicon نیز به واژه‌نامه‌ی برخط Splunk دسترسی خواهید داشت. این واژه‌نامه شامل تمام اصطلاحات مختص نرم‌افزار Splunk، توضیحی برای هر کدام، و لینک مطالب مربوط به واژه‌ی جستجو شده در مستندات Splunk است.

2 Splunk Enterprise چیست؟

Splunk Enterprise یک نرم‌افزار است که داده‌های فرستاده‌شده از تمام برنامه‌های کاربردی، سرویس‌دهنده‌ها، و تمام دستگاه‌های تشکیل‌دهنده‌ی ساختار شبکه را نمایش می‌دهد. این نرم‌افزار، یک موتور جستجو و تحلیل قدرتمند و همه‌کاره است که امکان نظارت، خطایابی، هشداردهی و گزارش‌دهی بر روی داده‌های در حال انتقال بر روی شبکه را به صورت زمان حقیقی به شما می‌دهد. Splunk همچنین نسبت به مقیاس بسیار

[1] Big data
[2] Real-time
[3] Web-style

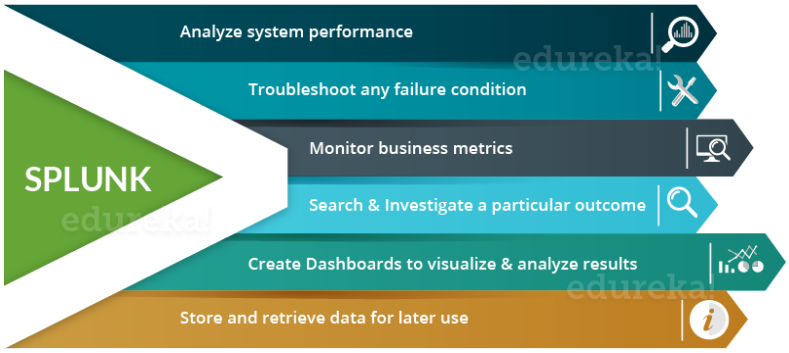
انعطاف‌پذیر است. می‌توان از Splunk به‌منظور حل مسائل جزئی استفاده کرد و یا آن را تبدیل به ستون اصلی تحلیل یک سازمان وسیع کرد.

1-2 امکانات و ویژگی‌های Splunk

Splunk دارای امکانات و ویژگی‌های زیادی می‌باشد. در ادامه برخی از این امکانات و ویژگی‌ها آمده است.

1. جمع‌آوری و نمایه‌سازی[4] داده‌ها از هر منبع داده‌ای به صورت زمان حقیقی
2. امکان جستجوی قدرتمند و استخراج اطلاعات مفید موجود در داده به صورت خودکار
3. تحلیل جامع و یافتن ارتباط بین رویدادها و فعالیت‌های مختلف
4. بصری‌کردن داده‌های مختلف از طریق نمودارهای متنوع و تنظیم گزارش
5. امکان تنظیم هشدار به‌منظور نظارت خودکار سیستم در هنگام رخ‌دادن رویدادهای خاص
6. امکان دسترسی امن به Splunk از هر مکانی
7. واسط کاربری کاربرپسند
8. امکان نمایه‌سازی داده در مقیاس بسیار بالا (صدها ترابایت ثبت[5] در روز)
9. ارائه شده به دو صورت نرم‌افزاری و سرویس ابری

و ...



شکل 1: برخی ویژگی‌های Splunk

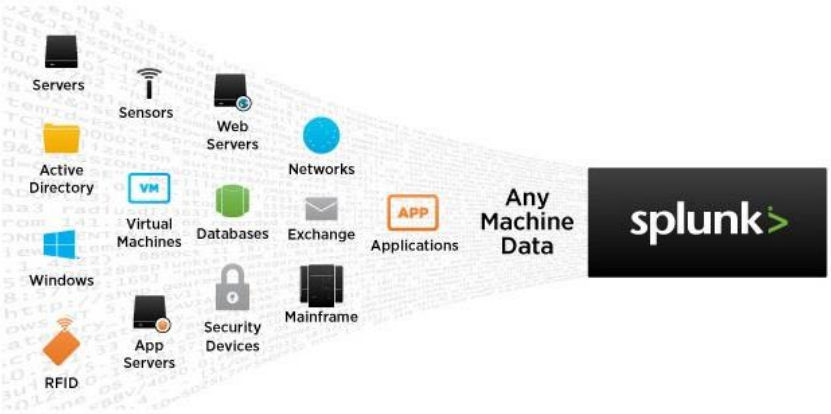
در ادامه به ارائه یک توضیح مختصر برای برخی از این ویژگی‌ها می‌پردازیم.

---

[4] Indexing
[5] Log

2-1-1 جمع‌آوری و نمایه‌سازی داده‌ها

Splunk چندین روش مختلف برای نمایه‌سازی همه‌ی داده‌های موجود در ساختمان شبکه‌ی شما به‌صورت زمان حقیقی را دارد. به این ترتیب Splunk می‌تواند اطلاعاتی مانند ترافیک جریان شبکه، فایل‌های ثبت، تله‌ها[6] و هشدارها، پیام‌ها، پیکربندی، اسکریپت‌ها، داده‌های اجرایی و اطلاعات آماری را از تمام برنامه‌های کاربردی، سرویس‌دهنده‌ها، و دستگاه‌های متصل به شبکه، بدون توجه به قالب‌بندی و مکان، در اختیار شما قرار دهد. با استفاده از Splunk می‌توانید بر تغییرات صورت‌گرفته در اسکریپت و پیکربندی سیستم‌فایل‌ها نظارت کنید، نظارت بر تغییرات سیستم‌فایل یا رجیستری ویندوز را فعال کنید، فایل‌های آرشیوی و تله‌های SNMP را بیابید، اثر پشته سرویس‌دهنده‌ی برنامه‌های کاربردی زنده و جداول حسابرسی پایگاه‌داده را شناسایی و پیگیری کنید، به درگاه‌های شبکه متصل شده و syslog و سایر موارد مربوط به شبکه را دریافت کنید.



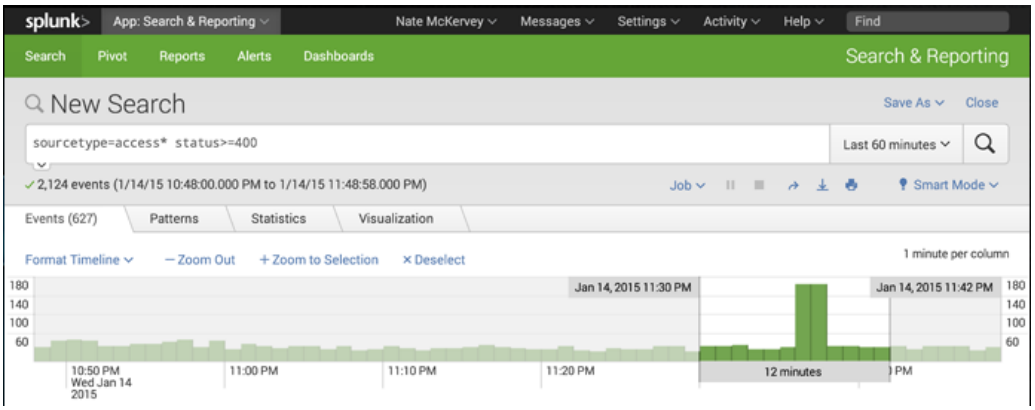
شکل 2: نمایی از قابلیت‌های ابزار

2-1-2 جستجو و بررسی

با استفاده از زبان قدرتمند عملیات جستجوی Splunk[7] می‌توان داده‌ها را جستجو کرد. Splunk قالب‌بندی‌های مختلف داده‌های شما را به صورت خودکار نرمال‌سازی کرده و به شما این امکان را می‌دهد که با استفاده از

[6] Traps
[7] Splunk Search Processing Language (SLP)

بیش از 140 دستور، انواع جستجوهای آماری را روی داده‌هایتان انجام دهید، محاسبه کنید و حتی شرایط خاص مد نظرتان را در داخل یک پنجره‌ی زمانی بیابید. بر روی خطوط زمانی[8] بزرگ‌نمایی[9] و کوچک‌نمایی[10] کنید تا روندها[11] و الگوها را به صورت خودکار ببینند و با یک کلیک، نتایج جستجو را ملاحظه نمایید.

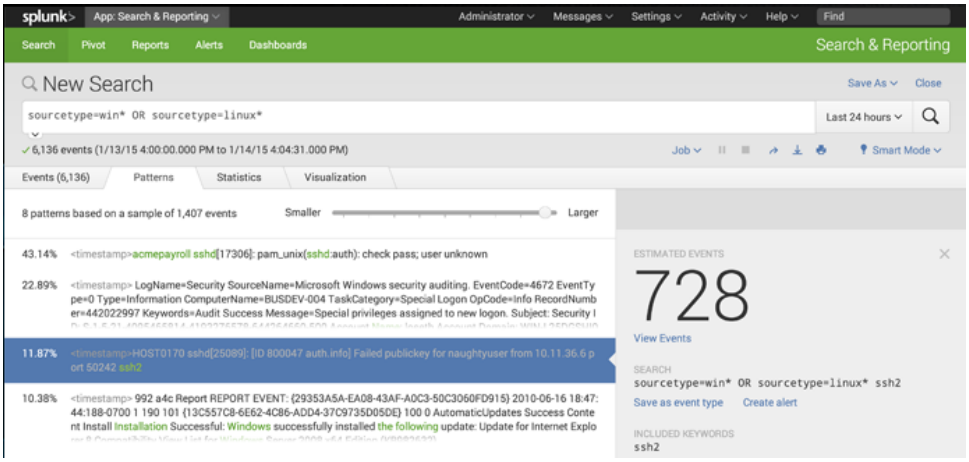


شکل 3: جست‌وجوی و اطلاعات آماری

3-1-2 تحلیل داده و یافتن ارتباط بین رویدادها و فعالیت‌ها

با استفاده از Splunk می‌توانید به راحتی ارتباط بین رویدادها و فعالیت‌های مختلف را بیابید. بر اساس زمان، مکان، و یا نتایج جستجو، آن‌ها را به یکدیگر مرتبط کنید. با استفاده از دستور Transaction رویدادهای مرتبط نظیر تراکنش یا نشست را شناسایی، و تراکنش‌های ناموفق را بررسی کنید. داده‌های دریافتی از منابع ناهمگون را با استفاده از Event Annotation رمزگشایی کنید. همچنین می‌توانید از یادگیری ماشین به‌منظور شناسایی خودکار ناهنجاری‌ها و وقایع دیگر استفاده کنید.

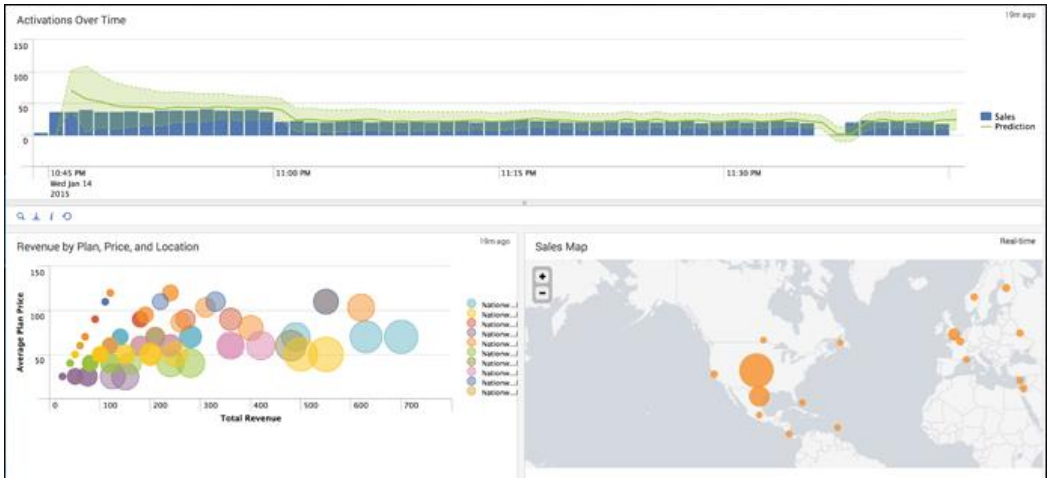
[8] Timelines
[9] Zoom in
[10] Zoom out
[11] Trends



شکل 4: تحلیل اطلاعات آماری

4-1-2 بصری‌کردن داده‌ها و تنظیم گزارش

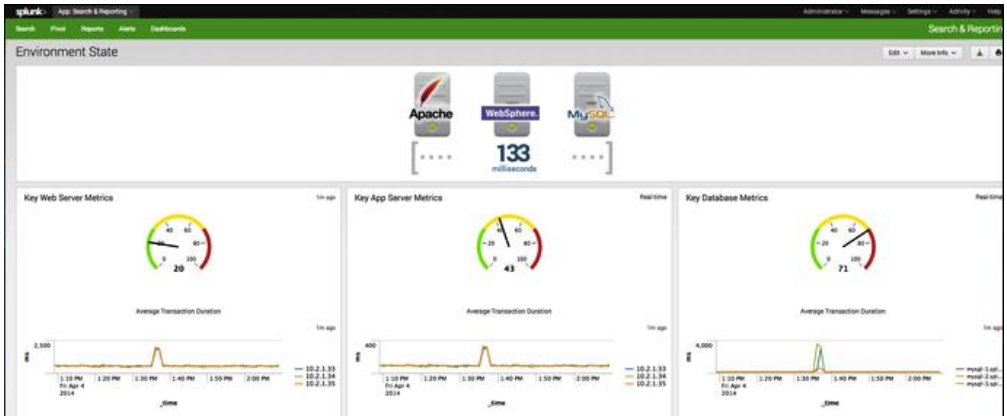
Splunk امکان نمایش داده به شکل انواع نمودار در گزارش‌ها و داشبوردهای متناسب با هر شغل، و یا نیازهای امنیتی را دارد. همچنین می‌توانید برای تحلیل بیشتر بر روی نمودارها zoom کنید. نمودارهای پیش‌بینی نیز به شما امکان پیش‌بینی بیشینه‌ها و کمینه‌ها را می‌دهند که می‌توانید با استفاده از آن‌ها منابع سیستم و بار کاری را پیشاپیش مدیریت کنید. شما این امکان را خواهید داشت که داشبوردها و گزارش‌ها را متناسب با افراد تولید کنید، آن‌ها را به صورت PDF به اشتراک بگذارید، و یا داخل سایر برنامه‌های کاربردی جاسازی کنید.



شکل 5: داشبورد و دید بصری ابزار

5-1-2 نظارت و هشدار

جستجوها را به هشدارهای زمان حقیقی تبدیل کنید تا در زمان رخ‌دادن یک رویداد خاص، خبر[12] آن را به صورت ایمیل یا RSS دریافت کنید. سپس فعالیت‌های ترمیمی را اجرا کنید و یا یک تله‌ی SNMP ارسال کنید. هشدارها در صورت وقوع شرایط خاصی که شما پیش‌تر تعیین کرده‌اید فعال می‌شوند. با استفاده از یک هشدار، سریع‌تر از وقوع مشکلات مطلع شده و آن‌ها را مدیریت کنید.

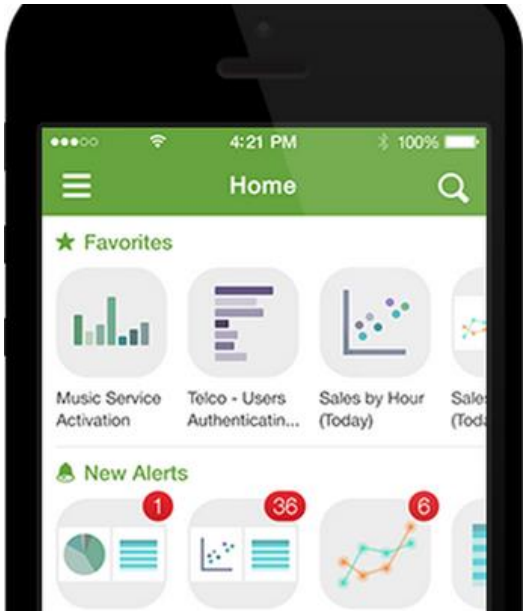


شکل 6: داشبورد نظارت و هشدار

6-1-2 Splunk در هر جایی همراه شما

مدیر و کاربران Splunk می‌توانند از طریق هر مرورگر استانداردی به صورت امن به این نرم‌افزار دسترسی داشته باشند. دسترسی راه‌دور Splunk به کاربران این اجازه را می‌دهد که با استفاده از iOS و یا دستگاه‌های موبایل اندرویدی با Splunk کار کنند. به کمک هشدارها و دیدها[13]، مدیران می‌توانند در زمان نیاز اقدامات لازم را انجام دهند و امکان نظارت و بررسی وضعیت عملیات را از هر جایی دارند.

[12] Notification
[13] Views



شکل 7: برنامه‌ی کاربردی همراه قابل نصب بر روی گوشی

2-2 چرا Splunk

در جدول 1 مقایسه‌ی Splunk با دو ابزار Sumo Logic و ELK آمده است.

جدول 1: مقایسه‌ی Splunk با دو ابزار Sumo Logic و ELK

Features	Splunk	Sumo Logic	ELK
Searching	✓	✓	Only possible with Integrations
Analysis	✓	✓	Only possible with Integrations
Visualization Dashboard	✓	✓	Only possible with Integrations
SaaS Setup	✓	✓	✓
On Premise Setup	✓	✗	✓
Plugins & Integration	✓	✓	✓
Input any data type	✓	Needs Plugins	Needs Plugins
Customer Support	✓	Available; but not proficient	Available; but not proficient
Documentation & Community	✓	✗	✓

3 نسخه‌ی رایگان و نسخه‌ی دارای مجوز نرم‌افزار Splunk

با دانلود و نصب نرم‌افزار Splunk Enterprise از Splunk.com، نسخه‌ی آزمایشی[14] آن به مدت 60 روز به صورت رایگان در اختیار شما قرار خواهدگرفت. با اتمام این زمان، در صورت تمایل می‌توانید با خریداری مجوز کار با نسخه‌ی enterprise را ادامه داده و یا در غیر این‌صورت، نسخه‌ی Spluk خود را به Free Splunk تغییر دهید که این کار به راحتی قابل انجام خواهد بود. در ادامه جزئیات بیشتری در این رابطه را مطالعه خواهید نمود.

3-1 مجوز نرم‌افزار Splunk Enterprise

در صورت خرید مجوز، دیگر محدودیتی برای تعداد کاربران، جستجوها، هشدارها، گزارش‌ها، داشبوردها و اشکال‌زدایی‌های خودکار نخواهید داشت.

هزینه‌ی مجوز بستگی به میزان داده‌ای دارد که شما روزانه نمایه‌سازی می‌کنید. به عبارت دیگر، مقدار داده‌های ثبتی که برای Splunk فرستاده می‌شود رابطه‌ی مستقیمی با هزینه‌ی مجوز شما دارد.

در صورتی که حجم نمایه‌سازی روزانه‌ی شما زیر 500 مگابایت باشد، Splunk را به صورت رایگان دانلود کرده و از آن استفاده نمایید.

شروع قیمت مجوز Enterprise از 5،175 دلار آمریکا برای نمایه‌سازی یک گیگابایت در روز، در ازای مجوز مادام‌العمر است. همچنین در صورت تمایل می‌توانید مجوز مدت‌دار را با 2،070 دلار برای نمایه‌سازی یک گیگابایت حجم در روز، به صورت سالانه خریداری کنید. بدیهی است که مجوز سالانه، پس از گذشت یک سال منقضی شده و شما باید دوباره کلید جدیدی را برای مجوز خریداری نمایید.

پیشنهاد می‌شود مجوزی را خریداری کنید که معادل بیشترین حجم داده‌ای است که انتظار دارید روزانه به Splunk خود بفرستید. شما فقط هزینه‌ی نمایه‌سازی داده را پرداخت خواهید کرد و پس از ذخیره‌ی داده، می‌توانید به تعداد بی‌شمار جستجو روی داده‌ی خود انجام دهید. همچنین برنامه انعطاف‌پذیری کاملی برای

[14] Trial

تنظیم زیربنا به شما خواهد داد که در نتیجه‌ی آن محدودیتی برای تعداد گره‌ها، هسته‌ها و سوکت‌ها نخواهید داشت.

3-1-1 مجوز مادام‌العمر و مجوز مدت‌دار

- مجوز مادام‌العمر[15]: این مجوز نسخه‌ی کامل Splunk Enterprise را در اختیار شما می‌گذارد.
- مجوز مدت‌دار: در صورت انتخاب این نوع مجوز می‌توانید به جای خرید مادام‌العمر و یک‌جا، هزینه‌ی مجوز را به صورت سالانه پرداخت کنید.

از طریق لینک زیر می‌توانید هزینه‌ی مجوز معادل حجم نمایه‌سازی روزانه‌ی خود را ملاحظه نمایید:

https://www.splunk.com/en_us/products/pricing.html?utm_expid=.OPF1ZinsTb2yA-taml2MNw.0&utm_referrer=https%3A%2F%2Fwww.google.co.uk%2F

- ✓ اعداد نوشته‌شده در جدول، برای مشتریان آمریکایی است و برای سایرین متفاوت خواهد بود.
- ✓ توجه داشته باشید که هزینه‌ی نسبی مجوز با افزایش حجم روزانه‌ی خریداری شده، کاهش می‌یابد.

Splunk ادعا می‌کند که هزینه‌های مجوزهای ذکر شده، در مقایسه با ابزارهای مشابه با Splunk بسیار مقرون به صرفه‌تر هستند.

3-2 نسخه‌ی رایگان Splunk

اگر حجم داده‌ای که روزانه نمایه‌سازی می‌کنید زیر 500 مگابایت باشد می‌توانید از نسخه‌ی رایگان Splunk استفاده کنید. مجوز نسخه‌ی رایگان هیچگاه منقضی نخواهد شد.

500 مگابایت سقف حجم داده‌ای است که قرار است روزانه نمایه‌سازی کنید؛ شما برای ذخیره‌ی داده سقفی نخواهید داشت. ممکن است روزی تنها 500 مگابایت به Splunk خود اضافه کنید ولی 10 ترابایت داده در Splunk داشته باشید.

Splunk Free به صورت پیوسته بر حجم داده‌ی شما نظارت خواهد داشت. اگر بیش از 3 بار در ماه (هر ماه 30 روز) از مقدار تعیین شده تخطی شود یا به عبارتی نمایه‌سازی روزانه بیش از 500 مگابایت باشد، Splunk

[15] Perpetual license

Free به نمایه‌سازی داده‌ی شما ادامه خواهد داد ولی عمل جستجو موقتاً برای شما غیرفعال خواهد شد. زمانی‌که تعداد هشدارهای شما کمتر از 3 بار در 30 روز باشد، عمل جستجو دوباره برای شما فعال می‌شود.

در لینک زیر می‌توانید قوانین مربوط به نقض مجوز و نحوه‌ی نظارت بر استفاده‌ی شما از Splunk Free را ملاحظه کنید:

http://docs.splunk.com/Documentation/Splunk/7.0.0/Admin/Aboutlicenseviolations

Splunk Free برای مصرف شخصی، جستجوی ad hoc و دستیابی به نمایش بصری داده‌های فناوری اطلاعات طراحی شده است. همچنین می‌توانید تا 3 بار در ماه، بیش از 500 مگابایت در یک روز را نمایه‌سازی کنید، که به شما این امکان را می‌دهد که هر چند وقت یک بار مجموعه‌داده‌های بزرگ را نیز بررسی کنید.

Splunk Free یک محصول تک‌کاربره است. تمام امکانات Splunk Enterprise را دارا است به استثناء موارد زیر:

- پیکربندی‌های مربوط به جستجوی توزیع‌شده (از جمله search head clustering)
- فوروارد کردن در فرمت TCP/HTTP. به این معنا که شما می‌توانید داده‌های خود را به مقصد دارای پلت‌فرم Splunk فوروارد کنید، ولی به نرم‌افزارهای غیر Splunk نه
- امکانات مربوط به مدیریت تعرفه
- هشدار (نظارت)
- خوشه‌بندی نمایه‌ساز
- Report acceleration summaries
- اگرچه یک Splunk Free می‌تواند به یک نمایه‌ساز Splunk Enterprise داده فوروارد کند اما نمی‌تواند سرویس‌گیرنده‌ی یک سرویس‌دهنده‌ی تعرفه باشد.
- امکان احراز اصالت، تعریف کاربر و مدیریت نقش وجود نخواهد داشت. به عبارت دیگر:
  - چیزی به نام login وجود ندارد. مرورگر و خط فرمان می‌توانند بدون استفاده از هرگونه نام‌کاربری و گذرواژه به تمام قسمت‌های Splunk Free دسترسی داشته باشند.
  - تمام دسترسی‌ها معادل دسترسی مدیر خواهد بود. فقط یک نقش وجود دارد و آن هم نقش مدیر. نمی‌توان نقش‌های دیگر و یا حساب کاربری اضافه کرد.
  - جستجوها روی نمایه‌های عمومی اجرا می‌شوند، 'index=*'
  - امکانات اعمال محدودیت در جستجو، مانند سهمیه‌ی کاربر و فیلترهای جستجو پشتیبانی نمی‌شوند.

- سیستم قابلیت‌ها[16] غیرفعال است. تمام قابلیت‌های موجود، برای تمام کاربرانی که از Splunk Free استفاده می‌کنند قابل دسترسی است.

جدول تفاوت امکانات نسخه‌ی رایگان و مجوز خریداری‌شده را می‌توانید در لینک زیر مشاهده نمایید.

https://www.splunk.com/en_us/products/features-comparison-chart.html

3-3 تبدیل نسخه‌ی آزمایشی Splunk Enterprise به Splunk Free

زمانی که برای اولین بار Splunk را دانلود و نصب کردید، به صورت خودکار در حال استفاده از نسخه‌ی آزمایشی Enterprise خواهید بود. بسته به نیازتان، می‌توانید بلافاصله بعد از نصب، آن را تبدیل به نسخه‌ی رایگان کنید و یا تا اتمام زمان مجوز آزمایشی صبر کنید و در این مدت از امکانات Splunk Enterprise استفاده کنید. بدیهی است که پس از تبدیل نسخه‌ی آزمایشی به Splunk Free، امکان استفاده از برخی امکانات برای شما امکان‌پذیر نخواهد بود.

- حساب‌های کاربری و نقش‌هایی که ایجاد کرده‌اید از کار می‌افتند.
- هر کسی که به Splunk Free دسترسی داشته باشد به‌صورت خودکار به عنوان مدیر وارد سیستم خواهد شد و شما دیگر صفحه‌ی login را نخواهید دید.
- تمامی اشیای دانش[17] (اعم از نوع رویداد، تراکنش، یا تعریف نوع منبع) که توسط هر کاربری به غیر از مدیر ساخته شده باشند، اگر تا لحظه‌ی تبدیل به Splunk Free به صورت عمومی به اشتراک گذاشته نشده باشند، دیگر در دسترس نخواهند بود. برای پیشگیری از بروز این مشکل، می‌توانید یکی از راه‌کارهای زیر را انجام دهید:
  - پیش از تبدیل به Splunk Free، با استفاده از Splunk Web تمام اشیاء را قابل دسترس عموم قرار دهید. لینک زیر را ببینید:

http://docs.splunk.com/Documentation/Splunk/7.0.0/Admin/Managingappobjects

  - پیکربندی فایل‌هایی که اشیاء مورد نظر در آن‌ها هستند را به صورت دستی ویرایش کنید. لینک زیر را ببینید:

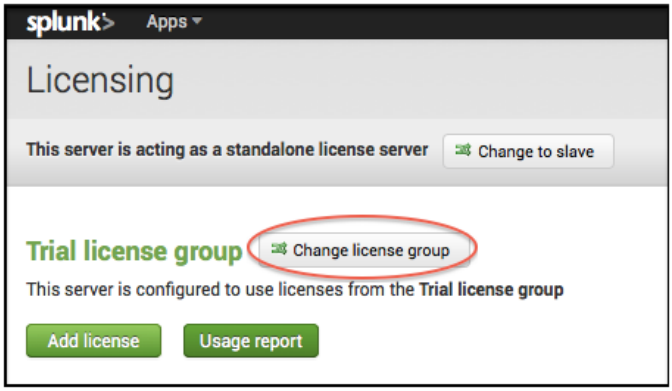
[16] Capability system
[17] Knowledge object

http://docs.splunk.com/Documentation/Splunk/7.0.0/Admin/Apparchitectureandobjectownership#Make_Splunk_knowledge_objects_globally_available

- هشدارهایی که تعریف کرده‌اید از کار خواهند افتاد. به عبارت دیگر شما هیچ هشداری از نرم‌افزار Splunk دریافت نخواهید کرد. هرچند شما همچنان می‌توانید جستجوهایتان را به منظور اجرای داشبوردها و نمایه‌سازی خلاصه[۱۸] برنامه‌ریزی کنید.
- پیکربندی‌های داخل outputs.conf که به منظور فورواردکردن در قالب TCP یا HTTP به یک شخص ثالث صورت گرفته بودند، از کار خواهند افتاد.

اگر در حال حاضر از نسخه‌ی Splunk Enterprise (چه آزمایشی و چه مجوز خریداری‌شده) استفاده می‌کنید، می‌توانید در هر زمانی به Splunk Free سوئیچ کنید. برای تبدیل به Splunk Free به صورت زیر عمل کنید:

1. به Splunk Web به عنوان مدیر وارد شوید و به بخش Settings > Licensing بروید.
2. بر روی Change license group در بالای صفحه کلیک کنید. (شکل 1)



شکل 8: تبدیل Splunk Enterprise به Splunk Free

3. Free license را انتخاب کرده بر روی دکمه‌ی Save کلیک کنید.
4. Restart کنید.

✓ آخرین نسخه ارائه شده تا زمان ثبت این گزارش، Splunk Enterprise 7.0.0 می‌باشد که در تاریخ 26 سپتامبر 2016 میلادی ارائه شده است.*(نسخه‌ی این برنامه Splunk Enterprise 6.4.3 در سایت‌های فارسی قابل دسترس می‌باشد.)*

[18] Summary indexing

4 Splunk Enterprise 7.0

در این بخش، نام ویژگی و یا امکانات اضافه شده در این نسخه، همراه با توضیح مختصری در مورد هر کدام از آن‌ها، ارائه شده است.

- معیارها:
  - امکان ذخیره‌ی اندازه‌گیری‌های معیار در مقیاس مورد نظر
  - دستور جدید mstat: یک دستور جدید برای SPL که معادل tstat برای داده‌های سری‌های زمانی از نمایه‌های معیارها است.
  - دستور جدید mcatalog: دستوری در SPL که کاربرد آن تجمیع مقادیر در نمایه‌های معیارها است، مانند میانگین‌گرفتن، جمع‌زدن و غیره.
  - Metrics Catalog: فهرست‌کردن معیارها، ابعاد، و مقادیر به دست آمده از نمایه‌های معیار
- Event Annotation:

می‌توانید ارتباط بین logها و معیارها را در یک تصویر ببینید.

- Chart Enhancements:

گزینه‌های جدیدی به کتابخانه‌ی نمودار اضافه شده است که کیفیت عمل نظارت در داشبوردها را بهبود می‌بخشند.

- Faster Search Performance:

با توجه به بهبود عملکرد موازی همزمان با نوشتن بر روی دیسک، سرعت عملیات جستجو افزایش یافته است.

- Report Actions:

به‌منظور سازگاری هرچه بیشتر و افزایش قابلیت‌های زمان‌بندی، یک انتخاب‌کننده هشدار سفارشی[19] به زمان‌بندی گزارش اضافه شده است.

[19] Custom alert actions selector

- Additional monitoring console panels:

پنل‌های جدیدی به عملیات نمایه‌سازی اضافه شده‌اند.

5 معماری Splunk

برای فهمیدن نحوه‌ی کارکرد Splunk لازم است که با معماری Splunk و اجزای آن آشنا شویم. Splunk اساساً از ترکیب 4 مؤلفه تشکیل شده است که به‌منظور هرچه بیشتر کردن کارایی، با هم همکاری می‌کنند. می‌توان این مؤلفه‌ها را بر حسب نیاز، بر روی یک یا چند سرویس‌دهنده‌ی مختلف نصب کرد. در ادامه به معرفی کلی هر یک از این 4 مؤلفه می‌پردازیم.

5-1 مؤلفه‌های معماری Splunk

- Search Head: Splunk search head در واقع همان واسط کاربر گرافیکی نرم‌افزار است که ما با استفاده از آن جستجو، تحلیل، و گزارش می‌کنیم.
- Forwarder: مؤلفه‌ی Splunk forwarder مانند یک مأمور مخفی برای Splunk عمل می‌کند! این مؤلفه داده‌ها را از منابع مختلف مانند Windows server، Linux server، مسیریاب‌ها، دیواره‌های آتش و غیره جمع‌آوری کرده و به منظور نمایه‌سازی به نمایه‌ساز ارسال می‌کند.

  Splunk دو نوع Forwarder دارد:

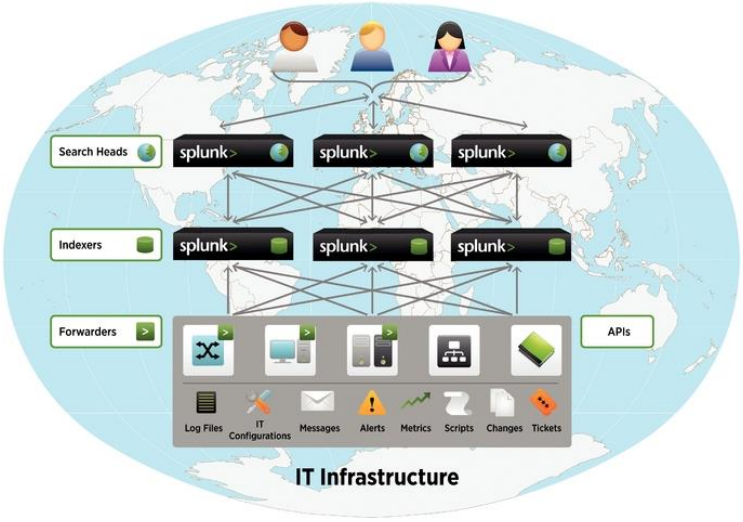
  - Universal Forward (UF): مأمور Splunk که بر روی یک سیستم غیر Splunk نصب شده است. قابلیت تجزیه یا نمایه‌سازی داده را ندارد.
  - Heavy Weight Forwarder (HWF): این نوع Forwarder دارای قابلیت‌های پیشرفته است. عموماً در نقش Forwarder سطح متوسط، جمع‌آوری‌کننده‌ی داده از راه دور، و گاهی فیلتر داده عمل می‌کند. HWFها داده را تجزیه می‌کنند.
- Indexer: این مؤلفه با ساختن و مدیریت‌کردن نمایه‌ها سر و کار دارد. عملیات اولیه‌ی یک نمایه‌ساز عبارتند از:
  - نمایه‌سازی داده‌ی ورودی
  - جستجو در داده‌ی نمایه‌شده

در شکل زیر سطوح نمایه‌سازی را مشاهده می‌کنید که در آن عملیات پردازش logها و ذخیره‌ی آن‌ها به‌منظور جستجو در آینده، انجام می‌گیرد.

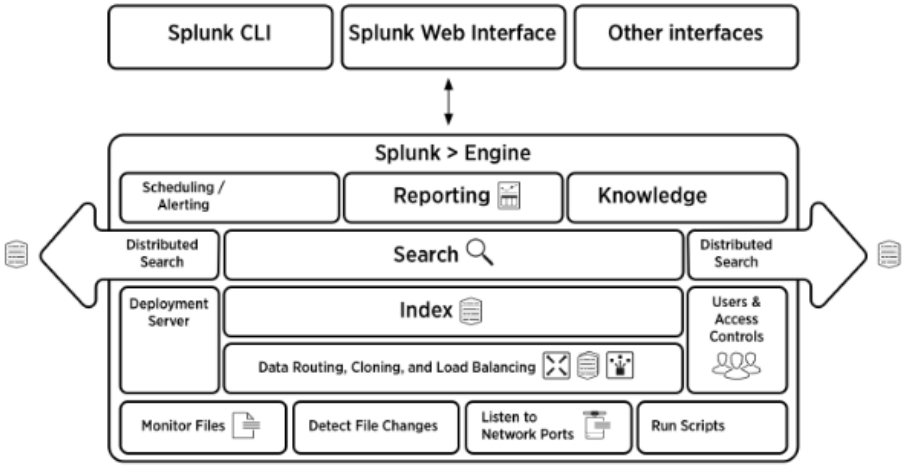
شکل 9: سطوح نمایه‌سازی در Splunk

- سرویس‌دهنده‌ی استقرار[20]: سرویس‌دهنده‌ی استقرار Splunk به عنوان یک میزبان، برنامه‌های کاربردی را روی مؤلفه‌های مختلف داخل ساختمان Splunk پیاده‌سازی می‌کند. از این سرویس‌دهنده معمولاً به‌منظور پیاده‌سازی افزودنی‌ها[21] روی Forwarderها و نمایه‌سازها استفاده می‌شود.
- سرویس‌دهنده‌ی مجوز[22]: این سرویس‌دهنده وظیفه‌ی مدیریت و نظارت بر کارکرد مجوز را برعهده دارد.

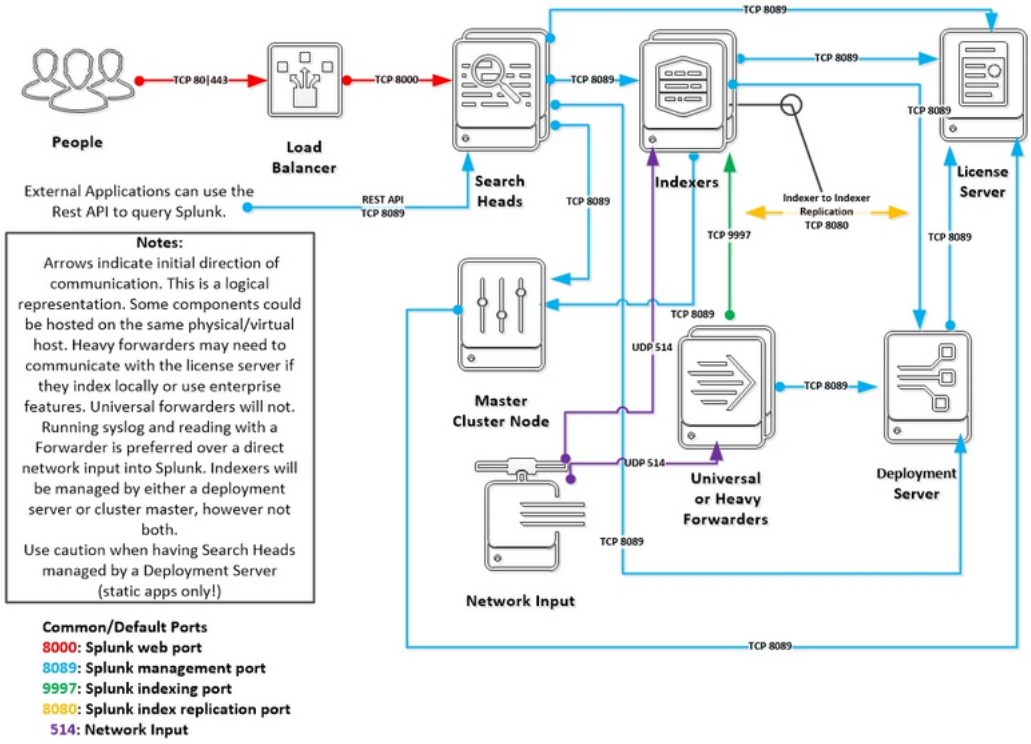
در اشکال زیر می‌توانید مؤلفه‌ها را، به‌همراه درگاه‌هایی که به‌منظور ارتباط بین آن‌ها مورد استفاده قرار می‌گیرند، ببینید.



[20] Deployment server
[21] Add-on
[22] Licensing server



شکل 10: معماری کلی و مولفه‌های ابزار



شکل 11: معماری کلی و مولفه‌های ابزار

توضیحات شکل بالا:

- بردارها بیان‌گر جهت شروع ارتباط هستند.
- این تصویر یک تصویر انتزاعی است.
- برخی از مؤلفه‌ها امکان قرارگرفتن بر روی میزبان فیزیکی/مجازی مشترک را دارند.

- Forwarderهای سنگین در صورت نمایه‌سازی داده‌های محلی و با استفاده از ویژگی‌های Enterprise، ممکن است نیاز به ارتباط با سرویس‌دهنده‌ی مجوز داشته باشند. Forwarderهای جهانی نیاز به این ارتباط نخواهند داشت.
- اجرای syslog و خواندن توسط یک Forwarder، به ورودی مستقیم از شبکه به Splunk ترجیح داده می‌شود.
- مدیریت نمایه‌سازها بر عهده‌ی یک سرویس‌دهنده‌ی استقرار یا یک cluster master است، اما نه هر دو.
- در صورت استفاده از Search headهایی که توسط یک سرویس‌دهنده‌ی استقرار مدیریت می‌شوند محتاطانه عمل کنید (فقط برنامه‌های کاربردی ایستا!).

2-5 درگاه‌های استفاده شده توسط Splunk

رایج‌ترین درگاه‌های استفاده شده توسط Splunk عبارتند از:

- Splunk Web Port: 8000
- Splunk Management Port: 8089
- Splunk Indexing Port: 9997
- Splunk Index Replication: 8080
- Splunk Network Port: 514 (به منظور ورود داده از درگاه شبکه)

شما می‌توانید در صورت نیاز این درگاه‌ها را تغییر دهید.

3-5 پردازه‌های Splunkd و Splunkweb

سرویس‌دهنده‌ی Splunk Enterprise پردازه‌ای به نام Splunkd را روی میزبان شما نصب می‌کند. Splunkd یک پردازه سیستمی است که وظیفه‌ی نمایه‌سازی، جستجو، Forwarding و (از Splunk Enterprise version 6.2 به بعد) واسط وب برای ورود به Splunk Enterprise را بر عهده دارد.

Splunkd یک سرویس‌دهنده‌ی C/C++ توزیع‌شده است که به جریان داده‌ی فناوری اطلاعات دسترسی پیدا کرده و آن را پردازش و نمایه می‌کند. همچنین رسیدگی به درخواست‌های جستجو توسط Splunkd صورت می‌گیرد.

Splunkweb واسط کاربری گرافیکی تعاملی نرم‌افزار Splunk است. شما توسط یک مرورگر وب به آن دسترسی خواهید داشت. Splunkweb واسط اولیه برای بررسی مشکلات، گزارش‌گیری روی نتایج جستجو، و مدیریت اجرایی Splunk Enterprise است.

اگر علاقه‌ای به کار با Splunkweb در محیط گرافیکی ندارید می‌توانید با استفاده از سرویس‌دهنده‌ی Splunkd در خط فرمان، با نرم‌افزار Splunk کار کنید.

6 نیازمندی‌های سیستم برای نصب Splunk Enterprise

6-1 نیازمندی‌های نرم‌افزاری سیستم

6-1-1 سیستم‌عامل‌های یونیکس

جدول 2: سیستم‌عامل‌های یونیکس و وضعیت پشتیبانی Splunk از آن‌ها

Operating system	Architecture	Enterprise	Free	Trial	Universal Forwarder
Solaris 10 and 11	x86 (64-bit)				X
	SPARC				X
Linux, kernel version 2.6 and later	x86 (64-bit)	X	X	X	X
Linux, kernel version 3.x and later	x86 (64-bit)	X	X	X	X
PowerLinux, kernel version 2.6 and later (includes Big Endian and Little Endian versions)	PowerPC				D
zLinux, kernel version 2.6 and later	s390x				X
FreeBSD 9	x86 (64-bit)				D
FreeBSD 10 and 11	x86 (64-bit)				X
Mac OS X 10.11 and macOS 10.12 and 10.13	Intel		X	X	X
AIX 7.1 and 7.2	PowerPC				X
ARM Linux	ARM				A

در جدول 2 داریم:

- A: نرم‌افزار مناسب این زیرساخت در splunk.com موجود است ولی هیچگونه پشتیبانی رسمی از آن نمی‌شود.
- D: Splunk فعلاً از این زیرساخت پشتیبانی می‌کند اما ممکن است در نسخه بعدی، دیگر این پشتیبانی صورت نگیرد.

2-1-6 سیستم‌عامل‌های ویندوز

جدول 3: سیستم‌عامل‌های ویندوز و وضعیت پشتیبانی Splunk از آن‌ها

Operating system	Architecture	Enterprise	Free	Trial	Universal Forwarder
Windows Server 2008 R2	x86 (64-bit)				D
Windows Server 2012, Server 2012 R2, and Server 2016	x86 (64-bit)	X	X	X	X
Windows 8	x86 (64-bit)				D
	x86 (32-bit)				N
Windows 8.1 and 10	x86 (64-bit)		X	X	X
	x86 (32-bit)		***	***	X

در جدول 3 داریم:

- D: Splunk فعلاً از این زیرساخت پشتیبانی می‌کند اما ممکن است در نسخه بعدی، دیگر این پشتیبانی صورت نگیرد.
- N: Splunk این زیرساخت و معماری را پشتیبانی نمی‌کند. در صورت نیاز به پشتیبانی از طرف Splunk، نسخه‌های قدیمی‌تر این نرم‌افزار را دانلود کنید.
- ***: Splunk از این زیرساخت پشتیبانی می‌کند اما استفاده از Splunk Enterprise بر روی این زیرساخت و معماری را توصیه نمی‌کند.

توصیه می‌شود که به منظور افزایش کارآیی Splunk Enterprise در سازمان شما، از سخت‌افزار رایج در محیط سازمان برای کار با این نرم‌افزار استفاده کنید. بدیهی است که این سخت‌افزار باید حداقل‌های لازم برای Splunk Enterprise را داشته باشد.

2-6 مرورگرهای سازگار با Splunk Enterprise

- Firefox (آخرین نسخه)
- Internet Explorer (نرم‌افزار Splunk از این مرورگر در حالت Compatibility Mode پشتیبانی نمی‌کند.)
- Safari (آخرین نسخه)
- Chrome (آخرین نسخه)

3-6 سخت‌افزار توصیه‌شده

Splunk Enterprise می‌تواند به هر اندازه که شما بخواهید گسترش یابد اما برای استفاده از این خاصیت مقیاس‌پذیری، نیاز به مدیریت ظرفیت است. برای دیدن راهنمای سطح بالای سخت‌افزار و جزئیات اینکه Splunk Enterprise دقیقاً چگونه از منابع سخت‌افزاری استفاده می‌کند به آدرس زیر مراجعه کنید.

http://docs.splunk.com/Documentation/Splunk/7.0.0/Capacity/IntroductiontocapacityplanningforSplunkEnterprise

موارد ذکر شده در جدول زیر برای نصب تنها یک نسخه Splunk Enterprise با کارکرد کم تا متوسط است.

جدول 4: سخت‌افزار توصیه‌شده برای نصب نسخه Splunk Enterprise با کارکرد کم تا متوسط

Platform	Recommended hardware capacity/configuration
Non-Windows platforms	2x six-core, 2+ GHz CPU, 12GB RAM, Redundant Array of Independent Disks (RAID) 0 or 1+0, with a 64 bit OS installed.
Windows platforms	2x six-core, 2+ GHz CPU, 12GB RAM, RAID 0 or 1+0, with a 64-bit OS installed.

4-6 Splunk Enterprise و ماشین مجازی

اگر Splunk Enterprise را در یک ماشین مجازی بر روی هر زیرساختی اجرا کنید، کارایی کاهش می‌یابد. دلیل این امر این است که مجازی‌سازی، در واقع ارائه‌ی مفهومیِ سخت‌افزار بر روی یک ماشین دارای منابع مورد نیاز است. ماشین‌های مجازی که شما روی سیستم خود تعریف می‌کنید از این منابع استفاده می‌کنند. Splunk Enterprise نیاز به دسترسی دائمی به برخی از این منابع، به خصوص ورودی/خروجی دیسک دارد. Splunk Enterprise به‌منظور نمایه‌سازی داده نیاز به دسترسی مستمر به این منبع دارد و در صورتی که این نرم‌افزار بر روی یک ماشین مجازی، همراه با چند ماشین مجازی دیگر در حال اجرا باشد، ممکن است عملیات نمایه‌سازی و جستجو با اختلال مواجه شود.

7 دانلود، نصب، و راه‌اندازی Splunk Enterprise

1-7 دانلود Splunk Enterprise

در ابتدا لازم است که شما یک حساب کاربری در Splunk.com ایجاد کنید. برای این کار کافی است به آدرس https://www.splunk.com/ مراجعه کرده و روی My Account > Sing up کلیک کنید. سپس به منظور

دانلود آخرین نسخه‌ی نرم‌افزار Splunk Enterprise، به لینک زیر مراجعه کرده و نسخه‌ی مطابق با سیستم‌عامل خود را انتخاب و دانلود کنید:

https://www.splunk.com/index.php/predownload?d=progeneric

✓ در نظر داشته باشید که وب‌سایت Splunk و تمام امکانات آنلاین این سازمان، برای IPهای ایران خارج از دسترس است.

2-7 نصب و راه‌اندازی Splunk Enterprise

1-2-7 نصب و راه‌اندازی Splunk روی ویندوز

در ادامه مراحل نصب و راه‌اندازی Splunk در ویندوز آمده است.

1. پیش از آغاز نصب، آنتی‌ویروس خود را غیرفعال کنید چرا که هر نرم‌افزاری که بین Splunk Enterprise و سیستم‌عامل مداخله کند ممکن است باعث محدود شدن قدرت پردازشی که باید در اختیار Splunk قرار داده شود گردد که نتیجه‌ی آن کندشدن سیستم و یا عدم پاسخگویی آن است.
2. پس از دانلود Splunk Enterprise مطابق با سیستم‌عامل خود، فایل splunk.msi را اجرا کنید تا فرآیند نصب آغاز شود.
3. پنل Welcome را Next کنید.
4. گزینه‌ی «I accept the terms in the license agreement» را select کرده و سپس Next کنید.
5. در قسمت Customer Information، جزئیات درخواست شده را تایپ کرده و Next کنید.
6. در پنل Destination Folder، در صورت نیاز به تغییر مسیر نصب فایل بر روی Change کلیک کنید و در غیر این صورت با کلیک بر روی Next، مسیر پیش‌فرض را انتخاب کنید.
   - Splunk Enterprise به صورت پیش‌فرض در مسیر \Program Files\Splunk نصب خواهد شد.
7. در پنل Logon Information، گزینه‌ی Local system user را انتخاب کرده و Next کنید.
   - در صورتی که بخواهید نرم‌افزار به عنوان کاربر دیگری اجرا شود، گزینه‌ی Domain Account را انتخاب کنید. در صفحه‌ای که با کلیک بر روی Next باز خواهد شد، نام کاربر مورد نظرتان را در قالب domain\username وارد کنید. این کاربر باید یک کاربر معتبر در سیستم شما بوده و در یک Active Directory عضوی فعال باشد. Splunk Enterprise باید توسط حساب کاربری

Local System و یا یک حساب کاربری معتبر با گذرواژه معتبر و امتیازات مدیر محلی اجرا شود. در غیر این صورت فرآیند نصب ناموفق خواهد بود.

8. پس از انتخاب اینکه آیا مایلید shortcut این نرم‌افزار را در منوی Start خود داشته باشید یا خیر، با کلیک بر روی Install فرآیند نصب خود را کامل کنید.
9. پس از اینکه برنامه با موفقیت بر روی سیستم شما نصب شد روی Finish کلیک کنید.
10. برنامه‌ی کاربردی را از منوی start باز کنید. از آنجایی که Splunk یک برنامه‌ی کاربردی مبتنی بر وب است در یک مرورگر باز خواهد شد.
11. زمانی که می‌خواهید برای اولین بار وارد نرم‌افزار شوید باید واژه‌ی admin را به عنوان نام‌کاربری و عبارت changeme را به عنوان گذرواژه وارد کنید. شما بلافاصله اجازه‌ی تغییر گذرواژه را خواهید داشت.
    - توجه داشته باشید که این حساب کاربری با حسابی که شما در Splunk.com برای خود ایجاد کردید متفاوت است. لذا برای شروع به کار با نرم‌افزار Splunk از نام‌کاربری و گذرواژه گفته شده استفاده نمایید.
12. از حساب کاربری خود در Splunk خارج شده و سپس دوباره وارد شوید. این کار باعث تکمیل‌شدن فرآیند نصب می‌شود.
13. در صورتی که مجوز خریداری کرده‌اید، به منظور نصب آن:
    1) در داخل برنامه به مسیر Settings > Licensing بروید.
    2) بر روی Add License کلیک کنید.
    3) روی Choose file کلیک کنید و مجوز را از مسیری که در آن قرار دارد انتخاب کنید، و یا روی copy & paste the license XML directly… کلیک کنید و متن فایل مجوز خود را در فیلدی که در اختیار شما قرار داده شده است paste کنید.
    4) با کلیک بر روی Install، نرم‌افزار مجوز شما را نصب خواهد کرد.
    5) اگر این اولین Enterprise license شما است Splunk Enterprise را دوباره راه‌اندازی کنید.

2-2-7 نصب و راه‌اندازی Splunk بر روی لینوکس

Splunk Enterprise سه گزینه برای نصب بر روی لینوکس ارائه داده است. شما می‌توانید از هر یک از RPM، DEB، و یا فایل tar. به منظور نصب این نرم‌افزار بر روی سیستم خود استفاده کنید.

پیش از آغاز فرآیند نصب، لازم است که شما به یک واسط خط فرمان دسترسی داشته باشید. هنگامی که در دستورهای مربوط به نصب تایپ می‌کنید، نام فایل Splunk Enterprise installer که پیش‌تر دانلود کرده‌اید را جایگزین عبارت splunk_package_name کنید.

- نصب Splunk Enterprise RPM

1. شما می‌توانید Splunk Enterprise RPM را در مسیر پیش‌فرض /opt/splunk و یا مسیر دلخواه خودتان نصب کنید.
2. برای نصب Splunk Enterprise از خط فرمان استفاده کنید.
   - به منظور نصب در مسیر پیش‌فرض، عبارت زیر را تایپ کنید:

```
rpm -i splunk_package_name.rpm
```

   - به منظور نصب در مسیری غیر از مسیر پیش‌فرض، پرچم prefix-- را به دستور نصب اضافه کنید. برای مثال:

```
rpm -i --prefix=/opt/new_directory splunk_package_name.rpm
```

- نصب Splunk Enterprise DEB package

با توجه به اینکه Splunk Enterprise DEB فقط در مسیر /opt/splunk قابل نصب است، دستور زیر را در خط فرمان تایپ کنید:

```
dpkg -i splunk_package_name.deb
```

- نصب Splunk Enterprise tar file

1. در صورت استفاده از فایل tar مسیر پیش‌فرض، "splunk" در مسیر جاری شما خواهد بود. شما می‌توانید با استفاده از گزینه‌ی C- برنامه را در مسیر به خصوصی مانند /opt/splunk نصب کنید.
2. با استفاده از دستور tar فایل را به مسیر دلخواه‌تان گسترش دهید. به منظور گسترش آن در مسیر /opt/splunk کافی است دستور زیر را در خط فرمان تایپ کنید:

```
tar xvzf splunk_package_name.tgz -C /opt
```

برای دیدن جزئیات بیشتر در رابطه با نصب Spunk Enterprise بر روی سیستم‌عامل لینوکس به لینک زیر مراجعه کنید:

http://docs.splunk.com/Documentation/Splunk/7.0.0/Installation/InstallonLinux

3-2-7 نصب و راه‌اندازی Splunk بر روی سیستم‌عامل Mac

نسخه‌ی کامل Splunk Enterprise برای این سیستم‌عامل موجود نمی‌باشد اما نسخه‌ی آزمایشی و رایگان آن قابل نصب است.

1. فایل DMG را اجرا کنید. یک پنجره‌ی Finder که شامل splunk.pkg است باز خواهد شد.
2. روی آیکون Install Splunk کلیک کنید تا فرآیند نصب آغاز شود.
3. پنل Introduction اطلاعاتی در مورد نسخه و قوانین کپی‌رایت در اختیار شما قرار می‌دهد. روی Continue کلیک کنید.
4. پنل License توافق‌نامه‌ی مربوط به مجوز نرم‌افزار را نمایش می‌دهد. بر روی Continue کلیک کنید.
5. از شما درخواست می‌شود که با مفاد توافق‌نامه‌ی مجوز نرم‌افزار موافقت کنید. روی دکمه‌ی Agree کلیک کنید.
6. در پنل Destination Select مسیر پیش‌فرض (Macintosh HD) را تغییر ندهید. روی Continue کلیک کنید.
7. در پنل Installation Type روی Install کلیک کنید. این کار باعث نصب‌شدن Splunk Enterprise در مسیر پیش‌فرض یعنی Applications/splunk خواهد شد.
8. شما باید یک گذرواژه را وارد کنید.
9. پس از اتمام فرآیند نصب، یک popup ظاهر خواهد شد و به شما اعلام خواهد کرد که به یک مقداردهی اولیه نیاز است. روی OK کلیک کنید.
10. popup دیگری ظاهر خواهد شد و از شما سؤال خواهد کرد که مایلید چه کاری انجام دهید. با کلیک بر روی Start and Show Splunk، صفحه‌ی ورود برای Splunk Enterprise در پنجره‌ی مرورگر شما باز خواهد شد.
11. یک میان‌بر در دسکتاپ ایجاد خواهد شد تا شما به سادگی به Splunk Enterprise خود دسترسی داشته باشید.

برای دیدن جزئیات بیشتر در رابطه با نصب Spunk Enterprise بر روی سیستم‌عامل Mac به لینک زیر مراجعه کنید:

http://docs.splunk.com/Documentation/Splunk/7.0.0/Installation/InstallonMacOS

8 منابع

[1] http://docs.splunk.com
[2] http://www.learnsplunk.com
[3] https://www.splunk.com
[4] https://www.slideshare.net
[5] https://answers.splunk.com/index.html
[6] https://www.edureka.co/