بسمه تعالی

معرفی، آموزش نصب و پیکربندی سامانه

HP Arcsight

(بخش سوم)

فهرست مطالب

1 مقدمه

برای برقراری امنیت و شناسایی حملات و مقابله با آن‌ها از ابزارهای مختلفی استفاده می‌شود. یکی از این ابزارها SIEM است که در مرکز عملیات امنیت مورد استفاده قرار می‌گیرد. تولیدکنندگان مختلف در سراسر جهان محصولات SIEM متنوعی را تولید کرده‌اند. یکی از این تولیدکنندگان ArcSight از زیرمجموعه های شرکت HP است که محصول ESM را در این حوزه ارائه کرده است. شرکت ArcSight علاوه بر ESM محصولات دیگری را نیز تولید کرده است که در حوزه SOC کاربرد دارند. در این سند مؤلفه‌های محصول ESM بررسی و نحوه نصب آن‌ها بیان می‌شود. همچنین قابلیت‌های مختلف محصول طی سناریوهای عملی معرفی می‌شوند.

2 نصب مؤلفه‌های معماری

در این بخش بااستفاده از یک سناریوی عملی، معرفی محصول انجام می‌شود. ابتدا نحوه نصب مؤلفه‌های محصول بیان می‌شود. این مؤلفه‌ها عبارتند از ESM، Console و SmartConnector.

2-1 نصب ESM روی Appliance

هنگامی که Appliance را روشن می‌کنید، ویزارد اولین راه‌اندازی سیستم‌عامل[1] به‌صورت خودکار شروع می‌شود. این ویزارد یک محیط خط فرمان است که پرسش‌هایی را برای انجام تنظیمات ضروری ارائه می‌کند. این پرسش‌ها به‌ترتیب در ادامه آورده شده‌اند.

1. صفحه ورود نمایش داده می‌شود، با نام کاربری root و گذرواژه arcsight وارد شوید.
2. گذرواژه جدیدی برای کاربر root انتخاب کنید.
3. گذرواژه جدیدی برای کاربر arcsight انتخاب کنید.
4. Hostname را برای Appliance تنظیم کنید.
5. آدرس IP را برای Appliance انتخاب کنید.
6. Netmask را وارد کنید.
7. Default gateway را وارد کنید.

[1] Operating System First Boot

8. آدرس DNS IP اصلی را وارد کنید.
9. آدرس DNS IP جایگزین را وارد کنید.
10. دامنه جستجوی DNS را تعیین کنید.
11. منطقه زمانی را تعیین کنید.
12. تاریخ را وارد کنید.
13. زمان را وارد کنید.
14. کارگزار NTP را تعیین کنید.

در انتها خلاصه‌ای از تنظیمات انجام‌شده را ارائه می‌کند. در صورت انصراف از انجام تنظیمات گزینه No را انتخاب کنید تا این مراحل از ابتدا شروع شوند. در صورت موافقت کلید Enter را بزنید. به‌این‌ترتیب نشست نصب خاتمه یافته و ویزارد پیکربندی شروع می‌شود.

توجه: در خاتمه نصب دستوری برای اجرای ویزاد پیکربندی نصب ارائه می‌شود که پس از خاتمه ویزارد به صورت خودکار شروع شود.

در ادامه با استفاده از آدرس IP تخصیص‌یافته به ESM متصل شده و فایل license را در آن بارگذاری کنید.

پس از خاتمه نشست انجام تنظیمات ضروری ویزارد پیکربندی شروع و به ترتیب زیر ادامه پیدا می‌کند.

1. پیغام خوشامدگویی را ملاحظه و در صورتی‌که فایل License را بارگذاری کرده‌اید، برای ادامه گزینه Yes را وارد کنید.
2. زبان مورد نظر را، برای نمایش ادامه نصب با آن زبان، انتخاب کرده و Enter بزنید.
3. در صورتی‌که می‌خواهید کاراکترهای گذرواژه به صورت مبهم نمایش داده شوند Enter بزنید و اگر می‌خواهید نمایش داده شوند، عبارت No را وارد کرده و سپس Enter بزنید.
4. گذرواژه CORR-Engine را وارد کرده و سپس مجدداً برای تائید گذرواژه آن را وارد کنید و Enter را فشار دهید.
5. اطلاعات حافظه ذخیره‌سازی CORR-Engine را وارد کرده و Enter بزنید. این اطلاعات عبارتند از:
   - اندازه حافظه ذخیره‌سازی سیستم: فضای حافظه‌ای که برای ذخیره‌سازی منابع مورد استفاده قرار می‌گیرد.
   - اندازه حافظه ذخیره‌سازی رویداد: فضای حافظه‌ای که برای ذخیره‌سازی رویدادها مورد استفاده قرار می‌گیرد.

- اندازه آرشیو رویداد برخط[2]: بیشترین اندازه فضای مورد استفاده برای آرشیو رویدادها.
- دوره نگهداری: مدت زمانی که رویدادها باید در حافظه نگهداری شوند.

6. ورود آدرس‌های پست الکترونیکی زیر:

- دریافت‌کننده اعلان خطا[3]: تعیین آدرس پست الکترونیکی برای این‌که اگر ESM با خطا مواجه شد، به آدرس واردشده اخطار پست الکترونیکی ارسال کند.
- از آدرس پست الکترونیکی[4]: آدرس پست الکترونیکی که به‌عنوان ارسال‌کننده از آن استفاده می‌شود.

سپس عبارت Yes را وارد کرده و Enter بزنید.

7. مسیر فایل License را وارد کرده و Enter بزنید.
8. حالت نصب را انتخاب کنید. دو حالت وجود دارد، Default Mode و FIPS Mode.

توجه: هر حالتی که برای نصب انتخاب می‌کنید هنگام نصب کنسول نیز باید همان حالت را انتخاب کنید. اگر حالت FIPS انتخاب شود، دیگر امکان برگشت به حالت پیش‌فرض وجود ندارد، اما اگر در حالت پیش‌فرض نصب شود، امکان تبدیل به حالت FIPS وجود دارد.

9. اگر حالت FIPS را انتخاب کرده‌اید انتخاب خود را تأیید کنید، در غیر این‌صورت این گام را رد کنید.
10. اگر حالت FIPS انتخاب شده باشد، در بخش Select the Cipher Suite Options پشته رمزنگاری را انتخاب کنید.
11. در بخش اطلاعات Manager، Host Name یا آدرس Manager IP را وارد کنید و نام‌کاربری و گذرواژه مدیر را وارد کنید. سپس Enter بزنید.
12. در بخش Packages اگر Package License را خریداری کرده‌اید آن را انتخاب کنید. به‌صورت پیش‌فرض License هیچ Packageای را ندارد. کلید Enter را برای ادامه بزنید.
13. هنگامی که سیستم پیغام Configuration Completed Successfully را داد Yes را تایپ کنید و برای خارج‌شدن از ویزارد پیکربندی Enter کنید.
14. به عنوان کاربر root واردشده و با اجرای دستور زیر برای راه‌اندازی سرویس‌های ضروری اقدام کنید:

/opt/arcsight/manager/bin/setup_services.sh

---

[2] Online Event Archive Size
[3] Error Notification Recipient
[4] From email address

2-2 نصب Console

کنسول یک واسط مبتنی بر میزبان برای دسترسی به ESM است که روی سه سکوی Linux، Windows و Macintosh نصب می‌شود.

مراحل نصب کنسول به‌ترتیب عبارتند از:

1. متناسب با سکو فایل نصب کنسول را اجرا کنید. برای نصب روی سکوی ویندوز فایل ArcSight-6.9.1.0-Console-Win.exe را اجرا کنید.
2. در صفحه بررسی فرآیند نصب گزینه Next را انتخاب کنید.
3. مقدمه‌ای نمایش داده می‌شود، آن را خوانده و Next کنید.
4. در صفحه موافقت با License برای فعال‌شدن گزینه موافقت تا انتهای متن را مرور کنید و سپس تیک آن را زده و Next کنید.
5. توضیحات ارائه شده در صفحه ویژه را خوانده و Next کنید.
6. مسیر نصب کنسول را انتخاب کرده و Next کنید.
7. مسیر ایجاد Shortcut را انتخاب کرده و Next کنید.
8. پس از مشاهده و مرور خلاصه‌ای از تنظیمات، گزینه Install را انتخاب کرده تا فرآیند نصب شروع شود. در صورتی‌که بخواهید تغییری اعمال کنید، با انتخاب گزینه Previous می‌توانید این کار را انجام دهید.

هنگام نصب ممکن است با پیغام "TZData update was not successful" مواجه شوید، گزینه OK را انتخاب کرده و Next کنید.

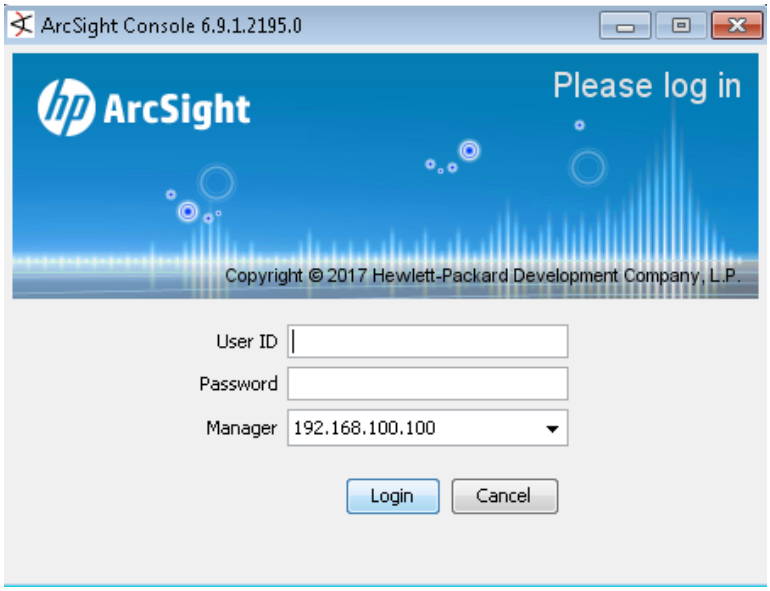
پس از نصب باید پیکربندی را انجام دهید.

1. ویزارد ابتدا می‌پرسد که آیا یک پیکربندی برای کنسولی که در حال حاضر نصب است دارید و مایل هستید آن پیکربندی را انتقال دهید. در صورتی‌که تمایل ندارید یا اولین بار است که کنسول را نصب کرده‌اید، گزینه No را انتخاب کرده و Next را بزنید.
2. حالت نصب را انتخاب کنید. از آنجایی‌که ESM در حالت پیش‌فرض نصب شد، حالت نصب کنسول را نیز پیش‌فرض انتخاب کنید. اگر بخواهید در حالت FIPS آن را نصب کنید از شما می‌خواهد پشته رمزنگاری را انتخاب کنید. گزینه Next را انتخاب کنید.
3. Manager Hostname که کنسول قرار است به آن متصل شود را وارد کنید، شماره درگاه آن را تغییر ندهید. Next را انتخاب کنید.

4. گزینه Use direct connection را انتخاب کرده و Next کنید. در صورتی‌که نمی‌توانید به Manager به‌صورت مستقیم وصل شوید، می‌توانید یک سرویس‌دهنده واسط را راه‌اندازی کرده و از طریق آن به Manager متصل شوید. در این‌صورت باید گزینه "Use proxy server" را انتخاب کرده و اطلاعات واسط را وارد کنید.
5. در این مرحله باید نوع احرازاصالت مشتری را انتخاب کنید. انواعی که پشتیبانی می‌شود عبارتند از:
   - احرازاصالت مبتنی بر گذرواژه
   - احرازاصالت SSL مبتنی بر مشتری و مبتنی بر گذرواژه
   - احرازاصالت SSL مبتنی بر مشتری یا مبتنی بر گذرواژه
   - احرازاصالت
6. در این مرحله محل فایل اجرایی مرورگر وب پیش‌فرضی که قرار است مورد استفاده قرار گیرد را وارد کرده و گزینه Browser Executable را انتخاب کرده و Next کنید.
7. تعیین می‌کنید که از کنسول نصب شده تنها یک کاربر می‌تواند استفاده کند، یا توسط چندین کاربر قابل استفاده است.
8. پیکربندی کنسول به اتمام رسیده است، گزینه Finish را انتخاب کنید.
9. گزینه Done را انتخاب کنید.

پس از خاتمه نصب Shortcut برای اجرای کنسول ایجاد می‌شود (شکل 1)، با دوبار کلیک روی آن به صفحه ورود اطلاعات احرازاصالت وارد می‌شوید (شکل 2).

شکل 1 آیکون اجرای کنسول



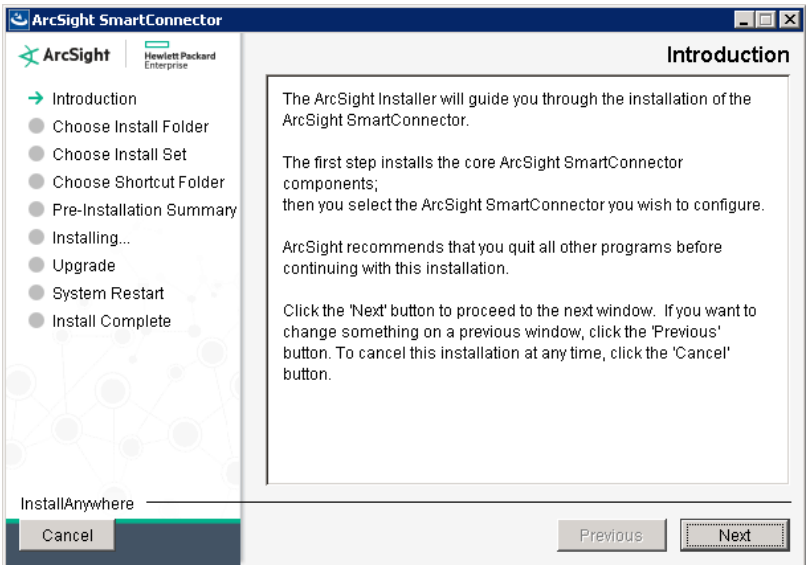
شکل 2 صفحه ورود اطلاعات احرازاصالت

3-2 نصب SmartConnector

SmartConnector را می‌توان روی سیستم‌عامل ویندوز و لینوکس نصب کرد. اما برای نصب باید از نسخه‌های مخصوص همان سیستم‌عامل استفاده کرد. در ادامه SmartConnector نسخه ArcSight-7.2.4.7831.0-Connector-Win را روی سیستم‌عامل ویندوز سرور 2008 نصب می‌کنیم. مراحل نصب SmartConnector روی نسخه‌های دیگر ویندوز نیز به‌همین صورت است، تنها باید از نسخه مناسب SmartConnector برای آن نوع سیستم‌عامل استفاده کرد. متناسب با نوع ارسال‌کننده اطلاعات (حس‌گر) از یک مرحله به بعد تنظیمات ممکن است متفاوت باشد/ در اینجا فرض می‌کنیم SmartConnector قرار است پیغام‌های syslog را دریافت کند. مانند شکل 3 روی فایل نصب SmartConnector کلیک می‌کنیم.

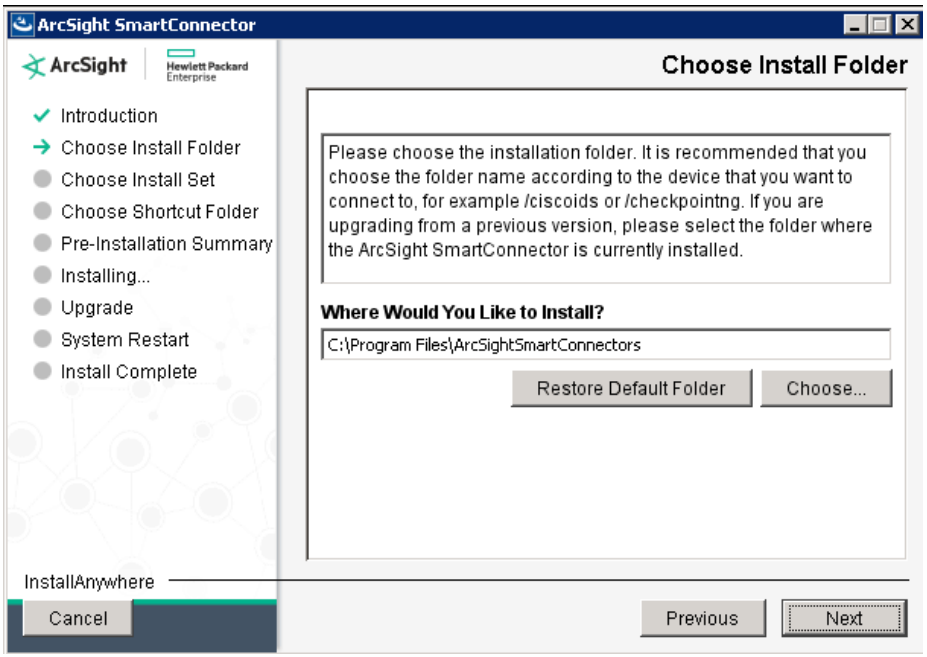
شکل 3 فایل نصب SmartConnector

فایل اجرا شده و صفحه شکل 4 را نمایش می‌دهد، در این صفحه توضیحات اولیه‌ای در مورد مراحل نصب ارائه می‌شود.



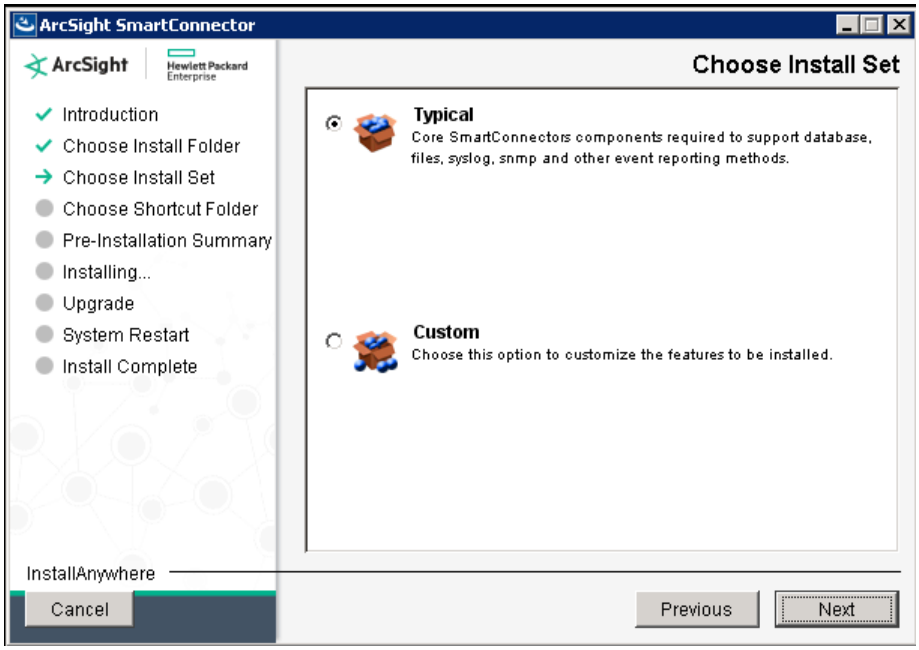
شکل 4 مقدمه‌ای در مورد مراحل نصب

روی گزینه Next کلیک کرده، شکل 5 نمایش داده می‌شود در این صفحه باید مسیر نصب SmartConnector را مشخص کنیم. مسیر مورد نظر را وارد کرده و گزینه Next را انتخاب می‌کنیم.



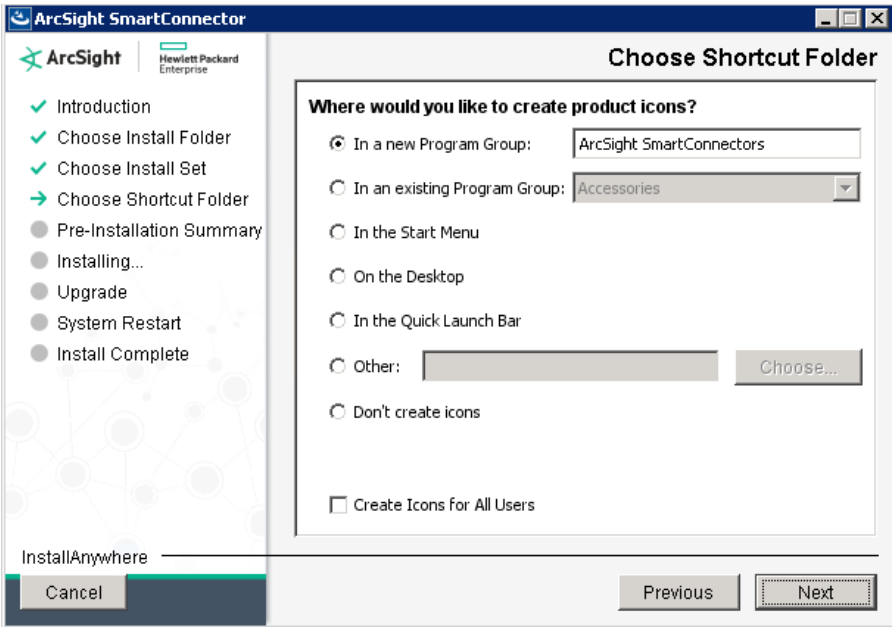
شکل 5 انتخاب محل نصب

صفحه شکل 6 نمایش داده می‌شود.



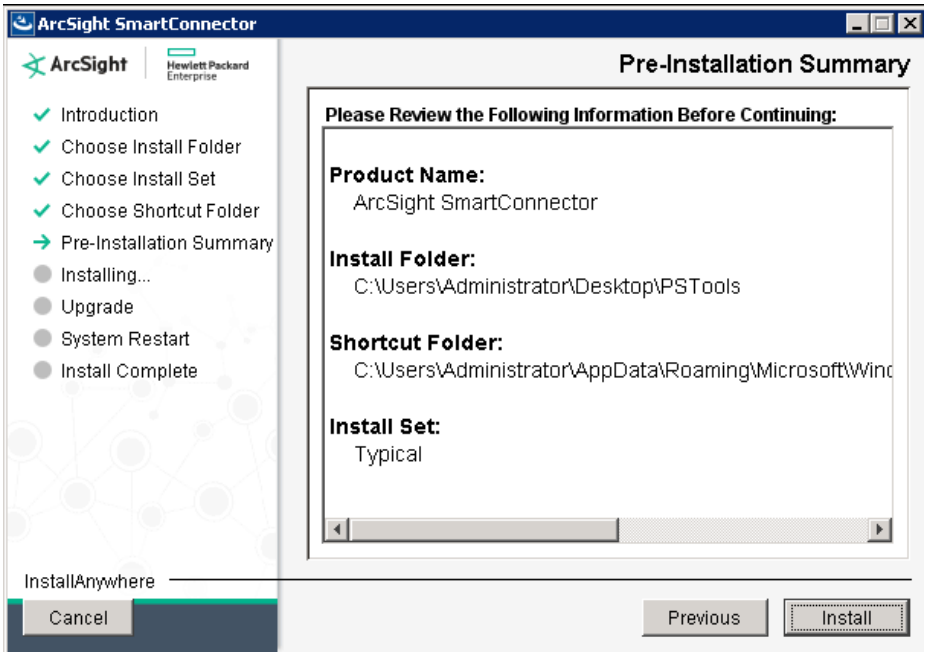
شکل 6 انتخاب نوع نصب

گزینه Typical را انتخاب کرده و Next می‌کنیم. صفحه شکل 7 نمایش داده می‌شود.



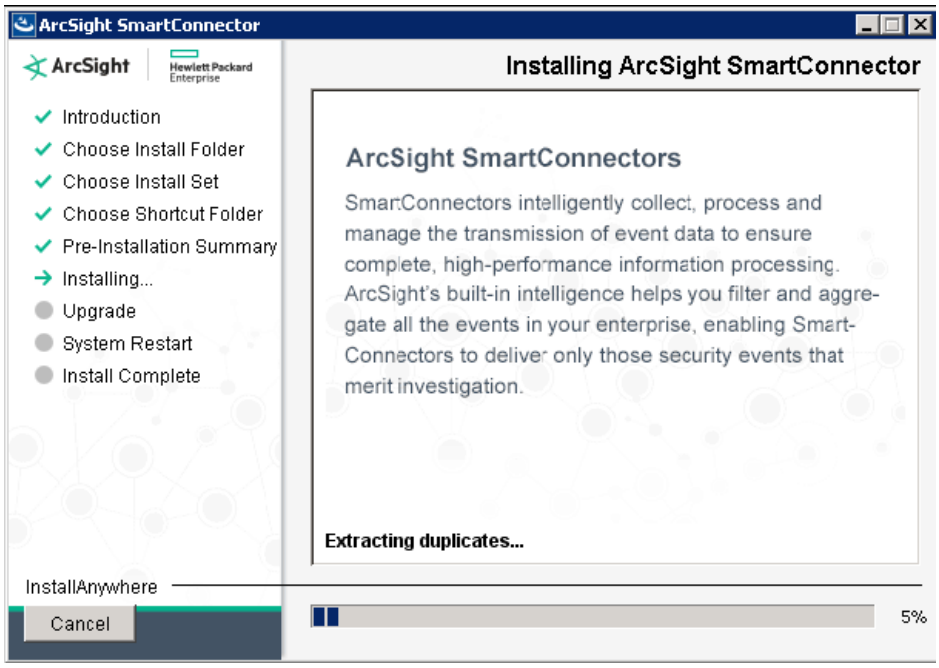
شکل 7 انتخاب محل ایجاد آیکون محصول

محل ایجاد آیکون محصول را تعیین کرده و گزینه Next را انتخاب کرده، شکل 8 نمایش داده می‌شود.



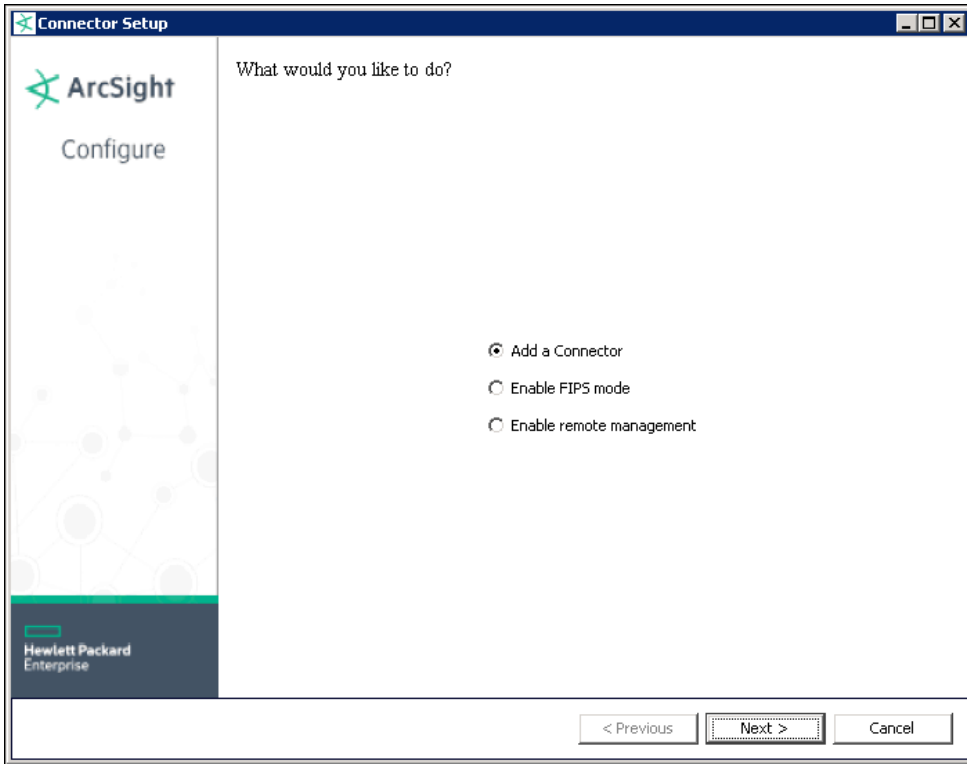
شکل 8 خلاصه‌ای از تنظیمات انجام‌شده

خلاصه‌ای از تنظیمات انتخاب شده را نمایش می‌دهد. درصورت موافقت با تنظیمات انجام‌شده گزینه Install را برای شروع فرآیند نصب انتخاب کرده، در غیراین‌صورت برای تغییر تنظیمات گزینه Previous را زده و تنظیمات قبلی را تغییر داده و پس از رسیدن به این مرحله گزینه Install را انتخاب کنید، مانند شکل 9 فرآیند نصب شروع می‌شود.

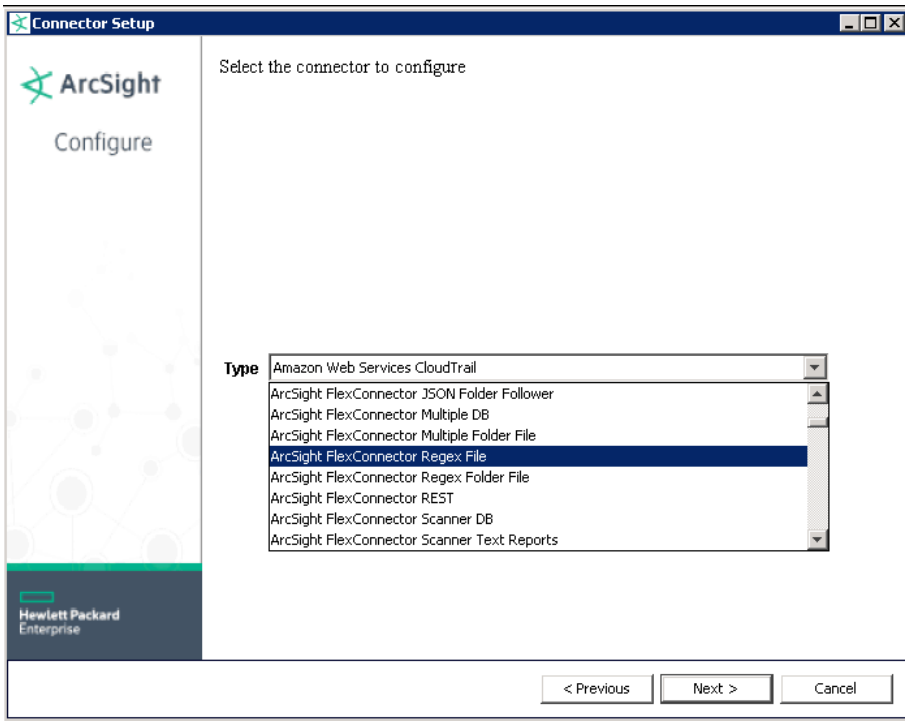


شکل 9 شروع نصب SmartConnector

پس از اتمام نصب، باید نقش SmartConnector را تعیین کنید. گزینه اول "Add a connector"را انتخاب کرده (شکل 10) و Next می‌کنیم. صفحه شکل 11 نمایش داده می‌شود.

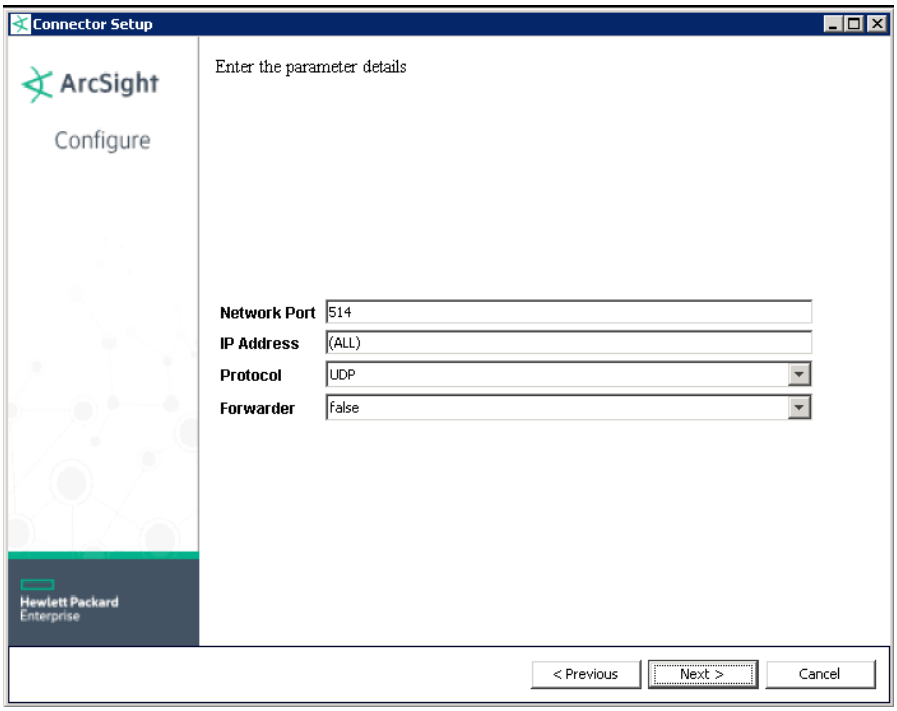


شکل 10 انتخاب نقش SmartConnector



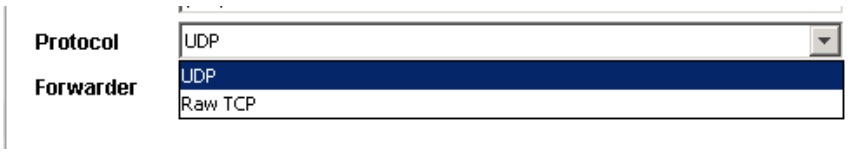
شکل 11 انتخاب نوع ارسال‌کننده داده

در این صفحه باید نوع Connector که قرار است نصب شود تعیین شود. متناسب با ارسال‌کننده هشدارها باید گزینه مناسب انتخاب شود. از این مرحله به بعد تنظیماتی که باید انجام شوند متناسب با نوع ارسال‌کننده هشدار ممکن است متفاوت باشد. پس از انتخاب نوع Connector گزینه Next انتخاب شود، شکل 12 نمایش داده می‌شود.



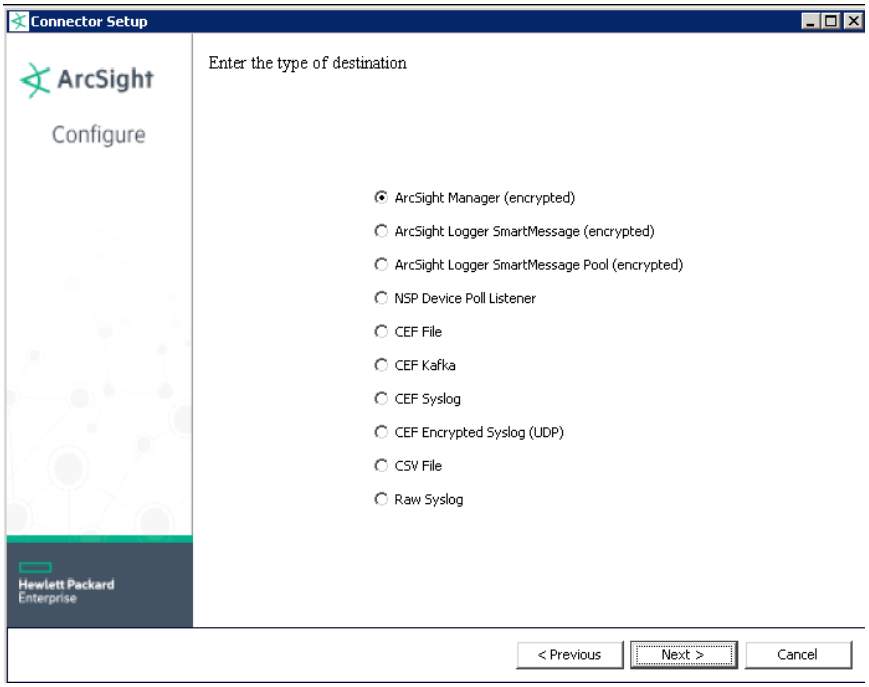
شکل 12 ورود پارامترهای ارتباط

از آنجایی‌که که SmartConnector قرار است پیغام‌های syslog را دریافت کند، شماره درگاه شبکه را 514 وارد کنید. می‌توان آدرس IP کارت شبکه‌ای که قرار است بسته‌ها را دریافت کند را وارد کرد یا این‌که با انتخاب گزینه SmartConnector All از همه کارت‌های شبکه هشدارها را دریافت کرد. برای این‌که قرار است بسته‌های UDP ارسال شوند، نوع پروتکل را UDP انتخاب کنید. همان‌طور که در شکل 13 ملاحظه می‌کنید امکان انتخاب دو نوع پروتکل وجود دارد. Forwarder را false انتخاب کرده (همانطور که در شکل 14 ملاحظه می‌شود دو گزینه true و false وجود دارد) و Next را انتخاب کنید. شکل 15 نمایش داده می‌شود.



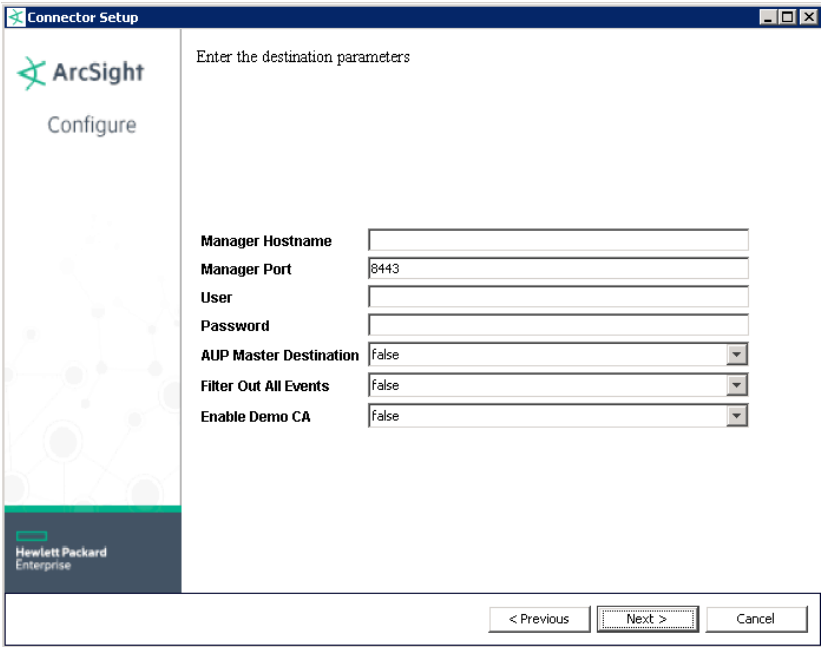
شکل 13 انواع پروتکل قابل پشتیبانی

شکل 14 انواع گزینه‌های Forwarder



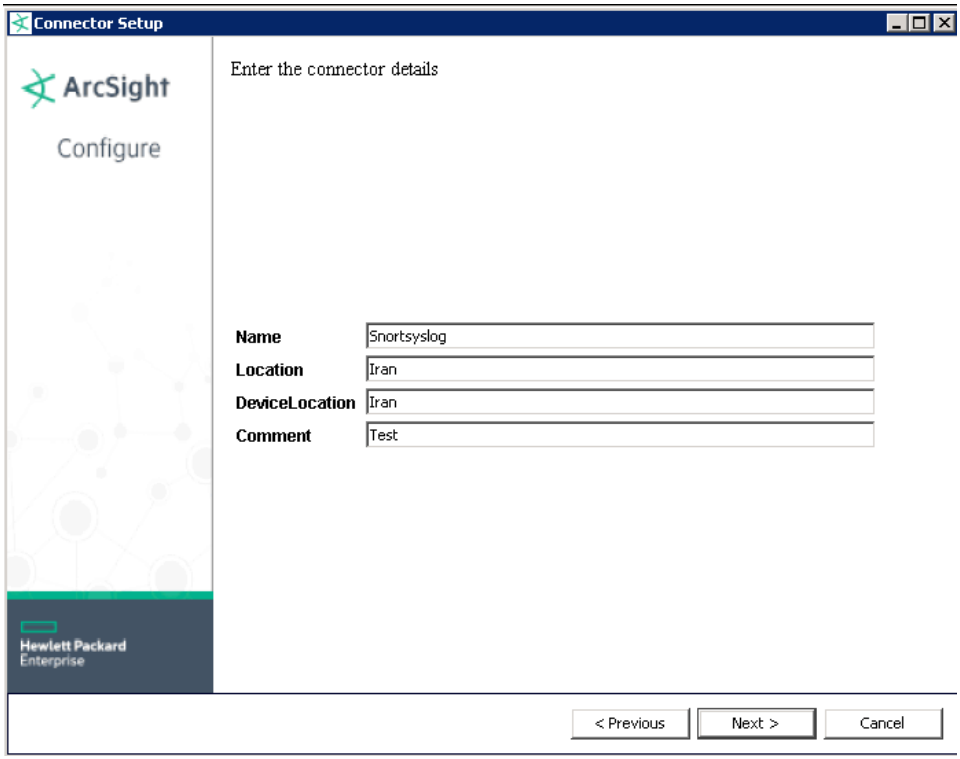
شکل 15 انواع مقصدهای قابل انتخاب

مقصدی که قرار است هشدارها از SmartConnector به آن‌جا ارسال شوند را در شکل 15 باید تعیین کنیم. از آنجایی‌که قرار است هشدارها به Manager ارسال شوند گزینه اول را انتخاب کرده و Next می‌کنیم. شکل 16 نمایش داده می‌شود.



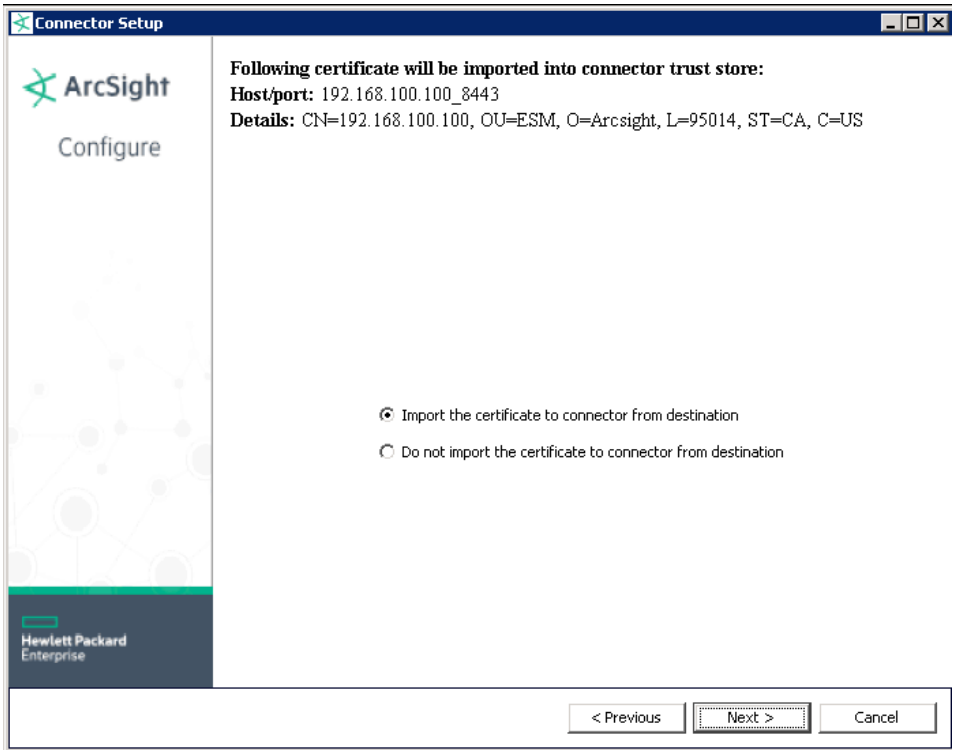
شکل 16 ورود پارامترهای مقصد

در شکل 16 ابتدا باید آدرس IP یا نام manager را وارد کرده، شماره درگاه manager که 8443 است باید حتماً وارد شود. همچنین نام‌کاربری و گذرواژه حساب کاربری که روی manager تعریف‌شده‌است را وارد کنید. ضرورتی ندارد این کاربر روی ESM مدیر باشد. سه گزینه بعدی را نیز False انتخاب کرده و Next می‌کنیم، شکل 17 نمایش داده می‌شود.



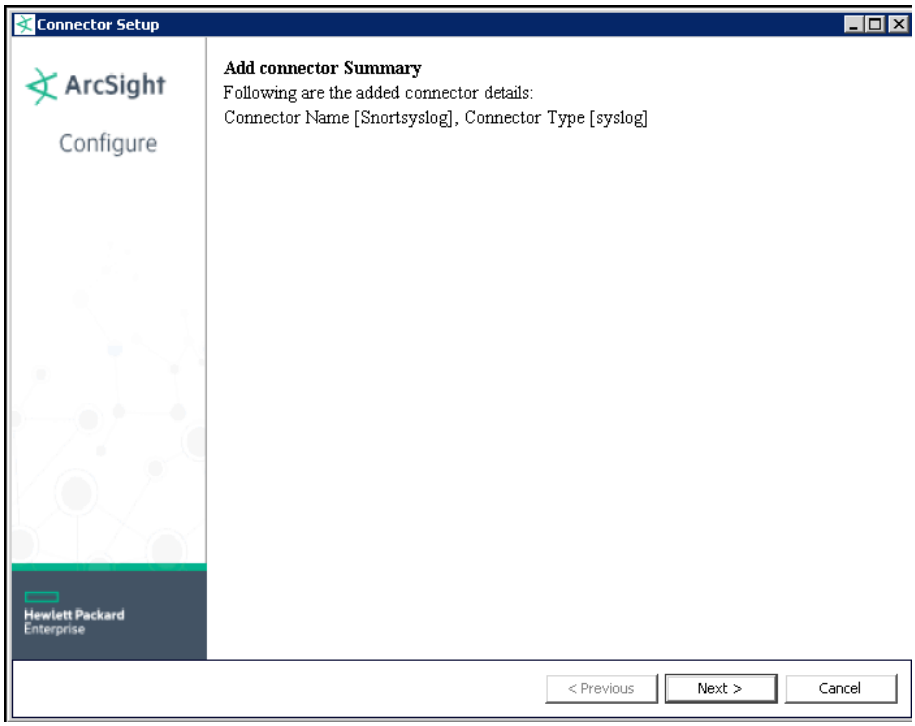
شکل 17 ورود اطلاعات SmartConnector

اطلاعاتی که در این صفحه وارد می‌شود، محل قرارگیری Connector در برگه Resources در بخش Connectors، ESM را مشخص می‌کند. نامی که در بخش Name وارد می‌کنیم، نام Connector را مشخص می‌کند و فولدری همنام با Location در بخش Connectorها در منابع ArcSight ایجاد می‌نماید. هنگامی که نصب SmartConnector کامل شد، با مراجعه به بخش Connectorها، فولدر ایجادشده را می‌بینیم. اطلاعاتی که در دو بخش دیگر وارد می‌شود، بیشتر جنبه توضیحات دارد. گزینه Next را انتخاب می‌کنیم. شکل 18 نمایش داده می‌شود.



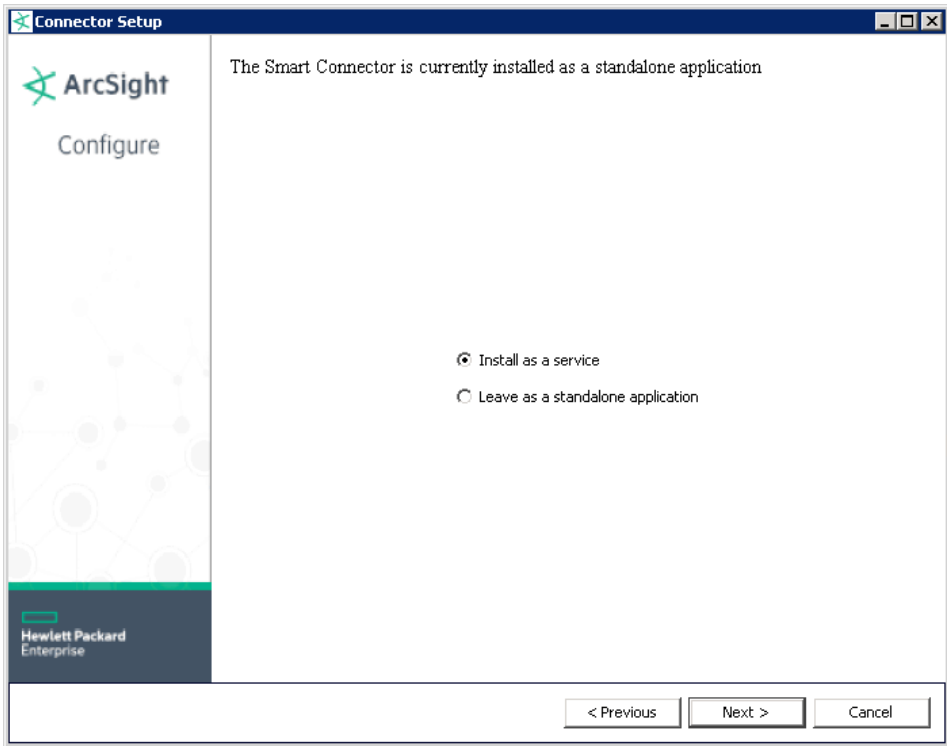
شکل 18 دریافت گواهی‌نامه دیجیتال از مقصد

گزینه اول را انتخاب کرده و Next می‌کنیم. شکل 19 نمایش داده می‌شود.



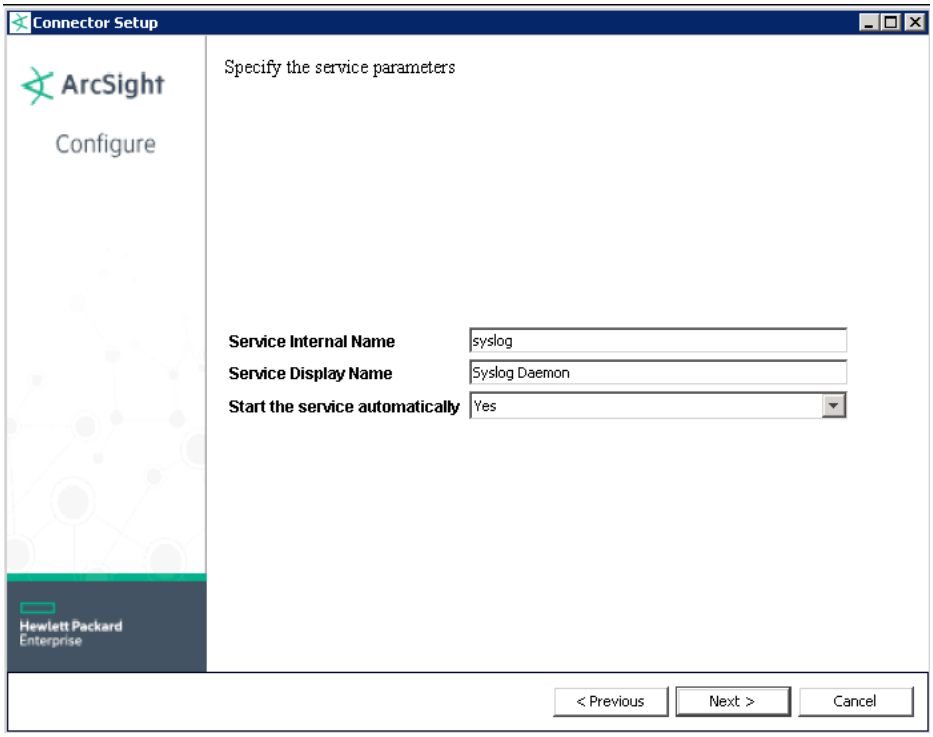
شکل 19 چکیده‌ای از تنظیمات انجام‌شده

چکیده‌ای از تنظیمات نمایش داده می‌شود. گزینه Next را انتخاب می‌کنیم. شکل 20 نشان داده می‌شود.



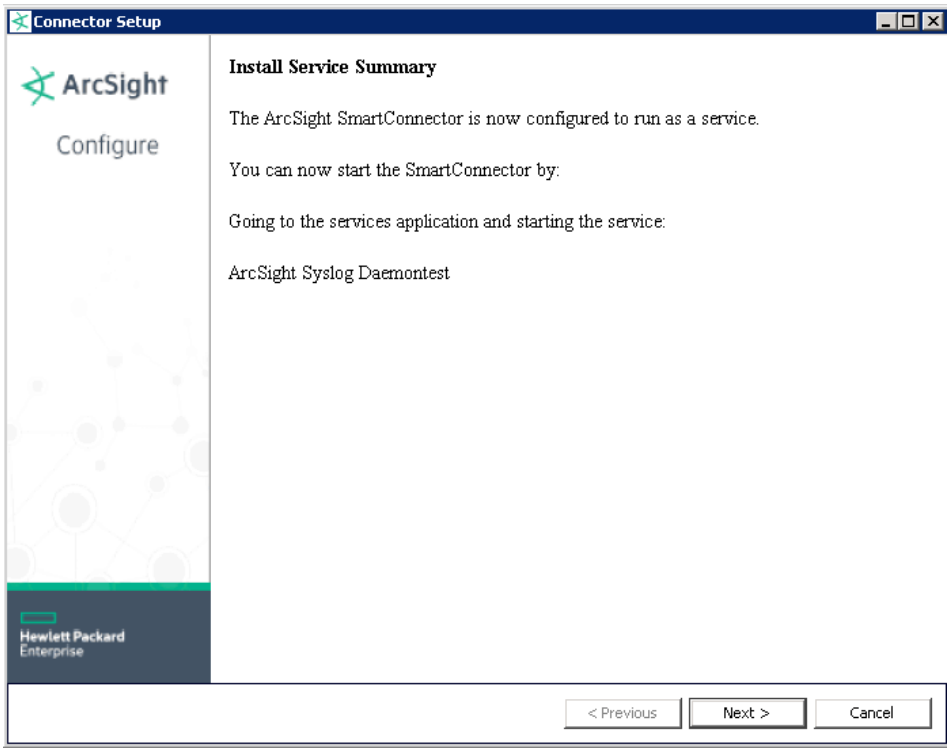
شکل 20 نصب SmartConnector به‌عنوان سرویس

در شکل 20 گزینه اول "Install as a service" را انتخاب کرده (با انتخاب این گزینه، هنگام روشن شدن میزبانی که SmartConnector روی آن نصب شده است، به‌صورت خودکار آماده دریافت هشدارها است، در غیر اینصورت باید به‌صورت دستی آن را اجرا کنیم) و Next می‌کنیم. شکل 21 نمایش داده می‌شود.



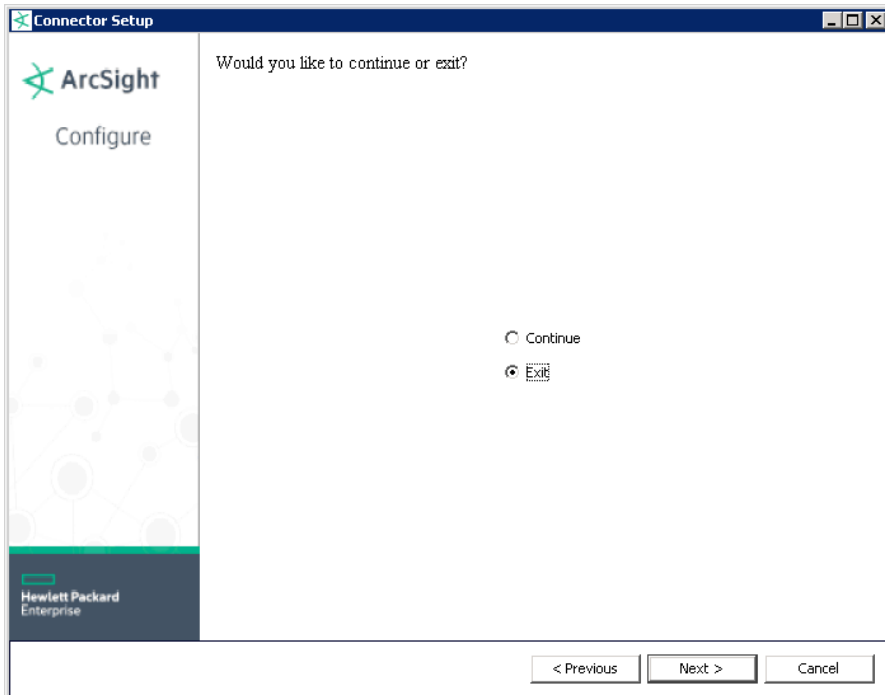
شکل 21 تعیین مشخصات سرویسی که قرار است نصب شود

در این شکل باید نام سرویسی که قرار است نصب شود را تعیین کنیم. نامی که در بخش "Service Display Name" وارد می‌کنید به‌عنوان نام سرویس در نظر گرفته می‌شود. پس از اتمام نصب سرویس را مشاهده می‌کنیم. گزینه بعدی را نیز Yes انتخاب می‌کنیم، Next کرده و به صفحه شکل 22 وارد می‌شویم.



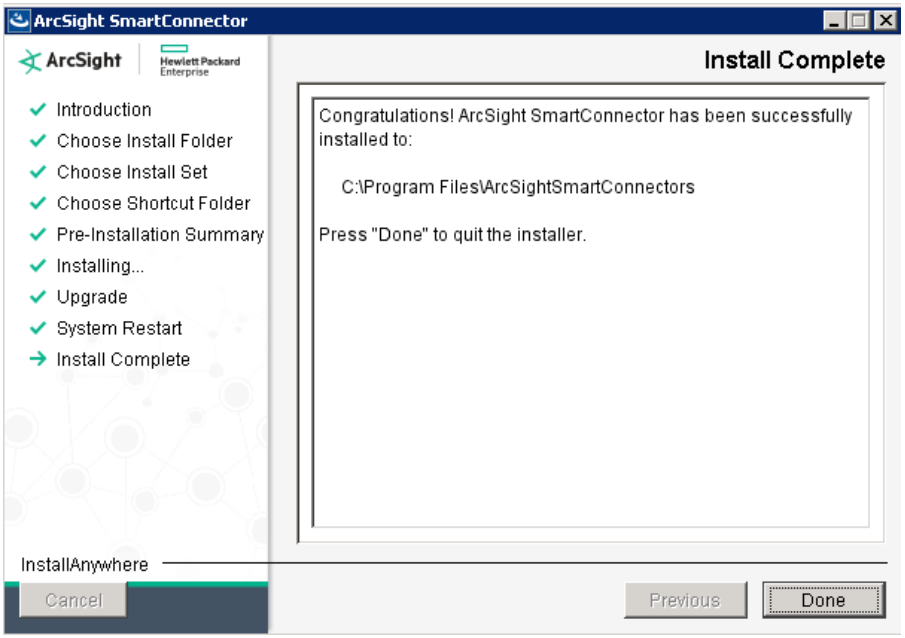
شکل 22 خلاصه‌ای از تنظیمات انجام‌شده برای نصب سرویس

خلاصه‌ای از تنظیمات انجام شده ارائه می‌شود، گزینه Next را انتخاب کرده و به صفحه شکل 23 می‌رویم.



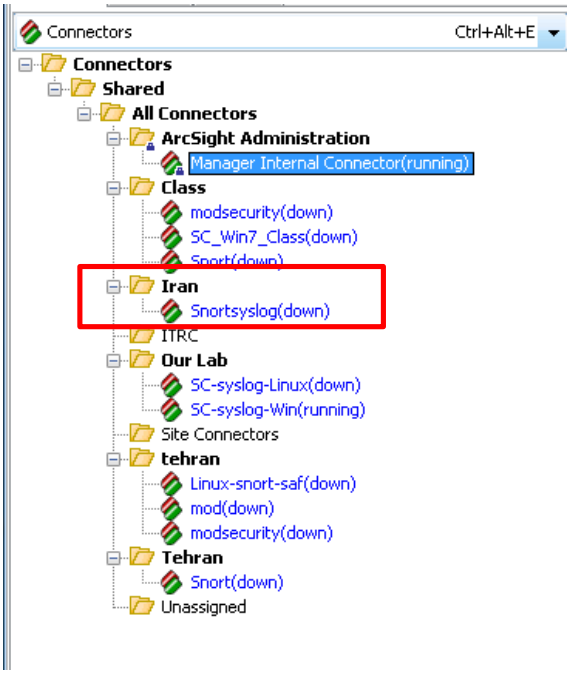
شکل 23 خاتمه نصب یا ادامه برای تغییر تنظیمات

فرآیند نصب در اینجا پایان می‌یابد. در صورتی‌که می‌خواهیم تنظیمات را تغییر دهیم، گزینه Continue و در غیر این‌صورت گزینه Exit را انتخاب می‌کنیم. گزینه Exit را انتخاب کرده و Next می‌کنیم، صفحه شکل 24 نمایش داده می‌شود.



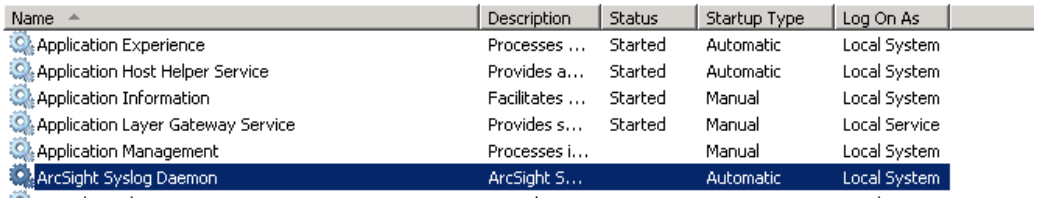
شکل 24 خاتمه موفقیت‌آمیز نصب

نصب با موفقیت انجام شده‌است، گزینه Done را زده و به فرآیند نصب خاتمه می‌دهیم. به بخش Connectors رفته و همان‌طور که در شکل 25 ملاحظه می‌کنید فولدر Iran به بخش All Connectors اضافه شده است و در آن Connector نصب شده، با همان نام Snortsyslog، اضافه شده است.



شکل 25 اضافه شدن SmartConnector به فولدر Iran

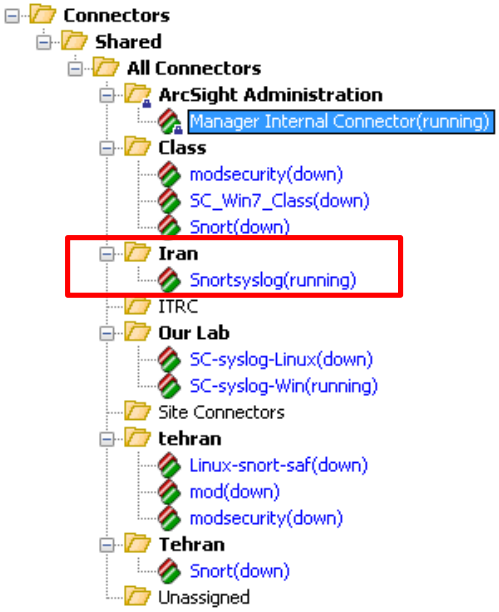
به بخش Services در ویندوز رفته و همان‌طور که در شکل 26 ملاحظه می‌کنید سرویس Syslog ArcSight Deamon اضافه شده است. همان نامی که در شکل 21 قبل از این تعیین کردیم.



Name	Description	Status	Startup Type	Log On As
Application Experience	Processes ...	Started	Automatic	Local System
Application Host Helper Service	Provides a...	Started	Automatic	Local System
Application Information	Facilitates ...	Started	Manual	Local System
Application Layer Gateway Service	Provides s...	Started	Manual	Local Service
Application Management	Processes i...		Manual	Local System
ArcSight Syslog Daemon	ArcSight S...		Automatic	Local System

شکل 26 سرویس SmartConnector که به بخش Services افزوده شده است

همان‌طور که در شکل 26 ملاحظه می‌شود، وضعیت SmartConnector Down گزارش شده است. برای فعال‌سازی آن روی سرویس راست‌کلیک کرده و Start را انتخاب می‌کنیم. اولین بار پس از نصب SmartConnector باید این کار به صورت دستی انجام شود. مجدداً به بخش Connectors در شکل 25 رفته و همان‌طور که در شکل 27 ملاحظه می‌کنید، وضعیت SmartConnector، Snortsyslog به running تغییر پیدا کرده است. از این پس هشدارهای دریافتی توسط SmartConnector به سمت ArcSight Express ارسال می‌شوند.



شکل 27 فعال شدن SmartConnector

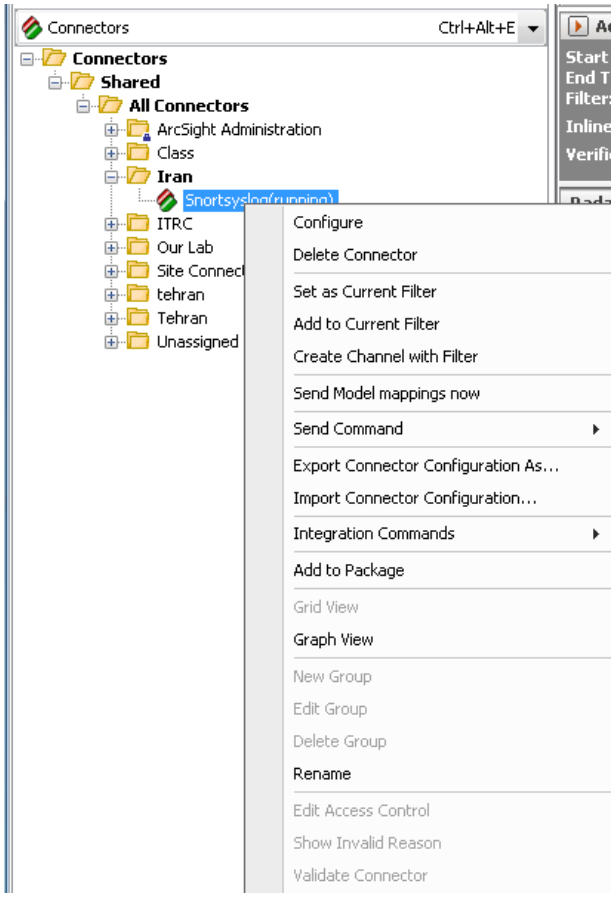
در ادامه قرار است در قالب یک سناریوی عملی قابلیت‌های محصول معرفی شود.

3 معرفی قابلیت‌های محصول

پیش از این‌که قابلیت‌های محصول را در قالب یک سناریو ببنیم، ضروری است با اصطلاحات و مفاهیمی آشنا شویم. این اصطلاحات در ادامه فهرست شده‌اند.

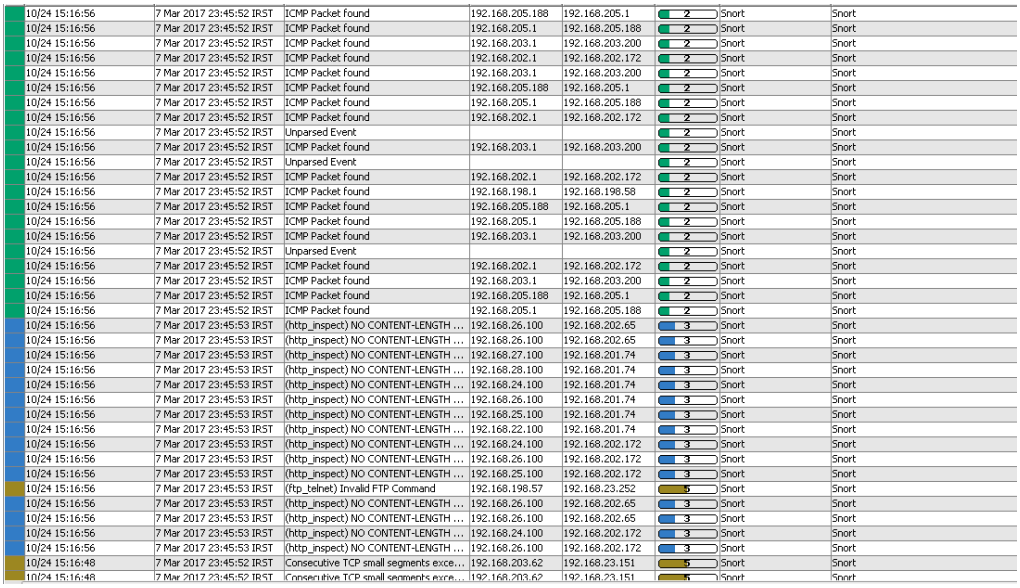
- Active Channels

همانطور که در بخش 3-1-2 عنوان شد، تعریف یک Active Channel شامل تعیین ویژگی‌هایی است که می‌خواهیم رویدادهایی که قرار است مشاهده کنیم داشته باشند. برای تعریف یک Active Channel می‌توان بر حسب نیاز و در سناریوهای مختلف عمل کرد. به عنوان مثال اگر بخواهیم هشدارهای ارسالی از یک Connector خاص را مشاهده کنیم، در بخش Navigator به برگه Resources رفته و از منو گزینه Connectors را انتخاب می‌کنیم. روی Connector که قرار است هشدارهای آن را مشاهده کنیم راست‌کلیک کرده (شکل 28) گزینه Create Channel with Filter را انتخاب می‌کنیم.



شکل 28 گزینه‌های مختلف مربوط به SmartConnector

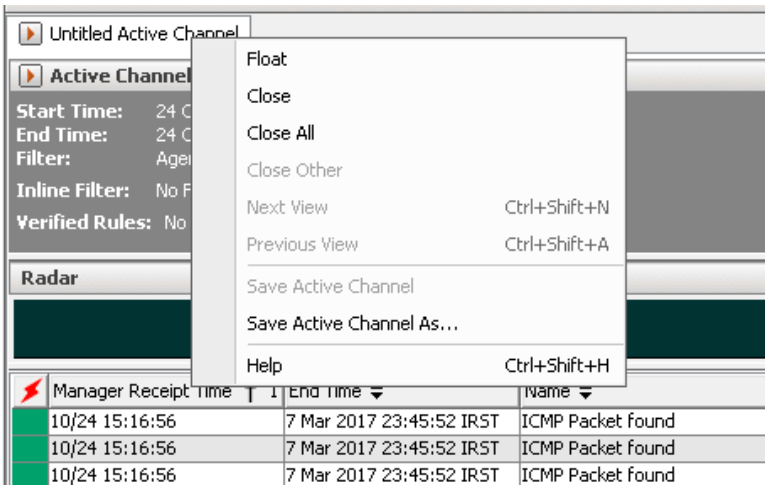
در بخش Viewer، هشدارهایی که شامل ویژگی‌ها و شرایط آن Active Channel هستند، نمایش داده می‌شوند. این هشدارها در شکل 29 نمایش داده شده است.



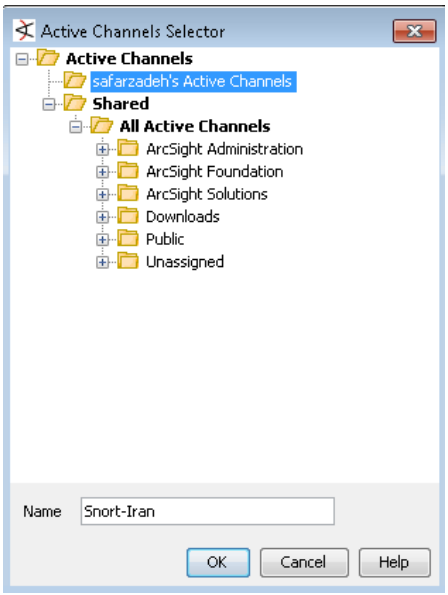
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.205.188	192.168.205.1	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.205.1	192.168.205.188	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.203.1	192.168.203.200	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.202.1	192.168.202.172	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.203.1	192.168.203.200	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.205.188	192.168.205.1	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.205.1	192.168.205.188	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.202.1	192.168.202.172	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	Unparsed Event			2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.203.1	192.168.203.200	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	Unparsed Event			2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.202.1	192.168.202.172	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.198.1	192.168.198.58	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.205.188	192.168.205.1	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.205.1	192.168.205.188	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.203.1	192.168.203.200	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	Unparsed Event			2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.202.1	192.168.202.172	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.203.1	192.168.203.200	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.205.188	192.168.205.1	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.205.1	192.168.205.188	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.26.100	192.168.202.65	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.26.100	192.168.202.65	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.27.100	192.168.201.74	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.28.100	192.168.201.74	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.24.100	192.168.201.74	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.26.100	192.168.201.74	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.25.100	192.168.201.74	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.22.100	192.168.201.74	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.24.100	192.168.202.172	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.26.100	192.168.202.172	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.25.100	192.168.202.172	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(ftp_telnet) Invalid FTP Command	192.168.198.57	192.168.23.252	5	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.26.100	192.168.202.65	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.26.100	192.168.202.65	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.24.100	192.168.202.172	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.26.100	192.168.202.172	3	Snort	Snort
10/24 15:16:48	7 Mar 2017 23:45:52 IRST	Consecutive TCP small segments exce...	192.168.203.62	192.168.23.151	5	Snort	Snort
10/24 15:16:48	7 Mar 2017 23:45:52 IRST	Consecutive TCP small segments exce...	192.168.203.62	192.168.23.151	5	Snort	Snort

شکل 29 هشدارهای استخراج‌شده بر اثر انتخاب یک Connector

این Active Channel بدون عنوان است. به‌منظور این‌که برای مراجعات بعدی نام مشخصی به آن تخصیص دهیم و آن را به‌عنوان یک Active Channel در بخش Active Channelهای برگه منابع ذخیره کنیم، روی عنوان آن مطابق با شکل 30 راست‌کلیک کرده و گزینه Save Active Channel As را انتخاب می‌کنیم. شکل 31 نمایش داده می‌شود.

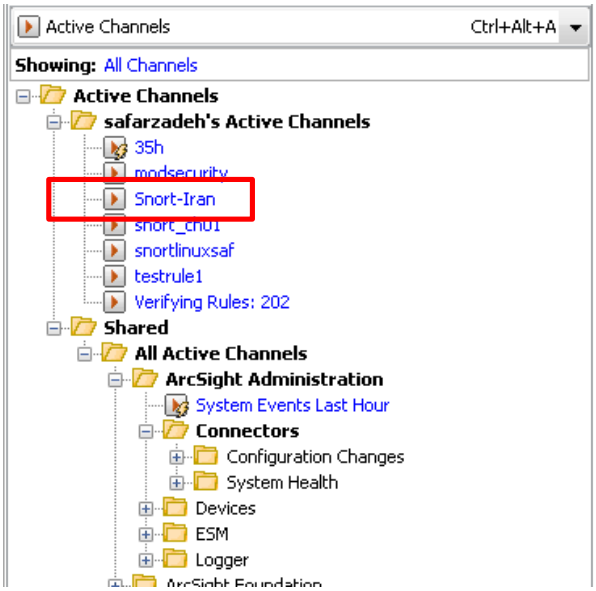


شکل 30 ذخیره کانال فعال



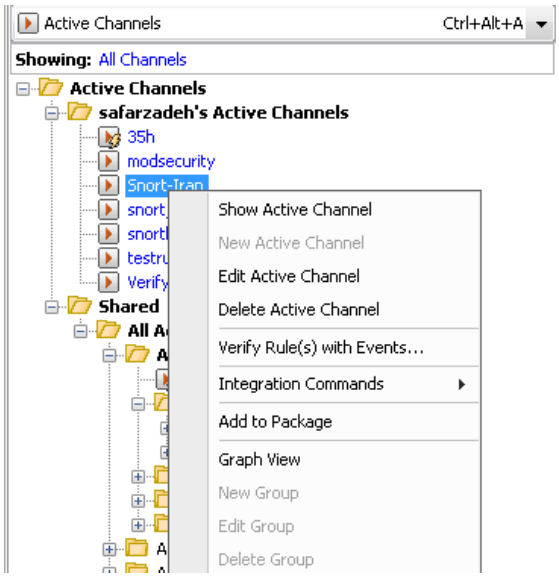
شکل 31 نام‌گذاری کانال فعال

با انتخاب فولدری که می‌خواهیم Active Channel در آن ایجاد شود، در بخش Name نامی را به آن تخصیص داده و گزینه OK را انتخاب می‌کنیم. مانند شکل 32 به بخش Active Channel در برگه منابع مراجعه کرده و کانال فعالی که اضافه شده است را ملاحظه می‌کنیم.



شکل 32 نمایش کانال فعال ایجادشده

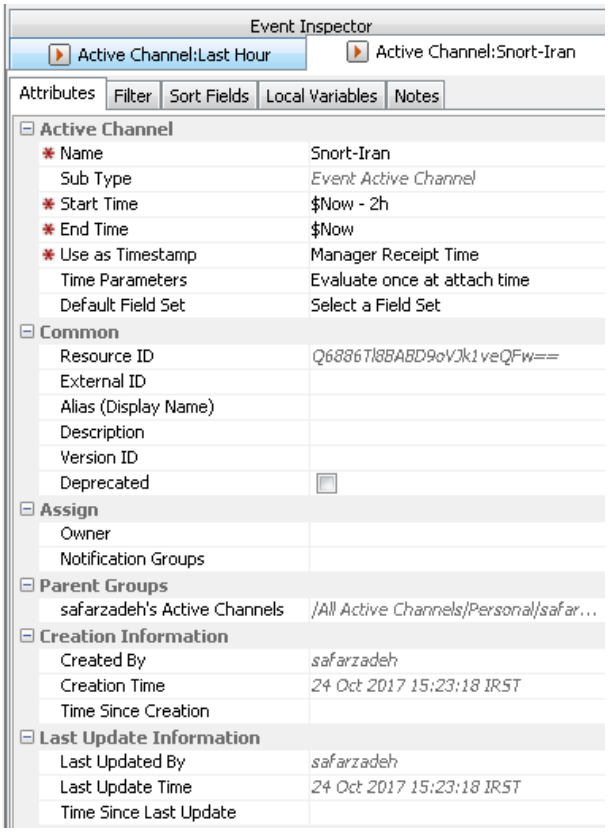
از این به بعد برای مشاهده رویدادهای این کانال فعال، با مراجعه به بخش کانال‌های فعال در برگه منابع، روی آن راست‌کلیک کرده و گزینه Show Active Channel را انتخاب کنید (شکل 33).



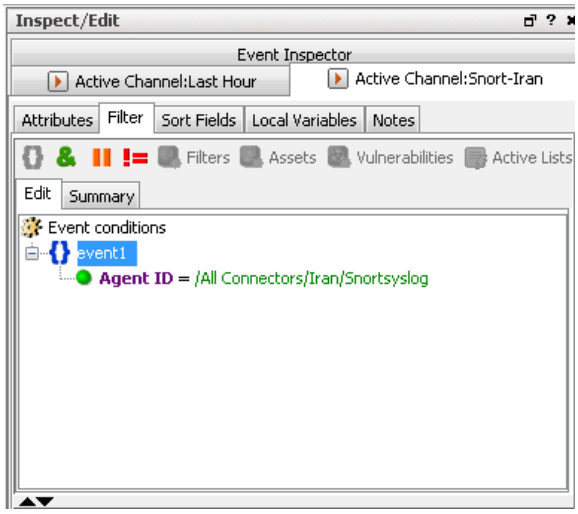
شکل 33 انتخاب گزینه نمایش پارامترهای پیکربندی

هر کانال فعال هشدارهایی که دارای ویژگی‌های تعیین شده هستند را در بخش Viewer نمایش می‌دهد. برای مشاهده یا تغییر این ویژگی‌ها روی کانال فعال راست‌کلیک کرده و گزینه Edit Active Channel را انتخاب کنید (شکل 33). همان‌طور که در شکل 34 مشخص شده است، در برگه Attributes نام کانال فعال قابل تغییر است. هر کانال فعال رویدادهای یک پنجره زمانی مشخص را استخراج کرده و نمایش می‌دهد. این پنجره

زمانی توسط دو فیلد Start Time و End Time مشخص می‌شود. عبارت $Now – 2h به معنی 2 ساعت پیش تا همین لحظه است. و هشدارهایی که از دو ساعت پیش تا همین لحظه دریافت شده‌اند را نمایش می‌دهد. علاوه بر تعیین پنجره زمانی برای نمایش رویدادها از جمله ویژگی‌های دیگر نام رویداد، نام محصول تولیدکننده هشدار و موارد دیگر است. این موارد در برگه Filter تعیین می‌شوند. آن را انتخاب کرده، به صفحه شکل 35 می‌رویم.

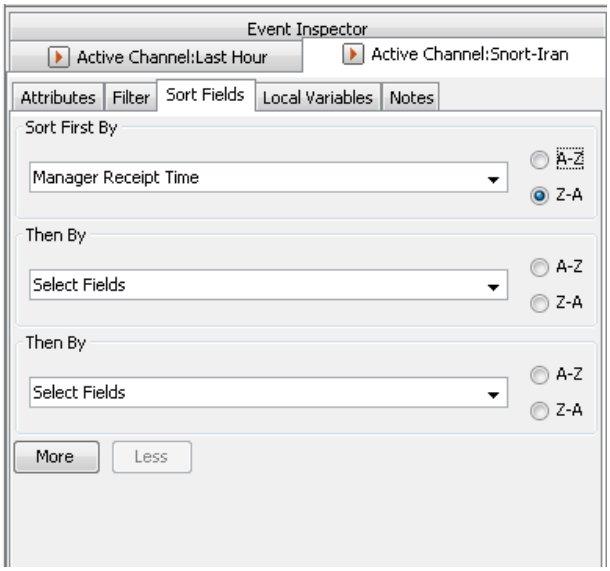


شکل 34 ورود نام و انجام تنظیمات پنجره زمانی



شکل 35 نمایش پارامترهای قابل تنظیم برگه Filter

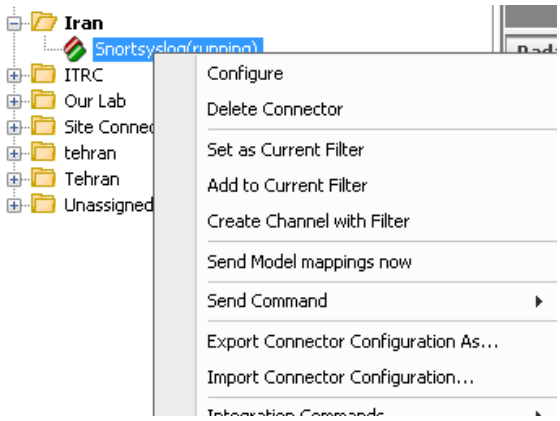
در این برگه مشخصات ارسال‌کننده رویداد تعیین می‌شود. همان‌طور که ملاحظه می‌کنید، از آنجایی‌که کانال فعال را با راست‌کلیک روی Connector در برگه Connectors ایجاد کردیم، به‌عنوان Filter مسیر Connector را در نظر گرفته است. می‌توانید برای استخراج هشدارهای دیگر انواع Filterها را تعریف کنید. برگه Sort Fields را انتخاب می‌کنیم، شکل 36 نمایش داده می‌شود.



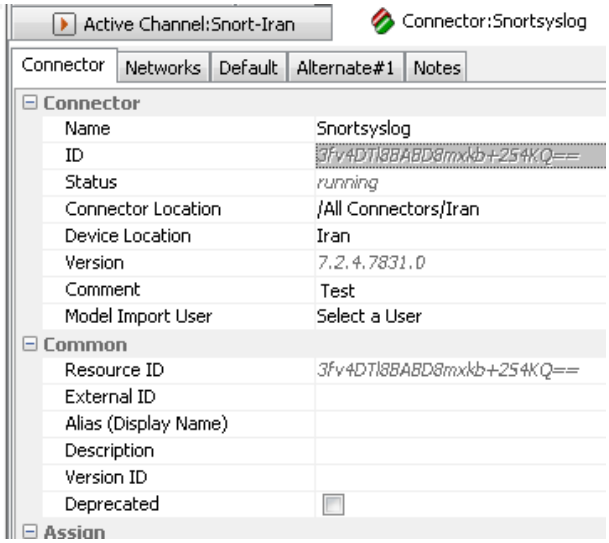
شکل 36 تنظیم پارامترهای برگه Sort Fields

در این برگه تعیین می‌کنیم که رویدادهایی که استخراج می‌شوند براساس کدام فیلد مرتب‌شده و سپس نمایش داده شوند. مقدار پیش‌فرض بر اساس زمان دریافت توسط Manager است. می‌توانید مرتب‌سازی را بر اساس فیلدهای دیگر نیز انجام دهید.

روش دیگر برای تعریف کانال فعال به این صورت است روی Connectorی که می‌خواهید رویدادهای آن را استخراج کنید، راست‌کلیک کرده و گزینه Configure را انتخاب کنید (شکل 37). با مراجعه به برگه Connector در بخش Inspect/Edit، روی ID راست‌کلیک کرده و گزینه کپی را انتخاب کنید، تا ID مربوط به Connector کپی شود (شکل 38).

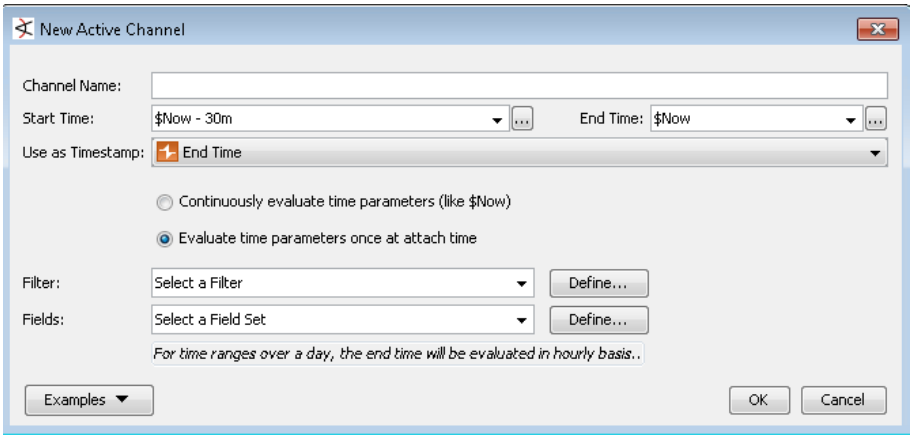


شکل 37 نمایش پارامترهای قابل تنظیم SmartConnector

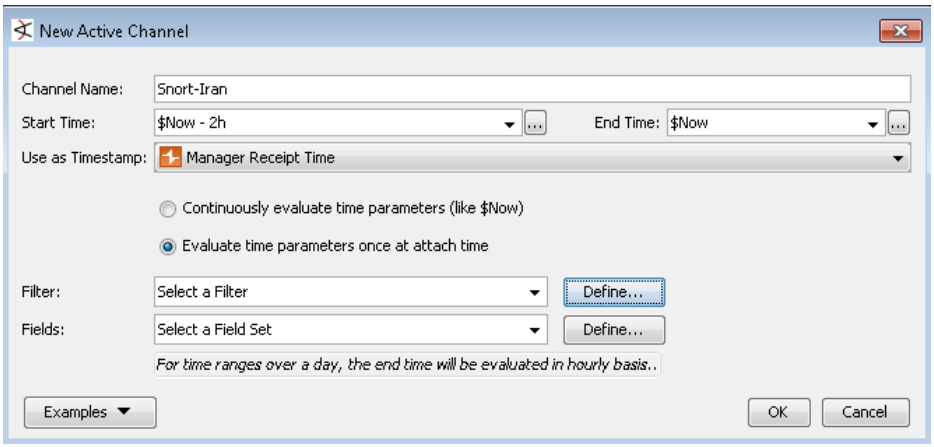


شکل 38 پارامترهای قابل تنظیم SmartConnector برگه Connector

سپس به برگه منابع مراجعه کرده و Active Channels را انتخاب کنید. روی فولدری که قرار است Active Channel جدید در آن ایجاد شود راست‌کلیک کرده و گزینه New Active Channel را انتخاب کنید. صفحه شکل 39 نمایش داده می‌شود. نامی را در بخش Channel Name وارد کرده و پنجره زمانی را با استفاده از فیلدهای Start Time و End Time تعیین کنید. در بخش Use as Timestamp گزینه Manager Reciept Time را انتخاب کنید (40).

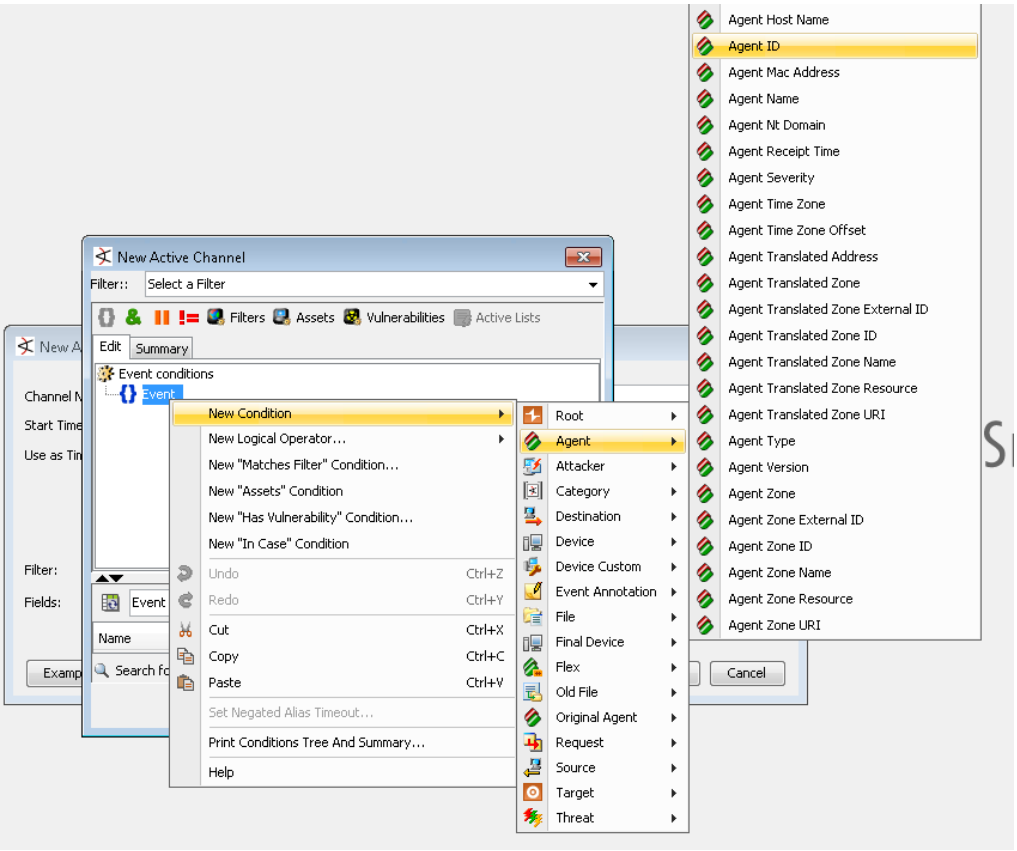


شکل 39 تنظیمات کانال فعال



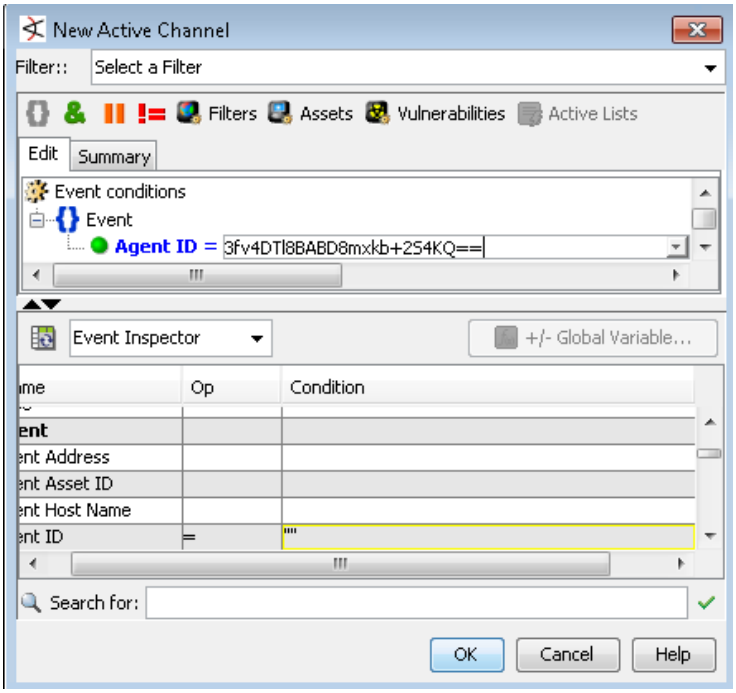
شکل 40 ورود تنظیمات کانال فعال

سپس برای تعیین فیلتر روی Define کلیک کرده و روی New Condition کلیک کنید. سپس گزینه Agent و در ادامه گزینه Agent ID را انتخاب کنید. همان‌طور که ملاحظه می‌شود، می‌توان گزینه‌های متنوع و زیادی را به‌عنوان شرایط انتخاب کرد. صفحه شکل 41 نمایش داده می‌شود.



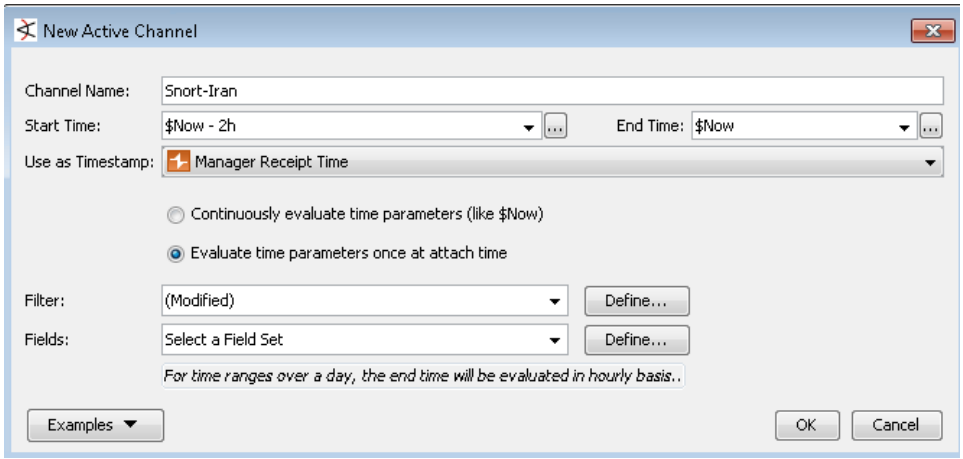
شکل 41 انتخاب شرایط نمایش هشدارها در کانال فعال

در پنجره مقابل عبارت Agent ID راست‌کلیک کرده و گزینه چسباندن را انتخاب کنید. مقدار Connector ID به آن اضافه می‌شود (شکل 42).



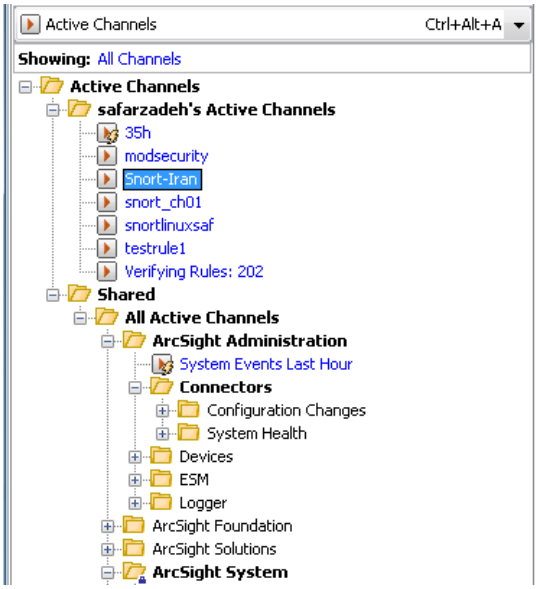
شکل 42 ورود Agent ID مربوط به Connector

گزینه OK را انتخاب کنید. شکل 43 نمایش داده می‌شود.



شکل 43 تکمیل مشخصات کانال فعال

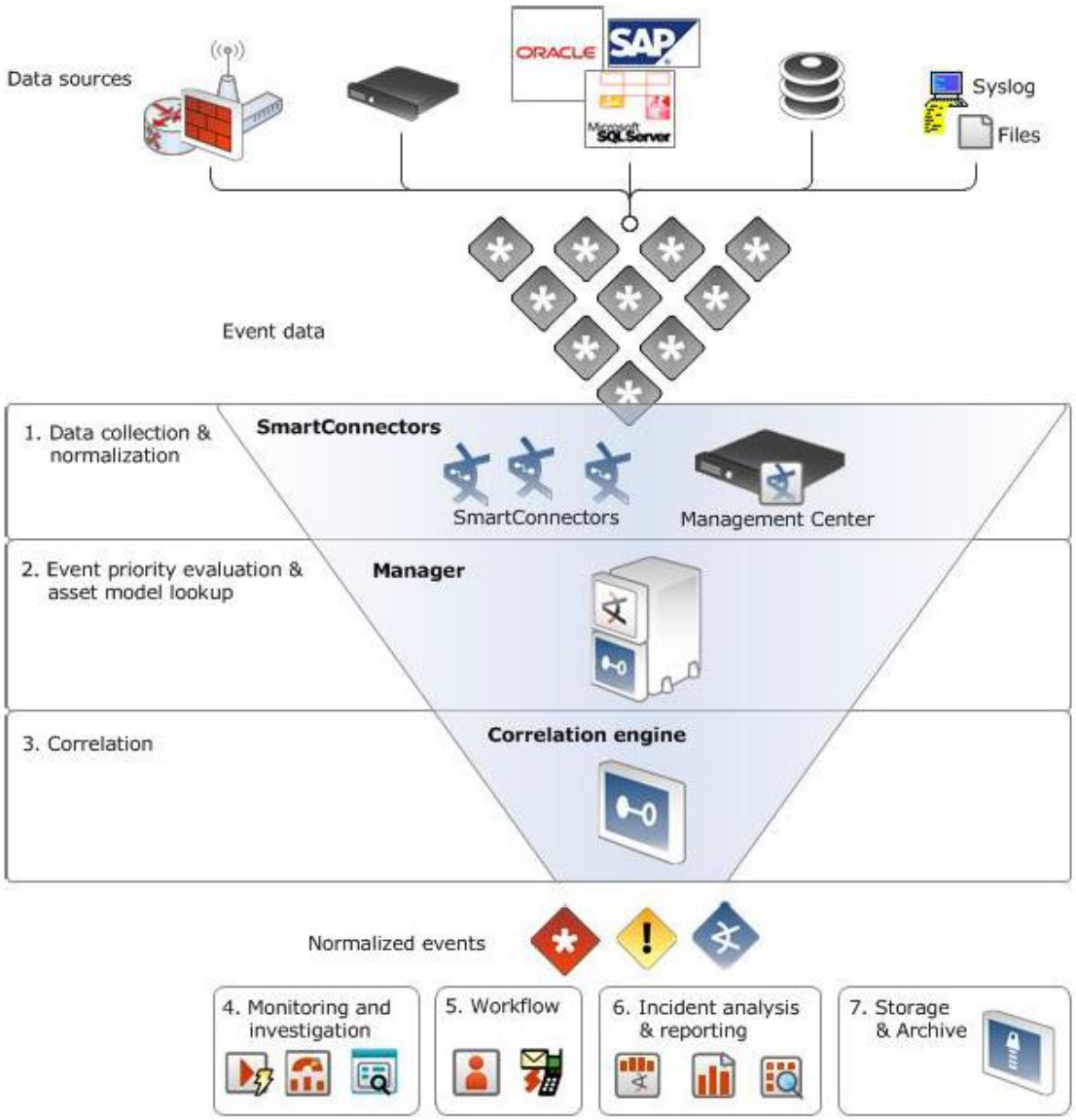
گزینه OK را برای ثبت تغییرات کلیک کنید. همان‌طور که در شکل 44 نمایش داده شده است، کانال فعال جدید افزوده شده است.



شکل 44 افزوده‌شدن کانال فعال به فهرست کانال‌های فعال

1-3 سناریوی مورد استفاده برای بیان قابلیت‌ها

همان‌طور که در شکل 45 نمایش داده شده است، انواع ورودی‌ها از حس‌گرهای مختلف به سمت SmartConnectorها ارسال می‌شوند. در SmartConnector در صورت اعمال تنظیمات، با تجمیع هشدارها آن‌ها را کاهش داده، و تنها هشدارهای مد نظر سیاست‌های امنیتی سازمان و مهم را به سمت ESM ارسال می‌کند. SmartConnector هشدارها را نرمال‌سازی کرده و به سمت ESM ارسال می‌کند. ESM آن‌ها را به Manager تحویل می‌دهد. Manager تحلیل‌ها و همبسته‌سازی را انجام می‌دهد و نتایج تحلیل و گزارش‌ها در کنسول ارائه می‌شوند.

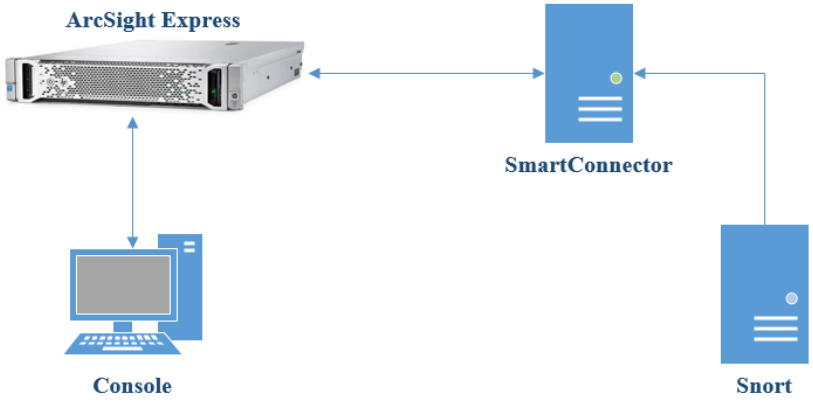


شکل 45 چرخه حیات یک رویداد

از آنجایی‌که آناتومی محصول این چنین است، سناریوی آموزشی نیز به‌همین ترتیب آماده شده است. سناریو انجام کار در گام‌های زیر بیان شده است:

1. نصب SmartConnector و اتصال SmartConnector به ArcSightExpress
2. انجام حمله و ارسال هشدارها از حس‌گر به سمت SmartConnector
3. دریافت هشدارها توسط SmartConnector و ارسال آن‌ها به سمت ESM
4. نوشتن قوانین همبسته‌سازی و تجمیع برای شناسایی حملات
5. مشاهده نتایج

نقشه شبکه‌ای که سناریو در آن اجرا شده است در شکل 46 نمایش داده شده است.



شکل 46 نقشه شبکه آزمون

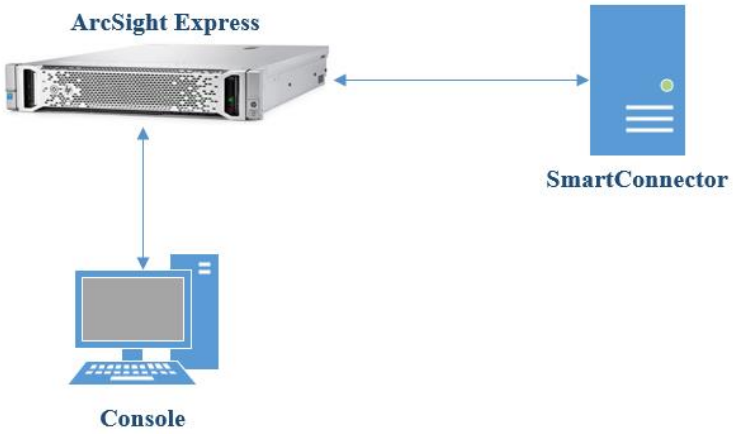
در این شبکه، همان‌طور که در شکل 46 مشاهده می‌شود، از سیستم‌های جدول 1 استفاده شده است.

جدول 1 مشخصات سیستم‌های مورد استفاده در سناریوها

نام سیستم	نقش	مشخصات
Snort	حس‌گر	نسخه اسنورت که روی یک ماشین مجازی نصب شده است
SmartConnector	جمع‌آوری کننده، نرمال‌ساز	نسخه ArcSight-7.2.4.7831.0-Connector-Win که روی ماشین مجازی با سیستم‌عامل ویندوز سرور 2008
ArcSight Express	تحلیل‌گر	نسخه ESM 6.9.1 روی Appliance نصب شده است
Console		نسخه 6.9.1 روی Appliance

3-1-1 نصب SmartConnector و اتصال SmartConnector به ArcSightExpress

مراحل نصب به‌صورت کامل در بخش 3-5 آورده شده است. SmartConnector نسخه ArcSight-7.2.4.7831.0-Connector-Win روی ویندوز سرور 2008 نصب شد، آن را به ArcSight Express متصل کردیم و در کنسول مشاهده کردیم وضعیت آن به running تغییر کرد. مسیر ارتباطی میان مؤلفه‌ها در شکل 47 به تصویر کشیده شده است.



شکل 47 نقشه شبکه آزمون

3-1-2 انجام حمله و ارسال هشدارها از حس‌گر به سمت SmartConnector

به‌عنوان حمله، مجموعه داده "ok-maccdc2011_00004_20110311221544.pcap" که شامل ترافیک حمله است را توسط سیستم تشخیص نفوذ اسنورت می‌خوانیم. این امر منجر به تولید هشدار شده، و با انجام تنظیمات این هشدارها را به سمت SmartConnector ارسال می‌کنیم. سپس به کنسول مراجعه کرده و دریافت هشدارها را تحقیق می‌کنیم.

1. انجام تنظیمات روی Snort برای ارسال هشدارها به سمت SmartConnector

برای ارسال هشدارهای اسنورت به سمت یک syslog server باید تنظیمات زیر انجام شوند. ابتدا برای اسنورت تعیین می‌کنیم هشدارها را به local5 بفرستد. به مسیر نصب اسنورت و محل قرارگیری فایل Snort.conf رفته و فایل پیکربندی را در بخش مربوط به خروجی، مطابق با شکل 48 تغییر دهید.

```
##################################################
# Step #6: Configure output plugins
# For more information, see Snort Manual, Configuring Snort - Output Modules
##################################################
# syslog
output alert_fast: snort.fast
output alert_syslog: LOG_LOCAL5 LOG_ALERT
```

شکل 48 تغییر فایل پیکربندی Snort برای نمایش هشدارها در قالب متنی

سپس در فایل /etc/rsyslog.conf دستور شکل 49 را وارد کنید. بعد از @ آدرس SmartConnector IP را وارد کنید.

```
#$AddUnixListenSocket /var/snort/de
local5.alert @10.1.223.31:514
#local3.debug /var/log/snort_debug
```

شکل 49 تغییر فایل پیکربندی Rsyslog

با استفاده از دستورات شکل‌های 50 و 51 به‌ترتیب سرویس اسنورت و rsyslog را دوباره راه‌اندازی کنید، تا تغییرات اعمال شوند.

```
root@ubuntu:~/Desktop# service snortd restart
```

شکل 50 راه‌اندازی مجدد سرویس اسنورت برای اعمال تنظیمات

```
root@ubuntu:/proc# service rsyslog restart
```

شکل 51 راه‌اندازی مجدد سرویس rsyslog برای اعمال تنظیمات

2. خواندن مجموعه داده توسط اسنورت و تولید هشدارها و ارسال آن‌ها به سمت SmartConnector

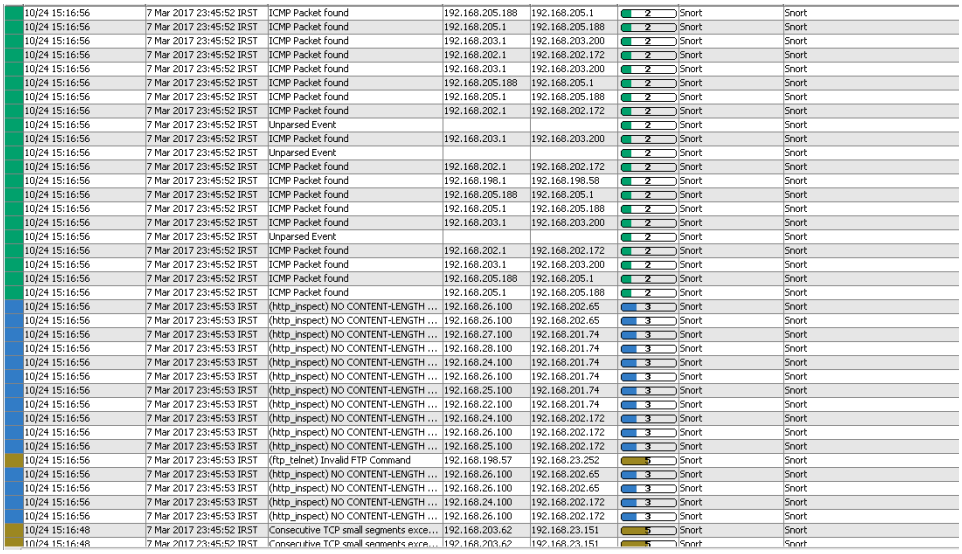
مجموعه داده ok-maccdc2011_00004_20110311221544.pcap با استفاده از دستور زیر توسط سیستم تشخیص نفوذ Snort خوانده می‌شود.

```
/usr/local/snort/bin/snort -c /usr/local/snort/etc/snort.conf -r /root/Desktop/ok-maccdc2011_00004_20110311221544.pcap
```

منتظر بمانید تا تمام هشدارها تولید شوند.

3-1-3 دریافت هشدارها توسط SmartConnector و ارسال آن‌ها به سمت ESM

با مراجعه به کنسول و مشاهده هشدارهای دریافتی روی ArcSight Express، از دریافت آن‌ها توسط SmartConnector و ارسال به ESM اطمینان حاصل می‌شود. به‌همین منظور برای مشاهده هشدارهای دریافتی باید یک کانال فعال تعریف شود. همان‌طور که در بخش 6 عنوان شد کانال فعال Snort-itran را تعریف کنید. همان‌طور که در شکل 52 ملاحظه می‌شود، هشدارهای ارسالی به‌درستی دریافت شده‌اند.



10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.205.188	192.168.205.1	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.205.1	192.168.205.188	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.203.1	192.168.203.200	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.202.1	192.168.202.172	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.203.1	192.168.203.200	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.205.188	192.168.205.1	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.205.1	192.168.205.188	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.202.1	192.168.202.172	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	Unparsed Event			2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.203.1	192.168.203.200	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	Unparsed Event			2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.202.1	192.168.202.172	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.198.1	192.168.198.58	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.205.188	192.168.205.1	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.205.1	192.168.205.188	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.203.1	192.168.203.200	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	Unparsed Event			2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.202.1	192.168.202.172	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.203.1	192.168.203.200	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.205.188	192.168.205.1	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:52 IRST	ICMP Packet found	192.168.205.1	192.168.205.188	2	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.26.100	192.168.202.65	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.26.100	192.168.202.65	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.27.100	192.168.201.74	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.28.100	192.168.201.74	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.24.100	192.168.201.74	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.26.100	192.168.201.74	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.25.100	192.168.201.74	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.22.100	192.168.201.74	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.24.100	192.168.202.172	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.26.100	192.168.202.172	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.25.100	192.168.202.172	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(ftp_telnet) Invalid FTP Command	192.168.198.57	192.168.23.252	5	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.26.100	192.168.202.65	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.26.100	192.168.202.65	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.24.100	192.168.202.172	3	Snort	Snort
10/24 15:16:56	7 Mar 2017 23:45:53 IRST	(http_inspect) NO CONTENT-LENGTH ...	192.168.26.100	192.168.202.172	3	Snort	Snort
10/24 15:16:48	7 Mar 2017 23:45:52 IRST	Consecutive TCP small segments exce...	192.168.203.62	192.168.23.151	5	Snort	Snort
10/24 15:16:48	7 Mar 2017 23:45:52 IRST	Consecutive TCP small segments exce...	192.168.203.62	192.168.23.151	5	Snort	Snort

شکل 52 نمایش هشدارهای ارسالی از اسنورت برای SmartConnector

3-1-4 نوشتن قوانین همبسته‌سازی و تجمیع برای شناسایی حملات

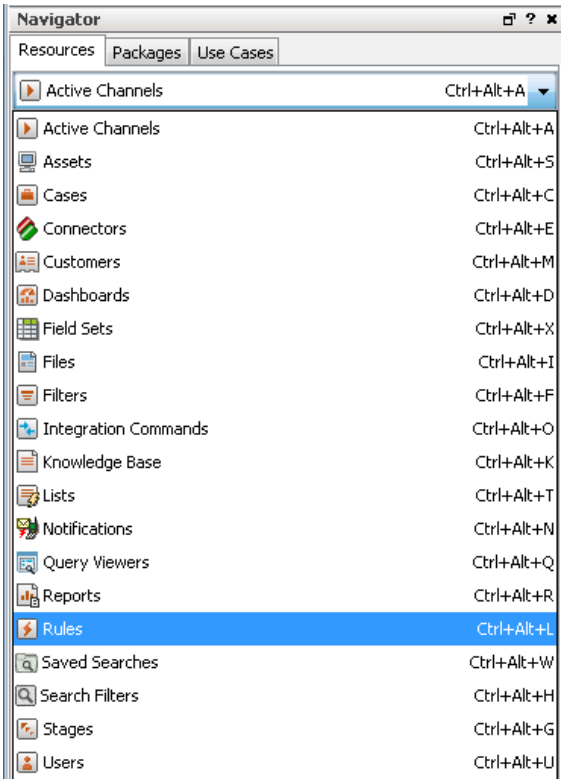
سه نوع قانون را می‌توان در ArcSight ESM ایجاد کرد. در ادامه این قوانین معرفی می‌شوند. برای ایجاد قانون باید رویدادهایی که باعث Trigger شدن قانون می‌شوند، آستانه‌ها (تعداد هشداری که پس از دریافت آن‌ها باید رویداد همبسته‌سازی تولید شود و پنجره زمانی دریافت این تعداد رویداد)، و اقداماتی که می‌خواهیم قانون انجام دهد را تعریف و مشخص کنیم. لذا قبل از ایجاد قانون باید تعیین شود قانون قرار است چه رویدادهایی را پایش کند، تعداد رویدادها چقدر است و چه فیلدهایی از رویدادها باید با یکدیگر مقایسه شوند. همچنین در صورت مشاهده چنین رویدادهایی چه اقدامی باید صورت گیرد. برای تعیین رویدادهایی که باعث Trigger شدن قانون می‌شوند از فیلدهای رویداد، نام و نوع تولیدکننده رویداد، نام و نوع ارسال‌کننده هشدار، زمان ارسال یا دریافت هشدار و سایر موارد می‌توان بهره گرفت.

از آنجایی‌که متناسب با سناریو حمله باید قانون تعریف شود، برای نمونه و با بررسی هشدارهای مجموعه داده مورد آزمون، قانونی برای دریافت هشدارهای Invalid FTP Command (ftp_telnet) می‌نویسیم. شش نوع هشدار با نام "Invalid FTP Command (ftp_telnet)"، از Product و Vendorی به نام Snort دریافت می‌شود. ما می‌خواهیم قانونی بنویسیم که اگر شش هشدار که نام آن‌ها یکسان و با " Invalid (ftp_telnet) FTP Command"بود، همچنین از حس‌گری که نام Product و Vendor آن Snort بود، در پنجره زمانی 2 دقیقه دریافت شود، آن‌ها را با یکدیگر همبسته کرده و یک رویداد همبسته‌سازی را تولید کند.

1-4-1-3 ایجاد قانون

برای نوشتن قانون به‌ترتیب زیر عمل شود:

از بخش Navigator، برگه Resources، گزینه Rule را برای تعریف قانون جدید انتخاب کنید (شکل 53).

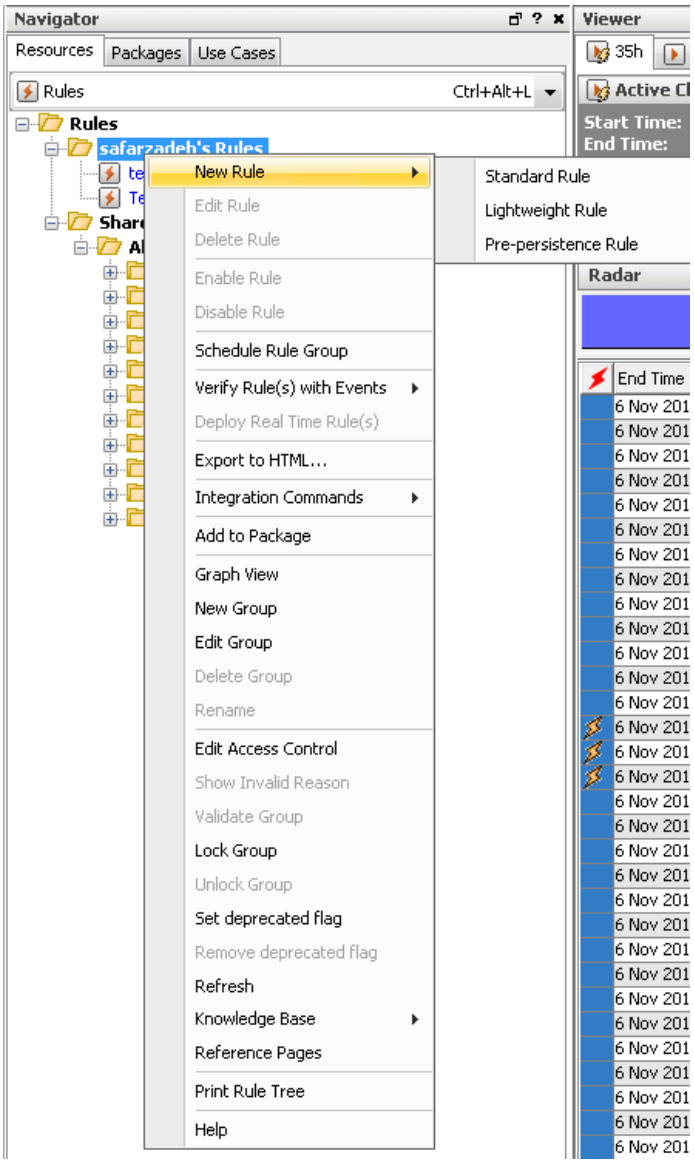


شکل 53 انتخاب منبع Rules برای تغییر در Ruleها

می‌توانید سه نوع قانون تعریف کنید. انواع قوانینی که قابل تعریف هستند عبارتند از:

- Standard Rules: این نوع قانون کامل‌ترین نوع قانون است. در این نوع قانون، در برگه شرایط بیش از یک شرط را می‌توان با استفاده از عملگرهای مختلف تعریف کرد، همچنین می‌توان رویدادها را در برگه Aggregation با یکدیگر تجمیع کرد و آن‌ها را کاهش داد. انواع اقدامات را در این قانون می‌توان تعریف کرد. امکان تبدیل این نوع قانون به دو نوع دیگر وجود دارد.
- Lightweight Rules: در این نوع قانون تنها یک شرط را می‌توان در برگه شرایط تعریف کرد و این قانون روی یک رویداد اعمال می‌شود. به‌این‌ترتیب امکان تجمیع رویدادها را نداریم. اما این قانون پیش از قوانین استاندارد اعمال می‌شود. به‌همین دلیل ساده‌تر هستند و سرعت پردازش آن‌ها بیشتر است. قوانین Lightweight تنها می‌توانند به‌عنوان پاسخ و واکنش روی Active List و Session List اقدامات را انجام دهند. تنها یک اقدام می‌توانند در پاسخ انجام دهد و آن "On Every Event" است. این قانون می‌تواند به سایر قوانین تبدیل شود.
- Pre-persistence Rules: در این نوع قانون نیز تنها یک شرط را می‌توان در برگه شرایط تعریف کرد و روی یک رویداد اعمال می‌شود و به‌این‌ترتیب امکان تجمیع رویدادها را نداریم. این قانون روی رویدادهای ورودی اعمال می‌شود. تفاوتی که این قانون با دو قانون دیگر دارد این است که اگر این قانون Trigger

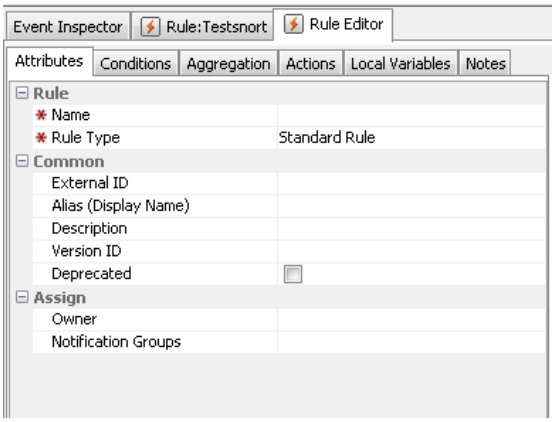
شود، مقدار فیلد مشخصی از یک رویداد ورودی را تغییر می‌دهد. سایر قوانین می‌توانند از نتیجه و تأثیری که این قانون روی رویدادهای ورودی می‌گذارد استفاده کنند. این قانون پیش از سایر قوانین اعمال می‌شود. گزینه Standard Rule را انتخاب کنید (شکل 54).



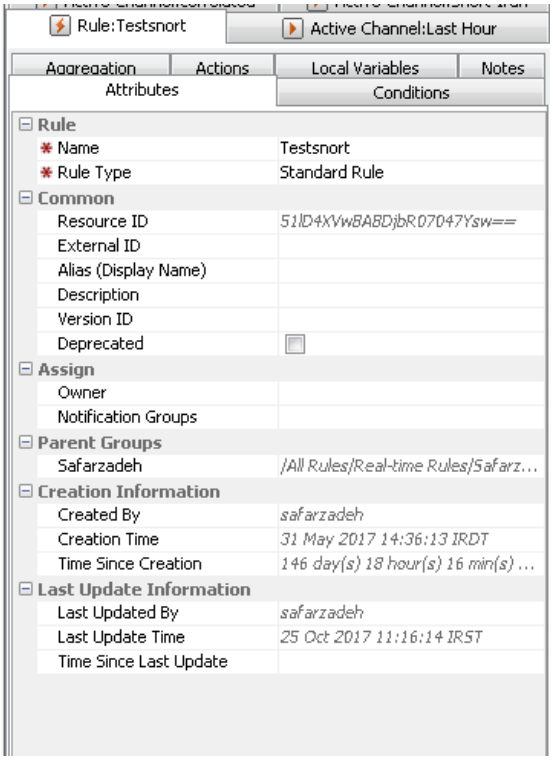
شکل 54 انتخاب نوع Rule

3-1-4-1-1 تخصیص نام به قانون

یک برگه در بخش Inspect/Edit به نام Rule Editor اضافه می‌شود (شکل 55). باید به قانون جدید نامی تخصیص داد، در برگه Attributes (شکل 56) در ویژگی Name، نام مناسبی به آن تخصیص می‌دهیم. در اینجا نام Testsnort را انتخاب کردیم. پس از تخصیص نام باید شرایطی که تحت آن قانون اعمال شود مشخص شود.



شکل 55 ورود مشخصات کلی Rule

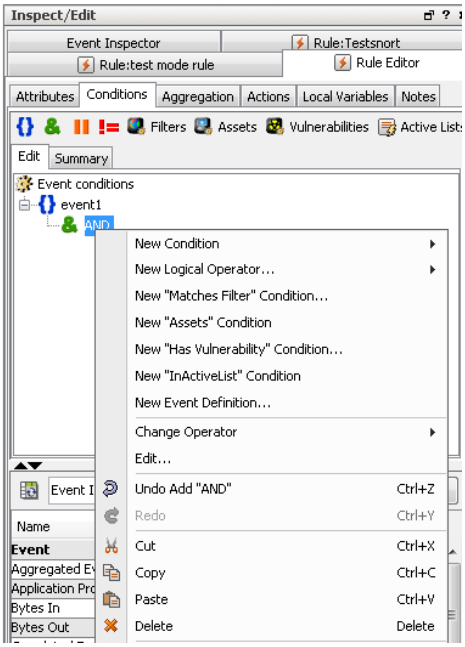


شکل 56 نام‌گذاری Rule تعریف‌شده

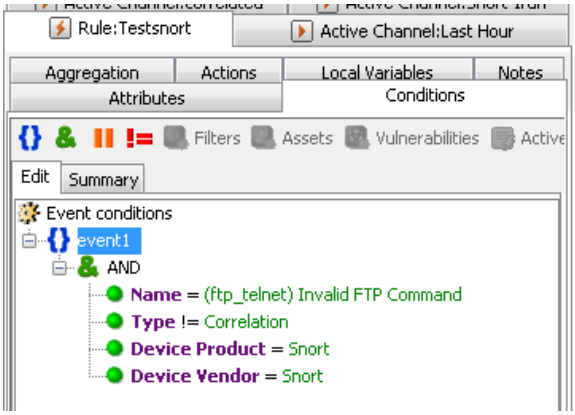
3-1-4-1-2 تعریف شرایط قانون

پس از تخصیص نام به قانون جدید باید شرایط اعمال قانون را مشخص کنیم. تعیین این شرایط متناسب است با حمله‌ای که قرار است آن را تشخیص دهیم. برای تعیین شرایط به برگه Conditions رفته، امکان استفاده از عملگرهای &، = !، || برای تعیین شرایط وجود دارد. در میان هشدرهای دریافت شده روی ESM، 6 هشدار با نام Invalid FTP Command (ftp_telnet) وجود دارد که این هشدارها در پنجره زمانی 2 دقیقه قطعاً ارسال می‌شوند. این هشدارها توسط حس‌گر اسنورت ارسال می‌شوند. در برگه شرایط می‌خواهیم بگوییم اگر از

حس‌گری با نوع Snort هشداری به نام Invalid FTP Command (ftp_telnet) دریافت شد و این هشدار از نوع همبسته شده نبود آن‌ها را با یکدیگر همبسته کن. از آنجایی‌که قانون از چند قسمت تشکیل شده است و تمام آن‌ها باید برقرار باشند عملگر & را انتخاب کرده (شکل 57)، سپس روی آن راست‌کلیک می‌کنیم. New Condition را انتخاب کرده و از بخش Root گزینه Name را انتخاب و نام هشدار را در آن‌جا وارد می‌کنیم. در بخش Root گزینه Type را تعیین می‌کنیم. نوع رویدادهایی که قانون روی آن‌ها اعمال می‌شود نباید از نوع Correlation باشد، به این معنی که این قانون تنها روی هشدارهای دریافتی اعمال می‌شود. سپس Root/Device Product و Snort Root/Device Vendor را وارد می‌کنیم. مانند شکل 58 گزینه Apply را انتخاب می‌کنیم.



شکل 57 تعریف شرایط اعمال Rule



شکل 58 نهایی‌سازی شرایط تعریف‌شده برای Rule

حال نوبت تعیین شرایط تجمیع است.

3-1-4-1-3 تعریف شرایط تجمیع قانون

برای تعیین شرایط کاهش هشدارها و تجمیع آن‌ها، به برگه Aggregation می‌رویم (شکل 59). در بخش # of matches باید تعداد دفعات تکرار هشدار مشخص شود. از آنجایی‌که 6 بار این هشدار دریافت می‌شود، عدد 6 را وارد می‌کنیم. در بخش پنجره زمانی باید مدت زمانی که منتظر می‌ماند 6 هشدار دریافت شوند تعیین شود. عدد 2 و معیار Minutes انتخاب می‌شود. همچنین تعیین می‌کنیم که اگر فیلدهای Name، Device Product و Device Vendor هشدارها یکسان بود، آن‌ها را با یکدیگر تجمیع کند. حال که شرایط کاهش و تجمیع هشدارها مشخص شد، در گام آخر باید تعیین کنیم اگر Manager با چنین شرایطی مواجه شود باید چه اقدامی را انجام دهد.

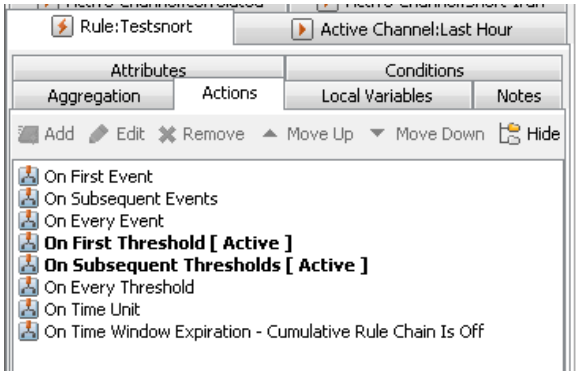
شکل 59 تعیین شرایط تجمیع و کاهش هشدارها

4-1-4-1-3 تعریف اقدام

برای تعیین اقدام به برگه Actions رفته و اقدام مورد نظر را انتخاب می‌کنیم (شکل 60). انواع اقدامات ممکنی که ESM می‌تواند انجام دهد در شکل 60 فهرست شده‌اند. در ادامه آن‌ها را معرفی می‌کنیم.

- On the first event: تنها زمانی که اولین رویداد را با مشخصات مشخص شده در قانون مشاهده کرد، یک رویداد همبسته‌سازی تولید می‌کند.
- On subsequent events: اگر برای بار دوم و سوم و دفعات بعدی به‌ترتیب هشدارهایی با شرایط تعریف‌شده در قانون مشاهده شود به‌ازای هر کدام یک رویداد همبسته‌سازی تولید می‌شود.
- On every event: به‌ازای هر رویداد با مشخصات مشخص‌شده در قانون اقدام را انجام می‌دهد. این اقدام تنها برای قوانین Lightweight و Pre-persistence اعمال می‌شود.
- On first threshold: هنگامی که برای اولین بار تعداد هشدارها با آستانه تعریف‌شده برابر شد، یک رویداد همبسته‌سازی تولید می‌کند.
- On subsequent thresholds: اگر برای بار دوم، سوم و به‌همین ترتیب دفعات بعدی هشدارهایی با شرایط تعریف‌شده در قانون و به تعداد دفعات مشخص شده در قانون دریافت شوند به‌ازای هر آستانه یک رویداد همبسته‌سازی تولید می‌شود.
- On every threshold: اگر تعداد هشدارها با مشخصات تعریف‌شده در قانون به مقدار آستانه تعریف‌شده برسد یک هشدار همبسته‌سازی تولید می‌شود.
- On time unit: اگر تعداد هشدارها در پنجره زمانی تعریف‌شده به تعداد آستانه تعریف‌شده برسد، یک رویداد همبسته‌سازی تولید می‌شود.
- On time window expiration: در صورتی‌که پنجره زمانی آستانه منقضی شود.

اقدامات On the first event و On subsequent events و سپس گزینه Apply را انتخاب می‌کنیم.

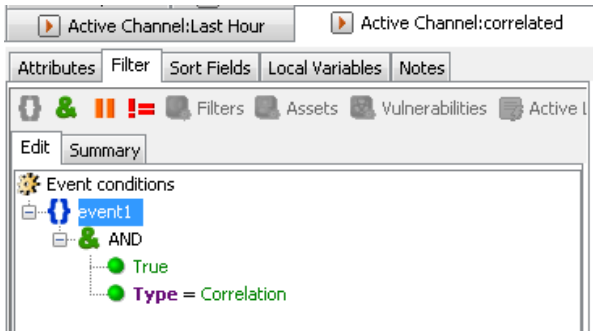


شکل 60 مشخص‌کردن اقدامی که باید انجام شود

برای نوشتن هر قانونی باید تمام این مراحل طی شود. سپس برای این‌که این قانون روی هشدارهای دریافتی اعمال شود، باید آن را به فولدر Real-time Rules انتقال داد. پس از تعریف قانون و اعمال آن با فشردن گزینه Apply، مطابق با بخش 6-1-4-1-2 مجدداً هشدارها را تولید کرده و سپس با مراجعه به کانال فعال پیش‌فرض Last Hour با راست‌کلیک روی آن و انتخاب گزینه Show Active Channel، نتیجه اقدام صورت گرفته که تولید یک رویداد است را مانند شکل 61 مشاهده می‌کنیم. کانال فعال Last Hour هشدارهایی که در یک ساعت اخیر تولید شده‌اند را نمایش می‌دهد.

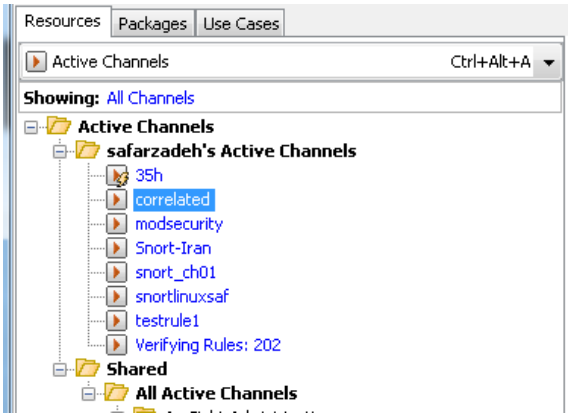
شکل 61 نتیجه اقدام تعیین‌شده برای Rule

برای این‌که تنها نتیجه قانون اعمال شده مشاهده شود و نه سایر رویدادها و هشدارها، کانال فعال با مشخصات شکل 62 را تعریف می‌کنیم.

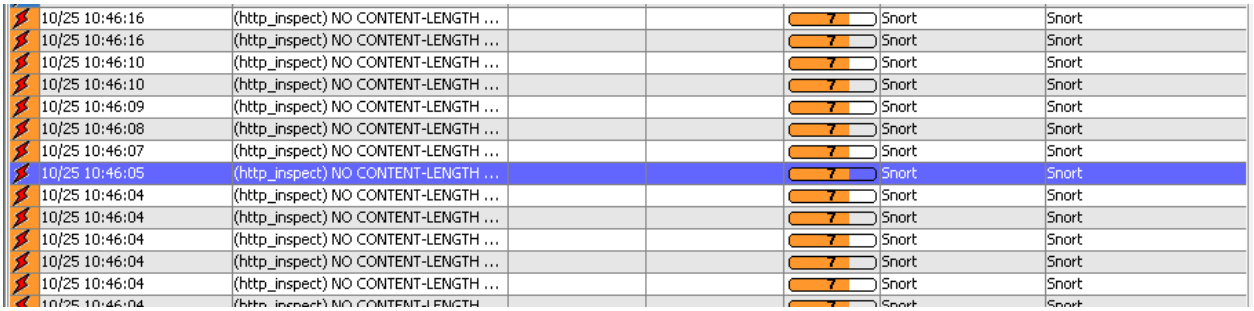


شکل 62 فیلتر کانال فعال برای مشاهده نتایج همبسته‌سازی

این کانال تمام هشدارهایی که به‌دلیل همبسته‌سازی تولید شده‌اند را استخراج کرده و نمایش می‌دهد. پس از فشردن گزینه Apply، همان‌طور که در شکل 63 نمایش داده شده است، کانال فعال به فهرست کانال‌های فعال افزوده می‌شود. با راست‌کلیک روی کانال تعریف‌شده و انتخاب گزینه Show Active Channel، همان‌طور که در شکل 64 نمایش داده شده است، فهرست هشدارهایی که در نتیجه همبسته‌سازی تولید شده‌اند را نمایش می‌دهد.



شکل 63 اضافه شدن کانال فعال برای مشاهده نتایج همبسته‌سازی



شکل 64 هشدارهایی که در نتیجه همبسته‌سازی تولید شده‌اند

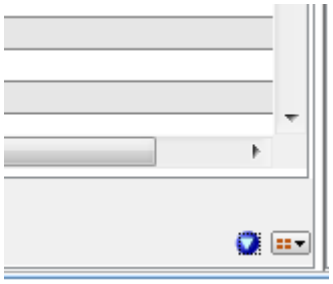
3-1-5 مشاهده نتایج

یکی از مواردی که در سامانه مدیریت رویداد و اطلاعات امنیتی حائز اهمیت است ارائه و بصری‌سازی داده‌های رویداد و نتایج تحلیل و همبسته‌سازی است. ESM این ارائه و بصری‌سازی را به سه صورت نمودار، گزارش و داشبورد ارائه می‌دهد. نمودار و گزارش را در محیط کنسول و داشبورد و گزارش را با دسترسی به ESM از طریق Command Center می‌توان مشاهده کرد. انواع داشبورد و گزارشی که می‌توان از طریق Command Center به آن دسترسی پیدا کرد در بخش 4-2 بیان شد، در ادامه نحوه مشاهده نمودارها و گزارش‌ها از طریق محیط کنسول بیان می‌شود.

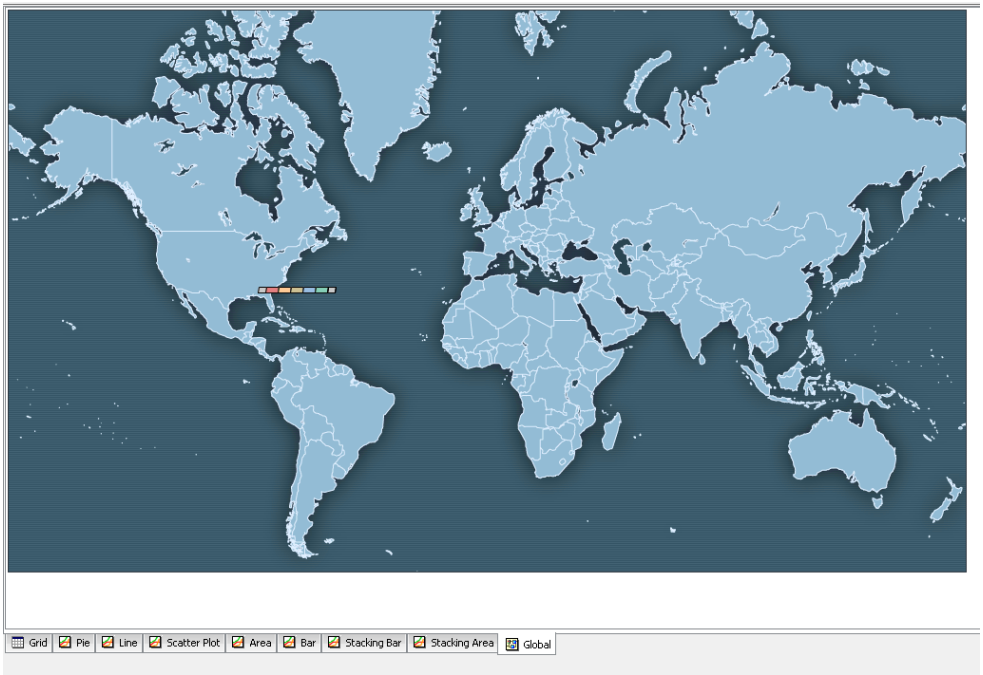
3-1-5-1 ارائه و بصری‌سازی از طریق نمودار

در بخش Viewer، قسمت انتهایی سمت راست، فلش آبی (شکل 65) نحوه نمایش نمودارها را مشخص می‌کند. اگر چند نمودار مختلف را باز کرده باشید، چیدمان آن‌ها را در بخش Viewer مشخص می‌کنید. در

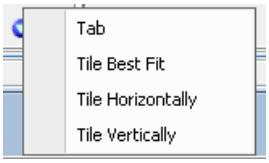
شکل 66 که 9 نمودار باز شده است، آن‌ها را به‌صورت برگه نمایش می‌دهد. انواع دیگر حالت‌های چیدمان در شکل 67 نمایش داده شده است.



شکل 65 گزینه مشاهده نحوه نمایش نمودارها

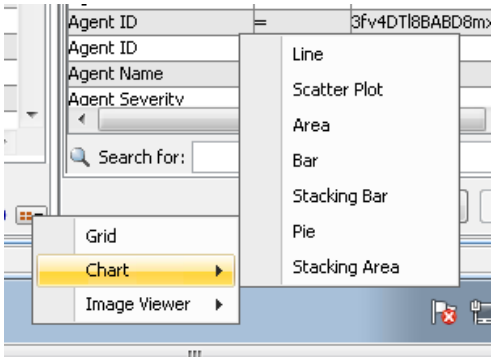


شکل 66 نمایش نمودارهای باز شده به شکل برگه در کنار یکدیگر



شکل 67 انواع حالت‌های نمایش نمودارهای باز شده در کنار یکدیگر

با استفاده از نمودارها می‌توان رویدادهایی که در یک کانال فعال قرار دارند را به شکل‌های مختلف نمایش داد. انواع نمودارهایی که می‌توان داده‌های رویداد را در قالب آن نمایش داد، در شکل 68 به تصویر کشیده شده است، به سه صورت Grid، Chart و Image Viewer است.



شکل 68 انواع دسته‌های نحوه نمایش نمودار

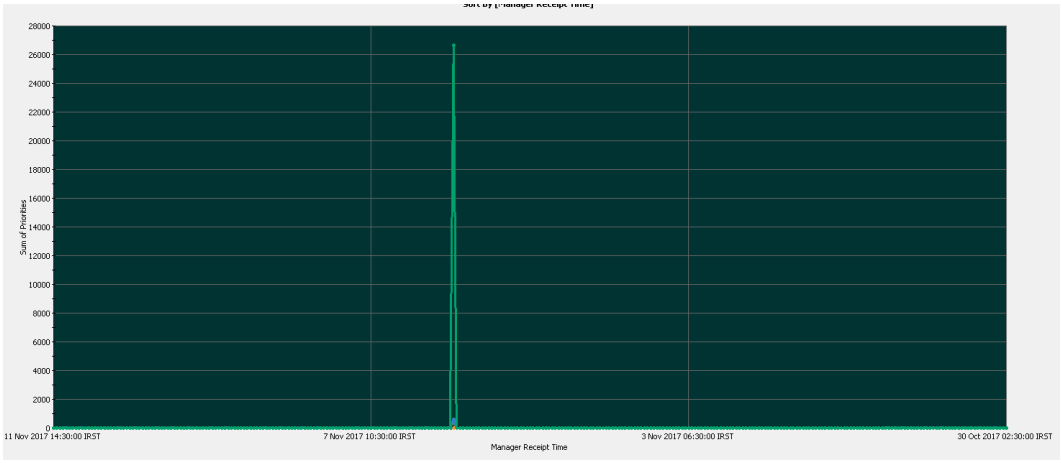
نمایش یک کانال فعال را انتخاب می‌کنیم، به‌صورت پیش‌فرض رویدادها را به‌صورت Grid نمایش می‌دهد (شکل 69).

Radar

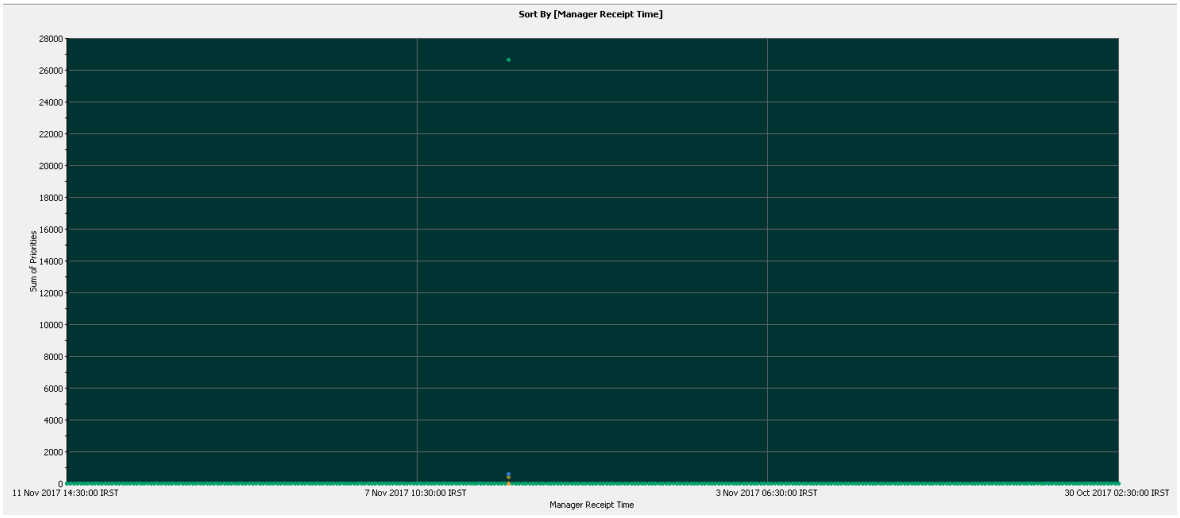
Manager Receipt Time	End Time	Name	Attacker Address	Target Address	Priority	Device Vendor	Device Product
11/11 14:52:09	11/11 14:58:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 14:47:09	11/11 14:53:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 14:42:09	11/11 14:48:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 14:37:09	11/11 14:43:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 14:32:09	11/11 14:38:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 14:27:09	11/11 14:33:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 14:22:09	11/11 14:28:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 14:17:09	11/11 14:23:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 14:12:09	11/11 14:18:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 14:07:09	11/11 14:13:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 14:02:08	11/11 14:08:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 13:57:08	11/11 14:03:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 13:52:08	11/11 13:58:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 13:47:08	11/11 13:53:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 13:42:08	11/11 13:48:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 13:37:08	11/11 13:43:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 13:32:08	11/11 13:38:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 13:27:08	11/11 13:33:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 13:22:08	11/11 13:28:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 13:17:08	11/11 13:23:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 13:12:08	11/11 13:18:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 13:07:08	11/11 13:13:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 13:02:08	11/11 13:08:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 12:57:08	11/11 13:03:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 12:52:08	11/11 12:58:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 12:47:08	11/11 12:53:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 12:42:08	11/11 12:48:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 12:37:07	11/11 12:43:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 12:32:12	11/11 12:38:01	Connector Raw Event Statistics			3	ArcSight	ArcSight
11/11 12:27:12	11/11 12:33:01	Connector Raw Event Statistics			3	ArcSight	ArcSight

شکل 69 نحوه نمایش Grid

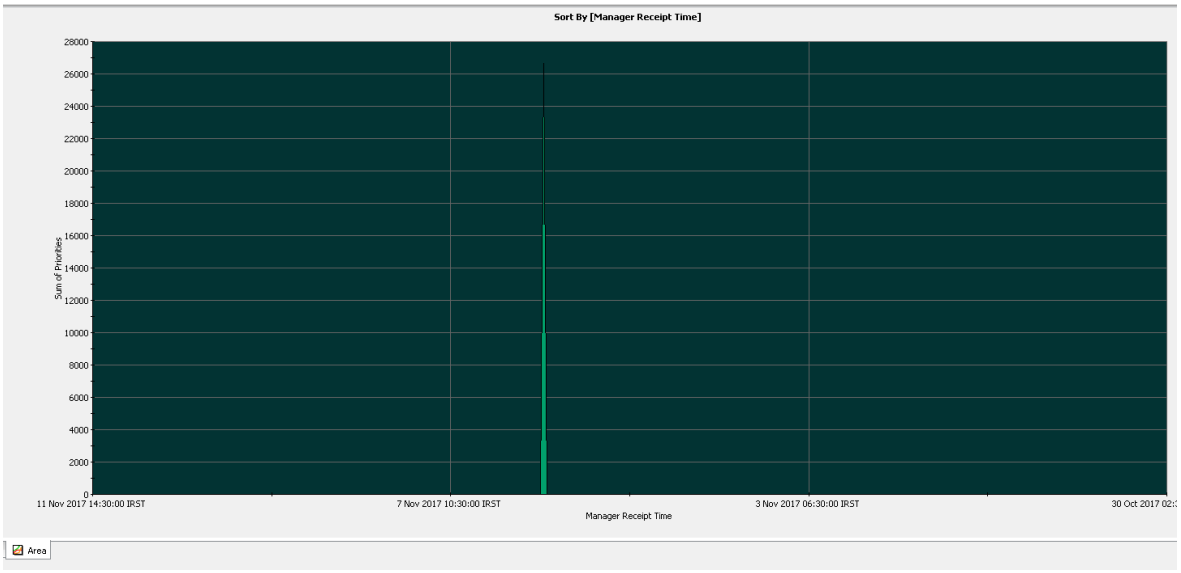
در صورتی‌که بخواهید رویدادها را به شکل Chart ببینید 7 حالت Line, Scatter Plot, Area, Bar, Stacking Bar, Pie, Stacking Area وجود دارد. در ادامه انواع این نمودارها برای کانال فعالی که نمودار Grid آن در شکل 69 نمایش داده شده است، آمده است (شکل‌های 70 تا 76).



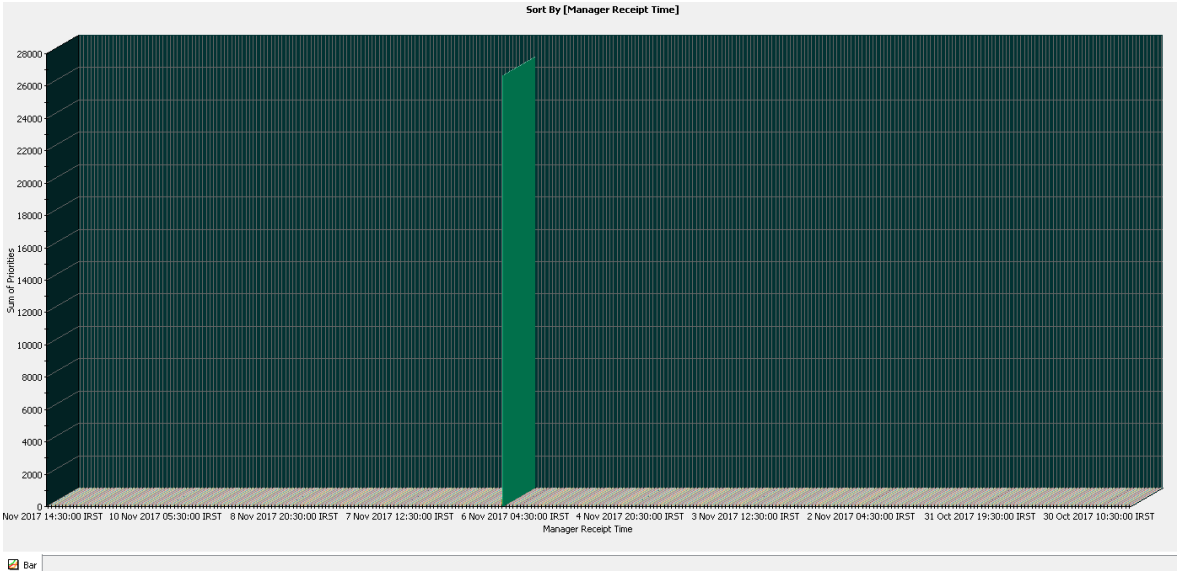
شکل 70 نحوه نمایش Line chartr



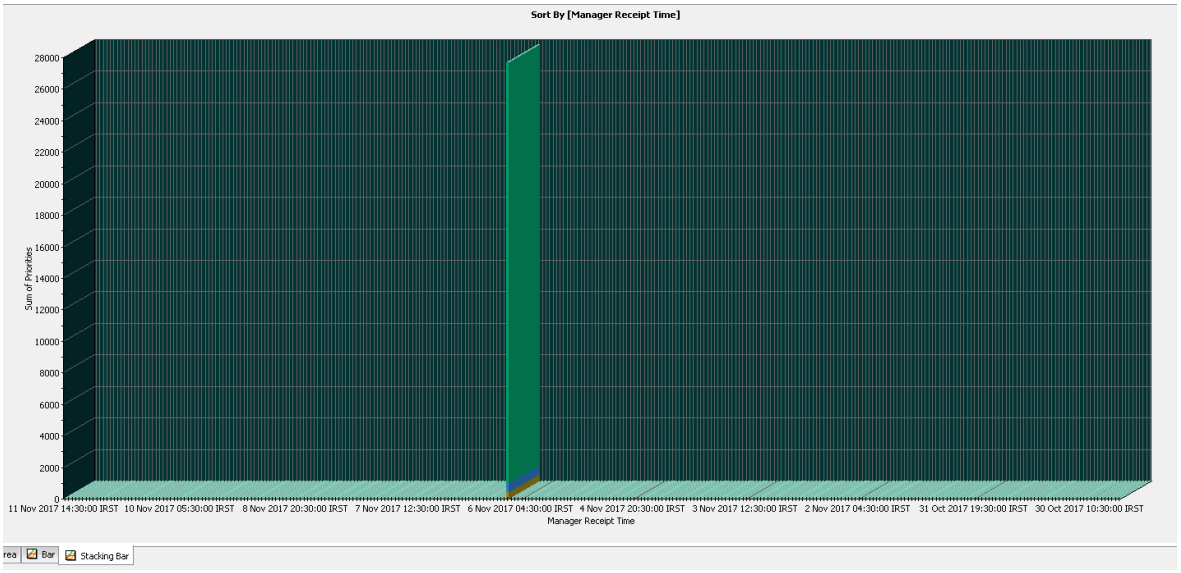
شکل 71 نحوه نمایش Scatter Plot



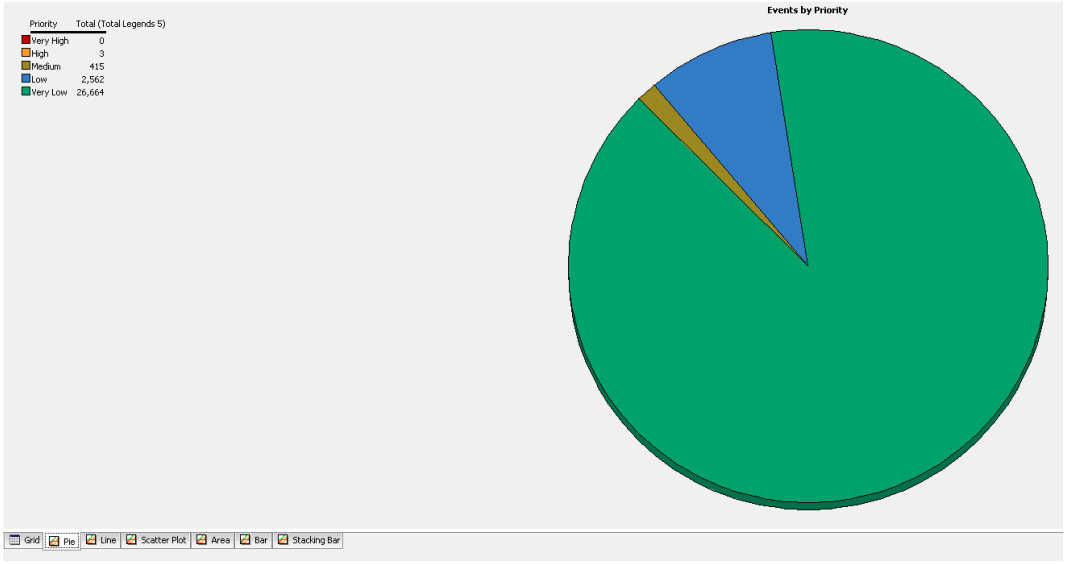
شکل 72 نحوه نمایش Area



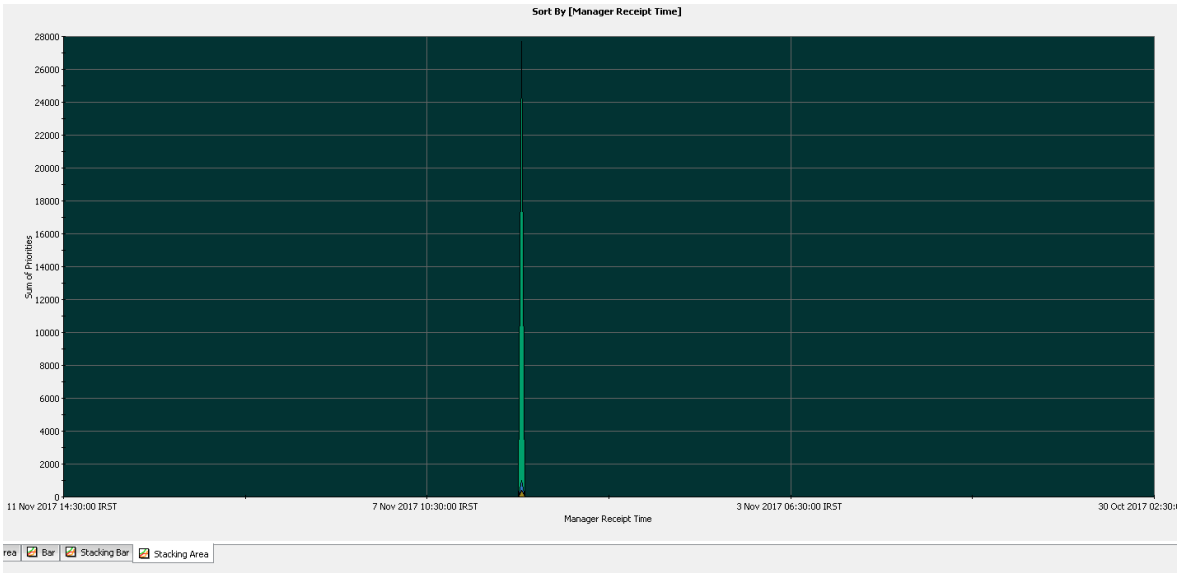
شکل 73 نحوه نمایش Bar



شکل 74 نحوه نمایشStacking bar

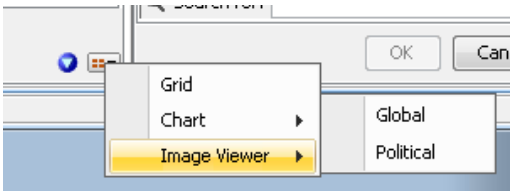


شکل 75 نحوه نمایش Pie



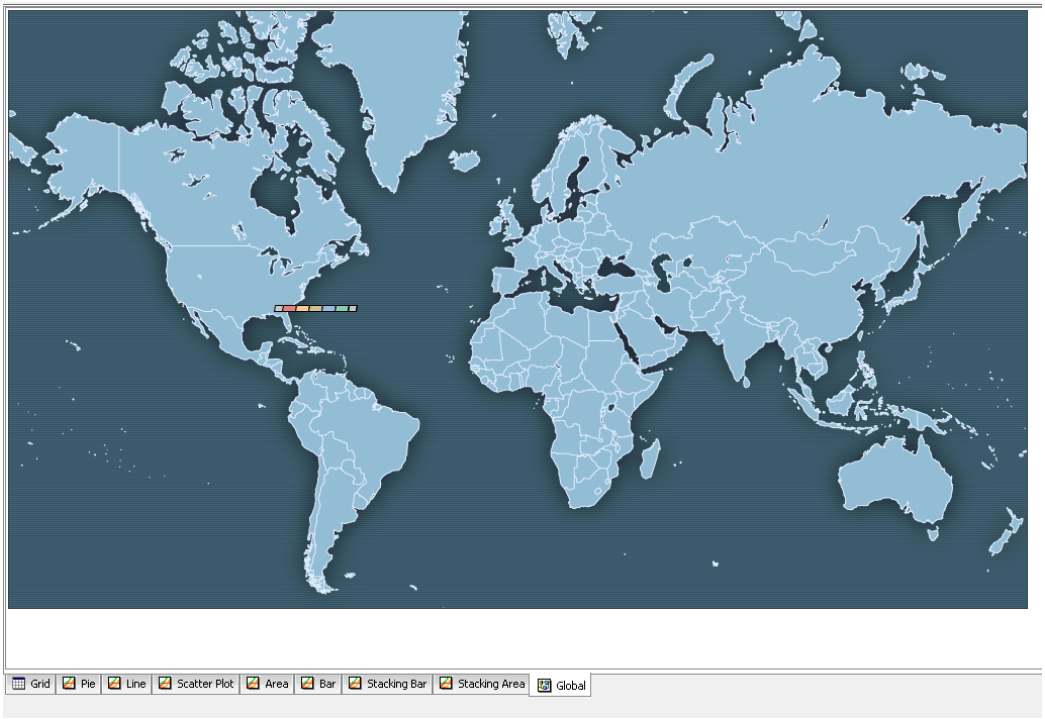
شکل 76 نحوه نمایش Stacking area

در صورتی‌که بخواهید رویدادها را با استفاده از مجموعه نمودارهای Image Viewer ببینید، با انتخاب یکی از دو نمودار Global و Political (شکل 77) این امر امکان‌پذیر است.



شکل 77 انواع نمودارهای دسته Image Viewer

در ادامه این دو نمودار برای کانال فعالی که سایر نمودارهای آن را دیدیم، نشان داده شده‌اند (شکل‌های 78 و 79).

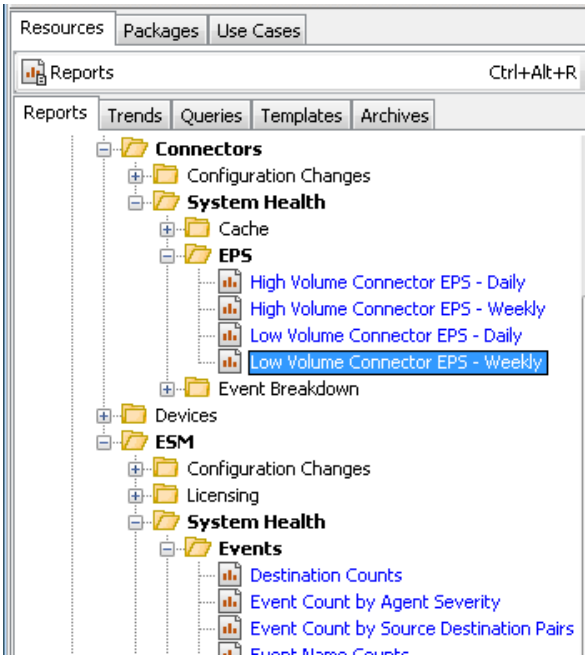


شکل 78 نحوه نمایش Global

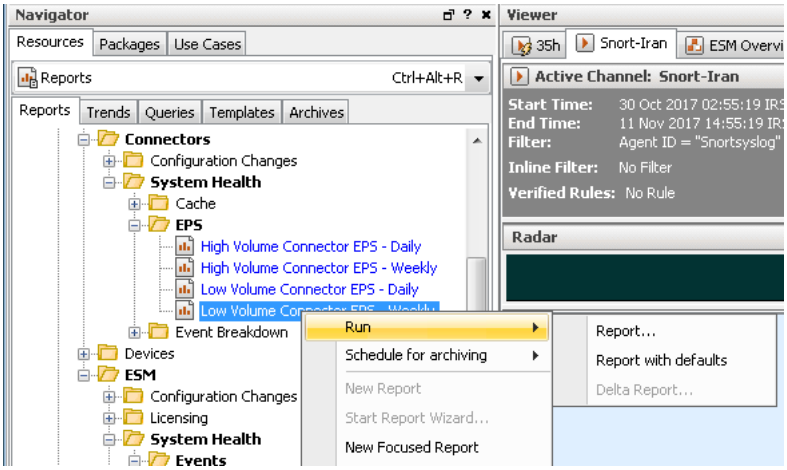
شکل 79 نحوه نمایش Political

3-1-5-2 ارائه و بصری‌سازی از طریق گزارش

در ESM، برگه منابع، بخش Reports، به‌صورت پیش‌فرض گزارش‌هایی تعبیه شده است (شکل 80). امکان ایجاد گزارش‌های سفارشی نیز وجود دارد. برای مشاهده یک گزارش روی آن راست‌کلیک کرده (شکل 81) گزینه Run و سپس Report را انتخاب کنید.

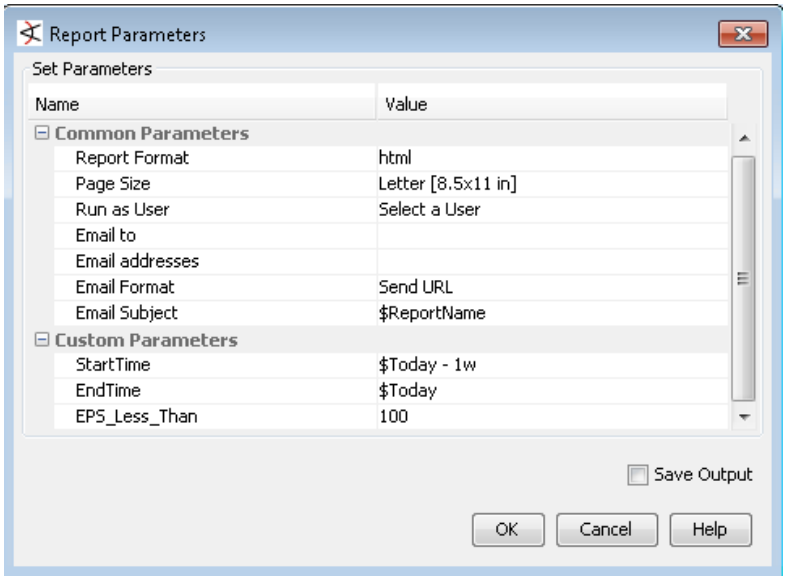


شکل 80 گزارش‌های از پیش تعریف‌شده

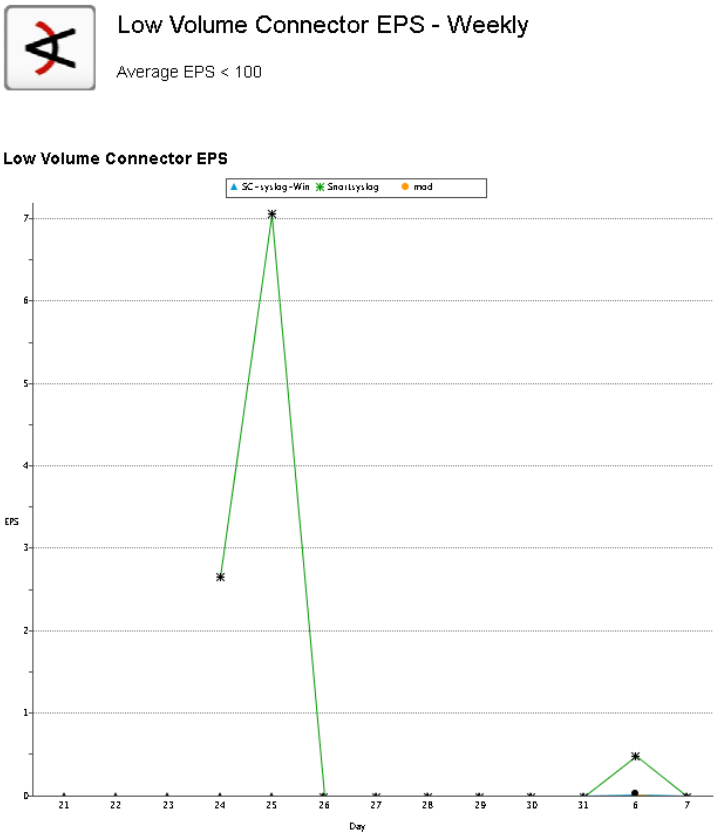


شکل 81 اجرا و نمایش گزارش

در صفحه‌ای که باز می‌شود (شکل 82)، می‌توان ویژگی‌های نمایش را تغییر داد به‌عنوان مثال با تغییر Start Time امکان تغییر پنجره زمانی فراهم شده است. سپس OK کنید. گزارش در شکل‌های 83 و 84 نمایش داده شده است.



شکل 82 تغییر مشخصات گزارش



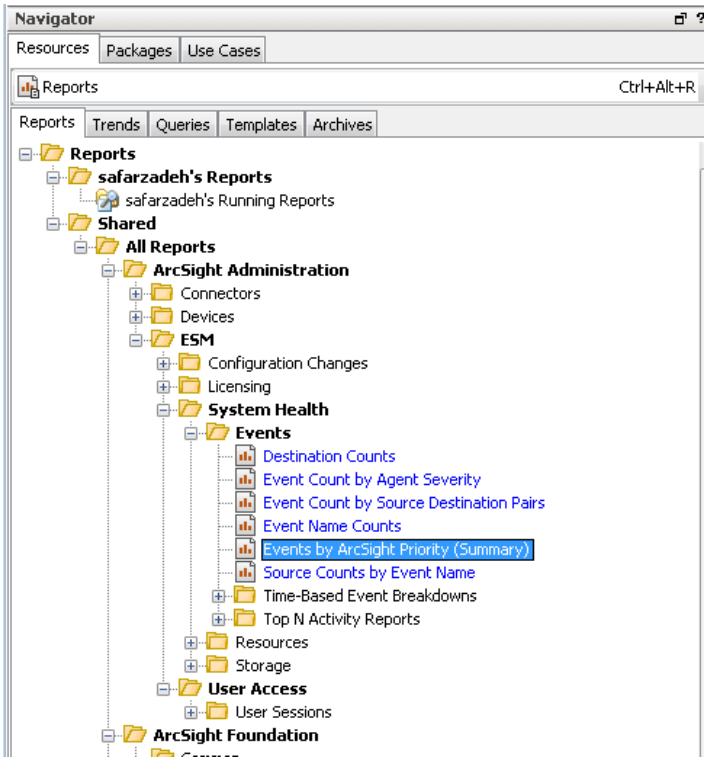
شکل 83 نتیجه اجرای گزارش

Low Volume Connector EPS Details

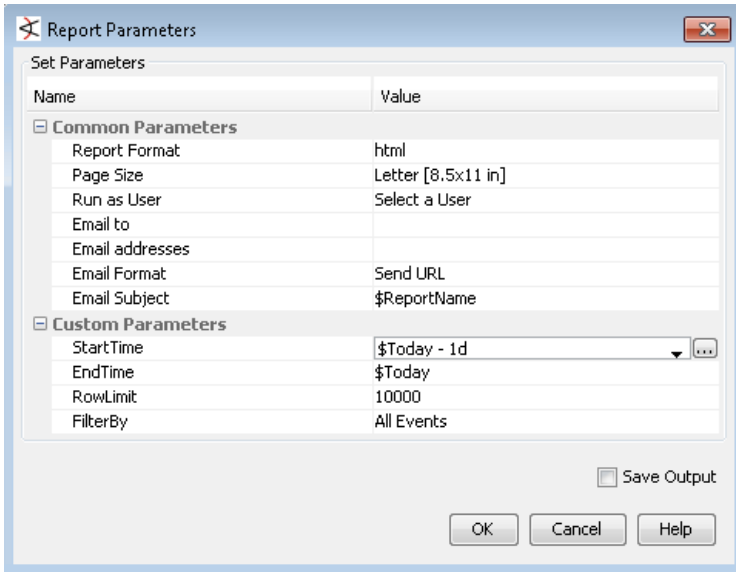
Connector Name	Day	Average EPS
/All Connectors/Iran/Snortsyslog	24	2.651
	25	7.05
	26	0
	27	0
	28	0
	29	0
	30	0
	31	0
	6	0.481
	7	0
	8	0
	9	0
/All Connectors/Our Lab/SC-syslog-Win	21	0
	22	0
	23	0
	24	0
	25	0
	26	0
	27	0
	28	0
	29	0
	30	0
	31	0
	6	0.009
	7	0
	8	0
	9	0
/All Connectors/tehran/mod	6	0.017
	7	0
	8	0
	9	0

شکل 84 نتیجه اجرای گزارش

یک نمونه گزارش دیگر در شکل‌های 85 تا 89 به تصویر کشیده شده است.



شکل 85 انتخاب گزارش برای اجرا



شکل 86 تغییر پارامترهای نمایش گزارش

Events by ArcSight Priority (Summary)

Priority	Name	Number of Events
8	ASM Database Status Change - Critical	10
	Deactivating the rule Storage Licensing Audit event Detected: CPU usage share 68.98449417807558 % > threshold 50	1
7	Connector Discovered or Updated	14
	Update Connector Connection Status	7
	Update Connector Caching Status	5
	Connector Up	5
	Connector Down	2
	Connector Caching	2
	Connector Still Caching	1
	Connector Cache Empty	1
	Denial of service event filtering triggered	1
	Scheduled execution skipped because previous execution has not ended (Resource Search Index Updater)	1
5	Agent is currently caching events	267
	Agent [Snort] heartbeat timeout	2
	Agent [Snortsyslog] heartbeat timeout	2
	Agent [modsecurity] heartbeat timeout	2
	Device Receipt Time from [ubuntu||Snort|Snort] may be incorrect - Device Receipt Time is smaller than Agent Receipt Time (Events are in the past)	1
	Agent [Linux-snort-saf] heartbeat timeout	1
	Agent [SC-syslog-Linux] heartbeat timeout	1
	Agent [SC_Win7_Class] heartbeat timeout	1
	Channel [35h] is empty	1
4	Event archive settings updated	7
3	Monitor Event	527052
	Connector Raw Event Statistics	5522
	Task successfully removed	4713
	Task successfully scheduled	4713
	ScheduledTask updated	4711
	ActiveList entry expired	4036
	ASM Database Status Change - Normal	2304
	ActiveList entry added	2045
	Database Insert Time - Last Hour	1339
	Event Throughput	1339
	Scheduled task executed (Resource Search Index Updater)	1332
	Successfully executed regular resource search index update	1327
	ActiveList entry updated	750
	Successful Trend-Query Run	704

شکل 87 نتیجه اجرای گزارش

Priority	Name	Number of Events
	Starting Trend Query	704
	Scheduled task executed (AUP Updater)	666
	Starting Trend Task	271
	Trend Task Ending	271
	Database Retrieval Time - Last Hour	267
	Database Retrieval Time - Last 24 Hours	130
	Database Insert Time - Last 24 Hours	122
	Scheduled task executed (PurgeStaleMarkSimilarConfigs)	111
	Scheduled task executed (Table Stats Updator)	111
	Scheduled task executed (Events Count)	111
	Scheduled task executed (Windows Events by Event and Device)	111
	Scheduled task executed (Sortable Fields Updater)	111
	Agent Login	101
	SessionList entry updated	59
	SessionList entry added	54
	AddToList: Success	41
	License Audit	28
	Successful SessionList Partition Operation	22
	Successful Trend Partition Operation	21
	File processing ended: Success	20
	File processing started	20
	Agent updated	16
	Archive created	8
3	Archive scheduled	8
	Archive archival success	8
	RemoveFromList: Failure	7
	RemoveFromList: Success	6
	ActiveList entry deleted	6
	Scheduled task executed (Storage Licensing Data)	5
	Scheduled task executed (Connector Total Events - Hourly)	5
	Scheduled task executed (QueryViewer Queries)	5
	Scheduled task executed (Report Queries)	5
	Scheduled task executed (ArcSight User Login Trends - Hourly)	5
	Scheduled task executed (Trend Queries)	5
	Scheduled task executed (Connector Average EPS - Last 7 days)	5
	Scheduled task executed (Failed Queries)	5
	Scheduled task executed (Connector Daily Average EPS)	5
	Supplemental Archive archival success	4
	Scheduled task executed (ASM Database Free Space)	4
	Successfully executed daily resource search index update	4
	Scheduled task executed (Dependent Resource Validator)	4
	Login succeeded for user name 'safarzadeh'	2
	Event Transport Fail Over	2
	ScheduledTask deleted	2
	ScheduledTask inserted	2
	Group [DatabaseTableSchema] updated	2
	Group [ScheduledTask] updated	2

شکل 88 نتیجه اجرای گزارش

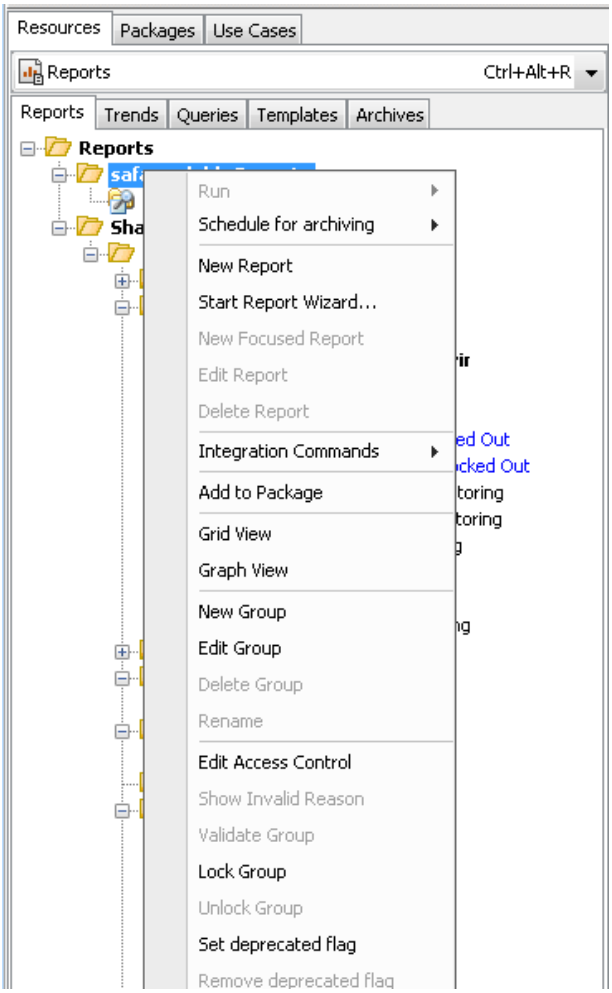
11/2/17 to 11/11/17

Priority	Name	Number of Events
	Agent [Snortsyslog] reconnected	2
	User updated	2
	Channel [35h] query completed	2
	UnassignedResourcesGroup [Rule] inserted	1
	Content for type [system-zone-mappings] updated to version [00000000000000061012] for Agent ID [3CG0xfI0BABCBpGhkimsX5A==]	1
	Group [Asset] updated	1
	Agent [SC-syslog-Win] type [syslog] started	1
	UnassignedResourcesGroup [ActiveChannel] inserted	1
	Channel [Snort-Iran] got attached	1
	ArcSight Manager Started	1
	UnassignedResourcesGroup [ScheduledTask] inserted	1
	Content for type [system-zone-mappings] updated to version [00000000000000061012] for Agent ID [3fw4DTI8BABD8mxkb+2S4KQ==]	1
	Agent [Snortsyslog] type [syslog] started	1
	DatabaseTableSchema deleted	1
	UnassignedResourcesGroup [FieldSet] inserted	1
	Channel [Snort-Iran] query completed	1
	ArcSight User Login	1
	UnassignedResourcesGroup [User] inserted	1
	AttachmentOnlyGroup [Package] inserted	1
	Agent [mod] type [sdkmultifolderreader] started	1
	DatabaseTableSchema inserted	1
	UnassignedResourcesGroup [Filter] inserted	1
	Successfully executed weekly rebuild of resource search index	1
	ArcSight User Login Timeout	1
	Group [ActiveChannel] inserted	1
	User Session Timed Out for user name 'safarzadeh'	1
	Channel [35h] got attached	1
	Agent cache empty	1
	UnassignedResourcesGroup [Package] inserted	1
	Content for type [system-zone-mappings] updated to version [00000000000000061012] for Agent ID [37ttAqVsBABDIz4eNfIIdvQ==]	1
	Successfully updated the resource search index	1
	Rule updated	1
	Group [ActiveChannel] updated	1
	Unable to resolve '/All Agents/Site Agents/SELECT_YOUR_NRM_AGENT'	1
2		239
	WAF pass	137

شکل 89 نتیجه اجرای گزارش

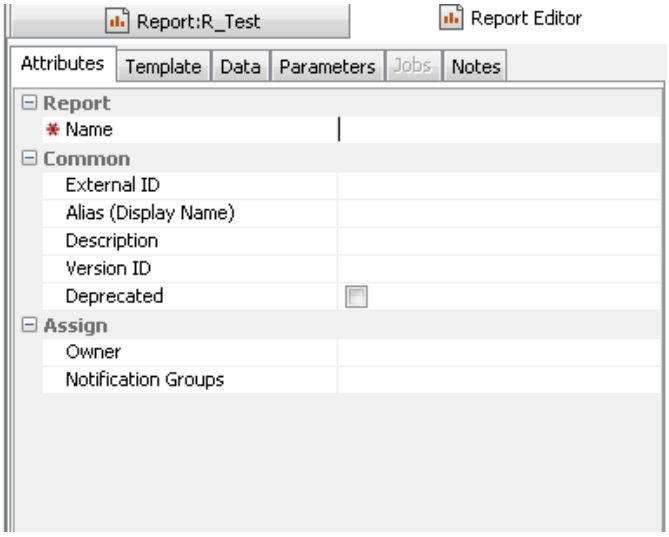
3-1-5-2-1 ایجاد گزارش سفارشی

برای ایجاد گزارش جدید یا سفارشی، در برگه Reports، روی فولدری که می‌خواهید گزارش در آن درست شود راست‌کلیک کرده و گزینه New Report را انتخاب کنید (شکل 90).

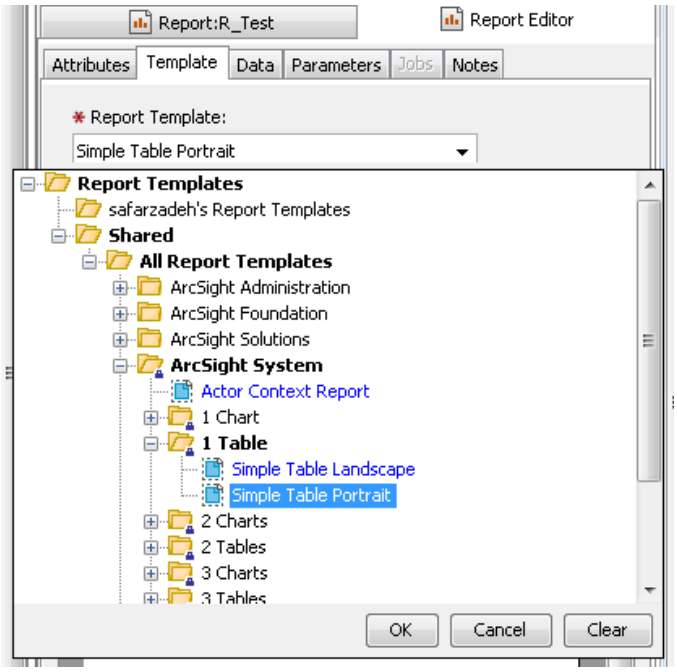


شکل 90 انتخاب گزینه New Report

سپس به بخش Inspect/Edit رفته و در برگه Attributes مشخصات اسمی گزارش را وارد کنید (شکل 91). به برگه template بروید. در این برگه قالبی که گزارش در آن نمایش داده می‌شود، قابل تعیین است (شکل 92).

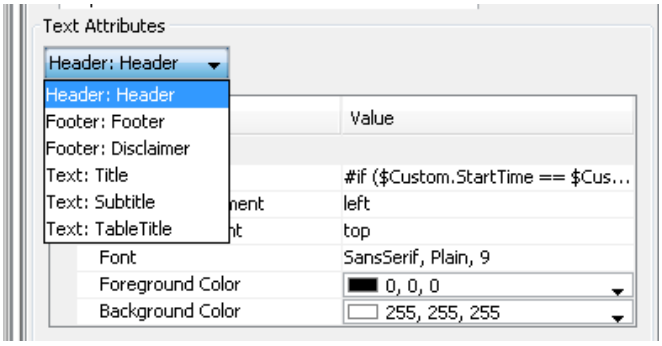


شکل 91 ورود مشخصات گزارش



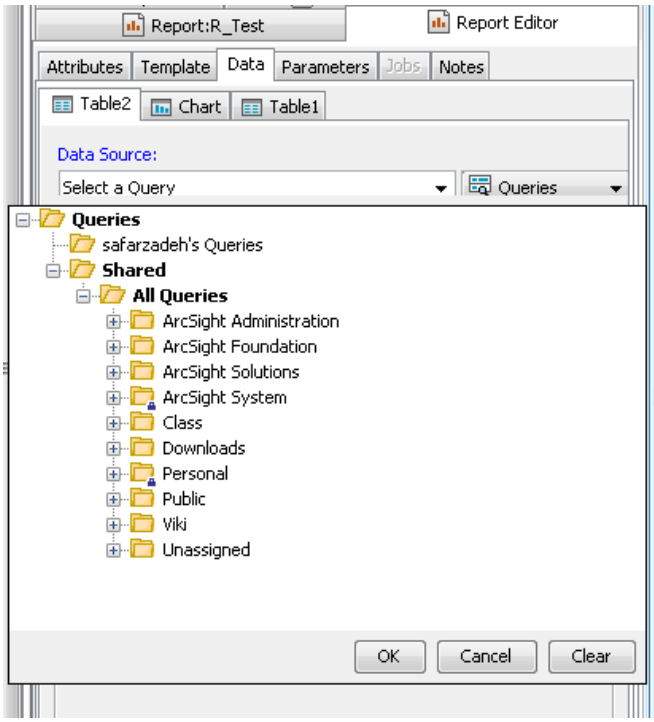
شکل 92 انتخاب قالب گزارش‌گیری

علاوه بر قالب امکان تعیین مشخصات سرآیند و پی‌آیند (شکل 93) وجود دارد.



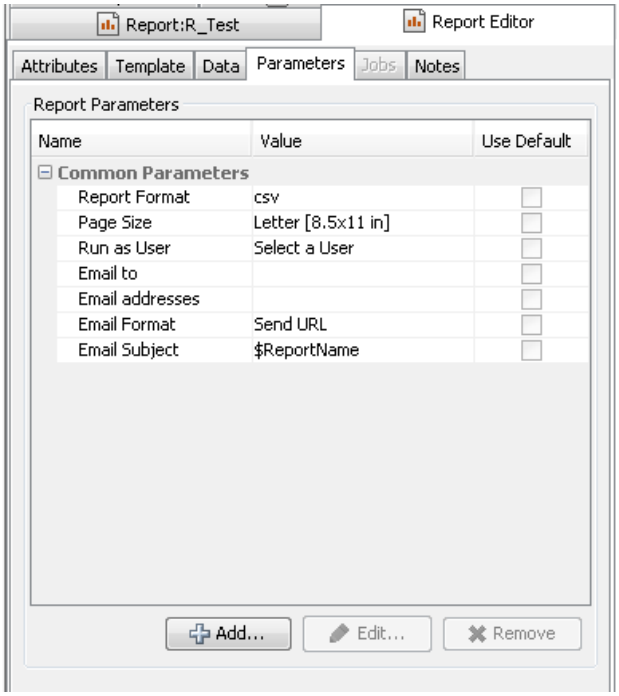
شکل 93 انتخاب مشخصات سرآیند و پی‌آیند

در برگه Data، باید منبع داده‌ای که قرار است اطلاعات از آن استخراج شود، تعیین شود (شکل 94).



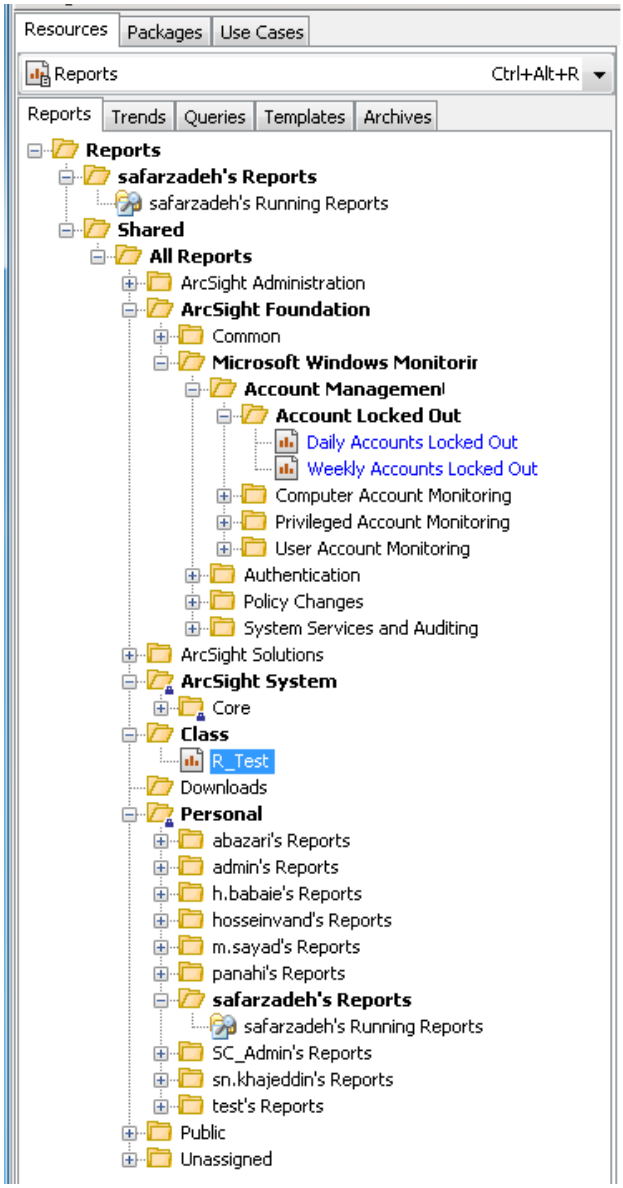
شکل 94 انتخاب منبع داده گزارش

در برگه Parameters (شکل 95)، می‌توان قالب گزارش (htm، pdf، csv و سایر موارد)، اندازه صفحه و مواردی از این قبیل را تعیین کرد.



شکل 95 تعیین مشخصات نحوه ارائه گزارش

با انتخاب گزینه Apply گزارش جدید ایجاد می‌شود. این گزارش را در شکل 96 ملاحظه می‌کنید.



شکل 96 گزارش جدید ایجاد شده

4 خطایابی یا Troubleshooting

در ادامه برخی دستورات مهم که هنگام مواجه با شرایط خطا کمک می‌کنند، آمده است. متناسب با مسیر نصب مسیر اجرای دستورات تغییر می‌کند.

اجرای ArcSight Manager:

/etc/init.d/arcsight_services start manager

بررسی اجرای موفقیت‌آمیز سرویس:

cd ARCSIGHT_HOME;tail -f logs/default/server.std.log

بررسی وضعیت سرویس‌ها:

/etc/init.d/arcsight_services status all

پیش از راه‌اندازی مجدد کارگزار ESM با استفاده از دستور زیر، سرویس‌ها متوقف شوند:

/etc/init.d/arcsight_services stop all

توقف ArcSight Manager:

/etc/init.d/arcsight_services stop manager

مسیر لاگ‌ها عبارت است از:

/opt/arcsight/manager/logs

در صورتی‌که هنگام اجرای ویزارد پیکربندی Manager خطایی رخ دهد مسیر لاگ‌های آن عبارت است از:

/opt/arcsight/manager/logs/default/serverwizard.log

در صورتی‌که با خطای Manager مواجه شدید فایل‌های ثبت وقایع آن در مسیر زیر ثبت می‌شوند:

ARCSIGHT_HOME>/logs/default/server.std.log

5 مراجع

[1] RepSM Plus Solution Guide
[2] ESM_101_6.9.1
[3] ESM_ArcSightConsole_UserGuide_6.9.1
[4] ESM_AdminGuide_6.9.1
[5] ESM_InstallGuide_6.9.1c
[6] https://marketplace.microfocus.com/arcsight/content/management-center-arcmc